Lyness Cycles, Elliptic Curves, and Hikorski Triples

Jonny Griffiths, mail@jonny-griffiths.net
MSc by Research in Mathematics
University of East Anglia, Norwich, UK
Department of Mathematics

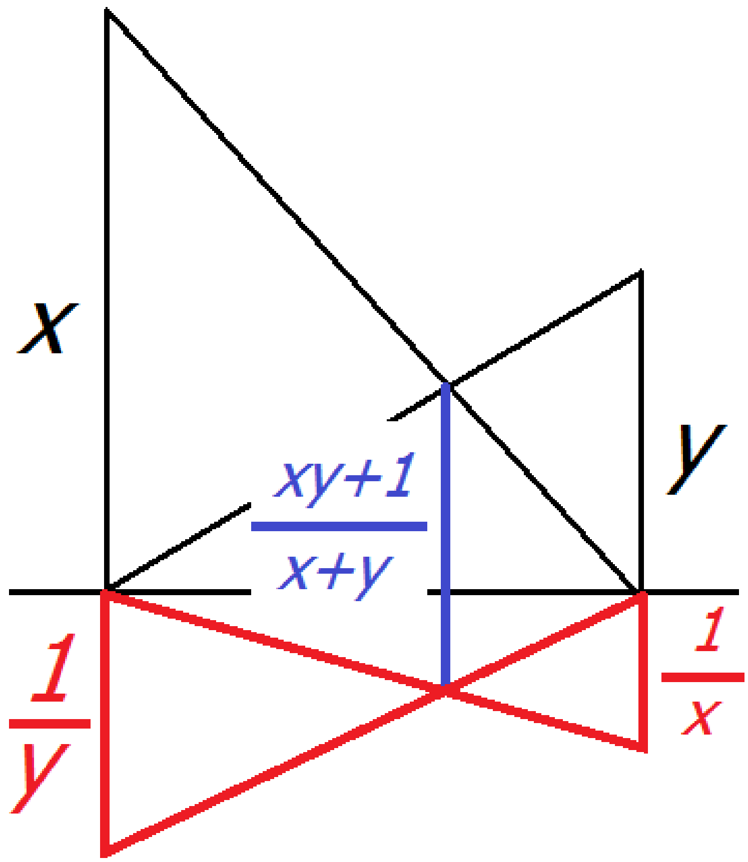
February 2012

Abstract

The heart of this thesis is an exploration of a new triple of natural numbers, $(a, b, \frac{ab+1}{a+b})$. These Hikorski Triples (or HTs) arise from a simple yet evocative mathematical situation, related to that leading to the cross-ratio function. There is also a link with the world of globally periodic recurrence relations, in that the order-2 recurrence

$$u_{n+2} = -\frac{u_{n+1}u_n + 1}{u_{n+1} + u_n}$$

is period-3 for all starting values u_0 and u_1 whose sum is not zero, and where $u_1 \neq \pm 1$. This is an example of a Lyness cycle; when the terms of such cycles are multiplied or added, they can give rise to elliptic curves, and a central part of this thesis is the way in which the periodicity of the cycles chosen correlates with the torsion of the elliptic curves generated (this work builds on that of John Silvester). Lyness cycles have links to the dilogarithm function, and also to Coxeter groups, where I extend the opening pages of an article by Sergey Fomin and Nathan Reading. Harold Edwards has recently proposed a new normal form for elliptic curves, which overlaps with the theory of HTs. In my final chapter I explore the way in which HTs form chains, that are related to the Chebychev polynomials and to the Dirichlet kernel.



Teach this triple truth to all:
a generous heart, kind speech,
and a life of service and compassion
are the things which renew humanity.

The Buddha

Acknowledgements

In 2009, Professor Graham Everest and I attended the same church. We talked a lot about maths together, and after he'd read an article I'd had published, he said, 'You should take your mathematics further'. He became my main supervisor at UEA in my first year, and his endless enthusiasm and vivid appreciation of mathematical beauty were a constant inspiration. Halfway through my course, his life was cut tragically short by cancer at the age of 52. This work is dedicated to his memory.

Professor Tom Ward supervised me throughout my time at UEA. Despite being Pro-Vice-Chancellor of the university, and thus a hugely busy man, Tom gave of his time for my project with great generosity, and his supervisions never failed to provide brilliant insight into what I was trying to do. As I began my work, Tom and Graham were happy for me to choose my own topic for research; this meant the material whenever I came to it was always alive, and I am grateful to them both for allowing me to take that risk.

Professor Shaun Stevens was kind enough to step into the breach after Graham's death, and his help swiftly became priceless. Whenever I came to Shaun with a problem, he was able in a few seconds to say something that reached to the heart of the matter. He also believed in me enough to set the bar high over the standards required for a thesis; if these pages read well mathematically, it is because of Tom and Shaun's refusal to accept anything second-rate.

I am also in debt to the members of the University of East Anglia Mathematics Department, for being perennially friendly and generous with their time and talent, and for taking me on in the first place, when that could have been seen as foolhardy at a time when places were precious. The department has shown me what true university mathematics entails, and I will be forever grateful. In particular, Dr Anish Ghosh kindly oversaw the assessment of my thesis, and he has my grateful thanks.

Bristol Grammar School supplied me with documents relating to R. C. Lyness, once their Head of Mathematics, and my thanks is due to Anne Bradley, their archivist. Lyness cycles were first introduced to me 34 years ago by Steve Russ, one of my sixth form mathematics teachers, now teaching at Warwick University. John Silvester at King's College, London once wrote an important note concerning Lyness cycles and elliptic curves which was sent to me by Ian Short of the Open University. Tony Barnard, also of King's College, London, sent me a helpful document about the period-5 cycle $x, y, \frac{y+1}{x}, \ldots$. Both Professor Igor Shparlinski and Professor Gerry Ladas kindly replied to my queries over Lyness cycles. At UEA, Dr Mark Cooker made an especially helpful comment about my final chapter. Dan Buck generously gave me advice over Latex and more. Professor Andy Hone travelled long distances to examine me for my viva, and his words and his detailed written comments transformed my understanding of the themes behind my work. To these teachers I offer my grateful thanks.

My day job for many years has been to teach at Paston College, and I am grateful to Peter Brayne and Ian Bloomfield in particular for arranging my timetable helpfully across my time at UEA. Enid, my grandmother, passed away in 2008 at the amazing age of 103, leaving a sum of money which meant that thankfully my tuition fees were covered; my gratitude goes to her. And finally, I thank Magzi, my soul-mate, who has done more than anyone else to make this thesis possible.

Copyright statement

Word Count – 30 000.

Notation

$a(n)$	the number of HTs with n as their highest element
$A = (A_n)$	the sequence A with terms $A_1, A_2, \ldots$
$\arg(z)$	the principal argument of the complex number z
$b(n)$	the number of HTs with n as their middle element
$\mathbb{C}$	the field of complex numbers
$\mathrm{C}(a,b,c,d)$	the cross-ratio of a, b, c and d, $\frac{(a-b)(c-d)}{(a-c)(b-d)}$
$c(n)$	the number of HTs with n as their smallest element
CTF	a cross-ratio-type function (see page 101)
$d(n)$	the number of (positive) divisors of n including n
$d \mid n$	d divides n
$d \nmid n$	d does not divide n
$D(x)$	the Wigner-Bloch dilogarithm function
$D_n(x) = D(n,x)$	the Dirichlet kernel of x
$\triangle$	the discriminant of an elliptic curve
$E(\mathbb{Q})$	the set of rational points on the elliptic curve E
$\mathbb{F}[u_1, u_2, \ldots, u_n]$	the set of polynomials in $u_1, u_2, \ldots, u_n$ with coefficients in the field $\mathbb{F}$
$\mathbb{F}(u_1, u_2, \ldots, u_n)$	the set of rational functions in $u_1, u_2, \ldots, u_n$ with coefficients in the field $\mathbb{F}$
F_i	the i^{th} Fibonacci number
$\gcd(a,b)$	the greatest common divisor of a and b
$h(n)$	the number of HTs in which n appears
HC	a Hikorski Chain (see page 181)
HT	a Hikorski Triple, that is, (a,b,c) or $\begin{pmatrix} a \\ b \\ c \end{pmatrix}$ where $c = \frac{ab+1}{a+b}$ and a, b and c are all positive integers with $a \geqslant b \geqslant c \geqslant 1$
HQ	a Hikorski Quartet (see page 184)
$\Im(z)$	the imaginary part of the complex number z
$j(E)$	the j-invariant of the elliptic curve E

$\mathrm{L_r}(z)$	the Rogers dilogarithm of z
$\mathrm{Li}_2(z)$	the dilogarithm of z
$\mathrm{Li}_3(z)$	the trilogarithm of z
$\ln(x)$	the natural logarithm of x
LHS	the left-hand side of an equation
LRS	a linear recurrence sequence
$m(P,c)$	the number of times the value c occurs in the LRS P
$m(P)$	the number of times 0 occurs in the LRS P
$\mathrm{MC}(a,b,c,d)$	the mini-cross-ratio function (see page 39)
$a_1 \equiv a_2 \pmod b$	b divides $a_1 - a_2$
MT	a Markov triple
$\mathbb{N}$	the set of natural numbers including 0
$\mathbb{N}^+$	the set of natural numbers not including 0
$\mathbb{O}$	the point at infinity for an elliptic curve
$\mathrm{OC}(a,b,c,d)$	the open cross-ratio function (see page 100)
order-n	describes a recurrence where the next term
	is expressed in terms of the previous n terms
$(\frac{p}{q})$	the Legendre symbol
period-n	describes a recurrence that is
	globally periodic with prime (minimal) period n
$PSL_2(\mathbb{F})$	the projective special linear group over the field $\mathbb{F}$
PT	a Pythagorean triple (primitive or otherwise)
$\Phi_K(x)$	the K^{th} cyclotomic polynomial
$\phi(x)$	the totient function,
	the number of $n, 0 < n < x$ so that $\gcd(n,x) = 1$
$\pi(x)$	the number of primes not exceeding x
$\mathbb{Q}$	the field of rational numbers
$\mathbb{Q}^*$	the field of rational numbers except for 0
$\mathbb{Q}(\sqrt{5})$	the field $\{a + b\sqrt{5} : a, b \in \mathbb{Q}\}$
$\mathbb{R}$	the field of real numbers
$\mathbb{R}^+$	the positive real numbers
rank-n	describes a Coxeter group of rank n
regular	a recurrence $u_1, u_2, \ldots, u_n, f(u_1, u_2, \ldots, u_n), \ldots$
	where $f \in \mathbb{Z}(u_1, u_2, \ldots, u_n)$ and f is a Mobius transformation
	in each of its arguments u_j
RHS	the right-hand side of an equation
$\mathrm{RMC}(a,b,c)$	the reduced mini-cross-ratio function (see page 42)

ROC(a, b, c)	the reduced open-cross-ratio function (see page 100)
$\sigma(n)$	the sum of the divisors of n including n
S_n	the symmetric group on a set of n elements
$T_n(x) = T(n, x)$	the Chebyshev polynomials of the first kind
T^R	the recurrence given by reversing T
UC	the uniqueness conjecture for HTs (see page 52)
$U_n(x) = U(n, x)$	the Chebyshev polynomials of the second kind
$\mathbb{Z}$	the ring of integers
$\mathbb{Z}^*$	the integers except for 0
z^*	the complex conjugate of z
$=_{ef}$	equality modulo the addition of elementary functions
$\bigoplus$	the direct product of two groups
$\bigotimes$	the pointwise product of two LRSs
$\sqcup$	the disjoint union of two sets

Contents

Chapter 1

Lyness Cycles

1.1 Periodic recurrence relations

Mathematics rolls on, even during a World War. In 1942, R.C. Lyness, a mathematics teacher at Bristol Grammar School, wrote to *The Mathematical Gazette*[42] concerning the recurrence relation

$$u_{n+1} = \frac{pu_n + p^2}{u_{n-1}}. \tag{1.1}$$

where p is a non-zero constant. He pointed out that the sequence created here is periodic with period 5 for all non-zero u_0 and u_1. Replacing u_k with an appropriate letter gives

$$x, y, \frac{py + p^2}{x}, \frac{p^2(x + y + p)}{xy}, \frac{px + p^2}{y}, x, y, \ldots. \tag{1.2}$$

With $p = 1$, we have

$$x, y, \frac{y + 1}{x}, \frac{x + y + 1}{xy}, \frac{x + 1}{y}, x, y, \ldots. \tag{1.3}$$

Such sequences Lyness called ‘cycles’ – besides the period-5 cycle above, he offered order-2 examples of periods 3, 4, and 6. All his cycles were of the form $x, y, f(x, y)$... with $f \in \mathbb{Z}(x, y)$. A 7-cycle had eluded him, and he asked if any reader could produce one.

These cycles will be the study of much of this thesis, and I must emphasize it is always *globally* periodic recurrences such as (1.1) that are considered, rather those that are only periodic for some particular starting values. If a cycle is described here as period-p, this should be understood as applying for any initial conditions, unless there are restrictions stated. Mestel [46] says

> *Globally periodic behaviour is very atypical of difference equations, and accordingly only a very restrictive class of functions* $[f(x, y)]$ *exhibit this behaviour.*

1.2 The Laurent Phenomenon

The recurrence (1.2) displays what is known as the *Laurent Phenomenon* [30]. A Laurent polynomial P in $u_1, u_2, u_3 \ldots, u_n$ is one whose terms are all multiples of powers of the various u_i, where the powers can be negative as well as positive, and where the coefficients come from some field $\mathbb{F}$. If the field is $\mathbb{Q}$, we have $P \in \mathbb{Q}[u_1^{\pm 1}, u_2^{\pm 1}, u_3^{\pm 1}, \ldots, u_n^{\pm 1}]$ for all $n \in \mathbb{Z}$. Thus we can write our recurrence relation (1.2) in Laurent polynomial form as

$$x, y, pyx^{-1} + p^2x^{-1}, p^2y^{-1} + p^2x^{-1} + p^3x^{-1}y^{-1}, pxy^{-1} + p^2y^{-1}, x, y, \ldots.$$

The celebrated Somos-4 recurrence relation may be defined by

$$w, x, y, z, \frac{xz + y^2}{w}, \frac{xyz + y^3 + wz^2}{wx},$$
$$\frac{x^3z^2 + 2x^2y^2z + xy^4 + wxyz^2 + wy^3z + w^2z^3}{w^2xy}, \ldots.$$

It transpires that every term (surprisingly) is a Laurent polynomial with integer coefficients in the variables w, x, y, z, despite the non-trivial denominator; as a consequence, if w, x, y and z are 1, then every term is an integer [31].

Hone [35] considers the order-3 recurrence

$$u_{n+3}u_n = u_{n+2}^2 + u_{n+1}^2 + \alpha, \tag{1.4}$$

and proves that this also possesses the Laurent property. If we say the first three terms are $u_0 = a, u_1 = b$ and $u_2 = c$, then the subsequent terms are

$$u_3 = \frac{b^2 + c^2 + \alpha}{a}, u_4 = \frac{a^2c^2 + b^4 + 2b^2c^2 + c^4 + \alpha(a^2 + 2b^2 + 2c^2) + \alpha^2}{a^2b},$$

$$u_5 = \frac{f(a,b,c)}{a^4b^2c}, u_6 = \frac{g(a,b,c)}{a^7b^4c^2}, \ldots$$

where f (with 29 terms) and g (with 104 terms) are polynomials in a, b and c (this last term is the surprising one, since $b^2 + c^2 + \alpha$ cancels, which means the sequence remains Laurent).

Now $R = \mathbb{Z}[a^{\pm 1}, b^{\pm 1}, c^{\pm 1}]$ is a unique factorisation domain, that is, it is a commutative ring where every element can be written uniquely as a product of irreducible (prime) elements. This means that we can consider the divisibility of the u_n modulo the monomials $a^j b^k c^l$ (which are all units in R). We proceed by induction. The statement S_n says

1. $u_i \in R$ for $0 \leqslant i \leqslant n+5$;
2. u_i, u_{i+1}, u_{i+2} for $0 \leqslant i \leqslant n+3$ are always pairwise coprime (modulo monomials); and
3. $u_{i\pm 1}^2 + \alpha$ for $0 \leqslant i \leqslant n+4$ are always coprime to u_i.

It is straightforward to check that S_1 is true. We may now assume S_n; to deduce S_{n+1} we need initially to show that $u_{n+6} \in R$.

Put $x = u_{n+1}, y = u_{n+2}$, and $z = u_{n+3}$.

Using (1.4), we have $x^2 + y^2 + \alpha = zu_n \equiv 0 \pmod{z}$.

Also $u_{n+4} \equiv \frac{y^2+\alpha}{x} \pmod{z}$, and $u_{n+5} \equiv \frac{y^4+\alpha(x^2+2y^2)+\alpha^2}{x^2y} \pmod{z}$. These give

$$\begin{aligned} u_{n+6}z &\equiv \frac{(y^2+\alpha)(x^2+y^2+\alpha)(y^4+\alpha(x^2+2y^2)+\alpha^2)}{x^4y^2} \pmod{z} \\ &\equiv 0 \pmod{z}, \end{aligned}$$

since $(x^2 + y^2 + \alpha) \equiv 0 \pmod{z}$. This means the z term will cancel exactly to give $u_{n+6} \in R$. Now

$$p \in R, p|u_{n+6}, p|u_{n+5} \Rightarrow p|(u_{n+6}u_{n+3} - u_{n+5}^2) \Rightarrow p|(u_{n+4}^2 + \alpha),$$

which implies by our induction hypothesis that p is trivial (a monomial). Similar arguments show that u_{n+6} and u_{n+4} are coprime, that $u_{n+5}^2 + \alpha$ and

u_{n+6} are coprime, and that $u_{n+6}^2 + \alpha$ and u_{n+5} are too. So by induction, $u_n \in R$ for all $n \in N$, and, given that we can reverse the recurrence, it follows that $u_n \in R$ for all $n \in \mathbb{Z}$.

1.3 Reversing the sequence

This mention of reversing the sequence deserves more attention. Let us examine the period-4 Lyness cycle

$$x, y, -\frac{(x+1)(y+1)}{y}, -\frac{x(y+1)+1}{x+1}, x, y, \ldots.$$

Can this be reversed? If so, we expect

$$y, x, -\frac{x(y+1)+1}{x+1}, -\frac{(x+1)(y+1)}{y}, y, x, \ldots$$

to be a periodic recurrence relation (which it is). Why? We can write

$$T : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} y \\ -\frac{(x+1)(y+1)}{y} \end{pmatrix}.$$

The periodic nature of the recurrence tells us $T^4 \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}$. We have

$$T^3 \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -\frac{x(y+1)+1}{x+1} \\ x \end{pmatrix}$$

which on iterating gives $T^6 \begin{pmatrix} x \\ y \end{pmatrix}, T^9 \begin{pmatrix} x \\ y \end{pmatrix}$ and $T^{12} \begin{pmatrix} x \\ y \end{pmatrix}$, which are

$$T^2 \begin{pmatrix} x \\ y \end{pmatrix}, T \begin{pmatrix} x \\ y \end{pmatrix}, \begin{pmatrix} x \\ y \end{pmatrix}$$

respectively. Thus $U : \begin{pmatrix} y \\ x \end{pmatrix} \mapsto \begin{pmatrix} x \\ -\frac{x(y+1)+1}{x+1} \end{pmatrix}$ (or $U' : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} y \\ -\frac{y(x+1)+1}{y+1} \end{pmatrix}$) is period-4, and a similar argument will show that any Lyness cycle of any period and any order can be reversed in this way. I will say the recurrence given by reversing T is T^R; clearly $(T^R)^R = T$.

1.4 Is x always followed by y?

Checking the Laurent property for a periodic recurrence relation (if one knows the period) involves simply a finite check. There is another property that Lyness cycles appear to possess, however, that can seem as mysterious as the Laurent one; if $u_n = u_0$, at any point, then it appears that without exception $u_{n+i} = u_i$, for $i \geqslant 0$. Consider the cycle

$$x, y, f_1(x, y), \ldots, f_i(x, y), f_{i+1}(x, y), \ldots, x, y, f_1(x, y), \ldots.$$

where $f_j(x, y) \in \mathbb{Q}(x, y)$ and where $f_i(x, y) = x$. It seems impossible for $f_{i+1}(x, y)$ to be a term other than y – why should this be?

Notice that if $f_1(x, y) \notin \mathbb{Q}(x, y)$, the phenomenon above does not always occur. Take the remarkable recurrence $x, y, |y| - x, \ldots$. This is globally period-9. If x is positive and y is negative, for example, with $x > -y$, then the sequence runs $x, y, -y - x, x, 2x + y, x + y, -x, -y, x - y, x, y, \ldots$. It transpires that for all permutations of the signs and relative sizes of x and y, the sequence remains period-9 [21]. Here we see that x is not immediately followed by y in every case.

1.5 Order-1, order-2 and order-3 regular cycles

Lyness cycles will be key to this thesis, especially those of the form

$$x, \frac{ax + b}{px + q}, \ldots, \tag{1.5}$$

an order-1 cycle, or

$$x, y, \frac{axy + bx + cy + d}{pxy + qx + ry + s}, \ldots, \tag{1.6}$$

an order-2 (or binary) cycle, or

$$x, y, z, \frac{axyz + bxy + cyz + dzx + ex + fy + gz + h}{pxyz + qxy + ryz + szx + tx + uy + vz + w}, \ldots, \tag{1.7}$$

an order-3 (or ternary) cycle, where all the coefficients are in $\mathbb{Q}$. Most of our examples will have integer coefficients; working over $\mathbb{Q}$ rather than $\mathbb{Z}$, however, has the advantage that $\mathbb{Q}$ is a field. The two are equivalent, since

$$f(u_1, u_2, \ldots, u_n) \in \mathbb{Q}(u_1, u_2, \ldots, u_n) \Leftrightarrow f(u_1, u_2, \ldots, u_n) \in \mathbb{Z}(u_1, u_2, \ldots, u_n).$$

This subset of Lyness cycles given by (1.5), (1.6) and (1.7) I will call *regular*; the recurrence is given in each case by a rational function whose elements are square-free in each of the starting terms. To put this another way, a recurrence $u_1, u_2, \ldots, u_n, f(u_1, u_2, \ldots, u_n), \ldots$ is regular if and only if $f \in \mathbb{Z}(u_1, u_2, \ldots, u_n)$ and f is a Mobius transformation in each of its arguments u_j. There are several reasons for choosing to work with regular cycles; one is that writing

$$\alpha = f(u_1, u_2, ...u_n) \tag{1.8}$$

where f is regular means that f is what I might call fully invertible, that is, we can always find the n inverses of f, given by making each u_i in turn the subject of (1.8), and moreover, these inverses will each be regular too. So if $z = f(u_1, u_2, ..., u_n)$ where f is regular then we can define $f_i^{-1}(u_1, ..., u_{i-1}, z, u_{i+1}, ..., u_n) = u_i$.

A second reason for concentrating on regular Lyness cycles is that there are two in particular that motivate this thesis. They are the period-3 cycle

$$x, y, -\frac{xy+1}{x+y}, x, y, \ldots,$$

and the period-6 cycle

$$x, y, \frac{xy-1}{x-y}, -x, -y, \frac{xy-1}{y-x}, x, y, \ldots.$$

These are related, in that

$$z = \frac{xy+1}{x+y} \Rightarrow x = \frac{yz-1}{y-z}, y = \frac{xz-1}{x-z}.$$

This pair of cycles will be a leitmotif running throughout these pages.

A third reason for studying regular cycles is that there is a cross-ratio method for generating periodic recurrence relations that we will study in Chapter 2. This method always, it seems, creates regular cycles.

Note that not all Lyness cycles are regular – for example, Lyness gives [42] the non-regular period-4 cycle

$$x, y, \frac{xy + y^2 - p}{x - y}, \frac{xy + x^2 - p}{y - x}, x, y, \ldots,$$

where the definition includes a y^2 term.

Note also that a cycle that is regular may contain later terms where the polynomials are not square-free. The period-8 cycle

$$x, y, z, \frac{y+z+1}{x}, \frac{xz+x+y+z+1}{xy}, \frac{y^2+xy+yz+zx+x+2y+z+1}{xyz},$$
$$\frac{xz+x+y+z+1}{yz}, \frac{x+y+1}{z}, x, y, z, \ldots. \tag{1.9}$$

(attributed to H. Todd) is regular, yet also includes a y^2 term.

1.6 The genesis of Lyness cycles

In a later note [43], Lyness reveals that he had chanced upon his period-5 cycle through investigating the following problem.

Find three distinct positive integers
so that the sum or difference of any pair is a square.

He claims to have found solutions (although he is tantalisingly quiet about what these might be!) He goes on to say

> *In examining these solutions I noticed that one could be derived from another by a certain substitution, and I thought at first by repeating this process I could get an infinite set of solutions.*

His plan failed, however; after four iterations, the first solution reappeared. He had found $a, b, c \in \mathbb{N}^+, a > b > c$ such that:

$$a + b = p^2, b + c = q^2, c + a = r^2, a - b = u^2, b - c = v^2, a - c = w^2 \tag{1.10}$$

for some integers p, q, r, u, v, w. Eliminating a, b, and c gives

$$p^2 - q^2 = w^2, p^2 - r^2 = v^2, r^2 - q^2 = u^2 \tag{1.11}$$

which implies that

$$u^2 + v^2 = w^2. \tag{1.12}$$

A solution in p, q, r, u, v, and w to any three of the four equations given by (1.11) and (1.12) will give us possible values for a, b and c. What was Lyness's iterative process (as developed with D. F. Ferguson [43])? Take these three equations in six variables:

$$p^2 - q^2 = w^2, p^2 - r^2 = v^2, v^2 - w^2 = u^2$$

Multiply the first by v^2, the second by w^2 and the third by p^2. This yields

$$(pv)^2 - (qv)^2 = (vw)^2, (pw)^2 - (rw)^2 = (vw)^2, (pv)^2 - (pw)^2 = (pu)^2$$

which is a triplet of equations, also in six variables. This second triplet can be written

$$(p')^2 - (v')^2 = (r')^2, (q')^2 - (u')^2 = (r')^2, (p')^2 - (q')^2 = (w')^2,$$

which is of the same form as (1.11), except that that $b > a > c$ this time. So if $\begin{pmatrix} p \\ q \\ r \\ u \\ v \\ w \end{pmatrix}$ is a solution to (1.10), then $\begin{pmatrix} pv \\ pw \\ vw \\ rw \\ qv \\ pu \end{pmatrix}$ is one too.

T^n	1	2	3	4	5
I	q	r	u	v	w
T	w/v	w	rw/v	q	u/v
T^2	$u/(qv)$	u/v	$uw/(qv)$	w/v	$rw/(qv)$
T^3	r/q	$rw/(qv)$	$ru/(qv)$	$u/(qv)$	u/q
T^4	v	u/q	rw/q	r/q	r
T^5	q	r	u	v	w

Table 1.1: Iterating T

What happens if we iterate this process? By switching to rational solutions to (1.10) without loss of generality, we can put $p = 1$, and then by dividing by v, we can make the top coordinate of each vector thereafter equal to 1 also. Now we can define $T : \begin{pmatrix} q \\ r \\ u \\ v \\ w \end{pmatrix} \mapsto \begin{pmatrix} w/v \\ w \\ rw/v \\ q \\ u/v \end{pmatrix}$; the iterations of T are given in Table 1.1. Columns 1 and 4 in particular took Lyness's eye. Column 4, for example, reads

$$v, q, \frac{w}{v}, \frac{u}{qv}, \frac{r}{q}, v, q, \ldots.$$

The similarity to (1.2) is clear. Lyness gives no exact details as to how he proceeds from here to the pentagonal cycle; it is fascinating to speculate how he might have proceeded. Say he realises that a periodic recurrence relation is in operation, and makes simplifying assumptions that allow him to carry out the calculation by hand. These might be that $w = f(v, q) = \alpha v + \beta q + \gamma$ for some constants α, β, and γ, and that the sequence reflects exactly by exchanging v with q, which means that u is symmetric in v and q, and that $r = f(q, v)$. The mathematics from here might have started by calculating

$$v, q, \frac{\alpha v + \beta q + \gamma}{v}, \frac{\alpha qv + \beta^2 q + v(\alpha\beta + \gamma) + \beta\gamma}{qv}, \ldots.$$

Equating coefficients of v and q in the fourth term gives $\alpha\beta + \gamma = \beta^2$ which yields the further simplification

$$v, q, \frac{\beta q + \alpha v - \alpha\beta + \beta^2}{v}, \frac{\alpha qv + \beta^2 q + \beta^2 v - \beta^2(\alpha - \beta)}{qv}, \ldots.$$

The next term is

$$\frac{-\alpha\beta q^2 - qv(\alpha^2 + \beta^2) + \beta q(\alpha^2 - \alpha\beta - \beta^2) - \beta^3 v + \beta^3(\alpha - \beta)}{-\beta q^2 - \alpha qv + \beta q(\alpha - \beta)},$$

and if we wish for the denominator here to be free from v, then $\alpha = 0$, which gives exactly cycle (1.2).

1.7 Lyness cycles and matrices

What if we 'take logs' with Lyness's iteration? Then

$$\begin{pmatrix} q \\ r \\ u \\ v \\ w \end{pmatrix} \to \begin{pmatrix} w/v \\ w \\ rw/v \\ q \\ u/v \end{pmatrix}$$

becomes

$$\begin{pmatrix} q \\ r \\ u \\ v \\ w \end{pmatrix} \to \begin{pmatrix} w - v \\ w \\ r + w - v \\ q \\ u - v \end{pmatrix}.$$

This gives us a linear transformation with matrix $A = \begin{pmatrix} 0 & 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & -1 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 \end{pmatrix}$, where $A^5 = I$.

While trying to replicate Lyness's period-5 iteration, I found that a period-2 cycle could have been produced by a similar path. Take

$$p^2 - q^2 = w^2, p^2 - r^2 = v^2, u^2 + v^2 = w^2.$$

Now multiply by v^2, w^2 and p^2 in turn, so the equations become

$$(pv)^2 - (qv)^2 = (vw)^2, (pw)^2 - (rw)^2 = (vw)^2, (pu)^2 + (pv)^2 = (pw)^2,$$

or

$$(w')^2 - (u')^2 = (v')^2, (p')^2 - (r')^2 = (v')^2, (q')^2 + (w')^2 = (p')^2,$$

which can be rewritten as

$$(p')^2 - (q')^2 = (w')^2, (p')^2 - (r')^2 = (v')^2, (u')^2 + (v')^2 = (w')^2.$$

So if $\begin{pmatrix} p \\ q \\ r \\ u \\ v \\ w \end{pmatrix}$ is a solution, then $\begin{pmatrix} pw \\ pu \\ rw \\ qv \\ vw \\ pv \end{pmatrix}$ is one too. If we iterate this as before, putting p equal to 1 and dividing by w, we arrive at the involution $U : \begin{pmatrix} q \\ r \\ u \\ v \\ w \end{pmatrix} \mapsto \begin{pmatrix} u/w \\ r \\ qv/w \\ v \\ v/w \end{pmatrix}$, where $\begin{pmatrix} 0 & 0 & 1 & 0 & -1 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & -1 \end{pmatrix}^2 = I$. This suggests the period-2 Lyness cycle $w, \frac{v}{w}, w \ldots$. So period-2 and period-5 cycles are evident in this situation; are any other periods possible?

1.8 Lyness the teacher

Robert Cranston Lyness was a Head of Mathematics at Bristol Grammar School, before becoming a member of Her Majesty's Inspectors of Schools. He also oversaw many of the young British teams that travelled to International Mathematics Olympiads. Dr Bob Burn remembers being inspected by him – Lyness asked if he knew of Klein's *Elementary Mathematics from an Advanced Viewpoint*. Bob replied that he owned a copy, and that it was one of his favourite books, whereupon Lyness immediately signed off his department with a Grade 1! The Nobel prize-winning theoretical chemist Sir John Pople was taught by Lyness at Bristol Grammar School, and in his autobiography [50] he describes being prepared by him for a scholarship in mathematics at Cambridge University.

> *During the remaining two years at BGS, I received intense personal coaching from Lyness and the senior physics master, T.A. Morris. Both were outstanding teachers.*

Lyness successfully combined life as a school-teacher with research into mathematics; as I try to do the same, he is thus an inspiration. (I would note too that Weierstrass spent 15 years as a school-teacher.) Although Lyness may not have been the first to discover these cycles, he was the first to bring

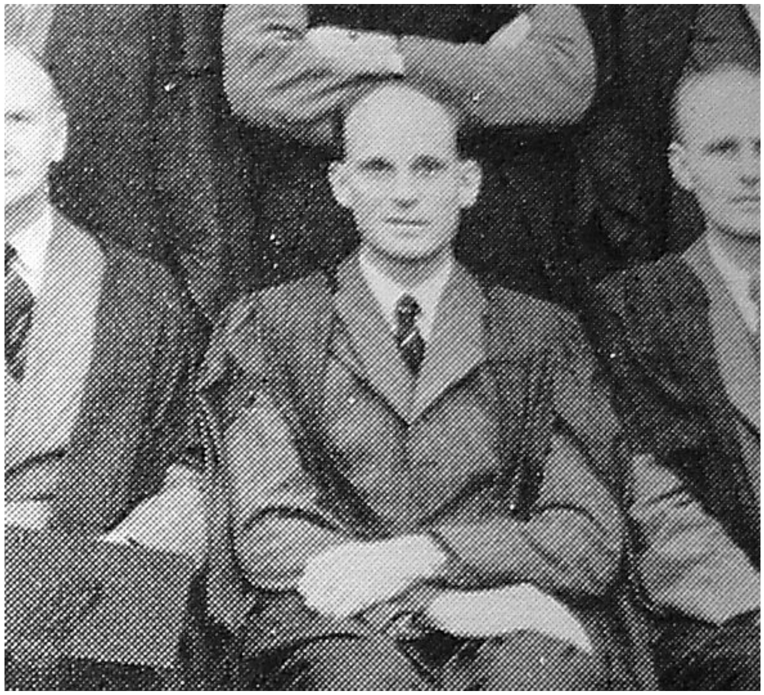


Figure 1.1: Robert Cranston Lyness

them to the attention of the broader mathematical community, and they now widely bear his name. Don Zagier once approached these cycles from a slightly different angle in the following words [62], and it is in this spirit that my thesis is written:

> *Imagine you have series of numbers such that if you add 1 to any number, you get the product of its left and right neighbours. Then this series will repeat itself at every fifth step! The difference between a mathematician and a non-mathematician is not just being able to discover something like this, but to care about it and to be curious why it's true, what it means and what other things it might be connected with. In this particular case, the statement itself turns out to be connected with a myriad of deep topics in advanced mathematics: hyperbolic geometry, algebraic K-theory, and the Schrodinger equation of quantum mechanics. I find this kind of connection between very elementary and very deep mathematics overwhelmingly beautiful.*

Chapter 2

The Cross-Ratio Method

So how did Lyness's cycles become much more than a soon-to-be-forgotten curiosity? In 1961, his work was resurrected by W.W. Sawyer, of *Mathematician's Delight* fame, who wrote to *The Mathematical Gazette* [51] to add to Lyness's note with a novel method for using the cross-ratio to produce cycles.

2.1 The Cross-ratio

Now the cross-ratio of four numbers a, b, c, and d is defined as

$$\mathrm{C}(a, b, c, d) = \frac{(a-b)(c-d)}{(a-c)(b-d)}$$

This function of four variables arises naturally in projective geometry. In Figure 2.1, elementary coordinate geometry enables us to calculate $\frac{AB.CD}{AC.BD}$, which simplifies to $\frac{(a-b)(c-d)}{(a-c)(b-d)}$. This (remarkably) is independent of both m and k; choose any straight line to fall across the four lines that have the origin as a common point, and the cross-ratio remains invariant.

The cross-ratio function also appears naturally in the study of Mobius transformations. There we have the fundamental theorem that given any three points in $\mathbb{C}$, say z_1, z_2 and z_3, there exists a Mobius transformation $h(z)$ mapping these points to any three points in $\mathbb{C}$, say w_1, w_2 and w_3. We can see this since $f(z) = \frac{(z-z_1)(z_2-z_3)}{(z-z_2)(z_1-z_3)}$ maps z_1, z_2 and z_3 to $0, \infty$ and 1 respectively, and $g(w) = \frac{(w-w_1)(w_2-w_3)}{(w-w_2)(w_1-w_3)}$ maps w_1, w_2 and w_3 to $0, \infty$ and 1

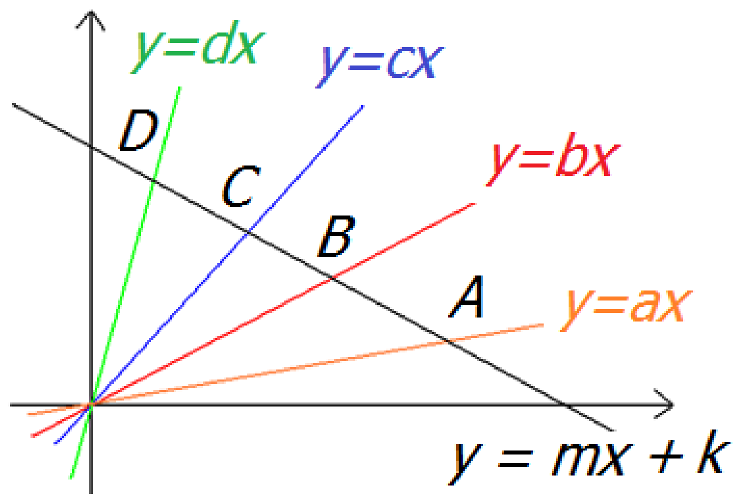


Figure 2.1: The cross-ratio

respectively, so to find $h(z)$, we can compose $f(z)$ with $g^{-1}(z)$ (which is also a Mobius transformation.) Thus to find $h(z)$, we need to solve

$$\frac{(z-z_1)(z_2-z_3)}{(z-z_2)(z_1-z_3)} = \frac{(w-w_1)(w_2-w_3)}{(w-w_2)(w_1-w_3)}$$

for w. One pleasing fact; the cross-ratio of four complex numbers is real if and only if the four complex numbers lie on a circle or straight line. The cross-ratio is also invariant under inversion; indeed, it is invariant under any Mobius transformation.

2.2 Generating Lyness cycles with the cross-ratio, including those with parameters

So what possible relevance could the cross-ratio have to our study of Lyness cycles? Suppose we say

$$x = \mathrm{C}(a,b,c,d), y = \mathrm{C}(b,c,d,e), z = \mathrm{C}(c,d,e,a). \tag{2.1}$$

Use the first equation to find a, and the second to find e. What does this give for z when we substitute in? Perhaps surprisingly, b, c, and d all cancel completely to give $z = \frac{x+y-1}{x-1}$. Is this a cycle? If it is, given the way we have cycled a to e, it will surely be period-5, and checking shows that that is indeed what we have:

$$x, y, \frac{x+y-1}{x-1}, \frac{xy}{(x-1)(y-1)}, \frac{x+y-1}{y-1}, x, y, \ldots. \tag{2.2}$$

What happens if we permute a, b, c and d here? We get the six period-5 cycles

$$x, y, \frac{x+y-1}{x-1}, \cdots, \quad \text{and} \quad x, y, \frac{xy-y}{xy-x-y}, \cdots, \quad \text{and} \quad x, y, \frac{1-y}{x}, \cdots,$$

$$x, y, \frac{x-1}{xy-1}, \cdots, \quad \text{and} \quad x, y, \frac{y}{xy-x}, \cdots, \quad \text{and} \quad x, y, \frac{xy-1}{xy-y}, \cdots, \tag{2.3}$$

which are all regular. Can we generate our original pentagonal recurrence (1.3) in this way? By adding a minus sign, we can. Write

$$x = -\,\mathrm{C}(a, d, c, b), y = -\,\mathrm{C}(b, e, d, c), z = -\,\mathrm{C}(c, a, e, d). \tag{2.4}$$

This time $z = \frac{y+1}{x}$. So far, so good; but how do we derive the version of our pentagonal recurrence (1.1) that includes a parameter? Our success with the minus sign in (2.4) suggests we experiment by rewriting our cross-ratio equations as

$$x = -p\,\mathrm{C}(a, d, c, b), y = -p\,\mathrm{C}(b, e, d, c), z = -pC(c, a, e, d).$$

This does indeed add the parameter p to our cycle, giving exactly (1.2), and returning to (2.2), if $x = p\mathrm{C}(a, b, c, d), y = p\mathrm{C}(b, c, d, e)$ and $z = p\mathrm{C}(c, d, e, a)$ we get

$$x, y, \frac{p(x+y-p)}{x-p}, \frac{pxy}{(x-p)(y-p)}, \frac{p(x+y-p)}{y-p}, x, y, \ldots. \tag{2.5}$$

Notice the homogenizing effect that introducing p has here – adding the degrees of x, y and p in each term for the numerator yields a constant, and likewise for the denominator.

As a further experiment, it seems worthwhile to investigate

$$x = p + \mathrm{C}(a, b, c, d), y = p + \mathrm{C}(b, c, d, e), z = p + \mathrm{C}(c, d, e, a).$$

Curiously, this once again yields a cycle free of a, b, c, d, and e, namely

$$x, y, \frac{x(p+1)+y-(p^2+3p+1)}{x-p-1},$$
$$\frac{(p+1)xy-p(p+2)x-p(p+2)y-(p^2+3p+1)}{(x-p-1)(y-p-1)},$$
$$\frac{x+y(p+1)-(p^2+3p+1)}{y-p-1}, x, y \ldots.$$

This is significantly different to (2.5), since it is not homogeneous in x, y and p.

How many parameters can we add like this? A further experiment suggests itself. Putting

$$x = \frac{p\,\mathrm{C}(a,b,c,d)+q}{r\,\mathrm{C}(a,b,c,d)+s}, y = \frac{p\,\mathrm{C}(b,c,d,e)+q}{r\,\mathrm{C}(b,c,d,e)+s}, z = \frac{p\,\mathrm{C}(c,d,e,a)+q}{r\,\mathrm{C}(c,d,e,a)+s},$$

we arrive at the regular period-5 cycle with four parameters that begins

$$x, y,$$
$$\frac{rxy(p(r+2s)+q(r+s))-px(p(r+s)+q(2r+s))-y(p^2(r+s)+2pqr+q^2r)+p(p^2+3pq+q^2)}{rxy(r^2+3rs+s^2)-x(p(r^2+2rs+s^2)+qr^2)-ry(p(r+2s)+q(r+s))+p(p(r+s)+q(2r+s))}, \ldots.$$

Of course, we do not quite have four parameters here; there is some duplication, since (kp, kq, kr, ks) will produce the same result as (p, q, r, s). To deal with this, we need to form the quotient group $GL_2(\mathbb{Q})/N$ where N is the normal subgroup formed by the set of scalar multiples of the identity matrix with matrix multiplication. This is dealt with more fully in Chapter 7; for the moment, we will live with the duplication we have here.

2.3 Conjugate Lyness cycles

Suppose that $x = 2, y = 3$ and $p = 1$ in (1.2). Then on substituting in, we get the periodic sequence $2, 3, 2, 1, 1, 2, 3, \ldots$. Suppose now that we multiply these terms by 4, and then add 5. We get $13, 17, 13, 9, 9, 13, 17 \ldots$ – can we find a regular order-2, period-5 Lyness cycle (with integer coefficients) that generates this sequence? It turns out that we can. We start with (1.3).

Multiplying the terms by 4 gives $4x, 4y, 4\frac{y+1}{x}, 4\frac{x+y+1}{xy}, 4\frac{x+1}{y}, 4x, 4y \ldots$. Now put $x' = 4x, y' = 4y$ and substitute, to get

$$x', y', \frac{4y'+16}{x'}, \frac{16x'+16y'+64}{x'y'}, \frac{4x'+16}{y'}, x', y', \ldots$$

Being a periodic sequence is trivially preserved here, but the property of being a periodic recurrence relation is too. Now adding 5 onto each of these terms gives

$$x'+5, y'+5, \frac{4y'+16}{x'}+5, \frac{16x'+16y'+64}{x'y'}+5, \frac{4x'+16}{y'}+5, x', y', \ldots.$$

Putting $x'' = x'+5, y'' = y'+5$ and substituting gives

$$x'', y'', \frac{5x''+4y''-29}{x''-5}, \frac{5x''y''-9x''-9y''+29}{(x-5)(y-5)}, \frac{4x''+5y''-29}{y''-5}, x'', y'' \ldots$$

which again works perfectly well as a recurrence relation.

Let us consider this phenomenon more generally. (Note that an arithmetic progression remains arithmetic when terms are multiplied by p and increased by q, but the same cannot be said for geometric progressions. If we multiply each term of the Somos-4 recurrence relation by p and then add q then the Laurent property disappears, since the denominator includes terms such as $(w'-q)$.)

Suppose we return to our transformation $T : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} y \\ f(x,y) \end{pmatrix}$, where the recurrence generated is period-n and regular. Now choose $u(x) \in \mathbb{Q}(x)$ where u is invertible (the only possibility for u in this case is to be a Mobius transformation.) Define $U : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} u(x) \\ u(y) \end{pmatrix}$. Figure 2.2 shows how our functions now combine. Our assertion is that the recurrence t as defined in Figure 2.2 is also period-n. This is self-evident, since t is conjugate to T, and $t^n = (U^{-1}TU)^n = U^{-1}T^nU = I$. This argument is easily extended for orders higher than 2. One special case deserves attention – when $u(x)$ is $\frac{1}{x}$. This gives us the initially startling fact that if $x, y, f(x,y), \ldots$ is a period-n cycle, then $x, y, \frac{1}{f(\frac{1}{x},\frac{1}{y})}, \ldots$ will be too. The question of conjugacy and recurrences is considered in a recent paper by Cima, Gasull, and Manosas [20].

$$
\begin{tikzcd}
\begin{pmatrix} x \\ y \end{pmatrix} \arrow[r, "t"] \arrow[d, "U"] & \begin{pmatrix} y \\ u^{-1}(f(u(x),u(y))) \end{pmatrix} \\
\begin{pmatrix} u(x) \\ u(y) \end{pmatrix} \arrow[r, "T"] & \begin{pmatrix} u(y) \\ f(u(x),u(y)) \end{pmatrix} \arrow[u, "U^{-1}"']
\end{tikzcd}
$$

Figure 2.2: Conjugacy at work

One immediate question now is, how many conjugacy classes do we have? The answer to this question is not completely straightforward, but the six cycles generated by the cross-ratio method in (2.3) are certainly all conjugate, and in these cases $u(\lambda)$ runs through the six functions

$$\lambda, \frac{1}{\lambda}, 1-\lambda, \frac{1}{1-\lambda}, \frac{\lambda-1}{\lambda}, \frac{\lambda}{\lambda-1}. \tag{2.6}$$

The group given by regarding these values as functions with the binary operation of composition is isomorphic to the symmetric group S_3; Lewin [41] calls this group 'the harmonic group of automorphic functions'. These six functions are certainly bijections from $\mathbb{C}$ together with the point at infinity to itself. The element λ has order 1, the elements $\frac{1}{\lambda}, 1-\lambda$ and $\frac{\lambda}{\lambda-1}$ have order 2, while $\frac{1}{1-\lambda}$ and $\frac{\lambda-1}{\lambda}$ each have order 3. The pair $\frac{1}{\lambda}$ and $1-\lambda$ together generate the group, as do other pairings (note the pair of transformations $-\frac{1}{\lambda}$ and $1+\lambda$ together generate the modular group, which is infinite). If $C(a,b,c,d)=\lambda$, then as a,b,c,d permute, the cross-ratio takes exactly the values in (2.6), each value four times. There is another way to look at this; we could say that the symmetric group S_4 acts on the cross-ratio by permuting a,b,c and d. The kernel of this group action is isomorphic to K, the Klein four-group; it consists of the permutations of order 2 such as $(ab)(cd)$ that leave the cross-ratio unchanged. The symmetry group is then S_4/K, which is isomorphic to S_3.

2.4 Using conjugacy to add parameters

Conjugacy gives us now another way to introduce parameters to a recurrence relation, this time for any period. Suppose we choose the period-6 cycle

$$x, y, \frac{y}{x}, \frac{1}{x}, \frac{1}{y}, \frac{x}{y}, x, y \ldots.$$

Define $U : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} \frac{px+q}{rx+s} \\ \frac{py+q}{ry+s} \end{pmatrix}$. Then $U^{-1} : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} \frac{q-sx}{rx-p} \\ \frac{q-sy}{ry-p} \end{pmatrix}$ and

$$U^{-1}TU \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} y \\ \frac{prxy(s-q)+qsx(r-p)+y(ps^2-q^2r)+qs(s-q)}{prxy(p-r)+x(p^2s-qr^2)+pry(q-s)+qs(p-r)} \end{pmatrix}.$$

Now $x, y, \frac{prxy(s-q)+qsx(r-p)+y(ps^2-q^2r)+qs(s-q)}{prxy(p-r)+x(p^2s-qr^2)+pry(q-s)+qs(p-r)}, \ldots$ is a period-6 cycle with four parameters (once again we have some duplication).

I will now add one more reason for studying regular cycles to those given on page 17; the conjugate of a regular cycle is itself regular. Conjugating $\frac{a_1xy+a_2x+a_3y+a_4}{b_1xy+b_2x+b_3y+b_4}$ gives the recurrence relation that begins

$$x, y, \frac{c_1xy + c_2x + c_3y + c_4}{d_1xy + d_2x + d_3y + d_4}, \ldots,$$

where $c_i, d_i \in \mathbb{Z}[a_j, b_k]$. This applies for all orders. So the regularity property for recurrences is invariant under conjugation.

2.5 Dual cycles

It is helpful now to introduce the idea of a 'dual' cycle. Take our pentagonal recurrence (1.2) once again. If we put $X = x$, then skip a term, then put $Y = \frac{py+p^2}{x}$, then skip a term again – what is $\frac{px+p^2}{y}$ in terms of X and Y? The answer is $\frac{p^2(X+p)}{XY-p^2}$. The same thing happens if we skip *two* terms each time, putting

$$X = x, Y = \frac{p^2(x+y+p)}{xy}, \quad \text{and} \quad Z = y.$$

We find that Z is $\frac{p^2(X+p)}{XY-p^2}$, and we can easily confirm that this gives the period-5 cycle

$$X, Y, \frac{p^2(X+p)}{XY-p^2}, \frac{XY-p^2}{p}, \frac{p^2(Y+p)}{XY-p^2}, X, Y \ldots.$$

What happens if we take the dual of this dual cycle? We return (whether skipping one or two terms) to our original pentagonal recurrence (1.2), so the dual of the dual is the original; our use of term 'dual' is justified. This idea of duality appears to hold for all period-5 cycles.

What happens if you apply this 'dual cycle' idea to other periods? Period-3 binary regular cycles are self-dual, a binary period-4 recurrence T has T^R as the only possible candidate for its dual, while the duality concept does not seem to apply sensibly to period-6 recurrences.

The six cycles generated in (2.3) fall neatly into the three pairs

$$x, y, \frac{x+y-1}{x-1}, \ldots \quad \text{and its dual} \quad x, y, \frac{xy-y}{xy-x-y}, \ldots,$$

$$x, y, \frac{1-y}{x}, \ldots, \quad \text{and its dual} \quad x, y, \frac{x-1}{xy-1}, \ldots,$$

and

$$x, y, \frac{y}{xy-x}, \ldots, \quad \text{and its dual} \quad x, y, \frac{xy-1}{xy-y}, \ldots.$$

2.6 Extending the cross-ratio method

Lyness was quick to notice [44] that Sawyer's cross-ratio method could be extended for other orders. Suppose we say

$$x = \frac{(a-b)(c-d)}{(a-c)(b-d)}, y = \frac{(b-c)(d-e)}{(b-d)(c-e)},$$
$$z = \frac{(c-d)(e-f)}{(c-e)(d-f)}, \alpha = \frac{(d-e)(f-a)}{(d-f)(e-a)}.$$

This produces the order-3 period-6 cycle

$$x, y, z, \frac{x+y+z-xz-1}{x+y-1}, \frac{xyz}{(x+y-1)(y+z-1)},$$

$$\frac{x+y+z-xz-1}{y+z-1}, x, y, z \ldots.$$

So the cross-ratio method works perfectly, it seems, for order-n period-$(n+3)$ cycles. For recurrence relations starting $w, x, y, z, f(w, x, y, z), \ldots$ it yields this order-4 period-7 cycle

$$\begin{gathered} w, x, y, z, \frac{w+x+y+z-xz-wy-wz-1}{x+y+w-wy-1}, \\ \frac{-wxyz}{(x+(1-w)(y-1))(x(z-1)-y-z+1)}, \\ \frac{w+x+y+z-xz-wy-wz-1}{x+y+z-xz-1}, w, x, y, z, \ldots, \end{gathered} \tag{2.7}$$

a partial reply to Lyness's request.

2.7 Searching for Lyness cycles using a computer

But is it possible for a regular *binary* recurrence relation to be period-7? Why not search with the aid of a computer? It is straightforward to generate some code (using Visual Basic in Excel below) for finding cycles, albeit in a rather ad hoc and far from comprehensive way. The following program checks whether or not we can find small integer values for a to u so that the binary recurrence

$$x, y, \frac{px^2+qxy+ry^2+sx+ty+u}{ax^2+bxy+cy^2+dx+ey+f} \cdots$$

is period-12 (note that this spreads the net wider than simply searching for regular recurrences).

```
   NOTE: n IS THE ROW FOR THE PRINTOUT
n = 2

   NOTE: SET UP POSSIBLE VALUES FOR a TO u
For a = −1 To 1
...
```

For $u = -1$ To 1

`NOTE: SET UP ARRAY OF VALUES FOR` $i(n)$
Dim $i(21)$
Dim j As Integer
For $j = 0$ To 20
$i(j) = j$
Next j

`NOTE: SENSIBLE CHOICE OF INITIAL VALUES`
$i(0) = 3.4$
$i(1) = 4.2$

`NOTE: RUN THE RECURRENCE RELATION`
For $m = 0$ To 18
$x = i(m)$
$y = i(m+1)$
If $(a * x^2 + b * x * y + c * y^2 + d * x + e * y + f) = 0$ Or Abs $(x) > 10000$ Or Abs $(y) > 10000$ Then
Else
$i(m+2) = (p * x^2 + q * x * y + r * y^2 + s * x + t * y + u)/(a * x^2 + b * x * y + c * y^2 + d * x + e * y + f)$
End If
Next m

`NOTE: SET SEARCH PERIOD AND CHECK SMALLER PERIODS DO NOT APPLY`
If $i(12) = 3.4$ And $i(2) <> 3.4$ And $i(3) <> 3.4$ And $i(4) <> 3.4$ And $i(6) <> 3.4$ Then
$n = n + 1$

`NOTE: PRINT POSSIBLY SUCCESSFUL VALUES FOR` a `TO` u
Cells(n, 1).Value $= a$
...
Cells(n, 12).Value $= u$
End If

```
NOTE: RUN A CHECK ON PROGRESS OF PROGRAM
Cells(3, 13).Value = a
...
Cells(3, 18).Value = f

NOTE: NEXT u TO a
Next u
...
Next a
```

Running this for small values of a to u suggests tentatively that 2, 3, 4, 5 and 6 are the only possible periods for binary rational Lyness cycles of the form checked here.

This program provides much output from what I call *pseudo-cycles* - when copies of a cycle are interwoven to produce a cycle of increased order and period. For example, if we take two copies of the the order-1 period-2 cycle $x, -x, x, \ldots$ and interweave them, we produce the order-2 period-4 binary pseudo-cycle $x, y, -x, -y, x, \ldots$. Since (as we shall see in Chapter 7) order-1 cycles with rational coefficients can be of period 2, 3, 4, and 6, these give binary pseudo-cycles of periods 4, 6, 8 and 12, and ternary pseudo-cycles of periods 6, 9, 12 and 18. It should be clear that given an order-m, period-n cycle, there is an order-(km) period-(kn) pseudo-cycle for all $k \geqslant 2$. The apparent triviality of the pseudo-cycles does not mean that they are worthless; their terms can add to create elliptic curves in a way we shall explore in Chapter 9.

The information on cycles we have so far is summarised in Table 2.1, where $\times$ indicates that as long as we insist that our coefficients be integer, or equivalently rational, no example has yet been found. If we allow our coefficients to come from the field $\mathbb{R}$, then any period is possible; the binary recurrence relation $x, y, ky - x, \ldots$, for example, can take any period we wish if we choose $k \in \mathbb{R}$ carefully [33]. For example, suppose we ask here for a period-7 cycle; it transpires after applying the recurrence repeatedly that k must be a root of $k^6 - 5k^4 + 6k^2 - 1$, and on solving, $k = -1.8019...$ is one of six possible values.

We are still left wondering over Lyness's challenge to produce a period-7 binary cycle with rational coefficients; can a proof of the impossibility of this be found? Kulenovic and Ladas [38] provide this for a special class of rational function recurrences.

Theorem 2.1. *Suppose that the binary recurrence defined by*

$$z = \frac{\alpha + \beta y + \gamma x}{A + By + Cx}, \quad or \quad x_n = \frac{\alpha + \beta x_{n-1} + \gamma x_{n-2}}{A + Bx_{n-1} + Cx_{n-2}}, \tag{2.8}$$

where $\alpha, \beta, \gamma, A, B,$ *and* C *are all non-negative real constants, defines a period-*p *cycle for all non-negative starting values for* x *and* y*. Then*

1. $C > 0 \Rightarrow A = B = \gamma = 0.$

2. $C = 0 \Rightarrow \gamma(\alpha + \beta) = 0.$

Proof. Choose $x_{-1} = 1$, so $x_{-1} = x_{p-1} = 1$. We have

$$x_p = \frac{\alpha + \beta + \gamma x_{p-2}}{A + B + Cx_{p-2}} = x_0.$$

This gives

$$(A + B)x_0 + (Cx_0 - \gamma)x_{p-2} = \alpha + \beta. \tag{2.9}$$

If $C > 0$ and $A + B > 0$, then choosing $x_0 > \max\{\frac{\alpha+\beta}{A+B}, \frac{\gamma}{C}\}$ means that (2.9) is impossible. So if $C > 0, A = B = 0$. If now $\gamma > 0$, then choosing $x_0 < \frac{\gamma}{C}$ makes (2.9) impossible once more. If $C = 0$ and $\gamma(\alpha + \beta) > 0$ then we can choose x_0 to be sufficiently small to make (2.9) impossible again. $\square$

So the possible recurrences become $x, y, \frac{\alpha+\beta y}{Cx}, \cdots$, and $x, y, \frac{\alpha+\beta y}{A+By}, \cdots$, and $x, y, \frac{\gamma x}{A+By}, \cdots$. These yield (to within a linear change of variables $x_n = \lambda X_n$) the cycles

$$x, \frac{1}{x}, x, \cdots, \quad \text{and} \quad x, y, \frac{1}{x}, \frac{1}{y}, x, \cdots, \quad \text{and} \quad x, y, \frac{y+1}{x}, \cdots, \quad \text{and} \quad x, y, \frac{y}{x}, \cdots,$$

but, it seems, nothing more. Thus the only possible values for p are 2, 4, 5 and 6 ($p = 3$ requires negative coefficients). Kulenovic and Ladas [38] leave the following as an open problem; if (2.8) converges to a period-p solution, is $p \in \{2, 4, 5, 6\}$?

Period	Order-1 (example)	Order-2 (example)	Order-3 (example)
1	x	$\times$	$\times$
2	$-x$	x	$\times$
3	$\frac{x-3}{x+1}$	$-x-y$	x
4	$\frac{x-1}{x+1}$	-$\frac{(x+1)(y+1)}{y}$	$-x-y-z$
5	$\times$	$\frac{y+1}{x}$	$-\frac{(z+1)(x(y+1)+1)}{x(y+1)(z+1)+z}$
6	$\frac{2x-1}{x+1}$	$\frac{y}{x}$	$\frac{-xy-yz-x-y-z-1}{z}$
7	$\times$	$\times$	$\times$
8	$\times$	$\frac{x-1}{x+1}$	$\frac{y+z+1}{x}$
9	$\times$	$\times$	$\frac{x-3}{x+1}$
10	$\times$	$\times$	$\frac{yz+1}{xyz}$
11	$\times$	$\times$	$\times$
12	$\times$	$\frac{2x-1}{x+1}$	$\frac{xy+y+z}{x-z}$
13	$\times$	$\times$	$\times$
14	$\times$	$\times$	$\times$
15	$\times$	$\times$	$\times$
16	$\times$	$\times$	$\times$
17	$\times$	$\times$	$\times$
18	$\times$	$\times$	$\frac{2x-1}{x+1}$

Table 2.1: Examples of order-1, order-2 and order-3 Lyness cycles

Chapter 3

A New Integer Triple

3.1 The initial problem

Mathematics is full of natural number triples. The most famous are the Pythagorean Triples (where (a, b, c) satisfies $a^2 + b^2 = c^2$), but there are Amicable Triples (where (a, b, c) satisfies $\sigma(a) = \sigma(b) = \sigma(c) = a + b + c$), Markov Number Triples (where (a, b, c) satisfies $a^2 + b^2 + c^2 = 3abc$), triples that arise from the Euler Brick problem ((a, b, c) where $a^2 + b^2, b^2 + c^2$ and $c^2 + a^2$ are all squares) and so on. (We could now add Lyness Triples (a, b, c), where $a > b > c$ and $a + b, b + c, c + a, a - b, b - c$ and $a - c$ are all squares.) I propose here a new triple of positive integers, that arises naturally from the following problem.

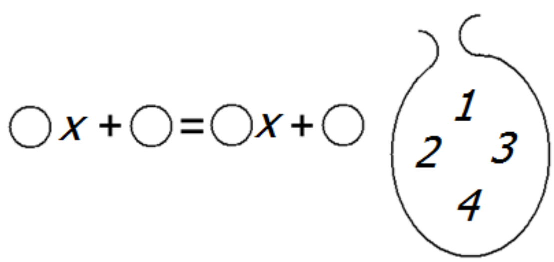


Figure 3.1: Numbers in a bag

Put the numbers in the bag into the circles
in any way you choose (no repeats!)

Solve the resulting equation.
What solutions are possible as you choose different orders?
What happens if you vary the numbers in the bag,
keeping them as distinct integers?

Suppose a, b, c, and d are in the bag. If $ax + b = cx + d$, then the solution to this equation is $x = \frac{d-b}{a-c}$. There are 24 possible equations, but they occur in pairs, for example, $ax + b = cx + d$ and $cx + d = ax + b$ will have the same solution. So there are a maximum of twelve distinct solutions, and this maximum is possible; for example, if $1, 2, 3$ and 8 are in the bag, then the solution set S is

$$\left\{3, 5, 7, -3, -5, -7, \frac{1}{3}, \frac{1}{5}, \frac{1}{7}, -\frac{1}{3}, -\frac{1}{5}, -\frac{1}{7}\right\}. \tag{3.1}$$

This suggests that if x is a solution to one of the equations, then $\frac{1}{x}, -x$ and $-\frac{1}{x}$ will be solutions to three of the others, and this is true, since if $ax + b = cx + d$, then

$$b\left(\frac{1}{x}\right) + a = d\left(\frac{1}{x}\right) + c, c(-x) + b = a(-x) + d, b\left(-\frac{1}{x}\right) + c = d\left(-\frac{1}{x}\right) + a.$$

So the twelve solutions generally fall into three distinct sets of four,

$$\{p, -p, \frac{1}{p}, -\frac{1}{p}\}, \{q, -q, \frac{1}{q}, -\frac{1}{q}\}, \{r, -r, \frac{1}{r}, -\frac{1}{r}\},$$

where p, q and r are greater than 1. So we can say that the solution set S is generated by $\{p, q, r\}$.

It may be that 1 is one of the solutions, for example, if $a + b = c + d$, which gives $\frac{d-b}{a-c} = 1$. In this case, $\frac{d-a}{b-c} = 1$ too, so the value 1 is repeated and the solution set S will be $\{p, -p, \frac{1}{p}, -\frac{1}{p}, 1, -1\}$. There is also the special case when $p = q$, for example, when the bag contains 1, 2, 4 and 7. Here

$$\frac{7-4}{2-1} = \frac{7-1}{4-2} = 3, \tag{3.2}$$

and so p and q are not distinct, but as we shall see below, such cases are easily characterised.

These particular cases aside, for any four distinct integers in the bag, there will be three distinct solutions in $(-\infty, -1)$, a further three in $(-1, 0)$, three more in $(0, 1)$ and a final three in $(1, \infty)$. In particular, there can be no more than three natural number solutions. This maximum is possible, as in (3.1).

If the four numbers in the bag produce three natural number solutions for three of the equations they generate, then these three natural numbers I call a *Hikorski Triple*. (The origin of this name is explained in Appendix C; hereafter such a triple is called simply an HT.) An HT may be written as (p, q, r) or as $\begin{pmatrix} p \\ q \\ r \end{pmatrix}$ with $p \geqslant q \geqslant r \geqslant 1$. Notice that $(n, 1, 1)$ is always an HT for $n \in \mathbb{N}^+$, as given by the bag $\{2n, n+1, n-1, 0\}$, for example, and is called the *trivial* HT.

3.2 The three laws and the mini-cross-ratio

If putting a, b, c and d in the bag produces a solution set S, then putting $a+k, b+k, c+k$, and $d+k$ in the bag produces exactly S as well (consider $\frac{d-b}{a-c}$). We might say that the numbers in the bag can be *TRANSLATED* without changing the solution set. So we can start with $0, a, b$ and c (a, b and c natural numbers with $0 < a < b < c$) in the bag without loss of generality.

Note too that if ka, kb, kc and kd are in the bag, then they create exactly S as well (again, consider $\frac{d-b}{a-c}$). We could call this a *DILATION* of a, b, c and d. The dilation property means that we can consider $0, 1, a$ and b to be in the bag, where a and b are rational with $1 < a < b$, without loss of generality.

A corollary of this is to note that a, b, c and d give the same solution set S as $-a, -b, -c$ and $-d$ (choosing k to be -1). We could call this *REFLECTING* the numbers in the bag. We can reflect about any point, using a dilation scale factor -1 followed by a translation. This reflection property means that we can add the restriction $b - a > 1$ (we find that $b - a = 1$ gives the special case similar to (3.2)), since if $b - a < 1$, then we can reflect $0, 1, a, b$ to get the numbers $-b, -a, -1, 0$, before adding b to get $0, b-a, b-1, b$, and dividing by $b-a$ to get $0, 1, \frac{b-1}{b-a}, \frac{b}{b-a}$. Now we have $\frac{b}{b-a} - \frac{b-1}{b-a} = \frac{1}{b-a} > 1$. We have thus converted a bag where $b-a<1$ into one where $b-a>1$. If the four numbers in the bag are given as $0,1,a,b$ with a and b rational, $1<a<b$ and $b-a>1$, then I will say the bag is in *standard form*.

Note that the cross-ratio function also obeys the translation law, the dilation law, and the reflection law. It makes sense, therefore, for us to call the function $\frac{a-b}{c-d}$ *the mini-cross-ratio*, or $\mathrm{MC}(a,b,c,d)$.

3.3 A formula for HTs

Given a bag in standard form, which resulting functions of a and b in S could give us the three natural number values that will make up our HT? Considering all $\frac{\alpha-\beta}{\gamma-\delta}$ with α, β, γ and δ taken from $0, 1, a$ and b without repetition, we get

$$b-a, \frac{b-1}{a}, \frac{b}{a-1}, \frac{1}{b-a}, \frac{a}{b-1}, \frac{a-1}{b}, a-b, \frac{1-b}{a}, \frac{b}{1-a}, \frac{1}{a-b}, \frac{a}{1-b}, \frac{1-a}{b}.$$

Thus if $1<a<b$ and $b-a>1$, the only possibilities for natural numbers are $b-a, \frac{b-1}{a}$ and $\frac{b}{a-1}$. How are these ordered? Clearly $\frac{b}{a-1} > \frac{b-1}{a}$; also $b-a > \frac{b-1}{a}$, since $b-a-\frac{b-1}{a} = \frac{(a-1)(b-a-1)}{a} > 0$. Thus $\frac{b}{a-1}$ will always be the smallest element of the HT; $\frac{b}{a-1} > b-a$ and $b-a > \frac{b}{a-1}$ are both possible, since $b=10, a=3$ gives $b-a > \frac{b}{a-1}$ while $b=7, a=2$ gives $b-a < \frac{b}{a-1}$. (Note: the case $b-a = \frac{b}{a-1}$, as discussed above at (3.2), leads to the triplet $\left(\frac{a}{a-2}, \frac{a}{a-2}, 1+\frac{2}{a(a-2)}\right)$, which can clearly never be an HT.)

Note that if $\frac{b}{a-1} = p$ and $b-a=q$, then $a = \frac{p+q}{p-1}$ and $b = \frac{pq+p}{p-1}$, so substituting in,

$$\frac{b-1}{a} = \frac{pq+1}{p+q}.$$

By symmetry we reach the same result if if $\frac{b}{a-1} = q$ and $b-a=p$. Note that if $\frac{pq+1}{p+q} = 1$, then $(p-1)(q-1)=0$, and so the HT is trivial.

Thus the only possible HTs are of the form (p,q,r), $p \geqslant q \geqslant r \geqslant 1$, with p,q,r natural numbers and with $r = \frac{pq+1}{p+q}$. Rearranging, we find that

$q = \frac{pr-1}{p-r}$, and $p = \frac{qr-1}{q-r}$, thus emphasizing again that p and q play reciprocal roles within the HT. Note that if $p = r+s$ and $q = r+t$, then $r = \frac{(r+s)(r+t)+1}{(r+s)+(r+t)}$. Multiplying out gives $ts = r^2 - 1$, showing the reciprocal role of p and q once more.

Given $(p, q, \frac{pq+1}{p+q})$, can we always find rational positive a, b with $b - a > 1$ that when placed in the bag together with 0 and 1 will give this HT? Suppose we take the HT $(7, 5, 3)$. If $\frac{b}{a-1} > b - a$ (call this Situation 1) then we have $\frac{b}{a-1} = 7, b - a = 5, \frac{b-1}{a} = 3$. This gives the bag $\{0, 1, 2, 7\}$ in standard form. If $b - a > \frac{b}{a-1}$ (call this Situation 2), then we have $b - a = 7, \frac{b}{a-1} = 5, \frac{b-1}{a} = 3$. This gives the bag $\{0, 1, 3, 10\}$ in standard form. Generalising this, in Situation 1 we have: $\frac{b}{a-1} = p, b - a = q, \frac{b-1}{a} = r$. This gives the bag $\{0, 1, \frac{p+q}{p-1}, \frac{pq+p}{p-1}\}$ in standard form $(p > q > 1)$. In Situation 2 we have $b - a = p, \frac{b}{a-1} = q, \frac{b-1}{a} = r$. This gives the bag $\{0, 1, \frac{p+q}{q-1}, \frac{pq+q}{q-1}\}$ in standard form $(p > q > 1)$. Once again, the reciprocal nature of p and q is seen. Moreover, any bag of distinct natural numbers in standard form giving an HT will be of one of these forms.

So (p, q, r) is a non-trivial HT with $p > q > r > 1$ if and only if $r = \frac{pq+1}{p+q} > 1$. We can find two bags in standard form for any HT, except that the trivial HT $(p, 1, 1)$ with $p > 1$ gives only $\{0, 1, \frac{p+1}{p-1}, \frac{2p}{p-1}\}$, which is not in standard form.

So to summarise, in general there are twelve solutions to our numbers-in-the-bag equation, which fall into three quartets,

$$\left\{p, -p, \frac{1}{p}, -\frac{1}{p}\right\}, \left\{q, -q, \frac{1}{q}, -\frac{1}{q}\right\}, \left\{\frac{pq+1}{p+q}, -\frac{pq+1}{p+q}, \frac{p+q}{pq+1}, -\frac{p+q}{pq+1}\right\}. \tag{3.3}$$

The heart of this thesis is dedicated to exploring the properties of the functions that make up the third quartet.

3.4 HTs and recurrence relations

Consider the second order recurrence relations defined by $p, q, f(p,q), \ldots$ where f runs through the twelve functions in (3.3). The first eight are clearly periodic; as we have already seen in Chapter 1, $p, q, -\frac{pq+1}{p+q}, \ldots$ is period-3, and so is $p, q, -\frac{p+q}{pq+1}, p, q, \ldots$. The recurrence relations $p, q, \frac{pq+1}{p+q}, \ldots$ and $p, q, \frac{p+q}{pq+1}, \ldots$ are not periodic, but if we put $r = \frac{pq+1}{p+q}$, then $p = \frac{qr-1}{q-r}$ and the recurrence $q, r, \frac{qr-1}{q-r}, \ldots$ is period-6, and if we put $r = \frac{p+q}{pq+1}$ then $p = \frac{q-r}{qr-1}$, and the recurrence $q, r, \frac{q-r}{qr-1}, \ldots$ is also period-6.

3.5 The reduced mini-cross-ratio

Consider also the equation $\mathrm{C}(a,b,c,d) = \frac{(a-b)(c-d)}{(a-c)(b-d)} = x$? We find this expands to

$$(ad + bc)x + (ac + bd) = (ab + cd)x + (ad + bc),$$

which is of the form

$$Ax + B = Cx + A. \tag{3.4}$$

If we choose A, B and C here, then eliminating a, b from

$$A = (ad + bc), B = (ac + bd), C = (ab + cd)$$

yields a quintic curve defined by the vanishing of a polynomial $P(c,d) = 0$ where P is of degree 5. Solving (3.4) gives $x = \frac{A-B}{A-C}$, which obeys the translation, dilation and reflection laws, so we can replace A, B and C with 0, 1 and λ without loss of generality. As A, B, and C permute, (3.4) gives for x the six values that the cross-ratio can take, $\lambda, \frac{1}{\lambda}, 1-\lambda, \frac{1}{1-\lambda}, \frac{\lambda-1}{\lambda}$ and $\frac{\lambda}{\lambda-1}$. Note that with the exception of a few special cases, only one of these six values can be a positive integer. The function $\frac{A-B}{A-C}$ I shall call *the reduced mini-cross-ratio*, or RMC(A,B,C).

Our HTs above arose from considering the marginally more complicated equation $Ax+B = Cx+D$. This thesis is based upon the hope that the complete simplicity of these equations does not imply triviality; indeed, perhaps it is the very everyday nature of this material that means that something may have been overlooked.

3.6 The frequency of HTs

How common are HTs? Excel is useful here, as Figure 3.2 shows. The orange row gives p, the orange column gives q, and where the cell is light blue, $r = \frac{pq+1}{p+q}$ is an integer. The light blue cells lie on rectangular hyperbolas. These HTs can be seen from a different angle in Figure 3.3; here the yellow row gives p, the yellow column gives r, and the cell is light blue if $q = \frac{pr-1}{p-r}$ is an integer (the cell (x, x) contains the number x for convenience rather than ∞). Looking at the '11' column here,

$$(11, 1, 1), (11, 4, 3), (11, 9, 5), (13, 11, 6),$$
$$(19, 11, 7), (29, 11, 8), (49, 11, 9), (109, 11, 10)$$

are all HTs, and 11 appears elsewhere in the table too, in row '11', yielding

$$(131, 12, 11), (71, 13, 11), (51, 14, 11), (41, 15, 11),$$
$$(35, 16, 11), (31, 17, 11), (26, 19, 11), (23, 21, 11).$$

Thus 11 features in 16 distinct HTs. The '12' column, however, contains only two HTs, $(12, 1, 1)$ and $(131, 12, 11)$, while the '12' row has additionally $(155, 13, 12)$ and $(25, 23, 12)$.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	1.25	1.4	1.5	1.571	1.625	1.667	1.7	1.727	1.75	1.769	1.786	1.8	1.8
3	1	1.4	1.667	1.857	2	2.111	2.2	2.273	2.333	2.385	2.429	2.467	2.5	2.5
4	1	1.5	1.857	2.125	2.333	2.5	2.636	2.75	2.846	2.929	3	3.063	3.118	3.1
5	1	1.571	2	2.333	2.6	2.818	3	3.154	3.286	3.4	3.5	3.588	3.667	3.7
6	1	1.625	2.111	2.5	2.818	3.083	3.308	3.5	3.667	3.813	3.941	4.056	4.158	4.2
7	1	1.667	2.2	2.636	3	3.308	3.571	3.8	4	4.176	4.333	4.474	4.6	4.7
8	1	1.7	2.273	2.75	3.154	3.5	3.8	4.063	4.294	4.5	4.684	4.85	5	5.1
9	1	1.727	2.333	2.846	3.286	3.667	4	4.294	4.556	4.789	5	5.19	5.364	5.5
10	1	1.75	2.385	2.929	3.4	3.813	4.176	4.5	4.789	5.05	5.286	5.5	5.696	5.8
11	1	1.769	2.429	3	3.5	3.941	4.333	4.684	5	5.286	5.545	5.783	6	6.2
12	1	1.786	2.467	3.063	3.588	4.056	4.474	4.85	5.19	5.5	5.783	6.042	6.28	6.5
13	1	1.8	2.5	3.118	3.667	4.158	4.6	5	5.364	5.696	6	6.28	6.538	6.7

Figure 3.2: Frequency of HTs: 1

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	1
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2		2	5	3.5	3	2.75	2.6	2.5	2.429	2.375	2.333	2.3	2.273	2.25	2.231	2.214	2.2	2.1
3			3	11	7	5.667	5	4.6	4.333	4.143	4	3.889	3.8	3.727	3.667	3.615	3.571	3.5
4				4	19	11.5	9	7.75	7	6.5	6.143	5.875	5.667	5.5	5.364	5.25	5.154	5.0
5					5	29	17	13	11	9.8	9	8.429	8	7.667	7.4	7.182	7	6.8
6						6	41	23.5	17.67	14.75	13	11.83	11	10.38	9.889	9.5	9.182	8.9
7							7	55	31	23	19	16.6	15	13.86	13	12.33	11.8	11.
8								8	71	39.5	29	23.75	20.6	18.5	17	15.88	15	14
9									9	89	49	35.67	29	25	22.33	20.43	19	17.
10										10	109	59.5	43	34.75	29.8	26.5	24.14	22.
11											11	131	71	51	41	35	31	28.
12												12	155	83.5	59.67	47.75	40.6	35.
13													13	181	97	69	55	46
14														14	209	111.5	79	62.
15															15	239	127	89.
16																16	271	14
17																	17	30
18																		1

Figure 3.3: Frequency of HTs: 2

3.7 The definition of $h(n)$

Let $h(n) =$‘number of HTs in which n is an element’, and note that

$$(n, 1, 1), (n^2 - n - 1, n, n - 1), (n^2 + n - 1, n + 1, n), (2n + 1, 2n - 1, n)$$

are always distinct HTs for $n > 2$. So we have $h(1) = \infty, h(2) = 2$ (2 only occurs in $(2, 1, 1)$ and $(5, 3, 2)$), and $h(n) \geqslant 4$ for $n \geqslant 3$.

Suppose we have an HT (p, q, r). Recall that if $p = r + s$ and $q = r + t$, then $ts = r^2 - 1$, showing that if $r^2 - 1$ has many factors (as with $r = 11$) there will be many resulting HTs that include r. Now $11^2 - 1 = 120$, which has 16 factors, while $12^2 - 1 = 143 = 11 \times 13$, which has only 4 factors. It is easy to conjecture that $h(n) = d(n^2 - 1)$, where $d(n) =$ ‘the number of factors of n’. Drawing up Table 3.1 for 11 and Table 3.2 for 12 sheds light on this. In each case, $\times$ denotes ‘not a natural number’.

Theorem 3.1. *The number of HTs in which n appears is $h(n) = d(n^2 - 1)$.*

Proof. We have that $d(k)$ is odd if and only if k is a square, and $n^2 - 1$ cannot be a square if $n > 1$, so $d(n^2 - 1) = 2j$ for some j. So there exist j pairs of integers (u, v) with $u > v$, so that $uv = n^2 - 1$, where $j \geqslant 2$ since

r	t	$q = r + t$	$s = \frac{r^2-1}{t}$	$p = r + s$	HT
1	10	11	0	1	(11,1,1)
2	9	11	$\times$	$\times$	$\times$
3	8	11	1	4	(11,4,3)
4	7	11	$\times$	$\times$	$\times$
5	6	11	4	9	(11,9,5)
6	5	11	7	13	(13,11,6)
7	4	11	12	19	(19,11,7)
8	3	11	21	29	(29,11,8)
9	2	11	40	49	(49,11,9)
10	1	11	99	109	(109,11,10)
11	0	11	$\times$	$\times$	$\times$
11	1	12	120	131	(131,12,11)
11	2	13	60	71	(71,13,11)
11	3	14	40	51	(51,14,11)
11	4	15	30	41	(41,15,11)
11	5	16	24	35	(35,16,11)
11	6	17	20	31	(31,17,11)
11	7	18	$\times$	$\times$	$\times$
11	8	19	15	26	(26,19,11)
11	9	20	$\times$	$\times$	$\times$
11	10	21	12	23	(23,21,11)
11	11	22	$\times$	$\times$	$\times$

Table 3.1: HTs containing 11

$1, n-1, n+1$ and n^2-1 all divide n^2-1.

How many HTs contain n? First consider the case where n is the smallest member of the HT. We can therefore write the HT as $(n+u, n+v, n)$ where $u, v \in \mathbb{N}^+, u > v$. We have

$$\frac{(n+u)(n+v)+1}{2n+u+v} = n \Leftrightarrow uv = n^2 - 1.$$

There are exactly j pairs for (u, v) that satisfy this, so there are j HTs with n as the smallest member.

r	t	$q = r + t$	$s = \frac{r^2-1}{t}$	$p = r + s$	HT
1	11	12	0	1	(12,1,1)
2	10	12	$\times$	$\times$	$\times$
3	9	12	$\times$	$\times$	$\times$
4	8	12	$\times$	$\times$	$\times$
5	7	12	$\times$	$\times$	$\times$
6	6	12	$\times$	$\times$	$\times$
7	5	12	$\times$	$\times$	$\times$
8	4	12	$\times$	$\times$	$\times$)
9	3	12	$\times$	$\times$	$\times$)
10	2	12	$\times$	$\times$	$\times$
11	1	12	120	131	(131,12,11)
12	0	12	$\times$	$\times$	$\times$
12	1	13	143	155	(155,13,12)
12	2	14	$\times$	$\times$	$\times$
12	3	15	$\times$	$\times$	$\times$
12	4	16	$\times$	$\times$	$\times$
12	5	17	$\times$	$\times$	$\times$
12	6	18	$\times$	$\times$	$\times$
12	7	19	$\times$	$\times$	$\times$
12	8	20	$\times$	$\times$	$\times$
12	9	21	$\times$	$\times$	$\times$
12	10	22	$\times$	$\times$	$\times$
12	11	23	13	25	(25,23,12)
12	12	24	$\times$	$\times$	$\times$

Table 3.2: HTs containing 12

Now consider the case where n is not the smallest member of the HT, so we may write the HT as $(u-n, n, n-v)$, where $n-v$ is the smallest element (we cannot be sure how $u-n$ and n are ordered), with $0 < v < n, u > n$. We have from the HT definition

$$\frac{(u-n)n+1}{u} = n - v \Leftrightarrow uv = n^2 - 1.$$

We know there are precisely j values for v between (and including) 1 and

$n-1$ that divide n^2-1, and each gives a value for u between (and including) $n+1$ and n^2-1 that divides n^2-1, and so $u-n$ is between (and including) 1 and n^2-n-1. We need to check that $u-n \geqslant n-v$ in every case, which is true if and only if $u+v \geqslant 2n$. But $u+v \geqslant 2\sqrt{uv}$ by the AM-GM inequality, and so $u+v \geqslant 2\sqrt{n^2-1}$ and since $u+v$ is an integer, $u+v \geqslant 2n$ for $n > 1$. Thus we always have exactly $2j$ HTs for a given $n > 1$, and so $h(n) = d(n^2-1)$. $\square$

Suppose $n = 2k+1, k > 16$. Then

$$h(n) = d((2k+1)^2-1) = d(2k(2k+2)) = d(4k(k+1)).$$

Either k or $k+1$ is even, so to find $h(n)$ we seek $d(8j(k+1))$ or $d(8kj)$ for some $j > 8, \gcd(j,k) = 1$. In each case, we have at least 16 factors (distinct since $k > 16$) readily visible; in the latter case for example, we have $1, 2, 4, 8, k, 2k, 4k, 8k, j, 2j, 4j, 8j, jk, 2jk, 4jk, 8jk$. So for sufficiently large odd $n, h(n) \geqslant 16$. In fact, $n = 33$ is the last odd number for which $h(n) < 16$. (Notice that $h(n)$ is not multiplicative, since $h(3)h(5)$ is not equal to $h(15)$.) If n is even, then $n+1$ and $n-1$ are both odd, and $\gcd(n-1, n+1) = 1$. So using the fact that $d(n)$ is multiplicative, $h(n) = d(n^2-1) = d((n-1)(n+1)) = d(n-1)d(n+1)$. If $n-1$ and $n+1$ are both prime (that is, they form a prime pair), then $d(n-1) = d(n+1) = 2$, so $h(n) = 4$, and the converse is true also. The conjecture that there are infinitely many n so that $h(n) = 4$ is equivalent to the twin prime conjecture.

3.8 Adding the elements of an HT

One early thought when dealing with HTs is; how can they be ordered? The question leads naturally on to two others: what happens when you add the elements of an HT, and what happens if you multiply them? If this sum or product is unique, then we have a natural HT ordering.

Adding the elements of an HT shows that many HTs can add to the same number. There are, for example, at least 14 HTs where the elements add to 3230, as shown in Table 3.3 (the significance of l and m will be explained later).

a	b	c	$a+b+c$	l	m
2924	157	149	3230	3809	-2445
2749	251	230	3230	3021	-1975
2623	321	286	3230	2979	-1625
2465	412	353	3230	2936	-1170
2229	556	445	3230	2896	-450
2092	645	493	3230	2889	-5
2089	647	494	3230	2889	5
1959	736	535	3230	2896	450
1763	880	587	3230	2936	1170
1648	971	611	3230	2979	1625
1564	1041	625	3230	3021	1975
1457	1135	638	3230	3089	2445
1392	1195	643	3230	3139	2745
1293	1291	646	3230	3229	3225

Table 3.3: HTs that add to 3230

Conjecture 3.2. *For all $n \in \mathbb{N}$, there exists $k \in \mathbb{N}$ such that*

$$|\{(a,b,c) \quad an\ HT \quad : a+b+c=k\}| > n.$$

That is, the number of HTs adding to k is unbounded as $k \to \infty$.

A rough heuristic argument might proceed like this:

if $a + b + \frac{ab+1}{a+b} = k, \quad$ where $\quad a, b, k, \in \mathbb{N}^+$ then

$a^2 + a(3b-k) + b^2 - kb + 1 = 0$

$\Rightarrow a = \frac{k-3b\pm\sqrt{5b^2-2bk+k^2-4}}{2}$

$\Rightarrow 5b^2 - 2bk + k^2 - 4 = l^2$ for some $l \in \mathbb{N}^+$

$\Rightarrow b = \frac{k\pm\sqrt{5l^2-4k^2+20}}{5}$

$\Rightarrow 5l^2 - 4k^2 + 20 = m^2$ for some $m \in \mathbb{N}^+$

$\Rightarrow k^2 - 5 = \frac{5l^2 - m^2}{4}$.

So l and m are either both odd or both even. Now if $l = 2t$ and $m = 2u$, we have $k^2 - 5 = 5t^2 - u^2$, yielding $b = \frac{k \pm 2u}{5}$ and $a = \frac{k \pm 5t \pm 3u}{5}$. So if we can write $k^2 - 5$ as $5t^2 - u^2$ in a large number of different ways, then we are likely to have a large number of natural number solutions for a, b and c. Note also that if k is even, then t and u are of opposite parity, so for each pair of integer values for t and u giving a pair of even values for l and m, we can use the identity

$$5t^2 - u^2 \equiv 5\left(\frac{7t - 3u}{2}\right)^2 - \left(\frac{15t - 7u}{2}\right)^2,$$

to give a corresponding pair of odd values for l and m. We also have the identities

$$5x^2 - y^2 \equiv (5x + 2y)^2 - 5(2x + y)^2 \quad \text{and} \quad x^2 - 5y^2 = 5(x + 2y)^2 - (2x + 5y)^2,$$

so whether we tackle the equation $k^2 - 5 = 5t^2 - u^2$ or $k^2 - 5 = u^2 - 5t^2$ is immaterial.

Now $3230 = 5.11.29.31.211$, and in general, it will serve our purpose if $k^2 - 5$ has many distinct prime factors. Helpfully, if we choose k carefully we can guarantee that $k^2 - 5$ will have as many distinct prime factors as we wish. For example, note that $7^2 \equiv 5 \pmod{11}$ and $6^2 \equiv 5 \pmod{31}$. If we solve simultaneously $x \equiv 7 \pmod{11}$ and $x \equiv 6 \pmod{31}$ we get 161, which by the Chinese Remainder Theorem, is the unique solution $\pmod{341}$. Now this gives $161^2 \equiv 7^2 \pmod{11}$, and $161^2 \equiv 6^2 \pmod{31}$, so we have $161^2 \equiv 5 \pmod{11}, 161^2 \equiv 5 \pmod{31}$ and $161^2 \equiv 5 \pmod{341}$. So choosing $k = 161, k^2 - 5 = 25916 = 2^2.11.19.31$, where 11 and 31 are factors. We may clearly add further primes p to the factorisation of some larger k in this way, as long as $\begin{pmatrix} 5 \\ - \\ p \end{pmatrix} = 1$.

We might notice too that $5.11.29.31.211 = (5 \times 1^2 - 0^2)(5 \times 2^2 - 3^2)(5 \times 3^2 - 4^2)(5 \times 4^2 - 7^2)(5 \times 10^2 - 17^2)$. This suggests the true statement that if p is an odd prime that divides $5x^2 - y^2$ where $\gcd(x, y) = 1$, then p can always be written as $5t^2 - u^2$. Certainly two primes of the form $5x^2 - y^2$ always multiply to an integer of the same shape, since $(5x_1^2 - y_1^2)(5x_2^2 - y_2^2)$

$$\equiv 5(5x_1x_2 + y_1y_2 + 2x_1y_2 + 2x_2y_1)^2 - (10x_1x_2 + 2y_1y_2 + 5x_1y_2 + 5x_2y_1)^2.$$

Consider the binary quadratic form $5x^2 - y^2 = (x\sqrt{5}+y)(x\sqrt{5}-y)$, where $x, y \in \mathbb{Z}$. Both $(x\sqrt{5}+y)$ and $(x\sqrt{5}-y)$ are integers in the quadratic field $\mathbb{Q}(\sqrt{5})$. Suppose the prime factorisation of $k^2 - 5$ in $\mathbb{Z}$ is $p_1p_2 \ldots p_n$. Now a prime splits in a field if it factorises in the ring of integers in that field. For example, any prime of the form $4n+1$ splits in the ring of Gaussian integers $\mathbb{Z}[i]$, since it can be written as x^2+y^2 in $\mathbb{Z}$ which splits into $(x+yi)(x-yi)$ in $\mathbb{Z}[i]$. Primes of the form $4n+3$ do not split in $\mathbb{Z}[i]$. No natural prime number splits in $\mathbb{Z}$, by definition. Now the following statements are equivalent (non-trivially) for a prime $p \neq 5$:

1. $p|(k^2 - 5)$ for some k, or $\begin{pmatrix} 5 \\ - \\ p \end{pmatrix}$ is 1,
2. p splits in $\mathbb{Z}[\sqrt{5}]$,
3. there exist x, y where $p \nmid x, p \nmid y$ and where $p = (5x^2 - y^2)$.

Let us consider again the example of 3230. The fact that each p_i splits in $\mathbb{Z}[\sqrt{5}]$ means that we have a technique for writing $k^2 - 5$ as $5t^2 - u^2$ in many different ways, by writing out the full factorisation of $k^2 - 5$ in $\mathbb{Z}[\sqrt{5}]$ as

$$\prod_i (x_i\sqrt{5} + y_i) \prod_i (x_i\sqrt{5} - y_i)$$

The first product simplifies to $\alpha\sqrt{5} + \beta$, while the second product becomes $\alpha\sqrt{5} - \beta$. If we then exchange a set of plus signs in the first product for the corresponding set of minus signs in the second, the pair of products becomes $(\alpha'\sqrt{5} + \beta')(\alpha'\sqrt{5} - \beta') = k^2 - 5$. For example,

$3230^2 - 5 = 5.11.29.31.211$

$= (5 \times 1^2 - 0^2)(5 \times 2^2 - 3^2)(5 \times 3^2 - 4^2)(5 \times 4^2 - 7^2)(5 \times 10^2 - 17^2)$

$= (1\sqrt{5} + 0)(2\sqrt{5} + 3)(3\sqrt{5} + 4)(4\sqrt{5} + 7)(10\sqrt{5} + 17) \times (1\sqrt{5} - 0)(2\sqrt{5} - 3)(3\sqrt{5} - 4)(4\sqrt{5} - 7)(10\sqrt{5} - 17)$

$= 5 \times 25128^2 - 56095^2$

$= (1\sqrt{5} + 0)(2\sqrt{5} + 3)(3\sqrt{5} + 4)(4\sqrt{5} - 7)(10\sqrt{5} + 17) \times (1\sqrt{5} - 0)(2\sqrt{5} - 3)(3\sqrt{5} - 4)(4\sqrt{5} + 7)(10\sqrt{5} - 17)$

$= 5 \times 3232^2 - 6465^2$

$= (1\sqrt{5} + 0)(2\sqrt{5} + 3)(3\sqrt{5} + 4)(4\sqrt{5} + 7)(10\sqrt{5} - 17) \times (1\sqrt{5} - 0)(2\sqrt{5} - 3)(3\sqrt{5} - 4)(4\sqrt{5} - 7)(10\sqrt{5} + 17)$

$= 5 \times 3572^2 - 7305^2$

$= (1\sqrt{5} + 0)(2\sqrt{5} - 3)(3\sqrt{5} + 4)(4\sqrt{5} - 7)(10\sqrt{5} + 17) \times (1\sqrt{5} - 0)(2\sqrt{5} + 3)(3\sqrt{5} - 4)(4\sqrt{5} + 7)(10\sqrt{5} - 17)$

$= 5 \times 1468^2 - 585^2$

The permutations above only begin to exhaust the 32 possibilities. The resulting values for a, b, and c are given in Table 3.4 (we are interested in where a, b and c are all positive - the symbol $\times$ means positive values are not possible). So if $k^2 - 5$ has many prime factors, then $|\{HTs \ \ (a, b, c) : a + b + c = k\}|$ will be large too (although it is hard to be precise about exactly how many such HTs will be generated).

t	u	l (odd)	m (odd)	b	a	c	$a+b+c$
25128	56095	7611	$\times$	$\times$	$\times$	$\times$	$\times$
3232	6465	3229	3225	1291	1293	646	3230
				1	3228	1	3230
3572	7305	3089	2445	1291	1293	646	3230
				157	2924	149	3230
1468	585	8521	17925	880	1763	587	3230
				412	2465	353	3230

Table 3.4: Some of the HTs given by the ‘exchanging signs’ method

It is possible to resolve Conjecture 3.2 more swiftly by considering the asymptotics of the situation. This more sophisticated approach is examined at the end of Chapter 12.

3.9 The Uniqueness Conjecture (or UC) for HTs

So *adding* the terms of an HT does not produce a unique result – *multiplying* the elements of an HT, however, proves to be more intriguing. Of course the trivial HTs $(n, 1, 1)$ can multiply to any whole number – what if we exclude these? A PARI program enables a reasonably swift check on the first 250 000 non-trivial HTs, and multiplying their elements gives distinct products. The first few HTs with their products are given in Table 3.5.

a	5	7	11	9	19	11	13
b	3	5	4	7	5	9	8
c	2	3	3	4	4	58	5
abc	30	105	132	252	380	495	520
a	17	13	29	15	19	23	41
b	7	11	6	13	11	10	7
c	5	6	5	7	7	7	6
abc	595	858	870	1365	1463	1610	1722

Table 3.5: Early HT Products

And so we have the following uniqueness conjecture that remains open as I type:

Conjecture 3.3. *If* (a, b, c) *and* (p, q, r) *are non-trivial HTs with* $abc = pqr = n$, *then* $(a, b, c) = (p, q, r)$.

Opinion is divided as to whether this is likely to be true or not – the intuition of most experienced observers suggests that it is false. If it *is* true, however, then it leads to a happy result concerning integer points on elliptic curves, which will be explored in Chapter 9. I conclude this chapter with two HTs (a, b, c) and (p, q, r) where abc is close to pqr – a counterexample to the idea that such products are constrained to be far apart.

The triple (1957, 1955, 978) is an HT,
and $1957 \times 1955 \times 978 = 3,741,764,430$,
while (7897, 719, 659) is also an HT,
and $7897 \times 719 \times 659 = 3,741,764,437$.

Chapter 4

Involutions and Coxeter Groups

In 2005, Sergey Fomin and Nathan Reading [29] published an article called *Root Systems and Generalised Associahedra*, which has an opening section seminal to this thesis; what follows in this chapter attempts to extend their ideas. They begin by considering Lyness's period-5 cycle (1.3), but with a twist; they invite us to consider the transformations

$$T_1 : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} \frac{y+1}{x} \\ y \end{pmatrix}, T_2 : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} x \\ \frac{x+1}{y} \end{pmatrix}.$$

4.1 The 'moving window'

Note that both T_1 and T_2 are self-inverse – they are both involutions, and T_2 is clearly related to T_1 in the sense that

$$T_2 = \theta^{-1} T_1 \theta, \quad \text{where} \quad \theta : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} y \\ x \end{pmatrix}, \quad \text{and where} \quad \theta^{-1} = \theta. \tag{4.1}$$

We say that the maps T_1 and T_2 are conjugate. What happens if we apply T_1 and T_2 alternately? This creates what Fomin and Reading call a 'moving window' for our pentagonal sequence.

$$\begin{pmatrix} x \\ y \end{pmatrix} \begin{pmatrix} \frac{y+1}{x} \\ y \end{pmatrix} \begin{pmatrix} \frac{y+1}{x} \\ \frac{x+y+1}{xy} \end{pmatrix} \begin{pmatrix} \frac{x+1}{y} \\ \frac{x+y+1}{xy} \end{pmatrix} \begin{pmatrix} \frac{x+1}{y} \\ x \end{pmatrix} \begin{pmatrix} y \\ x \end{pmatrix} \begin{pmatrix} y \\ \frac{y+1}{x} \end{pmatrix} \begin{pmatrix} \frac{x+y+1}{xy} \\ \frac{y+1}{x} \end{pmatrix} \begin{pmatrix} \frac{x+y+1}{xy} \\ \frac{x+1}{y} \end{pmatrix} \begin{pmatrix} x \\ \frac{x+1}{y} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

So $T_1^2 = I, T_2^2 = I$, and $(T_2T_1)^5 = I$; we can note also that $(T_1T_2)^5 = I$. But $T_1T_2 \neq T_2T_1$, which suggests that T_1 and T_2 could be viewed as reflections. It is helpful to imagine what is happening geometrically here, as in Figure 4.1.

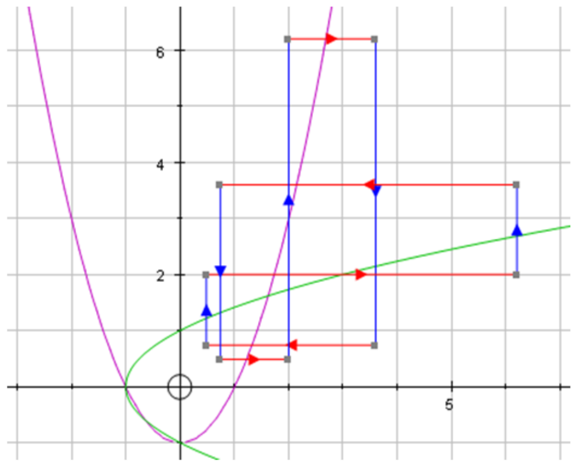


Figure 4.1: One-way Inversions

The fixed points of T_1 are given by $x = \frac{y+1}{x}$, or the parabola $x^2 = y + 1$, shown in purple in Figure 4.1. (The point where the green and purple parabolas cross in the first quadrant is (ϕ, ϕ), where ϕ is the Golden Ratio, and so if $x = \phi$ and $y = \phi$, the other three terms in the cycle will be ϕ also.) T_1 acts as what we might call a 'one-way inversion' – everything inside the purple parabola moves horizontally to its outside, and vice versa. In a similar way, the green parabola is fixed pointwise by T_2, and the one-way inversion applies vertically this time. Figure 4.1 shows that after alternating five applications of each of our transformations, we return to our starting point.

I should note here that the problem of breaking a cycle into two involutions has been given a deep treatment by Duistermaat [68] in relation to QRT maps [76]. Here the author defines a vertical switch and a horizontal switch (two involutions) on a biquadratic elliptic curve. Duistermaat's book has many implications for the work that appears in Chapter 8.

4.2 An involution with coefficients that grow

What does this process suggest? It is certainly not the case that any pair of involutions related by (4.1) treated this way as a pair creates a cycle. Consider

$$T_3 : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} \frac{-xy+2y^2-1}{y-x} \\ y \end{pmatrix}, T_4 : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} x \\ \frac{-xy+2x^2-1}{x-y} \end{pmatrix}. \tag{4.2}$$

Note that $T_3^2 = T_4^2 = I$. Applying these involutions alternately seems to lead to increasingly large terms. We can write the recurrence here as

$$x, y, \frac{-xy+2y^2-1}{y-x}, \frac{x^2-5xy+6y^2-2}{y-x}, \frac{2x^2-11xy+15y^2-6}{y-x},$$
$$\frac{6x^2-31xy+40y^2-15}{y-x}, \frac{15x^2-79xy+104y^2-40}{y-x}, \ldots. \tag{4.3}$$

Can we prove that the terms here never simplify, as they do, for example, for the period-5 sequence (1.3)?

Theorem 4.1. *The recurrence $x, y, \frac{-xy+2y^2-1}{y-x}, \ldots$ has general term*

$$u_i(x,y) = \frac{F_iF_{i+1}x^2 - (2F_{i+1}F_{i+2} + (-1)^{i+1})xy + F_{i+2}F_{i+3}y^2 - F_{i+1}F_{i+2}}{y-x},$$

where F_i is the i^{th} Fibonacci number (with $F_0 = 0, F_1 = 1$), and where $u_0(x,y)$ is the third term of the sequence.

Proof. For $n = 0$, we have $u_0(x,y) = \frac{0.1.x^2-(2.1.1-1)xy+1.2.y^2-1.1}{y-x}$, which is true. Let our inductive hypothesis for $0 \leqslant i \leqslant n+1$ be that the terms $u_i(x,y)$ form the above sequence. Let us say $u_n(x,y) = \frac{A}{y-x}$, and $u_{n+1}(x,y) = \frac{B}{y-x}$. Applying our recurrence relation,

$$u_{n+2}(x,y) = \frac{\frac{2B^2}{(y-x)^2} - \frac{AB}{(y-x)^2} - 1}{\frac{B}{y-x} - \frac{A}{y-x}}$$

$$= \frac{2B^2 - AB - (y-x)^2}{(B-A)(y-x)} = \frac{B(B-A) + B^2 - (y-x)^2}{(B-A)(y-x)}$$

$$= \frac{B(B-A)+(B-y+x)(B-x+y)}{(B-A)(y-x)}.$$

Now I claim that we can write $B-y+x$ as $C.D$, $B-x+y$ as $E.F$, and $B-A$ as $C.E$, where C, D, E and F are all linear polynomials in x and y. If true, this gives $u_{n+2}(x,y) = \frac{B+DF}{y-x}$. Now we know by our inductive hypothesis that, if n is even,

$$\begin{aligned} B-y+x &= F_{n+1}F_{n+2}x^2-(2F_{n+2}F_{n+3}+1)xy+F_{n+3}F_{n+4}y^2-F_{n+2}F_{n+3}-y+x \\ &= (F_{n+1}x-F_{n+3}y-F_{n+2})(F_{n+2}x-F_{n+4}y+F_{n+3}) = CD, \end{aligned}$$

as a simple check on the coefficients for x^2, y^2, xy, x, y and the constant term shows, remembering that

$$F_{k+1}F_{k+3}-F_{k+2}^2 = (-1)^k \quad \text{for all} \quad k \in \mathbb{Z}.$$

Similarly

$$B-x+y = (F_{n+1}x-F_{n+3}y+F_{n+2})(F_{n+2}x-F_{n+4}y-F_{n+3}) = EF.$$

We have similar factorisations if n is odd, giving $(B-y+x)(B-x+y) = CDEF$ for all values of n. We also have

$$\begin{aligned} B-A &= F_{n+1}F_{n+2}x^2-(2F_{n+2}F_{n+3}+(-1)^{n+2})xy+F_{n+3}F_{n+4}y^2-F_{n+2}F_{n+3} \\ &\quad -(F_nF_{n+1}x^2-(2F_{n+1}F_{n+2}+(-1)^{n+1})xy+F_{n+2}F_{n+3}y^2-F_{n+1}F_{n+2}) \\ &= x^2(F_{n+1}^2)-(2F_{n+2}^2+2(-1)^{n+2})xy+y^2(F_{n+3}^2)-F_{n+2}^2 \\ &= (F_{n+1}x-F_{n+3}y+F_{n+2})(F_{n+1}x-F_{n+3}y-F_{n+2}) = CE. \end{aligned}$$

Finally we have

$$\begin{aligned} B+DF &= F_{n+1}F_{n+2}x^2-(2F_{n+2}F_{n+3}+(-1)^{n+2})xy+F_{n+3}F_{n+4}y^2-F_{n+2}F_{n+3} \\ &\quad +(F_{n+2}x-F_{n+4}y+F_{n+3})(F_{n+2}x-F_{n+4}y-F_{n+3}) \\ &= F_{n+2}F_{n+3}x^2-(2F_{n+3}F_{n+4}+(-1)^{n+3})xy+F_{n+4}F_{n+5}y^2-F_{n+3}F_{n+4}, \end{aligned}$$

after careful checking of the coefficients once more. The expression $y-x$ will never divide exactly into a numerator that has a constant term, so

$$u_{n+2}(x,y) = \frac{F_{n+2}F_{n+3}x^2-(2F_{n+3}F_{n+4}+(-1)^{n+3})xy+F_{n+4}F_{n+5}y^2-F_{n+3}F_{n+4}}{y-x},$$

and by induction, the theorem is proved. $\square$

We can run the recurrence backwards too; the term before x and y in the sequence is $\frac{2x^2-xy-1}{x-y}$. Note that substituting $y = x+1$, or $y = x-1$ after running the recurrence means every term in the sequence will be an integer, whether the sequence runs forwards or backwards. Taking $y = x+1$, the first few polynomials generated are given in Table 4.1.

$u_{-2}(x, x+1)$	x
$u_{-1}(x, x+1)$	$x+1$
$u_0(x, x+1)$	x^2+3x+1
$u_1(x, x+1)$	$2x^2+7x+4$
$u_2(x, x+1)$	$6x^2+19x+9$
$u_3(x, x+1)$	$15x^2+49x+25$
$u_4(x, x+1)$	$40x^2+129x+64$
$u_5(x, x+1)$	$104x^2+337x+169$
$u_6(x, x+1)$	$273x^2+883x+441$
$u_7(x, x+1)$	$714x^2+2311x+1156$
$u_8(x, x+1)$	$1870x^2+6051x+3025$
$u_9(x, x+1)$	$4895x^2+15841x+7921$

Table 4.1: The sequence of polynomials generated by (4.3) with $y = x+1$

4.3 Breaking a period-4 cycle into two involutions

The following conjecture, however, is harder to assess; does every binary cycle come about by treating a pair of involutions related by (4.1) in this way? Consider the period-4 cycle (where w is a homogenising parameter)

$$x, y, -\frac{(x+w)(y+w)}{y}, -\frac{xy+xw+w^2}{x+w}, x, y \dots .$$

If we write

$$T_5 : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} -\frac{(x+w)(y+w)}{y} \\ y \end{pmatrix}, T_6 : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} x \\ -\frac{(x+w)(y+w)}{x} \end{pmatrix},$$

then $(T_5T_6)^2 = (T_6T_5)^2 = I$ (note that for even periods, the moving window does not return to $\begin{pmatrix} x \\ y \end{pmatrix}$ via $\begin{pmatrix} y \\ x \end{pmatrix}$ and thus cycles twice as fast). Neither T_5 nor T_6 is an involution. Could, however, the pair be broken down into involutions?

Theorem 4.2. *The transformation* $T_5 : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} -\frac{(x+w)(y+w)}{y} \\ y \end{pmatrix}$ *can be written as* P_1P_2 *where* P_1 *and* P_2 *are both involutions.*

Proof. Let us say

$$P_1 : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} \frac{axy+bx+cy+d}{hxy+ix-ay-b} \\ y \end{pmatrix}, P_2 : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} \frac{pxy+qx+ry+s}{txy+ux-py-q} \\ y \end{pmatrix} \tag{4.4}$$

for some constants a to u to be determined. Note that P_1 and P_2 are both involutions, since $f(x) = \frac{ax+b}{cx-a}$ is an involution.

It is worthwhile to pause as we embark upon on this calculation, and consider the tools to be employed. I am using Derive, a computer algebra package introduced by Texas Instruments in 1988. Many of the algebraic manipulations performed by Derive here would be extremely lengthy by hand. The chance of a mistake on a single line would be significant, and Derive calculations can run to several hundred lines. The availability of such packages is fantastically recent when viewed within the entire history of mathematics. The task of finding two involutions that compose to $-\frac{(x+1)(y+1)}{y}$ may be a calculation that has never been done before; it is certainly a task that has become immeasurably simpler within just the last decade.

Derive tells us that

$$P_1P_2 : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} -\frac{x(y^2(ap+ct)+y(aq+bp+cu+dt)+bq+du)+y^2(ar-cp)+y(as+br-cq-dp)+bs-dq}{x(y^2(at-hp)+y(au+bt-hq-ip)+bu-iq)-y^2(ap+hr)-y(aq+bp+hs+ir)-bq-is} \\ y \end{pmatrix} \tag{4.5}$$

Our strategy will be to put this expression equal to $-\frac{(x+w)(y+w)}{y}$ and then multiply out and rearrange to give $\sum x^m y^n P(m,n) = 0$, where $P(m,n) \in \mathbb{Z}[a, b, \cdots, u]$. Being identically zero for all values of x and y

means each of the polynomials $P(m,n)$ must be 0. This gives 12 equations to solve together in 12 unknowns:

$$at - hp = 0,$$
$$a(tw+u) + bt - h(pw+q) - ip = 0,$$
$$auw + b(tw+u) - hqw - i(pw+q) = 0,$$
$$w(bu - iq) = 0,$$
$$a(2p - tw) + ct + h(pw+r) = 0,$$
$$a(pw+2q-w(tw+u))+b(2p-tw)+cu+dt+h(pw^2+qw+rw+s)+i(pw+r) = 0,$$
$$aw(q-uw)+b(pw+2q-w(tw+u))+du+hw(qw+s)+i(pw^2+qw+rw+s) = 0,$$
$$w(b(q-uw) + i(qw+s)) = 0,$$
$$a(pw+r) - cp + hrw = 0,$$
$$a(pw^2+qw+s) + b(pw+r) - cq - dp + w(h(rw+s) + ir) = 0,$$
$$aqw^2 + b(pw^2+qw+s) - dq + w(hsw + i(rw+s)) = 0,$$

and

$$w^2(bq + is) = 0. \tag{4.6}$$

Placing all twelve equations into Derive to be solved simultaneously asks too much of the program. Solving the equations one by one, however, and avoiding degenerate solutions manually before substituting back into the others, eventually leads us to our goal. We can find the values for a to t in the order $a, b, c, d, h, s, r, t, q, p$ without encountering a surd. Our final equation is that

$$p^3 + 5p^2u + 8pu^2 + 4u^3 = 0,$$

which factorises to

$$(p+u)(p+2u)^2 = 0.$$

Now $p = -2u$ leads to a degenerate solution, but $p = -u$ does not. We can now find all our constants in terms of the remaining unchosen ones (i and u). Substituting back into (4.4), both i and u cancel, telling us the involutions

$$P_1 : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} -\frac{2wxy+2w^2x+w^2y+w^3}{4xy+2wx+2wy+2w^2} \\ y \end{pmatrix}, P_2 : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} -\frac{2wxy+2w^2x+w^2y+2w^3}{4xy+2wx+2wy+2w^2} \\ y \end{pmatrix}$$

give $P_1P_2 : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} -\frac{(x+w)(y+w)}{y} \\ y \end{pmatrix}$. □

The two involutions are remarkably similar; only a single w^3 term in the numerator distinguishes them.

So if we return to Fomin and Reading's moving window idea, we can define Q_1 and Q_2 as

$$Q_1 : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} x \\ -\frac{2wxy+2w^2y+w^2x+w^3}{4xy+2wy+2wx+2w^2} \end{pmatrix}, Q_2 : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} x \\ -\frac{2wxy+2w^2y+w^2x+2w^3}{4xy+2wy+2wx+2w^2} \end{pmatrix}$$

to give $Q_1Q_2 : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} x \\ -\frac{(x+w)(y+w)}{x} \end{pmatrix}$. This gives $(P_1P_2Q_1Q_2)^2 = I$, and $(P_2P_1Q_2Q_1)^2 = I$.

4.4 Breaking a period-4 cycle into three involutions

It is possible to write $\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} -\frac{(x+w)(y+w)}{y} \\ y \end{pmatrix}$ as the product of three involutions that are simpler than P_1 and P_2. If we say

$$V_1 : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} \frac{ax+by+c}{dx-a} \\ y \end{pmatrix}, V_2 : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} \frac{jx+ky+l}{mx-j} \\ y \end{pmatrix}, V_3 : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} \frac{px+qy+r}{sx-p} \\ y \end{pmatrix},$$

can we find choices for a to s so that $V_1V_2V_3 : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} -\frac{(x+w)(y+w)}{x} \\ y \end{pmatrix}$? By a procedure similar to the one above, we find that

$$V_1 : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} -x-w \\ y \end{pmatrix}, V_2 : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} -\frac{w(jx+ky+w(j+k))}{j(x+w)} \\ y \end{pmatrix},$$

$$V_3 : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} -\frac{w(jx+ky+wj)}{j(x+w)} \\ y \end{pmatrix}$$

give $V_1V_2V_3 : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} -\frac{(x+w)(y+w)}{y} \\ y \end{pmatrix}$. Putting $j = -k$ gives

$$V_1 \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} -x-w \\ y \end{pmatrix}, V_2 \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} \frac{w(y-x)}{x+w} \\ y \end{pmatrix}, V_3 \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} \frac{w(y-x-w)}{x+w} \\ y \end{pmatrix}$$

which give $V_1V_2V_3 : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} -\frac{(x+w)(y+w)}{y} \\ y \end{pmatrix}$.

4.5 Involutions and period-3 binary cycles

As we have seen above, if the period of a binary regular cycle $x, y, f(x, y), \ldots$ is even, then it seems the transformation $T : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} f(x,y) \\ y \end{pmatrix}$ will not necessarily be an involution. If the period of a binary regular cycle $x, y, f(x, y), \ldots$ is odd, however, then is T guaranteed to be an involution in the Fomin and Reading sense? This is certainly true for binary period-3 recurrences, as the following theorem tells us:

Theorem 4.3. *The most general possible regular binary period-3 cycle is*

$$x, y, \frac{axy + bx + by + c}{dxy - ax - ay - b}, x, y, \ldots \tag{4.7}$$

Proof. The fourth term in $x, y, \frac{axy+bx+cy+d}{pxy+qx+ry+s}, \ldots$ is

$$\frac{xy^2(a^2+bp)+xy(a(b+c)+bq+dp)+x(bc+dq)+y^2(ac+br)+y(ad+bs+c^2+dr)+cd+ds}{pxy^2(a+q)+xy(ar+bp+ps+q^2)+x(br+qs)+y^2(cp+qr)+y(cr+dp+s(q+r))+dr+s^2}.$$

We can equate this to x, and then form $\sum x^m y^n P(m, n) = 0$, where each $P(m, n) \in \mathbb{Z}[a, \cdots, s]$. Being identically zero for all values of x and y means each of the polynomials $P(m, n)$ must be 0. This gives 9 equations to solve together in 8 unknowns; we require the vector

$$[p(a+q), ar+bp+ps+q^2, br+qs, a^2+bp-cp-qr, a(b+c)+bq-cr-s(q+r), \cdots$$

$$bc + d(q - r) - s^2, ac + br, ad + bs + c^2 + dr, d(c + s)]$$

to be the zero vector. If we avoid assigning any constant the value 0, which leads to degenerate solutions, we arrive at $c = b, q = -a, r = -a, s = -b$. Reorganising our constants, this gives

$$x, y, \frac{axy + bx + by + c}{dxy - ax - ay - b}, x, y, \ldots$$

as the most general possible regular period-3 cycle. $\square$

Once again, we have duplication here, but this is the most useful form for us to use. Now we can note that $T : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} \frac{axy+bx+by+c}{dxy-ax-ay-b} \\ y \end{pmatrix}$ is an involution. Computer searches support the conjecture that binary period-5 cycles obey the same law.

Note too that if a recurrence is an involution in the Fomin and Reading sense, then this property is preserved under conjugation. If $T : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} f(x,y) \\ y \end{pmatrix}$ where $T^2 = I$, then clearly $(U^{-1}TU)(U^{-1}TU) = I$ also, where U is as defined on page 28.

4.6 Alternating periodic cycles

Fomin and Reading now 'take logs' and consider S_1 and S_2 where

$$S_1 : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} y - x \\ y \end{pmatrix}, S_2 : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} x \\ x - y \end{pmatrix}.$$

Here $S_1^2 = I, S_2^2 = I$, and $(S_2S_1)^3 = I$. Fomin and Reading also suggest alternating significantly different involutions with S_1 and S_2, namely

$$S_3 : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} x \\ 2x - y \end{pmatrix}, S_4 : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} x \\ 3x - y \end{pmatrix}. \tag{4.8}$$

These give $(S_3S_1)^4 = I, (S_4S_1)^6 = I$.

4.7 Coxeter groups

What we have here is a collection of examples of finite reflection groups (a reflection group is simply one generated by a set of reflections), or Coxeter groups (a Coxeter group is an abstraction of the idea of a reflection group; if the group is finite, they have an identical algebraic structure.) A Coxeter group is one with the presentation

$$< r_1, r_2, \dots r_n | (r_i r_j)^{m_{ij}} = 1 >,$$

with the extra conditions that $m_{ii} = 1$ for all i, and that $m_{ij} \geqslant 2$ for $i \neq j$. If there is no m_{ij} so that $(r_i r_j)^{m_{ij}} = 1$, then we write $m_{ij} = \infty$. These m_{ij} form a symmetric Coxeter matrix M, where $M = m_{ij}$. Our period-5 recurrence (1.3) gives us the Coxeter matrix $\begin{pmatrix} 1 & 5 \\ 5 & 1 \end{pmatrix}$; the other examples Fomin and Reading give above include those with Coxeter matrices $\begin{pmatrix} 1 & 3 \\ 3 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 4 \\ 4 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 6 \\ 6 & 1 \end{pmatrix}$.

The reflection group connection is seen by looking again at the elements of Fomin and Reading's moving window in Figure 4.2. Here s stands for T_1 and t stands for T_2. One tenth of the regular pentagon is chosen as a fundamental region (labelled 1), and two of this region's sides are chosen as reflecting hyperplanes in which the rest of the group is generated. The group here is the dihedral group containing five rotations (one the identity) and five reflections (the product of two reflections is a rotation.)

4.8 Rank-3 Coxeter groups

All the Coxeter groups seen thus far here have been rank-2 ('rank' refers to the number of independent reflections that generate the group); their Coxeter matrices have been 2×2 (every reflection group generated by just two reflections will be dihedral). Can we use our Lyness cycles to construct a group from a larger set of reflections? Our plan will be to choose two Lyness cycles and to place them side by side, before applying them alternately in the manner of (4.8), hoping that they will interact helpfully. Let us choose the two period-6 cycles

$$x, y, y-x, -x, -y, x-y, x, y \ldots \quad \text{and} \quad x, y, \frac{y}{x}, \frac{1}{x}, \frac{1}{y}, \frac{x}{y}, x, y \ldots,$$

with one being the 'log' of the other. Applying $y - x$ and $\frac{y}{x}$ alternately gives

$$x, y, y-x, \frac{y-x}{y}, \frac{xy - y^2 - x + y}{y}, 1-y, \frac{x - xy}{y}, \frac{x}{y}, x, y \ldots.$$

This is period-8 (and if we apply our functions in the other order, the same happens.) Both $y - x$ and $\frac{y}{x}$ are involutions in the Fomin and Reading sense,

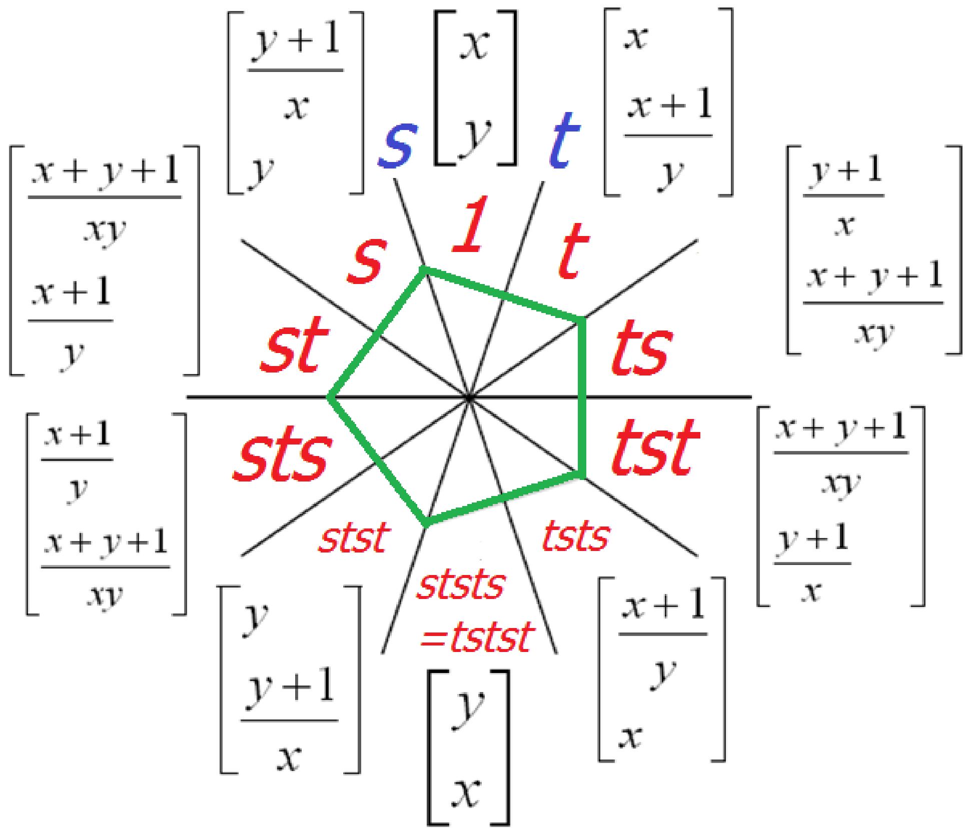


Figure 4.2: Symmetries of a regular pentagon

so we have

$$U_1\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} y-x \\ y \end{pmatrix}, U_2\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ x-y \end{pmatrix},$$

$$U_3\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} y/x \\ y \end{pmatrix}, U_4\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ x/y \end{pmatrix},$$

$$(U_1)^2 = I, (U_2)^2 = I, (U_3)^2 = I, (U_4)^2 = I,$$
$$(U_2U_1)^3 = I, (U_4U_3)^3 = I, (U_1U_2)^3 = I, (U_3U_4)^3 = I,$$
$$(U_4U_1)^4 = I, (U_2U_3)^4 = I, (U_1U_4)^4 = I, (U_3U_2)^4 = I.$$

Can our functions combine even more fully? Could we ask for U_1 and U_3 to alternate periodically too? In other words, if we regard U_1 and U_3 as involutions in x (effectively treating y as a constant) is $(U_1U_3)^n = I$ for some n? The answer is 'No', since we get

$$x, y-x, \frac{y}{y-x}, y-\frac{y}{y-x}, \frac{x-y}{x-y+1}, \frac{1}{x-y+1}+y-1, \frac{y(x-y+1)}{x(y-1)-y(y-2)}, \ldots .$$

where the terms rapidly become ever more complicated.

Consider instead the functions

$$f(x,y) = -\frac{xy+1}{x+y}, g(x,y) = -\frac{x+y}{xy+1}.$$

Then $x, y, f(x,y)...$ and $x, y, g(x,y)...$ are both period-3. Moreover $h_1(x) = f(x,y)$ and $h_2(x) = g(x,y)$ are both involutions. Alternating f and g gives the period-6 sequence

$$x, y, -\frac{xy+1}{x+y}, \frac{1}{x}, \frac{1}{y}, -\frac{x+y}{xy+1}, x, y \ldots .$$

while alternating $h_1(x)$ and $h_2(x)$ gives the period-4 sequence

$$x, -\frac{xy+1}{x+y}, \frac{1}{x}, -\frac{x+y}{xy+1}, x, y \ldots .$$

So we have

$$\begin{aligned}
V_1\begin{pmatrix} x \\ y \end{pmatrix} &= \begin{pmatrix} -\frac{xy+1}{x+y} \\ y \end{pmatrix}, V_2\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ -\frac{xy+1}{x+y} \end{pmatrix}, \\
V_3\begin{pmatrix} x \\ y \end{pmatrix} &= \begin{pmatrix} -\frac{x+y}{xy+1} \\ y \end{pmatrix}, V_4\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ -\frac{x+y}{xy+1} \end{pmatrix},
\end{aligned} \tag{4.9}$$

$$\begin{gathered}
(V_1)^2 = I, (V_2)^2 = I, (V_3)^2 = I, (V_4)^2 = I, \\
(V_2V_1)^3 = I, (V_4V_3)^3 = I, (V_1V_2)^3 = I, (V_3V_4)^3 = I, \\
(V_4V_1)^3 = I, (V_2V_3)^3 = I, (V_1V_4)^3 = I, (V_3V_2)^3 = I, \\
(V_3V_1)^2 = I, (V_2V_4)^2 = I, (V_1V_3)^2 = I, (V_4V_2)^2 = I.
\end{gathered}$$

A pair of Lyness cycles that combine so completely I call 'productive'.

What happens if we repeatedly apply V_1, V_2, V_3, and V_4 to $\begin{pmatrix} x \\ y \end{pmatrix}$ in any order? A Coxeter group is generated with 24 elements. The group appears to be rank-4, but in fact $V_1V_3V_2V_3V_1 = V_4$, so it is rank-3. Which one do we have? The Coxeter matrix is clearly $\begin{pmatrix} 1 & 3 & 2 \\ 3 & 1 & 3 \\ 2 & 3 & 1 \end{pmatrix}$. A list of all possible finite Coxeter groups is given in Table 4.2 [57]. For the order to be 24, the only possibilities are the symmetry groups of the 3-simplex and the rank-3 demihypercube. These polytopes happen to coincide; they are are both the tetrahedron. Thus the group we have is the permutation group on four elements, S_4.

Group Symbol	Alternative Symbol	Rank	Order	Related polytopes
A_n	A_n	n	$(n+1)!$	n-simplex
$B_n = C_n$	C_n	n	$2^n n!$	n-hypercube/ n-cross-polytope
D_n	B_n	n	$2^{n-1}n!$	n-demihypercube
E_6	E_6	6	51840	2_{21} polytope
E_7	E_7	7	2903040	3_{21} polytope
E_8	E_8	8	696729600	4_{21} polytope
F_4	F_4	4	1152	24-cell
G_2	none	2	12	hexagon
H_2	G_2	2	10	pentagon
H_3	G_3	3	120	icosahedron/ dodecahedron
H_4	G_4	4	14400	120-cell/600-cell
$I_2(p)$	D_2^p	2	$2p$	p-gon

Table 4.2: Finite Coxeter groups

4.9 Investigating rank-4 Coxeter groups

Can we extend the group given by (4.9) by adding another reflection? A natural reflection to try is

$$V_5 : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} -x \\ y \end{pmatrix}, \tag{4.10}$$

since this represents the pseudo-cycle $x, y, -x, -y, \ldots$, but this fails to combine helpfully; for example, $V\begin{pmatrix} x \\ y \end{pmatrix} = V_1V_5V_2V_3\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -\frac{x^2+2x+y}{x^2+2xy+1} \\ \frac{1}{x} \end{pmatrix}$, and V^n rapidly becomes more complicated as n increases. We therefore expect the group will be infinite, and that its Coxeter matrix will be $\begin{pmatrix} 1 & 3 & 2 & \infty \\ 3 & 1 & 3 & \infty \\ 2 & 3 & 1 & \infty \\ \infty & \infty & \infty & 1 \end{pmatrix}$. Using $V_6\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -x \\ -y \end{pmatrix}$, however, does work profitably, if trivially, simply doubling the size of the group to 48 by adding an extra element to the centre. The transformation V_6 does not represent a Lyness cycle in the way that (4.10) does. The Coxeter matrix of the group here is $\begin{pmatrix} 1 & 3 & 2 & 2 \\ 3 & 1 & 3 & 2 \\ 2 & 3 & 1 & 2 \\ 2 & 2 & 2 & 1 \end{pmatrix}$, which seems initially to be rank-4, yet if we consult Table 4.2, the only possibility for a Coxeter group of order 48 is C_3, which is rank-3. It is not immediately obvious how we find a set of generators; the set of V_i does not provide a triplet that will do.

There is a deeper point to be made here, which is that the Lyness pentagonal cycle (1.1) and Coxeter groups are linked via the topic of Cluster Algebras [72] [73]. The A_2 Dynkin quiver gives rise to (1.1), and more generally, any recurrence that arises from a finite Dynkin quiver will be periodic.

4.10 Productive pairs in general

Another example of a productive pair, where both f and g give period-6 recurrences, is

$$f(x, y) = \frac{xy - 1}{x - y}, g(x, y) = \frac{x - y}{xy - 1}$$

The group generated here is once again S_4. This leads us to conjecture that if $f(x,y)$ and $g(x,y)$ both define periodic recurrence relations, and if $f(x,y)g(x,y) = 1$ for all x and y, then f and g will be productive. Computer searches suggest that such pairs are rare! The only examples that have come to light thus far are

$$x, y, -\frac{axy + bx + by + a}{bxy + ax + ay + b}, x, y, \ldots$$

and its reciprocal; the two examples we have seen so far are of this type. Here it is easy to show that f and g are indeed productive, with Coxeter matrix $\begin{pmatrix} 1 & 3 & 2 \\ 3 & 1 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ as before.

4.11 Involutions and symmetric functions

It seems that we have

Conjecture 4.4. *Every regular period-5 cycle is of the form*

$$x, y, f(x,y), g(x,y) = g(y,x), f(y,x), x, y, \ldots,$$

where f is regular and an involution (in x), and where g is regular and symmetric in x and y.

We can note that if

$$f(x,y) = z = \frac{axy + bx + cy + d}{pxy + qx - ay - b},$$

which is an involution (in x), then f has two inverses, given by

$$x = \frac{z(ay + b) + cy + d}{z(py + q) - ay - b}$$

which is the involution (as expected) in z, $f(z,y)$, and

$$y = -\frac{qxz - bx - bz - d}{pxz - ax - az - c}$$

which is symmetric in x and z. I will call this second inverse f^{-1}.

Conversely, if $g(x, y)$ is symmetric in x and y, so that

$$g(x, y) = z = \frac{axy + bx + by + c}{pxy + qx + qy + r}$$

then g has two inverses that are identical, namely

$$x = -\frac{y(qz - b) + rz - c}{y(pz - a) + qz - b}$$

which is an involution (in y), and similarly,

$$y = -\frac{x(qz - b) + rz - c}{x(pz - a) + qz - b}.$$

which is an involution (in x). I will call this inverse g^{-1}.

The dual cycle idea is more understandable in this light. If we skip 0, 1, 2, 3, 4 steps each time for our period-5 cycle we have:

1. $x, y, f(x, y), g(x, y), f(y, x), x, \ldots$
2. $x, f(x, y), f(y, x), y, g(x, y), x, \ldots$
3. $x, g(x, y), y, f(y, x), f(x, y), x, \ldots$
4. $x, f(y, x), g(x, y), f(x, y), y, x, \ldots$
5. $x, x, x, x, x, x, \ldots$

Orders 1. and 4. give the starting recurrence and its reverse, 2. and 3. give our dual recurrence and its reverse, while 5. is degenerate.

For 3. we have $u = x, v = g(x, y)$. Now since g is regular, it is invertible, so we have $y = g^{-1}(x, v) = g^{-1}(u, v)$. So given the way we have cycled our terms, $u, v, g^{-1}(u, v), \ldots$ defines a recurrence relation, which gives our dual cycle as $u, v, g^{-1}(u, v), f^{-1}(u, v), g^{-1}(v, u), u, v, \ldots$. It is clear that repeating this procedure gets us back to our original recurrence.

For example, given $x, y, \frac{y+1}{x}, \frac{x+y+1}{xy}, \frac{x+1}{y}, x, y, \ldots$, then $z = \frac{y+1}{x}$ gives $x = \frac{y+1}{z}$ (an involution in z), and $y = xz - 1$ (which is symmetric), while $g(x, y) = z = \frac{x+y+1}{xy}$ gives $x = \frac{y+1}{yz-1}$ (which is an involution, in y), $y = \frac{x+1}{xz-1}$ (which is the same involution, in x). The dual sequence is thus

$$u, v, \frac{u+1}{uv-1}, uv - 1, \frac{v+1}{uv-1}, u, v, \ldots.$$

It is easy to extend our Conjecture 4.4 as follows:

Conjecture 4.5. *Every regular period-$(2n+1)$ cycle can be written as*

$$x, y, f_1(x, y), f_2(x, y), \ldots, f_n(x, y), f_{n-1}(y, x), \ldots f_1(y, x), x, y, \ldots$$

where $f_1(x, y)$ is an involution in x, and where $f_n(x, y)$ is regular and symmetric in x and y.

This is certainly true for $n = 1$, since $x, y, \frac{axy+bx+by+c}{cxy-ax-ay-b}, \ldots$ is the general regular period-3 cycle, and the central term is both an involution (in x) and symmetric. The conjecture would seem to be highly likely for $n = 2$, and the case for $n = 3$ represents perhaps the best hope of constructing a binary period-7 recurrence, should one exist.

To take a different angle, we are with duality defining a map $T^* : (x_0, x_2) \mapsto (x_2, x_4)$. Taking f as regular, we have $x_1 = f^{-1}(x_0, x_2)$, and $x_3 = f(x_1, x_2)$, so

$$x_4 = f(x_2, x_3) = f(x_2, f(x_1, x_2)) = f(x_2, f(f^{-1}(x_0, x_2), x_2)).$$

Chapter 5

The Dilogarithm Function

> *Almost all the dilogarithm's appearances in mathematics have something of the fantastical in them, as if this function alone among all others possessed a sense of humour.* Zagier [61]

Fomin and Reading begin their key article [29] by quoting our period-5 Lyness cycle (1.3). They add the comment

> *The discovery of this recurrence and its 5-periodicity are sometimes attributed to R. C. Lyness; it was probably already known to Abel. This recurrence is closely related to (and easily deduced from) the famous 'pentagonal identity' for the dilogarithm function, first obtained by W. Spence (1809), and rediscovered by Abel (1830) and C.H. Hill (1830).*

5.1 Defining the dilogarithm

What then is this identity (also rediscovered by Ramanujan), and what is the dilogarithm? It is a function on the complex plane defined for $|z| < 1$ as

$$\mathrm{Li}_2(z) = \frac{z}{1^2} + \frac{z^2}{2^2} + \frac{z^3}{3^2} + \cdots .$$

The logarithm reference comes in since

$$-\ln(1-z) = \frac{z}{1} + \frac{z^2}{2} + \frac{z^3}{3} + \ldots \quad \text{for} \quad |z| < 1.$$

Although the definition above only applies inside the unit disc, there is an analytic continuation for $\mathrm{Li}_2(z)$ to the whole plane save for the cut $[1, \infty)$, given by

$$\mathrm{Li}_2(z) = \int_0^z -\frac{\ln(1-u)}{u}\, du.$$

This is easily seen, since

$$\frac{d}{dz}\left(\frac{z}{1^2} + \frac{z^2}{2^2} + \frac{z^3}{3^2} + \cdots\right) = -\frac{\ln(1-z)}{z}.$$

The dilogarithm is the first in a more general set of functions called polylogarithms, where

$$\mathrm{Li}_n(z) = \frac{z}{1^n} + \frac{z^2}{2^n} + \frac{z^3}{3^n} + \cdots .$$

The dilogarithm is a transcendental function; it cannot be expressed as the solution of a polynomial equation whose coefficients are themselves polynomials (functions that can be so expressed are called algebraic). I refer below to elementary functions, which are the functions that can be formed by a finite process of composing exponentials, logarithms, n^{th} roots, constants and a single variable together with adding, multiplying, subtracting and dividing the functions so formed. The symbol $=_{ef}$ below stands for 'equality modulo the addition of elementary functions' – for an example of its use, see (5.1).

5.2 Functional equations

It is natural to seek further connections between the dilogarithm and the logarithm; for instance, does $\mathrm{Li}_2(xy) = \mathrm{Li}_2(x) + \mathrm{Li}_2(y)$? The answer is 'No', but the dilogarithm does possess many helpful functional equations, for example,

$$\mathrm{Li}_2(z) = \int_0^z -\frac{\ln(1-t)}{t}\, dt = \int_1^{1-z} \frac{\ln(s)}{1-s}\, ds \quad \text{(substituting} \quad s = 1-t)$$

$$= [-\ln(1-s)\ln(s)]_1^{1-z} + \int_1^{1-z} \frac{\ln(1-s)}{s}\, ds \quad \text{(using Integration by Parts)}$$

$$= \int_0^{1-z} \frac{\ln(1-s)}{s}\, ds - \int_0^1 \frac{\ln(1-s)}{s}\, ds.$$

$$= \int_0^{1-z} \frac{\ln(1-s)}{s}\, ds + [\mathrm{Li}_2(s)]_0^1,$$

$$=_{ef} -\mathrm{Li}_2(1-z). \tag{5.1}$$

This is known as Euler's identity for the dilogarithm. An entirely similar argument gives $\mathrm{Li}_2(z) =_{ef} \mathrm{Li}_2\left(\frac{1}{1-z}\right)$, which (once we use composition repeatedly) gives us the functional equations

$$\mathrm{Li}_2(z) =_{ef} -\mathrm{Li}_2(1-z) =_{ef} -\mathrm{Li}_2\left(\frac{1}{z}\right) =_{ef} -\mathrm{Li}_2\left(\frac{z}{z-1}\right)$$

$$=_{ef} \mathrm{Li}_2\left(\frac{1}{1-z}\right) =_{ef} \mathrm{Li}_2\left(\frac{z-1}{z}\right).$$

Notice that these arguments are precisely the six versions of the cross ratio $\mathrm{C}[0,1,\infty,z]$ as the four arguments permute. If $f(z)$ is one of these six arguments, then $\mathrm{Li}_2(z) =_{ef} (-1)^{k-1}\,\mathrm{Li}_2(f(z))$ where k is the order of $f(z)$ in the group they give under composition. The cross-ratio connection is also seen with the trilogarithm; here we have, in identities due to Landen [41],

$$\mathrm{Li}_3(z) + \mathrm{Li}_3(1-z) + \mathrm{Li}_3\left(\frac{z-1}{z}\right) =_{ef} 0,$$

and

$$\mathrm{Li}_3\left(\frac{1}{z}\right) + \mathrm{Li}_3\left(\frac{1}{1-z}\right) + \mathrm{Li}_3\left(\frac{z}{z-1}\right) =_{ef} 0.$$

5.3 Abel's identity

So what is the famous 'pentagonal identity' to which Fomin and Reading refer? Wikipedia [58] quotes

$$\mathrm{Li}_2\left(\frac{x}{1-y}\right) + \mathrm{Li}_2\left(\frac{y}{1-x}\right) - \mathrm{Li}_2(x) - \mathrm{Li}_2(y) - \mathrm{Li}_2\left(\frac{xy}{(1-x)(1-y)}\right)$$

$$= \ln(1-x)\ln(1-y) \quad \text{for} \quad x, y \notin [1,\infty) \tag{5.2}$$

Can we prove this? We know that $\frac{d}{dz}\mathrm{Li}_2(z) = -\frac{\ln(1-z)}{z}$, so if we differentiate (5.2) partially with respect to x, we find

$$\frac{\partial}{\partial x}\mathrm{RHS} = \ln(1-y)\frac{-1}{1-x}.$$

We also have

$$\frac{\partial}{\partial x}\operatorname{Li}_2\left(\frac{x}{1-y}\right)=\frac{-\ln\left(1-\frac{x}{1-y}\right)}{\frac{x}{1-y}}\frac{1}{1-y}=\frac{-\ln(1-x-y)}{x}+\frac{\ln(1-y)}{x},$$

$$\frac{\partial}{\partial x}\left(\operatorname{Li}_2\left(\frac{y}{1-x}\right)\right)=\frac{-\ln\left(1-\frac{y}{1-x}\right)}{\frac{y}{1-x}}\frac{y}{(1-x)^2}=\frac{-\ln(1-x-y)}{1-x}+\frac{\ln(1-x)}{1-x},$$

$$\frac{\partial}{\partial x}(-\operatorname{Li}_2(x))=\frac{\ln(1-x)}{x},\quad \frac{\partial}{\partial x}(-\operatorname{Li}_2(y))=0,$$

$$\frac{\partial}{\partial x}\left(-\operatorname{Li}_2\left(\frac{xy}{(1-x)(1-y)}\right)\right)=\frac{\ln\left(1-\frac{xy}{(1-x)(1-y)}\right)}{\frac{xy}{(1-x)(1-y)}}\frac{y(1-x)+xy}{(1-x)^2(1-y)},$$

$$=\frac{\ln(1-x-y)-\ln(1-x)-\ln(1-y)}{x}+\frac{\ln(1-x-y)-\ln(1-x)-\ln(1-y)}{1-x}.$$

Comparing the coefficients of $\ln(1-x-y),\ln(1-x)$ and $\ln(1-y)$, we see LHS = RHS. Differentiating partially with respect to y gives the same result, and the identity is clearly true for $x=0,y=0$, so Abel's identity holds for all x and y.

Rogers in 1907 [60] discovered that Abel's identity was in fact one in a hierarchy of dilogarithm identities. He found an identity in m variables with m^2+1 terms which simplifies to Euler's identity (5.1) for $m=1$, and to Abel's identity (5.2) for $m=2$. For $m=3$, the identity is equivalent to

$$\operatorname{Li}_2(x)+\operatorname{Li}_2(y)+\operatorname{Li}_2(z)-\operatorname{Li}_2(u)-\operatorname{Li}_2(v)-\operatorname{Li}_2(xyz)-\operatorname{Li}_2\left(\frac{xz}{u}\right)$$

$$-\operatorname{Li}_2\left(\frac{yz}{v}\right)+\operatorname{Li}_2\left(\frac{xv}{u}\right)+\operatorname{Li}_2\left(\frac{yu}{v}\right)=_{ef}0,$$

where $xv(1-yz)+yu(1-xz)=uv(1-xy)$ and $v(1-x)+u(1-y)=1-xyz$.

From the point of view of this thesis, however, there is a more helpful way to write Abel's identity than (5.2), which might suggest that the recurrences $x,y,\frac{y}{1-x}\ldots$ or $x,y,\frac{x}{1-y}\ldots$ are periodic, but neither are. The recurrence relation $x,y,\frac{1-y}{x}\ldots$ is, however, period-5, and remembering that $\operatorname{Li}_2(z)=_{ef}-\operatorname{Li}_2(\frac{1}{z})$, we have from (5.2)

$$\operatorname{Li}_2(x)+\operatorname{Li}_2(y)+\operatorname{Li}_2\left(\frac{1-y}{x}\right)+\operatorname{Li}_2\left(\frac{xy}{(1-x)(1-y)}\right)+\operatorname{Li}_2\left(\frac{1-x}{y}\right)=_{ef}0.$$

A problem still remains; the Lyness cycle goes

$$x, y, \frac{1-y}{x}, \frac{x+y-1}{xy}, \frac{1-x}{y}, x, y, \ldots, \tag{5.3}$$

so we need

$$\mathrm{Li}_2\left(\frac{xy}{(1-x)(1-y)}\right) =_{ef} \mathrm{Li}_2\left(\frac{x+y-1}{xy}\right).$$

This is true, since

$$\mathrm{Li}_2\left(\frac{xy}{(1-x)(1-y)}\right) =_{ef} -\mathrm{Li}_2\left(\frac{(1-x)(1-y)}{xy}\right)$$
$$=_{ef} \mathrm{Li}_2\left(1-\frac{(1-x)(1-y)}{xy}\right) =_{ef} \mathrm{Li}_2\left(\frac{x+y-1}{xy}\right).$$

So we can rewrite Abel's identity (5.2) as

$$\mathrm{Li}_2(x)+\mathrm{Li}_2(y)+\mathrm{Li}_2\left(\frac{1-y}{x}\right)+\mathrm{Li}_2\left(\frac{x+y-1}{xy}\right)+\mathrm{Li}_2\left(\frac{1-x}{y}\right) =_{ef} 0, \tag{5.4}$$

where $x, y, \frac{1-y}{x}, \frac{x+y-1}{xy}, \frac{1-x}{y}, x, y, \ldots$ is a Lyness cycle. Zagier [61] chooses to quote the Abel identity (from the many formulations open to him) as

$$\mathrm{Li}_2(x)+\mathrm{Li}_2(y)+\mathrm{Li}_2\left(\frac{1-x}{1-xy}\right)+\mathrm{Li}_2(1-xy)+\mathrm{Li}_2\left(\frac{1-y}{1-xy}\right)$$
$$=\frac{\pi^2}{6}-\ln(x)\ln(1-x)-\ln(y)\ln(1-y)+\ln\left(\frac{1-x}{1-xy}\right)\ln\left(\frac{1-y}{1-xy}\right).$$

Note that $x, y, \frac{1-x}{1-xy}, 1-xy, \frac{1-y}{1-xy}, x, y\ldots$ is a period-5 Lyness cycle, the dual of (5.3).

5.4 Moving from Abel's identity to Lyness's period-5 cycle

Fomin and Reading say that our original pentagonal cycle is easily obtained from Abel's identity – how? If we replace x and y with -x and -y in (5.4), we get

$$\mathrm{Li}_2(-x)+\mathrm{Li}_2(-y)+\mathrm{Li}_2\left(-\frac{1+y}{x}\right)+\mathrm{Li}_2\left(-\frac{x+y+1}{xy}\right)+\mathrm{Li}_2\left(-\frac{1+x}{y}\right) =_{ef} 0.$$

Suppose we now define an alternative version of the dilogarithm function

$$\mathrm{L}_{\mathrm{alt}}(z) = \mathrm{Li}_2(-x).$$

This yields

$$\mathrm{L}_{\mathrm{alt}}(x) + \mathrm{L}_{\mathrm{alt}}(y) + \mathrm{L}_{\mathrm{alt}}\left(\frac{1+y}{x}\right) + \mathrm{L}_{\mathrm{alt}}\left(\frac{x+y+1}{xy}\right) + \mathrm{L}_{\mathrm{alt}}\left(\frac{1+x}{y}\right) =_{ef} 0,$$

and we have the pentagonal cycle as part of a dilogarithm identity.

5.5 Alternative forms of the dilogarithm

In our discussion of the dilogarithm above, there were some awkward pieces of calculation whenever we had to find the elementary functions required by a particular identity. Fortunately, there are ways to remove the 'equality mod the addition of elementary functions' conditions above and replace them with simply 'equality', which enables computer searches for other possible identities to be carried out. The simplification requires that we use another alternative form of the dilogarithm function.

5.6 The Rogers dilogarithm

An adjusted dilogarithm that is of interest is due to Rogers. He defined

$$\begin{aligned}\mathrm{L}_{\mathrm{r}}(z) &= -\frac{1}{2}\int_0^z \frac{\ln(1-t)}{t} + \frac{\ln(t)}{1-t}\,dt \\ &= \mathrm{Li}_2(z) + \frac{1}{2}\ln(z)\ln(1-z).\end{aligned}$$

This gives, on substitution into Abel's identity (5.4),

$$\mathrm{L}_{\mathrm{r}}(x) + \mathrm{L}_{\mathrm{r}}(y) + \mathrm{L}_{\mathrm{r}}\left(\frac{1-y}{x}\right) + \mathrm{L}_{\mathrm{r}}\left(\frac{x+y-1}{xy}\right) + \mathrm{L}_{\mathrm{r}}\left(\frac{1-x}{y}\right) = 0,$$

with no elementary functions to complicate things; 'equality' here means exactly 'equality'.

5.7 The Wigner-Bloch dilogarithm

A more comprehensive way still to simplify our dilogarithm identities is given by the remarkable Wigner-Bloch dilogarithm [13], which is defined as

$$\mathrm{D}(z) = \Im(\mathrm{Li}_2(z)) + \arg(1-z)\ln|z|.$$

This elegant real-valued continuous function on the complex plane is real-analytic on the whole of $\mathbb{C}$ save for the points 0 and 1, and converts our basic functional dilogarithm identities into exactly

$$\mathrm{D}(z) = -\mathrm{D}(1-z) = -\mathrm{D}\left(\frac{1}{z}\right) = -\mathrm{D}\left(\frac{z}{z-1}\right) = \mathrm{D}\left(\frac{1}{1-z}\right) = \mathrm{D}\left(\frac{z-1}{z}\right).$$

Abel's identity becomes

$$\mathrm{D}(x) + \mathrm{D}(y) + \mathrm{D}\left(\frac{1-y}{x}\right) + \mathrm{D}\left(\frac{x+y-1}{xy}\right) + \mathrm{D}\left(\frac{1-x}{y}\right) = 0,$$

exactly as for the Rogers dilogarithm. Could we search for another identity akin to Abel's using another Lyness cycle? PARI includes the function 'dilog', so we can easily define $D(z)$ before programming such a search. A binary period-3 cycle seems to be a good place to start – by (4.7), the most general possible is

$$x, y, \frac{axy+bx+by+c}{dxy-ax-ay-b}, x, y, \ldots,$$

so we can look for an identity such as $\mathrm{D}(x)+\mathrm{D}(y)+\mathrm{D}\left(w = \frac{axy+bx+by+c}{dxy-ax-ay-b}\right) = 0$. Now $\mathrm{D}(z)$ has a maximum value of 1.0149... at $\frac{1+i\sqrt{3}}{2}$; Figure 5.1 shows how $\mathrm{D}(z)$ gets smaller the further from $\frac{1+i\sqrt{3}}{2}$ we travel in the upper half-plane (for the lower half-plane, $\mathrm{D}(z^*) = -\mathrm{D}(z)$). It is sensible to choose our starting values for x and y to be, say, $2+i$ and $-3+2i$, so that $D(x)$ and $D(y)$ are not close to 0.

Now we allow a, b, c, d to run from $-n$ to n for sensible $n \in \mathbb{N}^+$, checking that $d*x*y - a*x - a*y - b \neq 0$ each time. Then we must also check for each set of constants that w is not 0 or 1, before asking PARI to print these out if $D(x) + D(y) + D(w)$ is close to 0. In this case, we can run a second program to find if $D(x) + D(y) + D(w)$ is more generally 0. No examples

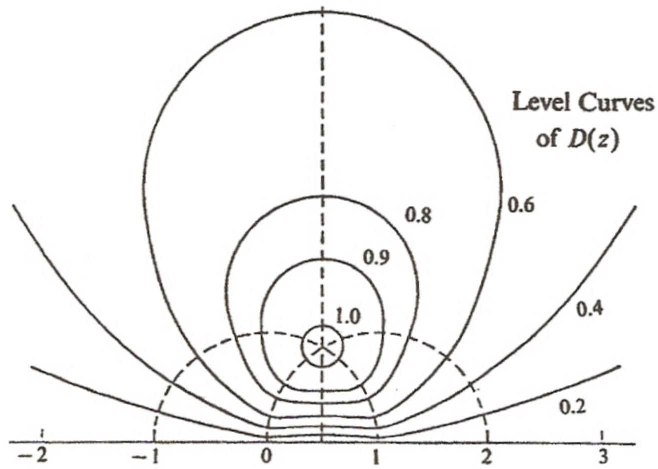


Figure 5.1: Level curves for D(z)([61])

where this has happened have been found thus far.

Lewin [41] refers to

> *the remarkable discovery by Zagier and Gangl at the Max-Planck-Institut fur Mathematik of a two-variable functional equation for the hexalogarithm - the first significant advance in the area [of finding new functional equations for polylogarithms] since Kummer's work of 150 years ago.*

The dilogarithm has received a huge amount of attention, and the above quotation suggests that the chance that a new and accessible identity remains undiscovered is slight. The opinion of experienced observers is that the more involved and advanced identities all seem to have a common root; the pentagon identity. Any other simple relation would have yielded higher identities too – the absence of these suggests that the pentagon recurrence is somehow the whole story. But maybe the dilogarithm has a joke to play on us yet...

Chapter 6

Order-1 cycles

This next chapter is devoted to the first column of Table 2.1. Initially I take a direct (maybe even naive) approach to rational order-1 cycles (which periods are possible, and how do we know this?), before turning to a more sophisticated view on these questions towards the end of the chapter.

6.1 The cycle $\frac{ax-1}{x+1}$

Consider the rational function $\frac{ax-1}{x+1}$. This is of interest when iterated, since if a = 0, we get the period-3 sequence

$$x, \frac{-1}{x+1}, \frac{-x-1}{x}, x \ldots,$$

while if a = 1, we get the period-4 sequence

$$x, \frac{x-1}{x+1}, \frac{-1}{x}, \frac{x+1}{1-x}, x \ldots,$$

and if a = 2, we get the period-6 sequence

$$x, \frac{2x-1}{x+1}, \frac{x-1}{x}, \frac{x-2}{2x-1}, \frac{1}{1-x}, \frac{x+1}{2-x}, x \ldots.$$

We would like to prove that for no other integer a is this rational function periodic in this way. It helps to consider powers of the matrix

$$A = \begin{pmatrix} a & -1 \\ 1 & 1 \end{pmatrix}$$

since iterating $f(x) = \frac{ax-1}{x+1}$ is equivalent to taking powers of A, with the proviso that $\begin{pmatrix} ka & -k \\ k & k \end{pmatrix}$ is identified with A.

$$A^1 = \begin{pmatrix} a & -1 \\ 1 & 1 \end{pmatrix}$$

$$A^2 = \begin{pmatrix} (a+1)(a-1) & -a-1 \\ a+1 & 0 \end{pmatrix}$$

$$A^3 = \begin{pmatrix} (a+1)(a^2-a-1) & -a(a+1) \\ a(a+1) & -a-1 \end{pmatrix}$$

$$A^4 = \begin{pmatrix} a(a-2)(a+1)^2 & (1-a)(a+1)^2 \\ (a-1)(a+1)^2 & -(a+1)^2 \end{pmatrix}$$

$$A^5 = \begin{pmatrix} (a+1)^2(a^3-2a^2-a+1) & -(a+1)^2(a^2-a-1) \\ (a+1)^2(a^2-a-1) & -a(a+1)^2 \end{pmatrix}$$

$$A^6 = \begin{pmatrix} (a-1)(a+1)^3(a^2-2a-1) & a(2-a)(a+1)^3 \\ a(a-2)(a+1)^3 & (1-a)(a+1)^3 \end{pmatrix}$$

$$A^7 = \begin{pmatrix} a(a+1)^3(a^3-3a^2+3) & -(a+1)^3(a^3-2a^2-a+1) \\ (a+1)^3(a^3-2a^2-a+1) & -(a+1)^3(a^2-a-1) \end{pmatrix}$$

$$A^8 = \begin{pmatrix} (a+1)^4(a^2-a-1)(a^2-3a+1) & (1-a)(a+1)^4(a^2-2a-1) \\ (a-1)(a+1)^4(a^2-2a-1) & a(2-a)(a+1)^4 \end{pmatrix}$$

$$A^9 = \begin{pmatrix} (a+1)^4(a^5-4a^4+2a^3+5a^2-2a-1) & -a(a+1)^4(a^3-3a^2+3) \\ a(a+1)^4(a^3-3a^2+3) & -(a+1)^4(a^3-2a^2-a+1) \end{pmatrix}$$

It appears, remarkably, that the sequence of polynomials $P_i(a)$ in each corner are one and the same sequence, save for phase and multiples of $(a+1)$ (for simplicity's sake, $P_i(a)$ will be called P_i below). Inspection suggests that the i^{th} matrix will be of the form

$$A^i = \begin{pmatrix} P_{i+2} & -(a+1)P_i \\ (a+1)P_i & -(a+1)^2 P_{i-2} \end{pmatrix} \tag{6.1}$$

It appears also that $P_n | P_{mn}$ here for $m, n \in \mathbb{N}^+$. Further inspection suggests that these polynomials obey the recurrence relations

$$P_i = (a+1)P_{i-1} - (a+1)P_{i-2} \tag{6.2}$$

and

$$P_i = aP_{i-1} - (a+1)P_{i-3}. \tag{6.3}$$

The initial terms are $P_0 = 0, P_1 = \frac{1}{a+1}$ which give $P_{-1} = -\frac{1}{(a+1)^2}, P_2 = 1$, $P_3 = a$. The recurrences defined by (6.2) and (6.3) are effectively the same, since the characteristic polynomial for (6.2) is $\lambda^2 - (a+1)\lambda + (a+1) = 0$, while for (6.3) it is $(\lambda + 1)(\lambda^2 - (a+1)\lambda + (a+1)) = 0$. So the general solution for P_i will be $p\lambda_1^n + q\lambda_2^n$ from (6.2) and $p'\lambda_1^n + q'\lambda_2^n + r'(-1)^n$ from (6.3). These formulations now have to be equal for $i = 1, 2$ and 3, which means $p = p', q = q'$, and $r' = 0$ which means (6.2) and (6.3) have the same solutions for P_i, and thus (6.3) holds whenever (6.2) does.

Theorem 6.1. *The matrix*

$$A^i = \begin{pmatrix} P_{i+2} & -(a+1)P_i \\ (a+1)P_i & -(a+1)^2 P_{i-2} \end{pmatrix} \tag{6.4}$$

where P_i is defined by (6.2) *and* (6.3)*, and where $P_0 = 0$ and $P_1 = \frac{1}{a+1}$.*

Proof. Let us assume that (6.2) and (6.3) hold for $3 \leqslant i \leqslant n$. Then

$$\begin{pmatrix} a & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} P_n & -(a+1)P_{n-2} \\ (a+1)P_{n-2} & -(a+1)^2 P_{n-4} \end{pmatrix}$$

$$= \begin{pmatrix} aP_n - (a+1)P_{n-2} & -a(a+1)P_{n-2} + (a+1)^2 P_{n-4} \\ P_n + (a+1)P_{n-2} & -(a+1)P_{n-2} - (a+1)^2 P_{n-4} \end{pmatrix}.$$

$$= \begin{pmatrix} P_{n+1} & -(a+1)P_{n-1} \\ (a+1)P_{n-1} & -(a+1)^2 P_{n-3} \end{pmatrix}.$$

So we have the next polynomial in the sequence P_{n+1} satisfies (6.3) for $i = n+1$, and since $P_{n-2} = P_{n-1} - \frac{P_n}{a+1}, P_{n+1}$ satisfies (6.2) also. So we have by induction that (6.3) and (6.2) hold for P_i for all i, and that the matrix A^i can be written as in (6.4) for all $i \in \mathbb{N}$. □

Now suppose $P_n = 0$ for some a and some n. Then

$$\begin{pmatrix} P_{n+2} & -(a+1)P_n \\ (a+1)P_n & -(a+1)^2 P_{n-2} \end{pmatrix} = \begin{pmatrix} P_{n+2} & 0 \\ 0 & -(a+1)^2 P_{n-2} \end{pmatrix}$$

By (6.2),

$$P_{n+2} = (a+1)P_{n+1} - (a+1)P_n = (a+1)P_{n+1}$$

$$= (a+1)(aP_n - (a+1)P_{n-2}) = -(a+1)^2 P_{n-2}.$$

So we have a zero for the polynomial P_n just if the rational function defined by A is period-n. Now we know P_n has zeroes for $a = 0, n = 1$, giving a period-3 sequence, for $a = 1, n = 2$, giving a period-4 sequence, and for $a = 2, n = 4$, giving a period-6 sequence. Can P_n be zero elsewhere? Finding an explicit form for P_n might help. Fortunately, solving a linear binary recurrence relation is straightforward. The recurrence (6.2) above tells us that $P_n = p\lambda_1^n + q\lambda_2^n$, where λ_1 and λ_2 are the solutions to the characteristic equation

$$\lambda^2 - (a+1)\lambda + (a+1) = 0$$

Putting $P_2 = 1$ and $P_3 = a$ gives two equations that can be solved for p and q. We arrive at

$$P_n = \frac{2^{-n}(a+b+1)^{n-2}(a+b-1)}{b} - \frac{2^{1-n}(a-b+1)^{n-2}(a-b-1)}{b}$$

where $b = \sqrt{(a+1)(a-3)}$. Putting $P_n = 0$ and solving for n gives $n = \frac{A+C}{B}$, where

$$A = \ln\left(\frac{(a-b-1)(a+b+1)^2}{(a+b-1)(a-b+1)^2}\right), B = \ln\left(\frac{a+b+1}{a-b+1}\right)$$

and $C = 0$, $2\pi i$ and $-2\pi i$ in turn. Substituting the values 0, 1 and 2 for a gives us $n = 1, 2,$ and 4, as we expect. Can we prove that these are the only possible natural number solutions?

6.2 Some theoretical background to linear recurrence sequences

Everest, van der Poorten, Shparlinski and Ward [25] define an order-n linear recurrence sequence (LRS) P as a sequence of terms (P_i) where $P_{n+k} = s_1 P_{n+k-1} + s_2 P_{n+k-2} + \cdots + s_n P_k$ for all k in $\mathbb{N}$. The characteristic polynomial is $f(\lambda) = \lambda^n - s_1\lambda^{n-1} - \cdots - s_{n-1}\lambda - s_n$, where $\{s_i\}$ lies in some ring.

We need to beware that an order-1 LRS can be disguised as an order-2 one; for example, $P_{n+1} = 2P_n$ implies $P_{n+2} = 2P_{n+1}$, and adding these equations gives $P_{n+2} = P_{n+1} + 2P_n$, apparently an order-2 LRS (similarly (6.3) appears to be an order-3 recurrence, but is in fact order-2, a version of (6.2)).

So we can classify $P_{n+1} = (a+1)P_n - (a+1)P_{n-1}$ as a binary LRS, with characteristic polynomial $f(\lambda) = \lambda^2 - (a+1)\lambda + (a+1)$. The matrix $\Omega = \begin{pmatrix} a+1 & -a-1 \\ 1 & 0 \end{pmatrix}$ can be used to calculate further terms, since putting $\omega_0 = \begin{pmatrix} P_1 \\ P_0 \end{pmatrix}$ means that $\omega_n = \begin{pmatrix} P_{n+1} \\ P_n \end{pmatrix} = \Omega^n \omega_0$.

An inhomogeneous linear recurrence relation is one that includes a constant term, as in

$$P_{n+k} = s_1 P_{n+k-1} + s_2 P_{n+k-2} + \cdots + s_n P_k + s_{n+1}$$

Here we have also

$$P_{n+k+1} = s_1 P_{n+k} + s_2 P_{n+k-1} + \cdots + s_n P_{k+1} + s_{n+1}$$

and so subtracting we have

$$P_{n+k+1} = P_{n+k}(1+s_1) + \sum_{i=1}^{n-1}(s_{i+1} - s_i)P_{n+k-i} - s_n P_k. \tag{6.5}$$

This adds the factor $\lambda - 1$ to the characteristic polynomial, and so 1 will always be a root of the characteristic equation for (6.5). Thus an order-n inhomogeneous linear recurrence relation leads to an order-$(n+1)$ homogeneous one.

An LRS is said to be *degenerate* if some $\frac{\lambda_1}{\lambda_2}$ is a root of unity, where λ_1 and λ_2 are both roots of the characteristic equation. If $\lambda_1 = 2$ and $\lambda_2 = -2$, for example, then $\lambda^2 - 4 = 0$ is the characteristic equation, and the LRS is $u_{k+2} = 4u_k$, leading to the degenerate sequence $(0, 1, 0, 4, 0, 16, \dots)$ if $u_0 = 0$ and $u_1 = 1$.

The m solutions λ_i to the characteristic polynomial (if it has no repeated roots and if the underlying field is of characteristic 0) give a general solution to the LRS of the form $P_n = \sum_{i=1}^{m} a_i \lambda_i^n$, for all n in $\mathbb{N}$, where the set of a_i is given by the initial conditions.

We can define the pointwise product of two LRSs $P = (P_n)$ and $Q = (Q_n)$ to be $P \bigotimes Q = (P_nQ_n)$. If $P_n = \sum_{i=1}^{j} a_i\lambda_i^n$ and $Q_n = \sum_{i=1}^{k} b_i\theta_i^n$, then (P_nQ_n) will be of the same form, and thus is also an LRS.

Let me at this point introduce a startling LRS due to Berstel:

$$a_{n+3} = 2a_{n+2} - 4a_{n+1} + 4a_n, a_0 = a_1 = 0, a_2 = 1.$$

Here

$$\begin{pmatrix} a_3 \\ a_2 \\ a_1 \end{pmatrix} = \begin{pmatrix} 2 & -4 & 4 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} a_2 \\ a_1 \\ a_0 \end{pmatrix},$$

and

$$\begin{pmatrix} a_{n+2} \\ a_{n+1} \\ a_n \end{pmatrix} = \begin{pmatrix} 2 & -4 & 4 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}^n \begin{pmatrix} a_2 \\ a_1 \\ a_0 \end{pmatrix}.$$

When does the LRS have zeroes for a_n? Clearly this happens for $n = 0$ and $n = 1$, and we also have

$$\begin{pmatrix} 2 & -4 & 4 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}^4 \begin{pmatrix} a_2 \\ a_1 \\ a_0 \end{pmatrix} = \begin{pmatrix} 0 \\ -4 \\ 0 \end{pmatrix} \Rightarrow a_4, a_6 = 0,$$

$$\begin{pmatrix} 2 & -4 & 4 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}^{13} \begin{pmatrix} a_2 \\ a_1 \\ a_0 \end{pmatrix} = \begin{pmatrix} -512 \\ -768 \\ 0 \end{pmatrix} \Rightarrow a_{13} = 0,$$

and

$$\begin{pmatrix} 2 & -4 & 4 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}^{50} \begin{pmatrix} a_2 \\ a_1 \\ a_0 \end{pmatrix} = \begin{pmatrix} 0 \\ -884763262976 \\ -201863462912 \end{pmatrix} \Rightarrow a_{52} = 0.$$

Thus this LRS attains six distinct zeroes, the last of which is highly unexpected. This is an excellent example of the truth that the terms of an LRS may simplify for some large n even though their initial behaviour suggests they will become steadily larger. The following important result comments upon the way which an LRS can attain zeroes in general.

Theorem 6.2 (Skolem, Mahler, Lech (1953) [25])**.** *The set of zeroes of a linear recurrence relation over a field of characteristic zero comprises a finite set together with a finite number of arithmetic progressions.*

As an example, consider the sequence $R = P \bigotimes Q$, where P is the Berstel LRS defined above, and where

$$Q = (1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, \ldots),$$

or

$$Q_{n+8} = Q_n, Q_0 = Q_1 = \ldots = Q_6 = 1, Q_7 = 0.$$

The recurrence R will have zeroes at $n = 0, 1, 4, 6, 13, 52$ and whenever 8 divides $n + 1$.

Let us define $m(P, c) =$ number of solutions to $P_n = c$ for some LRS P. We have that $m(P, c)$ is finite by the Skolem-Mahler-Lech Theorem unless the LRS is degenerate. Let us write $m(P, 0) = m(P)$ for convenience. Define also

$$\mu(n, R) = \sup_{P, m(P,c)<\infty} m(P, c) \quad \text{and} \quad \mu_0(n, R) = \sup_{P, m(P)<\infty} m(P),$$

where n is the order of the non-degenerate LRSs $\{P\}$, and where R is the underlying ring. We now have

Theorem 6.3. $\mu_0(2, R) = 1$ *for any ring R without zero divisors.*

Proof. Suppose a binary LRS over R solves to give $u_n = A\lambda_1^n + B\lambda_2^n$, where λ_1 and λ_2 are the two roots of the characteristic equation, and where A and B are non-zero. Suppose also that the LRS has two zeroes, u_r and u_{r+s}. Then $u_r = A\lambda_1^r + B\lambda_2^r = 0$, which gives $A\left(\frac{\lambda_1}{\lambda_2}\right)^r + B = 0$. Similarly we have $A\left(\frac{\lambda_1}{\lambda_2}\right)^{r+s} + B = 0$. Subtracting these two equations gives

$$A\left(\left(\frac{\lambda_1}{\lambda_2}\right)^{r+s} - \left(\frac{\lambda_1}{\lambda_2}\right)^r\right) = 0,$$

which yields $\left(\frac{\lambda_1}{\lambda_2}\right)^s = 1$, and thus the LRS is degenerate. $\square$

We also have $\mu_0(n, R) \leqslant \mu(n, R) \leqslant \mu_0(n+1, R)$, since if P is an order-n LRS, $P - c$ is an order-m LRS Q, where $m \leqslant n+1$. (If the characteristic equation of P has a root that is a root of unity, then Q will be degenerate, since 1 will certainly be one of the roots of the characteristic equation of Q.)

Let K be any field. It is clear from the above that $\mu_0(2, K) = 1$, since K is a ring. What might $\mu(2, K)$ be? This is much less obvious. Beukers and Schlickewei [12] have obtained the bound

$$\mu(2, \mathbb{C}) \leqslant 61;$$

the actual value is conjectured to be 6. For the ring $\mathbb{Z}$, Kubota [37], building on work by Laxton, proved that

$$\mu(2, \mathbb{Z}) \leqslant 4.$$

Beukers [10] has improved this result by showing that

$$m(P, c) + m(P, -c) \leqslant 3$$

and so $\mu(2, \mathbb{Z}) \leqslant 3$ for all binary integer non-degenerate LRSs (with a number of special cases that can be dealt with.) Beukers [11] has also shown that

$$\mu_0(3, \mathbb{Z}) = 6,$$

and this figure of 6 can be obtained, as shown by Berstel's sequence. Bavencoffe and Bezivin[7] have proved that

$$\mu_0(n, \mathbb{Z}) \geqslant \frac{n(n+1)}{2} - 1$$

and moreover, they have computational evidence suggesting that this is sharp for $n \geqslant 4$ – they show that the sequence with the characteristic polynomial $f(\lambda) = \frac{\lambda^{n+1} + (-2)^{n-1}\lambda + (-2)^n}{\lambda + 2}$ and with initial values $a_0 = 1$, $a_1 = \ldots = a_{n-1} = 0$ has at least that many zeroes. For $n = 3$, this result tells us that $\mu_0(3, \mathbb{Z}) \geqslant 5$; Berstel's sequence, with its extra zero at $n = 52$, shows the bound is not precise here. Williams [59] has shown that an LRS satisfying $P_{n+k} = s_1 P_{k+1} + s_2 P_k$ for any s_1, s_2 with $P_0 = 1$ and $P_1 = \ldots = P_{n-1} = 0$ has at least $\frac{n(n-1)}{2}$ zeroes.

6.3 Returning to the cycle given by $\frac{ax-1}{x+1}$

How does this illuminate our problem? We have to find the zeroes of P as defined in (6.2) for different values of a and n. We have that $\mu_0(2,\mathbb{Z}) = 1$, so for each value of a, there can be a maximum of one zero. If P is zero for some value of n, then A^n will be a multiple of the identity matrix, and A^{nm} will be too for all $m \in \mathbb{N}^+$. So P is zero for the arithmetic sequence of values $n, 2n, 3n$ and so on; in other words, P is degenerate, which means that $\frac{\lambda_1}{\lambda_2}$ is a root of unity, where λ_1 and λ_2 are the two roots of P's characteristic equation. This is $x^2-(a+1)x+(a+1)=0$, which gives $\lambda_1, \lambda_2 = \frac{a+1\pm\sqrt{a^2-2a-3}}{2}$, and we thus have $\frac{\lambda_1}{\lambda_2}, \frac{\lambda_2}{\lambda_1} = \frac{a-1\pm\sqrt{a^2-2a-3}}{2}$. Figure 6.1 shows that P can therefore only ever be degenerate for $a =$ -1, 0, 1, 2 or 3, since otherwise $\frac{\lambda_1}{\lambda_2}$ cannot be a root of 1.

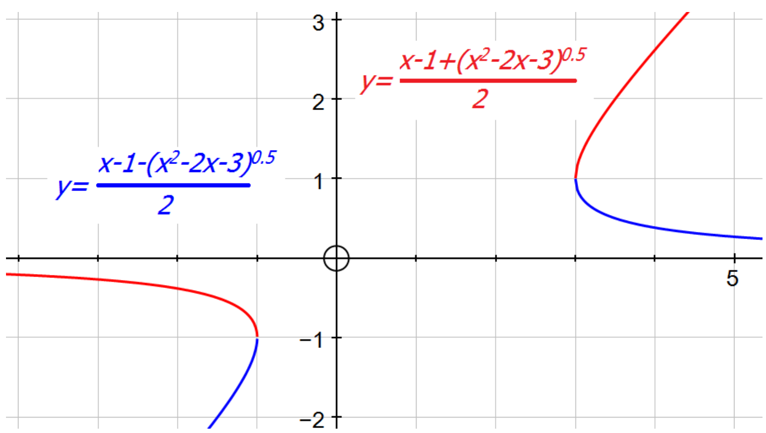


Figure 6.1: $y = \frac{x-1\pm\sqrt{x^2-2x-3}}{2}$

When $a = -1, \alpha_{-1} = \frac{\lambda_1}{\lambda_2} = \frac{\lambda_2}{\lambda_1} = -1$, and $\alpha_{-1}^2 = 1$. However, this means $A = \begin{pmatrix} -1 & -1 \\ 1 & 1 \end{pmatrix}$, and $\frac{-x-1}{x+1} = -1$, so we never return to x.

When $a = 0, \alpha_0, \beta_0 = \frac{\lambda_1}{\lambda_2}, \frac{\lambda_2}{\lambda_1} = -\frac{1}{2} \pm \frac{\sqrt{3}}{2}i$, and $\alpha_0^3 = \beta_0^3 = 1$, giving a period-3 cycle.

When $a = 1, \alpha_1, \beta_1 = \frac{\lambda_1}{\lambda_2}, \frac{\lambda_2}{\lambda_1} = \pm i$, and $\alpha_1^4 = \beta_1^4 = 1$, giving a period-4 cycle.

When $a = 2, \alpha_2, \beta_2 = \frac{\lambda_1}{\lambda_2}, \frac{\lambda_2}{\lambda_1} = \frac{1}{2} \pm \frac{\sqrt{3}}{2}i$, and $\alpha_2^6 = \beta_2^6 = 1$, giving a period-6 cycle.

When $a = 3, \alpha_3, \beta_3 = \frac{\lambda_1}{\lambda_2}, \frac{\lambda_2}{\lambda_1} = 1$, and $\alpha_3^1 = \beta_3^1 = 1$. However, if $A = \begin{pmatrix} 3 & -1 \\ 1 & 1 \end{pmatrix}$, then it is easily seen that $A_{11}^n \neq A_{22}^n$ for all n, and so we never have a cycle. Thus $a = 0, 1, 2$ are the only values for $a \in \mathbb{N}$ for which $x \mapsto \frac{ax-1}{x+1}$ gives a cycle, and the LRS $x, \frac{ax-1}{x+1}, \ldots$ can only be periodic when a is 0, 1 or 2.

6.4 Order-1 cycles; the general case

I began this chapter by exploring the iterations of the rational function $\frac{ax-1}{x+1}$. What happens if we investigate the general case? Consider the rational function $\frac{ax+b}{cx+d}$, where a, b, c, and d are integers – when is this periodic? If $f(x) = \frac{ax+b}{cx+d}$, when does $f^n(x) = x$? Once again, we can consider powers of a matrix, this time $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, since iterating $f(x)$ is equivalent to taking powers of B, where $\begin{pmatrix} ka & kb \\ kc & kd \end{pmatrix} \equiv B$.

$$B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$B^2 = \begin{pmatrix} a^2 + bc & ab + bd \\ ac + cd & bc + d^2 \end{pmatrix}$$

$$B^3 = \begin{pmatrix} a^3 + 2abc + bcd & b(a^2 + ad + bc + d^2) \\ c(a^2 + ad + bc + d^2) & abc + d(2bc + d^2) \end{pmatrix}$$

$$B^4 = \begin{pmatrix} a^4 + 3a^2bc + 2abcd + b^2c^2 + bcd^2 & b(a+d)(a^2 + 2bc + d^2) \\ c(a+d)(a^2 + 2bc + d^2) & a^2bc + 2abcd + b^2c^2 + 3bcd^2 + d^4 \end{pmatrix}$$

$$B_{11}^5 = a^5 + 4a^3bc + 3a^2bcd + abc(3bc + 2d^2) + bcd(2bc + d^2)$$

$$B_{12}^5 = b(a^4 + a^3d + a^2(3bc + d^2) + ad(4bc + d^2) + b^2c^2 + 3bcd^2 + d^4)$$

$$B_{21}^5 = c(a^4 + a^3d + a^2(3bc + d^2) + ad(4bc + d^2) + b^2c^2 + 3bcd^2 + d^4)$$

$B^5_{22} = a^3bc + 2a^2bcd + abc(2bc + 3d^2) + d(3b^2c^2 + 4bcd^2 + d^4)$

$B^6_{11} = a^6 + 5a^4bc + 4a^3bcd + 3a^2bc(2bc + d^2) + 2abcd(3bc + d^2)$
$+bc(b^2c^2 + 3bcd^2 + d^4)$

$B^6_{12} = b(a + d)(a^4 + a^2(4bc + d^2) + 2abcd + 3b^2c^2 + 4bcd^2 + d^4)$

$B^6_{21} = c(a + d)(a^4 + a^2(4bc + d^2) + 2abcd + 3b^2c^2 + 4bcd^2 + d^4)$

$B^6_{22} = a^4bc + 2a^3bcd + 3a^2bc(bc + d^2) + 2abcd(3bc + 2d^2) + b^3c^3$

$+6b^2c^2d^2 + 5bcd^4 + d^6$

Inspection suggests that

$$B^i = \begin{pmatrix} P_i(a,d) & bQ_i \\ cQ_i & P_i(d,a) \end{pmatrix}, \tag{6.6}$$

where P and Q form sequences of polynomials (P_i) and (Q_i) in a, b, c and d. We have that P_i and Q_i are symmetric in b and c; each Q_i is symmetric in a and d, while each P_i is not. I will write $P_i(a,b,c,d)$ as $P_i(a,d)$, $P_i(d,c,b,a)$ as $P_i(d,a)$, and $Q_i(a,b,c,d) = Q_i(d,c,b,a)$ as Q_i. We have (straightforwardly by induction, as before) that these polynomials obey the recurrence relations

$$P_{n+1}(a,d) = aP_n(a,d) + bcQ_n,$$

$$Q_{n+1} = aQ_n + P_n(d,a), \tag{6.7}$$

$$Q_{n+1} = dQ_n + P_n(a,d), \tag{6.8}$$

and

$$P_{n+1}(d,a) = dP_n(d,a) + bcQ_n.$$

The second pair of equations are simply the first pair with a and d transposed. These recurrences yield

$$P_{n+1}(a,d) = (a + d)P_n(a,d) - (ad - bc)P_{n-1}(a,d)$$

and

$$Q_{n+1} = (a + d)Q_n - (ad - bc)Q_{n-1}. \tag{6.9}$$

So P and Q are generated by the same binary linear recurrence relation; they differ only since their starting values are different.

$$P_1(a,d) = a, P_2(a,d) = a^2 + bc, P_3(a,d) = a^3 + 2abc + bcd$$

$$Q_1 = 1, Q_2 = a + d, Q_3 = a^2 + ad + bc + d^2$$

Two key variables from our starting matrix B appear in (6.9) – the trace $a + d$ (equal to the sum of the eigenvalues) and the determinant $ad - bc$. Now suppose $Q_n = 0$ for some a, b, c, d and some n. Then (6.6) becomes $\begin{pmatrix} P_n(a,d) & 0 \\ 0 & P_n(d,a) \end{pmatrix}$. Now by recurrence relations (6.8) and (6.7), if $Q_n = 0$ then $P_n(a,d) = P_n(d,a)$, and so the mapping $x \mapsto \frac{ax+b}{cx+d}$ is periodic. So we have a zero for the polynomial Q_n just if the rational function $\frac{ax+b}{cx+d}$ is period-n. It appears also that $Q_n | Q_{mn}$ for $m, n \in \mathbb{N}^+$. Now

$Q_1 = 1,$

$Q_2 = a + d,$

$Q_3 = a^2 + ad + bc + d^2,$

$Q_4 = (a + d)(a^2 + 2bc + d^2),$

$Q_5 = a^4 + a^3 d + 3a^2 bc + a^2 d^2 + 4abcd + ad^3 + b^2 c^2 + 3bcd^2 + d^4,$

$Q_6 = (a + d)(a^2 + ad + bc + d^2)(a^2 - ad + 3bc + d^2),$

$Q_7 = a^6 + a^5 d + 5a^4 bc + a^4 d^2 + 8a^3 bcd + a^3 d^3 + 6a^2 b^2 c^2 + 9a^2 bcd^2 + a^2 d^4$

$+9ab^2 c^2 d + ad^5 + b^3 c^3 + 6b^2 c^2 d^2 + 5bcd^4 + d^6,$

and

$Q_8 = (a + d)(a^2 + 2bc + d^2)(a^4 + 4a^2 bc + 4abcd + 2b^2 c^2 + 4bcd^2 + d^4).$

So we can put $B_{12}^n = 0$ for each n and treat this as a polynomial in b. When is this zero? If $a = d$ and $b = c = 0$, we get period 1:

$$x, x, \ldots.$$

If $a = -d$ we get period 2:

$$x, \frac{ax+b}{cx-a}, x, \ldots.$$

If $b = \frac{-a^2-ad-d^2}{c}$, we get period 3:

$$x, \frac{acx-(a^2+ad+d^2)}{c^2x+cd}, \frac{cdx+(a^2+ad+d^2)}{-c^2x+ac}, x, \ldots.$$

If $b = \frac{-a^2-d^2}{2c}$, we get period 4:

$$x, \frac{2acx-a^2-d^2}{2c^2x+2cd}, \frac{c(a-d)x-a^2-d^2}{2c^2x-ac+cd}, \frac{2cdx+a^2+d^2}{-2c^2x+2ac}, x, \ldots.$$

If $b = \frac{-a^2+ad-d^2}{3c}$, we get period 6:

$$x, \frac{3acx-a^2+ad-d^2}{3c^2x+3cd}, \frac{c(2a-d)x-a^2+ad-d^2}{3c^2x-c(a-2d)},$$

$$\frac{3c(a-d)x-2(a^2-ad+d^2)}{6c^2x-3c(a-d)}, \frac{cx(a-2d)-(a^2-ad+d^2)}{3c^2x-c(2a-d)},$$

$$\frac{3cdx+a^2-ad+d^2}{-3c^2x+3ac}, x, \ldots.$$

We would like to prove that for no other n is the recurrence defined by this rational function periodic for integers a, b, c and d. Can $Q_5 = 0$? Treating $a^4 + a^3d + 3a^2bc + a^2d^2 + 4abcd + ad^3 + b^2c^2 + 3bcd^2 + d^4$ as a quadratic in b and solving gives

$$b = \frac{-3a^2-4ad-3d^2 \pm \sqrt{5}(a+d)^2}{2c}$$

This includes $\sqrt{5}$ unless $a = -d$, which gives $b = \frac{-a^2}{c}$, yielding the matrix $B \equiv \begin{pmatrix} ac & -a^2 \\ c^2 & -ac \end{pmatrix}$, where $B^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, so we have no joy.

It remains now to examine the structure of Q; can we find a formula for Q_i in terms of i? For $i = 2$, 3, 4 and 6 there are integers a, b, c and d so that Q_i is zero; can Q be zero anywhere else?

The characteristic equation is $\lambda^2 - (a+d)\lambda + ad - bc = 0$, which has solutions $\lambda_1 = \frac{\sqrt{(a^2-2ad+4bc+d^2)}+a+d}{2}$ and $\lambda_2 = \frac{-\sqrt{(a^2-2ad+4bc+d^2)}+a+d}{2}$. The general solution to the LRS is $Q_n = p\lambda_1^n + q\lambda_2^n$, and p and q can be found from $Q_1 = 1$, and $Q_2 = a + d$, giving

$$Q_n = \frac{2^{-n}((a+d+s)^n - (a+d-s)^n)}{s}$$

where $s = \sqrt{a^2 - 2ad + 4bc + d^2}$. Putting n equal to 2, 3, 4 and 6 gives the solutions over $\mathbb{Z}$ we have above. Now let

$$\alpha_1, \alpha_2 = \frac{\lambda_1}{\lambda_2}, \frac{\lambda_2}{\lambda_1} = \frac{a^2 + 2bc + d^2 \pm (a+d)\sqrt{(a-d)^2 + 4bc}}{2(ad-bc)}. \tag{6.10}$$

For periodicity, we require $\alpha^n = 1$, and so $\alpha = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})$ for some n. We have by (6.10) that in this case $\cos(\frac{2\pi}{n})$ must be rational. Now we have from Theorem 6.4 below that if $\cos(\frac{2\pi}{n})$ is rational, then $\cos(\frac{2\pi}{n}) = 0$ or $\pm\frac{1}{2}$ or ± 1. Now from Table 6.1, we can see that $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ can be period-n just if $n = 1, 2, 3, 4$, or 6, since $\frac{1}{2} < \cos(\frac{2\pi}{n}) < 1$ for $n > 6$.

n	$\cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})$	real part rational
1	$\cos(2\pi) + i\sin(2\pi)$	1
2	$\cos(\pi) + i\sin(\pi)$	-1
3	$\cos(\frac{2\pi}{3}) + i\sin(\frac{2\pi}{3})$	$-\frac{1}{2} + \frac{\sqrt{3}}{2}i$
4	$\cos(\frac{\pi}{2}) + i\sin(\frac{\pi}{2})$	i
5	$\cos(\frac{2\pi}{5}) + i\sin(\frac{2\pi}{5})$	$\times$
6	$\cos(\frac{\pi}{3}) + i\sin(\frac{\pi}{3})$	$\frac{1}{2} + \frac{\sqrt{3}}{2}i$
7	$\cos(\frac{2\pi}{7}) + i\sin(\frac{2\pi}{7})$	$\times$
...	...	...

Table 6.1: n^{th} roots of unity with real part rational

Theorem 6.4. *If* $\cos(\frac{2\pi}{n})$ *is rational, then* $\cos(\frac{2\pi}{n}) = 0$ *or* $\pm\frac{1}{2}$ *or* ± 1.

Proof. We have

$$\cos((n+1)\theta) + \cos((n-1)\theta) = 2\cos(\theta)\cos(n\theta). \tag{6.11}$$

If we write $x = 2\cos(\theta)$, we can define a polynomial in $\mathbb{Z}[x]$ by $P_n(x) = 2\cos(n\theta)$. Then (6.11) can be written as

$$P_{n+1}(x) = xP_n(x) - P_{n-1}(x), \tag{6.12}$$

with $P_0(x) = 2, P_1(x) = x$. (Note the connection here between P_n and the Chebyshev polynomials of the first and second type, T_n and U_n, which both share the recurrence relation (8.11) with P_n, but with different initial conditions. The polynomials T_n and U_n are central to Chapter 15.) We can easily show by induction that $P_n(x)$ is monic and of degree n. Now suppose that $\cos(\frac{m\pi}{n}) = \frac{a}{b}$ in its lowest terms. Then $P_n(\frac{2a}{b}) = 2\cos(m\pi) = 2(-1)^m \in \mathbb{Z}$. Thus $x = \frac{2a}{b}$ is a solution of the equation $x^n + \cdots + c_{n-1}x + c_n = 0$, for some $c_i \in \mathbb{Z}$. Now I quote the 'rational roots test' – if $\frac{p}{q}$ is a solution to $a_n x^n + \cdots + a_0 = 0$, where each $a_i \in \mathbb{Z}$, then $p|a_0$ and $q|a_n$. This tells us that $b = 1$ and so $\frac{2a}{b} = \cos(\frac{m\pi}{n})$ must be an integer, and so $\frac{2a}{b} = 0, \pm 1, \pm 2$ are the only possibilities. Thus we have that if $\cos(\frac{m\pi}{n})$ is rational, then it equals $0, \pm\frac{1}{2}$, or ± 1. $\square$

6.5 Using the cyclotomic polynomials

A quick and clean proof of the fact that rational order-1 cycles can only be period-K where $K \in \{1, 2, 3, 4, 6\}$ is given by Cull, Flahive and Robson [22]. Say that we are iterating the map $f : x \mapsto \frac{ax+b}{cx+d}$ where a, b, c, d are rational. As we have seen, the characteristic equation for the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ (and for the LRS P it defines) is

$$\lambda^2 - (a + d)\lambda + (ad - bc) = 0.$$

Call the two roots of this polynomial λ_1 and λ_2; consider the quadratic equation with roots $\frac{\lambda_1}{\lambda_2}$ and $\frac{\lambda_2}{\lambda_1}$. It will be of the form $\gamma^2 + \theta\gamma + 1 = 0$, since the product of the roots is 1. Now

$$-\theta = \frac{\lambda_1}{\lambda_2} + \frac{\lambda_2}{\lambda_1} = \frac{\lambda_2^2 + \lambda_1^2}{\lambda_2\lambda_1} = \frac{(\lambda_2 + \lambda_1)^2}{\lambda_2\lambda_1} - 2 = \frac{(a + d)^2}{ad - bc} - 2,$$

which is rational. Now we know that if $f^K(x) = x$, where K is minimal, and P is degenerate, then γ must be a primitive K^{th} root of unity, and is thus a root of $\Phi_K(x)$, the K^{th} cyclotomic polynomial. This has integer coefficients, is irreducible in the ring $\mathbb{Z}[x]$ and is of degree $\phi(K)$. But if γ is a root of $\Phi_K(x) = 0$ AND the root of a rational quadratic equation, by the irreducibility of $\Phi_K(x), \phi(K)$ is 1 or 2. Now it is easily proved that if $n \geqslant 7$, then $\phi(n) > 2$. So $K \in \{1, 2, 3, 4, 6\}$; notice that K cannot be 5, since $\phi(5) = 4$.

6.6 A more general perspective

We now deal more subtly with the problem of duplication first encountered in Chapter 2. Suppose that $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, with $a, b, c, d \in \mathbb{Q}$. We are trying to solve $B^n = \lambda I$ for some scalar λ. The matrix B is in $GL_2(\mathbb{Q})$, the set of 2 by 2 invertible matrices with coefficients in $\mathbb{Q}$. Consider the natural homomorphism $\pi : GL_2(\mathbb{Q}) \mapsto PGL_2(\mathbb{Q})$, which is $GL_2(\mathbb{Q})/N$ where

$$N = \{\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} : \lambda \in \mathbb{Q}^*\},$$

which is a normal subgroup of $GL_2(\mathbb{Q})$.

If $B^n = \lambda I$, then $\pi(B^n) = \pi(\lambda I)$. Now $\pi(B^n) = (\pi(B))^n$, while $\pi(\lambda I) = \mathrm{Id}_{PGL_2(\mathbb{Q})}$. We also have that if $(\pi(B))^n = \mathrm{Id}_{PGL_2(\mathbb{Q})}$, then $\pi(B^n) = \mathrm{Id}_{PGL_2(\mathbb{Q})}$, which gives $B^n \in \mathrm{Ker}(\pi) = N$, so $B^n = \lambda I$. So solving $B^n = \lambda I$ is the same as discovering when $\pi(B)$ has order dividing n in $PGL_2(\mathbb{Q})$. This is part of a wider question over which finite subgroups are possible in the classical groups over any field, as tackled by Beauville [8] – I have explored here only the possible finite cyclic subgroups for $PGL_2(\mathbb{Q})$.

Chapter 7

The Mini-Cross-Ratio

We have seen how the cross-ratio provides a method for the construction of order-2 period-5 cycles, and how the method extends to providing more generally order-n period-$(n+3)$ cycles. The question arises, are there functions akin to the cross-ratio that yield cycles of other periods in a similarly happy fashion? Given its similarity to the cross-ratio in regard to the dilation, translation and reflection laws, the mini-cross-ratio (or MC) that we met in Chapter 3 suggests itself. We have defined $\mathrm{MC}(a,b,c,d)$ as $\frac{a-b}{c-d}$. We will now see that this function allows for the construction of order-n cycles that are period-$(n+2)$ for $n \geqslant 3$.

7.1 The geometrical significance of the MC

Firstly we can note that just as the cross-ratio has profound geometrical significance, it is not hard to find similar resonances for the MC. The humble gradient of the line joining (x_1, y_1) to (x_2, y_2) is of course $\mathrm{MC}(y_1, y_2, x_1, x_2)$. The condition for four lines $y = a_1x + a_2, y = b_1x + b_2, y = c_1x + c_2$, and $y = d_1x + d_2$ to meet is that both

$$\mathrm{MC}(a_2, b_2, b_1, a_1) = \mathrm{MC}(c_2, d_2, d_1, c_1)$$

and

$$\mathrm{MC}(a_1b_2, a_2b_1, a_1, b_1) = \mathrm{MC}(c_1d_2, c_2d_1, c_1, d_1).$$

The cross-ratio arose from considering four coincident lines and a transversal – so does the MC (see Figure 2.1 once more). Calculating $\frac{AB}{CD}$ rather than $\frac{AB.CD}{AC.BD}$ gives $\frac{(a-b)(c-m)(d-m)}{(c-d)(a-m)(b-m)}$. If we let m be infinite here, we have MC(a, b, c, d).

7.2 Finding cycles with the MC

So how does the MC help us in finding cycles? Put

$$x = \frac{a-b}{c-d}, y = \frac{b-c}{d-e}, z = \frac{c-d}{e-a}, \alpha = \frac{d-e}{a-b}.$$

Eliminating a and b before c and substituting into the fourth equation for c allows d and e to cancel. We arrive at

$$x, y, z, -\frac{xz+z+1}{xz(y+1)}, -\frac{y+1}{y(xz+z+1)}, x, y, z, \ldots,$$

a regular order-3 period-5 cycle. As with the cross-ratio, permuting a, b, c and d creates different cycles, in this case one for each of the 12 values the mini-cross-ratio can take. These 12 recurrences are given by the functions

$$-\frac{xz+z+1}{xz(y+1)}, \frac{xz-z+1}{xz(1-y)}, \frac{-1}{xyz+yz+z+1}, \frac{1}{yz+1-xyz-z},$$

$$\frac{yz-x-1}{xyz-xy-xz+1}, \frac{x+yz-1}{xyz+xy+xz-1}, \frac{-y-1}{xyz+xy+y}, \frac{y-1}{xyz-xy+y},$$

$$-\frac{xyz+xy+x+1}{xyz}, \frac{1-xyz+xy-x}{xyz}, \frac{y+z-xyz-1}{xyz-x+yz}, \frac{xyz-y-z-1}{xyz-x-yz}.$$

We can add parameters to the cycles as we did before. We find

$$x = \frac{p\mathrm{MC}(a, b, c, d)+q}{r\mathrm{MC}(a, b, c, d)+s}, y = \frac{p\mathrm{MC}(b, c, d, e)+q}{r\mathrm{MC}(b, c, d, e)+s},$$

$$z = \frac{p\mathrm{MC}(c, d, e, a)+q}{r\mathrm{MC}(c, d, e, a)+s}, \alpha = \frac{p\mathrm{MC}(d, e, a, b)+q}{r\mathrm{MC}(d, e, a, b)+s}$$

yields the regular order-3 period-5 cycle

$$x, y, z, f(x, y, z), g(x, y, z), x, y, z, \ldots,$$

where $f, g \in \mathbb{Q}(x, y, z)$ are regular and free of a, b, c, d, and e; f has 40 terms in both the numerator and the denominator. The method extends to order-n, period-$(n+2)$ cycles for $n > 3$ in the obvious way.

7.3 The RMC and its use to create cycles

What happens when we look at **three** coincident lines and a transversal? This leads to what in Chapter 3 we called the reduced mini-cross-ratio, or RMC. Calculating $\frac{AB}{AC}$ in Figure 7.1 gives $\frac{(a-b)(c-m)}{(a-c)(b-m)}$; once again taking m as infinite, we have $\mathrm{RMC}(a, b, c) = \frac{(a-b)}{(a-c)}$. This function also satisfies the dilation, translation and reflection laws – could it also produce Lyness cycles?

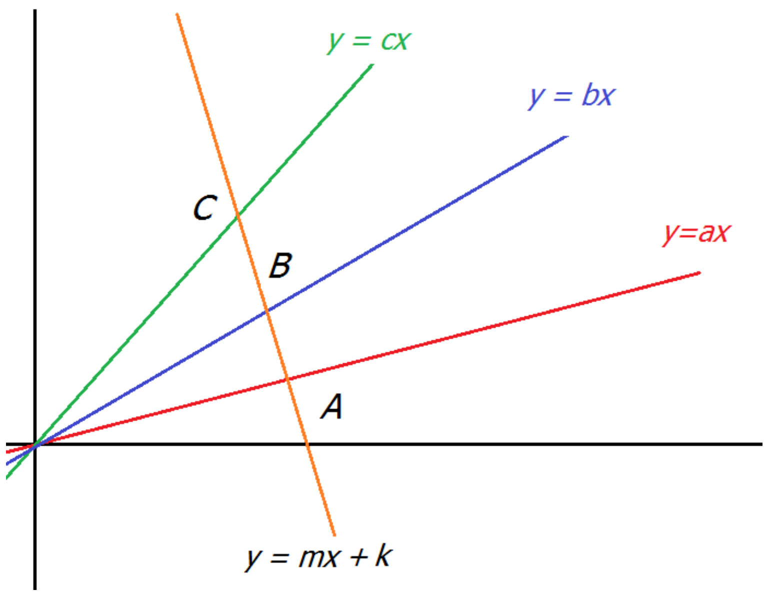


Figure 7.1: The Mini-cross-ratio

Consider

$$x = \frac{a-b}{a-c}, y = \frac{b-c}{b-d}, z = \frac{c-d}{c-a}.$$

We can find a from the first equation, d from the second, and substituting into the third, we arrive at

$$z = -\frac{(x-1)(y-1)}{y},$$

and

$$x, y, -\frac{(x-1)(y-1)}{y}, \frac{xy-x+1}{1-x}, x, y \dots$$

is one of the regular binary period-4 cycles that we met in Chapter 4.

Rather as with $C(a,b,c,d)$, the possible RMCs generate six sets of values, each of which generate a regular period-4 cycle. The six cycles are generated by

$$\frac{a-b}{a-c}, \frac{a-c}{a-b}, \frac{a-b}{a-d}, \frac{a-d}{a-b}, \frac{a-c}{a-d}, \frac{a-d}{a-c},$$

and are

$$x, y, -\frac{(x-1)(y-1)}{y}, \dots \quad \text{and its reverse (or dual)} \quad x, y, \frac{xy-x+1}{1-x}, \dots,$$

$$x, y, \frac{x}{(x-1)(y-1)}, \dots, \quad \text{and its reverse (or dual)} \quad x, y, \frac{xy-x}{xy-x+1}, \dots,$$

and

$$x, y, \frac{1}{xy-y+1} \dots, \quad \text{and its reverse (or dual)} \quad x, y, \frac{xy-x-1}{xy} \dots.$$

We can add parameters as we did above, since

$$x = \frac{p\mathrm{RMC}(a,b,c)+q}{r\mathrm{RMC}(a,b,c)+s}, y = \frac{p\mathrm{RMC}(b,c,d)+q}{r\mathrm{RMC}(b,c,d)+s}, z = \frac{p\mathrm{RMC}(c,d,a)+q}{r\mathrm{RMC}(c,d,a)+s}$$

yields the regular period-4 binary cycle that begins

$$x, y,$$

$$\frac{xy(p(r+s)^2+qrs)-x(p^2(r+s)+pq(r+s)+q^2r)-py(p(r+s)+q(r+2s))+p(p^2+2pq+2q^2)}{rxy(r^2+2rs+2s^2)-rx(p(r+s)+q(r+2s))-y(p(r^2+rs+s^2)+qr(r+s))+p^2r+pq(2r+s)+q^2r}, \dots.$$

The MC and RMC methods both yield order-n period-$(n+2)$ recurrences – are these significantly different? Is, for example, $\frac{(x-1)(y-1)(z-1)}{z(xy-x+1)}$, as given by the RMC method, conjugate to $\frac{xz-z+1}{xz(1-y)}$ as given by the MC method? Checking this appears to be a difficult task that pushes Derive to its limits.

7.4 The Open Cross-ratio

Let $\mathrm{OC}(a,b,c,d) = \frac{a-b+c-d}{a-c+b-d}$. The lack of brackets leads me to christen this the Open Cross-ratio function. Now the equations

$$x = \mathrm{OC}(a,b,c,d), y = \mathrm{OC}(b,c,d,e), z = \mathrm{OC}(c,d,e,a)$$

give us expressions for a, b and c in terms of x, y, z, d and e. Substituting these into $\mathrm{OC}(d,e,a,b)$ sees d and e cancel, yielding $-\frac{3xyz+3xy+3xz+5yz-x-3y-3z+1}{xyz+xy+xz+3yz-3x+3y+3z-1}$. As we by now expect,

$$x, y, z, -\frac{3xyz + 3xy + 3xz + 5yz - x - 3y - 3z + 1}{xyz + xy + xz + 3yz - 3x + 3y + 3z - 1},$$

$$-\frac{x(y(3z+5) + 3z - 3) + (z-1)(3y-1)}{x(y+1)(z+3) + y(z+3) - 3z - 1}, x, y, z, \cdots .$$

is an order-3 period-5 cycle; in general, we can find order-n period-$(n+2)$ cycles via the OC function. We also have (by putting $b = d$) the *Reduced Open Cross-ratio*, $\mathrm{ROC}(a,b,c) = \frac{a+c-2b}{a-c}$, which also provides order-n period-$(n+2)$ cycles. The equations

$$x = \mathrm{ROC}(a,b,c), y = \mathrm{ROC}(b,c,d), z = \mathrm{ROC}(c,d,a)$$

give $z = \frac{x-xy-2}{y+1}$, and

$$x, y, \frac{x - xy - 2}{y+1}, \frac{xy + y + 2}{1 - x}, x, y, \cdots$$

is a regular order-2, period-4 cycle. Derive is able to confirm that this cycle is conjugate to $x, y, -\frac{(x-1)(y-1)}{y}, \ldots$, where $u(x)$ here is $\frac{x+1}{2}$. The parameters p, q, r and s and can be added to OC and ROC cycles in exactly the way that we have done before.

7.5 Some further questions

It is noticeable that the cross-ratio method and its extensions described here consistently produce regular cycles, whatever the order; can this be proved in general? It seems sensible to attempt an induction proof, and while appearing to be possible, this becomes surprisingly complicated very quickly. Do these methods generate all possible such regular cycles? Both the MC and the RMC functions create order-n, period-$(n+2)$ cycles, while the cross-ratio deals with order-n, period-$(n+3)$ cycles (it is interesting to reflect that the RMC is the cross-ratio with $d = \infty$ – why then does it give cycles of a different period?). Can we find cross-ratio-type functions that will deal naturally with other periods and orders? We seem to be developing a notion of what a cross-ratio-type function (CTF) should look like.

7.6 Cross-ratio-type functions

Let $f(a_1, a_2 \ldots a_n)$ be a CTF, where T is the set of cardinality n from which the distinct a_i are drawn (without repetition), and S is the set of possible values that f can take as we vary the a_i.

We need that taking $f(a_1 + k, a_2 + k, \ldots, a_n + k)$ should give us the same set S; the translation law applies. In shorthand, $S(T) = S(T + k)$.

We require that $f(ka_1, ka_2 \ldots, ka_n)$ should give us the same set S; the dilation law applies, and so does the reflection law. In shorthand, $S(T) = S(kT)$.

We also require that f will generate Lyness cycles in the way that we have discussed above. These requirements are seen in Table 7.1.

CTF	$n = \|T\|$	$\|S\|$	$n!/\|S\|$	Lyness cycles?
$\mathrm{C}(a, b, c, d)$	4	6	4	Yes
$\mathrm{MC}(a, b, c, d)$	4	12	2	Yes
$\mathrm{RMC}(a, b, c)$	3	6	1	Yes
$\mathrm{OC}(a, b, c, d)$	4	12	2	Yes
$\mathrm{ROC}(a, b, c)$	3	6	1	Yes

Table 7.1: Cross-ratio-type functions

It is this final condition that proves difficult. We can easily construct CTFs where $S(T) = S(kT)$ and $S(T) = S(T + k)$, perhaps drawing on simple situations thrown up by geometry; a magic square obeys these laws. But finding a new such function that generates Lyness cycles proves tricky. For example, we might take a transversal $y = mx + k$ crossing six coincident lines, and arrive at $\frac{AB.CD.EF}{AD.BE.CF} = \frac{(a-b)(c-d)(e-f)}{(a-d)(b-e)(c-f)}$ (which is free of m and k). Intuition might suggest that Lyness cycles should flow from this, but they don't appear to. Are there any other CTFs that will successfully produce Lyness cycles, especially of orders and periods that are different to those we already have here?

The cross-ratio is a projective invariant, that is, it is invariant under a Mobius transformation, or $C(a,b,c,d) = C(f(a), f(b), f(c), f(d))$ where f is a fractional linear map. We could regard CTFs as those functions that are invariant under the Mobius group, or some subgroup of this. There is a substantial literature on invariant theory, that includes higher order invariants; to explore whether or not these give rise to cycles would a worthwhile area for future research.

Chapter 8

The Elliptic Curve Connection

8.1 Multiplying the terms of an order-1 cycle

In 1945, with peacetime in sight, Lyness continued his correspondence in *The Mathematical Gazette* [43] by shifting his concern towards geometrical interpretations of his cycles. He starts by quoting the order-1 period-4 cycle

$$x, \frac{3x+5}{1-x}, -\frac{x+5}{x+1}, \frac{x-5}{x+3}, x \ldots.$$

'What happens,' he asked, 'If we multiply the four terms together and set this to be a constant?' We derive the equation

$$x \times \frac{3x+5}{1-x} \times -\frac{x+5}{x+1} \times \frac{x-5}{x+3} = k.$$

Now if x is a solution to this, then $\frac{3x+5}{1-x}$ will be too, since substituting this for x will simply have the effect of cycling the terms along:

$$\frac{3x+5}{1-x} \times \frac{3\frac{3x+5}{1-x}+5}{1-\frac{3x+5}{1-x}} \times -\frac{\frac{3x+5}{1-x}+5}{\frac{3x+5}{1-x}+1} \times \frac{\frac{3x+5}{1-x}-5}{\frac{3x+5}{1-x}+3} = k. \tag{8.1}$$

So we have $x(x+5)(x-5)(3x+5) - k(x+1)(x-1)(x+3) = 0$, or

$$3x^4 + x^3(5-k) - x^2(3k+75) + x(k-125) + 3k = 0$$

as the quartic equation that results. So if we choose $x = 3$, say, as a root, giving $k = -14$, we can say immediately that the other roots are $-7, -2$ and $-\frac{1}{3}$, as given by

$$3, \frac{3(3)+5}{1-(3)}, -\frac{(3)+5}{(3)+1}, \frac{(3)-5}{(3)+3}. \tag{8.2}$$

8.2 The order-2 period-5 case

Lyness made the natural step of asking what happens if we apply this idea to his binary pentagonal recurrence (1.3). He found that the function

$$f(x, y) = \frac{(x+1)(y+1)(x+y+1)}{xy}$$

is obtained as the product of the five terms. Suppose that $f(a, b) = k$; if we define a curve by $f(x, y) = k$, or

$$(x+1)(y+1)(x+y+1) = kxy, \tag{8.3}$$

then the point $A = (a, b)$ is clearly on this cubic curve. Figure 8.1 shows the case when $k = 2$. Now, as Lyness points out, if (a, b) is on the curve then $\left(b, \frac{b+1}{a}\right)$, $\left(\frac{b+1}{a}, \frac{a+b+1}{ab}\right)$, $\left(\frac{a+b+1}{ab}, \frac{a+1}{b}\right)$ and $\left(\frac{a+1}{b}, a\right)$ will be also, by the cycling phenomenon observed in (8.1).

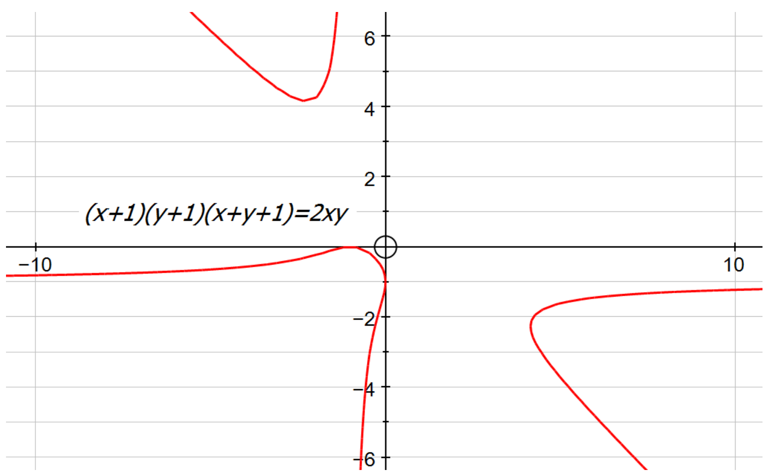


Figure 8.1: $(x + 1)(y + 1)(x + y + 1) = 2xy$

8.3 Invariants

Suppose we have the recurrence $x, y, f(x, y), \ldots$. If we also have a curve such that if (x, y) is upon it, then $(y, f(x, y))$ is too, then this curve is called the *invariant* of the recurrence. The curve $(x + 1)(y + 1)(x + y + 1) = kxy$ is thus an invariant for the recurrence $x, y, \frac{y+1}{x}, \ldots$. Of course, given a cycle, it is easy to find an invariant; simply multiply the terms of the cycle together and equate this product to k. But invariants also exist for non-periodic recurrences. Ladas [39] points out that the (regular) recurrence

$$x, y, \frac{ay+b}{(cy+d)x}, \cdots \tag{8.4}$$

for positive x, y, a, b, c, d has the invariant

$$\frac{(dxy+ax+ay+b)(cxy+dx+dy+a)}{xy} = k, \tag{8.5}$$

while Bastien and Rogalski [6] offer the recurrence

$$x, y, \frac{ay^2+by+c}{(y+a)x}, \ldots, \tag{8.6}$$

for positive x, y, a, b, c, which has the invariant

$$xy(x+y) + a(x^2+y^2) + b(x+y) + c - kxy = 0. \tag{8.7}$$

This fact leads Bastien and Rogalski to suggest that the recurrence (8.6) could prove to be as natural an object of study as the Lyness recurrence (1.2). Computer searches suggest neither (8.4) nor (8.6) are ever periodic, except for choices for a, b, c and d that give the recurrences with periods 2, 3, 4, 5 and 6 we have met already.

The recurrence (1.4) possesses the invariant

$$\frac{x^2+y^2+z^2+\alpha}{xyz} = k, \tag{8.8}$$

where k is given by the initial conditions. The morphism $T : \begin{pmatrix} x \\ y \\ z \end{pmatrix} \mapsto \begin{pmatrix} y \\ z \\ \frac{y^2+z^2+\alpha}{x} \end{pmatrix}$ maps one point on the surface (8.8) to another also on the surface.

8.4 Background elliptic curve theory

Returning to (8.3), it transpires that this defines not only a cubic curve, but an elliptic curve (more precisely, the affine part of an elliptic curve). It is helpful therefore to review here some general theory concerning elliptic curves, that will provide some background for our investigation.

It is well-known that the curve

$$ax + by + c = 0$$

is a straight line, and that

$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$

gives a conic. The cubic curve

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$

will generally be an elliptic curve, unless it is singular (possessing a cusp or a loop) or if it factorises into straight lines, or into a conic and a straight line. In this case, there will be points that do not have a unique tangent line, and the curve is called *degenerate*. There are higher degree curves that are elliptic too, but they will be singular (the singular points may be at infinity). The term 'elliptic' arises since these curves were originally studied as part of the theory of elliptic functions [15], integrals designed to ascertain, for example, the circumference of a ellipse. Elliptic curves have genus 1 (as complex projective curves they are topologically equivalent to a torus) while a conic has genus 0.

Any elliptic curve over $\mathbb{R}$ can be transformed into Weierstrass short normal form, that is, an equation of the shape

$$y^2 = x^3 + ax + b,$$

using a birational map (an invertible transformation without surds that maps from the original curve to the normal form curve and back). We say the curves in this case are *isomorphic*. For $y^2 = x^3 + ax + b$ to be non-singular, we require the discriminant to be non-zero, that is,

$$\Delta = 4a^3 + 27b^2 \neq 0.$$

If two elliptic curves are isomorphic, then their j-invariants are the same, where for $y^2 = x^3 + ax + b, j(E) = \frac{4a^3}{\Delta}$; the converse is true over $\mathbb{C}$, but not quite over $\mathbb{Q}$, where there are extra conditions (see Silverman in [34]). Two typical elliptic curves in Weierstrass short normal form are shown in Figure 8.2.

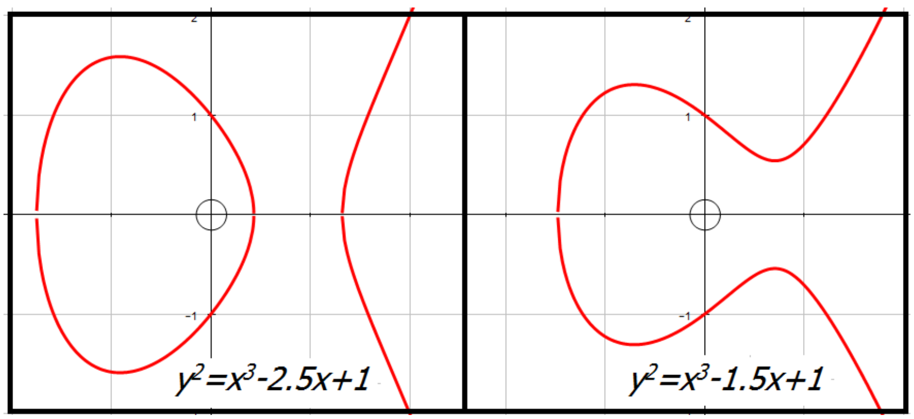


Figure 8.2: Elliptic curves in Weierstrass normal form

Suppose we draw the straight line $y = mx+c$ and the curve $y^2 = x^3+ax+b$ on the same axes. Where do they meet? Solving simultaneously we have

$$x^3 - m^2x^2 + x(a - 2cm) + b - c^2 = 0.$$

This is a cubic equation with real coefficients, so if it has two real solutions it must have a third real solution. Thus if we pick two points on the curve, the line joining them must cut the curve in a third point. Figure 8.3 shows that if the three collinear points on the curve are P, Q and R, we will write the formal relation $P + Q + R = 0$, or $P + Q = -R$, so $P + Q$ is the third point lying on PQ and the curve after reflection in $y = 0$. Notice that if P and Q share an x-coordinate, so that the line PQ is $x = c$, then R is the point 'at infinity', here called $\mathbb{O}$, which we formally append to the curve. (We should strictly write above $P + Q + R = \mathbb{O}$.) We now have defined a binary operation $+$ on the curve together with the point $\mathbb{O}$.

We can form multiples of a point by repeated addition, replacing the two intersections with a tangency. The tangent at P must cut the curve a third

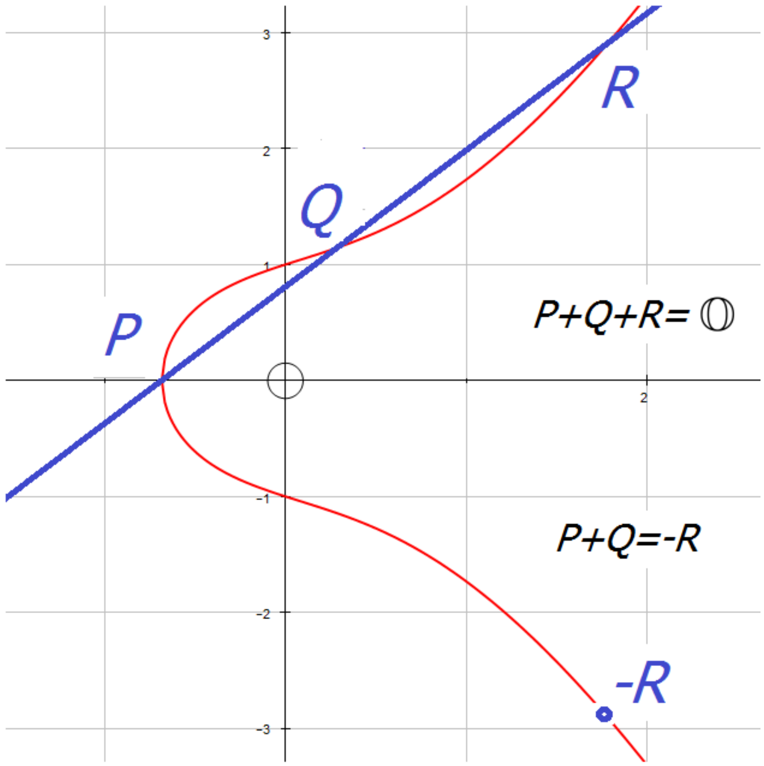


Figure 8.3: Adding points on an elliptic curve

time at $-2P$ (which might be the point at infinity). Negation is reflection in the x-axis. Sometimes we find that $kP = \mathbb{O}$, in which case we say that P is a torsion point of order k. Figure 8.4 shows a torsion point P of order 6; we can write that $6P = \mathbb{O}$.

We now learn an extraordinary fact – this binary operation of addition together with the set of points on the curve together with $\mathbb{O}$ form a group. Clearly we have closure, from the argument above. We define the identity to be $\mathbb{O}$, and the inverse of P is $-P$. Associativity is the difficult thing to prove, but it holds (see the discussion in [26]). Clearly the torsion points form a finite subgroup of the whole.

Suppose now that a and b are rational and we define $E(\mathbb{Q})$ to be the set of rational points on the curve, that is, points whose coordinates are rational.

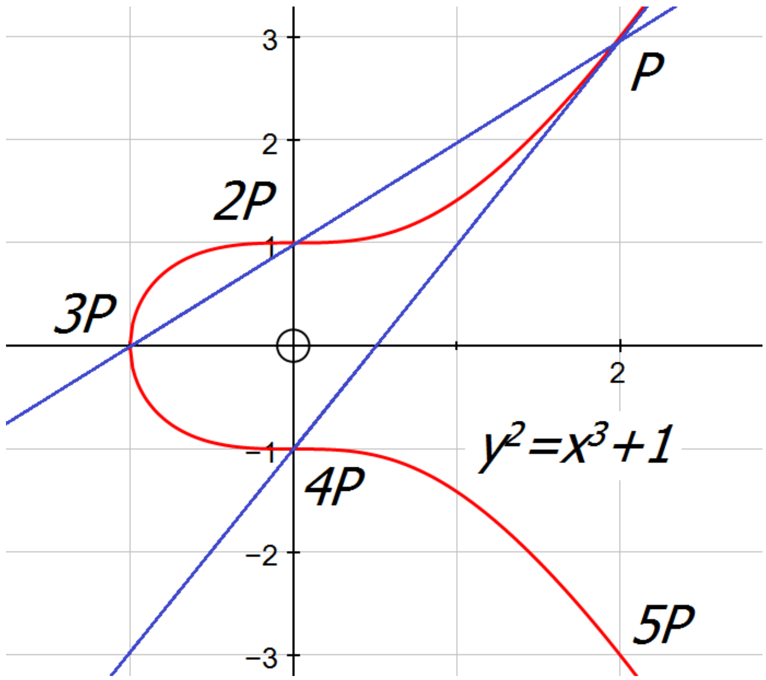


Figure 8.4: A 6-torsion point P on $y^2 = x^3 + 1$

If a, b, m and c are rational and

$$x^3 - m^2x^2 + x(a - 2cm) + b - c^2 = 0$$

has two rational solutions, then it must have a third rational solution, and so $E(\mathbb{Q})$ is a group with the addition law above. Given a rational point to start with (that is not a torsion point), we can continue constructing rational points ad infinitum via taking tangents and adding points – what then is the structure of this infinite group? We have

Theorem 8.1 (Mordell (1922)[47]). *If E is an elliptic curve defined over $\mathbb{Q}$, then $E(\mathbb{Q})$ is a finitely generated abelian group.*

The later Mordell-Weil theorem (1928) [55] generalises this to higher genus abelian varieties. Mordell's Theorem implies that $E(\mathbb{Q})$ is isomorphic to $E_{torsion}(\mathbb{Q}) \bigoplus \mathbb{Z}^r$ for some natural number r. The number r is called the rank of the curve, and for elliptic curves over $\mathbb{Q}$, nobody has yet been able to ascertain exactly what values this can take. It is conjectured that a rank can be arbitrarily large. An elliptic curve has been found by Elkies in 2006 with uncertain rank of at least 28. The largest rank that is known exactly so far found is 19 by Elkies (2009)[23].

We also have this key result:

Theorem 8.2 (Siegel (1929))**.** *If a, b and c are rational (and if $x^3 + ax^2 + bx + c = 0$ has no repeated solutions), then there are finitely many integer points on $y^2 = x^3 + ax^2 + bx + c$.*

How do we find the torsion points? The following theorem offers a method.

Theorem 8.3 (Nagell-Lutz (1935-37))**.** *If $E(\mathbb{Q})$ is the elliptic curve $y^2 = x^3 + ax + b$, where a and b are in $\mathbb{Z}$, then for all non-zero torsion points $P = (u, v)$,*

1. *u, v are in $\mathbb{Z}$,*
2. *If P is of order greater than 2, v^2 divides $4a^3 + 27b^2 = \Delta$,*
3. *If P is of order 2, then $v = 0$ and $u^3 + au + b = 0$.*

We can now compute the torsion points since v comes from a finite list of candidates; an algorithm based on this is built into PARI. Is there anything we can say about the structure of the torsion subgroup? We now have

Theorem 8.4 (Mazur (1977))**.** *The torsion subgroup of $E(\mathbb{Q})$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ for some n in $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$ or to $\mathbb{Z}/2n\mathbb{Z} \bigoplus \mathbb{Z}/2\mathbb{Z}$ for some n in $\{1, 2, 3, 4\}$.*

All of these fifteen group structures for the torsion subgroup are possible, as shown in Table 8.1 [49]. Finally, I will add to our collection of results

Theorem 8.5 (Faltings (1983))**.** *A hyperelliptic curve has finitely many rational points.*

A hyperelliptic curve is one that can be written over $\mathbb{R}$ or over $\mathbb{C}$ as $y^2 = f(x)$, where f is a polynomial with degree n greater than 4, and with n distinct roots. Such a curve will have a genus greater than 1.

Curve	Torsion Subgroup	Generators
$y^2 = x^3 - 2$	trivial	∞
$y^2 = x^3 + 8$	$\mathbb{Z}/2\mathbb{Z}$	$\{(-2, 0)\}$
$y^2 = x^3 + 4$	$\mathbb{Z}/3\mathbb{Z}$	$\{(0, 2)\}$
$y^2 = x^3 + 4x$	$\mathbb{Z}/4\mathbb{Z}$	$\{(2, 4)\}$
$y^2 - y = x^3 - x^2$	$\mathbb{Z}/5\mathbb{Z}$	$\{(0, 1)\}$
$y^2 = x^3 + 1$	$\mathbb{Z}/6\mathbb{Z}$	$\{(2, 3)\}$
$y^2 = x^3 - 43x + 166$	$\mathbb{Z}/7\mathbb{Z}$	$\{(3, 8)\}$
$y^2 + 7xy = x^3 + 16x$	$\mathbb{Z}/8\mathbb{Z}$	$\{(-2, 10)\}$
$y^2 + xy + y = x^3 - x^2 - 14x + 29$	$\mathbb{Z}/9\mathbb{Z}$	$\{(3, 1)\}$
$y^2 + xy = x^3 - 45x + 81$	$\mathbb{Z}/10\mathbb{Z}$	$\{(0, 9)\}$
$y^2 + 43xy - 210y = x^3 - 210x^2$	$\mathbb{Z}/12\mathbb{Z}$	$\{(0, 210)\}$
$y^2 = x^3 - 4x$	$\mathbb{Z}/2\mathbb{Z} \bigoplus \mathbb{Z}/2\mathbb{Z}$	$\{(2, 0)\}$ $(0, 0)\}$
$y^2 = x^3 + 2x^2 - 3x$	$\mathbb{Z}/4\mathbb{Z} \bigoplus \mathbb{Z}/2\mathbb{Z}$	$\{(3, 6),$ $(0, 0)\}$
$y^2 + 5xy - 6y = x^3 - 3x^2$	$\mathbb{Z}/6\mathbb{Z} \bigoplus \mathbb{Z}/2\mathbb{Z}$	$\{(-3, 18),$ $(2, -2)\}$
$y^2 + 17xy - 120y = x^3 - 60x^2$	$\mathbb{Z}/8\mathbb{Z} \bigoplus \mathbb{Z}/2\mathbb{Z}$	$\{(30, -90),$ $(-40, 400)\}$

Table 8.1: Possible torsion subgroup structures

8.5 The order-2 period-5 case revisited

Following Lyness's lead, we have the elliptic curve (8.3). Points upon it add to form a group in the manner described above, with the minor alteration that P and Q add to the third point on the curve that lies on PQ followed by reflection in $y = x$. Now $X = (0, -1)$ is on the curve, and as John Silvester points out in an important note [54], it is a 5-torsion point.

Write $A = (a, b)$, put $k = \frac{(a+1)(a+b+1)(b+1)}{ab}$ and consider $A + X$. Simple coordinate geometry tells us that the line AX is $y = \frac{b+1}{a}x - 1$, which solved simultaneously with the curve yields $x(a+b+1)(b+1)(x-a)(bx-a-1) = 0$. So we have the points A, X, and after reflection in $y = x$, $\left(\frac{a+b+1}{ab}, \frac{a+1}{b}\right)$ as $A + X$. We can see two terms of the recurrence here. Thus the mapping

$f : A \mapsto A + X$ when iterated gives the period-5 sequence

$$(a, b), \left(\frac{a+b+1}{ab}, \frac{a+1}{b}\right),$$

$$\left(b, \frac{b+1}{a}\right), \left(\frac{a+1}{b}, a\right), \left(\frac{b+1}{a}, \frac{a+b+1}{ab}\right), (a, b)\ldots,$$

and we have a geometrical interpretation for our Lyness cycle. There is also the curious fact that taking the sum of the five expressions would have given the same set of curves, since

$$x + y + \frac{y+1}{x} + \frac{x+y+1}{xy} + \frac{x+1}{y} = \frac{(x+1)(y+1)(x+y+1)}{xy} - 3.$$

So starting from a period-5 Lyness cycle, we have constructed an elliptic curve that has 5-torsion. If we then pick any point A on the curve, and repeatedly add a torsion point five times, we get back to A. Clearly $A + 5X$ will be A if X is a 5-torsion point, but what is not obvious is that if we choose (0, -1) as our torsion point, the points $A, A + X, A + 2X, A + 3X$, and $A + 4X$ give us the terms of our cycle. The torsion of the curve and the periodicity of the sequence appear to be intimately related.

8.6 Generalising the method to other periods

We have seen how Lyness's period-5 cycle creates an elliptic curve where the periodicity of the cycle is reflected in the torsion of the curve. How does this idea extend to cycles of other periods? If we have a period-n Lyness cycle $u_1, u_2 \ldots u_n, u_1 \ldots$, we can take any function $f(u_1, u_2, ...u_n)$ and then either

$$f(u_1, u_2, ..., u_n) + f(u_2, u_3, \ldots, u_1) + \cdots + f(u_n, u_1, \ldots, u_{n-1}) = k \quad (8.9)$$

or

$$f(u_1, u_2, \ldots, u_n) \times f(u_2, u_3, \ldots, u_1) \times \cdots \times f(u_n, u_1, \ldots, u_{n-1}) = k \quad (8.10)$$

will produce a curve where a period-n cycle of points on the curve is created.

The morphism $T : \begin{pmatrix} u_1 \\ u_2 \\ \cdots \\ u_{n-1} \\ u_n \end{pmatrix} \mapsto \begin{pmatrix} u_2 \\ u_3 \\ \cdots \\ u_n \\ u_1 \end{pmatrix}$ simply cycles the terms along, so the curves (8.9) and (8.10) are invariant under this. If we choose our function f carefully, we hope to derive an elliptic curve, where addition of points is possible. This idea is now applied to period-3, period-4 and period-6 cycles, the only periods other than 5 (as far as we know) where binary cycles exist over $\mathbb{Q}$.

8.7 The $-\frac{xy+1}{x+y}$ cycle and 3-torsion

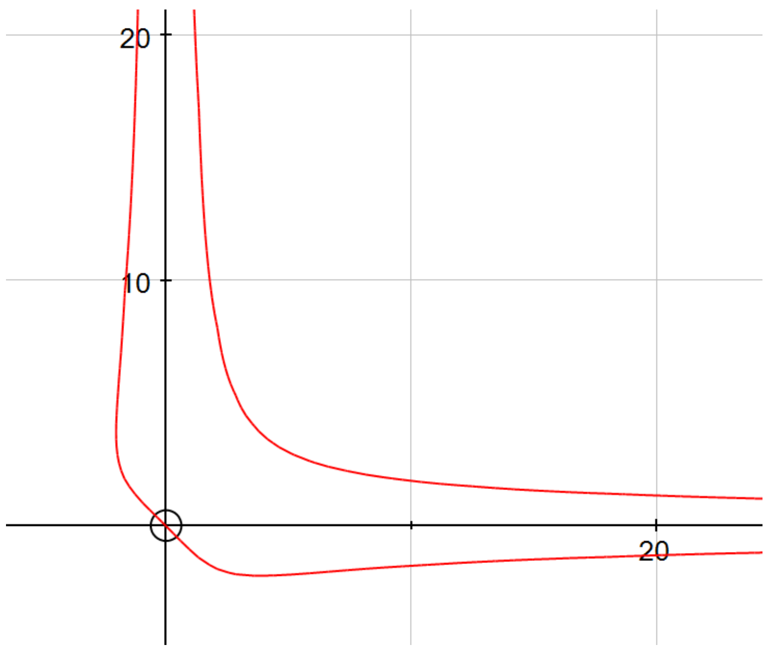


Figure 8.5: $xy(xy+1) = 30(x+y)$

Given our interest in HTs, the period-3 cycle

$$x, y, -\frac{xy+1}{x+y}, x, y \ldots . \tag{8.11}$$

needs special consideration. Multiplying the three terms and insisting that (a,b) is on the curve gives

$$-xy\frac{xy+1}{x+y} = -ab\frac{ab+1}{a+b}, \quad \text{or} \quad xy(xy+1)(a+b) = ab(ab+1)(x+y).$$

Is this an elliptic curve? If we compute the genus with Magma (for specific values for a and b), we find this to be 1, so it is. In order to add points, however, we cannot work with this equation in the classical way – being a biquadratic curve, some lines will cross this curve four times, as Figure 8.5 shows. We need to transform our curve into something akin to Weierstrass short normal form, which fortunately turns out to be straightforward. We begin with

$$xy\frac{xy+1}{x+y}=k, \tag{8.12}$$

which gives us

$$y^2(x^2)+y(x-k)=kx.$$

Completing the square by first multiplying by $4x^2$ we have

$$4y^2(x^4)+4yx^2(x-k)+(k-x)^2=4kx^3+(k-x)^2,$$

which yields

$$(2x^2y+x-k)^2=4kx^3+x^2-2kx+k^2.$$

On multiplying by $16k^2$, we get

$$(8kx^2y+4kx-4k^2)^2=64k^3x^3+16k^2x^2-32k^3x+16k^4.$$

Now substituting using the birational transformation

$$x=\frac{X}{4k}, y=\frac{2kY-2kX+8k^3}{X^2},$$

$$Y=8kx^2y+4kx-4k^2, X=4kx, \tag{8.13}$$

we have

$$Y^2=X^3+X^2-8k^2X+16k^4. \tag{8.14}$$

Let us first choose $(5,3)$ to be on the original curve (8.12), since $(5,3,2)$ is an HT, giving $k=30$. Substituting $k=30$ into (8.14) gives the curve in Figure 8.6. The equation (8.14) is close to Weierstrass short normal form, and is remarkably clean. We can now perform addition of points successfully on this curve. Note that if $X=0$ in (8.14) then $Y=\pm 4k^2$. Indeed, it turns out that $T=(0,4k^2)$ is a 3-torsion point, since if $Y^2=X^3+X^2-8k^2X+16k^4$, then differentiating implicitly, $Y'=\frac{3X^2+2X-8k^2}{2Y}$, so at $(0,4k^2), Y'=-1$, and the equations of the tangent is $Y+X=4k^2$. Solving simultaneously with

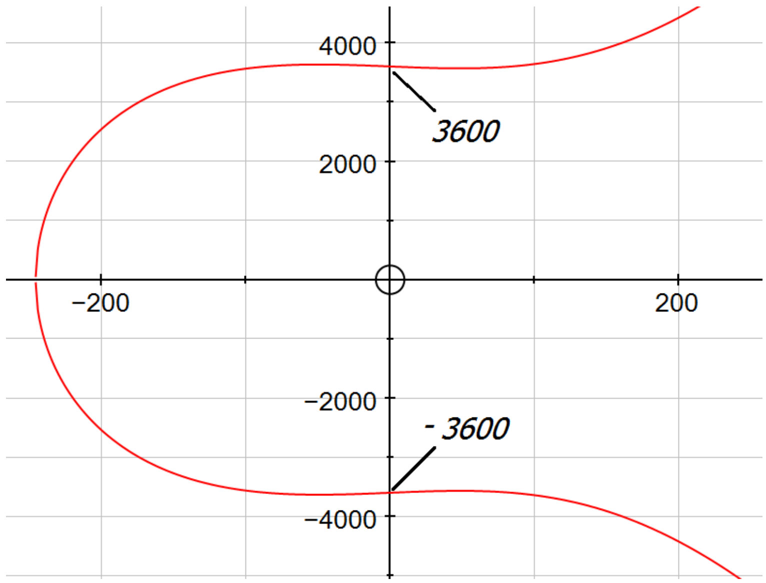


Figure 8.6: $Y^2 = X^3 + X^2 - 8k^2X + 16k^4, k = 30$

the curve, we get $(4k^2 - X)^2 = X^3 + X^2 - 8k^2X + 16k^4$, which simplifies to $X^3 = 0$. We can see that $(0, 4k^2)$ is a point of inflection.

With the elliptic curve generated by (8.3), we found that repeatedly adding the torsion point $(0, -1)$ created period-5 cycles. What happens if we repeatedly add $(0, 4k^2)$ to points on this curve?

Theorem 8.6. *If any point (p, q) on (8.12) maps to A on (8.14) using the transformation (8.13), then if T is $(0, 4k^2)$, and ATB is a straight line where B is also on (8.14), then B maps back to $\left(-\frac{pq+1}{p+q}, q\right)$ on (8.12), which after reflection in $y = x$ becomes $\left(q, -\frac{pq+1}{p+q}\right)$.*

Proof. Take the point (p, q) on (8.12). This means $k = \frac{pq(pq+1)}{p+q}$. Using (8.13), we have that (p, q) maps to $(4kp, 8kp^2q + 4kp - 4k^2)$. The line joining this point to $(0, 4k^2)$ has equation $Y = \frac{8kp^2q+4kp-8k^2}{4kp}X + 4k^2$. Substituting this into (8.14) gives an equation in X that has three roots. Two of these we know, 0 and $4kp$ – the third is found to be $\frac{-4k^2}{pq}$. So this third point on the curve is $\left(\frac{-4k^2}{pq}, \left(\frac{8kp^2q+4kp-8k^2}{4kp}\right)\left(\frac{-4k^2}{pq}\right) + 4k^2\right)$, which after simplifying, transforming back to the original curve and then reflecting, becomes $\left(q, \frac{-(pq+1)}{p+q}\right)$. (Notice that reflecting before transforming back gives $\left(\frac{-(pq+1)}{p+q}, p\right)$.) Iterating this process gives $\left(\frac{-(pq+1)}{p+q}, p\right)$ and (p, q) as the next two points.Thus we have an elliptic curve interpretation of the HT period-3 cycle. $\square$

So we take a recurrence to build a curve that we know will have a 3-cycle of points upon it; when we map this to Weierstrass normal form, we can understand this phenomenon as repeatedly adding a torsion point whose order is of the right period.

Magma supplies further information on the structure of the curves defined by (8.14) for various k, where k is the product of the three elements of a small HT, which is given in Table 8.2. Even relatively small values of k, however, give Magma too much to do. Notice that rank 2 and rank 3 curves are found here – what further ranks are possible as k increases?

k	Associated HT	Structure	Possible generator for torsion subgroup	Possible generators for the rest of $E(\mathbb{Q})$
30	(5,3,2)	$\mathbb{Z}/3\mathbb{Z} \bigoplus \mathbb{Z}^2$	(0,3600)	(600,15000), (-120,-3480)
105	(7,5,3)	$\mathbb{Z}/3\mathbb{Z} \bigoplus \mathbb{Z}^3$	(0,44100)	(2100,-105000), (44100,-9261000), (8820,829080)
132	(11,4,3)	$\mathbb{Z}/3\mathbb{Z} \bigoplus \mathbb{Z}^2$	(0,69696)	(2112,118272), (69696,-18399744)
252	(9,7,4)	$\mathbb{Z}/3\mathbb{Z} \bigoplus \mathbb{Z}^2$	(0,254016)	(-1008,-253008), (9072,898128)

Table 8.2: The structure of $E(\mathbb{Q})$ where E is given by (8.14)

8.8 Integer point implications

What will the integer points on (8.12) be if k is 30? Clearly they will include (5, 3), (3, -2) and (-2, 5) as given by the Lyness cycle that generates the curve, and their reflections in $y = x$, (3, 5), (-2, 3) and (5, -2). We also have (30, 1), (1, -1), (-1, 30) , (30, -1), (-1, 1) and (1, 30) from the trivial HT, a total of 12 integer points. But if the UC is true, this will be all, and we will therefore have a family of elliptic curves (as we vary k to give HT products) that each have 12 integer points (that are easily found), and only 12. The unlikelihood of this situation casts doubt on the veracity of the UC; but if unicity turns out to be the case, then the implications are exciting.

8.9 The order-2 period-6 case

Can we replicate our work with the HT period-3 cycle with period 6? Take the period-6 cycle

$$x, y, -\frac{2x+y+2}{3x+2}, -\frac{2x+1}{3x+2}, -\frac{2y+1}{3y+2}, -\frac{x+2(y+1)}{3y+2}, x, y, \ldots.$$

Adding the terms and insisting that (1, 2) is on the curve gives

$$x + y - \frac{2x+y+2}{3x+2} - \frac{2x+1}{3x+2} - \frac{2y+1}{3y+2} - \frac{x+2(y+1)}{3y+2} = -\frac{3}{10},$$

which leads to the elliptic curve

$$x^2y + y^2x - \frac{31}{30}xy + \frac{x^2}{3} + \frac{y^2}{3} - \frac{22}{15}x - \frac{22}{15}y - \frac{6}{5} = 0. \tag{8.15}$$

Completing the square gives

$$Y^2 = X^4 - 17\frac{X^3}{5} + 1067\frac{X^2}{300} + 734\frac{X}{75} + \frac{844}{225},$$

which maps to Weierstrass short normal form using a transformation I have adapted from Shioda [52]. The curve $y^2 = x^4 + ax^3 + bx^2 + cx + d$ maps to

$$v^2 = u^3 + \frac{3ac - b^2 - 12d}{48}u + \frac{27a^2d - 9abc + 2b^3 - 72bd + 27c^2}{1728} \tag{8.16}$$

using the birational transformation

$x = \frac{6(c+8v)-a(b-12u)}{3a^2-8(b+6u)}$,

$y = \frac{27a^3(c+8v)+9a^2(b+12u)(12u-b)-108ab(c+8v)+4(8b^3-864bu^2+27(c^2+16cv-64(2u^3-v^2)))}{3(3a^2-8(b+6u))^2}$,

$u = \frac{6x^2+3ax-6y+b}{12}$,

$v = -\frac{4x^3+3ax^2+2x(b-2y)-ay+c}{8}$.

The cyclical and symmetrical nature of (8.15) ensures that (1, 2), (2, -$\frac{6}{5}$), $(-\frac{6}{5}, -\frac{3}{5})$, $(-\frac{3}{5}, -\frac{5}{8})$, $(-\frac{5}{8}, -\frac{7}{8})$ and $(-\frac{7}{8}, 1)$ are all on the curve, together with their reflections in $y = x$. Mapping to Weierstrass short normal form gives

$$v^2 = u^3 - \frac{14173849}{4320000}u + \frac{53343170243}{23328000000}, \tag{8.17}$$

which PARI tells us has a 6-torsion point, $(\frac{467}{3600}, \frac{273}{200})$. The point (1, 2) on our original curve maps to $(-\frac{7093}{3600}, -\frac{21}{20})$ on (8.17), and repeatedly adding this to the 6-torsion point gives the period-6 cycle of points

$$\left(-\frac{7093}{3600}, -\frac{21}{20}\right), \left(\frac{11387}{3600}, -\frac{364}{75}\right), \left(\frac{131}{144}, \frac{117}{500}\right), \left(\frac{3827}{3600}, -\frac{7}{600}\right),$$

$$\left(\frac{14153}{14400}, -\frac{273}{2560}\right), \left(\frac{6707}{3600}, \frac{13}{8}\right), \left(-\frac{7093}{3600}, -\frac{21}{20}\right), \ldots.$$

When we map these points back to the original curve, we get

$$(1, 2), \left(2, -\frac{6}{5}\right), \left(-\frac{6}{5}, -\frac{3}{5}\right), \left(-\frac{3}{5}, -\frac{5}{8}\right), \left(-\frac{5}{8}, -\frac{7}{8}\right), \left(-\frac{7}{8}, 1\right), (1, 2), \ldots.$$

8.10 The order-2 period-4 case

Now take the (irregular) period-4 cycle

$$x, y, \frac{4y^2 + 4x + 4y - 2xy + 8}{3xy + 2x + 2y - 4}, \frac{4x^2 + 4x + 4y - 2xy + 8}{3xy + 2x + 2y - 4}, x, y, \ldots$$

Adding the terms and insisting that (1, 2) is on the curve gives

$$x + y + \frac{4y^2 + 4x + 4y - 2xy + 8}{3xy + 2x + 2y - 4} + \frac{4x^2 + 4x + 4y - 2xy + 8}{3xy + 2x + 2y - 4} = \frac{19}{2}$$

which simplifies to the elliptic curve

$$x^2y + y^2x - \frac{19}{2}xy + 2x^2 + 2y^2 - 5x - 5y + 18 = 0.$$

The cyclical and symmetrical nature of the curve ensures that (1, 2), (2, 4),(4, $\frac{5}{2}$) and ($\frac{5}{2}$, 1) are all on the curve, together with their reflections in $y = x$. Mapping to Weierstrass short normal form gives

$$v^2 = u^3 - \frac{172369}{768}u + \frac{31121497}{55296}, \tag{8.18}$$

which PARI tells us has a 4-torsion point, $(\frac{1513}{48}, -\frac{315}{2})$. The point (1, 2) on our original curve maps to $(\frac{73}{48}, -15)$ on (8.18) and repeatedly adding this to our torsion point gives the period-4 set of points

$$\left(\frac{73}{48}, -15\right), \left(-\frac{503}{48}, -42\right), \left(-\frac{647}{48}, \frac{135}{4}\right), \left(\frac{1}{48}, \frac{189}{8}\right), \left(\frac{73}{48}, -15\right), ...,$$

and when we map these points back to the original curve, we get

$$(1, 2), (2, 4), \left(4, \frac{5}{2}\right), \left(\frac{5}{2}, 1\right), (1, 2), ...$$

The humble pseudo-cycle $x, y, \frac{1}{x}, \frac{1}{y}, x, y, \cdots$ (which is regular) creates a 4-torsion curve in a similar way. Adding the terms gives $x + y + \frac{1}{x} + \frac{1}{y} = k$, or

$$x^2y + xy^2 - kxy + x + y = 0.$$

Completing the square and transforming to Weierstrass short normal form gives

$$v^2 = u^3 - u\frac{k^4 - 16k^2 + 16}{48} + \frac{k^6 - 24k^4 + 120k^2 + 64}{864},$$

and checking with PARI shows this has 4-torsion for $k = 1$ to 100 as long as the curve is non-singular.

8.11 The order-3 period-10 case

Do any of these insights apply to ternary recurrences? There is a period-10 cycle that is striking.

$$x, y, z, \frac{yz + 1}{xyz}, \frac{xy + yz + 1}{y(yz + 1)}, \frac{(xy + 1)(yz + 1)}{z(xy + yz + 1)}, \frac{xyz(xy + yz + 1)}{(xy + 1)(yz + 1)},$$

$$\frac{(xy+1)(yz+1)}{x(xy+yz+1)}, \frac{xy+yz+1}{y(xy+1)}, \frac{xy+1}{xyz}, x, y, z \ldots.$$

When we take the product here, we get (after much cancelling)

$$\frac{(xy+yz+1)(yz+1)(xy+1)}{xy^2z} = k, \tag{8.19}$$

or

$$(xy+yz+1)(xy+1)(yz+1) = kxy^2z \tag{8.20}$$

Suppose we now say that (1, 2, 3) is on the surface (Figure 8.7), giving $k = \frac{63}{4}$. The cyclic nature of the construction of the surface means that we immediately have ten rational points upon it, given by

$$(1,2,3), \left(2,3,\frac{7}{6}\right), \left(3,\frac{7}{6},\frac{9}{14}\right), \left(\frac{7}{6},\frac{9}{14},\frac{7}{9}\right), \left(\frac{9}{14},\frac{7}{9},\frac{18}{7}\right),$$
$$\left(\frac{7}{9},\frac{18}{7},\frac{7}{3}\right), \left(\frac{18}{7},\frac{7}{3},\frac{3}{2}\right), \left(\frac{7}{3},\frac{3}{2},\frac{1}{2}\right), \left(\frac{3}{2},\frac{1}{2},1\right), \left(\frac{1}{2},1,2\right).$$

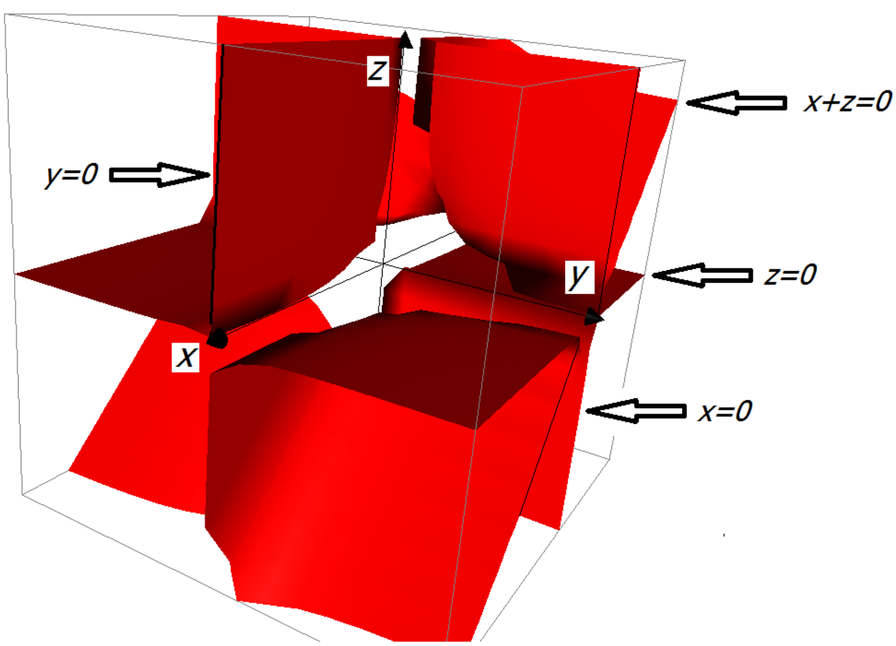


Figure 8.7: $(xy+yz+1)(xy+1)(yz+1) = 12xy^2z$

For large x, y and z the surface is close to the union of the three planes $x = y = z = 0$ together with the plane $x + z = 0$. Notice too that if $y = 1$, (8.20) becomes

$$(x + z + 1)(z + 1)(x + 1) = kxz, \tag{8.21}$$

which is precisely the curve (8.3) that Lyness created from his pentagonal cycle. In fact, if we put $u = xy, v = yz$ in (8.19), this gives (8.3) in terms of u and v.

If we transform $(xy + yz + 1)(xy + 1)(yz + 1) = kxy^2z$ into Weierstrass short normal form, treating y as a constant, using the transformation

$$x = \frac{k^3 - 7k^2 - k(12u + 5) + 12u + 24v - 1}{2y(k^2 + 6k - 12u + 1)},$$

$$z = \frac{k^4 - 6k^3 - 4k^2(6u + 1) + 6k(12u - 7) + 144u^2 + 48u - 144v - 5}{6y(k^3 - 5k^2 + k(7 - 12u) - 12u + 24v + 1)},$$

we obtain

$$v^2 = u^3 - \frac{k^4 - 12k^3 + 14k^2 + 12k + 1}{48}u + \frac{k^6 - 18k^5 + 75k^4 + 75k^2 + 18k + 1}{864}. \tag{8.22}$$

Note that this is free of y, for the reasons mentioned above; the elliptic curves created by choosing a value for y in (8.20) are all isomorphic. Is the period-10 character of the ternary curve visible at all in (8.22)? PARI shows that (8.22) has 5-torsion for k a positive integer less than 100, except in the cases when $k = 12$ or 18, where it has 10-torsion. In these cases (8.22) factorises, and so the vertex of the curve is a rational point with torsion of order 2.

Hirota, Kimura and Yahagi [75] examine a range of order-3 recurrences of the form $x, y, z, \frac{f(y,z)}{x}, \ldots$ and explore the invariant surfaces that can be constructed from them.

8.12 The order-3 period-12 case

The function $\frac{xy-1}{x-z}$ gives us the simple period-12 order-3 regular cycle

$$x, y, z, \frac{xy - 1}{x - z}, z - x, \frac{yz - 1}{x - z}, -x, -y, -z, \frac{xy - 1}{z - x}, x - z, \frac{yz - 1}{z - x}, x, y, z, \cdots .$$

Multiplying these terms together and putting the result equal to k^2 gives

$$x^2y^2z^2\frac{(xy-1)^2(yz-1)^2}{(x-z)^2}=k^2$$

We have here the union of the two surfaces

$$xyz\frac{(xy-1)(yz-1)}{(x-z)}=\pm k.$$

Let us take the plus sign on the RHS. Treating y as a constant, it is straightforward to map this to Weierstrass short normal form using the methods above to give

$$v^2=u^3-u\frac{24k^2+1}{48}+\frac{216k^4+36k^2+1}{864}.$$

Checking this with PARI finds 3-torsion (always) with 6-torsion for $k=1,5,15,34,65...$, as generated by the formula $\frac{n(n^2+1)}{2}$, the values for k where $u^3-u\frac{24k^2+1}{48}+\frac{216k^4+36k^2+1}{864}$ factorises over $\mathbb{Q}$ $((12u+3(n^2+1)^2-1)$ is a factor in this case), so that the vertex of the curve is a rational point.

With order-3 recurrences, it is normal to define two invariants for the recurrence, each defining a surface, and then to consider their intersection, which will be a curve of genus one. For an example of this, see Section 5 in [71].

8.13 Another pseudo-cycle and Todd's recurrence

The examples we have thus far could lead us to

Conjecture 8.7. *If we build an elliptic curve from a period-p cycle in the way described in Section 8.6, then the torsion of the elliptic curve produced will divide p.*

The following two examples show this attractive hypothesis needs to be refined. Take the period-9 pseudo-cycle

$$x,y,z,\frac{x-3}{x+1},\frac{y-3}{y+1},\frac{z-3}{z+1},\frac{x+3}{1-x},\frac{y+3}{1-y},\frac{z+3}{1-z},x,y,z,\ldots.$$

Adding the terms and equating to k gives an equation where the transformation $r = xyz, s = x + y + z$ enables us to eliminate y and z. Now putting $x = t^2$ for some constant t gives us an equation in r, s, k and t without surds, where we can complete the square for r. Choosing $t = 0$, for example, we arrive at

$$Y^2 = s^4 - 2ks^3 + k^2s^2 + 16ks.$$

After using (8.16), we have

$$v^2 = u^3 - uk^2\frac{k^2 + 96}{48} + k^2\frac{k^4 + 144k^2 + 3456}{864}$$

for Weierstrass short normal form. PARI reveals 3-torsion for all k up to 100, but with 6-torsion for $k = 2$.

In Chapter 1 we met the period-8 recurrence (1.9) due to Todd. If we add the terms and equate the result to k, we arrive at the surface

$$x^2(y + 1)(z + 1) + x(y^2(z + 1) + y(z^2 - kz + 3) + z^2 + 3z + 2)$$

$$+(y^2 + y(z + 2) + z + 1)(z + 1) = 0$$

If we insist that (-3,6,2) is on the surface, then $k = 3$. Completing the square for y and transforming as above leads to

$$Y^2 = x^4 + 2x^3\frac{z^2 - 5z + 1}{z + 1} + x^2\frac{z^4 - 8z^3 + 3z^2 - 36z + 1}{(z + 1)^2} + 2xz\frac{z^2 - 5z - 13}{z + 1} + z^2.$$

Let us take $z = 2$. Transforming into Weierstrass short normal form gives

$$v^2 = u^3 + u\frac{5183}{3888} + \frac{10069921}{629856}.$$

PARI reveals 9-torsion; how are we to interpret this?

8.14 Mazur's theorem and cycles

Mazur's Theorem beautifully enumerates the possible orders for the torsion subgroup for all elliptic curves. We have examined above the way that a periodic cycle can generate an elliptic curve where the torsion of the subgroup equals the period of the cycle. There is a discrepancy, however; the only possible periods we have discovered for order-2 cycles with rational coefficients are 2, 3, 4, 5 and 6, while Mazur's Theorem gives many more possibilities for the order of the torsion subgroup in $E(\mathbb{Q})$. The idea remains, however; is there some way of linking Mazur's Theorem to possible cycle periods, of perhaps finding some new theorem where the possible orders of the torsion subgroups and the possible periods of the cycles coincide? Such a theorem is provided by Tsuda [80], where he shows that for QRT maps over $\mathbb{Q}$ that are globally periodic, periods of 2, 3, 4, 5, 6 are the only ones possible.

8.15 The $\frac{xy-1}{x-y}$ cycle

Let us now consider the partner cycle to (8.11) above,

$$x, y, \frac{xy-1}{x-y}, -x, -y, \frac{xy-1}{y-x}, x, y, \ldots. \tag{8.23}$$

Multiplying the terms gives $\left(xy\frac{xy-1}{x-y}\right)^2 = k^2$, or the union of $xy(xy-1) = k(x-y)$ and $xy(xy-1) = -k(x-y)$. Figure 8.8 shows these curves in blue, together with $xy(xy+1) = k(x+y)$ in red for $k > 0$.

It is clear that each blue curve is simply a rotation of the red one; this means that all three will map to the same curve in Weierstrass short normal form, namely $y^2 = x^3 + x^2 - 8k^2x + 16k^4$ (the transformations are identical save for some sign changes). We have seen how repeatedly adding a torsion point recreates the period-3 cycle above – can we do the same for the period-6 cycle (8.23)?

Let us say that $xy(xy-1) = k(x-y)$ is curve A, $xy(xy-1) = -k(x-y)$ is curve B, and $y^2 = x^3 + x^2 - 8k^2x + 16k^4$ is curve K. Several plans suggest themselves, but this one gives us what we want; pick a point (p, q) on A, transform this to a point P on K, find Q where PTQ is a straight line and T is the 3-torsion point $(0, 4k^2)$, transform Q back to A, and then reflect in $y = x$ onto the curve B. Now repeat this from B to A, from A to B and so on. This cycles

$$(p, q), \left(q, \frac{pq-1}{p-q}\right), \left(\frac{pq-1}{p-q}, -p\right), (-p, -q), \left(-q, \frac{pq-1}{q-p}\right), \left(\frac{pq-1}{q-p}, p\right), (p, q), \ldots$$

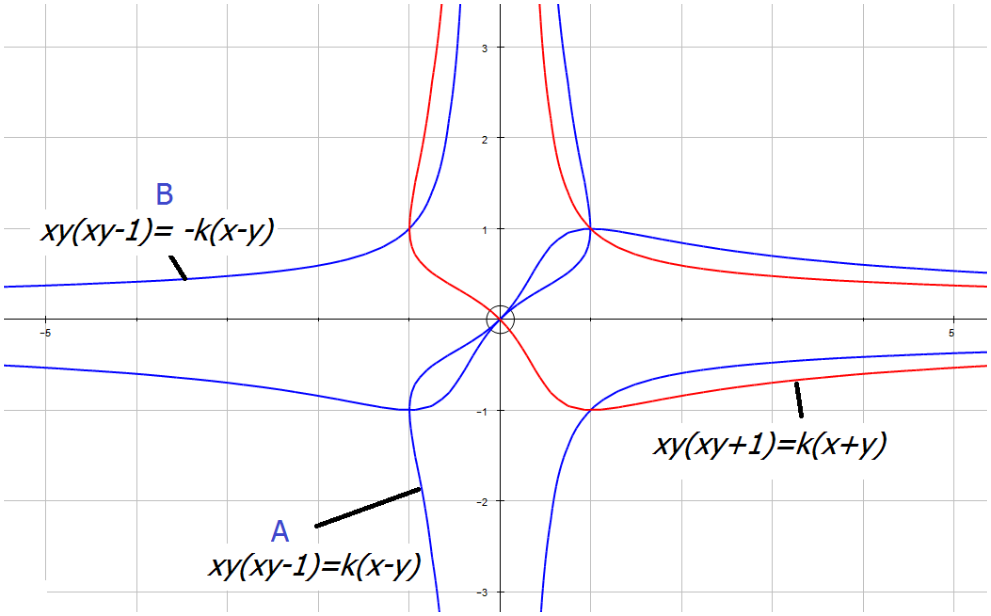


Figure 8.8: $xy(xy-1) = \pm k(x-y)$ and $xy(xy+1) = k(x+y)$

as can be seen in Figure 8.9.

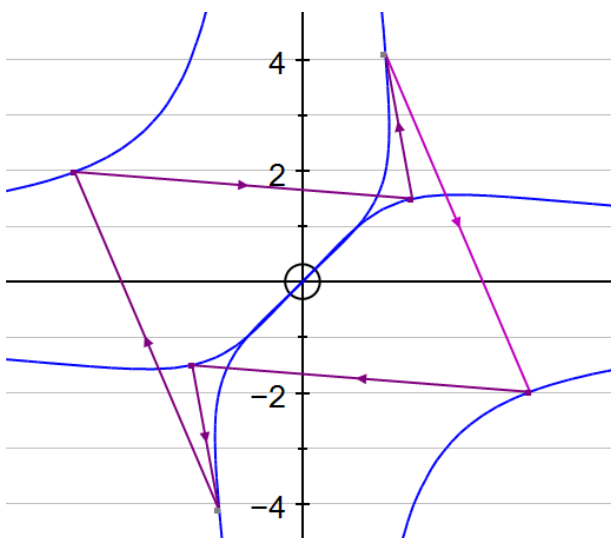


Figure 8.9: The period-6 cycle on $x^2y^2(xy-1)^2 = k^2(x-y)^2$

Note that the Fibonacci recurrence $x, y, x+y, \ldots$ has the invariant curve $(x^2+xy-y^2)^2 = k^2$, and so oscillates between two conics in a similar way.

8.16 The elliptic curve nature of invariant curves

I will conclude this chapter by briefly revisiting the three invariants (8.5), (8.7) and (8.8). The technique of completing the square for y, and then transforming the resulting quartic, means the first two invariants are readily written in Weierstrass short normal form. The curve

$$\frac{(dxy+ax+ay+b)(cxy+dx+dy+a)}{xy} = k, \tag{8.24}$$

where $a=1, b=2, c=3, d=4$, for example, and where (1, 2) is on the curve, giving $k = \frac{247}{2}$, transforms into

$$v^2 = u^3 - \frac{436337307u}{7311616} + \frac{1718871261147}{9885304832},$$

while the invariant curve

$$xy(x+y) + a(x^2+y^2) + b(x+y) + c - kxy = 0, \tag{8.25}$$

with $a=1, b=2, c=3$, for example, and where (1, 2) is on the curve, yielding $k=10$, transforms into

$$v^2 = u^3 - \frac{253u}{3} + \frac{24427}{108}.$$

For the third invariant curve, take the surface defined by

$$\frac{x^2+y^2+z^2+\alpha}{xyz} = k, \tag{8.26}$$

and consider the intersection of this with the plane $x=z$. On completing the square for y, the curve of intersection is seen to be of the form

$$Y^2 = x^4 - \frac{8x^2}{k^2} - \frac{4\alpha}{k^2},$$

which becomes

$$v^2 = u^3 + u\frac{3k^2\alpha - 4}{3k^4} - \frac{4(9k^2\alpha+4)}{27k^6}$$

after transforming. Notice this always factorises, to

$$v^2 = \frac{(3k^2u-4)(9k^4u^2+12k^2u+9k^2\alpha+4)}{27k^6},$$

and thus the curve always has at least 2-torsion.

The examples (8.24) and (8.25) above are demonstrations of symmetric QRT maps [77] [70]. For the example (8.26) arising from (1.4), we might say that surface has a elliptic fibration via projection onto $x = z$. Iterating the recurrence alters these curves, which means we do not have an integrable system (one with multiple invariants) here.

Chapter 9

Finding a Parametrisation for Triples

Recall that in Chapter 3, we defined an HT to be (p, q, r), where $r = \frac{pq+1}{p+q}$, where $p \geqslant q \geqslant r \geqslant 1$ and where p, q and r are all positive integers. It is natural to ask, is there is a parametrisation for HTs akin to the one that exists for Pythagorean triples (PTs)? That is, can we find polynomials f, g and h such that $(f(x_1, \ldots, x_k), g(x_1, \ldots, x_k), h(x_1, \ldots, x_k))$ is an HT for all positive integers x_1 to x_k, and moreover, that every HT is of this form for some set of values for x_i?

We can note at this point that 3.1 implies that if for each n, we write down all pairs (u, v) with $u > v$ and $uv = n^2 - 1$, then $(n + u, n + v, n)$ and $(u - n, n, n - v)$ will always be HTs (where the first two elements of the second bracket may need to be reordered) and moreover, every HT will be of one of these forms. Might this count as a parametrisation?

9.1 Parametrising the Pythagorean Triples

The elegant derivation of the PT parametrisation is worth recalling.

Theorem 9.1. *If m, n are coprime natural numbers of opposite parity with $m > n$, then $(2mn, m^2 - n^2, m^2 + n^2)$ is a primitive PT, and moreover, every primitive PT is of this form.*

Proof. We are given that $x^2+y^2=z^2$, where x, y and z are positive integers, and where x, y and z do not share a common factor (we have a primitive solution). If x and y are both even, then z is too, which contradicts the above. If x and y are both odd, then $z^2 = x^2+y^2 \equiv 2 \pmod 4$, which is impossible. So let us say x is even with $x = 2x'$, and y is odd, which means z is odd. Now

$$x^2 = z^2 - y^2 = (z+y)(z-y) = 4x'^2 \Rightarrow x'^2 = \left(\frac{z+y}{2}\right)\left(\frac{z-y}{2}\right),$$

where $\frac{z+y}{2}$ and $\frac{z-y}{2}$ are both integers (since z and y are both odd) that are clearly coprime. The Fundamental Theorem of Arithmetic now implies that $\frac{z+y}{2}$ and $\frac{z-y}{2}$ are both square, since their product is, and they are coprime. Say $z+y = 2m^2, z-y = 2n^2$, with $m > n, \gcd(m,n) = 1$, and where m and n are of opposite parity, since if m and n are both odd, y and z will both be even. Adding, we have that $z = m^2+n^2$, and subtracting, we have that $y = m^2 - n^2$. It follows that $x = 2mn$. $\square$

More generally, if m, n, r are any natural numbers with $m > n$,

$$(2mnr, r(m^2-n^2), r(m^2+n^2))$$

is always a PT, and every PT is of this form for some natural numbers n, m and r (although some PTs will occur more than once in this formulation).

9.2 A partial parametrisation for HTs

Can we find a similar parametrisation for HTs? Take a bag in Standard Form, that is, $0, 1, a, b$ where a and b are rational, $1 < a < b$ and $b - a > 1$. Suppose this gives rise to the HT

$$\left(\frac{b}{a-1}, b-a, \frac{b-1}{a}\right) = (r+s, r+t, r)$$

where r, s and t are all positive integers with $s > t$. Then

$$r = \frac{b-1}{a} \Rightarrow b = ar+1.$$

Moreover,

$$r+s = \frac{b}{a-1} = \frac{ar+1}{a-1} = r + \frac{r+1}{a-1} \Rightarrow s = \frac{r+1}{a-1} \Rightarrow r = as - s - 1.$$

We have $r + t = ar + 1 - a = a(as - s - 1) + 1 - a = (as - 1)(a - 1) - a$, which implies

$$(r + s, r + \frac{r^2 - 1}{s}, r) = (as - 1, (as - 1)(a - 1) - a, as - 1 - s). \quad (9.1)$$

For a and s positive integers, this will always give an HT (although we cannot be certain over the ordering of the first two elements). In our bag, however, a is rational, so restricting a to the natural numbers means there are some HTs that are omitted by this formula. What percentage of all HTs is given by (9.1) when a and s are integers?

9.3 HT patterns

Figure 9.1 is an Excel spreadsheet (symmetrical about $y = x$) showing the smaller HTs. The cell (x, y) where $x, y \in \mathbb{N}^+$ is coloured red if $\frac{xy+1}{x+y} \in \mathbb{N}^+$. We can see that there are straight lines running across the pattern – these represent sets of HTs where the elements move in arithmetic progression (for example, $(15n + 4, 10n + 1, 6n + 1)$). We can see this will happen, since if we fix a value for a in the HT $(as - 1, (as - 1)(a - 1) - a, as - s - 1)$, three arithmetic sequences are generated as s increases. At the bottom of Figure 9.1, there are parabolas. This is understandable too, since if we fix a value for s in the HT $(as - 1, (as - 1)(a - 1) - a, as - s - 1)$, a quadratic sequence is generated as a increases. Figure 9.2 shows the HTs in green that $(as - 1, (as - 1)(a - 1) - a, as - s - 1)$ covers as a and s vary (assuming $x > y$, the bottom right of the diagram only is considered).

So we have a partial parametrisation for HTs; we can add a second, 'parallel' to the first, namely $(as+1, (as+1)(a-1)+a, as-s+1)$. The additional HTs covered by this formula are coloured dark blue in Figure 9.2. There are still, however, many HTs that these formulae fail to include, as shown by the remaining dots in Figure 9.2. But if we look closely, all of these seem to lie on pairs of straight lines sharing a gradient – the brown pair of lines are a good example. Can we characterise these lines, and use this to arrive at a full parametrisation for HTs?

It is easy to find the arithmetic sequences that give rise to the straight lines in Figure 9.2. Here is a collection of the simplest such families, in order

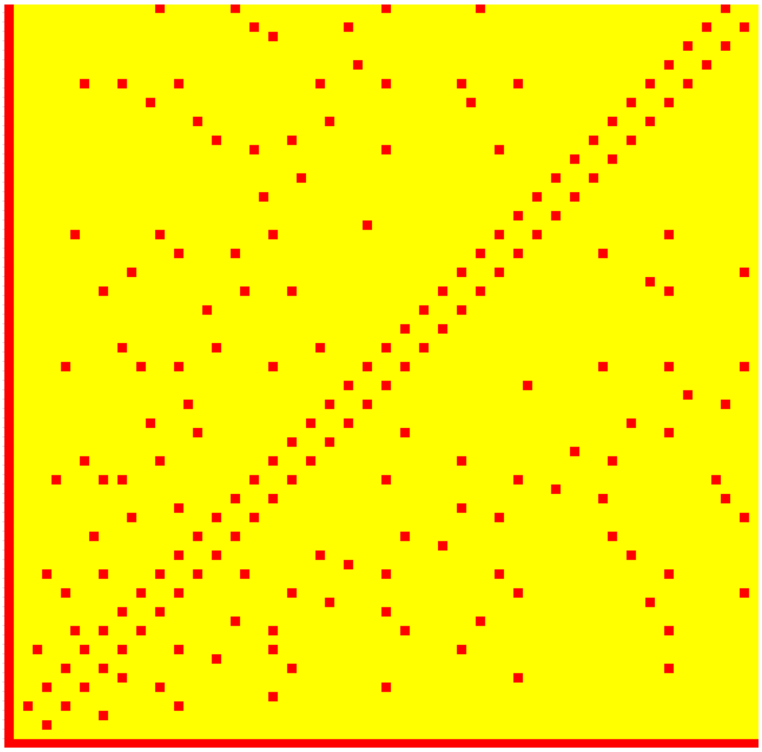


Figure 9.1: Small HTs

of decreasing gradient.

$$\begin{pmatrix}2n\pm3\\2n\pm1\\n\pm1\end{pmatrix},\begin{pmatrix}45n\pm19\\36n\pm17\\20n\pm9\end{pmatrix},\begin{pmatrix}28n\pm13\\21n\pm8\\12n\pm5\end{pmatrix},\begin{pmatrix}15n\pm4\\10n\pm1\\6n\pm1\end{pmatrix}\begin{pmatrix}40n\pm9\\24n\pm7\\15n\pm4\end{pmatrix}\begin{pmatrix}6n\pm5\\3n\pm1\\2n\pm1\end{pmatrix}$$

$$\begin{pmatrix}70n\pm29\\30n\pm11\\21n\pm8\end{pmatrix},\begin{pmatrix}35n\pm6\\14n\pm1\\10n\pm1\end{pmatrix},\begin{pmatrix}12n\pm7\\4n\pm1\\3n\pm1\end{pmatrix},\begin{pmatrix}63n\pm8\\18n\pm1\\14n\pm1\end{pmatrix}\begin{pmatrix}20n\pm9\\5n\pm1\\4n\pm1\end{pmatrix}\begin{pmatrix}30n\pm11\\6n\pm1\\5n\pm1\end{pmatrix}$$

It is noticeable that the coefficients of n are of the form ij, ik, jk in each case, with i, j, k natural numbers where $i > j > k$. So when is $\begin{pmatrix}ijn+p\\ikn+q\\jkn+r\end{pmatrix}$ an HT? This would mean that

$$\frac{(ijn+p)(ikn+q)+1}{ijn+p+ikn+q} = jkn+r,$$

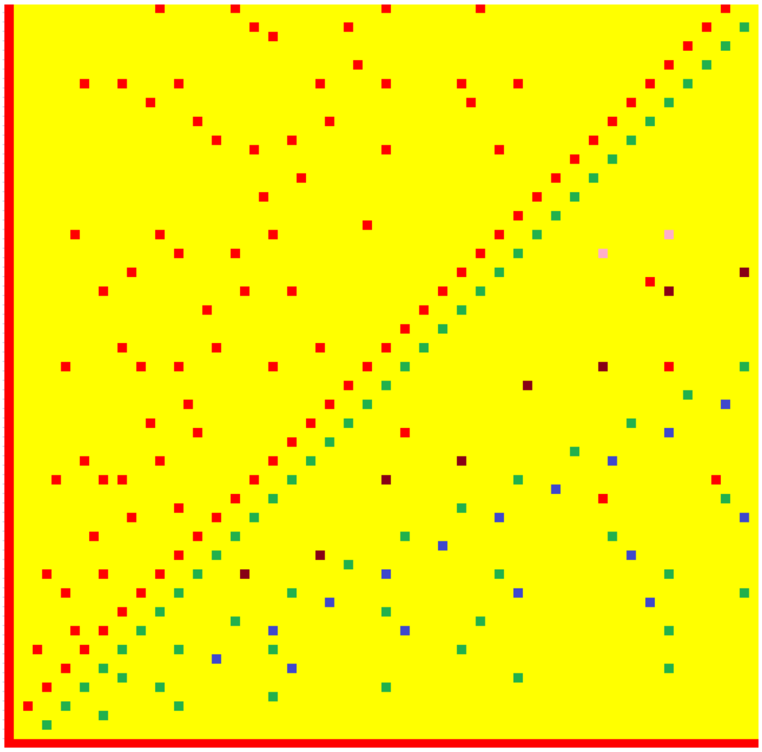


Figure 9.2: Small HTs forming arithmetic sequences

which simplifies to

$$ijn^2(i-j-k)+n(pk(i-j)+qj(i-k)-ri(j+k))+p(q-r)-qr+1=0.$$

For this to be true for all n, the coefficient of each power of n must be zero, giving the three equations

1. $i=j+k$,
2. $pk(i-j)+qj(i-k)-ri(j+k)=0 \Rightarrow r=\frac{pk^2+qj^2}{(j+k)^2}$,
3. $r=\frac{pq+1}{p+q}$.

A check on the families above confirms that $i=j+k$ in each case. Putting $n=0$ shows that (p,q,r) must be an HT for this to work, so the third equation must hold. The equation $\frac{pk^2+qj^2}{(j+k)^2}=\frac{pq+1}{p+q}$ simplifies neatly to

$$(j+k)^2=(pk-qj)^2 \tag{9.2}$$

or

$$\frac{k}{j} = \frac{q+1}{p-1} \quad \text{OR} \quad \frac{q-1}{p+1}. \tag{9.3}$$

Note that $\frac{k}{j}$ is the gradient of the line – for each gradient there are two families, the parallel pairs we can see running across the quadrant. So if we put $k = q+1, j = p-1$ for the first case, and $k = q-1, j = p+1$ for the second, we get that each HT (p, q, r) starts two families of HTs,

$$\begin{pmatrix} (p+q)(p-1)n+p \\ (p+q)(q+1)n+q \\ (p-1)(q+1)n+r \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} (p+q)(p+1)n+p \\ (p+q)(q-1)n+q \\ (p+1)(q-1)n+r \end{pmatrix}.$$

Note that if $\gcd(j, k) \neq 1$, then there will be gaps on the family - effectively we are multiplying n by $(\gcd(j, k))^2$ each time.

We can substitute for (p, q, r) one of the partial parametrisations we already have. Using $(as-1, (as-1)(a-1)-a, as-s-1)$, we arrive at

$$\begin{pmatrix} a^3ns^2 - 2a^2ns + as - 1 \\ a^4ns^2 - a^3ns(s+4) + a^2(2n(s+2)+s) - a(s+2) + 1 \\ a^3ns^2 - a^2ns(s+2) + as - s - 1 \end{pmatrix}.$$

What proportion of HTs will this give us as a, s and n vary over $\mathbb{Z}$? More generally, $\begin{pmatrix} (p+q)(p{\color{blue}\pm}1)n{\color{red}\pm}p \\ (p+q)(q{\color{blue}\mp}1)n{\color{red}\pm}q \\ (p{\color{blue}\pm}1)(q{\color{blue}\mp}1)n{\color{red}\pm}r \end{pmatrix}$ together with

$$(p, q, r) = (as{\color{green}\pm}1, (as{\color{green}\pm}1)(a-1){\color{green}\pm}a, as-s{\color{green}\pm}1)$$

(where the $\pm$ signs for each colour agree) gives a larger parametrisation.

9.4 Constructing a tree of HT families

If we look more closely at Figure 9.2, we see the following pattern; starting with the two families $(n+1, 1, 1)$, running just above the x-axis, and $(2n+3, 2n+1, n+1)$, running diagonally at 45^o, we can begin new families, not from every point, but from every other point, before beginning a new family from every other point on these new families, and so on, as in Figure 9.3. I will call this the set of *primitive families*. Now our horizontal starting

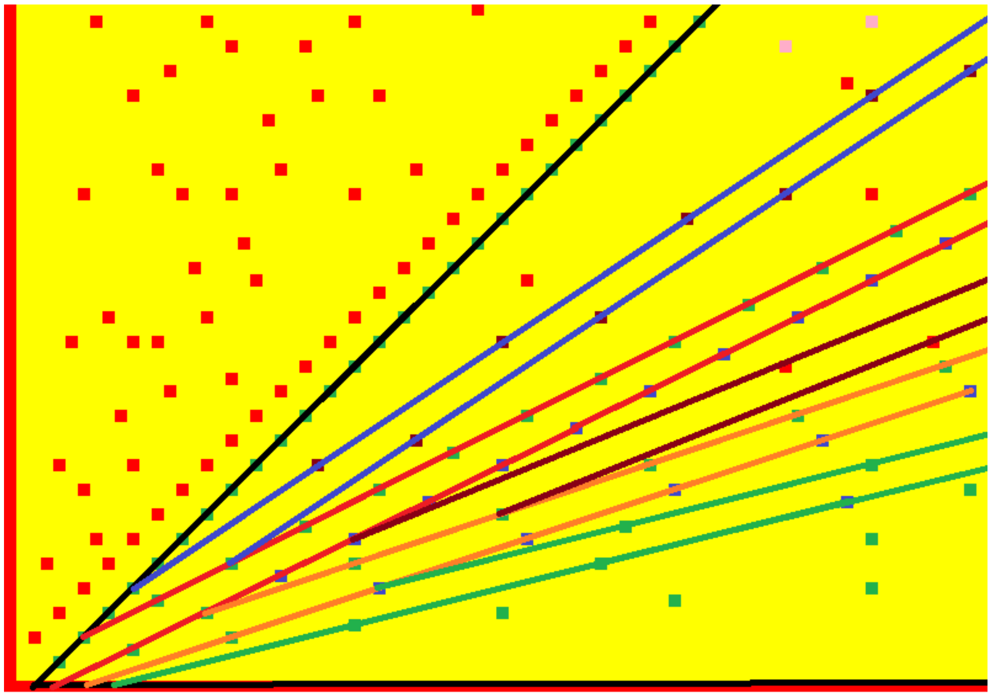


Figure 9.3: Taking every other point

family has $(j,k) = (1,0)$, and our other starting family, with gradient 1, has $(j,k) = (1,1)$. How are the new families created? In Figure 9.3, we can see, for example, the black family and the upper red family 'give birth to' the two dark blue families – in general, if the values for (j,k) for the two parent families are (j_1, k_1) and (j_2, k_2), then the two new 'offspring' families have $(j,k) = (j_1 + j_2, k_1 + k_2)$. This is reminiscent of Farey sequences and the Stern-Brocot tree, and it leaves us wanting to ask three questions:

1. is $\gcd(j,k)$ always equal to 1 using this addition rule?

2. if so, is every (j,k) with $j > k$ and $\gcd(j,k) = 1$ in our tree somewhere?

3. do we get any repeats?

These can be resolved simply by considering the Calvin-Wilf tree [17]. Figure 9.4 shows how the next row in the Calvin-Wilf tree is generated from the previous one, while Figure 9.5 shows the start of this tree. If we equate our parameters (j,k) with $\frac{k}{j}$, the gradient of our line in Figure 9.3, then we require the left-handed children in the tree at every stage.

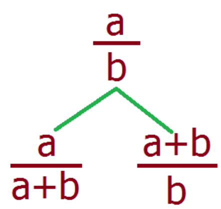


Figure 9.4: Parent and children

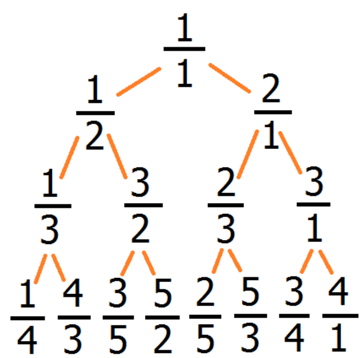


Figure 9.5: The Calvin-Wilf tree

Suppose not all fractions here are in their lowest terms. Then let $\frac{r}{s}$ be a fraction at the highest level so that $\gcd(r, s)$ is not 1. The 'parent' of $\frac{r}{s}$ will be either $\frac{r}{s-r}$ or $\frac{r-s}{s}$, which means there is a higher level so that a fraction is not in its lowest terms, and we have a contradiction.

Does every fraction $\frac{k}{j}$ occur? Let $\frac{r}{s}$ be the fraction of smallest denominator that does not occur, and after that of smallest numerator. If $r > s$, then $\frac{r-s}{s}$ does not occur either, since one of its children would be $\frac{r}{s}$ and that has a smaller numerator. If $r < s$, then $\frac{r}{s-r}$ does not occur, since one of its children would be $\frac{r}{s}$, and that has a smaller denominator. Again, we have a contradiction.

Can we have any repeats? Amongst all rationals that occur more than once, let $\frac{r}{s}$ have first the smallest denominator, and after this, the smallest numerator. If $r < s$, then $\frac{r}{s}$ is the child of two vertices, at both of which $\frac{r}{s-r}$ lives, which is a contradiction, and similarly if $s < r$.

So we build our tree by giving each HT in the tree a 'code' – the code $(j, k, n, p, q, r, u, v, w)$ represents the equation

$$\begin{pmatrix} (j+k)jn+p \\ (j+k)kn+q \\ jkn+r \end{pmatrix} = (u, v, w), \tag{9.4}$$

where (p, q, r) is an HT and where $\gcd(j, k) = 1$ (so (2, 1, 2, 7, 5, 3, 13, 8, 5), for example, represents (13, 8, 5)). There is some redundancy here – (j, k, n, p) is enough to determine the HT for $j > 2$, but the extra elements are included for convenience. Why $j > 2$? We know $q = \frac{k(p+1)}{j} + 1$ or $\frac{k(p-1)}{j} - 1$. These can only both be integers if $j|(p+1)$ and $j|(p-1)$, which implies that j is 1 or 2. Our starting triples from our starting families are

Row 1

(1,0,3,1,1,1,4,1,1)(1,1,1,3,1,1,5,3,2)

How do we derive the next row? If n is odd for a row, we obtain the next one by simply adding 1 to each n. If n is even for a row, we split the coded HTs into pairs (the number of HTs in any row is even) and replace each pair

$$(j_m, k_m, n_m, p_m, q_m, r_m, u_m, v_m, w_m),$$

$$(j_{m+1}, k_{m+1}, n_{m+1}, p_{m+1}, q_{m+1}, r_{m+1}, u_{m+1}, v_{m+1}, w_{m+1}),$$

with the four coded HTs

$$(j_m, k_m, n_m + 1, p_m, q_m, r_m, u_{m+2}, v_{m+2}, w_{m+2}),$$

$$(j_m + j_{m+1}, k_m + k_{m+1}, 1, u_m, v_m, w_m, u_{m+3}, v_{m+3}, w_{m+3}),$$
$$(j_m + j_{m+1}, k_m + k_{m+1}, 1, u_{m+1}, v_{m+1}, w_{m+1}, u_{m+4}, v_{m+4}, w_{m+4}),$$
$$(j_{m+1}, k_{m+1}, n_{m+1} + 1, p_{m+1}, q_{m+1}, r_{m+1}, u_{m+5}, v_{m+5}, w_{m+5}),$$

thus doubling the number of coded HTs in a row.

Row 2

(1,0,4,1,1,1,5,1,1)(1,1,2,3,1,1,7,5,3)

Row 3

(1,0,5,1,1,1,6,1,1)(2,1,1,5,1,1,11,4,3)(2,1,1,7,5,3,13,8,5)(1,1,3,3,1,1,9,7,4)

Row 4

(1,0,6,1,1,1,7,1,1)(2,1,2,5,1,1,17,7,5)(2,1,2,7,5,3,19,11,7)(1,1,4,3,1,1,11,9,5)

Row 5

(1,0,7,1,1,1,8,1,1)(3,1,1,7,1,1,19,5,4)(3,1,1,17,7,5,29,11,8)(2,1,3,5,1,1,23,10,7)...
(2,1,3,7,5,3,25,14,9)(3,2,1,19,11,7,34,21,13)(3,2,1,11,9,5,26,19,11)(1,1,5,3,1,1,13,11,6)

Row 6

(1,0,8,1,1,1,9,1,1)(3,1,2,7,1,1,13,9,7)(3,1,2,17,7,5,41,15,11)(2,1,4,5,1,1,29,13,9)...
(2,1,4,7,5,3,31,17,11)(3,2,2,19,11,7,49,31,19)(3,2,2,11,9,5,41,29,17)(1,1,6,3,1,1,15,13,7)

and so on.

The tree that results from the above is given in Figure 9.6; each green and each blue area represents a primitive family of HTs. The red lines show the starting HT; each blue family is started by a green HT and vice versa. No HT is repeated, since each new family that is added has a gradient in Figure 9.3 that lies between the two families that create it (if $\gamma = \frac{k_m+k_{m+1}}{j_m+j_{m+1}}$, then $\frac{k_m}{j_m} < \gamma < \frac{k_{m+1}}{j_{m+1}}$), and every (j,k) with $\gcd(j,k) = 1$ and $j \geqslant k$ is represented.

Now the following lemma is useful:

Lemma 9.2. *if (a,b,c) is an HT, then a, b and c are always pairwise coprime.*

Proof. For an HT, we have that $\frac{ab+1}{a+b} = c$ is a positive integer

$$\Rightarrow ab + 1 = ac + bc \Rightarrow a(c-b) + b(c) = 1 \Rightarrow \gcd(a,b) = 1.$$

Similarly $\gcd(a,c) = \gcd(b,c) = 1$. $\square$

So there can be only two kinds of HT: an 'odd' HT, where all three elements are odd, and an 'even' HT, where exactly one of the elements is even. Turning to our tree, it is noticeable that

Theorem 9.3. *HTs that start a primitive family are odd, while those that do not start a primitive family are even.*

Proof. Suppose that an even HT (a,b,c) begins a primitive family. Then there will be an even number of steps down to the starting HT (p,q,r) for the other primitive family on which (a,b,c) lies, since only every other HT starts a primitive family. Now since (a,b,c) is an even HT, and n is even in $(a,b,c) = \begin{pmatrix} (j+k)jn+p \\ (j+k)kn+q \\ jkn+r \end{pmatrix}$, (p,q,r) is an even HT, where $p < a, q < b, r < c$. Now we have a descent argument; the HT starting the other primitive family on which (p,q,r) lies is even too, and so on. But by inspection, there are no small even HTs that start primitive families. So we have a contradiction, and only odd HTs can start a primitive family. □

This tells us that there is a natural bijection between the set of even HTs and the set of odd HTs given by mapping each even HT (p,q,r) to the odd HT above it on the only primitive family on which (p,q,r) lies. We also have that in (9.4), (p,q,r) must be an odd HT.

So one question remains; given an HT, can we say which family it lies upon? In other words, what is its coding? Suppose we have an HT (u,v,w) – can this always be written as $\begin{pmatrix} (j+k)jn+p \\ (j+k)kn+q \\ jkn+r \end{pmatrix}$ for some $n,j,k, \in \mathbb{N}, \gcd(j,k) = 1$, with (p,q,r) an HT? We know from (9.3) that if $\begin{pmatrix} (j+k)jn+p \\ (j+k)kn+q \\ jkn+r \end{pmatrix}$ is a primitive family, then $\frac{k}{j} = \frac{q+1}{p-1}$ or $\frac{q-1}{p+1}$. If the former is true, then $p = \frac{j(q+1)}{k} + 1$, and so $\frac{v+1}{u-1} = \frac{k}{j}$, and similarly if $\frac{k}{j} = \frac{q-1}{p+1}, \frac{v-1}{u+1} = \frac{k}{j}$. This suggests an algorithm for finding j,k,n,p,q,r given (u,v,w): find $\frac{v+1}{u-1}$ and $\frac{v-1}{u+1}$ in their lowest terms. Put the numerator of the simpler fraction (where numerator + denominator is smaller) equal to k, and the denominator equal to j. Now find n so that

$u = (j+k)jn + p$ with $0 < p < 2(j+k)j$ and so that n is odd if (u, v, w) is an even HT, and so that n is even if (u, v, w) is an odd HT. There should be exactly one such value for n, and so we have our coding.

For example, say we have the HT (86, 59, 35). Now $\frac{v+1}{u-1} = \frac{60}{85} = \frac{12}{17}$, while $\frac{v-1}{u+1} = \frac{58}{87} = \frac{2}{3}$. So we put $j = 3, k = 2$, and $(86, 59, 35) = \begin{pmatrix} 15n + p \\ 10n + q \\ 6n + r \end{pmatrix}$, with n odd and $0 < p < 30$. The only possibility is $n = 5$, giving $(p, q, r) = (11, 9, 5)$, and so we have that $(86, 59, 35)$ is a member of the primitive family $\begin{pmatrix} 15n + 11 \\ 10n + 9 \\ 6n + 5 \end{pmatrix}$.

9.5 Arriving at the parametrisation

I said earlier that (j, k, n, p) is enough to determine any HT if $j > 2$. Certainly j and k are need to determine the gradient of the family, and n is needed to say how far along the family to go, while p tells us which of the two parallel lines we are choosing. We know from (9.3) that if $\begin{pmatrix} (j+k)jn + p \\ (j+k)kn + q \\ jkn + r \end{pmatrix}$ is a primitive family, then $q = \frac{k(p+1)}{j} + 1$, or $q = \frac{k(p-1)}{j} - 1$.

Taking the first of these possibilities, since $\gcd(j, k) = 1, j|(p+1)$ and so $p = mj - 1$. This means that (p, q, r) is $(mj - 1, mk + 1, km + 1 - \frac{k(km+2)}{j+k})$, and since $\gcd(j+k, k) = 1$, we need $km + 2 = l(j+k)$, or $(l)j - (m-l)k = 2$.

We can reverse this now. Given j and $k, \gcd(j, k) = 1$, define a and b by $aj - bk = 1$, where $0 \leqslant a < k, 0 \leqslant b < j$, and thus $2aj - 2bk = 2$. Comparing $(l)j - (m-l)k$ with this, we can put $2a = l, 2b = m - l$, and so $m = 2(a+b)$. This gives

$$\begin{pmatrix} u \\ v \\ w \end{pmatrix} = \begin{pmatrix} (j+k)jn + 2(a+b)j - 1 \\ (j+k)kn + 2(a+b)k + 1 \\ jkn + 2bk + 1 \end{pmatrix}.$$

The equation of this line is $y = \frac{k}{j}x + \frac{j+k}{j}$, which always goes through (-1, 1).

Taking the second of the possibilities, that $q = \frac{k(p-1)}{j} - 1$, and using the fact that if $aj - bk = 1$, then $(j-b)k - (k-a)j = 1$, we have $\begin{pmatrix} u \\ v \\ w \end{pmatrix} = \begin{pmatrix} (j+k)jn + 2(j+k-a-b)j + 1 \\ (j+k)kn + 2(j+k-a-b)k - 1 \\ jkn + 2(j-b)k - 1 \end{pmatrix}$. The equation of this line is $y = \frac{k}{j}x - \frac{j+k}{j}$, which always goes through (1, -1). Notice that in both cases, (p, q, r) is certain to be an odd HT, and can therefore start a primitive family.

We have thus arrived at what might be termed a parametrisation for HTs. Given j and k, with $j > k, \gcd(j,k) = 1$, we can derive the two primitive families with gradient $\frac{k}{j}$, and there are no omissions or repeats – each HT appears just once. It is possible that this formulation will now help us with other tasks, such as proving or disproving the UC.

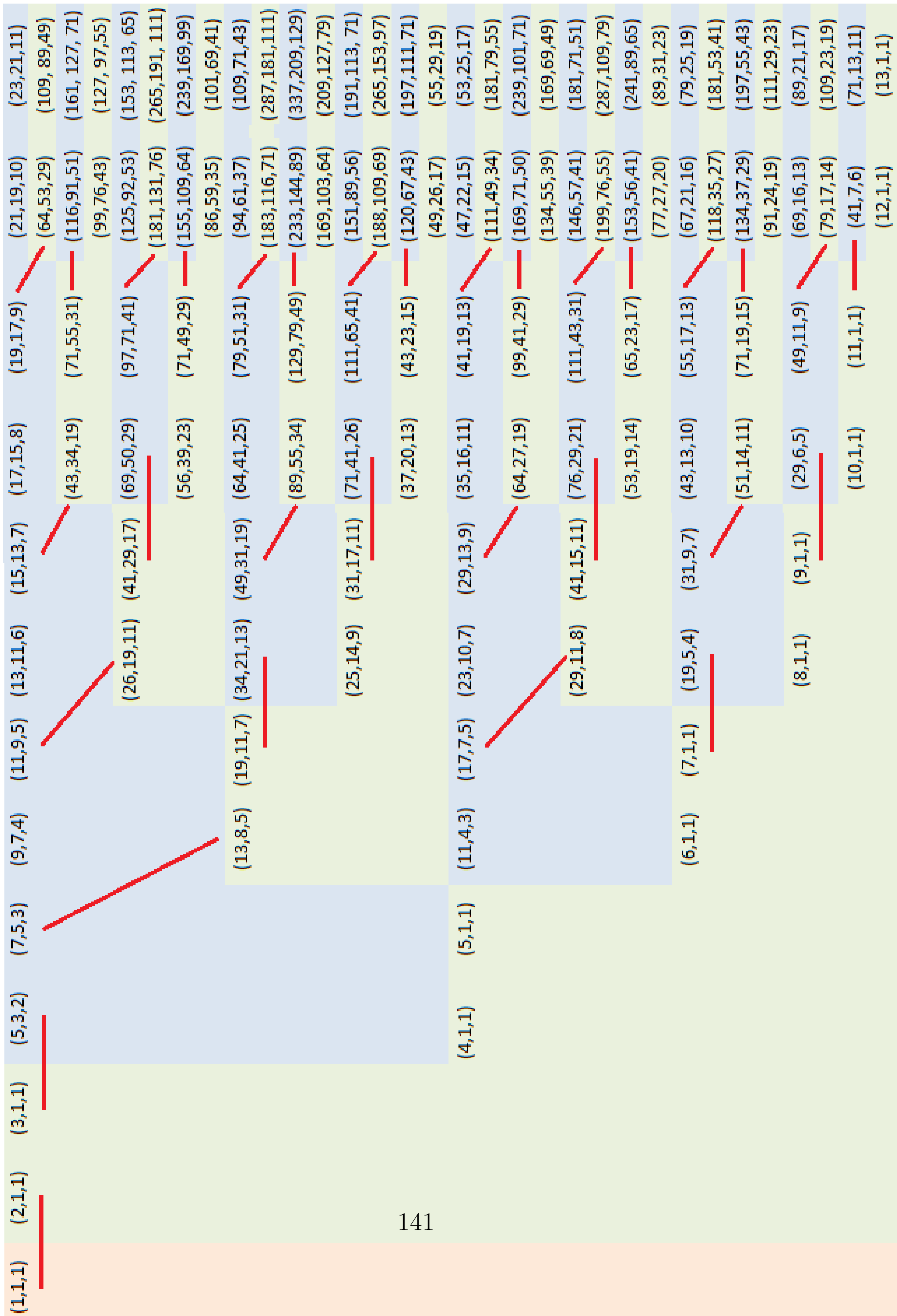


Figure 9.6: The HT tree

Chapter 10

Finding the general form for a regular period-m order-n cycle

As we collect examples of regular periodic recurrence relations over $\mathbb{Q}$, it is natural to seek to categorise them into the smallest possible number of families (with parameters as coefficients) that cover all cases. Broadly speaking, we have explored three methods for adding a parameter to a cycle;

1. by employing Derive to arrive at a set of simultaneous equations that can then be solved, using the procedure detailed in Chapter 4.

2. by employing the cross-ratio, MC, RMC, OC and ROC methods with parameters, using the ideas detailed in Chapters 2 and 8.

3. by employing the conjugacy method to add parameters, using the ideas outlined in Chapter 2.

These methods each have their advantages and disadvantages. Method 1 gives the cleanest and simplest results where they exist, but there are limits to Derive's capabilities, and the number of equations to be solved multiplies swiftly. A certain amount of 'faith' is required that simplification will occur. Method 2 only applies for the cross-ratio in the order-m period-$(m + 3)$ case, and for the MC, RMC, OC and ROC functions in the order-m period-$(m+2)$ case. Method 3 adds parameters to a cycle of any period and order, but the result may be over-complicated – for example, the period-3 cycle

$x, y, \frac{1}{xy}, x, y \ldots$ yields on conjugation

$$x, y, -\frac{xy(p^2q - r^2s) + x(pq^2 - rs^2) + y(pq^2 - rs^2) + q^3 - s^3}{xy(p^3 - r^3) + x(p^2q - r^2s) + y(p^2q - r^2s) + pq^2 - rs^2}, x, y, \ldots.$$

If we compare this to the general period-3, order-2 cycle

$$x, y, \frac{axy + bx + by + c}{dxy - ax - ay - b}, x, y, \ldots$$

as given by Method 1, we can see that the cycle given by the conjugacy method is of the correct shape but is in an over-elaborated form.

A combination of these methods is used here to give globally periodic regular order-m period-n cycles for $m, n \leqslant 6$; some of these formulations have already appeared in these pages, but they are collected together here for completeness. This list becomes less comprehensive as the period gets larger, where I have tried to balance the qualities of generality and simplicity. Pseudo-cycles such as $x, y, z, \frac{1}{x}, \frac{1}{y}, \frac{1}{z}, \ldots$ have been ignored. The parameters are given as p, q, r and s – throughout there is the question of duplication that we met in Chapter 7. I have chosen here to simply state each rational function in its homogenous form, and it is left to the reader to alter this if they so wish. The numerators and denominators are given in expanded form unless there is a factorisation that is especially neat or symmetric. I give each representation a rough D-score out of 10 – $D = 10$ is 'completely definitive' (or comprehensive), $D = 1$ is 'hardly definitive at all'. The lower D-scores have been awarded intuitively.

10.1 Period-1

10.1.1 Period-1 Order-1

$$x, x, x, \ldots \quad (D = 10)$$

10.2 Period-2

10.2.1 Period-2 Order-1

$$x, \frac{px+q}{rx-p}, x, \ldots \quad (D=10)$$

10.2.2 Period-2 Order-2

$$x, y, x, y, \ldots \quad (D=10)$$

10.3 Period-3

10.3.1 Period-3 Order-1

The RMC, ROC methods apply here.

$$x, \frac{pqx-(p^2+pr+r^2)}{q^2x+qr}, \frac{qrx+(p^2+pr+r^2)}{-q^2x+pq}, x, \ldots \quad (D=10)$$

10.3.2 Period-3 Order-2

$$x, y, \frac{pxy+qx+qy+r}{sxy-px-py-q}, x, y, \ldots \quad (D=10)$$

10.3.3 Period-3 Order-3

$$x, y, z, x, y, z, \ldots \quad (D=10)$$

10.4 Period-4

10.4.1 Period-4 Order-1

$$x, \frac{2pqx-p^2-r^2}{2q^2x+2qr}, \frac{q(p-r)x-p^2-r^2}{2q^2x-pq+qr}, \frac{2qrx+p^2+r^2}{-2q^2x+2pq}, x, \ldots \quad (D=10)$$

10.4.2 Period-4 Order-2

The MC, RMC, OC, ROC methods apply here. Method 1 provided this:

$$x, y, \frac{pxy(q^2+qs-rs)+p^2qx+p^2ry+p^3}{xy(r+s-q)(q^2+2qs+r^2+s^2)+prx(r+s-q)-py(q(r+s)+s^2)+p^2s},$$

$$\frac{-pxy(q(r+s)+s^2)-p^2rx+p^2sy-p^3}{xy(q-r-s)(q^2+2qs+r^2+s^2)+px(q^2+qs-rs)+pry(q-r-s)+p^2q},$$

$$x, y, \ldots \quad (D=9)$$

10.4.3 Period-4 Order-3

Method 1 provided this:

$$x, y, z, \frac{xyz(p+2)-xy-qxz-px-yz-py-pz-p^2}{rxyz-xy(p+2)-xz(p+2)-yz(p+2)+x+qy+z+p},$$

$$x, y, z, \ldots \quad (D=7)$$

We could use the conjugacy method on $x, y, z, p-x-y-z, \ldots$.

10.4.4 Period-4 Order-4

$$w, x, y, z, w, x, y, z, \ldots \quad (D=10)$$

10.5 Period-5

10.5.1 Period-5 Order-1

Does not exist with rational coefficients. $(D=10)$

10.5.2 Period-5 Order-2

The cross-ratio method applies here. Note that we have here involutions in the Fomin and Reading sense. (Version 1 and Version 2 together, $D = 7$)

Version 1 (without xy terms)

$$x, y, \frac{pqx + qry - p^2 - pr + r^2}{q^2x - pq},$$

$$\frac{pq^2xy + qx(r^2 - p^2) + qy(r^2 - p^2) + (p - r)(p^2 + pr - r^2)}{q^3xy - pq^2x - pq^2y + p^2q},$$

$$\frac{qrx + pqy - p^2 - pr + r^2}{q^2y - pq}, x, y, \ldots$$

Version 2 (including xy terms, the dual of Version 1).

$$x, y, \frac{pq^2xy + qx(r^2 - p^2) - p^2qy + (p - r)(p^2 + pr - r^2)}{q^3xy - pq^2x - pq^2y + q(p^2 - r^2)},$$

$$\frac{q^2xy - pqx - pqy + p^2 + pr - r^2}{qr},$$

$$\frac{pq^2xy - p^2qx + qy(r^2 - p^2) + (p - r)(p^2 + pr - r^2)}{q^3xy - pq^2x - pq^2y + q(p^2 - r^2)}, x, y, \ldots.$$

10.5.3 Period-5 Order-3

The MC, RMC, OC, ROC methods apply here. The simplest recurrence I know the conjugacy method could apply to is

$$x, y, z, \frac{(x - 1)(y - 1)(z - 1)}{z(xy - x + 1)}$$

$$\frac{x(y - 1) + y(z - 1) + 1}{(1 - x)(y(z - 1) + 1)}, x, y, z, \ldots. \quad (D = 3)$$

10.5.4 Period-5 Order-4

The conjugacy method can be applied to the following recurrence:

$$w, x, y, z, p - w - x - y - z, w, x, y, z, \ldots \quad (D = 3)$$

10.5.5 Period-5 Order-5

$$v, w, x, y, z, v, w, x, y, z, \dots \quad (D = 10)$$

10.6 Period-6

10.6.1 Period-6 Order-1

$$x, \frac{3pqx - p^2 + pr - r^2}{3q^2x + 3qr}, \frac{q(2p-r)x - p^2 + pr - r^2}{3q^2x - q(p-2r)}, \frac{3q(p-r)x - 2(p^2 - pr + r^2)}{6q^2x - 3q(p-r)},$$

$$\frac{qx(p-2r) - (p^2 - pr + r^2)}{3q^2x - q(2p-r)}, \frac{3qrx + p^2 + pr + r^2}{-3q^2x + 3pq}, x, \dots. \quad (D = 10)$$

10.6.2 Period-6 Order-2

The simplest recurrence known here is given by $\frac{y}{x}$, and we can use the conjugacy method on this. $(D = 3)$

$$x, y, -\frac{prxy(q-s) + qsx(p-r) + y(q^2r - ps^2) + qs(q-s)}{prxy(p-r) + x(p^2s - qr^2) + pry(q-s) + qs(p-r)},$$
$$-\frac{x(pq - rs) + (q+s)(q-s)}{x(p+r)(p-r) + pq - rs}, -\frac{y(pq - rs) + q^2 - s^2}{y(p^2 - r^2) + pq - rs},$$
$$-\frac{prxy(q-s) + x(q^2r - ps^2) + qsy(p-r) + qs(q-s)}{prxy(p-r) + prx(q-s) + y(p^2s - qr^2) + qs(p-r)}, x, y, \dots.$$

Note that the pattern here is $x, y, f(x,y), g(x), g(y), f(y,x), x, y, \dots$ where $g(x)$ is an involution. But not all period-6 cycles have this shape, for example,

$$x, y, \frac{(x-1)(y-1)}{x-y-1}, -\frac{x(y-2)+2}{y}, \frac{x(y-2)+y+2}{1-x}, -\frac{x(y-1)+y+1}{x-y-1}, x, y, \dots.$$

The conjugacy method could be used on this recurrence too. $(D = 3)$

10.6.3 Period-6 Order-3

The cross-ratio method applies here.

$$x, y, z, \frac{p^3xyz - p^2qxy + p^2qxz - pq^2x - 2pq^2y - 2pq^2z + 4q^3}{p(q-py)(pz+q)},$$

$$\frac{p^4xy^2z+p^3qxy^2+p^3qxyz-p^2q^2xy-2pq^3x+p^3qy^2z+p^2q^2y^2-p^2q^2yz-3pq^3y-2pq^3z+4q^4}{-p^4xyz+p^3qxy-p^3qxz+p^2q^2x+p^3qyz+3p^2q^2y+p^2q^2z-5pq^3},$$

$$\frac{p^3xyz + p^2qxz - 2pq^2x - p^2qyz - 2pq^2y - pq^2z + 4q^3}{p(q-py)(px+q)}, x, y, z, \dots \quad (D=3).$$

We could also use the conjugacy method on $x, y, z, \frac{xz^2}{y^2}, \dots$.

10.6.4 Period-6 Order-4

The MC, RMC, OC, ROC methods apply here. The simplest recurrence I know the conjugacy method could apply to is

$$w, x, y, z, \frac{(w-1)(x-1)(y-1)(z-1)}{xz + wz - xyz - wxz - z},$$

$$\frac{wxyz - wxy + xy + wx - x - wyz + yz + wy - y - w + 1}{(1-w)(xy - x + yz - y + 1)}, w, x, y, z, \dots \quad (D=3)$$

10.6.5 Period-6 Order-5

The conjugacy method can be applied to the following recurrence:

$$v, w, x, y, z, p - v - w - x - y - z, v, w, x, y, z, \dots \quad (D=3)$$

10.6.6 Period-6 Order-6

$$u, v, w, x, y, z, u, v, w, x, y, z, \dots \quad (D=10)$$

Chapter 11

HT Asymptotics

Number theorists care greatly about the asymptotic behaviour of the objects they study. Take, for example the Prime Number Theorem; we now know (thanks to Hadamard and de la Vallee Poussin in 1896) that $\frac{\pi(x)}{x}$, where $\pi(x)$ is the number of primes less than x, tends to $\frac{1}{\ln(x)}$ as x tends to infinity. Such a formulation is of great use to mathematicians – it makes sense, therefore, to examine HTs from this perspective.

11.1 Bounds for the elements of an HT

Suppose we are given an HT (p, q, r) with $p > q > r$. Note that $q < 2r$, since

$$\frac{2(pq+1)}{p+q} - q = \frac{2pq + 2 - pq - q^2}{p+q} = \frac{pq - q^2 + 2}{p+q} > 0.$$

We have $p > 2r$ since $p - 2r = p - (\frac{2pq+2}{p+q}) = \frac{p^2-pq-2}{p+q} = \frac{p(p-q)-2}{p+q} > 0$ for $p > 3$. Also $p \leqslant r^2 + r - 1$ since $p = \frac{qr-1}{q-r} = r + \frac{r^2-1}{q-r} \leqslant r^2 + r - 1$. So $r < q < 2r$, and $2r < p < r^2 + r - 1$. Now

$$pqr = n \Longrightarrow r \times r \times 2r < n < r \times 2r \times (r^2 + r - 1) < r \times 2r \times 2r^2.$$

So $2r^3 < n < 4r^4$, which gives $\sqrt[4]{\frac{n}{4}} < r < \sqrt[3]{\frac{n}{2}}$.

Now consider q. We have that $r < q < 2r$, so $\frac{q}{2} < r < q$. We also have $p = \frac{qr-1}{q-r} = \frac{q^2-1}{q-r} - q \leqslant q^2 - q - 1 < q^2$. So if $pqr = n$, then

$\frac{q}{2} \times q \times q < n < q \times q \times q^2$. So $\frac{q^3}{2} < n < q^4$ and $\sqrt[4]{n} < q < \sqrt[3]{2n}$.

Now consider p. We have $2r < p < 2r^2$, and $q < p < q^2$, so $\sqrt{\frac{p}{2}} < r < \frac{p}{2}$, and $\sqrt{p} < q < p$. We thus have that if $pqr = n$, $\sqrt[3]{2n} < p < \sqrt{n\sqrt{2}}$.

So taking our three inequalities $\sqrt[4]{\frac{n}{4}} < r < \sqrt[3]{\frac{n}{2}}, \sqrt[4]{n} < q < \sqrt[3]{2n}$, and $\sqrt[3]{2n} < p < \sqrt{n\sqrt{2}}$, we can arrive at a crude upper bound for pqr of $C(\sqrt[3]{n})(\sqrt[3]{n})(\sqrt{n}) \sim Cn^{7/6}$. So $|\{(p,q,r)$ an HT: $pqr = n\}| \leqslant Cn^{\frac{7}{6}}$. So $|\{(p,q,r)$ an HT: $pqr \leqslant n\}| \leqslant C\Sigma n^{\frac{7}{6}} \leqslant Cn^{\frac{13}{6}}$ (by integration). The UC suggests that

$$|\{(p,q,r) \quad \text{an HT} \quad : pqr \leqslant n\}| \leqslant n.$$

11.2 Exploring $h(n) = a(n) + b(n) + c(n)$

We have defined $h(n)$ to be the number of HTs (a,b,c) where $a \geqslant b \geqslant c$ in which n appears, and we can further write $h(n) = a(n) + b(n) + c(n)$, where $a(n)$ is the number of appearances for n as $a, b(n)$ for n as b and $c(n)$ for n as c (this includes the trivial HTs.) If $c = \frac{ab+1}{a+b}$, we have three helpful factorisations

$$(a+b)(a-c) = a^2 - 1, (a+b)(b-c) = b^2 - 1, \quad \text{and} \quad (a-c)(b-c) = c^2 - 1.$$

So $h(n)$ is the number of solutions (a,b,c) for the equations

$$(n+b)(n-c) = n^2 - 1, \quad \text{where} \quad n > b, n > c,$$

$$(a+n)(n-c) = n^2 - 1, \quad \text{where} \quad a > n > c, \quad \text{and}$$

$$(a-n)(b-n) = n^2 - 1 \quad \text{where} \quad a > n, b > n.$$

This implies $h(n) = d(n^2 - 1)$, supplying an alternative proof to Theorem 3.1. The task before us now is to examine $a(n)$ and $b(n)$ and their asymptotic behaviour.

11.3 Divisors d such that $a < d < 2a$

Table 11.1 shows the case when n = 11. Given that a is the largest element, only $(11,9,5), (11,4,3)$ and $(11,1,1)$ count here towards $a(11)$, which is 3

$d=a+b$	$a-c$	a	b	c
120	1	11	109	10
60	2	11	49	9
40	3	11	29	8
30	4	11	19	7
24	5	11	13	6
20	**6**	**11**	**9**	**5**
15	**8**	**11**	**4**	**3**
12	**10**	**11**	**1**	**1**

Table 11.1: HTs where the first or second term is 11

(the lines in red in Table 11.1). The other five HTs show $b(11)=5$, and we know $c(11)=8$. Consideration of Table 11.1 shows us that the divisors d of a^2-1 that give us a HT beginning with a are those such that $a<d<2a$. Let us define

$$\mathrm{A}(x)=\sum_{n=2}^{x} a(n)=\sum_{a=2}^{x}\sum_{d|a^2-1} 1, \quad \text{where} \quad a<d<2a.$$

So we have $\mathrm{A}(2)=1$, that is the HT (2,1,1), while $\mathrm{A}(5)=5$, counting the HTs (2,1,1), (3,1,1), (4,1,1), (5,1,1) and (5,3,2); only (1,1,1) is not included.

A. E. Ingham begins a paper germane to our study [36] by quoting a result of Ramanujan, that

$$\sum_{v=1}^{x}(d(v))^2 \sim \frac{1}{\pi^2}x(\ln x)^3.$$

where $d(x)$ is the number of positive divisors of x. Ingham goes on to prove the related result that

$$\sum_{v=1}^{x} d(v)d(v+k) \sim \frac{6}{\pi^2}\sigma_{-1}(k)x(\ln x)^2,$$

where k is a fixed positive integer and where $\sigma_a(k)$ is the sum of the a^{th} powers of the the divisors of k. The difference in the two results can be explained by the fact that if $d(v)$ is large, there is no guarantee that $d(v+k)$ will be also; in Ramanujan's result, the large values for $d(v)$ dominate.

Taking k as 2 in Ingham's result would seem to help us, since

$$d(a-1)d(a+1) = d(v)d(v+2) \quad \text{if} \quad v = a-1,$$

but $d(a^2-1)$ is only $d(a-1)d(a+1)$ when a is even (if a is odd, then $a-1$ and $a+1$ are not coprime, so we cannot use the multiplicative property of $d(x)$). We do, however, borrow from Ingham's line of argument in what follows. We differ from his account in that we require the extra condition that $a < d < 2a$. The literature on restricted divisor sums is collected by Broughan [14], who examines

$$\sum_{1 \leqslant n \leqslant x} d_\alpha(f(n)),$$

where $f(n)$ is one of several quadratic or linear polynomials, and where $d_\alpha(n) = |\{d : d|n, 1 \leqslant d \leqslant \alpha\}|$ for real $\alpha \geqslant 1$.

11.4 Forming quartets (l, r, m, s)

Take a positive integer value for x. Suppose that for some $0 < a < x, d|a^2-1$. Then we can write d as rs, where $r|(a+1)$ and $s|(a-1)$. So we have $lr = a+1$ and $ms = a-1$ for positive integers l, r, m, s, and $lr - ms = 2$. We thus have that $\gcd(l,m)|2, \gcd(r,s)|2$. We also insist that $a < d < 2a$. Our plan from here is this – we will define four sets for some value of x as follows:

1. $S = \{\text{HTs } (a,b,c) : a < x\}$,
2. $T = \{(a,d,d') : a < x, dd' = (a^2-1), a < d < 2a\}$,
3. $U = \{(l,r,m,s) : lr = a+1, ms = a-1, a < rs < 2a, a < x\}$.
4. $V = \{(l,m), lm < x\}$.

We will attempt to establish a bijection between S and some subset of V; counting elements of V is a standard if tricky problem. The sets T and U

will be intermediate aids in constructing this bijection.

Consider the sets S and T. There is a natural bijection between them, since we can map $(a,b,c) \in S$ to $(a, a+b, a-c) \in T$, with the inverse map taking $(a,d,d') \in T$ to $(a, d-a, a-d') \in S$.

Now there is a natural surjective map $f : U \mapsto T$ such that $f : (l,r,m,s) \mapsto (lr-1, rs, lm)$. Given any $(a,d,d') \in T$, we can write $d = rs$, where $r|(a+1), s|(a-1), l = \frac{a+1}{r}, m = \frac{a-1}{s}, d' = lm$ yielding an element of U that maps to (a,d,d').

But $f : U \mapsto T$ is not injective. Suppose that lm and rs are both even. This means d and d' are both even, and so $2d|(a^2-1)$, giving $\frac{d}{2}|\frac{a-1}{2}\frac{a+1}{2}$. Say $\frac{d}{2} = r's'$, where $r'|\frac{a+1}{2}$, and $s'|\frac{a-1}{2}$. Then

$$f : \left(l = \frac{a+1}{2r'}, 2r', m = \frac{a-1}{s'}, s'\right) \mapsto (a,d,d'),$$

and also

$$f : \left(l = \frac{a+1}{r'}, r', m = \frac{a-1}{2s'}, 2s'\right) \mapsto (a,d,d').$$

So if we say $U = U_1 \sqcup U_2$, where $U_1 = \{(l,r,m,s) : \text{either } rs \text{ or } lm \text{ is odd}\}$ and $U_2 = \{(l,r,m,s) : \text{both } rs \text{ and } lm \text{ are even }\}$, then f is bijective on U_1 but $2-1$ on U_2.

For example, take $(a,d,d') = (\text{even, odd, odd}) = (124,\ 205,\ 75)$. We have

$$rs = 205 = 5.41, r|125 = 5^3, s|123 = 3.41,$$

which gives $r = 5, s = 41$ and $(l,r,m,s) = (25,5,3,41)$ as the only possibility. If $(a,d,d') = (\text{odd, even, odd}) = (155,\ 168,\ 143)$, for example, we have

$$rs = 168 = 2^3.3.7, r|156 = 2^2.3.13, s|154 = 2.7.11,$$

which gives $r = 12, s = 14$ and $(l,r,m,s) = (13,12,11,14)$ as the only possibility. If $(a,d,d') = (\text{odd, odd, even}) = (125,\ 217,\ 72)$, for example, we have

$$rs = 217 = 31.7, r|126 = 2.3^2.7, s|124 = 31.2^2,$$

which gives $r = 7, s = 31$ and $(l, r, m, s) = (18, 7, 4, 31)$ as the only possibility. If, however, $(a, d, d') =$ (odd, even, even) $=$ (125, 126, 124), for example, we have

$$rs = 126 = 2.3^2.7, r|126 = 2.3^2.7, s|124 = 2^2.31,$$

which gives $r = 7$ or 63, $s = 1$ or 2 and $(l, r, m, s) = (1, 126, 124, 1)$ or (2,63,62,2) as the two possibilities. Notice in this last case that a pair of 2s 'moves outwards' in (l, r, m, s) from r and m to l and s. This cannot happen in the other three cases.

What happens when mapping from V to U? Since $lr - ms = 2$, $\gcd(l, m) = 1$ or 2. Suppose we have a pair of values (l, m) so that $lr - ms = 2$ and l and m are coprime – how many possible values for (r, s) are there? We have $a < d < 2a$, which means that $ms + 1 < rs < 2ms + 2$, and so

$$m + \frac{1}{s} < r < 2m + \frac{2}{s}. \tag{11.1}$$

Let us say that the general solution to $lr - ms = 2$ is $r = r_0 + \lambda m$, where $0 \leqslant r_0 < m$, and $s = s_0 + \lambda l$, where $0 \leqslant s_0 < l$. This gives from (11.1) that $m + \frac{1}{s} < r_0 + \lambda m < 2m + \frac{2}{s}$. If $\lambda = 0$, then this has no solutions, since $r_0 < m$. If $\lambda = 1$, then this has a solution unless $r_0 = s = 1$ or $r_0 = 0$, in which case it has none. If λ is 2, there will be no solution (since $r_0 + 2m > 2m + \frac{2}{s}$), unless $r_0 = s = 1$ or $r_0 = 0$, when it has one solution. Thus counting up, we have a unique solution for r and s (and thus for (a, d, d')) for each pair (l, m) with l and m coprime.

What happens when l and m are both even? When $\gcd(l, m) = 2$, let $l = 2h$, and $m = 2i$, so $lr - ms = 2$, which gives $2hr - 2is = 2$, or $hr - is = 1$. Say that the general solution to this is $r = r_0 + \lambda i$, where $0 \leqslant r_0 < i$, and $s = s_0 + \lambda h$, where $0 \leqslant s_0 < h$. This gives from (11.1) that $m + \frac{1}{s} < r_0 + \lambda i < 2m + \frac{2}{s}$, which leads to $2i + \frac{1}{s} < r_0 + \lambda i < 4i + \frac{2}{s}$, where $i \geqslant 1$. If λ is 0 or 1, then this has no solutions, since $r_0 < i$. If λ is 2, then there is one solution, unless $r_0 = s = 1$ or $r_0 = 0$. If λ is 3, there is always exactly one solution. If λ is 4, there will be no solution unless $r_0 = s = 1$ or $r_0 = 0$, in which case there is one. Thus counting up, we have exactly two solutions for r and s for each pair (l, m) with $\gcd(l, m) = 2$.

To summarise – given (l, m) in V where l and m are not both even, there is a single element in U to which (l, m) maps. If however, we are given (l, m)

in V where l and m are both even, there are now two elements in U to which (l, m) maps.

11.5 Partitioning T and V

It helps to consider all 16 parity combinations for l, r, m and s, as shown in Table 11.2. Where combinations are possible, examples are given. Note that only 0, 2 or 3 members of $\{l, r, m, s\}$ can be even, and that there is duplication in the (a, d, d') column and in the (l, m) column, since the mappings from U to T and from U to V are not 1-1.

An Excel spreadsheet removes the drudgery of the calculations for us, and makes testing hypotheses straightforward. Figure 11.1 shows some of the members of S calculated in the first three columns, followed by the corresponding members of T in the next three, and with finally the images (l, m) from the set V in the last two columns. Figure 11.2 shows the resulting points (l, m) plotted onto a Cartesian grid.

We can partition T into the four finite sets T_1 to T_4, where

1. $T_1(x) = \{(a, d, d'), a \text{ even}, d \text{ odd}, d' \text{ odd}, a < x\}$,
2. $T_2(x) = \{(a, d, d'), a \text{ odd}, d \text{ even}, d' \text{ odd}, a < x\}$,
3. $T_3(x) = \{(a, d, d'), a \text{ odd}, d \text{ odd}, d' \text{ even}, a < x\}$,
4. $T_4(x) = \{(a, d, d'), a \text{ odd}, d \text{ even}, d' \text{ even}, a < x\}$.

We can also partition V into the six finite sets V_1 to V_6, where

1. $V_1(x) = \{(l, m), \gcd(l, m) = 1, l \text{ odd}, m \text{ odd}, lm < x\}$ – Green,
2. $V_2(x) = \{(l, m), \gcd(l, m) = 2, 8|lm, lm < x\}$ – Red,
3. $V_3(x) = \{(l, m), \gcd(l, m) = 1, 4|lm, lm < x\}$ – Light blue,
4. $V_4(x) = \{(l, m), \gcd(l, m) = 1, 2|lm, 4 \nmid lm, lm < x\}$ – Yellow,
5. $V_5(x) = \{(l, m), \gcd(l, m) = 2, 8 \nmid lm, lm < x\}$ – Orange,
6. $V_6(x) = \{(l, m), \gcd(l, m) > 2, lm < x\}$ – Dark blue.

a	b	c	a	d	d'	l	m	l	m
8	1	1	8	9	7	1	7		
9	1	1	9	10	8	2	4	1	8
9	7	4	9	16	5	5	1		
10	1	1	10	11	9	1	9		
11	1	1	11	12	10	2	5	1	10
11	4	3	11	15	8	4	2		
11	9	5	11	20	6	6	1	3	2
12	1	1	12	13	11	1	11		
13	1	1	13	14	12	2	6	1	12
13	8	5	13	21	8	2	4		
13	11	6	13	24	7	7	1		
14	1	1	14	15	13	1	13		
15	1	1	15	16	14	2	7	1	14
15	13	7	15	28	8	8	1	4	2
16	1	1	16	17	15	1	15		

Figure 11.1: HTs and their (l, m) images

Experiment shows that there is a straightforward bijection between $T_1(x) \sqcup T_2(x)$ and $V_1(x)$, and another between $T_3(x)$ and $V_2(x)$. Elements in $T_4(x)$ map to two elements in U – we will define the bijection here as follows. If (a, d, d') maps to a pair that includes a member of $V_3(x)$, take that element as the image. If (a, d, d') maps to a pair of members of $V_4(x)$, take both elements, but count each as a half. These maps are both injective and surjective. This appears, after much testing, to cover every eventuality. Figure 11.2 helps to confirm that we have accounted for all appropriate (l, m) pairs.

11.6 Counting up

We now need to account for the various $V_i(x)$. We have that Green + Red + Light blue + Yellow + Orange + Dark blue cover all possibilities for (l, m). The subset of V in bijection with our set of HTs S is Green + Red + Light blue + $\frac{1}{2}$ Yellow. We can now quote the following helpful Tauberian theorem

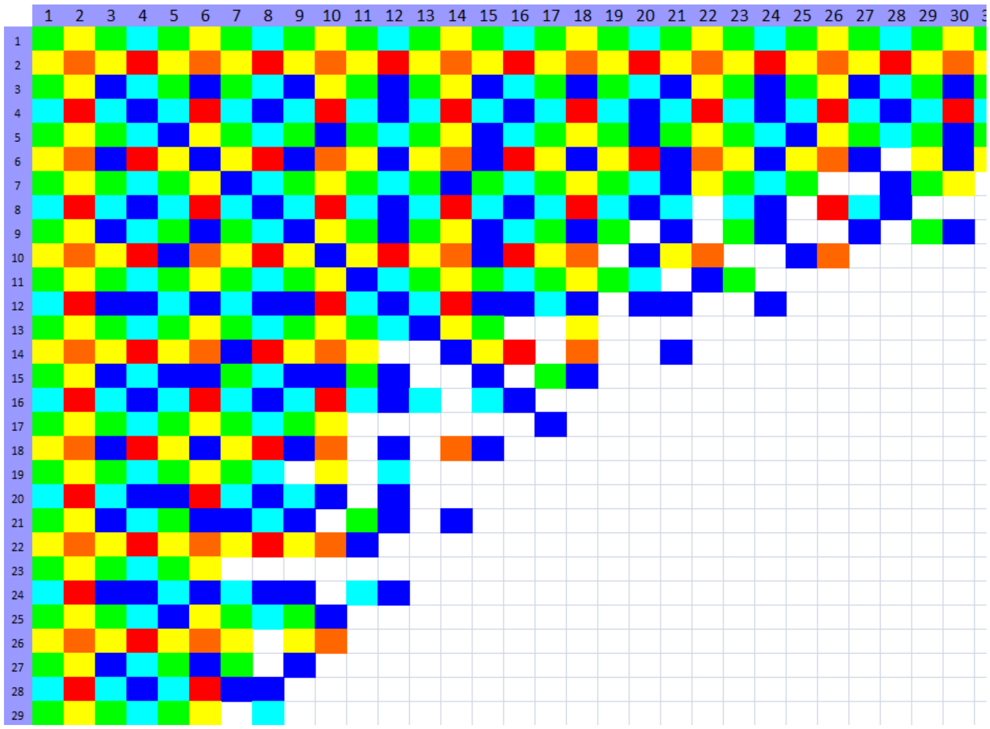


Figure 11.2: Points (l, m) on a Cartesian grid, $a < 300$

from analytic number theory, as outlined by Apostol [3]. This is

$$S_1(x) = \sum_{\gcd(l,m)=1, lm<x} 1 = \frac{6}{\pi^2} x \ln(x) + O(x).$$

We can additionally define

$$S_2(x) = \sum_{\gcd(l,m)=1, 2|lm, lm<x} 1,$$

$$S_3(x) = \sum_{\gcd(l,m)=1, 2\nmid lm, lm<x} 1,$$

$$S_4(x) = \sum_{\gcd(l,m)=1, 2\nmid m, lm<x} 1,$$

where clearly $S_1(x) = S_2(x) + S_3(x)$, so $S_3(x) = S_1(x) - S_2(x)$. Now

$$S_2(x) = \sum_{\gcd(2l',m')=1, 2l'm'<x} 1 + \sum_{\gcd(l',2m')=1, 2l'm'<x} 1$$

$$= 2S_4\left(\frac{x}{2}\right).$$

and

$$S_4(x) = \sum_{\gcd(l,m)=1, lm<x} 1 - \sum_{\gcd(l,m)=1, 2|m, lm<x} 1$$

$$= S_1(x) - \sum_{\gcd(l,2m')=1, 2lm'<x} 1$$

$$= S_1(x) - \sum_{\gcd(l,m')=1, 2\nmid l, lm'<\frac{x}{2}} 1$$

$$= S_1(x) - S_4\left(\frac{x}{2}\right),$$

and so $S_4(x) = S_1(x) - S_1\left(\frac{x}{2}\right) + S_1\left(\frac{x}{4}\right) - S_1\left(\frac{x}{8}\right), \ldots,$ which gives

$$S_4(x) = \frac{4}{\pi^2} x \ln(x) + O(x),$$

whereupon

$$S_2(x) = \frac{4}{\pi^2} x \ln(x) + O(x),$$

and

$$S_3(x) = \frac{2}{\pi^2} x \ln(x) + O(x).$$

Now we have (changing notation slightly)

$$\text{Green} = \sum_{\gcd(l,m)=1, 2\nmid lm, lm<x} (l, m) = S_3(x),$$

and

$$\text{Red} = \sum_{\gcd(l',m')=1, 2|l'm', 4l'm'<x} (2l', 2m') = S_2\left(\frac{x}{4}\right),$$

and

$$\text{Light blue} = 2 \sum_{\gcd(l',m')=1, 2\nmid m', 4l'm'<x} (4l', m')$$

$$= 2 \sum_{\gcd(l',m')=1, 2\nmid m', l'm'<\frac{x}{4}} (l', m') = 2S_4\left(\frac{x}{4}\right),$$

while

$$\text{Yellow} = 2 \sum_{\gcd(l',m')=1, 2\nmid l'm', 2l'm'<x} (2l', m') = 2S_3\left(\frac{x}{2}\right).$$

Adding up Green + Red + Light blue + $\frac{1}{2}$ Yellow, we arrive at

$$\text{LM}(x) = \frac{6}{\pi^2} x \ln(x) + O(x).$$

where $\text{LM}(x) = \{\text{HTs } (a,b,c) : lm < x\}$, where (l,m) is related to (a,b,c) using the bijection defined above. Now $a < rs < 2a$, so $\frac{a}{2} < lm < a$, and $\text{LM}\left(\frac{x}{2}\right) < \text{A}(x) < \text{LM}(x)$, and thus

$$\frac{3}{\pi^2} < \frac{\text{A}(x)}{x \ln(x)} < \frac{6}{\pi^2}$$

for large x. Experimental evidence supports these bounds.

Recall Conjecture 3.2, that the number of HTs adding to k is unbounded as $k \to \infty$. A more sophisticated way to proceed here might be to define

$$\text{HT}(x) = |\{\text{HTs} \quad (a,b,c) : a+b+c < x\}|.$$

Now

$$\text{HT}(x) \geqslant |\{\text{HTs} \quad (a,b,c) : \frac{a}{3} < x\}|,$$

which we now know is of the order of at least $Cx \ln(x)$ for some $C > 0$, and thus $\text{HT}(x) > O(x)$, and we have resolved the issue; Conjecture 3.2 is true.

a	d	d'	l	r	m	s	l	m
even 124	odd 205	odd 75	odd 25	odd 5	odd 3	odd 41	odd 25	odd 3
Impossible	×	×	odd	odd	odd	even	×	×
Impossible	×	×	odd	odd	even	odd	×	×
Impossible	×	×	odd	even	odd	odd	×	×
Impossible	×	×	even	odd	odd	odd	×	×
Impossible	×	×	odd	odd	even	even	×	×
odd 155	even 168	odd 143	odd 13	even 12	odd 11	even 14	odd 13	odd 11
odd 155	even 182	even 132	even 12	odd 13	odd 11	even 14	even 12	odd 11
odd 181	even 210	even 156	odd 13	even 14	even 12	odd 15	odd 13	even 12
odd 131	odd 143	even 120	even 12	odd 11	even 10	odd 13	even 12	even 10
Impossible	×	×	even	even	odd	odd	×	×
odd 191	even 304	even 120	even 12	even 16	even 10	odd 19	even 12	even 10
odd 191	even 304	even 120	even 24	even 8	odd 5	even 38	even 24	odd 5
odd 337	even 364	even 312	even 26	odd 13	even 12	even 28	even 26	even 12
odd 265	even 308	even 228	odd 19	even 14	even 12	even 22	odd 19	even 12
Impossible	×	×	even	even	even	even	×	×

Table 11.2: Parity combinations for l, r, m, s

Chapter 12

Cycling on three lines

We have seen how order-2 period-n recurrences can build an elliptic curve with torsion points of order n. Is it possible to find a (possibly degenerate) elliptic curve so that cycles of different periods can take place simultaneously upon it?

12.1 Combining period-6 and period-3 cycles on the same curve

Take the period-6 sequence $x, y, \frac{y}{x}, \frac{1}{x}, \frac{1}{y}, \frac{x}{y}, x, y, \ldots$. Multiplying the terms together gives 1. Adding and equating to j gives

$$x + y + \frac{y}{x} + \frac{1}{x} + \frac{1}{y} + \frac{x}{y} = j,$$

which simplifies to $x^2y + y^2x - jxy + x^2 + y^2 + x + y = 0$. This is the equation of a (possibly singular) elliptic curve. Including a parameter to give ourselves a degree of freedom, we can now look at $x, y, \frac{py}{x}, \frac{p^2}{x}, \frac{p^2}{y}, \frac{px}{y}, x, y....$ which yields the curve

$$x^2y + y^2x - jxy + px^2 + py^2 + p^2x + p^2y = 0. \tag{12.1}$$

Now consider the general period-3 Lyness cycle, $x, y, \frac{axy+bx+by+c}{dxy-ax-ay-b}, x, y \ldots$. Adding here and equating to, say, k, gives

$$x + y + \frac{axy + bx + by + c}{dxy - ax - ay - b} = k,$$

which simplifies to

$$dx^2y + dxy^2 - xy(a + dk) - ax^2 - ay^2 + akx + aky + bk + c = 0. \quad (12.2)$$

Can we choose our parameters here so that the two curves (12.1) and (12.2) are the same? If we choose $d = 1, b = 0, c = 0, a = k, j = 2k, p = -k$, then both curves become

$$x^2y + y^2x - 2kxy + -k(x^2 + y^2) + k^2(x + y) = 0. \quad (12.3)$$

Is this an elliptic curve? In fact (12.3) factorises to

$$(x - k)(y - k)(x + y) = 0,$$

that is, the three straight lines $x = k, y = k$, and $x + y = 0$. How does the addition of points work here? When presented with a degenerate elliptic curve that has a cusp or a double point, we can carry out our standard technique for addition as long as we avoid the obvious problem intersection points. With our three straight lines above, it is clear what $A + B$ must be if A and B are on different lines, but if they are on the same line? The group law fails to operate straightforwardly here.

12.2 Adding a period-5 cycle

Is it possible to find a period-5 cycle that also adds or multiplies to the invariant curve (12.3)? The period-5 Lyness cycle with two parameters

$$x, y, \frac{px + qy - p^2 - pq + q^2}{x - p}, \frac{x(py - p^2 + q^2) + (q - p)(y(p + q) - p^2 - pq + q^2)}{(x - p)(y - p)},$$
$$\frac{qx + py - p^2 - pq + q^2}{y - p}, x, y...$$

gives five terms that we can add, to give, say, l. Expanding this yields

$$x^2y + x^2(q - p) + xy^2 + xy(p - l) - x(2p^2 + p(2q - l) - 2q^2)$$
$$+y^2(q - p) - y(2p^2 + p(2q - l) - 2q^2) + 3p^3 + p^2(2q - l) - 4pq^2 + q^3 = 0.$$

Comparing coefficients with (12.3), if we put $p = k + q, q = l - 3k, l = k$ we have the cycle-sum

$$x + y + -k\frac{x + 2y - k}{x + k} + \frac{k(k(3y - k) - x(y - 3k))}{(x + k)(y + k)} - k\frac{2x + y - k}{y + k} = k$$

which simplifies again to (12.3).

12.3 Adding a period-4 cycle

Can we add a period-4 cycle to this collection? This would give the complete (as far as we know) set of periods for rational binary recurrences. Consider the (irregular) period-4 cycle

$$x, y, \frac{x+y^2}{xy-1}, \frac{x^2+y}{xy-1}, x, y, \ldots .$$

We can add two parameters p and q to this (using the conjugacy method, putting $r=-p, s=1$) to give the period-4 cycle

$$x, y, -\frac{px(py(q-2)-2q+1)+p^2y^2(q+1)+pqy(q-2)-q(q-2)}{p(px(3py+q-2)+py(q-2)-2q+1)},$$

$$-\frac{p^2x^2(q+1)+px(q-2)(py+q)+py(1-2q)-q^2+2q}{p(px(3py+q-2)+py(q-2)-2q+1)}, x, y, \cdots .$$

We can add these terms and equate to the result to m, say. Choosing $m=2k$, $q=1$ and $p=\frac{1}{k}$ gives the period-4 cycle

$$x, y, \frac{k(x(y+k)-2y^2+ky-k^2)}{x(3y-k)-k(y+k)},$$

$$\frac{k(2x^2-x(y+k)-k(y-k))}{k(y+k)-x(3y-k)}, x, y, \ldots,$$

and

$$x+y+\frac{k(x(y+k)-2y^2+ky-k^2)}{x(3y-k)-k(y+k)}+\frac{k(2x^2-x(y+k)-k(y-k))}{k(y+k)-x(3y-k)}=2k$$

gives exactly (12.3) once more.

12.4 All four cycles

So we now have Lyness cycles with periods 3, 4, 5 and 6, whose terms add as follows:

$$x+y+\frac{kxy}{xy-kx-ky}=k,$$

$$x+y+\frac{k(x(y+k)-2y^2+ky-k^2)}{x(3y-k)-k(y+k)}+\frac{k(2x^2-x(y+k)-k(y-k))}{k(y+k)-x(3y-k)}=2k,$$

$$x+y+\frac{k^2-kx-2ky}{x+k}+\frac{-k^2xy+3k^3x+3k^2y-k^3}{(x+k)(y+k)}+\frac{k^2-ky-2kx}{y+k}=k,$$

$$x+y+\frac{-ky}{x}+\frac{k^2}{x}+\frac{k^2}{y}+\frac{-kx}{y}=2k.$$

Each of these four equations simplifies to $(x-k)(x+y)(y-k)=0$.

Figure 12.1 shows these four cycles in action. Our starting point for each cycle is, let's say, (1, 2). For this to be on the curve, $(x-k)(x+y)(y-k)=0$ gives $k=1$ or $k=2$. Let us choose $k=1$. This gives the points (1,2), (2, -2), (-2,1) as the period-3 cycle; the points for the other cycles are produced in a similar way. The red lines are $y=1, x=1$ and $x+y=0$. The period-3 Lyness cycle is seen in dark blue. The period-4 cycle agrees with this for the first two dark blue lines, but then takes the green path. The period-5 cycle also coincides with the first two dark blue lines, but then diverges onto the orange path. Finally the period-6 cycle takes the first two dark blue vectors from (2, 1) before taking the purple route. Figure 12.2 shows the same paths, but on a isometric grid. We can create an animation here by varying k.

12.5 The cross-ratio cycle

Another degenerate cubic that is of interest is derived from the period-6 cycle

$$x, y, -\frac{y}{x}, \frac{1}{x}, \frac{1}{y}, -\frac{x}{y}, x, y, \ldots. \tag{12.4}$$

Adding the terms and equating to k gives

$$x^2y-x^2+xy^2-kxy+x-y^2+y=0. \tag{12.5}$$

Note that putting $y=1-x$ into (12.4) gives the terms

$$x, 1-x, \frac{x-1}{x}, \frac{1}{x}, \frac{1}{1-x}, \frac{x}{x-1},$$

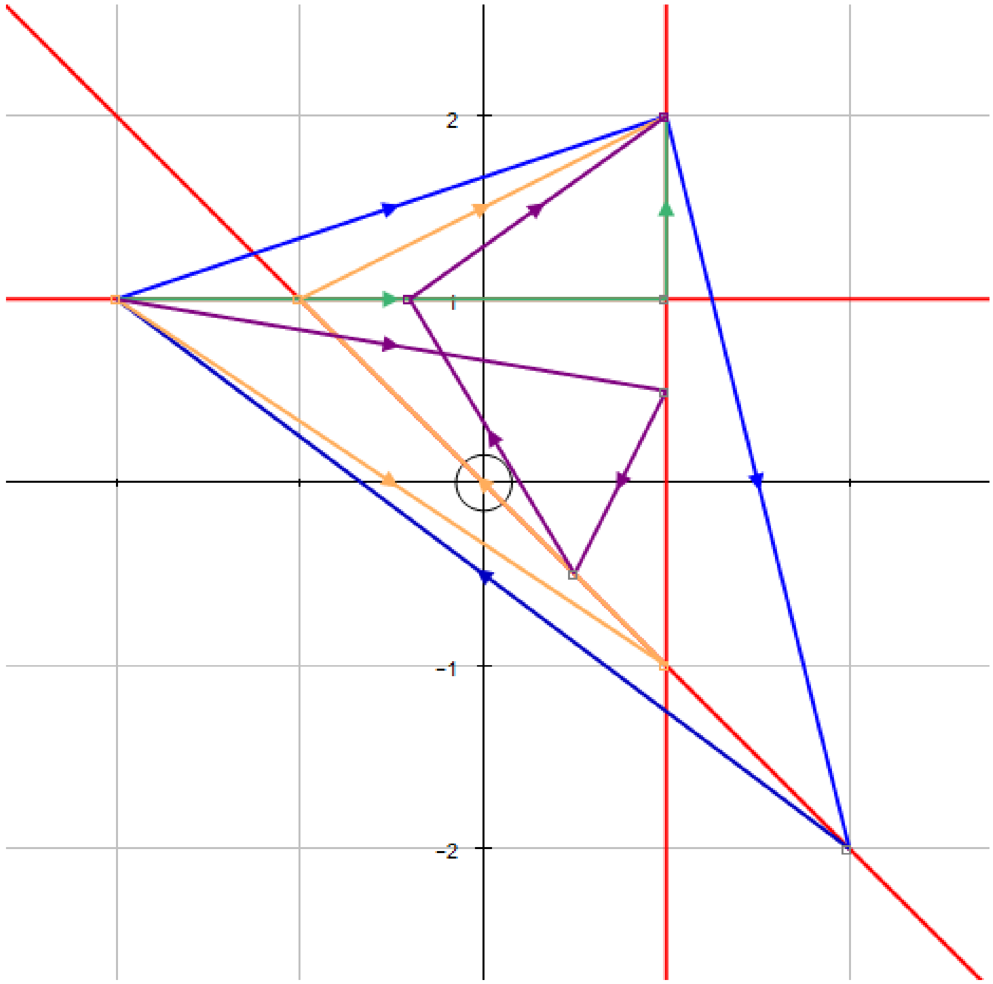


Figure 12.1: $(x - k)(y - k)(x + y) = 0$: Cartesian

precisely the values taken by the cross-ratio (substituting $y = \frac{x}{x-1}$ accomplishes the same thing). Now

$$x + 1 - x + \frac{x-1}{x} + \frac{1}{x} + \frac{1}{1-x} + \frac{x}{x-1} = 3,$$

so $k = 3$, and the curve (12.5) simplifies to $(x + y - 1)(xy - x - y) = 0$, a straight line together with a hyperbola, as shown in Figure 12.3. Plotting

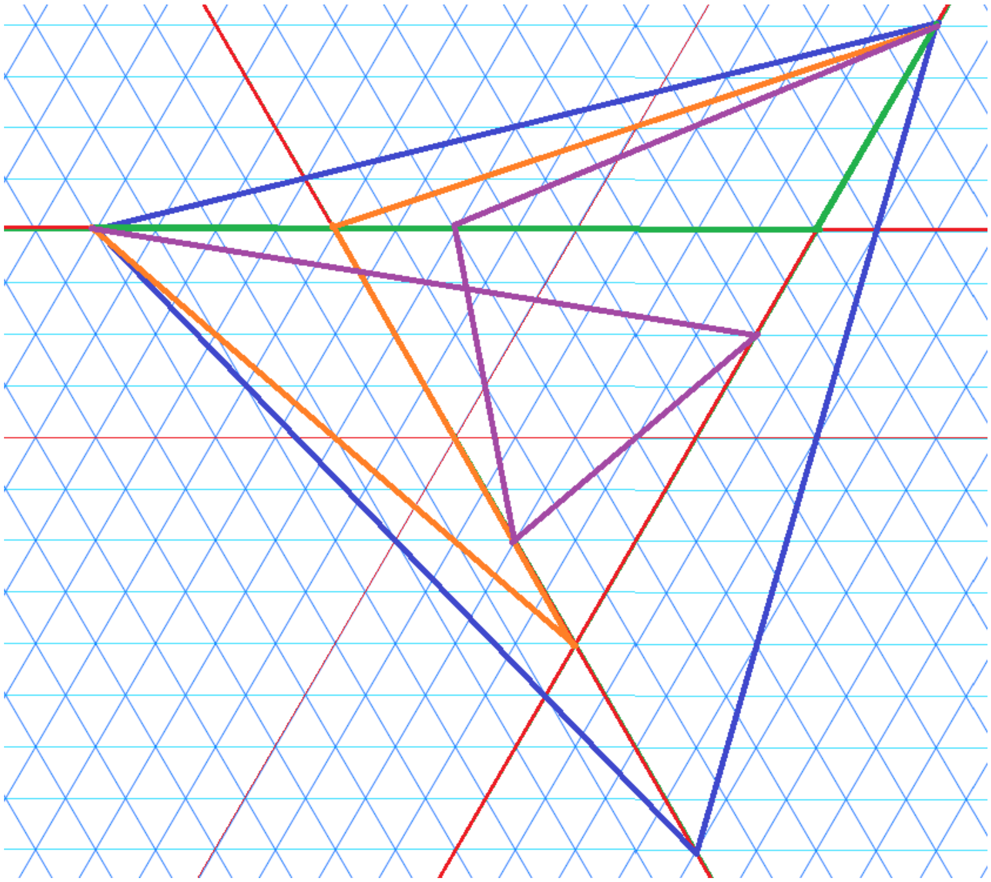


Figure 12.2: $(x-k)(y-k)(x+y)=0$: Isometric

the points

$$(a, 1-a), \left(1-a, \frac{a-1}{a}\right), \left(\frac{a-1}{a}, \frac{1}{a}\right), \left(\frac{1}{a}, \frac{1}{1-a}\right), \left(\frac{1}{1-a}, \frac{a}{a-1}\right), \left(\frac{a}{a-1}, a\right)$$

creates a cycle on the curve, as shown in Figure 12.4. Once again, we can create an animation as a varies.

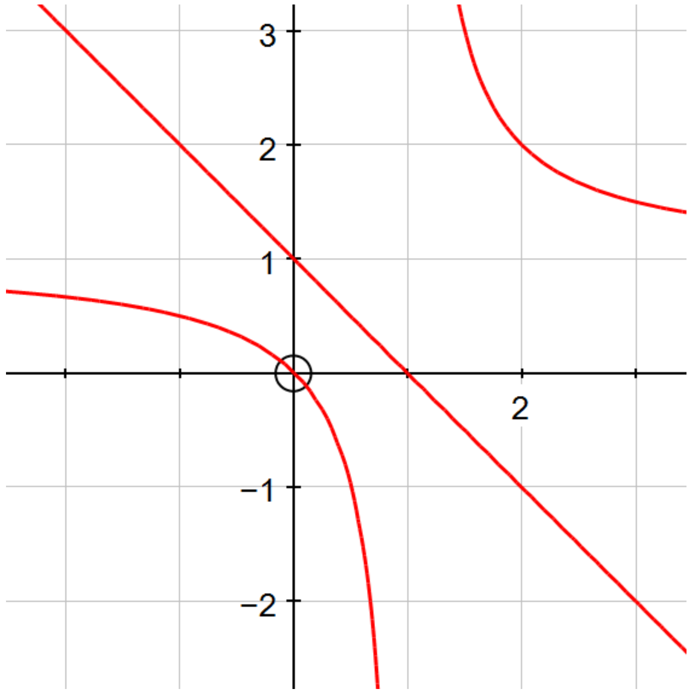


Figure 12.3: The cross-ratio invariant

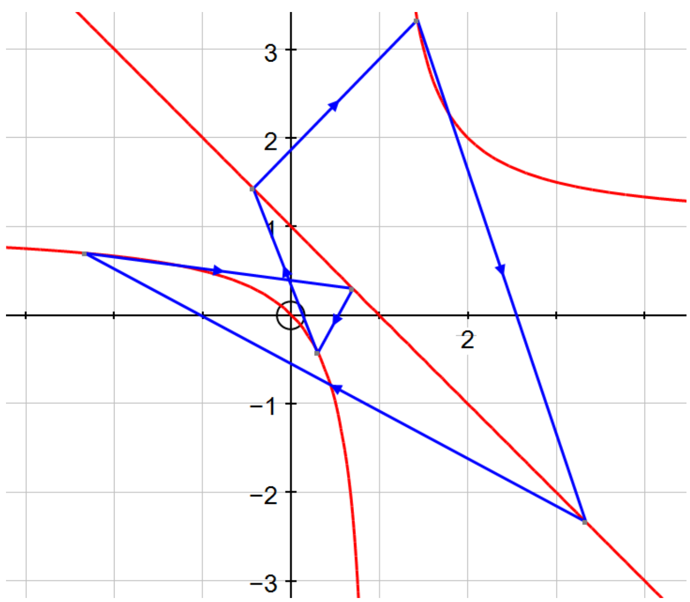


Figure 12.4: The cross-ratio cycle

Chapter 13

Proving the Uniqueness Conjecture for HTs

13.1 Initial assumptions

Recall that in Chapter 3 we stated the UC as

If (a, b, c) and (p, q, r) are non-trivial HTs with $abc = pqr = n$ then $(a, b, c) = (p, q, r)$.

Let us attempt a proof by contradiction. Suppose (a, b, c) and (p, q, r) are distinct HTs with $abc = pqr = n$, where neither (a, b, c) nor (p, q, r) are trivial. Let us assume without loss of generality that $a \leqslant p$. Now symbols $<, >$, and $=$ must lie between (a, b, c) and (p, q, r) somehow, for example:

$$\begin{pmatrix} a \\ b \\ c \end{pmatrix} \begin{matrix} < \\ = \\ > \end{matrix} \begin{pmatrix} p \\ q \\ r \end{pmatrix}$$

We have 27 possibilities to check. Clearly $a < p$ and $b < q$ means that $c < r$, since

$$\frac{pq+1}{p+q} - \frac{ab+1}{a+b} = \frac{(pa-1)(q-b)+(qb-1)(p-a)}{(a+b)(p+q)} > 0.$$

but this means $abc < pqr$, which is a contradiction. Similar checking reveals that the only three possibilities for the relations are

$$\begin{pmatrix} a \\ b \\ c \end{pmatrix} \begin{matrix} = \\ = \\ = \end{matrix} \begin{pmatrix} p \\ q \\ r \end{pmatrix}, \quad \begin{pmatrix} a \\ b \\ c \end{pmatrix} \begin{matrix} < \\ > \\ < \end{matrix} \begin{pmatrix} p \\ q \\ r \end{pmatrix}, \quad \begin{pmatrix} a \\ b \\ c \end{pmatrix} \begin{matrix} < \\ > \\ > \end{matrix} \begin{pmatrix} p \\ q \\ r \end{pmatrix}.$$

The first of these is ruled out by our initial assumption. Let us assume for the moment that the second relationship is true. Since $\frac{ab(ab+1)}{a+b} = \frac{pq(pq+1)}{p+q}$, it is clear that

$$a+b = p+q \Rightarrow ab(ab+1) = pq(pq+1) \Rightarrow ab = pq.$$

Now $a+b = p+q, ab = pq \Rightarrow a = p, b = q$, which is a contradiction. Similarly

$$ab = pq \Rightarrow ab(ab+1) = pq(pq+1) \Rightarrow a+b = p+q \Rightarrow a = p, b = q,$$

which is a contradiction. So we know either that $a+b > p+q$ and $ab > pq$, or $a+b < p+q$ and $ab < pq$.

13.2 Partitioning n into prime powers

Consider Table 13.1, and recall from Lemma (9.4) that for an HT (a, b, c), a, b and c are pairwise coprime. Write n as the product of prime powers $p_1^{\alpha_1} p_2^{\alpha_2}, \ldots p_n^{\alpha_n}$. As $abc = pqr = n$, then we are partitioning the prime factors of n into nine sets, where no prime power can be split between two sets, that multiply to give the coprime integers d, e, f, g, h, i, j, k, and l. These multiply in threes to give a, b, c, p, q and r as in Table 13.1.

$\times$	a	b	c
p	d	e	f
q	g	h	i
r	j	k	l

Table 13.1: Prime decomposition of n

In Table 13.2, $(2977, 2975, 1488)$ and $(20553, 1603, 400)$ both multiply to $13178583600 = 2^4 \times 3 \times 5^2 \times 7 \times 13 \times 17 \times 31 \times 229$. This would settle the UC, were it not for the fact that while $(2977, 2975, 1488)$ is an HT, $(20553, 1603, 400)$ is not.

$\times$	20553	1603	400
2977	13	229	1
2975	17	7	5^2
1488	3×31	1	2^4

Table 13.2: Prime decomposition of 13178583600

13.3 Proof when n is the product of four prime powers

The UC is easily proved if n is a product of exactly four distinct prime powers. Suppose we have $n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} p_4^{\alpha_4} = P_1 P_2 P_3 P_4$, with $P_1 < P_2 < P_3 < P_4$ where $P_i = p_i^{\alpha_i}$ is a prime power. We might have, for example, $(a, b, c) = (P_3 P_4, P_2, P_1)$ while $(p, q, r) = (P_4, P_2 P_1, P_3)$. This would give us (by the HT property) the two equations

$$P_3 P_4 P_2 + 1 = P_1(P_3 P_4 + P_2), P_4 P_2 P_1 + 1 = P_3(P_4 + P_2 P_1),$$

and subtracting, we have

$$P_3 P_4 P_2 - P_4 P_2 P_1 = P_1(P_3 P_4 + P_2) - P_3(P_4 + P_2 P_1),$$

and so P_4 divides $P_1 P_2 - P_3 P_2 P_1$, so $P_4 | (P_3 - 1)$, which is a contradiction. There are a limited number of possible ways to partition P_1 to P_4, which are easily checked, meaning the UC is proved by exhaustion in this case. Can we generalise this argument?

13.4 Proof for the general case?

We have that $(a, b, c) = (dgj, ehk, fil)$ and $(p, q, r) = (def, ghi, jkl)$. The HT property means that

$$dgjehk + 1 = dgjfil + ehkfil, defghi + 1 = defjkl + ghijkl.$$

Subtracting these two equations gives

$$dgjehk - defghi = dgjfil + ehkfil - defjkl - ghijkl$$

which means

$$dgjehk + defjkl + ghijkl = dgjfil + ehkfil + defghi. \tag{13.1}$$

This tells us, for example, that $d|(ehkfil - ghijkl)$, which means $d|hikl(ef-gj)$, which means $d|(ef-gj)$. This pattern holds for all of the nine possible divisors $\gamma \in \{d, e, f, g, h, i, j, k, l\}$; we always have that γ divides the difference (or the sum, according to (13.1)) of the product of the other two row elements and the product of the other two column elements. (I will call this the Sum-or-Difference Fact.) This gives us

$$d|(ef - gj), e|(hk - df), f|(il + de), g|(jd - ih), h|(gi - ke),$$
$$i|(gh + fl), j|(kl + dg), k|(jl + he), l|(fi - kj).$$

We are assuming that $\begin{pmatrix} a \\ b \\ c \end{pmatrix} \begin{matrix} < \\ > \\ < \end{matrix} \begin{pmatrix} p \\ q \\ r \end{pmatrix}$ holds, which means $\begin{pmatrix} dgj \\ ehk \\ fil \end{pmatrix} \begin{matrix} < \\ > \\ < \end{matrix} \begin{pmatrix} def \\ ghi \\ jkl \end{pmatrix}$.
This yields the nine inequalities

$$gj < ef, gi < ek, fi < jk, fl < gh, hi < dj, il < de, kl < dg, jl < eh, hk < df. \tag{13.2}$$

Note that earlier we deduced that $d|(ef - gj)$; the inequalities (13.2) tell us that $ef - gj$ is positive, and this means that $ef - gj = ds$, where s is a positive integer (s cannot be zero, for then $e = f = g = j = 1$ and $a = p$, which is a contradiction.) Similarly we have

$$et = df - hk, fu = de + il, gv = dg - hi, hw = ek - gi,$$
$$ix = gh + fl, jy = dg + kl, kz = eh + jl, l\alpha = jk - fi,$$

where d, e, f, g, h, i, j, k and l are all positive integers and pairwise coprime, and where s, t, u, v, w, x, y, z and α are all positive integers. Do these nine equations have a solution? If not (and work with Derive suggests any solution is far from straightforward) then the UC is true.

13.5 An alternative approach to the case of four prime powers

Theorem 13.1. *If n is the product of four distinct prime powers, and $abc = pqr = n$, where (a, b, c) and (p, q, r) are non-trivial HTs, then $(a, b, c) = (p, q, r)$.*

	a	b	c	
p	d	1	1	2
q	1	h	1	2
r	1	k	l	1
	2	1	2	

	a	b	c	
p	d	1	f	1
q	1	h	1	2
r	1	k	1	2
	2	1	2	

Figure 13.1: The four powers tables

Proof. Suppose $n = P_1P_2P_3P_4$ where P_i is a prime power. This means that Table 13.1 must contain the digit 1 five times. If any row or column contains three 1s, then one of a, b, c, p, q, r is 1, and so either (a, b, c) or (p, q, r) is a trivial HT, which is not permitted. So the number of 1s in the rows must be 2-2-1 in some order, and likewise for the columns. Now we have two cases:

1. the 1-row and the 1-column do not meet in a 1,

2. the 1-row and the 1-column meet in a 1.

For the first case, the 1s are arranged, for example, as in the case on the left of Figure 13.1, so two elements of (a, b, c) and (p, q, r) must be equal (in the example in Figure 13.1 we have $a = p$), and this again is not permitted. For the second case, four of the 1s will form a rectangle, as on the right of Figure 13.1, in which case, by the Sum-or-Difference Fact above, $\alpha|(\beta \pm 1)$, and $\beta|(\alpha \pm 1)$, where $\alpha, \beta \in \{d, e, f, g, h, i, j, k, l\}$. If $\alpha|(\beta - 1)$ and $\beta|(\alpha - 1)$ then the contradiction is clear. If $\alpha|(\beta + 1)$ and $\beta|(\alpha + 1)$, then $\alpha + 1 = k\beta$ and $\beta + 1 = j\alpha$, which gives $\beta = \frac{j+1}{jk-1}$, which gives $(j, k) = (2, 1), (3, 1), (2, 2)$ or (1, 2), and so α and β must both be small, which implies the elements of (a, b, c) and (p, q, r) are small, and we know the UC holds for small values. If $\alpha|(\beta + 1)$ and $\beta|(\alpha - 1)$, then $\alpha = \beta + 1$ (similarly for the other case). When can two prime powers differ by 1? Mihailescu's Theorem implies that the only possibilities here (for large values) are for α and β to be an odd prime and a power of 2 (in some order). But if we look at Figure 13.1 again, we see that the relationship between d and f is the same as that between h and k. We cannot have that one of d and f is a power of 2, and that one of h and k is a power of 2 also, and so the theorem is proved. □

13.6 Finding solutions to a necessary condition

A necessary but not sufficient condition for finding a counterexample to the UC is to find positive integers $p > a > b > q$ such that

$$ab(ab+1)(p+q) = pq(pq+1)(a+b). \tag{13.3}$$

Note that we are removing the conditions that $(a+b)|(ab+1)$ and $(p+q)|(pq+1)$ here. Solutions to (13.3) for small values of a, b, p and q are easily found with a computer search, and are given in Table 13.3. There are some very near misses here! Solutions are harder to find as p increases – could there be a finite number of solutions to (13.3)?

p	q	$\frac{pq+1}{p+q}$	a	b	$\frac{ab+1}{a+b}$
21	3	2.666...	8	6	3.5
143	13	11.923...	62	22	16.25
223	36	31	144	48	36.005...
368	46	40.89...	144	88	54.625
372	60	51.666...	221	85	61.39...
434	31	28.93...	93	91	46
481	39	36.07...	201	67	50.25...
555	140	111.8	160	158	129.5
690	12	11.79...	65	52	28.89...
780	12	11.819...	230	23	20.91...

Table 13.3: Small solutions to $ab(ab+1)(p+q) = pq(pq+1)(a+b)$

.

13.7 Another near miss

Suppose that $(2a, b, c)$ is an HT, so that

$$2ab+1 = (2a+b)c. \tag{13.4}$$

This yields $(2a+b)(2a-c) = (2a+1)(2a-1)$. Multiplying by a gives $(2a+b)(2a-c)a = (2a+1)(2a-1)a$. Now $(2a+1, 2a-1, a)$ is an HT – is

$(2a+b, 2a-c, a)$ ever an HT too? If so, we have a counter-example to the UC.

This requires that $\frac{(2a+b)(2a-c)+1}{2a+b+2a-c} = a$, which gives $\frac{4a^2-2ac+2ab-bc-1}{4a+b-c} = a$. But $-2ac+2ab-bc = 1$ by (13.4), and so $4a^2 = 4a^2 + a(b-c)$, which gives $a(b-c) = 0$, and thus $b = c$. The triplet $(2a+b, 2a-b, a)$ can only be an HT if b is 1, which means that $(2a+b, 2a-b, a)$ and $(2a+1, 2a-1, a)$ coincide, and we have no counter-example.

13.8 Special cases

We have proved the UC when n is the product of four prime powers. Can we deal with uniqueness in some further special cases? We have that

$$(n^2+n-1, n+1, n) \quad \text{and} \quad (n^3-n^2-2n+1, n^2-1, n^2-n-1)$$

are HTs for all natural numbers n. Solving

$$(n^2+n-1)(n+1)n - (m^2-1)(m^2-m-1)(m^3-m^2-2m+1) = 0$$

for n gives $n = \frac{\sqrt{(2\sqrt{(4m^7-8m^6-12m^5+24m^4+12m^3-20m^2-4m+5)}+3)}-1}{2}$. Is there a natural number m that gives a natural number n here?

In a similar vein, suppose that we have an HT of the form $\begin{pmatrix} (j+k)jn+2(a+b)j-1 \\ (j+k)kn+2(a+b)k+1 \\ jkn+2bk+1 \end{pmatrix}$, where $aj-bk = 1, 0 \leqslant a < k, 0 \leqslant b < j$. Given another HT $\begin{pmatrix} (h+i)hm+2(c+d)h-1 \\ (h+i)im+2(c+d)i+1 \\ him+2di+1 \end{pmatrix}$, where $ch-di = 1$, $0 \leqslant c < i, 0 \leqslant d < h$, we can equate the products of the elements in each case. Does the equation

$$((j+k)jn+2(a+b)j-1)((j+k)kn+2(a+b)k+1)(jkn+2bk+1) = ((h+i)hm+2(c+d)h-1)((h+i)im+2(c+d)i+1)(him+2di+1)$$

have solutions for appropriate $a, b, c, d, h, i, j, k, m, n$?

13.9 The Markov Triple uniqueness conjecture

Let us return to the recurrence (1.4), which we can write as

$$x, y, z, \frac{y^2 + z^2 + \alpha}{x}, \ldots \tag{13.5}$$

and which has the invariant $\frac{x^2+y^2+z^2+\alpha}{xyz} = k$. Putting $\alpha = 0$ and setting the first three terms equal to 1, the recurrence gives us the sequence of integers $1, 1, 1, 2, 5, 29, 433, 37666, \ldots$, while k is 3 and the invariant surface becomes $x^2 + y^2 + z^2 - 3xyz = 0$. What we have here is a subsequence of the Markov numbers; remember that a Markov Triple (or MT) is of the form (a, b, c) where $a^2 + b^2 + c^2 = 3abc$ (if a number appears in a MT, then it is called a Markov number). It is easy to show that if (a, b, c) is a MT then so is $(a, b, 3ab - c)$ (note that

$$T \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x \\ y \\ 3xy - z \end{pmatrix}.$$

is an involution). This fact is used to construct (see Figure 13.2) the infinite tree in Figure 13.3. Markov himself proved that every Markov number appears in this tree [45]. Despite much effort, the conjecture that no Markov number appears twice in the tree remains unproven.

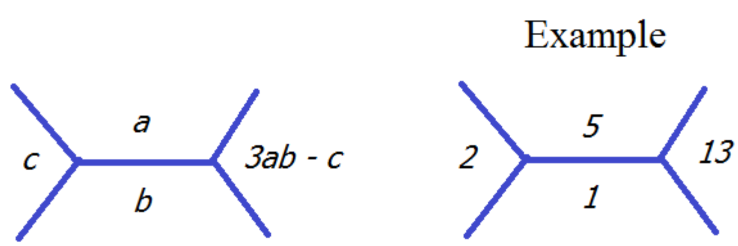


Figure 13.2: Constructing the Markov tree

The UC initially looks straightforward to prove, but the consensus of experienced observers is that if it holds, a proof may well be difficult. The status of the uniqueness conjecture for MTs reminds us that such problems can be extremely hard.

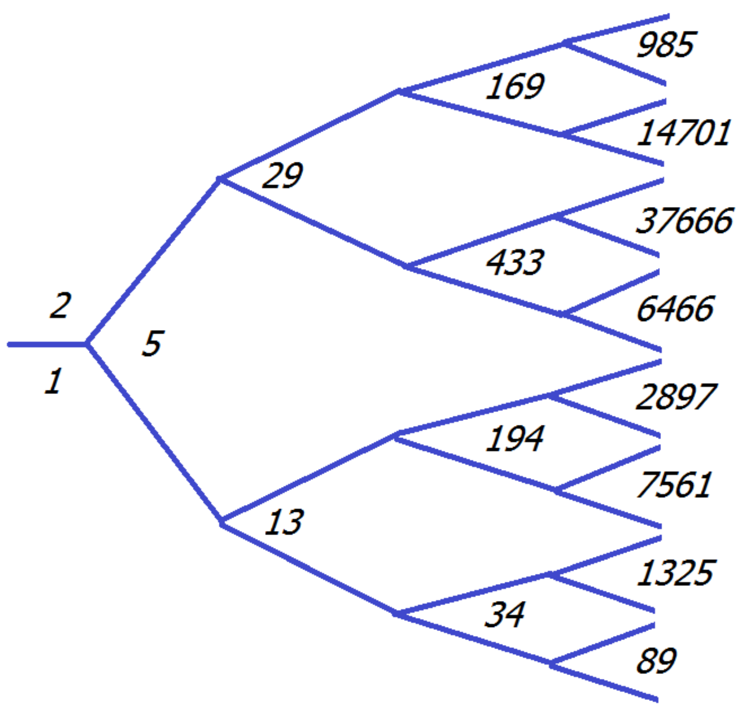


Figure 13.3: The start of the Markov number tree

Chapter 14

The Edwards Normal Form for an Elliptic Curve

This short and speculative chapter introduces a new development in elliptic curve theory, one that greatly aids cryptography calculations and security, that may link with our work on HTs.

14.1 Legendre Normal Form

Weierstrass short normal form is not the only standard form for an elliptic curve – Legendre normal form writes an elliptic curve as $y^2 = x(x-1)(x-\lambda)$, as long as the characteristic of the underlying field is not 2 or 3 ($\mathbb{R}, \mathbb{Q}$, and $\mathbb{C}$, of course, all have characteristic 0.) We can find the Legendre form for a curve to within six possibilities by transforming our initial curve (possibly via Weierstrass short normal form) to

$$y^2 = (x-a)(x-b)(x-c), a, b, c \in \mathbb{C}. \tag{14.1}$$

Choosing the first bracket to be X gives $y^2 = X(X-(b-a))(X-(c-a))$. Now choose $X' = \frac{X}{b-a}$, which yields $y^2 = X'(b-a)^2(X'-1)((b-a)X'-(c-a))$, and thus $Y^2 = X'(X'-1)\left(X' - \frac{c-a}{b-a}\right)$, where $Y = \frac{y}{(b-a)^{1.5}}$ (notice the appearance of RMC(a, b, c) here). Using this method, there are six possibilities over how we choose the brackets from (14.1), which mean that λ runs through the six possible values for the cross-ratio in the usual way. These six elliptic curves are isomorphic; the j-invariant for a curve in Legendre form is

$$\frac{(\lambda^2-\lambda+1)^3}{\lambda^2(1-\lambda)^2}$$

$$= \frac{1}{2}(\lambda^2+(1-\lambda)^2+\frac{1}{\lambda^2}+\frac{1}{(1-\lambda)^2}+\frac{(\lambda-1)^2}{\lambda^2}+\frac{\lambda^2}{(\lambda-1)^2}$$
$$+\lambda+(1-\lambda)+\frac{1}{\lambda}+\frac{1}{1-\lambda}+\frac{\lambda-1}{\lambda}+\frac{\lambda}{\lambda-1})$$

which remains constant if any of $\lambda, \frac{1}{\lambda}, 1-\lambda, \frac{1}{1-\lambda}, \frac{\lambda-1}{\lambda}, \frac{\lambda}{\lambda-1}$ are substituted for λ.

It is straightforward to convert $y^2 = x(x-1)(x-\lambda)$ to Weierstrass short normal form, giving

$$Y^2 = X^3 + X\frac{\lambda-\lambda^2-1}{3} + \frac{\lambda(\lambda+1)}{3}.$$

14.2 Edwards Normal Form and Legendre normal form

Another more recent normal form for elliptic curves is given by Edwards [24], who offers

$$x^2 + y^2 = a^2 + a^2x^2y^2. \tag{14.2}$$

as a helpful formulation. Figure 14.1 shows this curve in the cases $a = 0.9$ and 1.1.

What happens if we try to convert a curve in Edwards normal form into Legendre normal form? The result is simple and clean. Equation (14.2) yields

$$y^2(a^2x^2-1) = x^2 - a^2$$

which gives

$$y^2(a^2x^2-1)^2 = (a^2x^2-1)(x^2-a^2) = (ax-1)(ax+1)(x-a)(x+a).$$

Dividing now by $(x-a)^4$ gives

$$\left(\frac{y(x^2-a^2)}{(x-a)^2}\right)^2 = (a+(a^2-1)t)(a+(a^2+1)t)(1+2at)$$

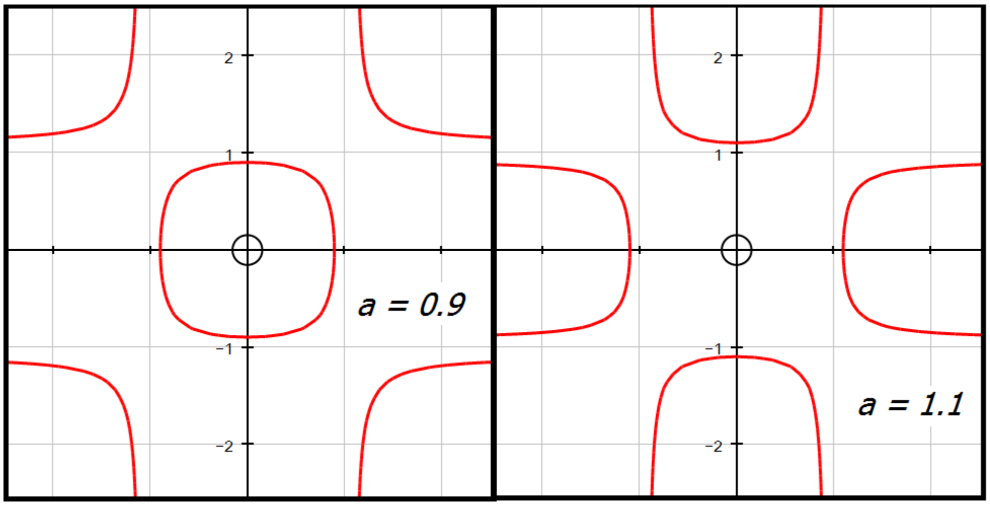


Figure 14.1: $x^2 + y^2 = a^2 + a^2x^2y^2$

where $t = \frac{1}{x-a}$. Proceeding now as for (14.1), we arrive at

$$Y^2 = X(X-1)\left(X + \frac{4a^2}{(a^2-1)^2}\right).$$

The six equivalent possibilities for λ here are clear. It is also straightforward to convert $y^2 = x(x-1)(x-\lambda)$ to Edwards normal form, giving

$$\frac{X^2Y^2+1}{X^2+Y^2} = \frac{\lambda - 2 \pm 2\sqrt{1-\lambda}}{\lambda}.$$

14.3 Edwards Normal Form and the addition formulae

Edwards suggests that his choice for normal form is revealing because the addition law for points on the elliptic curve becomes remarkably simple [27]. Suppose that (x, y) and (x', y') are on $x^2 + y^2 = a^2 + a^2x^2y^2$. If we now add these two points (where this could be understood as mapping to Legendre form and using chord and tangent methods before mapping back again), we arrive at (X, Y) where

$$X = \frac{xy' + x'y}{a(1 + xyx'y')}, Y = \frac{yy' - xx'}{a(1 - x'y'xy)}. \tag{14.3}$$

The identity element for an Edwards curve is $(0, a)$. The addition formulae for a curve in Weierstrass short normal form are given in (14.4) [27], and are far more cumbersome and much less symmetrical.

$$X = \frac{(y'-y)^2}{(x'-x)^2} - x - x', Y = (2x+x')\frac{y'-y}{x'-x} - \frac{(y'-y)^3}{(x'-x)^3} - y. \tag{14.4}$$

14.4 A link to HTs

The Edwards normal form relates to our previous work, in that (14.2) gives

$$\frac{x^2y^2+1}{x^2+y^2} = \frac{1}{a^2};$$

that is, if x^2, y^2 and $1/a^2$ are all integer values, where (x, y) is on the curve, then $(x^2, y^2, 1/a^2)$ is an HT. Is it possible for (x^2, y^2, z^2) to be an HT, where x, y and z are natural numbers? Excel shows the smallest example is $(3107^2, 339^2, 337^2)$, so the elliptic curve $337^2x^2 + 337^2y^2 = 1 + x^2y^2$ possesses the integer points $(\pm 3107, \pm 339)$.

The addition formulae have further resonances for us. The recurrences

$$x, y, -\frac{x+y}{kxy+1}, x, y \ldots, \tag{14.5}$$

and

$$x, y, \frac{x-y}{kxy-1}, -x, -y \ldots \tag{14.6}$$

are period-3 and period-6 respectively. If we put $x' = y' = -a$ into (14.3), (being aware that $(-a, -a)$ may not be on the curve) then the addition formulae become

$$X = -\frac{x+y}{a^2xy+1}, Y = \frac{x-y}{a^2xy-1}$$

The similarity to (14.5) and (14.6) is striking. (Note that addition formulae similar to these are given in [81], in the context of Jacobi elliptic functions. This text was written in 1927, so Edwards is here part of a tradition.)

Chapter 15

Hikorski Chains

As one plays with HTs, one notices that they sometimes overlap. For example, $(17, 7, 5)$ overlaps with $(7, 5, 3)$, which overlaps with $(5, 3, 2)$. A natural question is, how far can these overlaps be extended? We can define a *Hikorski Chain* (an HC) to be $[u_1, u_2, u_3, u_4, \ldots, u_n]$, a string of positive integers $u_1 > u_2 > u_3 > \ldots > u_n$ such that (u_1, u_2, u_3) is an HT, as is (u_2, u_3, u_4), as is $\ldots$ as is (u_{n-2}, u_{n-1}, u_n). The length of the chain is n.

15.1 The sequences A, B and the Fibonacci connection

To discover further terms in the sequence $(17, 7, 5, 3, 2)\ldots$, we can apply our recurrence relation, following the terms x, y, with $\frac{xy+1}{x+y}$. The next term in the sequence above would be $(3, 2, \frac{3\times2+1}{3+2})$ which is $(3, 2, \frac{7}{5})$. We can if we wish find preceding terms for the sequence, by adding $\frac{xy-1}{x-y}$ before the terms x and y; so preceding $(17, 9, 5)$ will be $(\frac{17\times7-1}{17-7}, 17, 7)$ which is $(\frac{59}{5}, 17, 7)$. We could view the numerators and the denominators of these terms as two sequences, A and B respectively, where (A_n) is $(\ldots 59, 17, 7, 5, 3, 2, 7, \ldots)$ and (B_n) is $(\ldots 5, 1, 1, 1, 1, 1, 5, \ldots.)$ Can we discover something about the structure of these sequences? This might help us to predict in particular any other occasions where B_n is 1, that is, when a member of the sequence is an integer. Some preliminary investigation suggests that we add to Table 15.1 showing A_n and B_n a row for $\frac{A_n+B_n}{2}$, and a row for $\frac{A_n-B_n}{2}$.

n	-8	-7	-6	-5	-4	-3	-2
A_n	-3691475	14753	-499	59	17	7	5
B_n	502829	1631	13	5	1	1	1
$\frac{A_n+B_n}{2}$	-1594323	8192	-243	32	9	4	5/2
$\frac{A_n-B_n}{2}$	-2097152	6561	-256	27	8	3	2
$\frac{A_n+B_n}{2}$	-3^{13}	2^{13}	-3^5	2^5	3^2	2^2	$5/2$
$\frac{A_n-B_n}{2}$	-2^{21}	3^8	-2^8	3^3	2^3	3^1	2^1

n	-1	0	1	2	3	4	5
A_n	3	2	7	19	109	1945	209953
B_n	1	1	5	17	107	1943	209951
$\frac{A_n+B_n}{2}$	2	3/2	6	18	108	1944	209952
$\frac{A_n-B_n}{2}$	1	1/2	1	1	1	1	1
$\frac{A_n+B_n}{2}$	2	$3/2$	3×2	$3^2 \times 2$	$3^3 \times 2^2$	$3^5 \times 2^3$	$3^8 \times 2^5$
$\frac{A_n-B_n}{2}$	1	$1/2$	1	1	1	1	1

Table 15.1: Fibonacci powers in A and B

The Fibonacci numbers appear as the powers of 2 and 3 here. What is happening becomes clearer if we consider a more general case, remembering that the Fibonacci sequence can also be run backwards;

$$\ldots \text{-8, 5, -3, 2, -1, 1, 0, 1, 1, 2, 3, 5, 8, } \ldots.$$

Instead of starting with terms x, y, let us begin instead with terms $\frac{p+j}{p-j}, \frac{q+k}{q-k}$. Notice that we can choose these to be any two fractions that we wish by picking p, q, j and k carefully. Suppose we wish to start with $\frac{a}{b}, \frac{c}{d}$, where $\gcd(a,b) = \gcd(c,d) = 1$. If a and b are both odd, then $p + j = a$ and $p - j = b$ will have integer solutions for p and j. If a and b are of opposite parity, then simply doubling top and bottom of the fraction gives $\frac{a}{b} = \frac{2a}{2b}$, and $p + j = 2a$ and $p - j = 2b$ will give (odd) integer values for p and j. A similar process follows for c and d. We can also note that $(p, j) = (q, k) = 1$.

So what happens if we apply our recurrence relation $\frac{xy+1}{x+y}$ repeatedly starting with $\frac{p+j}{p-j}, \frac{q+k}{q-k}$? We get the sequence

$$\frac{p+j}{p-j}, \frac{q+k}{q-k}, \frac{pq+jk}{pq-jk}, \frac{pq^2+jk^2}{pq^2-jk^2}, \frac{p^2q^3+j^2k^3}{p^2q^3-j^2k^3}, \frac{p^3q^5+j^3k^5}{p^3q^5-j^3k^5}, \ldots$$

And if we run this backwards?

$$\ldots \frac{p^5q^{-3}+j^5k^{-3}}{p^5q^{-3}+j^5k^{-3}}, \frac{p^{-3}q^2+j^{-3}k^2}{p^{-3}q^2-j^{-3}k^2}, \frac{p^2q^{-1}+j^2k^{-1}}{p^2q^{-1}-j^2k^{-1}}, \frac{p^{-1}q+j^{-1}k}{p^{-1}q-j^{-1}k}, \frac{p+j}{p-j}, \frac{q+k}{q-k}$$

It is an easy matter to prove by induction in either direction that the Fibonacci pattern here continues. If we return now to our original sequence, we can see that putting x and y equal to $\frac{3}{1}, \frac{2}{1}$, for example, then $p+j=3, p-j=1$, so $p=2, j=1$, and $q+k=4, q-k=2$ gives $q=3, k=1$. We can see now how this leads to the phenomenon observed in Table 15.1.

15.2 Exploring small HCs

Let us return to the topic of HCs and investigate further with an Excel spreadsheet. The one used to generate Table 15.2 constructs early HCs of length $\geqslant 4$ that start with the number in the left-hand column.

u_1	u_2	u_3	u_4	u_5
7	5	3	2	×
17	7	5	3	2
26	19	11	7	×
31	9	7	4	×
49	11	9	5	×
71	13	11	6	×
97	15	13	7	×
97	71	41	26	×
99	41	29	17	×
127	17	15	8	×
161	19	17	9	×
199	21	19	10	×
241	23	21	11	×

Table 15.2: Early HCs

An immediate thought is that $(17, 7, 5, 3, 2)$ is the anomaly rather than the rule. Run this program as far as $a = 30\ 000$ and it reveals no other HC with n greater than 4. This leads us to conjecture that with the exception of $(17, 7, 5, 3, 2)$, no HC contains more than four elements.

15.3 Basic HQs

An HC of four elements I shall call a *Hikorski Quartet*, or HQ. A great many HQs in the table above contain a central pair of odd numbers two apart. It is easy to see that $(2n^2 - 1, 2n + 1, 2n - 1, n)$ will always be an HQ – let us call HQs of this type *basic HQs*. Can the term before or the term after a basic HQ be an integer here, thus giving a quintet akin to $(17, 7, 5, 3, 2)$? The answer is 'No'.

Theorem 15.1. *A basic HQ cannot be extended in either direction to give an HC of length 5.*

Proof. Suppose $2n - 1$ and n are the first two terms of an HT. Then using the HT formula $\frac{xy+1}{x+y}$, we have $\frac{(2n-1)n+1}{2n-1+n} = \frac{2n^2-n+1}{3n-1}$ must be an integer. Now $\frac{2n^2-n+1}{3n-1} = \frac{2n}{3} - \frac{1}{9} + \frac{8}{9(3n-1)}$, which cannot be a positive integer, since $\frac{8}{9(3n-1)} < \frac{1}{9}$ for $n > 3$, and we have examined the cases for $n \leqslant 3$.

Suppose now that $2n^2 - 1$ and $2n + 1$ are the final two terms of an HT. Then using the reverse HT formula $\frac{xy-1}{x-y}$,

$$\frac{(2n^2-1)(2n+1)-1}{(2n^2-1)-(2n+1)} = \frac{2n^3+n^2-n-1}{n^2-n-1} = t,$$

where t is the first term of the HT. But then $t = 2n + 3 + \frac{4n+2}{n^2-n-1}$, which is clearly never an integer for $n \geqslant 6$. $\square$

Not all HQs are basic – removing the basic HQs from Table 15.2 gives Table 15.3. Are there any patterns here? Is the repeat of 1351 a coincidence? (There is additionally a Basic HQ $(1351, 53, 51, 26)$.) The answer again is 'No', since later in Table 15.3 we find the numbers given in Table 15.4.

u_1	u_2	u_3	u_4
26	19	11	7
97	71	41	26
99	41	29	17
244	71	55	31
362	265	153	97
485	109	89	49
577	239	169	99
846	155	131	71
1351	209	181	97
1351	989	571	362
1921	559	433	244
2024	271	239	127
2889	341	305	161

Table 15.3: Non-basic HQs

15.4 The Chebyshev polynomial connection and the Dirichlet kernel

Searching for 18817 and 19601 on the internet leads to the *Online Encyclopedia of Integer Sequences*[48]; both numbers appear in the number triangle associated with Chebyshev polynomials of the first kind, $T_n(x)$. The structure of this triangle is given in Table 15.5, and early values appear in Table 15.6.

Comparing Table 15.6 with columns 1 and 4 of Table 15.3, we see an astonishing overlap. Certainly the Chebyshev triangle $T(n,x) = T_n(x)$ must be intimately associated with our HQs. But how are these polynomials $T_n(x)$ defined? They may be found by writing $\cos(n\theta)$ as a polynomial in $\cos(\theta)$, and then replacing each $\cos(\theta)$ by x (in what follows in this chapter, θ is always $\arccos(x)$). We thus have $T_n(\cos\theta) = \cos(n\theta)$, or $T_n(x) = \cos(n(\arccos(x)))$. Notice that $T_{mn}(x) = T_m(T_n(x)) = T_n(T_m(x)) = \cos(mn\theta)$, and so $T_m(x)$ and $T_n(x)$ commute under composition. The first few of the polynomials $T_n(x)$ are given in Table 15.7.

u_1	u_2	u_3	u_4
18817	195	193	97
18817	2911	2521	1351
18817	13775	7953	5042
19601	199	197	99
19601	1189	1121	577
19601	8119	5741	3363

Table 15.4: HQs that repeat a first term

T(0,0)	T(0,1)	T(0,2)	T(0,3)	...
T(1,0)	T(1,1)	T(2,2)	...	...
T(2,0)	T(2,1)	...	...	...
T(3,0)	...	...	...	...
...	...	...	...	...

Table 15.5: $T(n,x)$ number triangle

They may also be defined by the recurrence relation

$$T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x), \quad \text{with} \quad T_0(x) = 1, T_1(x) = x.$$

The Chebyshev polynomials of the second kind $U_n(x)$ are generated by the same recurrence, but with different starting values (see Table 15.8).

$$U_{n+1}(x) = 2xU_n(x) - U_{n-1}(x), \quad \text{with} \quad U_0(x) = 1, U_1(x) = 2x.$$

There is a trigonometric link here too, since

$$U_n(\cos(\theta)) = \frac{\sin((n+1)\theta)}{\sin(\theta)}.$$

This is extremely close to the definition of the Dirichlet kernel, $D_n(x)$, used in Fourier analysis [32].

$$D_n(x) = \frac{\sin((2n+1)\frac{x}{2})}{\sin(\frac{x}{2})} = 1 + 2\sum_{k=1}^{n} \cos(kx).$$

$x \rightarrow$ / $n \downarrow$	0	1	2	3	4	5	6	7	8	9
0	1	1	1	1	1	1	1	1	1	1
1	0	1	2	3	4	5	6	7	8	9
2	-1	1	7	17	31	49	71	97	127	...
3	0	1	26	99	244	485	846	1351	...	
4	1	1	97	577	1921	4801	10081	...		
5	0	1	362	3363	15124	47525	...			
6	-1	1	1351	19601	119071	...				
7	0	1	5042	114243	...					
8	1	1	18817	...						
9	0	1	...							
10	-1	...								
...	...									

Table 15.6: Chebyshev triangle $T(n,x) = T_n(x)$ values

We will now for convenience write these functions as $T(n,x), U(n,x)$ and $D(n,x)$ rather than $T_n(x), U_n(x)$ and $D_n(x)$. Note that there is a possible confusion here with our use of x and θ. The functions $T(n,x)$ and $U(n,x)$ are polynomials in $\mathbb{Z}[x]$, while $D(n,x)$ is a polynomial in $\cos(x)$, which means $D(n, \arccos(x))$ is in $\mathbb{Z}[x]$ for all n (see Table 15.9). To go one step further, it is clear from the definition of $D(n,x)$ as a sum of cosines that $D(n,k\theta)$ is in $\mathbb{Z}[x]$ for all natural number n and k. The polynomials $T(n,x), U(n,x)$ and $D(n,k\theta)$ all play a part in this chapter. One final point; we can note that

$$U(n,x) + U(n-1,x) = \frac{\sin((n+1)\theta)}{\sin(\theta)} + \frac{\sin(n\theta)}{\sin(\theta)} = \frac{2\sin(\frac{(2n+1)\theta}{2})\cos(\frac{\theta}{2})}{2\sin(\frac{\theta}{2})\cos(\frac{\theta}{2})}$$

$$= D(n,\theta).$$

If we take, say, the thirteenth diagonal from the triangle in Table 15.6, we arrive at Table 15.10. Ignoring the more trivial numbers near the edge of the triangle, it appears in Table 15.10 that every $T(n, 13-n)$ is the starting number in an HQ. Moreover, most of these HQs end in $T(n-b, 13-n)$ for some b where $b|n$. Thus we have that if n is ab,

$$[T(ab, 13-ab), p(a,b), q(a,b), T((a-1)b, 13-ab)] \tag{15.1}$$

$T_0(x)$	1
$T_1(x)$	x
$T_2(x)$	$2x^2 - 1$
$T_3(x)$	$4x^3 - 3x$
$T_4(x)$	$8x^4 - 8x^2 + 1$
$T_5(x)$	$16x^5 - 20x^3 + 5x$
$T_6(x)$	$32x^6 - 48x^4 + 18x^2 - 1$
$T_7(x)$	$64x^7 - 112x^5 + 56x^3 - 7x$
$T_8(x)$	$128x^8 - 256x^6 + 160x^4 - 32x^2 + 1$
$T_9(x)$	$256x^9 - 576x^7 + 432x^5 - 120x^3 + 9x$

Table 15.7: Chebyshev polynomials of the first kind, $T(n, x)$

will always be an HQ for some numbers $p(a, b)$ and $q(a, b)$. In addition, $T(6, 7)$ starts two HQs that end in a non-standard way. These end numbers are also Chebyshev triangle numbers, and they start in turn three HQs that *do* end in the standard way, with $T(k, 13 - ab)$, as shown at the foot of Table 15.10.

15.5 A more general form for an HQ

So how do find $p(a, b)$ and $q(a, b)$ in (15.1)? By inspection these numbers do not occur in the Chebyshev triangle except in the trivial way as $T(1, n)$. Can we find a more general rule that applies beyond considering a particular diagonal? There are connections aplenty between the Chebyshev triangle numbers; some work on pattern-spotting reveals that

Theorem 15.2. *The chain of polynomials*

$$\left[T(ab, x), \frac{T(ab, x) - T((a-1)b, x)}{T(b, x) - 1}, \frac{T(ab, x) + T((a-1)b, x)}{T(b, x) + 1}, T((a-1)b, x)\right] \tag{15.2}$$

is an HQ for all $a, b \in \mathbb{N}^+$.

Proof. We have that

$$\frac{T(ab, x) - T((a-1)b, x)}{T(b, x) - 1} = \frac{\cos(ab\theta) - \cos((a-1)b\theta)}{\cos(b\theta) - 1}$$

$U_0(x)$	1
$U_1(x)$	$2x$
$U_2(x)$	$4x^2 - 1$
$U_3(x)$	$8x^3 - 4x$
$U_4(x)$	$16x^4 - 12x^2 + 1$
$U_5(x)$	$32x^5 - 32x^3 + 6x$
$U_6(x)$	$64x^6 - 80x^4 + 24x^2 - 1$
$U_7(x)$	$128x^7 - 192x^5 + 80x^3 - 8x$
$U_8(x)$	$256x^8 - 448x^6 + 240x^4 - 40x^2 + 1$
$U_9(x)$	$512x^9 - 1024x^7 + 672x^5 - 160x^3 + 10x$

Table 15.8: Chebyshev polynomials of the second kind $U(n, x)$

$D(0, \theta)$	1
$D(1, \theta)$	$2x + 1$
$D(2, \theta)$	$4x^2 + 2x - 1$
$D(3, \theta)$	$8x^3 + 4x^2 - 4x - 1$
$D(4, \theta)$	$16x^4 + 8x^3 - 12x^2 - 4x + 1$
$D(5, \theta)$	$32x^5 + 16x^4 - 32x^3 - 12x^2 + 6x + 1$
$D(6, \theta)$	$64x^6 + 32x^5 - 80x^4 - 32x^3 + 24x^2 + 6x - 1$
$D(7, \theta)$	$128x^7 + 64x^6 - 192x^5 - 80x^4 + 80x^3 + 24x^2 - 8x - 1$

Table 15.9: Dirichlet kernel polynomials $D(n, \theta)$

$$= \frac{-2\sin(\frac{b\theta}{2})\sin((ab - \frac{b}{2})\theta)}{-2\sin^2(\frac{b\theta}{2})}$$

$$= \frac{\sin(ab\theta - \frac{b\theta}{2})}{\sin(\frac{b\theta}{2})}.$$

We also have

$$\frac{T(ab, x) + T((a-1)b, x}{T(b, x) + 1)} = \frac{\cos(ab\theta) + \cos((ab - b)\theta)}{\cos(b\theta) + 1}$$

$$= \frac{2\cos(\frac{-b\theta}{2})\cos((ab - \frac{b}{2})\theta)}{2\cos^2(\frac{b\theta}{2})}$$

$$= \frac{\cos(ab\theta - \frac{b\theta}{2})}{\cos(\frac{b\theta}{2})}.$$

So the statement of the theorem becomes (where these can all be understood as polynomials in x) that

$$[\cos(ab\theta), \frac{\sin(ab\theta - \frac{b\theta}{2})}{\sin(\frac{b\theta}{2})}, \frac{\cos(ab\theta - \frac{b\theta}{2})}{\cos(\frac{b\theta}{2})}, \cos((a-1)b\theta)] \tag{15.3}$$

is an HQ for all $a, b, \in \mathbb{N}^+$. If we call these terms $[u_1, u_2, u_3, u_4]$, we need to show $u_3 = \frac{u_1 u_2 + 1}{u_1 + u_2}$. Now

$$\frac{\cos(ab\theta)\frac{\sin(ab\theta - \frac{b\theta}{2})}{\sin(\frac{b\theta}{2})} + 1}{\cos(ab\theta) + \frac{\sin(ab\theta - \frac{b\theta}{2})}{\sin(\frac{b\theta}{2})}}$$

$$= \frac{\cos(ab\theta)\sin(ab\theta)\cos(\frac{b\theta}{2}) - \cos^2(ab\theta)\sin(\frac{b\theta}{2}) + \sin(\frac{b\theta}{2})}{\sin(\frac{b\theta}{2})\cos(ab\theta) + sin(ab\theta)\cos(\frac{b\theta}{2}) - \cos(ab\theta)\sin(\frac{b\theta}{2})}$$

$$= \frac{\cos(ab\theta)\sin(ab\theta)\cos(\frac{b\theta}{2}) - \sin(\frac{b\theta}{2}) + \sin(\frac{b\theta}{2})\sin^2(ab\theta) + \sin(\frac{b\theta}{2})}{\sin(ab\theta)\cos(\frac{b\theta}{2})}$$

$$= \frac{\cos(ab\theta - \frac{b\theta}{2})}{\cos(\frac{b\theta}{2})}.$$

We also need to show $u_4 = \frac{u_2 u_3 + 1}{u_2 + u_3}$.

$$\frac{\frac{\sin((ab - \frac{b\theta}{2}))}{\sin(\frac{b\theta}{2})}\frac{\cos((ab - \frac{b\theta}{2}))}{\cos(\frac{b\theta}{2})} + 1}{\frac{\sin((ab - \frac{b\theta}{2}))}{\sin(\frac{b\theta}{2})} + \frac{\cos((ab - \frac{b\theta}{2}))}{\cos(\frac{b\theta}{2})}}$$

$$= \frac{\cos(ab\theta - \frac{b\theta}{2})\sin(ab\theta - \frac{b\theta}{2}) + \sin(\frac{b\theta}{2})\cos(\frac{b\theta}{2})}{\cos(\frac{b\theta}{2})\sin(ab\theta - \frac{b\theta}{2}) + \sin(\frac{b\theta}{2})\cos(ab\theta - \frac{b\theta}{2})}$$

$$= \frac{(\sin(ab\theta)\cos(\frac{b\theta}{2}) - \cos(ab\theta)\sin(\frac{b\theta}{2}))(\cos(ab\theta)\cos(\frac{b\theta}{2}) + \sin(ab\theta)\sin(\frac{b\theta}{2})) + \sin(\frac{b\theta}{2})\cos(\frac{b\theta}{2})}{\sin(ab\theta)}$$

$$= \frac{\sin(ab\theta)\cos(ab\theta)(\cos^2(\frac{b\theta}{2}) - \sin^2(\frac{b\theta}{2})) + \sin^2(ab\theta)\sin(\frac{b\theta}{2})\cos(\frac{b\theta}{2}) - \cos^2(ab\theta)\sin(\frac{b\theta}{2})\cos(\frac{b\theta}{2}) + \sin(\frac{b\theta}{2})\cos(\frac{b\theta}{2})}{\sin(ab\theta)}$$

$$= \frac{\sin(ab\theta)\cos(ab\theta)\cos(b\theta)+\sin^2(ab\theta)\sin(\frac{b\theta}{2})\cos(\frac{b\theta}{2})-(1-\sin^2(ab\theta))\sin(\frac{b\theta}{2})\cos(\frac{b\theta}{2})+\sin(\frac{b\theta}{2})\cos(\frac{b\theta}{2})}{\sin(ab\theta)}$$

$$= \cos(ab\theta)\cos(b\theta) + 2\sin(ab\theta)\cos(\frac{b\theta}{2})\sin(\frac{b\theta}{2})$$

$$= \cos(ab\theta)\cos(b\theta) + \sin(b\theta)\sin(ab\theta)$$

$$= \cos((a-1)b\theta).$$

□

Can (15.3) be simplified? We can certainly write

$$\frac{\sin(ab\theta - \frac{b\theta}{2})}{\sin(\frac{b\theta}{2})} = \frac{\sin((2(a-1)+1)\frac{b\theta}{2})}{\sin(\frac{b\theta}{2})},$$

which is $D(a-1, b\theta)$. We also have that

$$\frac{\cos(ab\theta - \frac{b\theta}{2})}{\cos(\frac{b\theta}{2})} = \frac{\sin(\frac{\pi}{2} - ab\theta + \frac{b\theta}{2})}{\sin(\frac{\pi}{2} - \frac{b\theta}{2})} = \frac{\sin(\pi(1-a) + (2a-1)\frac{\pi - b\theta}{2})}{\sin(\frac{\pi - b\theta}{2})}$$

$$= (-1)^{a-1}D(a-1, \pi - b\theta).$$

So we have that (15.3) can be written as

$$[T(ab,x), D(a-1,b\theta), (-1)^{a-1}D(a-1,\pi-b\theta), T((a-1)b,x)].$$

When b is 1, the HQ becomes

$$[T(a,x), D(a-1,\theta), (-1)^{a-1}D(a-1,\pi-\theta), T(a-1,x)]. \tag{15.4}$$

An alternative formulation of (15.4) is

$$[T(a,x), U(a-1,x)+U(a-2,x), -U(a-1,-x)-U(a-2,-x), T(a-1,x)].$$

For an example of another recurrence where the general term, at least for even index, involves $T(a,x)$ and $U(a,x)$, see Section 5 in [71].

15.6 HCs redefined

So if there are no Hikorski chains longer than four elements (except for one special case), it makes sense to redefine a Hikorski chain as an ordered list of positive integers $[u_1, u_2, u_3, \ldots u_n]$ so that (u_1, u_2, u_3) is an HT, as is (u_2, u_3, u_4), as is (u_4, u_5, u_6), as is (u_5, u_6, u_7), as is (u_7, u_8, u_9)... as is (u_{n-2}, u_{n-1}, u_n), that is, where (u_k, u_{k+1}, u_{k+2}) is an HT just if 3 does not divide k or k is not $n-1$ or n. Here is an example of an HC of length 28 (lengths can be as long as desired). Numbers in bold below do **not** begin HTs;

$$[3650401, 143207, \mathbf{137801}, 70226, 51409, \mathbf{29681}, 18817, 13775, \mathbf{7953}, 5042,$$

$$3691, \mathbf{2131}, 1351, 989, \mathbf{571}, 362, 265, \mathbf{153}, 97, 71, \mathbf{41}, 26, 19, \mathbf{11}, 7, 5, \ \mathbf{3,\ 2}].$$

This works with polynomials too; suppose we start with $T(9, x)$, which could lead to (taking b as 3);

$$[T(9, x), D(2, 3\theta), D(2, \pi - 3\theta), T(6, x), D(1, 3\theta), -D(1, \pi - 3\theta), T(3, x)],$$

that is

$$\begin{gathered}[256x^9 - 576x^7 + 432x^5 - 120x^3 + 9x, 64x^6 - 96x^4 + 8x^3 + 36x^2 - 6x - 1,\\ 64x^6 - 96x^4 - 8x^3 + 36x^2 + 6x - 1,\\ 32x^6 - 48x^4 + 18x^2 - 1, 8x^3 - 6x + 1, 8x^3 - 6x - 1, 4x^3 - 3x]. \qquad (15.5)\end{gathered}$$

We have here in effect a number of parametrisations in one variable for HTs; this links with the work in Chapter 9.

15.7 The missing recurrence

Consider again our quartet in Theorem 15.2. We know that the recurrence relation $\frac{xy+1}{x+y}$ takes the first two terms to the third and the second and third to the fourth (and the fourth and fifth to the sixth.) Is there a simple recurrence relation $f(x, y)$ that takes the third and fourth terms to the fifth, that is, so that

$$f\left(\frac{\cos(ab\theta - \frac{b\theta}{2})}{\cos(\frac{b\theta}{2})}, \cos((a-1)b\theta)\right) = \frac{\sin((a-1)b\theta - \frac{b\theta}{2})}{\sin(\frac{b\theta}{2})}?$$

Some experimentation suggests $\frac{xy-2y^2+1}{y-x}$ will work here (notice in $\frac{xy-2y^2+1}{y-x}$ the similarity to the recurrence in (4.2)).

Theorem 15.3. *If we begin with* $(x,y) = \left(T(ab,x), \frac{T(ab,x)-T((a-1)b,x)}{T(b,x)-1}\right)$*, applying* $\frac{xy+1}{x+y}$ *twice followed by* $\frac{xy-2y^2+1}{y-x}$ *once repeatedly produces an HC.*

Proof. We have proved what happens when we apply $\frac{xy+1}{x+y}$ twice; it remains to prove what happens in applying $\frac{xy-2y^2+1}{y-x}$ once. Returning to the formulation of our HQ in Theorem 15.2, we have

$$\frac{(\frac{\cos(ab\theta)+\cos((a-1)b\theta)}{\cos(b\theta)+1})(\cos((a-1)b\theta) - 2\cos^2((a-1)b\theta) + 1}{\cos((a-1)b\theta) - \frac{\cos(ab\theta)+\cos((a-1)b\theta)}{\cos(b\theta)+1}}$$

$$\frac{\cos(ab\theta)\cos((a-1)b\theta) - \cos^2((a-1)b\theta) - 2cos(b\theta)cos^2((a-1)b\theta) + 1 + \cos(b\theta)}{\cos(b\theta)cos((a-1)b\theta) - \cos(ab\theta)}$$

$$= \frac{\sin((a-2)b\theta) + \sin((a-1)b\theta)}{\sin(b\theta)}$$

$$= \frac{\sin((2a-3)\frac{b\theta}{2})}{\sin(\frac{b\theta}{2})}$$

$$= \frac{\sin((a-1)b\theta - \frac{b\theta}{2})}{\sin(\frac{b\theta}{2})}.$$

□

Sequences such as (15.5) can be reversed. Instead of repeatedly applying $\frac{xy+1}{x+y}$ twice and $\frac{xy-2y^2+1}{y-x}$ once, we can iterate applying $\frac{xy-1}{y-x}$ twice and $\frac{2y^2+xy-1}{x+y}$ once, which means the numbers in the HC increase in size. If we pick a polynomial $T(ab,x)$, and a second, $(-1)^a D(a, \pi - b\theta)$, as our starting inputs, then we are guaranteed to get a sequence of integer polynomials that increase in degree using this process.

u_1	u_1	u_2	u_3	u_4	u_4	b
T(11,2)	978122	716035	413403	262087	T(10,2)	1
T(10,3)	22619537	6727	6725	3363	T(5,3)	5
T(10,3)	22619537	1372105	1293633	665857	T(8,3)	2
T(10,3)	22619537	9369319	6625109	3880899	T(9,3)	1
T(9,4)	58106404	238631	237655	119071	T(6,4)	3
T(9,4)	58106404	16908641	13097377	7380481	T(8,4)	1
T(8,5)	46099201	9603	9601	4801	T(4,5)	4
T(8,5)	46099201	950599	931393	470449	T(6,5)	2
T(8,5)	46099201	10360559	8459361	4656965	T(7,5)	1
T(7,6)	17057046	3125123	2641211	1431431	T(6,6)	1
T(6,7)	3650401	2703	2701	1351	T(3,7)	3
T(6,7)	3650401	37829	37441	18817	T(4,7)	2
T(6,7)	3650401	564719	489061	262087	T(5,7)	1
T(6,7)	3650401	143207	137801	70226	T(9,2)	See below
T(6,7)	3650401	2672279	1542841	978122	T(11,2)	See below
T(5,8)	514088	68833	60705	32257	T(4,8)	1
T(4,9)	51841	323	321	161	T(2,9)	2
T(4,9)	51841	6119	5473	2889	T(3,9)	1
T(3,10)	3970	419	379	199	T(2,10)	1
T(2,11)	241	23	21	11	T(1,11)	1
T(9,2)	70226	2755	2651	1351	T(3,7)	3
T(9,2)	70226	51409	29681	18817	T(4,7)	2
T(11,2)	978122	716035	413403	262087	T(5,7)	1

Table 15.10: $T(n, 13-n)$

Appendix A

An HT Miscellany

Here is a chance to think more laterally about $\frac{xy+1}{x+y}$, $\frac{xy-1}{x-y}$ and related functions. Suppose we ask, 'To what question might $\frac{xy+1}{x+y}$ be the answer?' We can collect together replies to this and to similar queries, with the hope that some aspect of this work might unexpectedly benefit.

1. The Rectangle

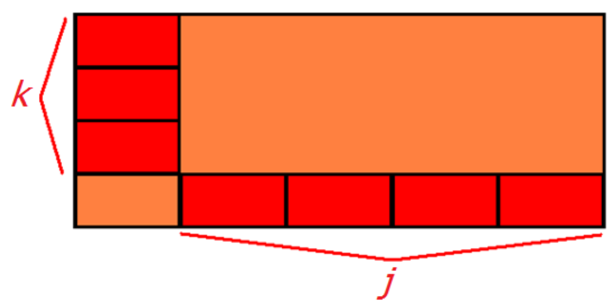


Figure A.1: The orange and red rectangle

The orange area in Figure A.1 divided by the red area is $\frac{jk+1}{j+k}$.

2. Relativity

If nothing can travel faster than the speed of light, how do we add speeds? For example, if someone is moving at three-quarters the speed of light down a train that is itself moving at three-quarters the speed of light, what is the person's resultant speed? If we say that the speed of light is 1, we can add parallel speeds relativistically as follows; define $\odot$ as

$$a \odot b = \frac{a+b}{1+ab}$$

and thus $\frac{3}{4} \odot \frac{3}{4} = \frac{24}{25}$. I assert the set of numbers in the interval $(-1, 1)$ in $\mathbb{R}$ together with the binary operation $\odot$ form a group. Do we have closure? Yes, since

$$\frac{a+b}{1+ab} \geqslant 1 \Rightarrow 0 \geqslant ab - a - b + 1 = (1-a)(1-b),$$

which is a contradiction, and similarly

$$\frac{a+b}{1+ab} \leqslant -1 \Rightarrow 0 \leqslant -(1+a)(1+b)$$

supplies a contradiction too. The identity is 0, and the inverse of a is $-a$. Associativity is easily checked [40]. So we have a group possessing the binary operation $\frac{a+b}{1+ab}$.

Can we find a group where the binary operation is $a \wedge b = \frac{ab+1}{a+b}$? We can, as follows; consider $S = \{\frac{x^a+1}{x^a-1} : a \in \mathbb{Z}^*\}$. If $a \wedge b = \frac{ab+1}{a+b}$, then

$$\frac{x^a+1}{x^a-1} \wedge \frac{x^b+1}{x^b-1} = \frac{x^{a+b}+1}{x^{a+b}-1},$$

and so we have closure, as long as we say the identity is $\frac{x^0+1}{x^0-1}$, which we append to the set S as the point at infinity, $\mathbb{O}$. The inverse of $\frac{x^a+1}{x^a-1}$ is $\frac{x^{-a}+1}{x^{-a}-1}$, and associativity is easily checked. The group $(S \cup \{\mathbb{O}\}, \wedge)$ is clearly isomorphic to the group $(\mathbb{Z}, +)$.

Are there any more pairs of groups with binary operations that are reciprocal?

3. The functions tanh and coth

We can simply note that [28]

$$\tanh(x+y) = \frac{\tanh(x)+\tanh(y)}{\tanh(x)\tanh(y)+1},$$

$$\coth(x+y) = \frac{\coth(x)\coth(y)+1}{\coth(x)+\coth(y)}.$$

4. A projective length

If Person A does a job in x hours, and Person B does the same job in y hours, how long does the job take if they work together? The answer is $\frac{xy}{x+y}$ hours, and this is represented by the length z in Figure A.2.

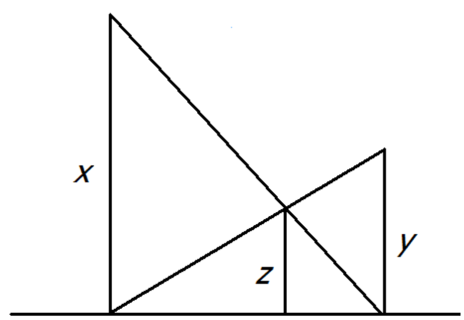


Figure A.2: Work-time diagram

As Figure A.3 shows, it is a simple matter to add $\frac{1}{x}$ to length y, and $\frac{1}{y}$ to length x to create the central length that is $\frac{xy+1}{x+y}$. This is always vertical, and is independent of the horizontal distance that separates x and y.

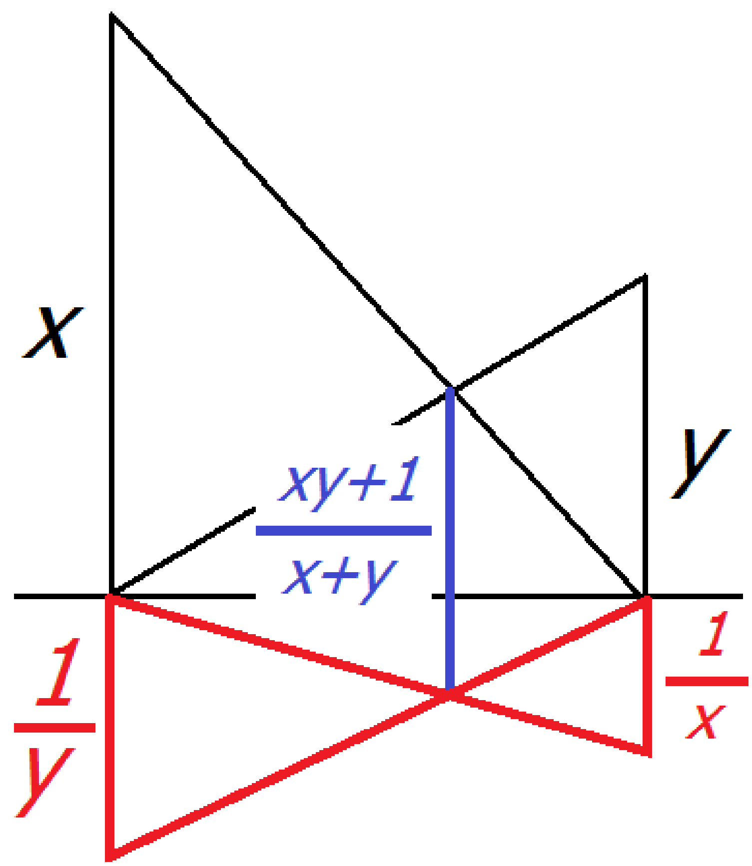


Figure A.3: Constructing $\frac{xy+1}{x+y}$

Appendix B

Software used

This is a thesis that has been heavily dependent on computing packages. I have used especially

Autograph (Douglas Butler); for producing graphs in two and three dimensions.

Derive (Texas Instruments); a computer algebra package that has been a real workhorse for this project.

Excel (Microsoft); especially the Visual Basic capability, for running programs to search, for example, for particular solutions to diophantine equations.

Magma (Computational Algebra Group at the University of Sydney); a professional algebra package, used here for checking genus and for finding the structure of an elliptic curve.

PARI (Henri Cohen and his co-workers at Université Bordeaux I, France); for swift number-theoretic calculations and programs, especially on elliptic curves.

Appendix C

Max Hikorski

In 1935, a group of predominantly French mathematicians decided to collaborate and publish together under the name 'Nicolas Bourbaki'. Over the years (the group still exists) they produced a vast body of work that proved to be influential in many areas of pure mathematics and mathematics education. Individuals from the group became well-known in their own right (Dieudonne, Weil, Grothendieck) but arguably the fictional mathematician Nicolas Bourbaki is more famous than any of them. Charles Bourbaki (1816 – 1897) was was a French general, about whom Wikipedia [56] says

> *[his name] was adopted by the group as a reference to a student anecdote about a hoax mathematical lecture, and also possibly to a statue. It was certainly a reference to Greek mathematics, Bourbaki being of Greek extraction. It is a valid reading to take the name as implying a transplantation of the tradition of Euclid to a France of the 1930s, with soured expectations.*

So the choice of name was careful, witty and allusive, qualities to which all mathematicians should aspire. I see naming as a primal skill for mankind – Adam in the garden of Eden practices naming very early, immediately after learning to listen and to garden. In our computer age, we get an extraordinary amount of practice at naming; every file we produce requires a name, and we reflect each time to find something clear and apposite that will swiftly recall for us the content when we return later.

One lunchtime in 2002, I first thought of this integer triple, $\left(x, y, \frac{xy+1}{x+y}\right)$. Its genesis was cathartic, in a way that I had never experienced in my mathematical life before. I was physically unable to teach the start of the lesson I was meant to be teaching next, because I was too distracted. I set some task to the group, and feverishly worked out the implications of my idea. Maybe I had a premonition that seven years later, I would begin work on these triples for a degree. Either way, my intuition said that they deserved a name.

Even I was not grandiose enough to reach for 'the Griffiths Triple' as a moniker. I needed some alter ego, someone like Nicolas Bourbaki. At the time, I was playing a role in the college production of 'They Shoot Horses, Don't They?', a musical about the dance marathons that were (and are) popular in the States, especially at the time of the Depression. I'd been asked to organise the music, so I recruited a small dance band, one that had to appear on stage for the entire show. The libretto named me as Max Hikorski, the band-leader, and I liked the sound of this. When I searched for 'Hikorski' on the Internet, there was only one; a Polish general, a fact that resonated with Charles Bourbaki's profession. 'Hikorski Triples' – the name was born.

Since then, my relationship to Max has matured. He was born in Poland on the same day as me, and he is also a mathematician (a better one than I am.) We both play the piano; he once played at a dance marathon in Ohio. His life mirrors mine; he is a me that I might have been, and a me that I might become. When I join a forum now, my user-name is Max Hikorski. My wish as I write is that I am not selling him short by borrowing his name for these triples – my fingers are crossed that they will one day win a small place in mathematics of which he would be proud.

Appendix D

Cycle Theorems

Lyness's cycles have received a great deal of attention since he first wrote to the *The Mathematical Gazette* in 1942, and it seems right to collect together here some of the related results that mathematicians have produced in recent years. In many cases here I have simplified statements of theorems, and couched them in the language of this thesis in order to unify. Theorems are given in chronological order.

D.1 Summary of Results

Theorem D.1 (Barbeau, Gelbord, Tanny (1995)[5]). *The recurrence* $x, y, \frac{y+c}{x}, \ldots$ *is period-p if and only if* $c = 0, p = 6$, *OR* $c = 1, p = 5$.

Theorem D.2 (Abu-Saris (2000)[1]). *If* $f(x) \in \mathbb{R}^+$ *for* $x \in \mathbb{R}^+$, *and* f *is continuous, then for all* $x, y \in \mathbb{R}^+$ *the recurrence* $x, y, \frac{f(y)}{x}, \ldots$ *is period-p if and only if*

$$\prod_{k=0}^{p-1} \frac{f(x_k)}{x_k^2} = 1 \quad AND \quad \left(\frac{x_0}{x_{-1}}\right)^p = \prod_{k=0}^{p-1} \left(\frac{f(x_k)}{x_k^2}\right)^k.$$

Theorem D.3 (Abu-Saris (2000)[1]). *If* $f(x) \in \mathbb{R}^+$ *for* $x \in \mathbb{R}^+$, *and* f *is continuous, then for all* $x, y \in \mathbb{R}^+$ *the recurrence* $x, y, \frac{f(y)}{x}, \ldots$ *is period-p then* $\frac{f(x)}{x^2}$ *is neither bounded above, nor bounded away from zero.*

Theorem D.4 (Csornyei, Laczkovich (2001)[21]). *Consider the recurrence*

$$x_n = \frac{a_0 + a_1 x_{n-1} \ldots + a_k x_{n-k}}{x_{n-k-1}}, a_1, \ldots, a_{k-1} \neq 0, a_k = 1.$$

If this is period-p, then one of the following is true:

1. $x_n = \frac{1}{x_{n-1}}, p = 2,$
2. $x_n = \frac{1+x_{n-1}}{x_{n-2}}, p = 5,$
3. $x_n = \frac{x_{n-1}}{x_{n-2}}, p = 6,$
4. $x_n = \frac{1+x_{n-1}+x_{n-2}}{x_{n-3}}, p = 8,$
5. $x_n = \frac{-1-x_{n-1}+x_{n-2}}{x_{n-3}}, p = 8.$

Theorem D.5 (Mestel (2003)[46]). *If $f(x) \in \mathbb{R}^+$ for $x \in \mathbb{R}^+$, and f is continuous, then for all $x, y \in \mathbb{R}^+$ the recurrence $x, y, \frac{f(y)}{x}, \ldots,$ is period-3 if and only if $f(x) = \frac{c}{x}$ for $c \in \mathbb{R}^+$.*

Theorem D.6 (Mestel (2003)[46]). *If $f(x) \in \mathbb{R}^+$ for $x \in \mathbb{R}^+$ then for all $x, y \in \mathbb{R}^+$ the recurrence $x, y, \frac{f(y)}{x}, \ldots,$ is period-4 if and only if*

$$f(x) = f\left(\frac{f(y)}{x}\right),$$

and if additionally f is continuous, then $f(x) = c$ for some $c \in \mathbb{R}^+$.

Theorem D.7 (Mestel (2003)[46]). *If $c, \alpha \in \mathbb{R}^+$, the recurrence*

$$x, y, \frac{c(c^\alpha + y^\alpha)^{1/\alpha}}{x}, \ldots,$$

is period-5.

For the next two theorems, consider the recurrence

$$x_{n+k} = \frac{a_0 + a_1 x_n + a_2 x_{n+1} \ldots + a_k x_{n+k-1}}{b_0 + b_1 x_n + b_2 x_{n+1} \ldots + b_k x_{n+k-1}},$$

where $a_i, b_i \geqslant 0, a_1 + b_1 > 0$, and where the initial conditions are positive, and where

$$\sum_{i=0}^{k} a_i > 0, \quad \text{and} \quad \sum_{i=0}^{k} b_i > 0.$$

Theorem D.8 (Cima, Gasull, Manosas (2004)[19]). *If the recurrence is order-2 or order-4, and period-p then it is equivalent to, or is a pseudo-cycle based on, either*

$$x, y, \frac{y+1}{x}, \ldots, p = 5,$$

or

$$x, y, \frac{y}{x}, \ldots, p = 6.$$

Theorem D.9 (Cima, Gasull, Manosas (2004)[19]). *If the recurrence is of odd order $k \leqslant 11$, and period-p, then it is equivalent to, or is a pseudo-cycle based on,*

$$x_{n+3} = \frac{1 + x_{n+1} + x_{n+2}}{x_n}, p = 8.$$

Theorem D.10 (Abu-Saris, Al-Jubouri (2004)[2]). *Define the function f as*

$$f(x) = \begin{cases} 1 & x \in \mathbb{Q} \\ 2 & x \in \mathbb{R}, x \notin \mathbb{Q} \end{cases}$$

Then the recurrence $x, y, \frac{f(y)}{x}, \ldots$ is period-4 for all $x, y \in \mathbb{R}$.

Theorem D.11 (Abu-Saris, Al-Jubouri (2004)[2]). *If $f(x), x, y \in \mathbb{R}^+$, the recurrence $x, y, \frac{f(y)}{x}, \ldots$ is period-5 if and only if $\frac{1}{x} f\left(\frac{f(x)}{y}\right) = \frac{1}{y} f\left(\frac{f(y)}{x}\right)$. So if $\frac{1}{x} f\left(\frac{f(x)}{y}\right)$ is symmetric in x and y, then $x, y, \frac{f(y)}{x}, \ldots$ is period-5.*

Theorem D.12 (Abu-Saris, Al-Jubouri (2004)[2]). *If $f(x), x, y \in \mathbb{R}^+$, and if $f(x) \neq \frac{c}{x}$ for some positive c, the recurrence $x, y, \frac{f(y)}{x}, \ldots$ is period-6 if and only if $f\left(\frac{1}{x} f\left(\frac{f(x)}{y}\right)\right) = \frac{1}{y^2} f(x) f\left(\frac{f(y)}{x}\right)$.*

Theorem D.13 (Berg, Stevic (2006)[9]). *Consider the recurrence*

$$x_n = \frac{1 + x_{n-1} + x_{n-2} \ldots + x_{n-k+1}}{x_{n-k}}.$$

This is period-p if and only if $k = 1, p = 2$, OR $k = 2, p = 5$, OR $k = 3, p = 8$.

For the next six theorems, f and g are continuous functions so that $f, g : \mathbb{R}^+ \mapsto \mathbb{R}^+$, and c is a positive constant, and the initial conditions are positive.

Theorem D.14 (Balibrea, Linero (2006)[4]). *Consider the recurrence* $x, y, f(y)g(x), \ldots$. *If this recurrence is period-3, then* $f(y)g(x) = \frac{c}{xy}$.

Theorem D.15 (Caro, Linero (2009)[18]). *Consider the recurrence* $x, y, f(y)g(x), \ldots$. *This recurrence is period-4 if and only if* $f(x) = c$, *and* $g(x)$ *is such that* $cg(cg(x)) = x$.

Theorem D.16 (Caro, Linero (2009)[18]). *If the recurrence* $x, y, f(y)g(x), \ldots$ *is period-*$p, p \geqslant 5$ *then* $g(x) = \frac{c}{x}$.

Theorem D.17 (Caro, Linero (2009)[18]). *The recurrence* $x, y, z, f(z)g(y)x, \ldots$ *is period-6 if and only if* $f(x) = \frac{1}{g(x)} = cx^2$.

Theorem D.18 (Caro, Linero (2009)[18]). *The recurrence* $x, y, z, \frac{f(y,z)}{x}, \ldots$ *is period-4 if and only if* $f(x, y) = \frac{c}{xy}$.

Theorem D.19 (Caro, Linero (2009)[18]). *The recurrence* $x, y, z, \frac{f(y,z)}{x}, \ldots$ *is never period-3 or period-5.*

Appendix E

Mathematicians Encountered

What follows is a list of the majority of mathematicians named in my text; every effort has been made to find full names, dates and nationalities for everyone, but sometimes this has been beyond me in the time available.

Abel, Niels, 1802-1829, Norway
Abu-saris, Raghib
Al-Jubouri, Neda'a
Apostol, Tom, 1923, Greece, USA
Barbeau, Ed, Canada
Bastien, Guy, France
Balibrea, Francisco, Spain
Beauville, Arnaud, 1947, France
Berg, Lothar, Germany
Berstel, Jean, France
Beukers, Frits, France
Bezivin, Jean-Paul, France
Bloch, Spencer, 1944, USA
Broughan, Kevin, 1946, New Zealand
Calkin, Neil, USA
Chebyshev, Pafnuty, 1821-1894, Russia
Cima, Anna, Spain
Coxeter, Harold, 1907-2003, England, Canada
Csornyei, Marianna, 1976, Hungary
Diophantus, 210-290 AD, Greece
Dirichlet, Peter, 1805-1859, Germany

Edwards, Harold, 1936, USA
Euler, Leonhard, 1707-1783, Switzerland
Everest, Graham, 1957-2010, England
Faltings, Gerd, 1954, Germany
Fibonacci, Leonardo, 1170-1250, Italy
Fomin, Sergey, Russia
Gasull, Armengol, Spain
Gelbord, Boaz, Israel
Hadamard, Jacques, 1865-1963, France
Hardy, Godfrey, 1877-1947, England
Hone, Andy, England
Ingham, Albert, 1900-1967, England
Kubota, Robert, USA
Kulenovic, Mustafa, Bosnia and Herzegovina, USA
Laczkovich, Miklos, Hungary
Ladas, Gerry, Greece, USA
Landen, John, 1719-1790, England
Laurent, Matthieu, 1841-1908, Luxembourg
Lech, Christer, Sweden
Legendre, Adrien-Marie, 1752-1833, France
Lewin, Leonard, USA
Linero, Antonio, Spain
Lutz, Elizabeth, 1914–2008, France
Lyness, Robert, 1909-1997, England
Mahler, Kurt, 1903-1988, Germany
Manosas, Francesc, Spain
Markov, Andrei, 1856-1922, Russia
Mazur, Barry, 1937, USA
Mestel, Ben
Mihailescu, Preda, 1955, Romania
Mobius, August, 1790-1868, Germany
Mordell, Louis, 1888-1972, United Kingdom, USA
Nagell, Trygve, 1895–1988, Norway
Pythagoras, 569-475 BC, Greece
Ramanujan, Srinivasa, 1887-1920, India
Reading, Nathan
Rogalski, Marc, France
Rogers, James, 1862-1933, England

Sawyer, Walter, 1911-2008, England
Schlickewei, Hans, Germany
Sharpe, David, England
Shioda, Tetsuji, Japan
Shparlinski, Igor, 1956, Russia
Siegel, Carl, 1896-1981, Germany
Silverman, Joseph, 1955, USA
Silvester, John, England
Skolem, Thoralf, 1887-1963, Norway
Sloane, Neil, 1939, United Kingdom, USA
Stevic, Stevo, Serbia
Somos, Michael, USA
Tanny, Steve, Canada
Tauber, Alfred, 1866-1942, Slovakia
de la Vallee Poussin, Charles-Jean, 1866-1962, Belgium
Weierstrass, Karl, 1815-1897, Germany
Van Der Poorten, Alf, 1942, Holland
Ward, Thomas, 1963, England
Weil, Andre, 1906–1998, France
Wigner, Eugene, 1905-1993, Hungary, USA
Wilf, Herbert 1931, USA
Wright, Edward, 1906-2005, England
Zagier, Don, 1951, Germany, USA

Bibliography

[1] R. Abu-Saris. Characterisation of Rational Periodic Sequences. *Journal of Difference Equations and Applications,* 6: 2, 233-242, 2000.

[2] R. Abu-Saris, N. Al-Jubouri. Characterisation of Rational Periodic Sequences II. *Journal of Difference Equations and Applications,* 10: 4,409-418, 2004.

[3] T. Apostol. *Introduction to Analytic Number Theory.* UTM, Springer, 1976.

[4] F. Balibrea, A. Linero. On global periodicty of $x_{n+2} = f(x_{n+1}, x_n)$. *Proceedings of the International Conference on Difference equations, Munich 2005,* World Scientific Publishing Company, Singapore, pages 41-50, 2007.

[5] E. Barbeau, B. Gelbord, S. Tanny. Periodicities of solutions of the generalized Lyness recursion. *Journal of Difference Equations and Applications,* 1, pages 291-306, 1995.

[6] G. Bastien, M. Rogalski. Global behavior of the solutions of the k-lacunary order 2k Lyness' difference equation, and of other more general equations. *Journal of Difference Equations and Applications,* Volume 13, Issue 1, pages 79 - 88 January 2007.

[7] E. Bavencoffe, J-P. Bezivin. Une famille remarqable de suites recurrentes lineaires. *Montash. Math.* 120, no 3-4, 189-203, 1995.

[8] A. Beauville. Finite Subgroups of $PGL_2(K)$. **arXiv:0909.3942v1,** 22 Sep 2009 (accessed August 2011)

[9] L. Berg, S. Stevic. Periodicity of some classes of holomorphic difference equations. *Journal of Difference Equations and Applications,* 12: 8, 827-835, 2006.

[10] F. Beukers. The multiplicity of binary recurrences. *Compositio Math.* 40 no 2, pp. 251-267, 1980.

[11] F. Beukers. The zero-multiplicity of ternary recurrences. *Compositio Math.* 77 no 2, pp. 165-177, 1991.

[12] F. Beukers, H.P. Schlickewei. The equation x + y = 1 in finitely generated groups. *Acta Arith.* 78 no 2 189-199, 1996.

[13] S. Bloch. Applications of the dilogarithm function on algebraic K-theory and algebraic geometry. *Proc. of the International Symp. pn Alg. Geometry* Kinokuniya, Tokyo, 1978.

[14] K. Broughan. Restricted Divisor Sums. *Acta Arithmetica* , 101.2, 2002.

[15] E. Brown. Three Fermat Trails to Elliptic Curves. *The College Mathematics Journal*, The Mathematical Association of America, Vol 31 No 3 May 2000.

[16] Y. Bugeaud, M. Mignotte, S. Siksek, M. Stoll, S. Tengley. Integral Points on Hyperelliptic Curves. **arXiv:0801.4459v4 [math.NT]** 16 Mar 2010 (accessed August 2011).

[17] N. Calkin, H. S. Wilf. Recounting the Rationals. *American Mathematical Monthly (Mathematical Association of America)*, 107 (4): 360–363, 2000.

[18] A. Caro, A. Linero. Existence and uniqueness of p-cycles of second and third order. *Journal of Difference Equations and Applications,* 15: 5, 489-500.

[19] A. Cima, A. Gasull, F. Manosas. On Periodic Rational difference Equations of Order k. *Journal of Difference Equations and Applications,* 10:6, 549-559, 2004.

[20] A. Cima, A. Gasull, F. Manosas. New periodic recurrences with applications. *Journal of Mathematical Anlaysis and Applications,* 382, pages 418-425, 2011.

[21] M. Csornyei, M. Laczkovich. Some Periodic and Non-periodic recursions. *Monatsh. Math.* 132, 215-236, 2001.

[22] P. Cull, M. Flahive, R. Robson. *Difference Equations; From Rabbits to Chaos.* UTM, Springer 2005.

[23] A. Dujella. **http://web.math.hr/ duje/tors/rankhist.html** (accessed August 2011).

[24] H.M. Edwards. A Normal Form for Elliptic Curves. *Bulletin of the American Mathematical Society* Volume 44, Number 3, pages 393-422, 2007.

[25] G. Everest, A. van der Poorten, I. Shparlinski, T. Ward. *Recurrence Sequences.* American Mathematical Society, 2003.

[26] G.R. Everest, T. Ward. *An Introduction to Number Theory.* GTM, Springer, page 97, 2007.

[27] The Explicit-Formulas Database. **http://hyperelliptic.org/EFD/index.html** (accessed August 2011).

[28] P. Fjelstad, G. Lasters, D. Sharpe. Relative Arithmetic. *Mathematical Spectrum* Volume 41, Number 3, 2008-9.

[29] S. Fomin and N. Reading. Root Systems and Generalised Associahedra, Lecture 1: Reflection and Roots. **arXiv:math.CO/0505518 V2,** 31 May 2005 (accessed August 2011).

[30] S. Fomin, A. Zelevinsky. The Laurent Phenomenon. **arXiv:math/0104241v1,** 2001 (accessed August 2011).

[31] D. Gale. The strange and surprising saga of the Somos sequences. *Mathematical Intelligencer*, 13 (1), pages 40-42, 1991.

[32] U. Gerlach. The Dirichlet kernel and Fourier analysis. **http://www.math.osu.edu/ gerlach/math/BVtypset/node21.html** (accessed August 2011).

[33] J. Griffiths. Periodic Recurrence Relations of the form y^k/x. *Mathematical Spectrum*, Volume 37 Number 2, 2004/5.

[34] G.H. Hardy, E.M. Wright, revised by D.R. Heath-Brown and J.H. Silverman. *An Introduction to the Theory of Numbers.* Sixth edition, Oxford, 2008.

[35] A.N.W. Hone. Diophantine non-integrability of a third-order recurrence with the Laurent property. *Journal of Physics Applications: Math. Gen.* 39, L171-177, 2006.

[36] A.E. Ingham. Some asymptotic formulae in the theory of numbers. *J. London Math. Soc.* (3) 2 pages 202-208, 1927.

[37] K.K. Kubota. On a conjecture of Morgan Ward. *Acta Arithmetica*, 33, Numbers 1 and 2, 1977.

[38] M. Kulenovic, G. Ladas. *Dynamics of Second Order Rational Difference Equations.* Chapman and Hall/CRC, 2002.

[39] G. Ladas. Invariants for Generalised Lyness Equations. Open Problems and Conjectures, *Journal of Difference Equations and Applications,* 1994.

[40] G. Lasters, D. Sharpe. From Squares to Circles by Courtesy of Einstein. *Mathematical Spectrum* Volume 38, Number 2, 2005-6.

[41] L. Lewin. Polylogarithms and associated functions. North Holland, New York, 1981.

[42] R.C. Lyness. *Mathematical Gazette*, 26, page 62, 1942.

[43] R.C. Lyness. *Mathematical Gazette*, 29, pages 231-233, 1945.

[44] R.C. Lyness. *Mathematical Gazette*, 45, pages 207-209, 1961.

[45] Markov, A. Sur les formes quadratiques binaires indéfinies. *Mathematische Annalen* (Springer Berlin / Heidelberg) 15: 381–406, 1879.

[46] B.D. Mestel. On globally periodic solutions of the difference equations $x_{n+1} = f(x_n)/x_{n-1}$. *Journal of Difference Equations and Applications,* 9(2), 201-209,2003.

[47] L.J. Mordell. On the rational solutions of the indeterminate equations of the fourth and third degrees. *Proc. Cambridge Phil Soc.* 21, 179-192, 1922.

[48] Online Encyclopedia of Integer Sequences. **http://oeis.org/** (accessed August 2011).

[49] PlanetMath. **http://planetmath.org/?op=getobj&from=objects&id=5871** (accessed August 2011).

[50] J. Pople. **http://nobelprize.org/nobel_prizes/chemistry/ laureates/1998/pople.html** (accessed August 2011).

[51] W. Sawyer. *Mathematical Gazette*, 45, page 207, 1961.

[52] T. Shioda. Weierstrass Transformations and Cubic Surfaces. **http://www.rkmath.rikkyo.ac.jp/math/shioda/papers/wtcs.pdf** (accessed August 2011).

[53] J. Silverman. *The Arithmetic of Elliptic Curves.* GTM, Springer, Second Edition 2009.

[54] J. Silvester. Cubics and Periodic Sequences. unpublished note, pre-2003.

[55] A. Weil. L'arithmetique sur les courbes algebriques. *Acta Math.* 52, pages 281-315, 1929.

[56] Wikipedia. Nicolas Bourbaki. **http://en.wikipedia.org/wiki/Nicolas_Bourbaki** (accessed August 2011).

[57] Wikipedia. Finite Coxeter Group Table. **http://en.wikipedia.org/wiki/Coxeter_groups** (accessed August 2011).

[58] Wikipedia. N. Abel's Dilogarithm Identity, quoted at **http://en.wikipedia.org/wiki/Polylogarithm** (accessed August 2011).

[59] S. Williams. Zeros in n^{th} order linear recurrence sequences. Master's Thesis, Macquarie University, 1994.

[60] Wolfram Mathworld. Rogers L-function. **http://mathworld.wolfram.com/RogersL-Function.html** (accessed August 2011).

[61] D. Zagier. The Dilogarithm Function. *Frontiers in Number Theory, Physics and Geometry II,* 3-65, Springer, Berlin, 2007.

[62] D. Zagier. quoted by Mariana Cook. *Mathematicians, an Outer View of the Inner World* Princeton, page 162, 2009.

A number of relevant texts and papers of which I was unaware when writing my thesis were recommended by my examiners after their reading of my work – references to these are given below.

[63] M. Abramowitz, I. Stegun. *Handbook of Mathematical Functions.* Dover Publications (1964).

[64] A. Baragar. On the Unicity Conjecture for Markoff Numbers. *Canad. Math. Bull.* Vol. 39 (1), 1996 pp. 3-9.

[65] J. Button. The Uniqueness of the Prime Markoff Numbers. *J. London Math. Soc.* (2) 58 (1998) pp. 9-17.

[66] A. Cima, A. Gasull, V. Manosa. Some properties of the k-dimensional Lyness map. *Journal of Physics Applications: Math. Theor.* 41 (2008) 285205.

[67] B. Keller. On cluster theory and quantum dilogarithm identities. **arXiv 1102.4148 v4** 2011. (accessed January 2012).

[68] J. Duistermaat. *QRT and Elliptic Surfaces.* Springer, 2010. (updated edition 2012).

[69] B. Grammaticos, A. Ramani, T. Tamizhmani. Investigating the integrability of the Lyness mappings. *Journal of Physics Applications: Math. Theor.* 42 (2009) 454009.

[70] A. Hone. Sigma function solution of the initial value problem for Somos 5 sequences. *Trans. A.M.S.* 359 (2007) 5019-5034.

[71] A. Hone. Non-linear recurrence sequences and Laurent polynomials. Number Theory and Polynomials. *LMS Proceedings and Lecture Notes* (ed C. Smyth and J. McKee) pp 188-210.

[72] S. Fomin, A. Zelevinsky. Cluster Algebras 1: Foundations. **arXiv:Math / 0104151 v1** 2001. (accessed January 2012).

[73] S. Fomin, A. Zelevinsky. Cluster Algebras 2: Finite Type Classification. **arXiv:Math / 0208229 v2** 2003. (accessed January 2012).

[74] A. Gasull, V. Manosa, X. Xarles. Rational periodic sequences for the Lyness recurrence. **arXiv:1004.5511v1** (accessed January 2012).

[75] R. Hirota, K. Kimura, H. Yahagi. How to find the conserved quantities of non-linear discrete equations. *Journal of Physics Applications: Math. Gen.* 34 (2001) 10377-10386.

[76] G.R.W. Quispel, J.A.G. Roberts, C.J. Thompson. Integrable Mappings and soliton equations. Phys. Lett. 126 (1988) 419-421.

[77] G.R.W. Quispel, J.A.G. Roberts, C.J. Thompson. Integrable Mappings and soliton equations II. Phys. D. 34 (1989) 183-192.

[78] M. Sierakowski. A generalisation of Zeeman's family. *Fundamenta Mathematicae* 162 (1999) 277-286.

[79] D. Tran, P. van der Kamp, G. Quispel. Sufficient number of integral for the pth order Lyness equation. *Journal of Physics Applications: Math. Theor.* 42 (2010) 302001.

[80] T. Tsuda. Integrable mappings via rational elliptic surfaces. *Journal of Physics Applications: Math. Gen.* 37 (2004) 2721-30.

[81] E. Whittaker, G. Watson. A Course of Modern Analysis. Cambridge University Press, 1996.

[82] E. Zeeman. A geometric unfolding of a difference equation. *Journal of Difference Equations and Applications* (to appear).

Various papers by by Alexander Veselov are also pertinent.