NUMBER THEORY

John O'Connor
2009/10

CONTENTS

§0 INTRODUCTION

§0.1 References

[1] R B J T Allenby and E J Redfern, *Introduction to number theory with computing* (Edward Arnold 1989)

[2] H Davenport, *The Higher Arithmetic, an introduction to Number Theory* (CUP 1st ed. 1952, 8th ed. 2006)

[3] A Baker, *A concise introduction to the theory of numbers* (CUP 1990)

§0.2 Preamble

This course examines some interesting properties of the ring **Z** of integers. The subject has been studied since the earliest times (the Babylonians and Ancient Greeks made notable contributions) and has exercised the talents of some of the greatest mathematicians (Diophantus, Fermat, Euler, Gauss, Hilbert, ...). With the widespread use of computers much of what a few years ago could be regarded as a dry academic study has come back into the mainstream of mathematics.

As G H Hardy and E M Wright wrote in the Preface to *An Introduction to the Theory of Numbers* (1938):

> *... the subject matter is so attractive that only extravagant incompetence could make it dull.*

Carl Friedrich Gauss (1777 – 1855)

> *Mathematics is the queen of the sciences and number theory is the queen of mathematics.*

Leopold Kronecker (1823 – 1891)

> *Die ganze Zahl schuf der liebe Gott, alles Übrige ist Menschenwerk.*
> [*God made the integers, all else is the work of man.*]

§1 PRIME NUMBERS

§1.1 Basic properties

Definition

A positive integer > 1 is called **prime** if it is not divisible by any positive integer other than itself or 1

Remarks

1) 0 and 1 are not regarded as primes. It is sometimes convenient to take the negative numbers –2, –3, –5, –7, ... as primes also.

2) We can locate the primes 2, 3, 5, 7, 11, 13, 17, ... by using the *Sieve of Eratosthenes* (276 BC – 195 BC).
Start with the natural numbers from 2 onwards and strike out all multiples of 2, then 3, then 5 , ... At each stage remove all multiples of the smallest number remaining. This process (for numbers < 1 000 000 say) is surprisingly efficient.

Theorem (Euclid about 300BC)

There are infinitely many prime numbers

Proof

Suppose there are only finitely many: $p_1, p_2, p_3, \dots p_n$. Then look at the number $p_1 p_2 p_3 \dots p_n + 1 = N$

Now any number is either prime or divisible by a prime (if it is composite then apply the same argument to each factor) and *N* leaves a remainder on division by $p_1, p_2, p_3, \dots p_n$.

Hence it is a prime, contradicting the original assumption. □

Definition

The **highest common factor** (or **greatest common divisor**) of a pair of positive integers *a, b* is the largest integer hcf (*a, b*) dividing both.
If hcf (*a, b*) = 1 then *a, b* are called **coprime**.

We recall the result:

The Euclidean Algorithm

The highest common factor *d* of integers *a, b* can be written in the form $d = ax + by$ for some x, y in **Z**. □

Example
The highest common factor of 123 and 456 is 3

$$\begin{array}{rr|ll}
a = & 123 & 456 & = b \\
b - 3a = & \underline{87} & \underline{369} & = 3a \\
-b + 4a = & 36 & 87 & = b - 3a \\
6b - 22a = & \underline{30} & \underline{72} & = -2b + 8a \\
-7b + 26a = & 6 & 15 & = 3b - 11a \\
 & \underline{6} & \underline{12} & = -14b + 52a \\
 & 0 & \mathbf{3} & \boldsymbol{= 17b - 63a}
\end{array}$$

Remarks

1) The proof that the algorithm works is essentially by construction, following the above example.

2) Note that to prove the Euclidean algorithm we only needed the Division algorithm to hold.

3) We note that this process is "computationally efficient". That is, its difficulty increases in proportion to the number of digits of *a, b* not in proportion to the size of *a, b*.

We use the Euclidean algorithm to prove:

The Fundamental Theorem of Arithmetic

Every positive integer can be written as a product of primes in an essentially unique way (i.e. unique up to the order of the factors).

Proof

a) It is easy to see that any number can be written as a product of primes:
If n is not prime it can be written as a product of smaller numbers. Then apply the argument to each of these smaller numbers until one is left with a product of numbers which cannot be split up further.

b) Uniqueness is the tricky bit.

Lemma

If a prime p divides a product ab then it either divides a or it divides b.

Proof

If p does not divide a then (since the only factors of p are 1 and p) hcf(a, p) = 1 and so by the Euclidean Algorithm $ax + py = 1$ for some x, y in **Z**.

Hence $abx + pby = b$ and since p divides both terms on the LHS it must divide b. □

To finish the proof of the theorem

If $N = p_1 p_2 p_3 \dots p_n = q_1 q_2 q_3 \dots q_m$ is a product of primes in two ways, then p_1 divides $q_1(q_2 q_3 \dots q_m)$ and hence either $p_1 = q_1$ or p_1 divides $q_2 q_3 \dots q_m$ and we can repeat the process to (eventually) get p_1 = some q_i .

Then cancel out these two and repeat the process to match each of the p_i s with one of the q_js.

i.e. the two factorisations are "essentially" the same. □

Remarks

1) Although the Fundamental Theorem may seem "obvious" the uniqueness property is by no means trivial. There are systems in which, although factorisation is possible, uniqueness fails.

2) The above proof shows that any ring which has a "Division Algorithm" [a can be written as $qb + r$ with $|r| < b$] and hence a Euclidean Algorithm will have unique factorisation. There are other systems in which unique factorisation holds even though they do not have a division algorithm.

3) There is a different proof of the above theorem in [1] §1.4 and in [2] §1.4.

4) Factoring numbers is in general a computationally very difficult process. Hence although for small numbers (say < 1000) finding the hcf by factorising them is OK, the Euclidean Algorithm is much easier for bigger ones.

§1.2 Some applications of Group Theory

We recall some facts from elementary group theory.

Theorem

The set of all integers in the range 1, 2, 3, ... , *n* – 1 which are coprime to *n* forms an abelian group under multiplication modulo *n*. □

This group is called U_n (the group of *units* in the ring $\mathbf{Z}_n$).
In particular, if *p* is prime then $U_n = \mathbf{Z}_p - \{0\}$.

Definition

The order of the group is called **Euler's ϕ-function**. That is, $\phi(n)$ is the number of integers in {1, 2, 3, ... , *n* – 1} which are coprime to *n*.

If *p* is prime than $\phi(p) = p - 1$.
For other numbers we may calculate $\phi(n)$ using the result:

Theorem (Euler 1760)

1) If *m, n* are coprime then $\phi(mn) = \phi(m)\phi(n)$.
2) If *p* is prime and *k* is any positive integer, then

$$\phi(p^k) = p^{k-1}(p-1) = p^k\left(1 - \frac{1}{p}\right).$$

Proof

1) By elementary ring theory, if *m, n* are coprime then $\mathbf{Z}_{mn}$ is the direct product $\mathbf{Z}_m \times \mathbf{Z}_n$. The multiplicative identity in $\mathbf{Z}_m \times \mathbf{Z}_n$ is (1, 1) and so an element (*a, b*) in $\mathbf{Z}_{mn}$ has a multiplicative inverse if and only if *a* is invertible in $\mathbf{Z}_m$ and *b* is invertible in $\mathbf{Z}_n$. Hence the number of invertible elements in $\mathbf{Z}_m \times \mathbf{Z}_n$ is $\phi(m)\phi(n)$.

2) The only elements in 1, 2, 3, ... , p^k which are not invertible modulo p^k are the p^{k-1} elements $p, 2p, 3p, \ldots, p^k - p, p^k$.
Hence $\phi(p^k) = p^k - p^{k-1}$. □

Remark

You can find direct proofs of this in [1] §3.3 and in [2] §II.4.

Example

To calculate $\phi(72)$
$72 = 2^3 3^2$ and so $\phi(72) = \phi(2^3)\phi(3^2) = 2^2(2-1)3(3-1) = 24$.

From elementary group theory recall:

Corollaries to Lagrange's Theorem

If g is an element of a finite group G the order of g divides $|G|$ and $g^{|G|} = id$. □

Applying this to U_n we deduce

Theorem (Euler again)

For any n and a coprime to n, we have $a^{\phi(n)} = 1 \pmod{n}$ □

and in particular:

Fermat's Little Theorem (Fermat 1640, proof Leibniz)

If p is prime then $a^p = a \pmod{p}$ for any integer a or $a^{p-1} = 1 \pmod{p}$ for any a coprime to p. □

Remark

Direct proofs of Fermat's Little Theorem are in [1] §3.2 and [2] II.3

Another result easy to deduce from elementary algebra is:

Wilson's Theorem (John Wilson, 1770 though Leibniz knew it earlier)

If p is prime then $(p - 1)! = -1$ modulo p.

Proof

Since $\mathbf{Z}_p$ is a field $(p - 1)!$ consists of the products of all the elements in the field. Hence every element is cancelled by its inverse except for those which are their own inverses. The only such elements are ±1. □

Remark

In fact the converse of this result is true. That is if $(p - 1)! = -1$ modulo p then p is prime.

We can use Fermat's Little Theorem to make:

Test for primality Mark I

To test whether a number n is prime or not, evaluate $a^{p-1} \pmod{p}$ for some numbers a. If the answer is not 1 then n is not prime.

Remarks

1) Some numbers do satisfy $a^{n-1} = 1 \pmod n$ without being prime. Such a number is called a *pseudo-prime wrt a*.
In fact some numbers are so perverse that they satisfy $a^n = a \pmod n$ for any a. (That is, they are pseudoprimes wrt any integer coprime to them.)
Such numbers are called *Carmichael numbers* (after R D Carmichael (1879 – 1967) who discovered them in 1909).
The smallest Carmichael number is 561 and the next one is 1729.

2) Nevertheless, the above is still a useful test for primality (or rather for non-primality) since calculating $a^k \pmod n$ is not computationally too difficult. The amount of calculation is proportional to the number of digits of k rather than to the size of k.

Method of calculating powers

To calculate $a^k \pmod n$ start with a and calculate a^2 (mod n) and then find a^4, a^8 and so on by squaring each time. Then write k in binary notation and piece together a^k from the various powers already calculated.

e.g. $2^{197} \pmod{11}$

In binary 197 = 128 + 64 + 4 + 1 and we can calculate that mod 11:
$2^2 = 4, 2^4 = 5, 2^8 = 3, 2^{16} = 9, 2^{32} = 4, 2^{64} = 5, 2^{128} = 3$ and so
$2^{197} = 3 \times 5 \times 5 \times 2 = 7 (\text{mod } 11)$

So now we'll try and improve the above test using the following.

Theorem

If p is an odd prime then the equation $x^2 = 1$ has exactly two solutions in $\mathbf{Z}_p$.

Proof

We have $x^2 - 1 = (x-1)(x+1) = 0$ if and only if one of x – 1 or x + 1 = 0 modulo p. (This is because $\mathbf{Z}_p[x]$ is an "Integral domain" for those who know what that means!) □

So now suppose we have tested whether or not n was prime as above by calculating a^{n-1} and getting 1 (modulo n). Then suppose $q = \frac{1}{2}(n-1)$ (an integer since we must have n odd) and calculate $x = a^q \pmod n$. If this is not ±1 then we would have three solutions to $x^2 = 1$ and so n could not be prime.

In fact if $a^q = +1$ and q is even, we can repeat the process by calculating $a^{q/2}$ and so on.

If we never detect that a composite number *n* is a non-prime by this process we call *n* a **strong pseudoprime wrt *a***.

Examples

$2^{560} = 1 \bmod(561)$, $2^{280} = 1 \bmod(561)$, $2^{140} = 67 \bmod(561)$ and so 561 is not prime (and although it is a pseudoprime wrt 2 it is not a strong pseudoprime).
$2^{1728} = 1 \bmod(1729)$, $2^{864} = 1$, $2^{432} = 1$, $2^{216} = 1$, $2^{108} = 1$, $2^{54} = 1065$ and so 1729 is not prime (and although it is a pseudoprime wrt 2 it is not a strong pseudoprime).

Remark

The smallest strong pseudoprime wrt 2 is 2047. There is no number $< 3 \times 10^9$ which is a strong pseudoprime wrt 2, 3, 5 and 7.

We us the above as the basis for:

Primality test Mark II

To test *n* for primeness (or non-primeness in fact!):
Divide $n - 1$ by 2 until you get an odd number *q* (say).
Then calculate (modulo *n*) $m = a^q$. If $m = \pm 1$ then *n* passes the test for *a*. If $m \neq \pm 1$ then calculate $m^2 = a^{2q}$. If this is –1 then n passes, but if it is +1 then *n* fails. If it is ≠ ±1 then square again.

Repeat the test for several different values of *a*.

Remark

This is the primality test used in Maple and other symbolic computation packages.

§1.3 Fermat and Mersenne primes

Fermat (1601 – 1663) examined integers of the form $2^k + 1$. He proved:

Theorem

If a number of the form $2^k + 1$ is prime, then $k = 2^m$ for some *m*.

Proof

Recall that $x^3 + 1 = (x+1)(x^2 - x + 1)$ and in general, if *n* is odd, $x^n + 1 = (x+1)(x^{n-1} - x^{n-2} + ... + 1)$. (Use the Remainder theorem or the sum of a GP.)

So if *k* = *ab* with *b* odd, we may put $x = 2^a$ and get $2^k + 1 = x^b + 1$ which is hence divisible by $x + 1 = 2^a + 1$. Hence if $2^k + 1$ is prime, *k* has no odd factors and must be a power of 2. □

Remarks

1) The number $2^{2^m} + 1$ is called the *m*th Fermat number F_m. The first few are: $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$ and these are prime. Fermat (1640) believed/hoped that all the F_m were prime. However, Euler (1732) proved that $F_5 = 4294967297$ is divisible by 641.

2) $F_6 = 2^{64} + 1 = 18446744073709551617 = 67280421310721 \times 274177$ In fact no other prime F_ms are known.

3) Gauss proved the amazing fact that if F_m is prime then a regular F_m-gon can be constructed by ruler-and-compass methods.

Factorising F_m is helped by the following:

Theorem (Euler)

Any prime factor of F_m is of the form $q\,2^{m+1} + 1$ for some *q*.

Proof

Suppose *p* divides F_m. Then $2^{2^m} = -1 \pmod{p}$ and so squaring gives $2^{2^{m+1}} = +1 \pmod{p}$. By Fermat's Little Theorem $2^{p-1} = 1 \pmod{p}$.

Let $d = \text{hcf}(p-1, 2^{m+1}) = (p-1)x + 2^{m+1}y$.

Then $2^d = \left(2^{p-1}\right)^x \left(2^{2^{m+1}}\right)^y = 1^x 1^y = 1 \pmod{p}$.

Now d is a power of 2, say $d = 2^k$ and since $2^{2^m} \neq 1 \pmod p$ but $2^{2^{m+1}} = 1 \pmod p$ we must have $k \geq m + 1$. i.e. $d = 2^{m+1}$.

Hence $p - 1$ is divisible by 2^{m+1} as required. □

Application

Any prime factor of $F_5 = 2^{32} + 1$ must be of the form $64k + 1$. So the possibilities are: 65, 129, 193, 257, 321, 385, 449, 513, 577, 641, ... and so ignoring those which are not prime we need only try a few before finding a factor.

Remark

The factor 274177 of F_6 mentioned above is $2142 \times 128 + 1$. The other factor is $525628291490 \times 128 + 1$

Another set of primes of great interest was studied by Mersenne (1588 – 1648).

Theorem

If $2^m - 1$ is prime then m is prime.

Proof

Note that $x - 1$ divides $x^a - 1$ and so if $m = ab$ then (put $x = 2^b$) we have $2^m - 1 = \left(2^b\right)^a - 1$ is divisible by $2^b - 1$. □

Remarks

1) The number $2^m - 1$ is called the mth Mersenne number M_m.

2) Note that M_m is not prime for all primes m.
e.g. $2^{11} - 1 = 2047 = 23 \times 89$
The values of m for which it is known that M_m is prime are: 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, ...
Mersenne himself got some of them wrong.
Lucas (1842 – 1891) proved in 1876 that M_{127} was prime. Until the computer age this was the largest known prime.

3) The set of Mersenne numbers is a popular place to look for the largest known prime. This is because there is a convenient mathematical test (Lucas 1876) to show that they are prime. There are now 47 Mersenne primes known; the latest discovered in April 2009. The largest known is $M_{43112609}$ which has 12 978 189 decimal digits.

4) One may prove a similar result about the factors of Mersenne numbers to that about the Fermat numbers above.

Theorem (Fermat 1640)

Any prime factor of $2^m - 1$ is of the form $2mk + 1$.

Proof

If a prime p divides $2^m - 1$ then $2^m \equiv 1 \pmod p$ and $2^{p-1} \equiv 1 \pmod p$ by Fermat's Little Theorem. Let d = hcf(p – 1, m) and write $d = (p - 1)x + my$. So (as before) $2^d \equiv 1 \pmod p$. Since $2^d - 1$ is divisible by p we cannot have $d = 1$ and since m is prime we must have m divides $p - 1$. Since $p - 1$ is even it follows that $2m$ divides $p - 1$. □

The Ancient Greeks were interested in:

Definition

A number is called **perfect** if it is the sum $\sigma(n)$ of all its proper divisors.

Examples

$\sigma(6) = 1 + 2 + 3 = 6$, $\sigma(28) = 1 + 2 + 4 + 7 + 14 = 28$, etc.

Theorem (Euclid c 300BC)

A number of the form $2^{m-1}(2^m - 1)$ where $2^m - 1$ is prime is a perfect number.

Proof

If $2^m - 1$ is prime then the proper divisors are:

1, 2, 4, ... , 2^{m-1} and p, $2p$, $4p$, ... , $2^{m-2}p$ and summing gives $2^m - 1 + p(2^{m-1} - 1) = 2^{m-1}p$. □

Remarks

1) The first few of this form are 6, 28, 496, 8128, 33550336, ... with m = 2, 3, 5, 7, 13, ...

2) Euler (in a posthumously published paper) proved that any *even* perfect number must be of this form.

3) It is (still) not known if there is an odd perfect number. If there is it is greater than 10^{200}.

§1.4 The distribution of primes

Primes become rarer as they get larger – roughly speaking because there are more possible divisors for a large number than for a small one.

For example:

up to 1 000 000	there are about 80 000 primes
up to 2 000 000	there are about 140 000 primes
up to 10 000 000	there are about 620 000 primes
up to 100 000 000	there are about 5 000 000 primes

In fact the way the primes are distributed is very regular. The big result is:

The Prime Number Theorem

If π(x) = # primes ≤ x then $\pi(x) \sim \dfrac{x}{\log_e x}$ where we say $a \sim b$ if $\dfrac{a}{b} \to 1$ as $x \to \infty$.

Remarks

1) This was conjectured by Gauss (1777 – 1855) and Legendre (1752 – 1833) and eventually proved in 1896 by so-called *Analytic Number Theory* by Hadamard and de la Vallée Poussin, though Erdös and Selberg found a proof in 1949 which did not use Complex Analysis.

2) Gauss and Legendre came up with different estimates of π(x).
Legendre verified experimentally that $L(x) = \dfrac{x}{\log(x) + 1.08366}$ is a "good fit" for π(x).

Gauss (in 1792 at the age of 15) defined the Logarithmic Integral $\displaystyle\int_2^x \frac{dt}{\log(t)}$ which is also a good fit for π(x).

3) Riemann connected the problem with the ζ-function (defined by $\zeta(s) = \sum \dfrac{1}{n^s}$) and more advanced study of this part of number theory involves looking at this function.

We shall prove a "weak" version of the Prime Number Theorem following the method of Chebyshev (1821 – 1894) in 1850.

A weak Prime Number Theorem

If n is large then $0.66\dfrac{n}{\log n} < \pi(n) < 1.7\dfrac{n}{\log n}$.

(Chebyshev actually proved it with better bounds: ±11%)

Proof

We look at the binomial coefficient $\binom{2n}{n} = \dfrac{2n!}{(n!)^2}$. The numerator contains the product of all the primes from n to $2n$ and none of these can be cancelled by the numbers in the denominator. Since each of primes between n and $2n$ is > n) we have $\binom{2n}{n} \geq \prod\limits_{\substack{\text{primes}\\ n<p_i<2n}} p_i > n^{\pi(2n)-\pi(n)}$.

Also $4^n = (1+1)^{2n} = 1 + ... + \binom{2n}{n} + ... + 1$ and so $4^n > \binom{2n}{n}$.

Hence $n^{\pi(2n)-\pi(n)} < 4^n$ and taking logs gives

$\log(n)(\pi(2n) - \pi(n)) < n\log(4)$ or $\pi(2n) - \pi(n) < 1.39\dfrac{n}{\log n}$.

So take (say) n > 1400 and assume by induction that $\pi(n) < 1.7\dfrac{n}{\log n}$.

Then $\pi(2n) < 1.39\dfrac{n}{\log n} + 1.7\dfrac{n}{\log n} = 3.09\dfrac{n}{\log n} <_* 1.7\dfrac{2n}{\log 2n}$ where * is equivalent to $3.09\log(2n) < 0.34\log n$ or $3.09\log 2 < 0.31\log n$ or $\log n > 6.91$ or n > 1002. Hence the result is valid for $2n$.

Now we'll do it for $2n$ + 1.

$\pi(2n+1) \leq \pi(2n) + 1 < 3.09\dfrac{n}{\log n} + 1 <_* 1.7\dfrac{2n+1}{\log(2n+1)}$ where * is:

LHS < $3.09\dfrac{n}{\log n} + 0.01\dfrac{n}{\log n} < 3.1\dfrac{n}{\log n} = A$ and

RHS > $1.7\dfrac{2n+1}{\log(2.01n)} = B$ and as above we can verify that A < B holds for n > 1359.

So our inductive step holds and we have proves half of our result.

For the other half:

Lemma

If p is prime and p^m is the largest power of p dividing $\binom{n}{k}$ then $p^m \leq n$.

Proof

e.g. $\begin{pmatrix}12\\5\end{pmatrix} = 792 = 9 \times 8 \times 11$ $\quad \begin{pmatrix}16\\5\end{pmatrix} = 1140 = 16 \times 13 \times 11 \times 5$

If p^{r_1} is the largest power of p dividing n! then (See Tutorial 3) $r_1 = \left[\dfrac{n}{p}\right] + \left[\dfrac{n}{p^2}\right] + \ldots + \left[\dfrac{n}{p^t}\right]$ where p^t is the largest power of $p \le n$.

Then if p^{r_2} is the largest power of p dividing k! and p^{r_3} is the largest power of p dividing $(n - k)$! then the largest power of p dividing $\begin{pmatrix}n\\k\end{pmatrix} = \dfrac{n!}{k!(n-k)!}$ is $\left\{\left[\dfrac{n}{p}\right] - \left[\dfrac{k}{p}\right] - \left[\dfrac{n-k}{p}\right]\right\} + \left\{\left[\dfrac{n}{p^2}\right] - \left[\dfrac{k}{p^2}\right] - \left[\dfrac{n-k}{p^2}\right]\right\} + \ldots$ and each term in { } is ≤ 1. Hence this largest power is $\le t$ and $p^t \le n$. □

Now $\begin{pmatrix}n\\k\end{pmatrix}$ is divisible by at most $\pi(n)$ primes and from the lemma, each

power of these dividing $\begin{pmatrix}n\\k\end{pmatrix}$ is $\le n$. i.e. $\begin{pmatrix}n\\k\end{pmatrix} \le n^{\pi(n)}$.

Also $(1+1)^n = 1 + \begin{pmatrix}n\\1\end{pmatrix} + \begin{pmatrix}n\\2\end{pmatrix} + \ldots + \begin{pmatrix}n\\n-1\end{pmatrix} + 1$

and so the RHS is $\le (n+1)n^{\pi(n)}$.

i.e. $2^n \le (n+1)n^{\pi(n)}$ and taking logs gives

$n \log 2 \le \log(n+1) + \pi(n)\log(n)$.

So $\pi(n) \ge \dfrac{n}{\log n}\log 2 - \dfrac{\log(n+1)}{\log n} >_* \dfrac{2}{3}\dfrac{n}{\log n}$.

* is equivalent to $3\log 2 - \dfrac{\log(n+1)}{\log n} \ge 2$ or $\dfrac{\log(n+1)}{n} \le 0.08$ which is true for $n > 200$ since $\dfrac{\log 201}{200} = 0.027$. □

Remark

Chebyshev was more careful with his estimates and hoped that methods like this would prove that $(1-\varepsilon)\dfrac{n}{\log n} < \pi(x) < (1+\varepsilon)\dfrac{n}{\log n}$ for arbitrarily small ε, but later mathematicians failed to do this.

§1.5 Factorisation

Factorisation of large numbers is still a difficult process though much progress has been made recently. (The record of about 190 digits took 5 months in 2005.)

Methods

1) *Trial division*

   Divide by all the primes up to √*n*.

   A variant is to choose a product *P* of the first few hundred primes (say) and the calculate hcf(*P, n*) using the (efficient!) Euclidean Algorithm.

2) *Fermat's method*

   Fermat used (with some success) the fact that $(x-y)(x+y)=x^2-y^2$ and so if a number can be factored (into odd factors, say) then it can be written as the difference of two squares. (Once you know *x* and *y*, it's easy!)

How to do it

To factorise $n=x^2-y^2$, start with *y* = 1 and test whether $n+y^2$ is a perfect square; then take *y* = 2, etc.

Fermat tested this by observing that only a few pairs of digits can end a perfect square and so he only needed to go further in a few cases. This is called "Sieving". Fermat's method is still used by computers, but since taking roots (even on a machine) is still a difficult process, the computer will sieve several times working modulo several different numbers and eliminate numbers which cannot be squares.

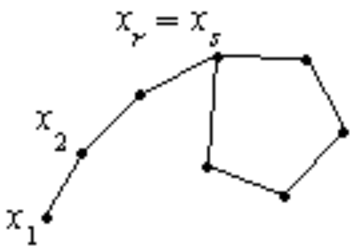
Fermat challenged the English mathematicians of his day to factorise 2027651281 = 44021 × 46061. Using his method he needed to only go as far as *y* = 1020 before finding factors.

3) *Pollard's ρ-method*

   This was introduced in 1975

   The idea is that if *p* is a factor of *n* and we choose random numbers $x_1,x_2,x_3,...$ in $\mathbf{Z}_n$ then it is more likely that $p\,|\,x_i-x_j$ than that $n\,|\,x_i-x_j$. Since one doesn't know *p* one detects this situation by taking $\mathrm{hcf}(n,x_i-x_j)$.

   In fact, iterating a formula like $f(x)=x^2+1\ (\mathrm{mod}\,n)$ generates a suitable "random" sequence. This has the advantage



that if $x_r \equiv x_s \pmod p$ then $x_{r+1} \equiv x_{s+1} \pmod p$ etc.

So the sequence becomes periodic with period *s* – *r*.

If *k* is the smallest multiple of *s* – *r* > *r* then 2*k* is also a multiple of s – r and so $x_k \equiv x_{2k} \pmod p$ and so we need only calculate $\text{hcf}(n, x_k - x_{2k})$.

This method was used in 1980 to factorise the 8th Fermat number $F_8 = 2^{256} + 1$. This is called the *ρ*-method because of the appearance of the diagram above.

Example

Take *n* = 77 (It should be easy to spot the hcf !)

i	1	2	3	4	5	6	...
x_i	2	5	26	61	26	61	...
$x_i - x_{i/2}$		3		56		35	

Note that the sequence is already periodic.

Then hcf(77, 56) = 7 and we have a factor.

4) *Other methods*

More recent methods have been developed to exploit the speed of modern computers. They include Pollard's *p* – 1 and *p* + 1 methods, the *Elliptic Curve Method*, the *Quadratic Sieve Method*, ...

The work in earlier sections showed that numbers of the form $2^m \pm 1$ had restrictions on what could be their factors. It turns out that if *n* ± 1 have convenient factorisations then some clever shortcuts may allow the factorisation of *n*. So if you want a number *n* which is difficult to factorise you should take precautions that it is not one which such methods may be able to tackle.

§1.6 Cryptography

Cryptography is a process used to conceal information from anyone not possessing "the key" to deciphering it.

In *The Dancing Men* in *The Return of Sherlock Holmes*, Holmes is able to decipher a simple substitution code and writes a letter in it to summon the criminal.

> *"If the lady is hurt as bad as you say, who was it that wrote this note?" He flung it on the table.*
> *"I wrote it to bring you here"*
> *"You wrote it? There was no one on earth outside the Joint who knew the secret of the dancing men. How came you to write it?"*
> *"What one man can invent, another can discover" said Holmes.*

With a traditional cipher system anyone who knew enough to decipher messages could, with little extra effort, determine the enciphering key. Here is a quotation from the autobiography of Casanova.

> *Five or six weeks later, she* [*Madame dUrfé*] *asked me if I had deciphered the manuscript which had the transmutation process. I told her that I had.*
> *"Without the key, sir, excuse me if I believe the thing impossible."*
> *"Do you wish me to name your key madame?"*
> *"If you please."*
> *I then told her the key word, which belonged to no language and saw her surprise. She told me this was impossible, for she believed herself the only possessor of that word which she kept in her memory and had never written down.*
> *I could have told her the truth — that the same calculation which had served me for deciphering the manuscript had enabled me to learn the word — but on a caprice it struck me to tell her that a genie had revealed it to me. That day I became master of her soul, and I abused my power. Every time I think of it, I am distressed and ashamed, and I do penance now in the obligation under which I place myself in telling the truth in writing my memoirs.*

As an application of primes and factorisation we consider the RSA (Rivest, Shamir, Adleman, 1978) public-key encryption system.

The object of this is to arrange for A (Alice) to send B (Bob) a message without an outsider who intercepts it being able to decipher it. Such methods in the past had always involved A and B arranging between themselves a method of encryption/decryption known only to them. This usually involved the swapping of "keys". Such systems in the past were *nearly always* broken.

The public-key system has the property that the encoding system that A uses to encipher her message is *public*, but *only* B can decipher it.

This is done via a "trap-door" function" (a function which is easy to calculate but whose inverse is hard to calculate). The RSA system uses the fact that it is easy to write down the product of two (prime) factors, but it is very hard to find the factors if only the product is known.

Theory

Let pq be a product of two (big) primes. Then $\mathbf{Z}_{pq} \supset U_{pq} \cong C_{p-1} \times C_{q-1}$
Let m = lcm(p – 1, q – 1). Then $x^m = 1$ for any $x \in U_{pq}$.
Choose numbers: c a coding power
d a decoding power
with cd = 1 (mod m) (using the Euclidean algorithm).
Then $x^{cd} = x$ for any $x \in U_{pq}$.
Note that $cd = 1 \pmod{p-1}$ and $\pmod{q-1}$. Then if $x \in \mathbf{Z}_{pq}$ we have $x^{p-1} = 1 \pmod{p}$ and so $x^{cd} = x \pmod{p}$. Similarly $x^{cd} = x \pmod{q}$ and so $x^{cd} = x \pmod{pq}$.
So we get two maps $\mathbf{Z}_{pq} \to \mathbf{Z}_{pq}$: coding: $x \mapsto x^c$ and decoding: $x \mapsto x^d$ which are mutually inverse.

Method

B chooses two big primes p, q and calculates $N = pq$. He calculates m = lcm(p – 1, q – 1) and chooses (at random!) a number c coprime to m, B calculates d with cd = 1 (mod m) and then destroys p, q, m and publishes N, c. He keeps d *very* safe.
Then if A wants to send a message she translates her characters into (say) ASCII code (in blocks of 3 digits). She puts all these blocks together into blocks smaller than the length of N (and not a multiple of 3 otherwise one just gets a substitution code!)

Then she (or her computer) raises each block to the power of c (mod N of course) and sends then to B.

B can recover the original message by raising each block to the power of d.

Remarks

1) Note that a public-key system gives a lot of help to a would-be cracker.

   a) The cracker has "unlimited time" to attempt the factorisation.

   b) Although factorisation is difficult, for some products it may turn out to be easy. The code-setter should apply all known algorithms to the product before releasing it — and hope that the cracker doesn't know any new ones!

2) One can be confident of the source of a message by using the system to give a "signature". Alice can put an authentication into her message by raising a message to her decoding power. Then if B raises this to Alice's coding power (public!) he can recover the message and be confident that it comes from someone who knows the decoding power. (Alice had better not use the same authentication string every time!

§2 SOME OTHER ARITHMETIC SYSTEMS

§2.1 Gaussian integers

There are some other arithmetic systems which give insight into what happens in **Z**. Here is an example.

Definition

The set of **Gaussian integers Z**[i] is the lattice of integer points in **C**.

i.e. $\mathbf{Z}[\mathrm{i}] = \{a + \mathrm{i}b \mid a,b \in \mathbf{Z}\}$

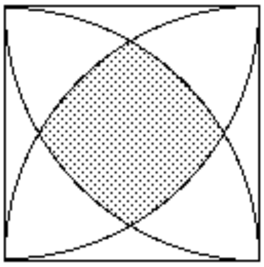
It turns out that this set has some very nice algebraic properties.

Definitions

The **norm** of a Gaussian integer $a + \mathrm{i}b$ is

$N(a + \mathrm{i}b) = |a + \mathrm{i}b|^2 = a^2 + b^2 \in \mathbf{Z}$

A Gaussian integer u **divides** a Gaussian integer v if $v = uq$ for some (quotient) $q \in \mathbf{Z}[\mathrm{i}]$.



Then we have

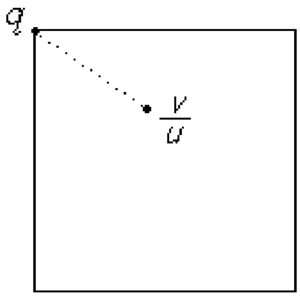
Theorem (The division algorithm for the Gaussian integers)

If $u,v \in \mathbf{Z}[\mathrm{i}]$ then $\exists\, q,r \in \mathbf{Z}[\mathrm{i}]$ (quotient/remainder) such that $v = uq + r$ with $N(r) < N(u)$.

Remark

Note that if we measure the "size" of a Gaussian integer with N this is similar to the division algorithm for **Z** where "size" of r is measured with $| r |$.

Proof



Look at $\frac{v}{u} \in \mathbf{C}$. This lies in a "cell" of the integer lattice in the complex plane. We may choose a point q of the lattice within distance 1 of $\frac{u}{v}$ and so we have $q \in \mathbf{Z}[\mathrm{i}]$ and $s = \frac{v}{u} - q$ with $| s | < 1$. Then take $r = us$ and then $N(r) = |us|^2 = |u|^2|s|^2 < |u|^2 = N(u)$. □

Remark

Note that (unlike in **Z**) the quotient q is not always uniquely determined. For example, if $\frac{u}{v}$ is in the shaded area there are *four* possible quotients within distance 1.

Definitions

The **highest common factor** hcf (or gcd) of two Gaussian integers is the largest (in Norm) Gaussian integer dividing them both.

Exactly as in the **Z** case we have the Euclidean Algorithm to determine this.

Definitions

A **unit** in **Z**[i] is an element with a multiplicative inverse. The units, for which we must have $N(u) = 1$, are the elements ±1 and ±i.

An **irreducible** or **prime** element in **Z**[i] is one which cannot be written as a product of smaller (size measured with N) ones.

Then (because we have the Euclidean algorithm) the proof of §1.1 shows that:

Theorem

Factorisation into primes in **Z**[i] is unique (up to order of factors and multiplication by units). □

Which elements of **Z**[i] are prime ?

Examples

2 is not prime since $2 = (1 + i)(1 - i)$.
5 is not prime since $5 = (2 + i)(2 - i)$.

1) If $N(u)$ is prime in **Z** then u is prime in **Z**[i].

Proof

If $u = vw$ then $N(u) = N(v)\, N(w)$ and so the norm would factor also. □

Remark

The norm of a Gaussian integer cannot be a prime of the form $4k + 3$.
You can see this by working modulo 4 where a square is either 0 or 1.

2) For a "real" or "purely imaginary" Gaussian integer: $a + 0\mathrm{i}$ or $0 + a\mathrm{i}$ to be prime we must have a a prime in $\mathbf{Z}$ and it must be of the form $4k + 3$ otherwise we could write it as a product of Gaussian integers.
This follows from the result:

Theorem (Fermat)

Any prime of the form $4k + 1$ can be written as the sum of two squares.

Proof

By Wilson's Theorem $(p - 1)! = (4k)! = -1 \pmod p$.
Now $(4k)! = 1.2.3. \ldots .2k \times (p - 2k)\ (p - 2k + 1). \ldots .(p - 1)$ and if we write $x = (2k)!$ this is $x \times (-1)^{2k} x = x^2 \pmod p$. Hence p divides $x^2 + 1 = (1 + x\mathrm{i})(1 - x\mathrm{i})$.
But p cannot divide $(1 \pm ix)$ in $\mathbf{Z}[\mathrm{i}]$ since $\frac{1}{p} \pm \frac{x\mathrm{i}}{p} \notin \mathbf{Z}[\mathrm{i}]$ and so p must be a product of non-units in $\mathbf{Z}[\mathrm{i}]$.
Then $p = (a + b\mathrm{i})(c + d\mathrm{i})$ and taking Norms we get $p^2 = (a^2 + b^2)(c^2 + d^2)$ and hence $p = a^2 + b^2 = c^2 + d^2$ is a sum of squares. □

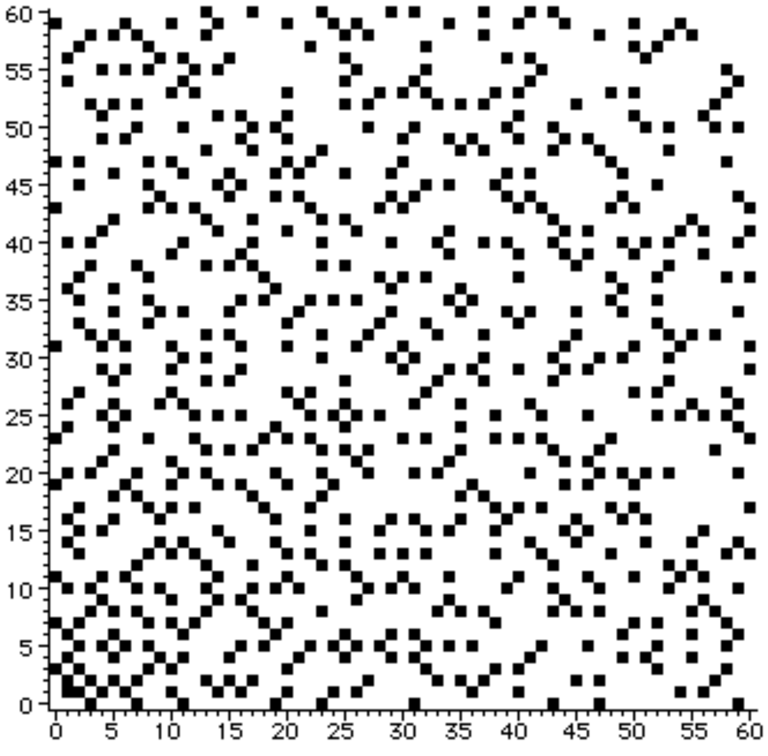
Summary

The primes in $\mathbf{Z}[\mathrm{i}]$ are:

a) $u \in \mathbf{Z}[\mathrm{i}]$ with $N(u) = 2$ or a prime of the form $4k + 1$.

b) $a + 0\mathrm{i}$ or $0 + a\mathrm{i}$ for a a prime of the form $4k + 3$.

A picture of the prime Gaussian integers in the "first quadrant"



We can now factorise numbers in **Z**[i].

Example

Factorise $u = 12 + 11i$ in **Z**[i].
$N(u) = 144 + 121 = 265 = 5 \times 53$.
Hence a factor of u must have a norm which divides $N(u)$ and so if u is a non-unit its norm must be either 5 or 53.
Since both 5 and 53 are primes of the form $4k + 1$ we can write them as sums of squares
So the possible factors of u are $1 \pm 2i$ and $7 \pm 2i$
(Factors are only determined up to multiplication by ±1 and ±i.)
Experiment with these to get
$(1 - 2i)(7 + 2i) = 11 - 12i = -i(12 + 11i)$

We can use the above to write numbers as the sum of two squares.
Writing an integer n in this form is equivalent to finding an element u in **Z**[i] with $N(u) = n$.
To find such a Gaussian integer u, observe that the norm of any factor of u must divide $N(u)$.

Method

1) Factorise n (in **Z**). Say $n = 2^{\alpha} p_1 p_2 \dots p_k q_1 q_2 \dots q_l$ where the primes $p_1, p_2, \dots$ are of the form $4k + 1$ and the primes $q_1, q_2, \dots$ are of the form $4k + 3$.
The primes of the form $4k + 3$ can only come from factors of the form $q + 0i$ or $0 + qi$ and hence these will occur as *squares* in the factorisation of $n = N(u)$.

2) Write each of the primes p_i as a sum of two squares $a^2 + b^2$ giving a factor of u of the form $a \pm bi$. (The factors of 2 are $1 \pm i$.)

3) Piece together suitable multiples of these factors to get a candidate with $N(u) = u$.

Example

To write $650 = 2 \times 5^2 \times 13$ as a sum of two squares.
i.e. Find $u \in \mathbf{Z}[i]$ with $N(u) = 650$.
Possible prime factors of u will have norms 2, 5 or 13. i.e. $1 \pm i$, $2 \pm i$, $3 \pm 2i$.

Taking combinations of (respectively) one, two and one of these will give a Gaussian integer with the correct norm and a suitable representation of *u* as a sum of squares in three ways.

$$(1+i)(2+i)(2-i)(3+2i) = 5(1+5i) = 5+25i \Rightarrow 650 = 5^2 + 25^2$$
$$(1+i)(2+i)^2(3+2i) = (1+i)(3+4i)(3+2i) = -17+19i \Rightarrow 650 = 17^2 + 19^2$$
$$(1+i)(2+i)^2(3-2i) = (1+i)(3+4i)(3-2i) = 11+23i \Rightarrow 650 = 11^2 + 23^2$$

You can verify that choosing 1 – i in place of 1 + i would give the same sums of squares.

Remark

Fermat showed that if the primes in the factorisation of *n* of the form 4*k* + 1 are $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ then the number of ways of writing *n* as a sum of *positive* squares is $\left[\frac{1}{2}(\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1)\right]$ except that if all the are even then add 1 before dividing by 2 (to allow for $n = A^2 + A^2$ or $n = A^2 + 0^2$).

e.g. $8 \times 5^3 \times 7^2 \times 13^4 \times 17 = 23791313000$ can be written as a sum of two squares in 20 ways: $153958^2 + 9394^2$, ...

§2.2 Integers in Quadratic Number Fields

Some other "subrings" of **C** (and of **R**) have some interesting number theory.

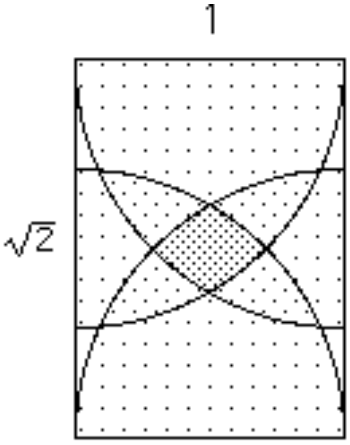
Those of the form $\left\{a + b\sqrt{d} \mid a, b \in \mathbf{Q}\right\}$ where d is a square-free integer (≠ 1) are called **Quadratic Number Fields**.

An element of one of these is called an **algebraic integer** if it satisfies an equation $x^2 + bx + c$ with $b, c \in \mathbf{Z}$.
The quadratic integers then form a subring of **R** or **C**.
We'll be most interested in the *Imaginary QNFs* where $d < 0$.

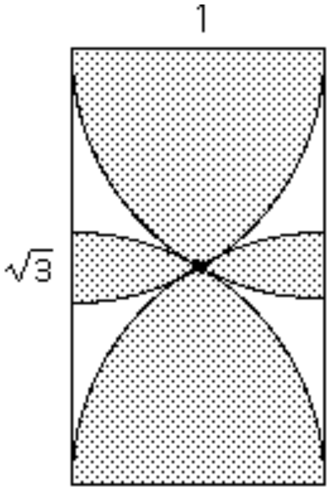
Examples

1) If $d = -1$ the quadratic integers are the Gaussian integers $\mathbf{Z}[i]$. Note that this is a ring with a division algorithm and hence a Euclidean algorithm and has unique factorisation.

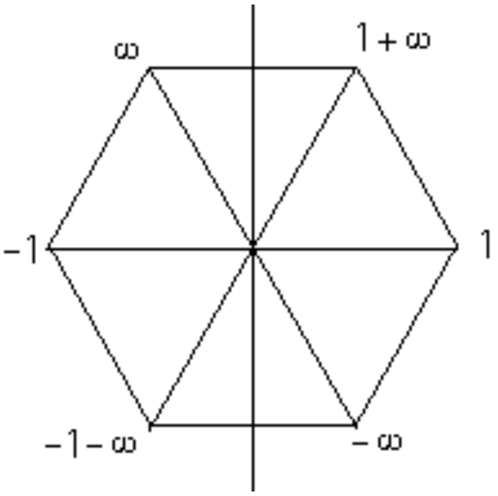
2) If $d = -2$ the quadratic integers are all of the form $a + b\sqrt{-2} \in \mathbf{Z}[\sqrt{-2}]$.
We can work as in the Gaussian integer case by taking $\frac{v}{u}$ in a "cell" and choosing a lattice point within distance 1.
As before we have a choice of quotients for some pairs.
Since we have a division algorithm we have a Euclidean algorithm and hence unique factorisation.



3) If $d = -3$ we may look at the elements of the form $a + b\sqrt{-3} \in \mathbf{Z}[\sqrt{-3}]$ but this time the method of proving the division algorithm fails because we might have $\frac{u}{v}$ right in the middle and distance exactly 1 from each lattice point.
And indeed, unique factorisation fails for this ring.



4) In fact, if d = –3 the element $\omega = \frac{1}{2}(-1+\sqrt{-3})$ is an algebraic integer and the algebraic integers are of the form $a + b\omega + c\omega^2$ where *a, b, c* are integers and ω is a cube root of 1. We write this as $\mathbf{Z}[\omega]$. These then form a lattice in **C** as shown and again we can always choose a lattice point within distance 1 of any quotient $\frac{u}{v}$.



These are sometimes called the *Eisenstein integers*.

Remarks

1) The algebraic integers in the QNF with d = ±2 or 3 (mod 4) are generated by 1 and √d; if d = 1 (mod 4) they are generated by 1 and $\frac{1}{2}(-1+\sqrt{d})$.

For d < 0 the values –1, –2, –3, –7, –11 are the only ones with a division algorithm. For d = –19, –43, –67 and –163 the rings of algebraic integers have unique factorisation. (It finally proved that these were the *only* ones in 1966.)

2) The rings of algebraic integers with d > 0 are more difficult to deal with. The formula $N(a + b\sqrt{d})$ = $a^2 - b^2 d$ gives a *norm* for the ring just as in the complex case.

Some of these rings have division algorithms and many more (nobody knows how many!) have unique factorisation.

In 1876 Lucas devised a cunning test for Mersenne primes based on **Z**[√3].

§2.3 Lagrange's four squares theorem.

This was proved by Joseph-Louis Lagrange (1736 – 1813) in 1770 following work by Euler. It had been conjectured earlier by Bachet (1581 – 1638), by Girard (1595 – 1632) and by Fermat — possibly even by Diophantus.

Theorem

Any integer can be written as a sum of four squares.

We will not prove this in the way it was originally done but instead use:

Definitions

The **quaternions** or **Hamiltonians H** are the set

$\{a + bi + cj + dk \mid a,b,c,d \in \mathbf{R}\}$

which add "like vectors" and multiply using the rules

$i^2 = j^2 = k^2 = -1 \quad ij = k = -ji$ etc.

The *norm* of an (integer) quaternion is given by

$N(a + bi + cj + dk) = a^2 + b^2 + c^2 + d^2 \in \mathbf{Z}$

As in the Gaussian integers we have $N(q_1 q_2) = N(q_1)N(q_2)$ for $q_1, q_2 \in \mathbf{H}$.

Writing an integer *n* as a sum of four squares is equivalent to finding an integer quaternion with *n* as norm and so we deduce:

Lemma 1 (Euler 1748)

If integers *m, n* are expressible as sums of four squares, so is *mn*. □

Remark

In fact $(a^2 + b^2 + c^2 + d^2)(A^2 + B^2 + C^2 + D^2) = X^2 + Y^2 + Z^2 + T^2 =$ $(aA + bB + cC + dD)^2 + (aB - bA - cD + dC)^2 + (aC + bD - cA - dB)^2 +$ $(aD - bC + cB - dA)^2$ which is what Euler discovered without knowing anything about quaternions.

Lemma 1 means we need only prove the result for primes.

Lemma 2

If *p* is an odd prime then one may write *mp* as a sum of four squares for some $0 < m < p$.

Proof

In fact we will prove that $mp = x^2 + y^2 + 1$ (a sum of three squares).
Take $q = \frac{1}{2}(p-1)$. Look at $\{x^2 \mid x = 0,1,2,\dots,q\} \subset \mathbf{Z}_p$.
This is a set of $q + 1$ distinct elements (distinct since if ${x_1}^2 = {x_2}^2$ then $x_1 = x_2$ or $x_1 = p - x_2$ and only one of these is in the "lower half" of 0, 1, 2, ... $p - 1$)
Similarly $\{-1 - y^2 \mid y = 0,1,2,\dots,q\} \subset \mathbf{Z}_p$ is a set of $q + 1$ distinct elements. Hence these sets overlap and we have $x^2 = -1 - y^2$ in $\mathbf{Z}_p$ or $x^2 + y^2 + 1$ is divisible by p and so $mp = x^2 + y^2 + 1$ for some m.
Also $x \leq q < \frac{1}{2}p$ and $y \leq q < \frac{1}{2}p$ and so $x^2 + y^2 + 1 < \frac{1}{4}p^2 + \frac{1}{4}p^2 + 1 < p^2$ and so $m < p$. □

Proof of the four squares theorem

We use the *method of descent* first introduced by Fermat to prove the theorem for an odd prime p.
We have shown that mp is a sum of four squares and we'll show that we can find a smaller multiple rp which is a sum of four squares.

We start with $mp = a^2 + b^2 + c^2 + d^2$. Reduce *a, b, c, d* mod m to get *A, B, C, D* and then we get $mr = A^2 + B^2 + C^2 + D^2$ for some r. We claim that $r < m$. As above, we can choose either A or –A so that we choose the one in the "lower half" of $\mathbf{Z}_m$ so that $A^2 \leq \frac{1}{4}m^2$ etc. So $A^2 + B^2 + C^2 + D^2 \leq m^2$.
The only time we get equality is if $A = B = C = D = \frac{1}{2}m$ in which case m is even and $a^2 = \frac{1}{4}m^2 (\mathrm{mod}\, m^2)$ and so
$a^2 + b^2 + c^2 + d^2 = m^2 (\mathrm{mod}\, m^2) = 0\ (\mathrm{mod}\, m^2)$.
But then $mp = 0\ (\mathrm{mod}\, m^2) \Rightarrow p = 0\ (\mathrm{mod}\, m)$ which is impossible since $0 < m < p$ and p is prime.
Multiply together the expressions for mp and mr as sums of four squares to get $m^2 pr = (a^2 + b^2 + c^2 + d^2)(A^2 + B^2 + C^2 + D^2)$ and use Lemma 1 to write this as $m^2 pr = X^2 + Y^2 + Z^2 + T^2$ and it is easy to check that $X = aA + bB + cC + dD = a^2 + b^2 + c^2 + d^2 (\mathrm{mod}\, m) = 0\ (\mathrm{mod}\, m)$ and that the other terms are also 0 (mod m).
So we may divide the expression $m^2 pr = X^2 + Y^2 + Z^2 + T^2$ by m^2 and we have written pr as a sum of four squares with $r < m$.
Since we cannot keep reducing r, we are led to the conclusion that the result holds with $r = 1$. □

Remarks

1) In fact one only needs four squares for integers of the form $4^m(8k+7)$ and three are enough for all the others.

2) One can generalise this result to higher powers. For example, every integer can be written as a sum of 9 cubes and of 19 fourth powers.
Edward Waring (1736 – 1798) asserted that for any number *k* there is an integer *g*(*k*) such that every number can be written as a sum of *g*(*k*) *k*th powers. This was proved by David Hilbert (1862 – 1943) in 1909.

§3 MODULAR ARITHMETIC

§3.1 Some group theory

In 1801 in *Disquisitiones Arithmeticae* Gauss invented modular arithmetic $\mathbf{Z}_n$ of residue classes modulo n under addition and multiplication modulo n and answered some of the most important questions in it.

In fact elementary group theory allows us to get some of the results more easily. Here are some results from that theory

1) A group (written multiplicatively) is **cyclic** if it consists of the powers of some element: a **generator**.
We denote the cyclic group of order n by C_n.
The group ($\mathbf{Z}_n$, +) is a cyclic group with 1 as a generator.

2) Any subgroup of a cyclic group is cyclic.

3) The **order** of an element of a group is the smallest power of that element which is equal to the identity.

4) (Lagrange's theorem) The order of any element of a finite group divides the order of the group.

5) If *m, n* are coprime then $C_{mn} \cong C_m \times C_n$

6) Any finite abelian group A can be written as a direct product $A \cong C_{a_1} \times C_{a_2} \times \ldots \times C_{a_k}$ of cyclic groups in two ways:
   a) each a_i is a power of a prime,
   b) $a_1 \mid a_2 \mid \ldots \mid a_k$.

7) If a finite cyclic group of order n has a generator g then g^k is also a generator for any k coprime to n.

§3.2 Primitive roots

Definitions

For any integer *n* the invertible elements of $\mathbf{Z}_n$ are called **units** .
An element *k* in $\mathbf{Z}_n$ is invertible if *k, n* are coprime.
The units form a subgroup $U_n \subset \mathbf{Z}_n$ of order $\phi(n)$.

e.g. $|U_8| = 4$ and $U_8 \cong C_2 \times C_2$, $|U_9| = 6$ and $U_9 \cong C_6$,

If the group U_n is cyclic then a generator of U_n is called a **primitive root** for *n*.

e.g. Since U_8 is not cyclic, 8 does not have a primitive root.
$U_9 \cong$ {1, 2, 4, 5, 7, 8} and 2 is a primitive root for 9. So is 7 = –2.

Gauss proved the most important result about primitive roots.

Theorem (Gauss 1801)

Primitive roots exist only for *n* = 2, 4, p^k or 2 p^k with *p* an odd prime.

Proof of Gauss's theorem

1) $U_2 \cong C_1$ and $U_4 \cong C_2$ so both these are cyclic.
If $n = 2^k$ with $k \geq 2$ then U_n has $U_8 \cong C_2 \times C_2$ as a subgroup and so is not cyclic by (2) of the last section.

2) If *n* is divisible by two odd primes *p, q* then U_n has $U_p \times U_q$ as a subgroup and since both U_p and U_q have even order this contains $C_2 \times C_2$ as a subgroup and cannot be cyclic. Similarly, if *n* is divisible by 4 and by an odd prime then U_n cannot be cyclic.

3) Let *p* be an odd prime. Then *p* has a primitive root.

Proof

The ring $\mathbf{Z}_p$ is a field and in any field a polynomial *P* of degree *d* can have at most *d* zeros since if *a* is a zero of *P* we may write *P* = (*x* – *a*)*Q* with *Q* a polynomial of degree *d* – 1.
Now if U_p is not cyclic we may write it as a direct product $C_{a_1} \times C_{a_2} \times \ldots \times C_{a_k}$ with $a_1 \mid a_2 \mid \ldots \mid a_k$. But then all the elements would satisfy the equation $x^{a_k} = 1$ and this would give too many solutions. □

4) Let p be an odd prime. Then p^k has a primitive root.

Proof

The ring homomorphism $\mathbf{Z}_{p^k} \to \mathbf{Z}_p$ given by x a $x \pmod{p}$ is an onto map and so maps some element to the primitive root r for p. So a suitable power of this element y (say) has order $p - 1$.
The element $z = 1 + p \in \mathbf{Z}_{p^2}$ satisfies $z^p = 1$ (by expanding by the binomial theorem and using the fact that the binomial coefficient $\binom{n}{k} = 0 \pmod{p}$ for $k > 0$). Hence this element has order p.
A similar proof shows that $z = 1 + p \in \mathbf{Z}_{p^k}$ has order p^{k-1}. (This time one needs to check that $p^{k-2} \neq 1$)
Then the product of the elements y and z has order $\phi(p^k) = p^{k-1}(p-1)$. Hence this is a primitive root. □

5) Let p be an odd prime. Then $2p^k$ has a primitive root.

Proof

Since the rings $\mathbf{Z}_2 \times \mathbf{Z}_{p^k}$ and $\mathbf{Z}_{2p^k}$ are isomorphic and $U_2 \cong C_1$, it follows that U_{p^k} and U_{2p^k} are isomorphic groups and hence are both cyclic. □

Remarks

1) There is no "good" way of finding a primitive root for a given prime. The table below gives some examples,

Root	Primes < 200 with this as smallest primitive root
2	3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83, 101, 107, 131, 139, 149, 163, 173, 179, 181, 197
3	7, 17, 31, 43, 79, 89, 113, 127, 137, 199
5	23, 47, 73, 97, 103, 157, 167, 193
6	41, 109, 151
7	71
19	191

2) If r is a primitive root for n then (7) in the last section shows how to find $\phi(\phi(n))$ of them.

3) Although it is not obvious from the proof above, if r is a primitive root for p then either r or $r + p$ is a primitive root for each p^k with $k \geq 2$.

4) If r is a primitive root for an odd prime p then for any integer $0 < n < p$ we have $n = p^k$ for some k. However, finding this k is a computationally difficult process known as the *modular logarithm problem*. This can be used as the basis of an encryption method similar to the RSA system outlined earlier.

5) Alternative proofs of the existence of primitive roots are in [2] pg 127 – 129 and [3] pg 23 – 25.

§3.3 Quadratic residues

We now consider which elements of the ring $\mathbf{Z}_n$ have square roots.

Definitions (due to Euler)

If an element s in $\mathbf{Z}_n$ is the square of some element (i.e. has a square root) it is called a **quadratic residue**. The other elements are **quadratic non-residues**.

In general, the pattern is hard to spot.
For example, in $\mathbf{Z}_{12}$ 1 and 4 have 4 square roots; 0 and 9 have two square roots and the other elements have none.
In $\mathbf{Z}_{16}$ 0, 1, 4 and 9 have 4 square roots and the other elements have none.
In $\mathbf{Z}_9$ 0 has 3 square roots; 1, 4, 7 have two and the other elements have none.

For primes things are easier.

Theorem

If p is an odd prime then *half* the elements of $\mathbf{Z}_p - \{0\}$ are quadratic residues.

Proof

The multiplicative group $\mathbf{Z}_p - \{0\}$ is cyclic with generator a primitive root r (say). Then the quadratic residues are *even* powers of r and the non-residues are the *odd* powers. □

Remark

If p is an odd prime then every quadratic residue has two square roots (±).

Corollary 1

The product of two quadratic residues or of two quadratic non-residues is a quadratic residue. The product of a residue and a non-residue is a non-residue.

Proof

Look at the powers of a primitive root. □

Example

In $\mathbf{Z}_{17}$ 3 is a primitive root. The powers of 3 are (with residues in bold):

3, **9**, –7, **–4**, 5, **–2**, –6, **–1**, –3, **–9**, 7, **4**, –5, **2**, 6, **1**

and you may verify the above corollary.

Corollary 2 (Euler's criterion)

Let p be an odd prime and $q = \frac{1}{2}(p-1)$. Then $a \in \mathbf{Z}_p - \{0\}$ is a quadratic residue if and only if $a^q = 1$ (and a non-residue if $a^q = -1$).

Proof

If a is an *even* power of the generator r then $a^q = (r^{2x})^q = (r^x)^{2q} = 1$ since $2q$ is the order of the group. □

Application

When does the equation $x^2 + 1 = 0$ have a solution modulo an odd prime?
That is, when is –1 a quadratic residue?
Answer: ⇔ $(-1)^q = 1 \pmod{p} \Leftrightarrow$ q is even ⇔ p is of the form $4k + 1$.

Remark

Euler proved this result before the idea of a primitive root was introduced.

Legendre (1752 – 1833) introduced a notation to help with calculation:

Definition

Let p be an odd prime and $a \in \mathbf{Z}_p - \{0\}$. Then the **Legendre symbol** $\left(\frac{a}{p}\right)$ is defined to be +1 if a is a quadratic residue modulo p and –1 if a is a non-residue. (Call it 0 if $a = 0 \pmod{p}$).

Remarks

1) We can now interpret the above corollaries as:

a) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$

b) If $q = \frac{1}{2}(p-1)$ then $\left(\frac{a}{p}\right) = a^q$ mod p. In particular $\left(\frac{-1}{p}\right) = (-1)^q$.

2) If r is a primitive root and $a = r^k$ for $a \in \mathbf{Z}_p - \{0\}$ then $\left(\frac{a}{p}\right) = (-1)^k$.

Here is a different way of deciding if something is a quadratic residue.

Theorem (Gauss's Lemma)

Let p be an odd prime and $q = \frac{1}{2}(p-1)$. Consider the numbers a, $2a$, $3a$, ... , qa (mod p). Let k be the number of these which are $> q$. Then a is a quadratic residue if k is even.

Example

Take $p = 17$, $q = 8$, $a = 7$

We get: 7, 14, 4, 11, 1, 8, 15, 5 and so $k = 3$ and 7 is a non-residue.

Proof

Note that the above list is 7, –3, 4, –6, 1, 8, –2, 5 and that the numbers 1, 2, ... , q occur once with either ±.

This always happens since the numbers a, $2a$, ... , qa must be distinct mod p (since a is invertible in $\mathbf{Z}_p$) and if we take these numbers to lie in the range $[-q, q]$ and we were to have (say) $ar_1 = -ar_2$ then $a(r_1 + r_2) = 0 \Rightarrow r_1 + r_2 = 0 \pmod{p}$ which can't happen since r_i is in the range $[1, q]$.

Multiplying $a \times 2a \times ... \times qa = \pm 1 \times \pm 2 \times ... \times \pm q$ with the appropriate choice of signs on the right and this is $(-1)^k q!$ Thus $a^q = (-1)^k$ and the result follows from Euler's criterion. □

Application

For which primes p is 2 a quadratic residue modulo p ?

Take $q = \frac{1}{2}(p-1)$ and we get a list: 2, 4, ... , $2q = p - 1$.

Put $p = 8k + r$ and look at the different values of r.

Answer: 2 is a residue if $r = 1$ or 7 and a non-residue if $r = 3$ or 5.

Remark

One may phrase this as $\left(\frac{2}{p}\right) = (-1)^{\frac{1}{8}(p^2-1)}$.

§3.4 The Law of Quadratic Reciprocity

This is a result which was conjectured (independently) by Euler, Legendre and Gauss and eventually proved by Gauss (the first of seven proofs in 1796, at the age of 19) "after great effort".

It connects the condition for a prime p_1 being a quadratic residue modulo a prime p_2 in terms of p_2 being a quadratic residue modulo p_1.
We can state it most conveniently using Legendre symbols.

Theorem (The Law of Quadratic Reciprocity)

Let p_1 and p_2 be distinct odd primes. Put $q_i = \frac{1}{2}(p_i - 1)$.

Then $\left(\frac{p_1}{p_2}\right)\left(\frac{p_2}{p_1}\right) = (-1)^{q_1 q_2}$.

This can be phrased as:

The quadratic character of $p_1 \pmod{p_2}$ *and* $p_2 \pmod{p_1}$ *are "the same" unless both are* 3 (mod 4) *in which case they are opposite.*

Proof

The following is a variation of a proof found by Gauss in 1808 and modified by Eisenstein (1823 – 1852).

We use the Gauss lemma to calculate $\left(\frac{p_1}{p_2}\right)$.

Write $p_1, 2p_1, \ldots, q_2 p_1$ and subtract a suitable multiple of p_2 so that each is in the range $(-q_2, q_2]$.

Then the number of minuses we get is the number of pairs $xp_1 - yp_2$ which lie in $(-q_2, 0)$ for *x* lying in the range $(0, q_2]$ (*x, y* integers).

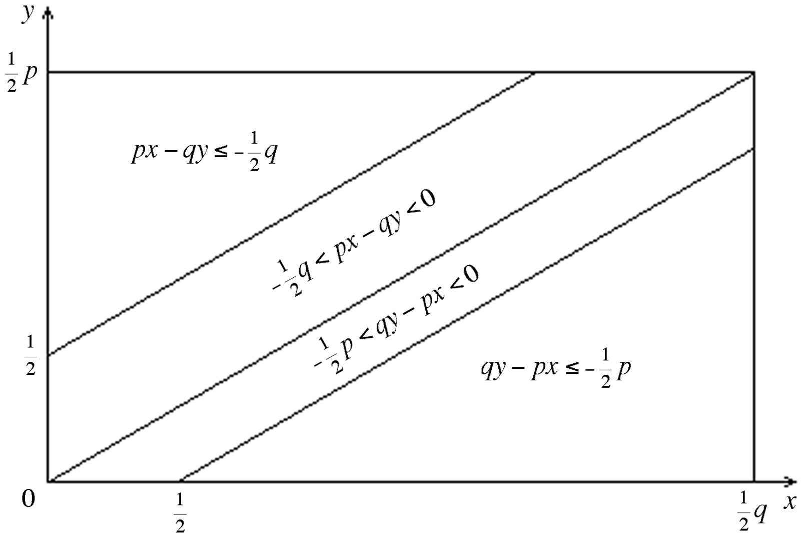
$-q_2 < xp_1 - yp_2 \Rightarrow y < x\frac{p_1}{p_2} + \frac{q_2}{p_2} < y < q_2\frac{p_1}{p_2} + \frac{q_2}{p_2} < \frac{1}{2}(p_1 + 1)$ and this is $< \frac{1}{2}p_1$ since *y* is an integer. Thus $0 < y < \frac{1}{2}p_1$.

So the number *l* of (*x, y*)s to count are the number of lattice points in the rectangle $0 < x < \frac{1}{2}p_2 \times 0 < y < \frac{1}{2}p_1$ which satisfy $-q_2 < xp_1 - yp_2 < 0$.

Then $\left(\frac{p_1}{p_2}\right) = (-1)^l$. Similarly $\left(\frac{p_2}{p_1}\right) = (-1)^m$ where m is the number of lattice points in the rectangle satisfying $-q_1 < xp_2 - yp_1 < 0$

We are trying to show that $(-1)^{q_1q_2} = (-1)^{l+m}$ or equivalently that $q_1q_2 - (l+m)$ is even.

This number is the number of lattice points in the upper and lower triangles of the diagram below.



y
$\frac{1}{2}p$
$px - qy \le -\frac{1}{2}q$
$-\frac{1}{2}q < px - qy < 0$
$-\frac{1}{2}p < qy - px < 0$
$\frac{1}{2}$
$qy - px \le -\frac{1}{2}p$
0
$\frac{1}{2}$
$\frac{1}{2}q$
x

The map $x' = \frac{1}{2}(p_2+1) - x,\ \ y' = \frac{1}{2}(p_1+1) - x$ gives a 1-1 correspondence between the top triangle and the bottom one and so the total number of lattice points is even as required.

Applications

To calculate Legendre symbols:

1) $\left(\frac{15}{71}\right) = \left(\frac{3}{71}\right)\left(\frac{5}{71}\right) = -\left(\frac{71}{3}\right)\left(\frac{71}{5}\right) = -\left(\frac{2}{3}\right)\left(\frac{1}{5}\right) = 1$ so 15 is a qr mod 71

(in fact √15 = ±21 mod 71)

2) $\left(\frac{56}{97}\right) =^{*} \left(\frac{14}{97}\right) = \left(\frac{2}{97}\right)\left(\frac{7}{97}\right) =^{**} 1\left(\frac{97}{7}\right) = \left(\frac{-1}{7}\right) =^{***} -1$

*: since we can always take out squared factors

: since $97 = 8k + 1$ *: since $\left(\frac{-1}{p}\right) = (-1)^q$

3) When is 3 a quadratic residue mod p ?

$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$ if $p = 1$ mod 4 and $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right)$ if $p = 3$ mod 4.

The only quadratic residue mod 3 is 1 so

$\left(\frac{3}{p}\right) = 1$ if $p = 1$ (mod 4) and 1 (mod 3) $\Leftrightarrow p = 1$ (mod 12)

or if $p = 3 \pmod 4$ and $2 \pmod 3$ $\Leftrightarrow p = 11 \pmod{12}$
i.e. $p = \pm 1 \pmod{12}$

§3.5 Square roots modulo non-primes

As seen earlier, working modulo non-primes, a number may have more than two square roots.

Theorem

Let $a \in \mathbf{Z}_n$ with $n = p_1^{s_1} p_2^{s_2} \dots p_k^{s_k}$ a product of distinct prime powers. Then a has a square root if and only if a has a square root modulo each $p_i^{s_i}$.

If a has m_i roots modulo $p_i^{s_i}$ then it has $m_1 m_2 \dots m_k$ roots modulo n.

Proof

Use the Chinese remainder theorem to reduce the problem to one modulo each $p_i^{s_i}$. □

Example

Let $n = 30 = 2 \times 3 \times 5$.

Then 15 has one square root (= 1) mod 2 and one root (= 0) mod 3 and mod 5. Hence it has one root (= 15) mod 30

By contrast 19 has one square root (= 1) mod 2 and two roots (= ±1) mod 3 and two roots (= ±2) mod 5. Hence it has four roots (= ±7, ±13) mod 30.

The problem of determining if a has a root modulo an odd prime power is made easier by:

Theorem

Let p be an odd prime. The element a ($\neq 0 \bmod p$) has a square root modulo p^k if and only if it has a square root modulo p.

Proof

If $x^2 = a \pmod{p^k}$ then clearly $x^2 = a \pmod p$.

For the converse, if a has a root mod p put $y^2 = a \pmod p$ and then put $x = y + bp$ and solve $x^2 = a \pmod{p^2}$. This is $(y+bp)^2 = y^2 + 2bpy + b^2p^2 = a$ or $2bpy = a - y^2 \pmod{p^2}$ and we can solve this for bp since $2y$ and p are coprime.

Similarly we may start with a root modulo p^2 find a root modulo p^3 etc.

□

Remark

The number of square roots modulo a prime power is not obvious. For example modulo 27 the element 9 has six square roots (±3, ±6, ±12).

There is a generalisation of the Legendre symbol which is helpful in calculation.

Definition

Let *a, n* be coprime where $n = p_1 p_2 \dots p_k$ is a product of (not necessarily distinct) odd primes.

Then the **Jacobi symbol** is $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right)$.

Remarks

1) If *n* is an odd prime this coincides with the Legendre symbol.

2) If $\left(\frac{a}{n}\right) = 1$ then it does *not* necessarily follow that *a* has a square root modulo *n*. For example $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = -1 \times -1 = 1$ but 2 has no square root mod 15. However if $\left(\frac{a}{n}\right) = -1$ then *a* has no square root.

The following may be deduced from the results for Legendre symbols.

Properties

1) If *a, b* are coprime to the odd *n* then $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$.

2) If *a* is are coprime to the odd *m*, *n* then $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$.

3) $\left(\frac{-1}{n}\right) = (-1)^{\frac{1}{2}(n-1)}$; $\left(\frac{2}{n}\right) = (-1)^{\frac{1}{8}(n^2-1)}$

4) (*Quadratic reciprocity*)

If *m, n* are coprime then $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{1}{4}(m-1)(n-1)}$.

Example

1) $\left(\frac{11}{27}\right) = \left(\frac{11}{3}\right)^3 = \left(\frac{2}{3}\right)^3 = (-1)^3 = -1$ and so 11 has no square root mod 27

2) The Jacobi symbol may be used to calculate Legendre symbols

$$\left(\frac{335}{2999}\right) = -\left(\frac{2999}{355}\right) = -\left(\frac{-16}{355}\right) = -\left(\frac{-1}{355}\right) = -(-1)^{117} = 1$$

Hence (since 2999 is a prime) this Legendre symbol is +1 and so 335 is a quadratic residue ($\sqrt{335} = \pm 1001 \pmod{2999}$)

Remark

Although the above methods do not construct square roots there are computationally efficient ways to do so.

§4 CONTINUED FRACTIONS

§4.1 Introduction

Definition

You can think of calculating the decimal expansion of a (positive) real number as the result of implementing the algorithm:

(*) Make a note of the integer part of the number. Subtract this from the number. This gives a number x in the range $[0,1)$. If $x \neq 0$ then:

** *Multiply x by* 10 **

This (perhaps) gives a number ≥ 1. Now repeat the loop from (*).

We can replace the step at ** ... ** by anything else that makes x bigger.

In particular, if we put in:

** *Take the reciprocal* $\frac{1}{x}$ *of* x **

then we get the **Continued fraction expansion** of x.

Example

For example, if you start with $\frac{424}{37}$ then you get $\frac{424}{37} = 11 + \cfrac{1}{2+\cfrac{1}{5+\cfrac{1}{1+\frac{1}{2}}}}$

which is written $\frac{424}{37} = 11 + \frac{1}{2+}\frac{1}{5+}\frac{1}{1+}\frac{1}{2}$ or as [11; 2, 5, 1, 2].

If you have a calculator with a **1/*x*** key, you can experiment with this.

One can see that this is related to the calculation of the hcf of two numbers by the Euclidean algorithm.

$$\begin{array}{rclcl}
424 & = & 37 \times 11 & + & 17 \\
37 & = & 17 \times 2 & + & 3 \\
17 & = & 3 \times 5 & + & 2 \\
3 & = & 2 \times 1 & + & 1 \\
2 & = & 2 \times 1 & + & 0
\end{array}$$

One can rewrite this as:

$$\frac{424}{37}=11+\frac{17}{37}=11+\cfrac{1}{\frac{37}{17}}=11+\cfrac{1}{2+\frac{3}{17}}=11+\cfrac{1}{2+\cfrac{1}{\frac{17}{3}}}=11+\cfrac{1}{2+\cfrac{1}{5+\frac{2}{3}}}$$

$$=11+\cfrac{1}{2+\cfrac{1}{5+\cfrac{1}{\frac{3}{2}}}}=11+\cfrac{1}{2+\cfrac{1}{5+\cfrac{1}{1+\frac{1}{2}}}}$$

In general given $\lambda \in \mathbf{R}$ start with $a_0=[\lambda]$ (integer part) and then if $a_0 \neq \lambda$ write $\lambda = a_0 + \frac{1}{\lambda_1}$ and $a_1=[\lambda_1]$ then if $a_1 \neq \lambda_1$ we take $\lambda_1 = a_1 + \frac{1}{\lambda_2}$ etc.

Definition

The integers a_i are called the **partial quotients**. The real numbers λ_i are called the **complete quotients**.

The argument with the Euclidean algorithm above shows that every *rational number* has a continued fraction expansion $[a_0;\ a_1, a_2, \ldots, a_n]$ which terminates after a finite number of steps. The expansion is unique except that if the last partial quotient a_n = 1 then we may combine it with the previous one.

In exactly the same way, we may define the continued expansion of an *irrational number* and in this case we get an expansion with an *infinite* number of terms.

Examples

If we apply the above process to some well-known irrationals we get:

$\phi = \frac{\sqrt{5}-1}{2}$ = 1.618034 ... = [1; 1, 1, 1, 1, ...]

√2 = 1.414214 ... = [1; 2, 2, 2, 2, ...]

π = 3.141593 ... = [3; 7, 15, 1, 292, 1, 1, 1, 2, ...]

e = 2.718282 ... = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, 1, 1, ...]

Euler discovered this last result and also:

$\frac{e^2-1}{e^2+1}$ = 0.761594 ... = [0; 1, 3, 5, 7, 9, 11, ...]

Just as one can approximate a real number by truncating its decimal expansion, one can approximate a number given by a continued fraction by truncating its continued fraction expansion.

Definition

If a (positive) real number λ has a continued fraction expansion $[a_0;\ a_1, a_2, a_3, \ldots]$ then the rational numbers

$C_n = \dfrac{p_n}{q_n} = [a_0;\ a_1, a_2, \ldots, a_n]$ for $n \geq 0$ are called the **convergents** of λ.

We can calculate the convergents recursively.

Theorem

The convergents $C_n = \dfrac{p_n}{q_n}$ of $[a_0;\ a_1, a_2, a_3, \ldots]$ satisfy

$p_0 = a_0,\ q_0 = 1,\ p_1 = a_0 a_1 + 1,\ q_1 = a_1$ and then

$p_n = a_n p_{n-1} + p_{n-2},\ q_n = a_n q_{n-1} + q_{n-2}$ for $n \geq 2$.

Proof

It is easy to check that $C_n = \dfrac{p_n}{q_n}$ is as claimed for $n = 0, 1$.

Then by induction assume the recurrence holds for k.

Then $C_{k+1} = [a_0;\ a_1, a_2, \ldots, a_k, a_{k+1}] = [a_0;\ a_1, a_2, \ldots, a_k + 1/a_{k+1}]$

$$= \frac{(a_k + 1/a_{k+1})p_{k-1} + p_{k-2}}{(a_k + 1/a_{k+1})q_{k-1} + q_{k-2}} = \frac{a_{k+1}(a_k p_{k-1} + p_{k-2}) + p_{k-1}}{a_{k+1}(a_k q_{k-1} + q_{k-2}) + q_{k-1}} = \frac{a_{k+1} p_k + p_{k-1}}{a_{k+1} q_k + q_{k-1}}$$

which is what the recurrence relation gives with $n = k + 1$. □

Remark

Note that the numerators and denominators both satisfy the same recurrence relation, similar to that defining the Fibonacci numbers.

Examples

1) The convergents of the continued fraction: [1; 1, 1, 1, 1, ...] are $\frac{1}{1}, \frac{2}{1}, \frac{2+1}{1+1} = \frac{3}{2}, \frac{3+2}{2+1} = \frac{5}{3}, \frac{5+3}{3+2} = \frac{8}{5}, \frac{8+5}{5+3} = \frac{13}{8}, \ldots$ It is well-known that the ratios of successive Fibonacci numbers converge to $\phi = \frac{\sqrt{5}+1}{2}$.

2) The convergents of the continued fraction [3; 7, 15, 1, 292, 1, 1, 1, 2, ...] calculated for π are $\frac{3}{1}, \frac{22}{7}, \frac{15 \times 22 + 11}{15 \times 7 + 1} = \frac{333}{106}, \frac{333+22}{106+7} = \frac{355}{113}, \ldots$ which have decimal approximations: 3, 3.142857... , 3.141509... , 3.141592... , ...

3) The convergents of our first (rational) example [11; 2, 5, 1, 2] are $\frac{11}{1}, \frac{23}{2}, \frac{5 \times 23 + 11}{5 \times 2 + 1} = \frac{126}{11}, \frac{126+23}{11+2} = \frac{149}{13}, \frac{2 \times 149 + 126}{2 \times 13 + 11} = \frac{424}{37}$ which finishes with the number we started with.

Remarks

1) We will see later that the sequence of convergents of the continued fraction of an irrational λ does indeed converge to λ.

2) The numbers p_n and q_n whose ratios are the convergents are coprime.

3) The numbers q_n increase as n increases.

4) What we are considering are sometimes called simple continued fractions to distinguish them from the more general $a_0 + \frac{a_1}{b_1 +} \frac{a_2}{b_2 +} \frac{a_3}{b_3 +} \ldots$.

5) MAPLE has a command: `convert(expr, confrac)` which produces continued fractions. Use the Help to find out how to get the convergents.

§4.2 Approximating real numbers with rationals.

The easiest way of approximating a real number λ by a rational $\frac{p}{q}$ is to divide up the real line into segments of length $\frac{1}{q}$ and take the nearest multiple of this to λ. One can then be sure that $\left|\lambda - \frac{p}{q}\right| \le \frac{1}{2q}$.

For example one may approximate π by $\frac{3142}{1000}$ to better that $\frac{1}{2000}$.

Dirichlet proved one could do better than this.

Theorem

Given any real number λ and integer Q one can find a rational $\frac{p}{q}$ with $q < Q$ such that $\left|\lambda - \frac{p}{q}\right| \le \frac{1}{q^2}$.

Proof

We use the "pigeon-hole principle": With n pigeonholes and $n+1$ pigeons, at least one hole contains more than one pigeon.

Consider the $Q + 1$ points in the interval [0, 1] given by: 0, $\{\lambda\}$, $\{2\lambda\}$, ... $\{(Q - 1)\lambda\}$, 1 where { } means the fractional part.

Divide up the unit interval into Q intervals of length $\frac{1}{Q}$ and we deduce that two of these must lie in the same sub-interval.

That is $|\{q_1\lambda\} - \{q_2\lambda\}| < \frac{1}{Q}$. Hence for some integers p, q we must have $|q\lambda - p| < \frac{1}{Q}$ and so $\left|\lambda - \frac{p}{q}\right| < \frac{1}{qQ} < \frac{1}{q^2}$. □

Remark

This is only an existence theorem. To find such an approximation we will use continued fractions.

We start by deducing a corollary of the theorem of the last section.

Corollary

The convergents C_n satisfy $C_{n-1} - C_n = \dfrac{(-1)^n}{q_{n-1}q_n}$.

Proof

Using the above recurrence relations for p_n and q_n and induction we may prove $p_{n-1}q_n - p_n q_{n-1} = (-1)^n$ .Then divide by $q_{n-1}q_n$. □

From the definition above $\lambda = [a_0;\ a_1, a_2, \ldots, a_{n-1}, \lambda_n]$ with $0 < a_n \le \lambda_n$ and so $0 < \dfrac{1}{\lambda_n} \le \dfrac{1}{a_n}$ and λ lies between C_{n-1} and C_n.

Thus λ is closer than $\dfrac{1}{{q_n}^2}$ to C_n as claimed earlier.

Remarks

1) Note that from the above corollary, the convergents are alternately larger (C_{odd}) and smaller (C_{even}) than λ .

2) In fact one may show that the sequence (C_{odd}) is monotonic decreasing and the sequence (C_{even}) is monotonic increasing. (Both of course converge to λ.) Thus the sequence of convergents alternately underestimate and overestimate the final limit.

3) In fact one may show that the convergent $C_n = \dfrac{p_n}{q_n}$ approximates λ better than any rational number with a denominator smaller than q_n and so the approximations arising from continued fractions are in a sense best possible.

§4.3 Continued fractions of square roots

It turns out that the square root of any integer has a *periodic* continued fraction (cf example 2 of §4.01).

Another example

Start with √7.

$$\lambda_0 = \lambda = \sqrt{7} \qquad a_0 = [\lambda_0] = 2$$

$$\lambda_1 = \frac{1}{\sqrt{7}-2} = \frac{\sqrt{7}+2}{3} \qquad a_1 = [\lambda_1] = 1$$

$$\lambda_2 = \frac{3}{\sqrt{7}-1} = \frac{3(\sqrt{7}+1)}{6} = \frac{\sqrt{7}+1}{2} \qquad a_2 = [\lambda_2] = 1$$

$$\lambda_3 = \frac{2}{\sqrt{7}-1} = \frac{2(\sqrt{7}+1)}{6} = \frac{\sqrt{7}+1}{3} \qquad a_3 = [\lambda_3] = 1$$

$$\lambda_4 = \frac{3}{\sqrt{7}-2} = \frac{3(\sqrt{7}+2)}{3} = \sqrt{7}+2 \qquad a_4 = [\lambda_4] = 4$$

$\lambda_5 = \frac{1}{\sqrt{7}-2} = \lambda_1$ and the process then repeats itself.

In general the continued fraction of a square root of an integer is of the form $[a_0;\ a_1, a_2, \ldots, a_k, a_1, a_2, \ldots, a_k, \ldots]$ which we write as $\left[a_0;\ \overline{a_1, \ldots, a_k}\ \right]$.

Remarks

1) The periodic part of the continued fraction of √*N* starts at a_1.

2) The periodic part has a very specific symmetrical form. In fact $a_1, a_2, \ldots, a_k$ always has the form $a_1, a_2, \ldots, a_2, a_1, 2a_0$.
e.g. $\sqrt{19} = \left[4;\ \overline{2,1,3,1,2,8}\right]$ $\qquad \sqrt{103} = \left[10;\ \overline{6,1,2,1,1,9,1,1,2,1,6,20}\right]$

3) As above, each λ_n reduces to $\dfrac{\sqrt{N}+r_n}{s_n}$ and in fact the numbers r_n, s_n satisfy $r_n = a_{n-1} - r_{n-1}$ and $s_n = \dfrac{N - {r_n}^2}{s_{n-1}}$.

4) More generally any *quadratic irrational* of the form $\dfrac{\sqrt{a}+b}{c}$ with *a, b* and *c* integers and *a* not a square, has a periodic continued fraction (not necessarily starting at the beginning) *and conversely.*

Examples

1) We showed earlier that the continued fraction of $\phi = \frac{\sqrt{5}+1}{2}$ is $[1;\ 1, 1, \ldots]$.

2) $\lambda = [3;\ 3, 3, 3, 3, \ldots]$

Then $\lambda = 3 + \cfrac{1}{3 + \cfrac{1}{3 + \ldots}} = 3 + \frac{1}{\lambda}$ and so $\lambda^2 - 3\lambda - 1 = 0$ and so $\lambda = \frac{3+\sqrt{13}}{2}$

.

3) $\lambda = [0;\ 3, 2, 3, 2, \ldots]$

Then $\lambda = \cfrac{1}{3 + \cfrac{1}{2+\lambda}} = \frac{2+\lambda}{7+3\lambda}$ and so $3\lambda^2 + 6\lambda - 2 = 0$ and so $\lambda = \frac{\sqrt{15}-3}{3}$.

§4.4 Pell's equation

This is the equation $x^2 - dy^2 = 1$ over the integers (*d* not a perfect square).

It was called Pell's equation by Euler as a result of a misunderstanding of work by Wallis and Brouncker. In fact it had been studied earlier by Fermat and much earlier by the Indian mathematicians Brahmagupta and Bhaskara. One can indeed trace it back to work by Archimedes on approximating square roots.

Examples

$d = 2$ Solutions are (1, 0), (3, 2), (17, 12), (99,70), ...

$d = 5$ Solutions are (1, 0), (9, 4), (161, 72), (2889,1292), ...

Brahmagupta (628 AD) looked at $d = 83$

Solutions are (1, 0), (82, 9), (13447, 1476), (2205226, 242055), ...

Remarks

1) Recall (§2. 2) that if $d > 0$ the norm of $x + y\sqrt{d}$ in $\mathbf{Z}[\sqrt{d}]$ is $x^2 - dy^2$ and the norm satisfies $N(uv) = N(u)\,N(v)$. So if (x, y) is a solution of Pell's equation then $x + y\sqrt{d}$ has norm 1 and so do all its powers. This allows us to generate an infinite number of solutions from a "fundamental" one. For example, if $d = 5$ the smallest non-trivial solution gives us $9 + 4\sqrt{5}$ whose square is $161 + 72\sqrt{5}$ giving the next solution. Its cube is $2889 + 1292\sqrt{5}$ and so on.

2) It follows from the above that if (x_i, y_i) are the solutions of Pell's equation then the x_i satisfy a recurrence relation of the form $x_i = rx_{i-1} - x_{i-2}$ where $r = 2x_1$. The y_i satisfy a similar one.

We can find the fundamental solution to the equation using the continued fraction expansion of √*d*.

Theorem

If the continued fraction expansion of √*d* is $\left[a_0;\ \overline{a_1, \ldots, a_k}\ \right]$ then the convergent $\frac{p_{k-1}}{q_{k-1}} = C_{k-1}$ corresponding to the penultimate term of the first periodic block gives the fundamental solution (p_{k-1}, q_{k-1}) of the equation $x^2 - dy^2 = (-1)^k$.

So if *k* is even this is a solution of Pell's equation. If *k* is odd then we need to go to the last but one convergent of the *next* block.

In both cases all the penultimate convergents of the rest of the blocks give solutions of $x^2 - dy^2 = \pm 1$. □

Example

Let $d = 7$

From above we have √7 = [2; 1, 1, 1, 4, 1, 1, 1, 4, ...] so $k = 4$ and (after a little calculation) the convergents are: $C_0, C_1, \ldots =$

$$\frac{2}{1}, \frac{3}{1}, \frac{5}{2}, \frac{5+3}{2+1} = \frac{8}{3}, \frac{4\times 8+5}{4\times 3+2} = \frac{37}{14}, \frac{37+8}{14+3} = \frac{45}{17}, \frac{45+37}{17+14} = \frac{82}{31}, \frac{82+45}{31+17} = \frac{127}{48}, \ldots$$

and the solutions of $x^2 - 7y^2 = 1$ come from the 3rd, 7th, ... convergents and are: (8, 3), (127, 48), ...

Note that $\left(8+3\sqrt{7}\right)^2 = 127 + 48\sqrt{7}$ as in Remark 1) above.

Let $d = 10$

Then √10 = [3; 6, 6, 6, ...] so $k = 1$ and the convergents are

$$\frac{3}{1}, \frac{19}{6}, \frac{6\times 19+3}{6\times 6+1} = \frac{117}{37}, \frac{6\times 117+19}{6\times 37+6} = \frac{721}{228}, \ldots$$

The 0th convergent gives a solution of $x^2 - 10y^2 = -1$ and we need the next (19, 6) to get a solution of Pell's equation.

(117, 37) satisfies $x^2 - 10y^2 = -1$ while (721, 228) is a solution of Pell's equation.

Note that $\left(19+6\sqrt{10}\right)^2 = 721 + 228\sqrt{10}$

Brahmagupta's example: $d = 83$

Then √83 = [9; 9, 18, 9, 18, ...] so $k = 2$ and the convergents are

$$\frac{9}{1}, \frac{82}{9}, \frac{18\times 82+9}{18\times 9+1} = \frac{1485}{163}, \frac{9\times 1485+82}{9\times 163+9} = \frac{13447}{1476}, \ldots$$

giving the solutions mentioned above.

Note that $\left(82+9\sqrt{83}\right)^2 = 13447 + 1476\sqrt{83}$ as usual.

Remark

You can find a proof of this last theorem in [2] pg 108 and in [3] pg 75.

§5 DIOPHANTINE EQUATIONS

§5.1 Linear equations

A *Diophantine equation* is one with integer solutions. It is named after Diophantus of Alexandria (see the exercise below).

We start with linear equations.

Theorem

A Diophantine equation $ax + by = c$ (to be solved for x, y) has a solution if and only if $d = \text{hcf}(a, b)$ divides c.

Proof

Since d divides a and b it divides $ax + by = c$ and so the condition is necessary.
Conversely, if $c = md$ then use the Euclidean algorithm to write $d = pa + qb$ and then $x = mp, y = mq$ is a solution. □

Remarks

1) Since the p, q in the above proof are not uniquely determined, if the equation has a solution it will have infinitely many.

2) A similar result holds for equations in more than two variables.

3) Diophantus would only have been interested in *positive* solutions. Then the problem is much harder.
For example, J J Sylvester (1814 – 1897) sent the following puzzle to the *Educational Times.*

> *I have a large number of stamps to the value of* 5*d and* 17*d only. What is the largest denomination which I cannot make up with a combination of these two different values?*

§5.2 Higher order equations

Here the problem is much harder. Finding the integer solutions of a general polynomial equation or even deciding whether such a solution exists is in general very difficult.

One may sometimes prove results about non-existence using modular arithmetic.

Example

A numerical search for solutions of $2x^2 + 3y^2 = z^2$ suggests that there is no non-zero solution. Working modulo 3 should convince you of this fact!

One quadratic case has attracted more attention than others - even going back to the Ancient Egyptians and Babylonians.

Definition

A **Pythagorean triple** (*x, y, z*) satisfies $x^2 + y^2 = z^2$.

We can characterise all such solutions.

Theorem

If (*x, y, z*) are coprime integers satisfying $x^2 + y^2 = z^2$ with (say) *y* even, then $x = a^2 - b^2$, $y = 2ab$, $z = a^2 + b^2$ for some integers *a, b*.

Proof

Note that $(a^2 - b^2)^2 + 4a^2b^2 = (a^2 + b^2)^2$ and so we get a solution starting with any *a, b*.

To see that such *a, b* exist, write the equation in the form $y^2 = z^2 - x^2 = (z + x)(z - x)$. Since *x, z* are coprime it follows that that $\text{hcf}(z + x,\ z - x) = 2$ and the other prime factors of *x* – *z* and *x* + *z* must be squared. Hence $x - z = 2a^2$, $x + z = 2b^2$ as required. □

§5.3 Fermat's Last Theorem

Fermat (1636) wrote in his copy of Diophantus's *Arithmetica* (in the section dealing with Pythagorean triples):

> *It is impossible to separate a cube into two cubes, a biquadrate into two biquadrates or in general any power beyond the second into two powers of the same degree. I have discovered a truly remarkable proof of this which this margin is too small to contain.*

That is: $x^n + y^n = z^n$ with $n > 2$ has no solution in integers.

Fermat gave the proof for $n = 4$; Euler proved (though incompletely) the case $n = 3$ (in 1770), Dirichlet and Legendre did $n = 5$ in 1820 and Lamé proved it for $n = 7$ in 1839.

Gauss gave a proof for $n = 3$ which used $\mathbf{Z}[\omega]$:
If $x^3 + y^3 = z^3$, factorise the LHS: $(x+y)(x+\omega y)(x+\omega^2 y) = z^3$ and use the unique factorisation property in $\mathbf{Z}[\omega]$ to prove the result.

Lamé (in 1847) thought he had a proof using $\mathbf{Z}[\zeta, \zeta^2, \ldots, \zeta^{p-1}]$ with ζ a pth root of 1 but unfortunately the proof required this ring to have the unique factorisation property (which it doesn't if $p \geq 23$).

Fermat's Last Theorem was finally proved by Andrew Wiles in 1994 using methods which would certainly not have been available to Fermat.

Here is Fermat's proof for the case $n = 4$. It uses the "Method of descent". In fact it proves a slightly stronger result.

Theorem

There is no positive integer solution to the equation $x^4 + y^4 = z^2$.

Proof

If we are given a smallest such solution, then (x^2, y^2, z) is a Pythagorean triple with (say) y even and so $x^2 = a^2 - b^2$, $y^2 = 2ab$, $z = a^2 + b^2$.
Now b must be even since if a were even and b odd then we would have $x^2 = -1 \pmod 4$ which is impossible.
Then (x, b, a) is a Pythagorean triple and we have
$x = c^2 - d^2$, $b = 2cd$, $a = c^2 + d^2$. Then $y^2 = 4cd(c^2 + d^2)$

Since $c^2, d^2, c^2 + d^2$ are pairwise coprime we have $c = e^2$, $d = f^2$, $c^2 + d^2 = g^2$ for integers *e, f, g*.

Thus $e^4 + f^4 = g^2$ and $g \le g^2 = a \le a^2 < z$ and we get a contradiction to the assumption that we had started with the smallest solution. □

§6 QUADRATIC FORMS

The problem of writing an integer as a sum of squares $n = x^2 + y^2$ dates back to (and was solved by) Fermat. Later mathematicians (Euler, Lagrange, Gauss, etc.) investigated (for example) which integers could be written as (say) $n = x^2 + 2y^2$ or $n = x^2 + 3y^2$ etc.

Definitions

A (binary) **quadratic form** is a (homogeneous) polynomial
$f(x,y) = ax^2 + bxy + cy^2$ denoted (*a, b, c*).

The **discriminant** of such a form is the integer *d* = $b^2 - 4ac$.

A number *n* is said to be **represented** by a form *f* if we can find *x, y* such that $n = f(x,y)$.

Remark

This is the notation used by Lagrange, Kronecker, Dedekind and Davenport. Legendre, Gauss and Dirichlet used the notation $ax^2 + 2bxy + cy^2 = \begin{pmatrix} x & y \end{pmatrix}\begin{pmatrix} a & b \\ b & c \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$ with the discriminant $b^2 - ac$ which is –1 × (the determinant of the matrix).

Two quadratic forms are "equivalent" if they can represent the same set of integers.

Example

If $n = x^2 + y^2$ then put $x' = x + y,\ y' = y \Rightarrow x = x' - y',\ y = y'$ and then $n = (x' - y')^2 + y'^2 = x'^2 - 2x'y' + 2y'^2$ and so the binary forms (1, 0, 1) and (1, -2, 2) are equivalent.

More formally, we have

Definition

Two forms are said to be (unimodularly) **equivalent** if they differ by a unimodular transformation.
$x = px' + qy',\ y = rx' + sy'$ with *ps* – *qr* = 1

That is if we have a matrix $P = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$ with unit determinant such that

$$\begin{pmatrix} a' & \frac{1}{2}b' \\ \frac{1}{2}b' & c' \end{pmatrix} = P^{t} \begin{pmatrix} a & \frac{1}{2}b \\ \frac{1}{2}b & c \end{pmatrix} P.$$

Remarks

1) Two such forms will represent the same set of integers.

2) Since the matrix P is invertible (over the integers) this is a symmetric relation. It is in fact an equivalence relation.

3) Since determinants are multiplicative, it follows that the discriminants of equivalent forms are equal. The converse is not true. For example, the forms $x^2 + 3y^2$ and $2x^2 + 2xy + 2y^2$ both have discriminant –12 but are not equivalent.

Definitions

A form is called **definite** if its discriminant $d < 0$.
(**Positive definite** if in addition $a > 0$; **negative definite** if $a < 0$)

A form is called **reduced** if either $-a < b \le a < c$ or $0 \le b \le a = c$

Theorem

Any positive definite form is equivalent to a reduced form.

Proof

If $a > c$ then apply the unimodular transformations $x = y',\ y = -x'$ to swap a and c. Then use $x = x' \pm y',\ y = y'$ (which replaces b by $b \pm 2a$) to make $|b| < a$. □

Remarks

1) It is not obvious (but true) that every positive definite form is equivalent to a *unique* reduced form.

2) The reduced form is the form with the smallest a for an equivalence class of definite forms.

2) There are a *finite* number of reduced forms for any given discriminant.
(If f is reduced then $-d = 4ac - b^2 > 3ac$ and so a, c and $b \le \frac{1}{3}|d|$)

3) The number of reduced forms for a given d is called the **class number** of d, written $h(d)$.
For $d = -3, -4, -7, -8, -11, -19, -43, -67, -163$ the class number is 1.
For $d = -12, -15, -16, -24, -27, -28, \ldots$ the class number is 2.
For $d = -23, -31, \ldots$ the class number is 3. ...
For many values of d there is no positive definite form with this discriminant.

4) In 1934 it was proved that there was at most one more discriminant with class number 1 other than those listed above; in 1966 it was proved that this "tenth discriminant" did not exist.

5) Jacobi conjectured in 1832 (and Gauss did also) that one could calculate the class number $C(d)$ of a discriminant $-p$ with p prime in the following way.
Let A be the sum of the quadratic residues mod p and let B be the sum of the non-residues. Then $C(-p) = \frac{1}{p}(B - A)$.
This was proved by Dirichlet in 1838 and is known as *Dirichlet's class number formula*.

e.g. Work modulo 23.
qr = { 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18} which sum to $A = 92$
The qnr sum to $B = 161 - 92 = 69$ and so $C(-23) = 3$.

Definition

A number n is said to be **properly represented** by a binary quadratic form f if $n = f(x, y)$ with x, y coprime.

Theorem

A number n can be properly represented by a binary form with discriminant d if and only if d has a square root modulo $4n$.

Proof

Suppose $b^2 = d \pmod{4n}$. Then define $c = b^2 - 4nc$ and take $a = n$, Then the form $f(x, y) = ax^2 + bxy + cy^2$ has discriminant d and $f(1,0) = n$.

Conversely, suppose that f has discriminant d and $f(p,r) = n$ with $\text{hcf}(p,r) = 1$. Then for some q, s we have $ps - qr = 1$ and so f is equivalent to a form f' with $a' = n$. But f, f' have the same discriminant and so mod *n* the equation $x^2 = d$ has a solution b'.

Application

Take $f(x, y) = x^2 + y^2$ so that $d = -4$ and this is the only reduced form with this discriminant.
So *n* can be properly represented as $x^2 + y^2$ if and only if -1 is a quadratic residue modulo all the primes dividing *n*. i.e. if and only if *n* is a product of primes of the form 2 or $4k + 1$.
Thus we get the result proved by Fermat: *n* is representable in the form $x^2 + y^2$ if and only if all the primes of the form $4k + 3$ which divide *n* are present as *even* powers.

Exercises

1) *Euclidean Algorithm*

a) Write the *Highest Common Factor* of 129 and 1728 in the form $129x + 1728y$.

b) If hcf(a,b) = 1 and $ax + by = 1$ show that x is determined up to integer multiples of b.
i.e. If we can also write $ax' + by' = 1$ then $x - x'$ is an integer multiple of b.

c) More generally, if d = hcf(a,b) > 1 and $ax + by = d$ what choice do we have for x and y ?

2) *Chinese Remainder Theorem*

Let p and q be coprime and suppose that $pr + qs = 1$ for integers r and s. Verify that the integer $x = prb + qsa$ is a solution of the *simultaneous congruences*

$x = a$ (modulo p) *and* $x = b$ (modulo q).

Show that this solution is *unique* modulo the product pq.

[This result can be traced back to mediaeval Chinese manuscripts, though the Greeks probably knew it too.]

Find a solution to the simultaneous congruences

$x = 5$ (modulo 13) and $x = 7$ (modulo 8).

3) *Euclid's proof of the infinitude of the primes*

a) Let the first n prime numbers be $p_1, p_2, \ldots, p_n$. Is the number $p_1 p_2 \ldots p_n + 1$ always prime? How does this affect Euclid's proof of the infinitude of the primes?

b) What about the number $p_1 p_2 \ldots p_n - 1$?

4) *Primes of the form* $4k - 1$

If $q_1, q_2, \ldots, q_n$ are primes of the form $4k - 1$, prove that the number $4q_1 q_2 \ldots q_n - 1$ cannot have all its factors of the form $4k + 1$. Imitate Euclid's proof to deduce that there are infinitely many primes of the form $4k - 1$.

Can one use the same method to prove that there are infinitely many primes of the form $4k + 1$?

5) *Hilbert's example of a system where factorisation is not unique*
Let H be the set of numbers of the form $4k + 1$ for $k = 0, 1, 2, \ldots$ i.e. $H = \{1, 5, 9, 13, \ldots\}$ Call an element of H an *H-prime* if it cannot be written as a product of smaller numbers from H.
Write down the first ten H-primes.
Show that 693 can be written as a product of H-primes in two distinct ways.

6) *Ring isomorphisms*
Show that the map from $\mathbf{Z}_3 \times \mathbf{Z}_5$ to $\mathbf{Z}_{15}$ given by $(x,y) \mapsto 5x + 3y$ is an isomorphism of additive groups which is *not* a ring isomorphism.
Prove that the map $(x,y) \mapsto 10x + 6y$ is a ring isomorphism.
Use the Euclidean algorithm to define a ring isomorphism from $\mathbf{Z}_m \times \mathbf{Z}_n$ to $\mathbf{Z}_{mn}$ if *m, n* are coprime.

7) *Pseudo-primes*
Show that $2^{10} = 1$ modulo 11 and $2^5 = 1$ modulo 31. Deduce that $2^{340} = 1$ modulo 341 and that hence 341 is a pseudo-prime with respect to 2.
Use a similar argument to show that 91 is a pseudo-prime with respect to 3.
Is 341 a pseudo-prime with respect to 3? Is 91 a pseudo-prime with respect to 2?
Is 341 a *strong* pseudo-prime with respect to 2? Is 91 a *strong* pseudo-prime with respect to 3?
Prove that 1105 is a pseudo-prime with respect to *any* integer coprime to 5, 13 and 17.
Prove that 1105 is *not* a strong pseudo-prime with respect to 2.

8) *Carmichael numbers*
Suppose that a is coprime to 561. Use Fermat's Little Theorem to deduce that $a^{560} = 1$ modulo 3, 11 or 17.
Deduce that $a^{560} = 1$ mod 561 and so 561 is a Carmichael number.
Use a similar argument to prove that *Ramanujan's number* 1729 is also a Carmichael number.
[Hint: $1729 = 7 \times 13 \times 19$]
Show, more generally, that for any integer t the number
$(6t + 1)(12t + 1)(18t + 1)$ is a Carmichael number whenever the three factors are prime numbers.
Hence find a larger Carmichael number than either of the above. Use MAPLE to find a *really* big one.

9) *Calculating powers*

If a is a fixed integer what are the minimum number of multiplications necessary to calculate:

(i) a^{17} (ii) a^{27} (iii) a^{37} (iv) a^{47} (v) a^{57}

10) *Converse of Wilson's theorem*

Prove that if $(p-1)! = -1 \pmod{p}$ then p is prime.

11) *Applications of Fermat’s Little Theorem*

a) If p and q are distinct primes, prove that $p^{q-1} + q^{p-1} = 1 \pmod{pq}$.

b) (Euler 1732) If a prime p does not divide a or b, prove that p divides $a^{q-1} - b^{p-1}$.

Does this result still hold if p is composite ?

12) *Mersenne numbers*

Use your calculator to find factors of the Mersenne numbers $2^{23} – 1$ and $2^{29} – 1$.

(The next composite Mersenne number $2^{37} – 1$ is probably outside your range.)

13) *Perfect numbers*

Show that any even perfect number is a *triangular number.*

(i.e. of the form 1 + 2 + ... + *n* for some integer *n.*)

Show that the reciprocals of the divisors of an even perfect number (including the number itself) sum to 2.

14) Uniqueness of *factorisation*

If we *do* take notice of the order in which the factors (> 1) of a number are written down, show that 24 has 4 distinct factorisations, while 72 has 10 distinct factorisations.

If n is the number $2^{\alpha}3^{\beta}$ then how many different factorisations does n have, taking account of the order in which the factors are written?

15) *A quotation from* ***Leonardo Fibonacci*** *of Pisa* (1170 – 1250)

> "*If two numbers are relatively prime and have an even sum, and if the triple product of the two numbers and their sum is multiplied by the number by which the greater number exceeds the smaller number, there results a number which will be a multiple of twenty-four*."

Prove it!

16) *Binomial coefficients*

Prove that if p is prime then the binomial coefficient $\binom{p}{k}$ is divisible by p for $1 \le k < p$.

[Hint: In the quotient $\frac{p(p-1)...(p-k+1)}{k!}$ one can never cancel out p.]

Use this fact and induction to give another proof of Fermat's Little Theorem.

Prove that if p is prime then the binomial coefficient $\binom{p-1}{k} = (-1)^k$ modulo p for $1 \le k < p$.

[Hint: Note that for any integer a we have $p - a = -a$ modulo p]

17) *Powers of primes dividing factorials*

Prove that the highest power of a prime p dividing $n!$ is given by the sum $\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + ... + \left[\frac{n}{p^t}\right]$ where $[x]$ is the integer part of x and p^t is the largest power of $p \le n$.

How many zeroes are at the end of 100! ? At the end of 1000! ?

18) *Bertrand's conjecture*

Bertrand (1822 – 1900) conjectured that if n is any integer ≥ 2 then there is a prime in the interval n ... $2n$.

The Prime Number Theorem can be used to show that for any $\varepsilon > 0$, there is an N such that if $n > N$ there is a prime in any interval n ... $(1 + \varepsilon)n$. Use the PNT to prove it for $\varepsilon = 1$.

Remark

Unfortunately the approximation in the version of the PNT proved in lectures is so crude that using this form one can only deduce that there is a prime in each interval of the form n ... $3n$, but Chebyshev's version was good enough to prove the conjecture.

Paul Erdös (one of the mathematicians to prove the PNT by "elementary" methods) summarised Bertrand's conjecture as:

Chebyshev said it and I'll say it again:
"There's always a prime between n and 2*n".*

19) *Wolstenholme's Theorem* (1872)

Let $p > 3$ be a prime. Prove that the numerator of the fraction

$$1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\ldots\ldots+\frac{1}{p-1} \text{ is divisible by } p.$$

[Hint: multiplying through by $(p-1)!$ will not affect the value of the numerator modulo p.]

(In fact the numerator is divisible by p^2 but this is harder to prove.)

20) *Fermat's factorising method*

a) Which two-digit numbers can be at the end of a perfect square ?

b) Use Fermat's method to factorize the number 33490021.

21) *Pollard's ρ–method*

Use Pollard's ρ-method to factorise the number $391 = 17 \times 23$. (I've given you the factors to make it easy to find the hcf.)

If you know enough MAPLE, write a routine to handle bigger numbers and factorise 18223380144071. (You will need a sequence of length about 6000.)

22) *Fermat primes*

Multiply out the expression

$$(2^9+2^7+1)(2^{23}-2^{21}+2^{19}-2^{17}+2^{14}-2^9-2^7+1)$$

and hence prove that the Fermat number $F_5 = 2^{32}+1$ is not prime.

23) *The Vigenère cipher*

This cryptographic system dates from the 16th century and was widely believed to be "unbreakable" though Babbage cracked it (but did not publish how) in the 19th Century.

It uses a "keyword" which is written repeatedly under the text to be encoded. The letter of the keyword then describes how much to shift the letter above it. So, for example, if the keyword had the letter C, the letter above would be shifted by 3 places from D to G (say) or from Y to B etc.

Encode the word UNBREAKABLE using the keyword BANANA (a very bad choice!).

Decode the message

LYXLERQPNAXUQURWPRJPREVNAJRZFHW

which has been encoded using the keyword CAT.

Show that such a cipher may be decoded by encoding the cipher text with an "anti-key" word. What is the anti-key word of CAT?

24) *RSA Cryptography*

What would happen if you took the a product of three primes to use for encoding rather than a product of two primes? Or the square of a prime?

25) *Factorising a number if you know ϕ*

If $n = pq$ with p, q distinct primes, prove that

$n - \phi(n) = p + q - 1$ and $(p + q)^2 = (p - q)^2 + 4n$.

Deduce that finding the value of the ϕ-function of a number is equivalent in difficulty to factorising it.

Given that $\phi(14933) = 14688$, factorise it.

26) *RSA*

The number $N = 1003$ is to be used for RSA encoding with coding power $c = 3$.

Given that N can be factored as 17×59 calculate the decoding power.

Use your calculator to encode the message STANDREWS using 01 for A, 02 for B etc. and and then using a block length of 3.

You will have to use a computer to decode the message

726, 583, 979, 104, 072, 828, 655, 117

27) *Questions to ponder* (or maybe try MAPLE on)

a) Is every odd integer ≥ 3 either a prime or a sum of a prime and a power of 2?

b) Is every even integer ≥ 4 a sum of two primes?

28) *Calculations in the Gaussian integers*

a) Find a quotient and remainder on dividing the Gaussian integer 2 + 3i by 2 + 2i ensuring that the norm of the remainder is less the the norm of 2 + 2i.

How many different such quotients and remainders are there ?

b) Find examples of pairs of Gaussian integers where there is a choice of

(i) four quotients, (ii) three quotients, (iii) two quotients,

(iv) just one quotient.

29) *Factorising Gaussian integers*

a) Write the Gaussian integers $9 + 5\mathrm{i}$, $14 + 10\mathrm{i}$ and $55 + \mathrm{i}$ as products of irreducibles in $\mathbf{Z}[\mathrm{i}]$.

b) Factorise the Gaussian integers $a = 5 + 3\mathrm{i}$ and $b = 7 + 8\mathrm{i}$ and hence or otherwise find their highest common factor. Is this hcf unique?

30) *Sums of two squares*

a) Use the Gaussian integers to prove that if two integers can be written as the sum of two squares, so can their product.
Write $(a^2 + b^2)(c^2 + d^2)$ as a sum of two squares.

b) Write the integers $725 = 5^2 \times 29$ and $20808 = 2^3 \times 3^2 \times 17^2$ as sums of two squares in as many ways as possible.

c) Find a condition which guarantees that a number can be written as a sum of two non-zero squares in two different ways.
What are the smallest numbers which can be written as a sum of two non-zero squares in three (respectively, four) different ways.

31) Prove that -4 is a fourth power in $\mathbf{Z}[\mathrm{i}]$. What other integers have fourth roots in $\mathbf{Z}[\mathrm{i}]$ but not in $\mathbf{Z}$? Are there any integers which have cube roots in $\mathbf{Z}[\mathrm{i}]$ but not in $\mathbf{Z}$?

32) *Failure of unique factorisation.*
Prove that the elements 2, $1 \pm \sqrt{-3}$ are irreducible in $\mathbf{Z}[\sqrt{-3}]$. Deduce that the element 4 can be written as a product of irreducibles in $\mathbf{Z}[\sqrt{-3}]$ in two ways.
Find a number with two distinct factorisations in $\mathbf{Z}[\sqrt{-5}]$.

33) *Quadratic number fields in* $\mathbf{R}$
Let d be a *positive* integer not divisible by a square > 1. If the *norm* of an element of the ring $\mathbf{Z}[\sqrt{d}]$ is defined by $N(a + b\sqrt{d}) = a^2 - b^2 d$ show that $N(uv) = N(u)N(v)$ for u, v in $\mathbf{Z}[\sqrt{d}]$.
Show that the element 3 is not irreducible in $\mathbf{Z}[\sqrt{2}]$.
Work modulo 5 to show that there is no element in $\mathbf{Z}[\sqrt{2}]$ with norm 5 and deduce that the element 5 is irreducible.

34) *Calculations in the Eisenstein integers*

Let ω be the complex cube root of 1 given by $\frac{1}{2}(-1+\sqrt{3}\mathrm{i})$.

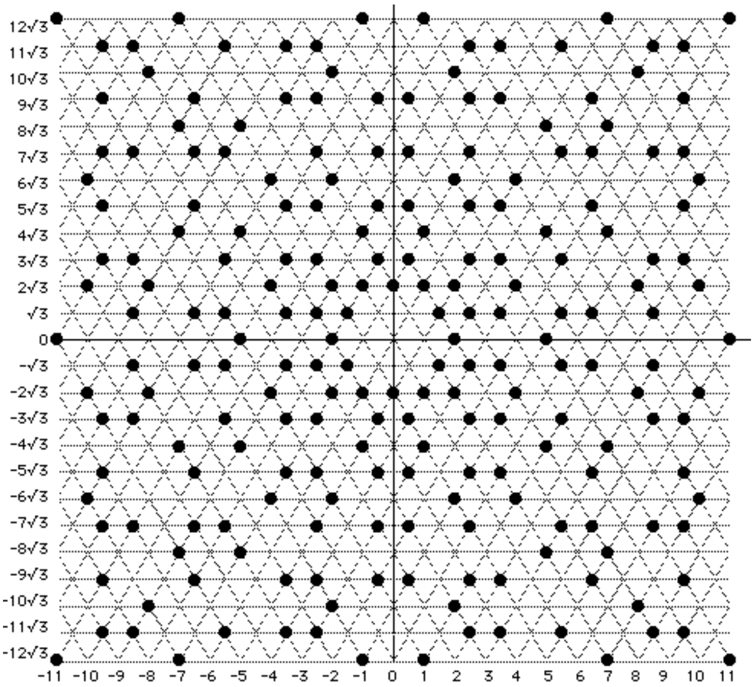
Prove that the *norm* of $a + b\omega$ in $\mathbf{Z}[\omega]$ is given by $N(a + b\omega) = a^2 - ab + b^2$.

Show that any unit (an element with a multiplicative inverse) in $\mathbf{Z}[\omega]$ must have norm 1 and hence find all such units.

If u is a unit and p is a prime in $\mathbf{Z}[\omega]$ prove that up is also a prime and deduce that the picture of primes in $\mathbf{Z}[\omega]$ will have six-fold rotational symmetry.

Prove that if n is an integer and is a prime of the form $6k + 5$ then n is also a prime in $\mathbf{Z}[\omega]$.

Show that 2 is a prime in $\mathbf{Z}[\omega]$ but that 3 is not.



Primes in $\mathbf{Z}[\omega]$ *are shown here*

35) *Sums of four squares.*

Show that if $n = 7 \pmod 8$ then it cannot be written as a sum of three squares.

In fact Legendre proved in 1798 that any number which is not of the form $4^m(8n+7)$ *can* be written as a sum of three squares.

Find integers u and v which can both be expressed as sums of three *non-zero* squares, but whose product uv cannot be.

Primes can be written as sums of two squares in a unique way. Is their representation as a sum of four squares unique? What about as sums of four non-zero squares?

36) *Primitive roots*

Which of the following have primitive roots? 12, 18, 42, 54, 266.
Find the smallest integer of the form $4k + 2$ which has no primitive root.
Write down all the primitive roots of 10.
Verify that 3 is a primitive root of 250. How many primitive roots are there for 250?
Find some others besides 3.
Verify that 7 is a primitive root of 5 but not of 25. Is 2 a primitive for both 5 and 25?
Can you find a primitive which works for 5, 10, 25 and 50?

37) *Quadratic residues*

a) Calculate the Legendre symbols $\left(\frac{133}{577}\right)$, $\left(\frac{123}{4567}\right)$, $\left(\frac{209}{409}\right)$.

b) Determine how many elements have square roots working modulo 630. List a few of them.

c) Let q be a prime divisor of the number $N = (p_1p_2..p_m)^2 - 2$. Prove that 2 is a quadratic residue mod q and hence that q is of the form $8k \pm 1$.
Prove that N cannot have all its divisors of the form $8k + 1$. Adapt Euclid's proof of the infinitude of the primes to prove that there are infinitely many primes of the form $8k + 7$.

d) By considering the number $(p_1p_2..p_m)^2 + 2$, prove that there are infinitely many primes of the form $8k + 3$.

38) *Quadratic reciprocity*

Find those primes p for which the integer 5 is a quadratic residue.
Find those primes p for which the integer 7 is a quadratic residue.
Prove that $\left(\frac{-3}{p}\right) = 1$ if $p = 1 \pmod 6$ and -1 if $p = 5$ mod 6.

39) *Jacobi symbols*

Calculate the Jacobi symbols $\left(\frac{21}{55}\right)$, $\left(\frac{17}{217}\right)$, $\left(\frac{269}{889}\right)$.

Prove that if the Jacobi symbol $\left(\frac{a}{b}\right) = -1$ then a does not have a square root modulo b.

(A counterexamle to the converse was given in lectures.

40) The manual on the first computer I owned explained how the Random Number Generator on the ZX 81 worked. It used the fact that 65537 = $2^{16} + 1$ is a prime and that hence the group $\mathbf{Z}_{65537} - \{0\}$ is a cyclic group under multiplication modulo 65537. The powers of a generator then list the elements of this group in apparently random order.The manual continues “Using the Law of Quadratic Reciprocity one can see that 75 is a primitive (i.e. a generator of the group) for this prime”. Use the Law to prove that 75 is not a quadratic residue and hence prove that 75 has order 65536 and is hence a generator.

41) *Calculating continued fractions*

a) Calculate the continued fraction expansions of the rationals $\frac{13}{15}, \frac{23}{45}, \frac{33}{35}$.

b) Use your calculator to investigate the continued fraction expansions of $\frac{e-1}{e+1}$ and $\frac{\sqrt{e}-1}{\sqrt{e}+1}$.

42) *Convergents*

a) Use the convergents of the continued fraction expansion of *e* in §4.1 to find some good rational approximations to *e*. ($\frac{2721}{1001}$ is a memorable one, if you get that far!)

b) Use the convergents of the continued fraction expansion of √2 in §4.1 to find some good rational approximations to √2.

c) When Archimedes performed his calculation of π he needed √3 as a starting point. In the absence of a decimal notation he showed that $\frac{265}{153} < \sqrt{3} < \frac{1351}{780}$. Confirm his calculation by finding these fractions as convergents of the continued fraction expansion for √3.

43) *Continued fractions of square roots*

Calculate the continued fraction expansions of √17 and √15 and verify periodicity.

Compare the rational approximations to √2 produced from continued fractions with those given by Newton's method applied to $x^2 - 2 = 0$. Say, $x_1 = 1,\ x_{n+1} = x_n - (x_n{}^2 - 2)/2x_n$.

44) Find the quadratic irrationals whose continued fraction expansions are $[0;\overline{1,4}]$ and $[0;\overline{1,2,3}]$.

45) *Pell's equation*

a) Find solutions for Pell's equation with $d = 6$ and $d = 15$.

b) If (a, b) is a solution of $x^2 - dy^2 = 1$ prove that $(a^2 + db^2, 2ab)$ is also a solution.
More generally, prove Brahmagupta's result (about 600 AD) that if (a, b) and (A, B) are both solutions so is ($aA + dbB, aB + bA$).

c) In fact Brahmagupta knew the more general result that if (a, b) is a solution of the equation $x^2 - dy^2 = k_1$ and (A,B) is a solution of the equation $x^2 - dy^2 = k_2$ then ($aA + dbB, aB + bA$) is a solution of $x^2 - dy^2 = k_1k_2$. Prove this.

46) Prove that $x^2 - 31y^2 = -1$ does not have a solution in the integers.
[Hint: Quadratic residues!]
How would you find a solution of $x^2 - 31y^2 = 1$?
Find the general solution to the Diophantine equation $5x + 3y = 104$.

47) Solve Sylvester's problem of §5.1. Investigate the general problem of finding the largest denomination which cannot be made up with stamps with values *a, b* pence.