Prime Numbers

Paul Underwood

February 1, 2024

Contents

Chapter 1

Nomenclature

1.1 Numbers

The easiest numbers to understand are the counting numbers $1, 2, 3, \ldots$ which mathematicians refer to as the *natural numbers*. These may be split up into those that are divisible by a smaller number greater than 1, and those that are not. For instance, 4 can be written as 2×2 but 3 can *only* be written as a product involving itself and a *unit*, that is 1. Numbers that are indivisible are called *prime numbers*. Apart from the unit, the rest, the ones that can be written as a product of two smaller numbers are called *composite numbers*.

We can extend the natural numbers to include *negative* numbers and *zero* to form *integer numbers* or more succinctly the *integers*

$$\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$$

which have *unique factorisation*.

To cope with fractions of whole numbers we extend the integers. This new collection is called the *quotients*. The top, the *numerator*, is an integer and the bottom, the *denominator*, is a natural number.

Some numbers cannot be represented by quotients. Such numbers are called *irrational numbers*. For example the number which when multiplied by itself is 2, the *square root*, represented by $\sqrt{2}$. To see this, suppose $\sqrt{2} = \frac{a}{b}$. We now square both sides of the equality to get $2 = \frac{a^2}{b^2}$. Now multiply both sides by b^2 to get $2b^2 = a^2$. We now have a contradiction since the number of 2's is imbalanced because of the unique factorisation there must be an odd number of them that divide the left side of the equality and even number of them that divide the right. Our assumption that $\sqrt{2}$ could be written as a fraction of whole numbers was wrong.

Together with the rational numbers the irrational numbers make up the *real numbers* or more simply the *reals*. By considering the numbers so far introduced as distances from a point on a straight line which stretches infinitely in both directions and using a standard unit of measure we can plot the whole line.

To cope with numbers such as the one which when multiplied by itself is -1 we need to extend the reals. Let $i^2 = -1$ where i is the *imaginary unit*.

Complex numbers consist of a real term and an imaginary term. For example, $\sqrt{-4}$ is totally imaginary. It is represented by $0 + i2$ or $0 - i2$.

We can add and multiply complex numbers. For addition:

$$(a + ib) + (c + id) = (a + c) + i(b + d).$$

Remembering that $i^2 = -1$, multiplication is:

$$(a + ib)(c + id) = (ac - bd) + i(bc + ad).$$

Complex numbers can be represented by a point on a plane surface. We map the real component in one direction (say left to right) and the imaginary component in the other direction (down to up). Thus every point on the plane corresponds to one complex number and every complex number is represented by a point on the plane.

Other number systems can be created, so long as we give a definition of what they are and how they *operate*.

1.2 Sets

A *set* is a collection of things. This book is only concerned with sets of numbers and sets of matrices of numbers. Sets may be unordered and may not have repeating elements.

Throughout this text sets are represented by math capital letters or a list enclosed in braces. For example the set of all natural numbers can be represented as $\mathbb{N}$ or as $\{1, 2, 3, 4, 5, \ldots\}$.

An *element* is represented as belonging to a set with the symbol $\in$. To express that something does *not* belong we use $\notin$. For example $1 \in \mathbb{N}$ but $\frac{1}{2} \notin \mathbb{N}$.

A set may be constructed by removing *all* the elements of one set from another. This *set difference* is represented with the symbol $\setminus$.The set of all counting numbers except 2 and 3 may be represented by $\{1, 4, 5, 6, 7, 8, \ldots\}$ or $\mathbb{N} \setminus \{2, 3\}$.

To express that *all* elements of a set are to be considered we use the symbol $\forall$, which is read as *for all*. By way of example,to express that all counting numbers are equal to themselves we could write:

$$(\forall x \in \mathbb{N}) \;\; x = x.$$

To show the *existence of at least one* member we use the symbol $\exists$.We could state that there is at least one counting number equal to itself by:

$$(\exists x \in \mathbb{N}) \;\; x = x.$$

1.3 Groups

A *group* $\mathcal{G}$ is a set together with a *binary operation*, denoted with the $\circ$ symbol, which acts on any two (maybe identical) members of the set whose result is also a member of the set:

$$(\forall f, g \in \mathcal{G}) \;\; f \circ g \in \mathcal{G}.$$

A group is *associative*. That is:

$$(\forall f, g, h \in \mathcal{G}) \;\; f \circ (g \circ h) = (f \circ g) \circ h.$$

A group has an *identity* which when operated with a member of the set has no effect.

$$(\exists e \in \mathcal{G})(\forall g \in \mathcal{G}) \;\; e \circ g = g \circ e = g.$$

Also each element has an *inverse*:

$$(\forall g \in \mathcal{G})(\exists g^* \in \mathcal{G}) \;\; g \circ g^* = e.$$

Addition of counting numbers does *not* form a group because there is no identity element: $(\nexists 0 \in \mathbb{N}) \;\; g + 0 = g$.

Addition of whole numbers both positive and negative, the *integers* $\mathbb{Z}$, does form a group. To see this we need to check the conditions for a group:

- $\mathbb{Z}$ is a set.
- $+$ is a valid operator on the set.
- closure: $(\forall a, b \in \mathbb{Z}) \;\; a + b \in \mathbb{Z}$.
- associativity: $(\forall a, b, c \in \mathbb{Z}) \;\; a + (b + c) = (a + b) + c$.
- identity: $(\exists 0 \in \mathcal{G})(\forall a \in \mathbb{Z}) \;\; a + 0 = 0 + a = a$.
- inverse: $(\forall a \in \mathbb{Z})(\exists(-a) \in \mathcal{G}) \;\; a - a = 0$.

An *Abelian group* is one in which the operation *commutes*:

$$(\forall g, f \in \mathcal{G}) \;\; f \circ g = g \circ f.$$

1.4 Rings

A *ring* is a set together with *two* operators which act on any two (maybe identical) elements of the set. The operators are usually denoted by $+$ and $\times$. There are many kinds of rings. The rules that govern addition and multiplication vary between these rings.

Formally, a *commutative ring with identity* $\mathcal{S}$ is an abelian group both under addition and multiplication, and obeys the *distributive law*:

1. $\mathcal{S}$ is a set.
2. $+$ and $\times$ are a valid operators on the set.
3. additive closure : $(\forall a, b \in \mathcal{S}) \;\; a + b \in \mathcal{S}$.
4. additive associativity : $(\forall a, b, c \in \mathcal{S}) \;\; a + (b + c) = (a + b) + c$.

5. additive identity : $(\exists 0 \in \mathcal{S})(\forall a \in \mathcal{S})\ \ 0 + a = a + 0 = a.$

6. additive inverse : $(\forall a \in \mathcal{S})(\exists(-a) \in \mathcal{S})\ \ a - a = 0.$

7. additive commutativity : $(\forall a, b \in \mathcal{S})\ \ a + b = b + a.$

8. multiplicative closure : $(\forall a, b \in \mathcal{S})\ \ a \times b \in \mathcal{S}.$

9. multiplicative associativity : $(\forall a, b, c \in \mathcal{S})\ \ a \times (b \times c) = (a \times b) \times c.$

10. multiplicative identity : $(\exists 1 \in \mathcal{S})(\forall a \in \mathcal{S})\ \ 1 \times a = a \times 1 = a.$

11. multiplicative commutativity : $(\forall a, b \in \mathcal{S})\ \ a \times b = b \times a.$

12. distributive laws : $(\forall a, b, c \in \mathcal{S})\ \ a \times (b + c) = (a \times b) + (a \times c)$ and $(b + c) \times a = (b \times a) + (c \times a).$

If we relax condition 10 and 11 the ring is called just a *ring*. With just condition 10 dropped the ring is called a *commutative ring*. Apart from a ring with one element, the units of a commutative ring form an Abelian group called the *center*.

1.5 Fields

A *field* is a *commutative ring with identity* in which every non zero element has a multiplicative inverse. To our definition of a ring we need only add:

$$(\forall x \in \mathcal{S} \setminus \{0\})(\exists x^{-1})\ \ x \times x^{-1} = 1$$

where $1 \neq 0$.

1.6 Modular Arithmetic

Modular arithmetic is the arithmetic of remainders. It makes no difference whether we make a modular reduction prior to or after a calculation. Numbers are equivalent to one another if the remainders when divided by the *modulo* number are the same. For example, six is equivalent to one modulo five. This is expressed as:

$$6 \equiv 1 \pmod 5.$$

In fact all the numbers in the set $\{\ldots -9, -4, 1, 6, 11 \ldots\}$ are equivalent modulo five.

1.7 Matrices

An n by n square matrix is an arrangement into a grid of n^2 elements. It is easiest to start with 2 by 2 matrices. Let

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

Multiplication by a *scalar* v of the matrix A is equal to the matrix with each of its elements multiplied by v:

$$v \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} va & vb \\ vc & vd \end{pmatrix}.$$

Addition of two matrices is equal to the matrix which is formed by adding element wise:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}.$$

Multiplication is the result:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}.$$

The *determinant* of a matrix A is $|A| = ad - bc$ and the *trace* of a matrix is sum of the diagonal elements.

1.8 Symbols

$a :: b$	ratio of a to b.
$\gcd(a, b)$	greatest common divisor of a and b.
$a \wedge b$	greatest common divisor of a and b.
$a \mid b$	a divides into b exactly.
$a \equiv b \pmod{n}$	a and b have the same remainder when divided by n.
$\exists x$	existential quantification of x, *there exists* x.
$\forall x$	universal quantification of x, *for all* x.
$a \in \mathcal{S}$	a is a member of the set $\mathcal{S}$.
$\mathcal{S} \setminus \mathcal{T}$	set difference of $\mathcal{S}$ and $\mathcal{T}$.
$\mathbb{P}$	set of all prime natural numbers.
$\mathbb{N}$	set of all natural i.e. all positive whole numbers.
$\mathbb{Z}$	set of all integer i.e. both positive and negative whole numbers.
$\mathbb{Q}$	set of all rational i.e. a ratio of integer numbers over natural numbers.
$\mathbb{R}$	set of all real numbers needed to account for numbers such as $\sqrt{2}$.
$\mathbb{I}$	set of all imaginary numbers that are real numbers multiplied by i.
$\mathbb{C}$	set of all complex numbers which are pairs of real and imaginary numbers.
i	imaginary unit where $i^2 = -1$.
$A \otimes B$	multiplication of two matrices A and B.
I_n	n by n identity matrix.
$Tr(A)$	sum of the diagonal elements of the matrix A, the *trace*.
$\lvert A \rvert$	determinant of the matrix A.
$-a$	negative a.
$a + b$	a added to b.
$a - b$	a minus b.
$a.b$	a multiplied by b.
$a \times b$	a multiplied by b.
$\frac{a}{b}$	a divided by b.
a^{-1}	the reciprocal of a equivalent to $\frac{1}{a}$.
$a = b$	a equals b.
(a/b)	Legendre/Jacobi/Kronecker Symbol of a over b.
$J(a, b)$	Jacobi Symbol of a over b.
$< a, b >$	ordered pair of a and b.
$X \Rightarrow Y$	proposition X logically implies Y.
Σ	sum of.
$\prod$	product of.

Chapter 2

Euclid

2.1 Primes

A *prime* number is number which has two smaller factors. Any natural number that has proper factors is said to be *composite*. For example four is two times two and therefore is composite, but three has only itself and one as factors and so is prime. One is a special case and is called a *unit*.

A natural number greater than one can be *decomposed* into its constituent prime factors. Any one arrangement of those factors can be mapped to another arrangement. That is to say that any natural number can be decomposed into its prime factors *uniquely* apart from order. For example, six is two times three is three times two, but the only proper prime factors of six are two and three. That is not to say that we may have repeated prime factors.

$$n = p_1^{k_1} \times \ldots \times p_i^{k_i}.$$

Any sum (or difference) of numbers each divisible by a prime is also itself divisible by that prime. We factor out the prime from each number and use the distributive law to show that the prime divides the sum:

$$n = a.p + b.p + c.p = (a + b + c).p.$$

Euclid showed that there are infinitely many prime numbers. He argued that if we multiplied together all of the primes from a set of supposedly finite set of primes and add one then the resulting number would be impossible.

$$n = (p_0 \times p_1 \times p_2 \ldots \times p_{limit}) + 1.$$

We see that any prime p_k dividing n *must* be chosen from our known set of primes $\{p_0, p_1, p_2 \ldots p_{limit}\}$. Then since p_k also divides the product $p_0 \times p_1 \times p_2 \ldots \times p_{limit}$ it divides the difference namely 1. This is a contradiction to p_k being prime.

Also any prime dividing a product of numbers must divide at least one of them:

$$(p \mid n = a.b) \Rightarrow (p \mid a) \; and/or \; (p \mid b).$$

2.2 Euclid's Algorithm

Given two numbers, what is the largest number that would divide both of them:

$$\gcd(a, b) =?$$

We assume without loss of generality that a is greater than or equal to b:

$$a \geq b.$$

If a and b are equal then clearly the largest number dividing both of these is also equal:

$$(\forall a, b \in \mathbb{N}) \;\; (a = b) \Rightarrow (\gcd(a, b) = a).$$

On the other hand, if a is greater than b, a is equal to a maximal number q_{max} of $b\,s$ plus a remainder:

$$a = q_{max_0}.b + r_0. \tag{2.1}$$

Here we see that the *greatest common divisor* (gcd), also called *the highest common factor*, of a and b must also divide the remainder, r_0:

$$(\forall a, b \in \mathbb{N})(\exists x_{max}, r_0 \in \mathbb{N}) \;\; (x_{max} \mid a)(x_{max} \mid b) \Rightarrow (x_{max} \mid r_0).$$

If $r_0 = 0$ then gcd must divide both a and the b. The gcd is then b since b is assumed to be smaller than a and we can stop there.

Otherwise we can continue recursively. The gcd of a and b is also the gcd of b and the remainder r_0. We repeat the process with b and r_0:

$$b = q_{max_1}.r_0 + r_1.$$

Notice that problem is a reduced one: the pair of numbers b and r_0 are smaller than a and b since r_0 is less than b. Thus at some stage the process *must* come to an end:

$$\begin{aligned}
r_0 &= q_{max_2}.r_1 + r_2 \\
r_1 &= q_{max_3}.r_2 + r_3 \\
&\vdots \\
r_{i-4} &= q_{max_{i-2}}.r_{i-3} + r_{i-2} \\
r_{i-3} &= q_{max_{i-1}}.r_{i-2} + r_{i-1} \\
r_{i-2} &= q_{max_i}.r_{i-1} + r_i
\end{aligned}$$

The process comes to an end with $r_i = 0$ i.e.

$$r_{i-2} = q_{max_i}.r_{i-1}.$$

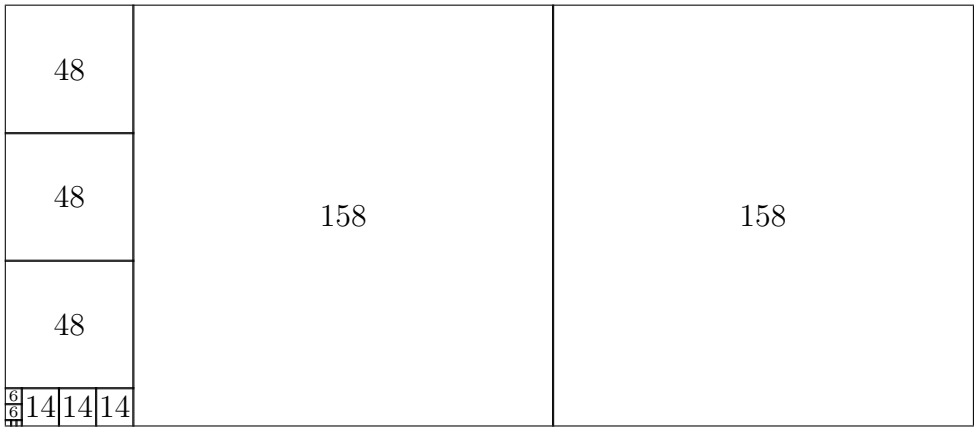

Figure 2.1: Geometric representation of Euclid's Algorithm for the ratio 158 :: 364

Therefore, working back up the algorithm we see that the gcd r_{i-1} is the gcd of r_{i-1} and r_{i-2}, and is the gcd of r_{i-2} and r_{i-3} and so on, and consequently is the gcd of a and b. Thus the gcd is the last non-zero remainder:

$$\gcd(a, b) = r_{i-1}.$$

For example, Euclid's algorithm to find the greatest common divisor for the pair of numbers 364, 158 is:

$$\begin{aligned} 364 &= 2 \times 158 + 48 \\ 158 &= 3 \times 48 + 14 \\ 48 &= 3 \times 14 + 6 \\ 14 &= 2 \times 6 + 2 \\ 6 &= 3 \times 2 + 0 \end{aligned}$$

The greatest common divisor is therefore 2 or written mathematically:

$$\gcd(364, 158) = 2.$$

2.3 Back Substitution

In the preceding section it was shown that the last non-zero remainder in Euclid's Algorithm is the greatest common divisor. We can write q_{max_i} as q_i, assuming we are taking the

maximum value:

$$\begin{aligned} a &= q_0.b + r_0 \\ b &= q_1.r_0 + r_1 \\ r_0 &= q_2.r_1 + r_2 \\ r_1 &= q_3.r_2 + r_3 \\ &\vdots \\ r_{i-4} &= q_{i-2}.r_{i-3} + r_{i-2} \\ r_{i-3} &= q_{i-1}.r_{i-2} + r_{i-1} \\ r_{i-2} &= q_i.r_{i-1} + 0 \end{aligned}$$

We now rewrite the above as:

$$\begin{aligned} r_0 &= a - b.q_0.b \\ r_1 &= b - q_1.r_0 \\ r_2 &= r_0 - q_2.r_1 \\ r_3 &= r_1 - q_3.r_2 \\ &\vdots \\ r_{i-3} &= r_{i-5} - q_{i-3}.r_{i-4} && (2.2) \\ r_{i-2} &= r_{i-4} - q_{i-2}.r_{i-3} && (2.3) \\ r_{i-1} &= r_{i-3} - q_{i-1}.r_{i-2} && (2.4) \\ 0 &= r_{i-2} - q_i.r_{i-1} && (2.5) \end{aligned}$$

We can substitute r_{i-2} in equation 2.3 into equation 2.4:

$$r_{i-1} = r_{i-3} - q_{i-1}(r_{i-4} - q_{i-2}.r_{i-3}).$$

Note that equation 2.3 is now written in terms of r_{i-3} and r_{i-4}. We can replace r_{i-3} with the right hand side of the equation 2.2. Repeating the processes we will end with:

$$r_{i-1} = Xa + Yb$$

for some X and Y.

For example given $a = 167$ and $b = 105$ what is:

$$a \wedge b = Xa + Yb?$$

Firstly use Euclid's Algorithm:

$$\begin{aligned} 167 &= 1 \times 105 + 62 \\ 105 &= 1 \times 62 + 43 \\ 62 &= 1 \times 43 + 19 \\ 43 &= 2 \times 19 + 5 \\ 19 &= 3 \times 5 + 4 \\ 5 &= 1 \times 4 + 1 \\ 4 &= 4 \times 1 + 0 \end{aligned} \tag{2.6}$$

Rearrange the above:

$$62 = 167 - 1 \times 105 \tag{2.7}$$
$$43 = 105 - 1 \times 62 \tag{2.8}$$
$$19 = 62 - 1 \times 43 \tag{2.9}$$
$$5 = 43 - 2 \times 19 \tag{2.10}$$
$$4 = 19 - 3 \times 5 \tag{2.11}$$
$$1 = 5 - 1 \times 4 \tag{2.12}$$
$$0 = 4 - 4 \times 1 \tag{2.13}$$

Substituting 4 from equation 2.11 into equation 2.12 we have:

$$1 = 5 - 1(19 - 3 \times 5)$$

rearranging terms:

$$1 = 4 \times 5 - 19$$

substituting 5 from equation 2.10 we have:

$$1 = 4(43 - 2 \times 19) - 19$$

rearranging terms:

$$1 = 4 \times 43 - 9 \times 19$$

substituting 19 from equation 2.9:

$$1 = 4 \times 43 - 9(62 - 1 \times 43)$$

rearranging terms:

$$1 = 13 \times 43 - 9 \times 62$$

substituting 43 from equation 2.8:

$$1 = 13(105 - 1 \times 62) - 9 \times 62$$

rearranging terms:

$$1 = 13 \times 105 - 22 \times 62$$

substituting 62 from equation 2.7:

$$1 = 13 \times 105 - 22(1 \times 167 - 105)$$

rearranging terms:

$$1 = 35 \times 105 - 22 \times 167$$

checking we see that indeed:

$$1 = 3675 - 3674$$

therefore $X = 35$ and $Y = -22$

2.4 Field Inverse

In the preceding sections we have shown how to compute

$$a \wedge b = aX + bY.$$

Now if b is prime and b does not divide a we have:

$$a \wedge b = 1$$

and since b divides bY we have:

$$1 \equiv aX \pmod{b}.$$

That is X is the inverse of a modulo prime b

To find X we compute Euclid's Algorithm for a and b, then use back substitution to find X.

In the previous section we showed that:

$$105 \wedge 167 = 35 \times 105 - 22 \times 167.$$

Given that 167 is prime and 167 does not divide 105, we see that:

$$1 \equiv 35 \times 105 \pmod{167}.$$

Dividing by 105 we have:

$$105^{-1} = 35 \pmod{167}.$$

Chapter 3

Pythagoras

A *right-angled triangle* is a triangle with one square corner. *Pythagoras's Theorem* states that for any right-angled triangle, the square of the side opposite the right angle equals the sum of the squares of the other two sides. We may express this as:

$$x^2 = y^2 + z^2.$$

There are infinitely infinite many differently *shaped* right angled triangles relative to some unit measure. If any two sides have common factors the third side must have that factor. Removal of common factors from the sides of a triangle represents a *scaling* down of it. In its most scaled down version a triangle will have sides *prime* to one another. We now restrict our view to all integer length Pythagorean triangles whose sides are mutually prime to one another. To distinguish such triangles we shall denote them by:

$$a^2 = b^2 + c^2. \tag{3.1}$$

The squares of the odd numbers are:

$$1, 9, 25, 49, \ldots$$

The remainders of these when divided by four are:

$$1, 1, 1, 1, \ldots$$

The quantity a must be *odd*. If it was *even* its square a^2 would be divisible by four and the other two sides, being relatively prime to a would have to be odd, but the sum of the squares of two odd numbers is never divisible by four:

$$1 + 1 \not\equiv 0 \pmod 4.$$

We now assume that one of the other two sides is even. Without loss of generality we assume that c is even. By rewriting the equation 3.1 as $c^2 = a^2 - b^2$ we can factorise the quantity on the right:

$$c^2 = (a + b)(a - b).$$

Since a and b are odd, both the quantities $a+b$ and $a-b$ are even. Any number dividing both $a+b$ and $a-b$ would divide both the sum and difference of the two expressions, that is $2a$ and $2b$, which is only 2 because $\gcd(a,b)=1$. Since $(a+b)(a-b)=c^2$ we may now write:

$$a+b = 2s^2 \tag{3.2}$$
$$a-b = 2t^2. \tag{3.3}$$

where $\gcd(s,t)=1$. This means *either* s or t is even, and because $a>b$ that $s>t$. Hence:

$$c^2 = 4(st)^2. \tag{3.4}$$

By summing and by taking the difference of the equations 3.2 and 3.3, and by taking positive square roots of 3.4 we see that the a, b and c can rewritten:

$$\begin{aligned} a &= s^2+t^2 \\ b &= s^2-t^2 \\ c &= 2st. \end{aligned}$$

By choosing relatively prime numbers s and t we can generate the infinite set of relatively prime sided right angled triangles.

For example, for $s=7$ and $t=4$ we have

$$\begin{aligned} a &= 7^2+4^2 \\ &= 49+16 \\ &= 65 \\ b &= 7^2-4^2 \\ &= 49-16 \\ &= 33 \\ c &= 2.7.4 \\ &= 56. \end{aligned}$$

This resulting 65, 33, 56 triangle satisfies:

$$65^2 = 33^2+56^2.$$

Checking we see that $4225 = 1089+3136$.

Chapter 4

Fibonacci Numbers

4.1 Classically

The Fibonacci numbers form an infinite sequence starting with one and one and followed by numbers which are equal to the sum of the two correspondingly preceding numbers in that sequence:

$$1, 1, 2, 3, 5 \ldots$$

We can represent these numbers mathematically with a pair of initial conditiond and a recurrence relation:

$$\begin{aligned} fib_1 &= 1 \\ fib_2 &= 1 \\ (\forall k)(k > 3) \quad fib_k &= fib_{k-1} + fib_{k-2}. \end{aligned} \tag{4.1}$$

4.2 Negatively

We notice that equation 4.1 can be be rewritten as:

$$(\forall k > 3) \quad fib_{k-2} = -fib_{k-1} + fib_k.$$

This gives us an expression for a Fibonacci number in terms of it's two successive numbers. Thus we may go negatively and by relaxing the condition for k from being greater than three to being any whole number, zero or negative number we may increase the Fibonacci numbers to:

$$\ldots -3, 2, -1, 1, 0, 1, 1, 2, 3, 5 \ldots$$

4.3 Alternative Definition

We can deduce the whole negatively extended Fibonacci sequence from *any* consecutive pair and the recurrence relationship. We can now define another sequence with different initial values:

$$\begin{aligned} g_0 &= 1 \\ g_1 &= 0 \\ (\forall k \in \mathbb{Z})\ g_k &= g_{k-1} + g_{k-2}. \end{aligned}$$

4.4 Addition

We may now add our alternative Fibonacci sequence in an interesting way:

k	$\ldots$	0	1	2	3	4	5	6	7	8	9	10$\ldots$	
g_k	$\ldots$	1	0	1	1	2	3	5	8	13	21	34$\ldots$	
g_{k+1}	$\ldots$	0	1	1	2	3	5	8	13	21	34	55$\ldots$	+
g_{k+2}	$\ldots$	1	1	2	3	5	8	13	21	34	55	89$\ldots$	=

(4.2)

4.5 Reversing

To evaluate a particular Fibonacci number we can start with an initial pair and make additions for the successive numbers in the sequence until we get to the one we require. We could also ask what is our required Fibonacci number in terms of its preceding Fibonacci number pair and for each of these what are they in terms of their preceding Fibonacci pairs and so on until we get back to a particular pair? We start with:

$$g_n = g_{n-1} + g_{n-2}.$$

From the recurrence relationship we can replace g_{n-1} with $g_{n-2} + g_{n-3}$:

$$\begin{aligned} g_n &= g_{n-2} + g_{n-3} + g_{n-2} \\ &= 2g_{n-2} + g_{n-3}. \end{aligned}$$

Using the recurrence relationship again, we replace g_{n-2} with $g_{n-3} + g_{n-4}$:

$$\begin{aligned} g_n &= 2g_{n-3} + 2g_{n-4} + g_{n-3} \\ &= 3g_{n-3} + 2g_{n-4}. \end{aligned}$$

We replace g_{n-3} with $g_{n-4} + g_{n-5}$:

$$\begin{aligned} g_n &= 3g_{n-4} + 3g_{n-5} + 2g_{n-4} \\ &= 5g_{n-3} + 3g_{n-4}. \end{aligned}$$

We may continue this process indefinitely. Note: the *coefficients* for each calculation of g_n are themselves a pair of Fibonacci numbers.

4.6 Multiplication

In the foregoing section we saw that a Fibonacci number can be expressed as:

$$(\forall n, i \in \mathbb{Z}) \;\; g_n = g_{i+1}g_{n-i} + g_{i+2}g_{n-i-1}.$$

A pair of Fibonacci numbers act as coefficients of an *inner product*. The pair of coefficients that map a pair to the first of that pair, the identity is the pair $1, 0$ since:

$$g_n = 1.g_n + 0.g_{n+1}.$$

The next pair $0, 1$ has the effect of calculating the second Fibonacci number in a given pair:

$$g_{n+1} = 0.g_n + 1.g_{n+1}.$$

The next pair $1, 1$ has the effect of calculating the Fibonacci number from its preceding pair:

$$g_{n+2} = 1.g_n + 1.g_{n+1}.$$

The next pair $1, 2$ has the effect of calculating the Fibonacci number that is two after the pair g_n and g_{n+1}:

$$g_{n+3} = 1.g_n + 2.g_{n+1}.$$

In general a pair of Fibonacci numbers act as coefficients with another pair to produce another Fibonacci. Given a initial pair we can find the one that occurs say k steps after the first if we know what the coefficient pair g_k, g_{k+1} are.

Conveniently we may use a set of matrices defined as:

$$M_i = \begin{pmatrix} g_i & g_{i+1} \\ g_{i+1} & g_{i+2} \end{pmatrix}$$

so that the identity is given by:

$$M_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

and the matrix M_1 is given by:

$$M_1 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

and the matrices have the following properties

$$\begin{aligned} M_i &= M_{i-1} \oplus M_{i-2} \\ M_{i+j} &= M_i \otimes M_j. \end{aligned}$$

For example, given that we know the Fibonacci pair g_5, g_6 is $3, 5$ we can easily calculate g_{11} as follows:

$$\begin{aligned}
M_5 &= \begin{pmatrix} 3 & 5 \\ 5 & 3+5 \end{pmatrix} \\
M_6 &= \begin{pmatrix} 5 & 8 \\ 8 & 5+8 \end{pmatrix} \\
M_{11} &= M_5 \otimes M_6 \\
&= \begin{pmatrix} 3 & 5 \\ 5 & 8 \end{pmatrix} \otimes \begin{pmatrix} 5 & 8 \\ 8 & 13 \end{pmatrix} \\
&= \begin{pmatrix} 3\times 5 + 5 \times 8 & 3 \times 8 + 5 \times 13 \\ 5 \times 5 + 8 \times 8 & 5 \times 8 + 8 \times 13 \end{pmatrix} \\
&= \begin{pmatrix} 15 + 40 & 24 + 65 \\ 25 + 64 & 40 + 104 \end{pmatrix} \\
&= \begin{pmatrix} 55 & 89 \\ 89 & 144 \end{pmatrix}.
\end{aligned}$$

Hence g_{11} is the top left entry of the matrix M_{11} which is 55.

4.7 Exponentiation

In order to show how we may calculate large Fibonacci numbers we shall proceed by way of an example. Suppose we wish to ascertain the value of g_{23}. Firstly, we convert the value of our number, 23, to binary:

$$23 = 1 \times 16 + 0 \times 8 + 1 \times 4 + 1 \times 2 + 1 \times 1 = 10111_2.$$

Next we calculate M_{23} by building up our binary string in the following way:

$$M_1 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

$$\begin{array}{rcccl}
M_{10} &=& M_{1+1} &=& M_1 \otimes M_1 \\
M_{100} &=& M_{10+10} &=& M_{10} \otimes M_{10}.
\end{array}$$

To get the value of M_{101} from M_{100} we can multiply by M_1, but in practice this is simply means adding the entries of the matrix:

$$M_{101} = \begin{pmatrix} g_{100} + g_{101} & g_{101} + g_{110} \\ g_{101} + g_{110} & g_{110} + g_{111}. \end{pmatrix}$$

Thus we may continue:

$$\begin{array}{rcccl}
M_{1010} &=& M_{101+101} &=& M_{101} \otimes M_{101} \\
M_{1011} &=& M_{1010+1} &=& M_{1010} \otimes M_1 \\
M_{10110} &=& M_{1011+1011} &=& M_{1011} \otimes M_{1011} \\
M_{10111} &=& M_{10110+1} &=& M_{10110} \otimes M_1.
\end{array}$$

We the simply extract the value of g_{10111} from the top–left corner of M_{10111}. The complete calculation is then:

$$
\begin{aligned}
M_{10} &= \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} &&= \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \\
M_{100} &= \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \otimes \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} &&= \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix} \\
M_{101} &= \begin{pmatrix} 3 & 5 \\ 5 & 3+5 \end{pmatrix} &&= \begin{pmatrix} 3 & 5 \\ 5 & 8 \end{pmatrix} \\
M_{1010} &= \begin{pmatrix} 3 & 5 \\ 5 & 8 \end{pmatrix} \otimes \begin{pmatrix} 3 & 5 \\ 5 & 8 \end{pmatrix} &&= \begin{pmatrix} 34 & 55 \\ 55 & 89 \end{pmatrix} \\
M_{1011} &= \begin{pmatrix} 55 & 89 \\ 89 & 55+89 \end{pmatrix} &&= \begin{pmatrix} 55 & 89 \\ 89 & 144 \end{pmatrix} \\
M_{10110} &= \begin{pmatrix} 55 & 89 \\ 89 & 144 \end{pmatrix} \otimes \begin{pmatrix} 55 & 89 \\ 89 & 144 \end{pmatrix} &&= \begin{pmatrix} 10946 & 17711 \\ 17711 & 28657 \end{pmatrix} \\
M_{10111} &= \begin{pmatrix} 17711 & 28657 \\ 28657 & 17711+28657 \end{pmatrix} &&= \begin{pmatrix} 17711 & 28657 \\ 28657 & 46368 \end{pmatrix}
\end{aligned}
$$

The required value of g_{23} is 17711 .

Chapter 5

Quadratic Equations

5.1 Quadratic Equations

The general form of a quadratic in x is:

$$y = ax^2 + bx + c.$$

This can be represented on a x, y graph by a curve whose locus is in exact correspondence with the equation. A quadratic's curve is called a *parabola*. The values of a, b and c are arbitrary constants. Thus an instance of the general form might be:

$$y = x^2 - 3x + 2. \tag{5.1}$$

For every given value of x there corresponds a value for y.

5.2 Quadratic Roots

Quite often we are interested in finding the *roots* of an equation. For the quadratic this means finding values of x for which the value of y is zero. Geometrically, this means when the parabola crosses or touches the *x–axis*, with the exception of quadratic equations whose roots are complex. The equation 5.1 has two roots at $x = 2$ and $x = 1$. In fact all quadratics have *two* (maybe equal) roots. The equation for a quadratic at its roots is:

$$0 = (x - \alpha)(x - \beta). \tag{5.2}$$

We can the relate the coefficients a, b and c in the general equation in terms of α and β:

$$\begin{aligned} \alpha &= \frac{-b + \sqrt{b^2 - 4ac}}{2a} \\ \beta &= \frac{-b - \sqrt{b^2 - 4ac}}{2a}. \end{aligned}$$

Equation 5.2 may be written as:

$$0 = x^2 - (\alpha + \beta)x + \alpha\beta. \tag{5.3}$$

Substituting the values of α and β we have:

$$\begin{aligned}
0 &= x^2 - (\frac{-b + \sqrt{b^2 - 4ac}}{2a} + \frac{-b - \sqrt{b^2 - 4ac}}{2a})x \\
&\quad +(\frac{-b + \sqrt{b^2 - 4ac}}{2a})(\frac{-b - \sqrt{b^2 - 4ac}}{2a}) \\
&= x^2 - (\frac{-2b}{2a})x + \frac{b^2 - (\sqrt{b^2 - 4ac})^2}{4a^2} \\
&= x^2 - (\frac{-b}{a})x + \frac{b^2 - (b^2 - 4ac)}{4a^2} \\
&= x^2 + (\frac{b}{a})x + \frac{4ac}{4a^2} \\
&= x^2 + (\frac{b}{a})x + \frac{c}{a}.
\end{aligned}$$

Multiplying through by a we have the general quadratic equation at its roots:

$$0 = ax^2 + bx + c.$$

5.3 Powers of Roots

In this section we shall only be concerned with one quadratic equation:

$$0 = x^2 - x - 1.$$

This may be rewritten as:

$$x^2 = x + 1.$$

Multiplying both sides of the equation by x^i we have:

$$x^i x^2 = x^i x + x^i 1.$$

This simplifies to:

$$x^{i+2} = x^{i+1} + x^i.$$

That is to say the n^{th} power of x is the sum of the two preceding powers of x. We can use this to calculate powers of x:

$$\begin{aligned}
x^3 &= x^2 + x^1 \\
&= x + 1 + x \\
&= 2x + 1.
\end{aligned}$$

Using this we can calculate:

$$\begin{aligned} x^4 &= x^3 + x^2 \\ &= 2x + 1 + x + 1 \\ &= 3x + 2. \end{aligned}$$

Using this we can calculate:

$$\begin{aligned} x^5 &= x^4 + x^3 \\ &= 3x + 2 + 2x + 1 \\ &= 5x + 3. \end{aligned}$$

We can continue this process indefinitely. Notice that the coefficients of x and x^0 are in a Fibonacci sequence. We now have a general expression for any power of x:

$$x^n = g_n x + g_{n-1}.$$

Where g_n is defined as as:

$$\begin{aligned} g_0 &= 1 \\ g_1 &= 0 \\ (\forall k \in \mathbb{Z}) \quad g_k &= g_{k-1} + g_{k-2}. \end{aligned}$$

5.4 Sums of Powers

We now define f as:

$$f_n = \alpha^n + \beta^n.$$

The sum of the powers raised to zero is the number of roots:

$$f_0 = \alpha^0 + \beta^0 = 2.$$

Recapping that:

$$y = x^2 - (\alpha + \beta)x + \alpha\beta$$

we see that:

$$\begin{aligned} \alpha + \beta &= 1 \\ \alpha\beta &= -1. \end{aligned}$$

Since they are roots, α and β satisfy this equation $x^2 - x - 1 = 0$:

$$\begin{aligned} \alpha^n &= g_{n+1}\alpha + g_n \\ \beta^n &= g_{n+1}\beta + g_n. \end{aligned}$$

From our definition of f_n we have:

$$\begin{aligned} f_n &= g_{n+1}(\alpha+\beta) + g_n + g_n \\ &= g_{n+1} + 2g_n \\ &= g_n + g_{n-1} + 2g_{n-1} + 2g_{n-2} \\ &= g_n + 2g_{n-1} + g_{n-1} + 2g_{n-2} \\ &= f_{n-1} + f_{n-2}. \end{aligned}$$

Thus f may be defined as:

$$\begin{aligned} f_0 &= 2 \\ f_1 &= 1 \\ (\forall k \in \mathcal{Z})\ f_k &= f_{k-1} + f_{k-2}. \end{aligned}$$

This is the same as the definition for g_n, except it has different initial conditions. The sequence is:

$$\ldots, 2, 1, 3, 4, 7, 11, 18 \ldots, f_n = f_{n-2} + f_{n-1}, \ldots$$

We are now in a position to rapidly calculate any f_n, the sums of the powers of the roots of the equation $y = x^2 - x - 1$, by using the methods of addition, multiplication and exponentiation introduced the previous chapter on Fibonacci Numbers and the matrix sequence M_n:

$$\begin{pmatrix} f_n \\ f_{n+1} \end{pmatrix} = M_n \otimes \begin{pmatrix} 2 \\ 1 \end{pmatrix}.$$

Remember that:

$$M_i = \begin{pmatrix} g_i & g_{i+1} \\ g_{i+1} & g_{i+2} \end{pmatrix}.$$

So that:

$$\begin{aligned} f_n &= 2g_n + g_{n+1} \\ &= g_n + g_n + g_{n+1} \\ &= g_n + g_{n+2}. \end{aligned}$$

That is f_n is equal to the sum of the diagonal elements of M_n, denoted as:

$$f_n = Tr(M_n).$$

Chapter 6

Pascal's Triangle

6.1 Pascal's Triangle

The *expansion* of the powers of the *binomial* $x+y$ may be obtained as follows. Let z equal the sum $x+y$. We are now studying the equation:

$$z^n = (x+y)^n = \overbrace{(x+y)(x+y)\ldots(x+y)}^{n}.$$

What we want to find is what is the equation when all the brackets have been removed. That is what is it when all the bracketed factors have been multiplied out. We note that:

$$\begin{aligned} z^0 &= 1 \\ z^1 &= x+y. \end{aligned}$$

We can equate the square of z with the *binomial expansion* of $x+y$, by twice using the distributive law of arithmetic:

$$\begin{aligned} z^2 &= (x+y)(x+y) \\ &= x(x+y)+y(x+y) \\ &= x^2+xy+yx+y^2. \end{aligned}$$

We know from the commutative law that $xy = yx$. Rearranging the terms we see that:

$$z^2 = x^2+2xy+y^2.$$

The third power can be calculated thus:

$$\begin{aligned} z^3 &= z^2.z^1 \\ &= (x^2+2xy+y^2)(x+y) \\ &= x^3+2xyx+y^2x+x^2y+2xyy+y^2y. \end{aligned}$$

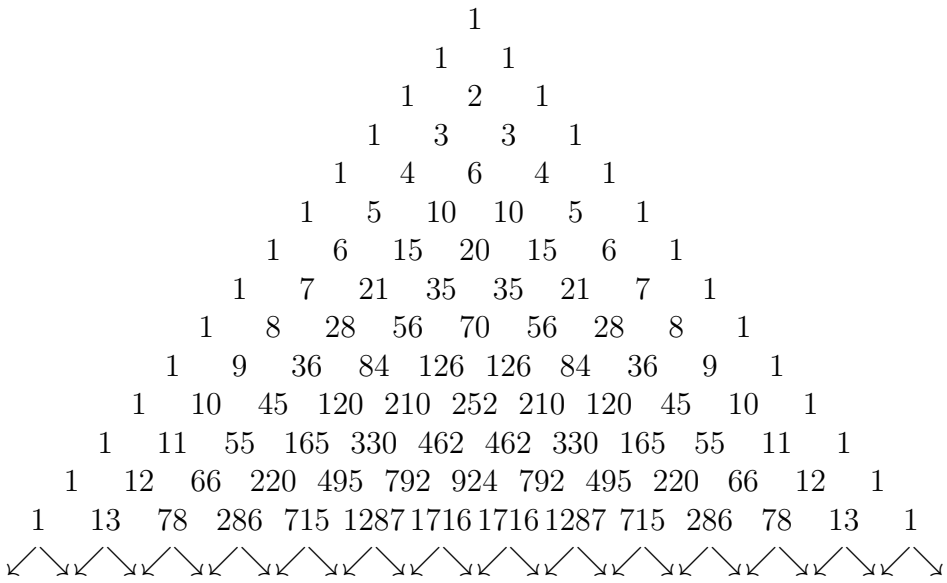

Figure 6.1: Pascal's Triangle for the first thirteen rows

Rearranging the last part of the equation string reveals that:

$$z^3 = x^3 + 3x^2y + 3xy^2 + y^3.$$

Any expansion can be easily calculated from the preceding expansion:

$$\begin{aligned} z^n &= z^{n-1}.z^1 \\ &= z^{n-1}(x+y). \end{aligned}$$

By looking only at the coefficients of the terms in x^iy^j where i and j are integers, we can form what is known as *Pascal's Triangle*, whose rows are the coefficients of x^iy^j and i and j are the diagonal coordinates of the coefficient.

6.2 Prime Rows

Ignoring the ones on the sides of the triangle, each row that corresponds to a prime number has coefficients that are divisible by the prime. The non-end coefficients in rows that correspond to composite numbers are not *all* divisible by that number. This is very difficult to prove. Could this provide a test of *primality*? We could check each coefficient to see if it divisible by the number we wish to test for primality. Since the triangle is *symmetric* about the middle coefficient for even numbers and the middle two for odd coefficients we could reduce are work load. Unfortunately it takes considerable computation to generate the coefficients and we would have to check about as many them as half the number we wish to test for primality.

Chapter 7

Mersenne Numbers

To test a number for primality by *trial division*, that is by checking *all possible* divisors is time-consuming. We check the remainders are not zero, starting with two and proceeding up to the square root of the number to be tested. In the seventeenth century *Father Marin Mersenne* claimed to have checked all the numbers m_n which are of the form:

$$M_n = 2^n - 1$$

for values of n up to 257. He did make a few errors, but it is interesting to note that in order to test $2^{61} - 1$ by *trial division* would have required an enormous amount of computation since he would have had to check the remainders of about a trillion divisions!

The exponent n itself must be prime since otherwise if it equalled a composite say pq the the Mersenne Number could be factorised:

$$M_{pq} = 2^{pq} - 1 = (2^p - 1)(2^{p(q-1)} + 2^{p(q-2)} + \ldots + 2^p + 1).$$

GIMPS stands for *Great Internet Mersenne Prime Search*. This is a systematic distributed search using thousands of computers around the world, over *The Internet*.

$n : m_n \in \mathbb{P}$	m_n	date	who
2	3	unknown	unknown
3	7	unknown	unknown
5	31	unknown	unknown
7	127	unknown	unknown
13	8191	unknown	unknown
17	131071	1588	Cataldi
19	524287	1588	Cataldi
31		1772	Euler
61		1883	Pervushin
89		1911	Powers
107		1914	Powers
127		1876	Lucas
521		1952	Raphael Robinson – SWAC

Figure 7.1: The first thirteen Mersenne Primes

n	date	who	computer
607	1952	Raphael Robinson	SWAC
1279	1952	Raphael Robinson	SWAC
2203	1952	Raphael Robinson	SWAC
2281	1952	Raphael Robinson	SWAC
3217	1957	Hans Riesel	BESK
4253	1961	Alexander Hurwitz	IBM 7090
4423	1961	Alexander Hurwitz	IBM 7090
9689	1963	Donald Gillies	ILLIAC-II
9941	1963	Donald Gillies	ILLIAC-II
11213	1963	Donald Gillies	ILLIAC-II
19937	1971	Bryant Tuckerman	IBM 360-91
21701	1978	Laura Nickel and Curt Noll	CYBER 174
23209	1979	Curt Noll	CYBER 174

Figure 7.2: The second thirteen Mersenne Primes

n	date	who	computer
44497	1979	David Slowinski	CRAY-1
86243	1982	David Slowinski	CRAY-1
110503	1988	Colquitt&Welsh	
132049	1983	David Slowinski	CRAY-XMP
216091	1985	David Slowinski	CRAY-XMP
756839	1992	Slowinski&Gage	CRAY-2
859433	1994	Slowinski&Gage	
1257787	1996	Slowinski&Gage	CRAY T94
1398269	1996	GIMPS, Armengaud	
2976221	1997	GIMPS, Spence	
3021377	1998	GIMPS, Clarkson	
6972593	1999	GIMPS, Hajratwala	
13466917	2001	GIMPS, Cameron	

Figure 7.3: The third thirteen Mersenne Primes

n	date	who
20996011	2003	GIMPS, Shafer
24036583	2004	GIMPS, Findley
25964951	2005	GIMPS, Nowak
30402457	2005	GIMPS, Cooper,Boone
32582657	2006	GIMPS, Cooper,Boone
37156667	2008	GIMPS, Elvenich
42643801	2009	GIMPS, Strindmo
43112609	2008	GIMPS, Smith
57885161	2013	GIMPS, Cooper
74207281	2016	GIMPS, Cooper
77232917	2017	GIMPS, Pace
82589933	2018	GIMPS, Laroche

Figure 7.4: The final twelve known Mersenne Primes

Chapter 8

Pierre de Fermat

8.1 Fermat's Little Theorem

Here we wish to show that any number multiplied by itself a prime number of times has a remainder equal to the number when divided out by the prime number:

$$a^p \equiv a \pmod{p}.$$

In order to show this we use *pure mathematical induction* with the *basis* of $a = 0$. Clearly:

$$0^p \equiv 0 \pmod{p}.$$

Next assume that what we wish to show is true up to a value of k:

$$k^p \equiv k \pmod{p}. \tag{8.1}$$

We then perform the *induction step* on k:

$$(k+1)^p = k^p + \left(\begin{array}{c} p \\ 1 \end{array} \right) k^{p-1} + \left(\begin{array}{c} p \\ 2 \end{array} \right) k^{p-2} + \ldots + \left(\begin{array}{c} p \\ p-1. \end{array} \right) k^1 + k^0.$$

Each of the binomial coefficients are divisible by p since by definition they are:

$$\left(\begin{array}{c} p \\ i \end{array} \right) = \frac{p(p-1)(p-2)\ldots 2.1}{(i(i-1)(i-2)\ldots 2.1)((p-i)(p-i-1)(p-i-2)\ldots 2.1)}.$$

The *numerator* is clearly divisible by p and the *denominator* is not because p is prime and the denominators factors are all less than p. Hence:

$$(k+1)^p \equiv k^p + 1 \pmod{p}.$$

Using the *induction hypothesis*, given by equation 8.1,shows us that:

$$(k+1)^p \equiv k + 1 \pmod{p}.$$

Thus we have shown that what we wish to prove is true for *all* values of k. Notice this is a statement about prime exponents. For composite numbers we cannot complete the proof because we cannot make the same statement about the binomial coefficient denominator. For some values of a with composite n the statement $a^n \equiv a \pmod{n}$ may be true but for other values of a it is *not*.

8.2 Probable Prime

If we choose at random a number less than the one we want to test, is it likely to be equal to itself when multiplied by itself a number of times equal to the number we wish to test?:

$$(test\, n \in \mathbb{N})(a \in \mathbb{Z}_n) \;\; a^n \equiv a \pmod{n}?$$

If the number we wish to test is prime then Fermat s Little Theorem shows us that all such randomly chosen numbers will have the property:

$$(\forall p \in \mathbb{P})(\forall a \in \mathbb{Z}_p) \;\; a^p \equiv a \pmod{p}.$$

If on the other hand the number we wish to test is composite what is the chance of it having the property? To improve our chances, we can repeat the test with other random a.

8.3 Fermat Numbers

The definition for the n^{th} *Fermat Number* is given by

$$F_n = 2^{2^n} + 1. \tag{8.2}$$

Pierre de Fermat claimed that F_4 was prime. To test it by *trial division* would require some 256 long division calculations. Even with the probabilistic approach we can never be *absolutely sure* until we have performed the test on a very large number of times in deed. So how did he do it?

8.4 Fermat's Last Theorem

Fermat's Last Theorem is really a question: can we find natural numbers a, b, c, n such that:

$$a^n = b^n + c^n?$$

For $n = 1$ we can solve the equation:

$$a = b + c.$$

F_n	*primality*	*factorisation*	*who*
1	*prime*	5	*unknown*
2	*prime*	17	*unknown*
3	*prime*	257	*unknown*
4	*prime*	65537	*Fermat*
5	*composite*	641.	*Euler*, 1732
6	*composite*	274117.	*Landry*, 1880
7	*composite*		*Brillhart and Morrison* 1971
8	*composite*		*Brent and Pollard*
$9-11$	*all composite*	*all factored*	

Figure 8.1: Fermat Numbers for values up to eleven

There are infinitely many solutions. For $n = 2$ the equation reduce to Pythagoras's Theorem about right sided triangles with integer lengths.This also has infinitely many solutions:

$$a^2 = b^2 + c^2.$$

Next we shall consider the exponent and the trivial solutions for a, b, c of zero and one:

$$\begin{aligned} 0^n &= 0^n + 0^n \\ 1^n &= 1^n + 0^n. \end{aligned}$$

These equations are true for all exponents.

We will not here settle Fermat's Last Theorem for the non-trivial cases of a, b, c for exponents greater than two. During history many great mathematicians have proved this theorem for a finite number of exponents. Recently, Dr. Andrew Wiles completely solved this famous conjecture by Fermat.

Chapter 9

Legendre, Jacobi and Kronecker

9.1 The Legendre Symbol

Consider the complete set, $\mathcal{A}$, of non-zero congruences for an odd prime number p:

$$\mathcal{A} = \{1, 2, 3, \ldots, p-3, p-2, p-1\}$$

and the set of its squares, denoted here by S:

$$\mathcal{S} = \{1, 4, 9, \ldots, (p-3)^2, (p-2)^2, (p-1)^2\}$$

and note that:

$$\begin{aligned} (p-1)^2 &= p^2 - 2p + 1^2 \\ &\equiv 1 \pmod{p} \end{aligned}$$

and:

$$\begin{aligned} (p-2)^2 &= p^2 - 4p + 2^2 \\ &\equiv 4 \pmod{p} \end{aligned}$$

and so on. In general

$$\begin{aligned} (p-a)^2 &= p^2 - 2ap + a^2 \\ &\equiv a^2 \pmod{p}. \end{aligned}$$

so that $\mathcal{S}$ looks like:

$$\mathcal{A} = \{1, 4, 9, \ldots, 9, 4, 1\} \pmod{11}.$$

There are $(n-1)/2$ (unique) members in total belonging to $\mathcal{S}$ and $(n-1)/2$ remaining that are not members of $\mathcal{S}$.

For example, take p=11. Then:

$$\mathcal{A} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

and

$$\mathcal{S} = \{1, 4, 9, 16, 25, 36, 49, 64, 81, 100\}$$

and by taking modular reductions:

$$\mathcal{S} \equiv \{1, 4, 9, 5, 3, 3, 5, 9, 4, 1\} \pmod{11}.$$

Removing repeats we have:

$$\mathcal{S} \equiv \{1, 4, 9, 5, 3\} \pmod{11}.$$

The non–zero elements that belong to the set of squares are called *quadratic residues* and those that do not belong to it are called *quadratic non-residues*. The quadratic residues and non residues are represented by the *Legendre Symbol*. A quadratic residue, s, is denoted by:

$$(s/n) = 1.$$

Otherwise if s is a quadratic non-residue it is written as:

$$(s/n) = -1.$$

9.2 The Jacobi Symbol

The Jacobi Symbol extends the Legendre Symbol to all odd numbers n not just the primes. Fortunately for testing of primality, a Jacobi Symbol of -1 implies a non-square. A Jacobi Symbol of 1 cannot indicate the number is definitely a square over n. The algorithm to compute the symbol [5] is not much more than that of a gcd.

9.3 The Kronecker Symbol

The Kronecker Symbol is the same as the Jacobi Symbol but also includes even numbers n.

Chapter 10

Euler's Phi Function

How many times do we have to multiply a number by itself to be itself when it is considered as the remainder of a division by some number?

$$a^{k?} \equiv a \pmod{n}$$

That is, given any a and some n in the above equation, what is the value of k for which the equation makes sense? If n is prime, say p, we use Fermat's *Little* Theorem to see that k is equal to p:

$$(\forall a \in \mathbb{Z}) \;\; a^p \equiv a \pmod{p}.$$

Apart from the value of one, what then is the value of k when n is composite?

The number of values that have a multiplicative inverse is given by the *Euler Phi Function*. Assume that:

$$n = p_1^{i_1} p_2^{i_2} \dots p_j^{i_j}$$

where the individual p_k are distinct and are as many as shown in their respective exponents. We then list the n elements:

$$1, 2, 3, \dots, n.$$

For each distinct ${p_k}^{i_k}$ we only loose values divisible by ${p_k}^1$: If ${p_k}^{i_k}$ divides any element chosen from the list then ${p_k}^{i_k - 1}$ divides that element and inductively p_k also divides it. Then the Euler Phi Function of n which is usually denoted by $\varphi(n)$ is given as:

$$\varphi(n) = (p_1 - 1)p_1^{i_1 - 1}(p_2 - 1)p_2^{i_2 - 1} \dots (p_j - 1)p_j^{i_j - 1}.$$

The Euler Phi Function is useful since for all a such that $\gcd(a, n) = 1$

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Although the the proof of this is a little daunting it can be best illustrated by an example. Suppose that $n = 15$. Its proper prime factors are 3^1 and 5^1. That is

$$15 = 3 \times 5.$$

We discount the numbers in the list that are divisible by three or five:

$$1, 2, \not{3}, 4, \not{5}, \not{6}, 7, 8, \not{9}, \not{10}, 11, \not{12}, 13, 14, \not{15}.$$

This leaves eight elements of the list. Alternatively by calculation of the Euler Phi Function:

$$\varphi(n) = (3-1)3^0(5-1)5^0 = 2.4 = 8.$$

Trivially:

$$1 \equiv 1 \pmod{n}.$$

Now we check a number relatively prime to fifteen, for example two:

$$2^8 \equiv 256 \equiv 15 \times 17 + 1 \equiv 1 \pmod{15}.$$

In general for values of a that are relatively prime to n form a group known as the *multiplicative group*. The number of elements of the group is given by the Euler Phi Function. Group theorist have proven that each element's order divides the size of the group.

Chapter 11

Lucas Sequences

Classically the *Lucas sequence* [7] is defined as:

$$\begin{aligned} V_0 &= 2 \\ V_1 &= 1 \\ V_n &= V_{n-1} + V_{n-2} \end{aligned}$$

which generates

$$< 2, 1, 3, 4, 7, 11, 18, \ldots > .$$

In the same way the *Fibonacci* sequence is defined by:

$$\begin{aligned} f_0 &= 1 \\ f_1 &= 1 \\ f_n &= f_{n-1} + f_{n-2} \end{aligned}$$

generating

$$< 1, 1, 2, 3, 5, 8, 13, \ldots > .$$

We can represent these sequences by matrices:

$$\begin{aligned} M_0 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ M_1 &= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \\ M_n &= M_{n-1} + M_{n-2}. \end{aligned}$$

noting that the traces give the Lucas sequence and the top left elements give the Fibonacci sequence.

Generalising the Lucas sequence with integer parameters, P and Q, we define:

$$\begin{aligned} V_0 &= 2 \\ V_1 &= P \\ V_n &= PV_{n-1} - QV_{n-2} \end{aligned}$$

and the corresponding matrix element sequence as:

$$\begin{aligned} U_0 &= 1 \\ U_1 &= P \\ U_n &= PU_{n-1} - QU_{n-2}. \end{aligned}$$

We represent the by matrices as:

$$\begin{aligned} M_0 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ M_1 &= \begin{pmatrix} P & -Q \\ 1 & 0 \end{pmatrix} \\ M_n &= PM_{n-1} + QM_{n-2} \end{aligned}$$

noting that

$$M_n = M^n$$

and that

$$M_{a+b} = M_a M_b.$$

The characteristic equation is:

$$M^2 = PM - Q$$

or

$$M^2 - PM + Q = 0.$$

Although the matrix representation can help with mathematical manipulation of Lucas sequences, in practice there are much quicker ways to compute them.

Consider the case when $Q = -1$ with the Lucas V-sequence being:

$$\begin{aligned} V_0 &= 2 \\ V_1 &= P \\ V_n &= PV_{n-1} - V_{n-2}. \end{aligned}$$

Here is a very fast algorithm to compute the n^{th} pair of $V(P, -1, n)$ modulo n with the Jacobi Symbol $J(P^2 - 4, n) = -1$ for a Lucas PRP test:

```
Assign u=2 and v=P
Loop over the bits of n, high to low:
  If the current bit is 1 then:
    Assign u=u*v-P mod n
    Assign v=v*v-2 mod n
  Else (if the current bit is 0):
    Assign v=u*v-P mod n
    Assign u=u*u-2 mod n
Finally check that u=P and v=2.
```

Chapter 12

Frobenius and Gaussian Primes

12.1 Frobenius

A Frobenius test is taken modulo n and modulo a polynomial equation in one variable. Note that we have effectively two zeroes. For an example of such a polynomial take $x^2 - 3x + 1 = 0$. We can calculate say powers of bases by reducing $\pmod{x^2 - 3x + 1}$, where we can recursively or otherwise reduce x^2 to $3x - 1$, and then reducing the remaining coefficients by modulo n. These two modular reductions are written as $\pmod{n, x^2 - 3x + 1}$.

12.2 Gaussian Primes

Consider the the polynomial $x^2 + 1$. We see for integers a and b that $ax + b \pmod{x^2 + 1}$ form the *Gaussian integers*. The expression $-ax + b$ is called the *conjugate* of $ax + b$.

Gaussian integers can be prime in their own way. For example $2x + 1$ and $x + 1$ are neither ± 1 nor $\pm x$ (the units) and their product:

$$(2x + 1)(x + 1) \equiv 2x^2 + 3x + 1 \equiv 3x - 1 \pmod{x^2 + 1}$$

is by definition composite.

A *Gaussian prime* $ax + b \pmod{x^2 + 1}$ occurs when the *norm* $|a^b + c^2|$ is a prime integer. For example $3x - 1 \pmod{x^2 + 1}$ is not a Gaussian prime because it has the norm $3^2 + 1 = 10$ which is not a prime integer. Another example: $2x + 1 \pmod{x^2 + 1}$ is a Gaussian prime because its norm $2^2 + 1 = 5$ is a prime integer.

The set of *associates* of $ax + b$ results from multiplication by $\{\pm 1, \pm x\}$. For example the associates of $2x + 1$ are in $\{2x + 1, -2x - 1, x + 2, -x - 2\}$.

So any number that can be written as a product of $\{\pm 1, \pm x\}$ and an integer prime of the form $4k + 1$, which Fermat showed can be written uniquely as $a^2 + b^2$, forms a Gaussian prime. For example the integer prime $101 = 4.25 + 1$ can be written uniquely as $10^2 + 1$. Consequently $10x + 1$ is a Gaussian prime as are its associates and the conjugates of all four of them.

Chapter 13

Perrin Sequence

13.1 Perrin Sequence

Consider the sequence f_n:

$$\ldots, 3, 0, 2, 3, 2, 5, 5, 7, 10, 12, 17, 22, \ldots \; f_n = f_{n-2} + f_{n-3}, \ldots$$

If n is prime then: $f_n \equiv 0 \pmod{n}$ since: $\alpha+\beta+\gamma \equiv \alpha^n+\beta^n+\gamma^n \pmod{n}$. However the converse is not true. The value $271441 = 521^2$ is the first *pseudoprime* in this sequence:

$$\alpha+\beta+\gamma \equiv \alpha^{271441}+\beta^{271441}+\gamma^{271441} \pmod{271441}.$$

The idea can be extended to the sequence for the general equation $y = x^m - x^r - 1$. If n is prime then:

$$\sum_{j=1}^{j=m} \alpha_j \equiv \sum_{j=1}^{j=m} \alpha_j^n \pmod{n}.$$

However there always seems to be composite n for which this condition also holds. This does not, then, provide us with a hard and fast test for primality.

13.2 Characteristic Function

Consider the function: $F : F(a, b, r) = a^m - a^r - 1$. We know by Fermat's Little Theorem that if F is prime: $a^F \equiv a \pmod{F}$.

To date the author has done much testing and has not found a case for which the above equation holds for a composite F, with the exception of $F(2, m, m-1) = 2^{m-1} - 1$.

If F is prime, the condition is passed on to the sums of the powers of the roots : for all k:

$$(\forall k \in \mathbb{Z}) \;\; \sum_{j=1}^{j=m} \alpha_j^k \equiv \sum_{j=1}^{j=m} \alpha_j^{kF}. \pmod{F}$$

In fact, all symmetric functions in α_i are equivalent to them in ${\alpha_i}^F$ modulo F.

Chapter 14

Carmichael Numbers

We saw that Fermat's little Theorem can be used to do a probabilistic test for primality. If a number fails Fermat's little Theorem test it is definitely composite. We cannot say it is definitely prime if it does pass. Furthermore there are some numbers that pass whatever base is chosen. These numbers are known as Carmichael Numbers. The first is 561:

$$(\forall a \in \mathbb{Z}) \;\; a^{561} \equiv a \pmod{561}.$$

We have to use something else to test such numbers. This could be strengthening Fermat's little theorem by taking successive square roots of 1 which are known to be ± 1 for primes. Or we can use Lucas Sequences or higher order fields (which can also be strengthened).

Chapter 15

RSA Cipher

15.1 RSA Algorithm

No one has found a quick method for factorising very large composite numbers. In 1978 Rivest, Shamir and Aldeman published their work on a cipher that takes very good advantage of this.

$$\begin{aligned} Encode : E(x) &\equiv x^s \pmod{p.q} \\ Decode : D(x) &\equiv x^t \pmod{p.q} \end{aligned}$$

$$where\, p, q \in \mathbb{P}\, and\, s.t \equiv 1 \pmod{(p-1)(q-1)}.$$

The sender of the message does not know the decoding key. In fact only the receiver does. An intercepted encrypted message can not be decoded without the required decoding key. The values of p and q are chosen to be big because factorising them is prohibitively time consuming. A would be attacker cannot compromise the cipher without knowing what $\varphi(pq)$ is.

We need to show that $D(E(x)) = x$ in order to prove that algorithm works:

$$\begin{aligned} D(E(x)) &\equiv (x^s)^t \pmod{n} \\ &\equiv x^{st} \pmod{n}. \end{aligned}$$

We choose s such that it is relatively prime to $(p-1)(q-1)$. This means that $\gcd(s, (p-1)(q-1)) = 1$. We then know there exists numbers t and k such that:

$$st + (p-1)(q-1)k = 1.$$

Hence:

$$x^{st+(p-1)(q-1)k} = x^1.$$

The order of multiplying x by itself is given by Euler's Phi Function as:

$$\varphi(pq) = (p-1)(q-1).$$

Hence:

$$x^{st} \equiv x \pmod{pq}$$

and so:

$$D(E(x)) = x.$$

To construct the code:

- obtain two large distinct primes p and q.
- choose s: $s \wedge (p-1)(q-1) = 1$.
- using Euclid's algorithm calculate t: $st \equiv 1 \pmod{(p-1)(q-1)}$.

We can choose s to be small for quick encoding. Or choose t to be small and compute s via the extended euclidian algorithm so that decoding is quick.

15.2 RSA over $x^2 - ax + 1$

- Find a such that the Jacobi Symbols $J(a^2-4, p) = -1$ and $J(a^2-4, q) = -1$ where p and q are two distinct large primes and let $n = pq$.
- Choose s such that $s \wedge (p^2-1)(q^2-1) = 1$.
- Use Euclid's extended algorithm to compute $t \equiv s^{-1}$ over $(p^2-1)(q^2-1)$.
- Then we can encode u and v with $E(ux+v)$ as $Ux+V \equiv (ux+v)^s \pmod{n, x^2-ax+1}$.
- Decode with $D(Ux+V)$ as $ux+v \equiv (Ux+V)^t \pmod{n, x^2-ax+1}$.

Note that $D(E(ux+v)) \equiv (ux+v)^{st} \equiv ux+v \pmod{n, x^2-ax+1}$.

Chapter 16

The Selfridge Unit of Measure

When calculating exponents of a number, for example for a *little Fermat test*, a matrix or a Lucas sequence, we perform mostly additions, multiplications and modular reductions. Multiplication operations are much more time-consuming than addition ones, and modulo operations are the most time-consuming as they involve division.

There are some techniques to reduce multiplication time such as Karatsuba's Method and *fast Fourier transforms*. The times for these are of the order of:

school boy n^2

Karatsuba $n^{1.58}$

FFT $n.log(n)log(log(n))$

In practice small numbers are best calculated not by FFT. There is a optimal length at which FFT should be used. A lot depends on the architecture of the computer being used. Thus for an arbitrary number size we have to choose which number is optimal. Hence the function for the timing of modular exponentiation with its additions, multiplications and modular reductions is affected by the methods used, be they school boy, Karatsuba, or FFT.

The time taken to do one Fermat test $a^n \pmod n$ is called a *selfridge* [2]. Note that the time to do a strong Fermat test is almost the same.

The Lucas modular n-exponentiation for $(P, -1, n)$ can be done in 2 selfridges. The devil is in the detail: It is important to analize the exponentiating algorithm to reduce the overall operations. Computers have different circuits for addition than multiplication, on some being performed simultaneously, and it is the art of the programmer to maximise throughput.

Chapter 17

Trinomial Recurrence

17.1 A Cubic Recurrence

Here we consider the equation:

$$0 = x^3 - x - 1.$$

This can rewrite this as:

$$x^3 = x + 1.$$

We may now compute any power of x greater than 3 by multiplying both sides by x^{n-3}:

$$x^n = x^{n-2} + x^{n-3}. \tag{17.1}$$

We can use this for any value of $n \in \mathcal{Z}$.

Obviously the following holds:

$$\begin{aligned} x^0 &= 1 \\ x^1 &= x \\ x^2 &= x^2. \end{aligned}$$

Using the relation 17.1 we can compute x^4 as:

$$x^4 = x^2 + x.$$

Using the relation 17.1 repeatedly, we can compute x^5 as:

$$\begin{aligned} x^5 &= x^3 + x^2 \\ &= (x+1) + x^2 \\ &= x^2 + x + 1. \end{aligned}$$

Notice that, whatever power of x we wish to compute, we can reduce it to a quadratic of the form $Ax^2 + Bx + C$ for some A,B and C.

We now build a table of the powers of x:

	x^0	x^1	x^2	x^3	x^4	x^5
1	1	0	0	1	0	1
x	0	1	0	1	1	1
x^2	0	0	1	0	1	1

We can easily compute the next column, for x^6. Since we know that $x^6 = x^4 + x^3$, we simply add the corresponding values row-wise. The table for the first ten values are:

	...	x^0	x^1	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9	...
1	...	1	0	0	1	0	1	1	1	2	2	...
x	...	0	1	0	1	1	1	2	2	3	4	...
x^2	...	0	0	1	0	1	1	1	2	2	3	...

Now consider the values under x^i, x^{i+1} and x^{i+2} as the matrix M_i. Thus:

$$M_1 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Squaring this we see:

$$\begin{aligned} (M_1)^2 &= \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \\ &= M_2. \end{aligned}$$

Next consider the calculation:

$$\begin{aligned} M_3 \otimes M_4 &= \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 2 \\ 0 & 1 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 2 \\ 2 & 3 & 4 \\ 2 & 2 & 3 \end{pmatrix} \\ &= M_7. \end{aligned}$$

In general we have:

$$M_i \otimes M_j = M_{i+j}.$$

From the recurrence relationship, we also have:

$$M_k = M_{k-2} + M_{k-3}.$$

17.2 Roots

Let α, β and γ be the roots of the cubic equation $y = x^3 - x - 1$:

$$(x-\alpha)(x-\beta)(x-\gamma) = 0.$$

Multiplying out we get:

$$x^3 - (\alpha+\beta+\gamma)x^2 + (\alpha\beta+\beta\gamma+\gamma\alpha)x - \alpha\beta\gamma = 0.$$

We can now equate the coefficients with $x^3 - x - 1 = 0$:

$$\begin{aligned} \alpha+\beta+\gamma &= 0 \\ \alpha\beta+\beta\gamma+\gamma\alpha &= -1 \\ \alpha\beta\gamma &= 1. \end{aligned}$$

The right hand side of these equations are called the *elementary symmetric functions*. From this we can deduce:

$$\begin{aligned} 0 &= (\alpha+\beta+\gamma)^2 \\ &= \alpha^2+\beta^2+\gamma^2+2(\alpha\beta+\beta\gamma+\gamma\alpha) \\ &= \alpha^2+\beta^2+\gamma^2+2(-1) \\ &= \alpha^2+\beta^2+\gamma^2-2. \end{aligned}$$

We can rewrite this as:

$$\alpha^2+\beta^2+\gamma^2 = 2.$$

Since α, β and γ are all non-zero:

$$\alpha^0+\beta^0+\gamma^0 = 3.$$

Since α, β and γ satisfy the equation $x^3 = x+1$ we deduce that for all $n \in \mathbb{Z}$:

$$\begin{aligned} \alpha^n &= \alpha^{n-2}+\alpha^{n-3} \\ \beta^n &= \beta^{n-2}+\beta^{n-3} \\ \gamma^n &= \gamma^{n-2}+\gamma^{n-3}. \end{aligned}$$

Summing these:

$$\alpha^n+\beta^n+\gamma^n = \alpha^{n-2}+\beta^{n-2}+\gamma^{n-2}+\alpha^{n-3}+\beta^{n-3}+\gamma^{n-3}.$$

We can use this to compute:

$$\begin{aligned} \alpha^3+\beta^3+\gamma^3 &= \alpha^1+\beta^1+\gamma^1+\alpha^0+\beta^0+\gamma^0 \\ &= 0+3 \\ &= 3. \end{aligned}$$

Thus we can compute any sum of the powers of the roots:

$$\begin{aligned}
\alpha^0 + \beta^0 + \gamma^0 &= 3 \\
\alpha^1 + \beta^1 + \gamma^1 &= 0 \\
\alpha^2 + \beta^2 + \gamma^2 &= 2 \\
\alpha^3 + \beta^3 + \gamma^3 &= 3 \\
\alpha^4 + \beta^4 + \gamma^4 &= 2 \\
\alpha^5 + \beta^5 + \gamma^5 &= 5 \\
\alpha^6 + \beta^6 + \gamma^6 &= 5 \\
\vdots &= \vdots
\end{aligned}$$

Let f_n represent the sum of the n^{th} powers of the roots:

$$f_n = \alpha^n + \beta^n + \gamma^n.$$

The sequence for f_i is:

$$\ldots 3, 0, 2, 3, 2, 5, 5, 7, 10 \ldots (f_{k-3} + f_{k-2} = f_k) \ldots$$

It's recurrence relationship can be defined by:

$$\begin{aligned}
f_0 &= 3 \\
f_1 &= 0 \\
f_2 &= 2 \\
(\forall k \in \mathbb{Z}) \quad f_k &= f_{k-2} + f_{k-3}.
\end{aligned}$$

We now return to the table, this time summing the diagonals in a south easterly sense:

	$\ldots$	x^0	x^1	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9	$\ldots$
1	$\ldots$	1	0	0	1	0	1	1	1	2	2	$\ldots$
x	$\ldots$	0	1	0	1	1	1	2	2	3	4	$\ldots$
x^2	$\ldots$	0	0	1	0	1	1	1	2	2	3	$\ldots$
				$\searrow$	3	0	2	3	2	5	5	$\ldots$

This shows that the sum of the diagonal elements, called the *trace*, of M_n is equal to the sum of the n^{th} powers of the roots of the equation $y = x^3 - x - 1$:

$$Tr(M_n) = f_n.$$

17.3 Periodicity

The sum of the powers of the roots of the equation: $y = a^3 - a - 1, f(n)$, must have a finite period over a prime field. We call this period $\tau(f, p)$. Notice that, $\ldots, 0, 0, 0, \ldots$ never occurs because this would result in a sequence of zeroes. This leaves $p^6 - 1$ possible triplets in the sequence. The period divides this:

$$\tau(f, p) \mid p^6 - 1.$$

17.4 General Trinomial

In the chapter on the Cubic Equation we considered the equation $0 = x^3 - x - 1$. In this chapter we consider the equation:

$$0 = x^m - x^r - 1.$$

We transfer the ideas and summarise some of the ideas introduced in the Cubic Equation chapter. M_0 is the m by m identity matrix:

$$M_0 = I_m.$$

The *companion matrix* M_1 is the m by m matrix:

$$M_1 = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & 0 & 1 \\ 1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 & \vdots \\ \dots & \dots & \dots & \dots & \dots & \dots & 1 \\ 0 & 0 & 0 & \dots & 0 & 0 & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 & \vdots \\ 0 & 0 & 0 & \dots & 0 & 1 & \vdots \end{pmatrix}$$

The bottom left $m-1$ by $m-1$ elements is equal to the matrix I_{m-1}. The "floating" 1 on the right hand column is in the $(r+1)^{th}$ row.

We state here without much explanation that:

$$M_{i+j} = M_i \otimes M_j.$$

The matrices also satisfy for all k the recurrence:

$$M_{m+k} = M_{r+k} + M_{1+k}.$$

Also the sum of the diagonal elements of the matrix M_k is equal to the sum of the k^{th} powers of the roots of the equation $y = x^m - x^r - 1$:

$$Tr(M_k) = \sum_{j=1}^{j=m} \alpha_j^k.$$

For example, we may now easily answer the following question: what is the sum of the 7^{th} powers of the roots of the equation $y = x^5 - x^2 - 1$?

To answer this compute the following table:

	x^0	x^1	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9	...			
1	1	0	0	0	0	1	...							
x		1	0	0	0	0	1	...						
x^2			1	0	0	1	0	1	...					
x^3				1	0	0	1	0	1	...				
x^4					1	0	0	1	0	1	...			
					$\searrow$	5	0	0	3	0	5	3	0	...

Thus

$$\sum_{j=1}^{j=5} \alpha_j^7 = 0.$$

17.5 Reducibility

Not all the expression of the form $x^m - x^r - 1$ are *irreducible*. For example:

$$x^5 - x^4 - 1 = (x^3 - x - 1)(x^2 - x + 1),$$

Therefore $x^5 - x^4 - 1$ can never be prime.

Chapter 18

The Monster and its Children

18.1 The Monster

Consider the function:

$$F = a^r \prod_{i \in \mathbb{N}} (a^{r_i} - 1)^{t_i} - 1.$$

Examining the left hand side, the product:

$$a^r \prod_{i \in \mathbb{N}} (a^{r_i} - 1)^{t_i},$$

we see that it is equal to 0 when $a = 0$ or when a $a^{r_i} - 1 = 0$. In the latter case a is a root of unity determined by the r_i. Note that t_i is the multiplicity of the various $a^{r_i} - 1$.

When F is irreducible and not $a^2 - a - 1$ it is conjectured that the value is prime if

$$a^F \equiv a \pmod{F}.$$

18.2 The Fermatian Child

Consider the simpler expression:

$$F = a^A (a-1)^B (a+1)^C - 1.$$

It is conjectured that for distinct x, y and z that the Fermat-like trinomial

$$Ax^n + By^n + Cz^n = 0.$$

has no non-trivial integer solutions for

$$n \geq |A| + |B| + |C|.$$

Note that with arrangement this simpler F is a *child*:

$$F = a^A(a^2-1)^C(a-1)^{B-C} - 1.$$

For example consider

$$F = a^2(a-1)^3(a+1)^5 - 1.$$

Then it is conjectured that

$$2x^n + 3y^n + 5z^n = 0.$$

has no non-trivial integer solutions for

$$\begin{aligned} n &\geq |2| + |3| + |5| \\ n &\geq 10. \end{aligned}$$

18.3 The Quadratic Child

Now for our F let $r = 0$, $i = 1$, $s_1 = 2$ and $t_1 = 1$ such that:

$$F = a^2 - 2.$$

Odd F of this form would be conjecturally prime if

$$a^{2(F-1)} \equiv 2^{F-1} \pmod{F}.$$

We may strengthen this to

$$a^{F-1} \equiv 2^{\frac{F-1}{2}} \pmod{F}$$

and by Fermat's little Theorem it would be sufficient to test

$$2^{\frac{F-1}{2}} \equiv 1 \pmod{F}.$$

This 1-selfridge test is very fast for a computer to perform, but note that it has zero density in the natural numbers.

Chapter 19

Quadratic PRP Tests

19.1 Introduction

There are algorithms, such as ECPP (elliptic curve primality proving), that test numbers fully for their primality, leaving no doubt. However, sometimes speed is important. There are quicker tests which have a very small chance of failure. That is the test may mis-identify a composite number as a prime. An attack on some crypto systems is possible if an attacker presents a composite number knowing the receiving primality testing algorithm will be fooled into thinking the number is prime.

An arbitrary number found by quick methods is called a *probable prime* (PRP). A composite number that is mis-identified as a prime is called a *pseudoprime*.

Trial division by primes to the square root of a 150 digit number to show itself is prime is infeasible. So we must use other methods such as those based on Fermat's "little theorem", or Lucas Sequences *etc*.

There are counterexamples to Lucas Sequence tests too. Despite *strengthening* these tests, as John Selfridge *et al* have done, counterexamples are known. Even with repeated random applications with different parameters some counterexamples are known.

A Fermat Little Theorem test is said to take 1 *selfridge* [2]: log_2 multiplications and modular reductions are done over the number being tested. The quickest general Lucas Sequence tests take 2 selfridges.

The Baillie-PSW composite test [1] combines a Little Fermat test with a Lucas Sequence test, but has no known counterexamples. It is $1 + 3$ selfridges. Jon Grantham's Random Quadratic Frobenius Test [3] is 3 selfridges.

19.2 A Quadratic Test

Consider the matrix

$$M = \begin{pmatrix} a & -1 \\ 1 & 0 \end{pmatrix}$$

whose characteristic equation is

$$x^2 - ax + 1 = 0$$

and let

$$M^* = M - X$$

where

$$X = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$$

or written in full:

$$\begin{pmatrix} 0 & -1 \\ 1 & -a \end{pmatrix} = \begin{pmatrix} a & -1 \\ 1 & 0 \end{pmatrix} - \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}.$$

Note the symmetry between M^* and M causing them to be computationally the same. For example:

$$\begin{aligned} M^2 &= \begin{pmatrix} a & -1 \\ 1 & 0 \end{pmatrix}^2 \\ &= \begin{pmatrix} a^2 - 1 & -a \\ a & -1 \end{pmatrix} \\ M^{*2} &= \begin{pmatrix} 0 & -1 \\ 1 & -a \end{pmatrix}^2 \\ &= \begin{pmatrix} -1 & a \\ -a & a^2 - 1 \end{pmatrix}. \end{aligned}$$

Let's now take the n^{th} power in the style of a Little Fermat test of M^*:

$$M^{*n} = (M - X)^n$$

noting that the matrix X commutes with M under multiplication, so that for odd n:

$$M^{*n} = M^n + \Sigma_{i=1}^{i=n-1} \begin{pmatrix} n \\ i \end{pmatrix} (-X)^i M^{n-i} - X^n.$$

If we assume n to be an odd prime then the indicated binomial coefficients are all 0 modulo n:

$$\begin{pmatrix} n \\ i \end{pmatrix} \equiv 0 \pmod{n}.$$

Thus by assuming n is an odd prime we have:

$$M^{*n} \equiv M^n - X^n \pmod{n}.$$

Since M^* and M are computationally the same we need only compute

$$\begin{aligned} &M^n \pmod{n} \\ &X^n \pmod{n} \end{aligned}$$

and check the difference is

$$M^{*n} \pmod{n}.$$

Calculating the traces of M_n and M_{n+1} is much quicker than matrix multiplication.

With a strong Jacobi Symbol for the discriminant of the characteristic equation

$$J(a^2 - 4, n) = -1$$

the stronger equation happens due to the Frobenius endomorphism:

$$M^n \equiv \frac{I}{M} \pmod{n}$$

where

$$\frac{I}{M} = \begin{pmatrix} 0 & 1 \\ -1 & a \end{pmatrix}.$$

Looking at the traces we see that the equivalent Lucas-V sequences with the strong Jacobi Symbol are

$$\begin{aligned} V_n &= a \\ V_{n+1} &= 2. \end{aligned}$$

Thus the test for a chosen x is very quick:

$$\begin{aligned} J(a^2 - 4, n) &= -1 \\ a^{n-1} &\equiv 1 \pmod{n} \\ x^{n+1} &\equiv 1 \pmod{n, x^2 - ax + 1}. \end{aligned}$$

Unfortunately, there are plenty of pseudoprimes for this test. However, we can strengthen the test in a number of ways. Firstly, we can use a *minimal* parameter a, as the Baillie-PSW test does; and, secondly, we can repeat the test on n with different parameters. Thirdly, we can strengthen the Little Fermat test by letting $n - 1 = d \cdot 2^s$ where d is odd. Then either:

$$a^d \equiv 1 \pmod{n}$$

or

$$a^{2^r \cdot d} \equiv -1 \pmod{n}$$

for some r such that $0 \leq r < s$.

Fourthly, in a similar way, we can strengthen the Lucas Sequence test as follows. Let $n + 1 = e \cdot 2^f$ where e is odd, Then either:

$$V(2, a, < e - 1, e >) \equiv < a, 2 > \pmod{n}$$

or

$$V(2, a, < 2^g \cdot e - 1, 2^g \cdot e >) \equiv < -a, -2 > \pmod{n}$$

for some g such that $0 \leq g < f$.

These strengthening conditions of the Little Fermat tests and the Lucas Sequence tests are easily calculated with left-to-right binary exponentiation.

19.3 A Double Quadratic Test

Define the two matrices M and N as follows:

$$\begin{aligned} M &= \begin{pmatrix} a-2 & -1 \\ 1 & 0 \end{pmatrix} \\ N &= \begin{pmatrix} a+2 & -1 \\ 1 & 0 \end{pmatrix} \end{aligned}$$

with

$$\begin{aligned} X &= \begin{pmatrix} a-2 & 0 \\ 0 & a-2 \end{pmatrix} \\ Y &= \begin{pmatrix} a+2 & 0 \\ 0 & a+2 \end{pmatrix}. \end{aligned}$$

Consider the following equations

$$\begin{aligned} M^* &= M - X \\ N^* &= N - Y \end{aligned}$$

written out in full as

$$\begin{aligned} \begin{pmatrix} 0 & -1 \\ 1 & -a+2 \end{pmatrix} &= \begin{pmatrix} a-2 & -1 \\ 1 & 0 \end{pmatrix} - \begin{pmatrix} a-2 & 0 \\ 0 & a-2 \end{pmatrix} \\ \begin{pmatrix} 0 & -1 \\ 1 & -a-2 \end{pmatrix} &= \begin{pmatrix} a+2 & -1 \\ 1 & 0 \end{pmatrix} - \begin{pmatrix} a+2 & 0 \\ 0 & a+2 \end{pmatrix}. \end{aligned}$$

The idea is to compute for a suspected prime n

$$\begin{aligned} M^{*n} &\equiv M^n - X^n \pmod{n} \\ N^{*n} &\equiv N^n - Y^n \pmod{n} \end{aligned}$$

where the Jacobi Symbols for the quadratic characteristic equations

$$\begin{aligned} x^2 - (a-2)x + 1 &= 0 \\ y^2 - (a+2)y + 1 &= 0 \end{aligned}$$

are strong:

$$\begin{aligned} J((a-2)^2 - 4, n) &= -1 \\ J((a+2)^2 - 4, n) &= -1 \end{aligned}$$

and computing and checking

$$\begin{aligned} (a-2)^{n-1} &\equiv 1 \pmod{n} \\ (a+2)^{n-1} &\equiv 1 \pmod{n} \\ x^{n+1} &\equiv 1 \pmod{n, x^2 - (a-2)x + 1} \\ y^{n+1} &\equiv 1 \pmod{n, y^2 - (a+2)y + 1}. \end{aligned}$$

The matrix exponents can be quickly calculated using Lucas sequences

$$\begin{aligned} M: &\quad < V_n, V_{n+1} > \equiv < a-2, 2 > \pmod{n} \\ N: &\quad < V_n, V_{n+1} > \equiv < a+2, 2 > \pmod{n}. \end{aligned}$$

In order to find suitable x and y we require that n is non-square and

$$\gcd(30, n) = 1$$

Note that when strengthening the Lucas Sequence tests the following is conjectured to be true:

$$\begin{aligned} M^{\frac{n+1}{2}} &\equiv \pm I \pmod{n} \\ N^{\frac{n+1}{2}} &\equiv \mp I \pmod{n}. \end{aligned}$$

respectively.

It is observed that

$$Tr\begin{pmatrix} 3 & -1 \\ 1 & 0 \end{pmatrix}^{2 \cdot n} = Tr\begin{pmatrix} 7 & -1 \\ 1 & 0 \end{pmatrix}^{n}$$

for all n. Hence the test with parameter pair $\{3, 7\}$, i.e. when the Jacobi Symbol $J(5, n) = -1$, requires two Little Fermat tests and only one Lucas Sequence test. Therefore, for this limited parameter pair:

$$\begin{pmatrix} 3 & -1 \\ 1 & 0 \end{pmatrix}^{\frac{n+1}{2}} \equiv -1 \pmod{n}$$

for prime n.

19.4 Second Double Quadratic Test

Rather than using the pair of characteristic equations of matrices to test the probable primality of a number n

$$\begin{aligned} x^2 - (a-2)x + 1 &= 0 \\ y^2 - (a+2)y + 1 &= 0 \end{aligned}$$

with strong discriminants, i.e. for which the Jacobi Symbols are -1, we could instead use:

$$\begin{aligned} x^2 - (a-1)x + 1 &= 0 \\ y^2 - (a+1)y + 1 &= 0 \end{aligned}$$

with strong Jacobi Symbols for the discriminants

$$\begin{aligned} J((a-1)^2 - 4, n) &= -1 \\ J((a+1)^2 - 4, n) &= -1 \end{aligned}$$

and check that

$$\begin{aligned} x^{2n} - (a-1)^n x^n + 1^n &\equiv 0 \pmod{n} \\ y^{2n} - (a+1)^n y^n + 1^n &\equiv 0 \pmod{n} \end{aligned}$$

simply be computing

$$\begin{aligned} (a-1)^{n-1} &\equiv 1 \pmod{n} \\ (a+1)^{n-1} &\equiv 1 \pmod{n} \\ x^{n+1} &\equiv 1 \pmod{n, x^2 - (a-1)x + 1} \\ y^{n+1} &\equiv 1 \pmod{n, y^2 - (a+1)y + 1}. \end{aligned}$$

Computing the Lucas V sequences, the traces of the matrices, is quicker.

A boundary condition is that $\gcd(a, n) = 1$ because if not then for some common divisor, d, we would trivially have:

$$\begin{aligned} M^2 + M + 1 &\equiv 0 \pmod{d} \\ N^2 - N + 1 &\equiv 0 \pmod{d}. \end{aligned}$$

which make the equations cyclotomic over the divisor.

Also, to find a suitable pair, $a-1$ and $a+1$, we further require that n is non-square and $\gcd(210a, n) = 1$. The requirement that $\gcd(7, n) = 1$ is a practical one because searching for a strong Jacobi pair of parameters is fruitless for $n = 7 \cdot r^2$.

No counterexamples to this test have been found.

19.5 A Two Selfridge Test

When computing intermediate values $sx + t$ of left to right binary exponentiation over $x^2 - ax + 1 = 0$ it is notable that:

$$(sx + t)^2 \equiv s^2x^2 + 2stx + t^2 \equiv s(sa + 2t)x + t^2 - s^2 \pmod{x^2 - ax + 1}.$$

Since a will be small the calculation of the coefficient of x is dominated by one major multiplication and modular reduction. Note that the term $t^2 - s^2$ can be expressed by $(t - s)(t+s)$ which is also dominated by one major multiplication and a modular reduction. This means that exponentiation is dominated by two major multiplications and two modular reductions per step.

This test is suggested for non-square odd n using minimal $a \geq 0$ such that $J(a^2-4, n) = -1$:

$$(x + 2)^{n+1} \equiv 2a + 5 \pmod{n, x^2 - ax + 1}.$$

This has been verified for *minimal* a for $n < 2^{50}$ [4].

The runtime may be be improved for $a > 2$ by using base $x + 1$ instead of base $x + 2$.

Chapter 20

Restricted Domain PRP Tests

20.1 Introduction

There have been many publications regarding probable prime tests over the last forty years or so since the seminal paper of Baillie, Pomerance, Selfridge and Wagstaff (BPSW) [1]. The basic idea of BPSW is to perform a strong base 2 Fermat probable prime test in conjunction with an Lucas probable prime test with carefully chosen parameters.

The BPSW test is very fast and reliable; It is $1 + 3$ Selfridges, where a Selfridge is the time taken to do a Fermat probable prime test, and to date nobody has yet claimed the $30 offered for a counterexample or a proof that none exist. In contrast, Elliptic Curve Primality Proving (ECPP) is of the order $O(log(n)^{4+\epsilon})$ for some $\epsilon > 0$.

For the Lucas component of the BPSW test, parameters are chosen from $\mathbb{Z}$ by one of two methods, one given by Selfridge and the other by Pomerance in their paper. In this chapter the domain of a parameter is restricted to 2^r or 3^r for some integer r. Then r itself is restricted after the full Lucas probable prime test is transformed into a computationally efficient Euler probable prime test plus a simple Lucas probable prime chain test. The resulting restricted domain test is $1 + 2$ Selfridges and a brief look is taken to see how a "fused" probable prime test can be performed in 2 Selfridges.

A practical algorithm is given and some statistical results are also presented.

20.2 Definitions

A Fermat probable prime (PRP) is an n for which $a^n \equiv a \bmod n$ for some a. It is called a-PRP. If $\gcd(a, n) = 1$ it can be divided by a:

$$a^{n-1} \equiv 1 \pmod{n}.$$

There are Fermat pseudoprimes (PSP) to the PRP test such as 341 which is 2-PSP. There are also Carmichael (absolute pseudoprime) numbers for which $a^n = a \bmod n$ for all bases a; For example 561.

An Euler probable prime (EPRP) is one for which $a^{\frac{n-1}{2}} \equiv J(a,n) \bmod n$, where $J(a,n)$ is the Jacobi symbol of a over n.

A *strong* Fermat probable prime (SPRP) is calculated as follows. Let $n = 2^s d+1$ where d is odd. Compute $a^d \bmod n$. If it is ± 1 declare n do be a-SPRP. Square up to $s-1$ times checking for equivalence to -1. If so declare n to be a-SPRP.

A (proper) Lucas probable prime (LPRP) is test of odd n over the quotient ring $\mathbb{Z}_n[x]/(x^2 - Px + Q)$ with a strong Jacobi symbol of the discriminant $P^2 - 4Q$ over n, i.e. equal to -1 so that the square root of the discriminant has no solution in $\mathbb{Z}_n$ which ensures the Frobenius automorphism forms the augmented solutions for x:

$$x = \frac{P \pm \sqrt{P^2 - 4Q}}{2}.$$

An LPRP is calculated thusly: $x^{n+1} \equiv Q \pmod{n, x^2 - Px + Q}$ such that $x^2 = Px - Q$ is repeatedly used to calculate powers of x, usually by a left-right binary exponentiation method. The general LPRP(n, P, Q) test has many pseudoprimes, for example LPRP(51, 17, 25). The Q value could be restricted to 2 and then test LPRP(n, P, 2), but again there are many pseudoprimes which can be found easily, for example LPRP(1387, 511, 2).

An LPRP(n, P, 1) test can be very efficiently calculated by a Lucas binary exponentiation chain and is denoted in this paper as an LPRP chain.

Define a *strong* Lucas probable prime chain (SLPRP chain) test as follows. Let $n = 2^t e - 1$ where e is odd. Calculate the chain up to the power of e. If it is ± 1 declare n to be SLPRP chain. Square the chain up to $t-1$ times further checking for a result of -1 and if this is the case declare n to be SLPRP chain.

20.3 Domain Restriction

The domain of an LPRP test has its P restricted to 2^r for integer r and Q to 2. Thus $x^2 - 2^r x + 2 = 0$ where the Jacobi symbol of the discriminant $4^r - 8$ over n is the strong value of -1. The rationale is that a smaller domain will produce fewer pseudoprimes. Given that the multiplicative order of 2 over $\mathbb{Z}_n$ is much smaller then the domain of freely varying P across $\mathbb{Z}_n$, this seems a good way to greatly reduce the number of pseudoprimes. With the aid of a few choice GCDs, shown in the next section, finding a pseudoprime is very difficult. In a later section r itself is restricted, further diminishing the domain 2^r.

20.4 Transformation

The LPRP(n, 2^r, 2) test is strengthened into a 2-EPRP test of n and a test for $z^{\frac{n+1}{2}}$ equal to the Jacobi symbol of 2 over n working modulo n and $z^2 - (\frac{4^r}{2} - 2)z + 1$. That is a 2-EPRP and an LPRP chain test. This can shown with $x^2 - Px + Q$ companion matrix

calculations:

$$\begin{pmatrix} P & -Q \\ 1 & 0 \end{pmatrix}^{n+1} = \begin{pmatrix} P^2-Q & -PQ \\ P & -Q \end{pmatrix}^{\frac{n+1}{2}} = \begin{pmatrix} \frac{P^2}{Q}-1 & -P \\ \frac{P}{Q} & -1 \end{pmatrix}^{\frac{n+1}{2}} \begin{pmatrix} Q & 0 \\ 0 & Q \end{pmatrix}^{\frac{n+1}{2}}.$$

The characteristic equation of the left hand matrix of the product (the determinant of which is 1) is $z^2 - (\frac{P^2}{Q} - 2)z + 1 = 0$.

The right hand matrix of the product raised to power of $\frac{n+1}{2}$ is equivalent $J(Q,n)Q$ mod n and dividing by Q which is assumed to be invertible mod n then $Q^{\frac{n-1}{2}} \equiv J(Q,n)$ mod n. Consequently working over $\mathbb{Z}_n[z]/(z^2 - (\frac{P^2}{Q} - 2)z + 1)$ that $z^{\frac{n+1}{2}}$ should also be equivalent to $J(Q,n)$.

With the substitution of 2^r for P and 2 for Q, note that if either $\gcd(4^r - 2, n)$ or $\gcd(4^r - 4, n)$ is not 1 then over some factor of n the quadratic polynomial $z^2 - (\frac{4^r}{2} - 2)z + 1$ would be cyclotomic, making it easier to find pseudoprimes. Also note that trivially $\gcd(2^r, n) = 1$ for odd n.

20.5 Further Domain Restriction

The domain of P has already been restricted to 2^r. As shown in the previous section it is required that $\gcd(4^r - 4, n) = 1$ and $\gcd(4^r - 2, n) = 1$, but it is known that a 2-EPRP implies $2^{n-1} - 1 \equiv 0 \bmod n$. Hence by choosing r such that $\gcd((r-1)(2r-1), n-1) \leq 3$ by the extended Euclidean algorithm $M(r-1)(2r-1) + N(n-1) \leq 3$ for some integers M and N, the domain 2^r is further reduced and the two GCDs can be replaced with $\gcd(7, n) = 1$ and $\gcd(3, n) = 1$.

20.6 Fusion into 2 Selfridges

Combining back the 2-EPRP test with the LPRP chain test for z by multiplication gives: $(2z)^{\frac{n+1}{2}} = 2 \pmod{n, z^2 - (\frac{4^r}{2} - 2)z + 1}$. It is now shown that this can be computed with 2 Selfridges.

Let $sz + t$ be the intermediate value during left-right binary exponentiation of the base $2z$. For squaring: $(sz+t)^2 = s(as+2t)z + (t-s)(t+s) \pmod{n, z^2 - az + 1}$ and multiplying by the base where the current bit is a 1 in the binary expansion: $(sz+t)(2z) = 2(as+t)z - 2s \pmod{n, z^2 - az + 1}$ where $a = \frac{4^r}{2} - 2$ which in practice is assumed to be small. Left-right exponentiation at each stage is then dominated by the two multiplications and two modular reductions i.e. s by $as + 2t \bmod n$ and $t - s$ by $t + s \bmod n$. Thus it is 2 Selfridges.

20.7 A Practical Algorithm

A practical algorithm written in PARI/GP is now given which is $1 + 2$ Selfridges:

```
{RDPRP(n)=local(r,t,k);
if(n==2||n==3||n==7,return(1));
if(n<2||n%2==0||n%3==0||n%7==0||issquare(n),return(0));
k=kronecker(2,n);
if(Mod(2,n)^((n-1)/2)!=k,return(0));
r=0;t=Mod(4,n)^r;
while(kronecker(lift(t)-8,n)!=-1||gcd((r-1)*(2*r-1),n-1)>3,r++;t*=4);
Mod(Mod(z,n),z^2-(t/2-2)*z+1)^((n+1)/2)==k;}
```

The above code is only a guide; Some trial division could be performed as well for instance. Furthermore, like the BPSW test, the 2-EPRP and LPRP chain tests can be made stronger.

20.8 Test Results

There are $118,968,378$ odd numbers in Feitsma's list of 2-PSPs $\leq 2^{64}$ [13]. Of these $63,912,692$ are 2-EPRP. No pseudoprimes were found with these against the RDPRP test.. All numbers $n \leq 5 \cdot 10^{13}$ pass the LPRP-chain(n, $\frac{4^r}{2} - 2$, 1) test for all applicable r, with and without the further GCD restriction prevoiusly given, and for the 2 Selfridge version.

By sampling Feitsma's list it was found that on average the domain of a 2-EPSP n was reduced to about $n^{0.408}$. If the GCD method with a strong discriminant were employed the domain of the exponent r itself would be reduced by a factor of about 0.16 making the domain of an LPRP chain n about $n^{0.065}$. One could say that this paper's method is about $n^{0.935}$ times better than choosing P linearly.

On the other hand the counts of 2-PSPs that are also Euler pseudoprimes and pseudoprime for LPRP(n, P, 2) with $J(P^2 - 8, n) = -1$, $\gcd(P^2 - 2, n) = 1$, $\gcd(P^2 - 4, n) = 1$, $\gcd(P, n) = 1$ and $1 \leq P \leq \frac{n-1}{2}$ are tabulated as follows, along with the expectation of the total number of pseudoprimes for any r of this paper's test and the probability of the test RDPRP failing:

Digits	#2-EPSPs	Count	$10^{0.935 \times digits}$	Lower Exp'n	Upper Exp'n	Probability
4	11	0	5495	0	0	0
5	24	26	47315	0.000549509	0.004731574	10^{-13}
6	78	98	407380	0.000240562	0.002071225	10^{-15}
7	261	312	3507518	0.000088952	0.00076587	10^{-17}
8	696	1608	30188517	0.000053246	0.000458444	10^{-19}
9	1868	15072	260015956	0.000057966	0.000499081	10^{-21}
10	4776	101630	1778279410	0.000057151	0.000390861	10^{-23}

For example for all 10 digit numbers tested with the method presented in this paper have a total expectation of between 0.000057151 and 0.000390861 pseudoprimes. Consequently a 10 digit composite number has about 10^{-23} chance of passing the test RDPRP.

If a pseudoprime is found for some r then there will be spectacularly any number between $n^{0.2}$ and $n^{0.999\ldots}$ of other r failures due to the multiplicative order of 2 modulo n.

20.9 Another Test

The domain of an LPRP test is restricted to $P = 3^r$ and $Q = -3$. Thus the test for n such that $\gcd(6, n) = 1$ is essentially

$$x^{n+1} \equiv -3 \pmod{n, x^2 - 3^r x - 3}$$

where the Jacobi symbol of the discriminant $9^r + 12$ over n is the strong value of -1, with $\gcd(r - 1, n - 1) = 1$.

The LPRP(n, 3^r, -3) test is strengthened into a base -3 EPRP test of n and a test for $z^{\frac{n+1}{2}}$ equal to the Jacobi symbol of -3 over n working modulo n and $z^2 - (\frac{9^r}{-3} - 2)z + 1$. That is a 3-EPRP and an LPRP chain test.

Consequently working over $\mathbb{Z}_n[z]/(z^2 - (\frac{P^2}{Q} - 2)z + 1)$ that $z^{\frac{n+1}{2}}$ should also be equivalent to $J(Q, n)$. Now a substitution is made of 3^r for P and -3 for Q.

We want to avoid $z^2 \pm z + 1$ in our testing because otherwise finding counterexamples becomes easier. It seems that only $z^2 - z + 1$, which has discriminant -3, needs to be avoided for $Q = -3$. Thus $z^2 - (-3^{2r-1} - 3 + 3 - 2)z + 1$ is key and $3^{2r-2} + 1 = 0$ should be avoided. That is $3^{4(r-1)} = 1$ can be avoided by taking $\gcd(r - 1, n - 1)$.

Combining back the base -3 EPRP test with the LPRP chain test for z by multiplication gives: $(-3z)^{\frac{n+1}{2}} = -3 \pmod{n, z^2 - (-3^{2r-1} - 2)z + 1}$. It is now shown that this can be computed with 2 Selfridges. Let $sz + t$ be the intermediate value during left-right binary exponentiation of the base $-3z$. For squaring: $(sz+t)^2 = s(as+2t)z+(t-s)(t+s) \pmod{n, z^2 - az + 1}$ and multiplying by the base where the current bit is a 1 in the binary expansion: $(sz + t)(-3z) = -3(as + t)z + 3s \pmod{n, z^2 - az + 1}$ where $a = -3^{2r-1} - 2$ which in practice is assumed to be small. Left-right exponentiation at each stage is then dominated by the two multiplications and two modular reductions i.e. s by $as + 2t$ mod n and $t - s$ by $t + s$ mod n. Thus it is 2 Selfridges.

Chapter 21

Beyond Quadratic

21.1 The Perrin Sequence

Perrin's sequence $3, 0, 2, 3, 2, 5, 5, 7 \ldots$ can be defined formally by initial values $P_0 = 3$, $P_1 = 0$, $P_2 = 2$ with the recurrence relation $P_n = P_{n-2} + P_{n-3}$ for $n \geq 3$.[8][9][10][11][12]

It is not shown here that each binary digit of left-right binary exponentiation of P can be calculated with 6 multiplications and respectively 6 modular reductions plus sundry additions and subtractions.

The existence of Perrin pseudoprimes has hitherto made it a poor test when compared with the quicker Baillie-PSW [1] test which has no known counterexamples, although it is believed there are infinitely many counterexamples to the Baillie-PSW test albeit each with a large number of digits.

21.2 Extending the Perrin Sequence

A novel approach is taken; For $n \geq 9$ choose a small $k : 3 \leq k \leq n$ with $x^n \not\equiv x \pmod{n, x^k - x - 1}$. With increasing k, the total number of multiplications with modular reductions for finding a suitable k after reaching t tests for a probable prime is given by $(log_2 n)\Sigma_{k=3}^{t+2} \frac{k(k+1)}{2}$ with the chance thereof $\frac{(t+2)!-1}{(t+2)!}$ for suitability.

With the above non-equivalence condition met and $x^n \pmod{n, x^k - x - 1}$ already calculated there are two required checks: (i) check $\gcd(A, n) = 1$ where A is the resulting coefficient of x^{k-1} from the exponentiation; (ii) After the inexpensive calculation $(x^n)^k \pmod{n, x^k - x - 1}$ check that $x^{kn} - x^n - 1 \equiv 0 \pmod{n, x^k - x - 1}$. Here is the function TPPPE written in the number theory package PARI/GP interpreted language [8]:

```
{
kill(x);TPPPE(n)=my(k=2,X=x);
while(X==x,k++;X=Mod(Mod(x,n),x^k-x-1)^n);
gcd(polcoef(lift(lift(X)),k-1),n)==1&&X^k-X-1==0;
}
```

Substantial testing has been done without finding a single extended pseudoprime: All: $9 \leq n \leq 10^{11}$; All of Jan Feitsma's base 2 Fermat pseudoprimes less than 2^{64} [13]; and all Perrin pseudoprimes provided by Holger Stephan at his internet website [14]; All of Jacobsen's PPPs at OEIS [15]

21.3 The General Test

For $k > 2$ let

$$f(x) = x^k - 1 - \Sigma_{i=1}^{k-2} a_i x^i$$

where the a_i are either unity or not all zeroes, so as to avoid cyclotomy. It is stipulated that $f(x)$ is not of the degenerative form where, for all i, $\gcd(k, i)|b$ for some $b > 1$.

Note that the sum of the roots is 0 and the product of the roots is a unit.

The following are valid examples:

$$x^3 - x - 1$$
$$x^4 - x - 1$$
$$x^5 - x - 1$$
$$x^5 - x^2 - 1$$
$$x^5 - x^3 - 1$$
$$x^5 - x^2 - x - 1$$
$$x^5 - x^3 - x^2 - 1$$
$$x^5 - x^3 - x^2 - x - 1$$
$$x^{12} - x^9 - x^2 - 1$$

whereas the following are invalid examples:

$$x^4 - x^2 - 1$$
$$x^6 - x^2 - 1$$
$$x^6 - x^3 - 1$$
$$x^6 - x^4 - 1$$
$$x^8 - x^2 - 1$$
$$x^8 - x^4 - 1$$
$$x^8 - x^6 - 1$$
$$x^8 - x^4 - x^2 - 1$$
$$x^8 - x^6 - x^4 - 1$$
$$x^8 - x^6 - x^4 - x^2 - 1$$

With a pseudo-primality test in mind we require for n that $x^n \not\equiv x \pmod{n, f(x)}$. As such, after exponentiation, check that the greatest common divisor of the resulting coefficient of x^{k-1} with n is 1. Secondly check that $f(x^n) \equiv 0 \pmod{n, f(x)}$.

Bibliography

[1] R. Baillie and S. S. Wagstaff, Jr., "Lucas pseudoprimes", *Mathematics of Computation*, vol. 35, pp. 1391–1417, October 1980. https://www.ams.org/journals/mcom/1980-35-152/S0025-5718-1980-0583518-6/S0025-5718-1980-0583518-6.pdf

[2] Atkin, A. O. L. "Intelligent primality test offer", *Computational Perspectives on Number Theory (D. A. Buell and J. T. Teitelbaum, eds.), Proceedings of a Conference in Honor of A. O. L. Atkin, International Press*, pp. 1–11, 1998.

[3] Grantham, J "A Frobenius Probable Prime Test With High Confidence", *eprint arXiv:1903.06823*, 1998. https://arxiv.org/pdf/1903.06823.pdf

[4] Underwood, P. "Quadratic Frobenius probable prime tests costing 2 selfridges", *eprint arXiv:1706.01265*, 2017. https://arxiv.org/pdf/1706.01265.pdf

[5] Caldwell, C. https://t5k.org/glossary/page.php?sort=JacobiSymbol

[6] PARI/GP. https://pari.math.u-bordeaux.fr/

[7] Lucas, É. (1878). "Théorie des fonctions numériques simplement périodiques". American Journal of Mathematics. The Johns Hopkins University Press. 1 (3): 197–240. American Mathematical Society. 39 (159): 255–300. http://edouardlucas.free.fr/oeuvres/Theorie_des_fonctions_simplement_periodiques.pdf

[8] Perrin, R. (1899). "Query 1484". L'Intermédiaire des Mathématiciens. 6: 76.

[9] Adams, William; Shanks, Daniel (1982). "Strong primality tests that are not sufficient". Mathematics of Computation. https://www.ams.org/journals/mcom/1982-39-159/S0025-5718-1982-0658231-9/S0025-5718-1982-0658231-9.pdf

[10] Arno, Steve (1991). "A NOTE ON PERRIN PSEUDOPRIMES". https://www.ams.org/journals/mcom/1991-56-193/S0025-5718-1991-1052083-9/S0025-5718-1991-1052083-9.pdf

[11] Grantham, J. "There are Infinitely Many Perrin Pseudoprimes". https://arxiv.org/pdf/1903.06825.pdf

[12] Stephan, H. 'Millions of Perrin pseudoprimes including a few giants". https://arxiv.org/pdf/2002.03756.pdf

[13] Feitsma, J. http://www.cecm.sfu.ca/Pseudoprimes/

[14] Stephan, H. Perrin pseudoprimes. Data Sets, Weierstrass Institute Berlin (2019), http://doi.org/10.20347/WIAS.DATA.4

[15] OIES, A013998, https://oeis.org/A013998

List of Figures