NUMBER

THEORY

John O'Connor

2009/10

**CONTENTS**

|  |  |  |  |
| --- | --- | --- | --- |
| §0 | Introduction | |  |
|  | 0.1 | References | 2 |
|  | 0.2 | Preamble | 2 |
|  |  |  |  |
| §1 | Prime numbers | |  |
|  | 1.1 | Basic properties | 3 |
|  | 1.2 | Applications of group theory | 6 |
|  | 1.3 | Fermat and Mersenne primes | 10 |
|  | 1.4 | Distribution of primes | 13 |
|  | 1.5 | Factorisation | 16 |
|  | 1.6 | Cryptography | 17 |
|  |  |  |  |
| §2 | Other algebraic systems | |  |
|  | 2.1 | Gaussian integers | 21 |
|  | 2.2 | Integers in Quadratic Number Fields | 26 |
|  | 2.3 | Lagrange's four square theorem | 28 |

|  |  |  |  |
| --- | --- | --- | --- |
| §3 | Modular arithmetic | |  |
|  | 3.1 | Some group theory | 31 |
|  | 3.2 | Primitive roots | 32 |
|  | 3.3 | Quadratic residues | 35 |
|  | 3.4 | The Law of Quadratic reciprocity | 38 |
|  | 3.5 | Square roots modulo non-primes | 40 |

|  |  |  |  |
| --- | --- | --- | --- |
| §4 | Continued fractions | |  |
|  | 4.1 | Introduction | 43 |
|  | 4.2 | Approximating reals by rationals | 47 |
|  | 4.3 | Continued fractions of square roots | 49 |
|  | 4.4 | Pell's equation | 51 |
|  |  |  |  |
| §5 | Diophantine equations | |  |
|  | 5.1 | Linear equations | 53 |
|  | 5.2 | Higher order equations | 54 |
|  | 5.3 | Fermat's Last Theorem | 55 |
|  |  |  |  |
| §6 | Quadratic forms | | 57 |
|  |  | |  |
|  | Exercises | | 61 |

**§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: . Then look at the number 

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 .

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 + b*y for some *x, y* in **Z**.  

**Example**

The highest common factor of 123 and 456 is 3

|  |  |  |  |
| --- | --- | --- | --- |
| *a* = | 123 | 456 | = *b* |
| *b* – 3*a* = | 87 | 369 | = 3*a* |
| –*b* + 4*a* = | 36 | 87 | = *b* – 3*a* |
| 6*b* – 22*a* = | 30 | 72 | = –2*b* + 8*a* |
| –7*b* + 26*a* = | 6 | 15 | = 3*b* – 11*a* |
|  | 6 | 12 | = –14*b* + 52*a* |
|  | 0 | **3** | **= 17*b* – 63*a*** |

**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  is a product of primes in two ways, then  divides  and hence either  or  divides  and we can repeat the process to (eventually) get  = some .  
Then cancel out these two and repeat the process to match each of the s with one of the s.

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  (the group of *units* in the ring  ).

In particular, if *p* is prime then .

**Definition**

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

If *p* is prime than .

For other numbers we may calculate  using the result:

**Theorem** (Euler 1760)

1) If *m, n* are coprime then .

2) If *p* is prime and *k* is any positive integer, then

.

**Proof**

1) By elementary ring theory, if *m, n* are coprime then  is the direct product . The multiplicative identity in  is (1, 1) and so an element (*a, b*) in  has a multiplicative inverse if and only if *a* is invertible in  and *b* is invertible in . Hence the number of invertible elements in  is .

2) The only elements in 1, 2, 3, ... ,  which are not invertible modulo  are the  elements .

Hence . 

**Remark**

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

**Example**

To calculate 

 and so .

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 . 

Applying this to  we deduce

**Theorem** (Euler again)

For any *n* and *a* coprime to *n*, we have  

and in particular:

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

If *p* is prime then  for any integer *a* or  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  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  for some numbers *a*. If the answer is not 1 then *n* is not prime.

**Remarks**

1) Some numbers do satisfy  without being prime. Such a number is called a *pseudo-prime wrt a*.

In fact some numbers are so perverse that they satisfy  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  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  start with *a* and calculate  (mod *n*) and then find  and so on by squaring each time. Then write *k* in binary notation and piece together  from the various powers already calculated.

e.g. 

In binary 197 = 128 + 64 + 4 + 1 and we can calculate that mod 11:

and so



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

**Theorem**

If *p* is an odd prime then the equation  has exactly two solutions in .

**Proof**

We have  if and only if one of *x* – 1 or *x* + 1 = 0 modulo *p*. (This is because  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  and getting 1 (modulo *n*). Then suppose  (an integer since we must have *n* odd) and calculate . If this is not ±1 then we would have three solutions to  and so *n* could not be prime.

In fact if  and *q* is even, we can repeat the process by calculating  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**

 and so 561 is not prime (and although it is a pseudoprime wrt 2 it is not a strong pseudoprime).

  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 <  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*) . If *m* = ±1 then *n* passes the test for *a*. If *m* ≠ ±1 then calculate . 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 . He proved:

**Theorem**

If a number of the form  is prime, then  for some *m*.

**Proof**

Recall that  and in general, if *n* is odd, . (Use the Remainder theorem or the sum of a GP.)

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

**Remarks**

1) The number  is called the *m*th Fermat number . The first few are:  and these are prime. Fermat (1640) believed/hoped that all the  were prime. However, Euler (1732) proved that   is divisible by 641.

2)  =  In fact no other prime s are known.

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

Factorising  is helped by the following:

**Theorem** (Euler)

Any prime factor of  is of the form  for some *q*.

**Proof**

Suppose *p* divides . Then  and so squaring gives . By Fermat's Little Theorem .

Let .

Then .

Now *d* is a power of 2, say  and since  but  we must have *k* ≥ *m* + 1. i.e. .

Hence *p* – 1 is divisible by  as required. 

**Application**

Any prime factor of  must be of the form 64*k* + 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  mentioned above is . The other factor is 

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

**Theorem**

If  is prime then *m* is prime.

**Proof**

Note that *x* – 1 divides  and so if *m = ab* then (put ) we have  is divisible by . 

**Remarks**

1) The number  is called the *m*th Mersenne number .

2) Note that  is not prime for all primes *m*.

e.g. 

The values of *m* for which it is known that  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  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  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  is of the form 2*mk* + 1.

**Proof**

If a prime *p* divides  then  and  by Fermat's Little Theorem. Let *d* = hcf(*p* – 1, *m*) and write *d* = (*p* – 1)*x* + *my*. So (as before) . Since  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 2*m* divides *p* – 1. 

The Ancient Greeks were interested in:

**Definition**

A number is called **perfect** if it is the sum  of all its proper divisors.

**Examples**

 = 1 + 2 + 3 = 6, = 1 + 2 + 4 + 7 + 14 =28, etc.

**Theorem** (Euclid c 300BC)

A number of the form  where  is prime is a perfect number.

**Proof**

If  is prime then the proper divisors are:

1, 2, 4, ... ,  and *p*, 2*p*, 4*p*, ... ,  and summing gives . 

**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 .

**§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  where we say *a ~ b* if  as .

**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  is a "good fit" for π(*x*).

Gauss (in 1792 at the age of 15) defined the Logarithmic Integral  which is also a good fit for π(*x*).

3) Riemann connected the problem with the **-function (defined by ) 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 .

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

**Proof**

We look at the binomial coefficient . The numerator contains the product of all the primes from *n* to 2*n* and none of these can be cancelled by the numbers in the denominator. Since each of primes between *n* and 2*n* is > *n*) we have .

Also  and so .

Hence  and taking logs gives

 or .

So take (say) *n* > 1400 and assume by induction that .

Then  where \* is equivalent to  or  or

 or *n* > 1002. Hence the result is valid for 2*n*.

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

 where \* is:

LHS <  and

RHS >  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  is the largest power of *p* dividing  then .

**Proof**

e.g.  

If  is the largest power of *p* dividing *n*! then (See Tutorial 3)  where  is the largest power of *p* ≤ *n*.

Then if  is the largest power of *p* dividing *k*! and  is the largest power of *p* dividing (*n – k*)! then the largest power of *p* dividing  is  and each term in { } is ≤ 1. Hence this largest power is ≤ *t* and . 

Now  is divisible by at most *π*(*n*) primes and from the lemma, each power of these dividing  is ≤ *n*. i.e. .

Also 

and so the RHS is ≤ .

i.e.  and taking logs gives .

So .

\* is equivalent to  or  which is true for *n* > 200 since . 

**Remark**

Chebyshev was more careful with his estimates and hoped that methods like this would prove that  for arbitrarily small **, 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  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**

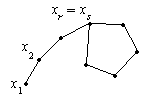
To factorise **, start with *y* = 1 and test whether  is a perfect square; then take *y* = 2, etc.

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 -method*

This was introduced in 1975

The idea is that if *p* is a factor of *n* and we choose random numbers  in  then it is more likely that  than that . Since one doesn't know *p* one detects this situation by taking .

In fact, iterating a formula like  generates a suitable "random" sequence. This has the advantage that if  then  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  and so we need only calculate .

This method was used in 1980 to factorise the 8th Fermat number . This is called the **-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 | ... |
|  | 2 | 5 | 26 | 61 | 26 | 61 | ... |
|  |  | 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  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 

Let *m* = lcm(*p* – 1, *q* – 1). Then  for any .

Choose numbers: *c* a coding power

*d* a decoding power

with *cd* = 1 (mod *m*) (using the Euclidean algorithm).

Then  for any .

Note that  and . Then if  we have  and so . Similarly  and so.

So we get two maps : coding:  and decoding: 

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. 

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

**Definitions**

The **norm** of a Gaussian integer *a +* i*b* is



A Gaussian integer *u* **divides** a Gaussian integer *v* if *v = uq* for some (quotient) .

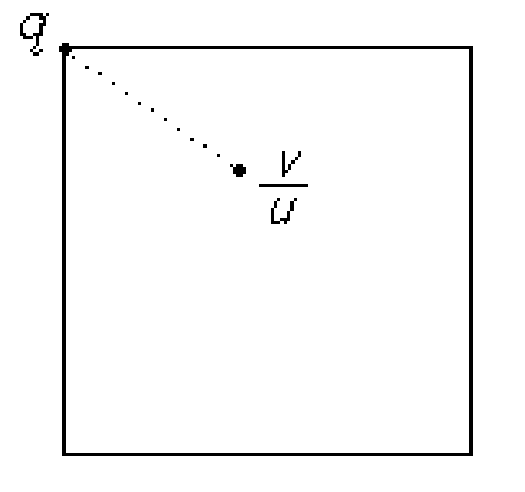
Then we have

**Theorem** (The division algorithm for the Gaussian integers)

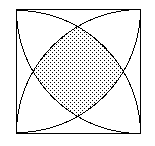
If  then  (quotient/remainder) such that *v = uq + r* with *N*(*r*) < *N*(*u*).

**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 . 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  and so we have  and  with | *s* | < 1. Then take *r = us* and then . 



**Remark**

Note that (unlike in **Z**) the quotient *q* is not always uniquely determined. For example, if  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 4*k* + 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* + 0i or 0 + *a*i to be prime we must have *a* a prime in **Z** and it must be of the form 4*k* + 3 otherwise we could write it as a product of Gaussian integers.

This follows from the result:

**Theorem** (Fermat)

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

**Proof**

By Wilson's Theorem (*p* – 1)! = (4*k*)! = –1 (mod *p*).

Now (4*k*)! = 1.2.3. ... .2*k* × (*p* – 2*k*) (*p* – 2*k* + 1). ... .(*p* – 1) and if we write *x* = (2*k*)! this is . Hence *p* divides .

But *p* cannot divide (1 ± *ix*) in **Z**[i] since  and so *p* must be a product of non-units in **Z**[i].

Then *p* = (*a + b*i)(*c + d*i) and taking Norms we get

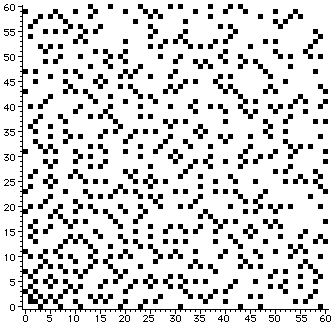
 and hence  is a sum of squares. 

**Summary**

The primes in **Z**[i] are:

a)  with *N*(*u*) = 2 or a prime of the form 4*k* + 1.

b) *a* + 0i or 0 + *a*i for *a* a prime of the form 4*k* + 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 × 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 4*k* + 1 we can write them as sums of squares

So the possible factors of *u* are 1 ± 2i and 7 ± 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  where the primes  are of the form 4*k* + 1 and the primes  are of the form 4*k* + 3.

The primes of the form 4*k* + 3 can only come from factors of the form *q* + 0i or 0 + *q*i and hence these will occur as *squares* in the factorisation of *n* = *N*(*u*).

2) Write each of the primes  as a sum of two squares  giving a factor of *u* of the form *a* ± *b*i. (The factors of 2 are 1 ± i.)

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

**Example**

To write 650 =  as a sum of two squares.

i.e. Find  with *N*(*u*) = 650.

Possible prime factors of *u* will have norms 2, 5 or 13. i.e. 1 ± i, 2 ± i, 3 ± 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.







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  then the number of ways of writing *n* as a sum of *positive* squares is  except that if all the are even then add 1 before dividing by 2 (to allow for  or ).

e.g.  can be written as a sum of two squares in 20 ways: , ...**§2.2** **Integers in Quadratic Number Fields**

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

Those of the form  where *d* is a square-free integer (≠ 1) are called **Quadratic Number Fields**.

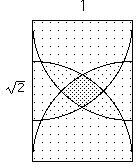
An element of one of these is called an **algebraic integer** if it satisfies an equation  with .

The quadratic integers then form a subring of **R** or **C**.

We'll be most interested in the *Imaginary* *QNFs* where *d* < 0.

**Examples**

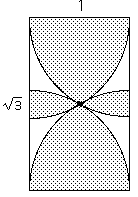
1) If *d* = –1 the quadratic integers are the Gaussian integers **Z**[*i*]. Note that this is a ring with a division algorithm and hence a Euclidean algorithm and has unique factorisation.



2) If *d* = –2 the quadratic integers are all of the form [√–2].

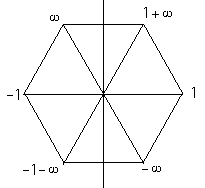
We can work as in the Gaussian integer case by taking  in a "cell" and choosing a lattice point within distance 1.

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 [√–3] but this time the method of proving the division algorithm fails because we might have  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  is an algebraic integer and the algebraic integers are of the form  where *a, b, c* are integers and *ω* is a cube root of 1. We write this as . These then form a lattice in **C** as shown and again we can always choose a lattice point within distance 1 of any quotient .

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 .

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*√*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



which add "like vectors" and multiply using the rules

 etc.

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



As in the Gaussian integers we have  for .

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  =  =

 +  +  +

 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  (a sum of three squares).

Take . Look at .

This is a set of *q* + 1 distinct elements (distinct since if  then  or  and only one of these is in the "lower half" of 0, 1, 2, ... *p* – 1)

Similarly  is a set of *q* + 1 distinct

elements. Hence these sets overlap and we have  in  or  is divisible by *p* and so  for some *m*.

Also  and  and so  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 . Reduce *a, b, c, d* mod *m* to get *A, B, C, D* and then we get  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  so that  etc. So .

The only time we get equality is if  in which case *m* is even and  and so

.

But then  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  and use Lemma 1 to write this as  and it is easy to check that  and that the other terms are also 0 (mod *m*).

So we may divide the expression  by  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  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  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 .

The group (, +) 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 

6) Any finite abelian group *A* can be written as a direct product  of cyclic groups in two ways:

a) each  is a power of a prime,

b) .

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

**§3.2 Primitive roots**

**Definitions**

For any integer *n* the invertible elements of  are called **units** .

An element *k* in  is invertible if *k, n* are coprime.

The units form a subgroup  of order .

e.g.  and  ,  and ,

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

e.g. Since  is not cyclic, 8 does not have a primitive root.

 {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,  or 2 with *p* an odd prime.

**Proof of Gauss's theorem**

1)  and  so both these are cyclic.

If  with *k* ≥ 2 then  has  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  has  as a subgroup and since both  and  have even order this contains  as a subgroup and cannot be cyclic. Similarly, if *n* is divisible by 4 and by an odd prime then  cannot be cyclic.

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

**Proof**

The ring  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  is not cyclic we may write it as a direct product  with . But then all the elements would satisfy the equation  and this would give too many solutions. 

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

**Proof**

The ring homomorphism  given by  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  satisfies  (by expanding by the binomial theorem and using the fact that the binomial coefficient  for *k* > 0). Hence this element has order *p*.

A similar proof shows that  has order . (This time one needs to check that )

Then the product of the elements *y* and *z* has order . Hence this is a primitive root. 

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

**Proof**

Since the rings  and  are isomorphic and , it follows that  and  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  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  with *k* ≥ 2.

4) If *r* is a primitive root for an odd prime *p* then for any integer 0 < *n* < *p* we have  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  have square roots.

**Definitions** (due to Euler)

If an element *s* in  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  1 and 4 have 4 square roots; 0 and 9 have two square roots and the other elements have none.

In  0, 1, 4 and 9 have 4 square roots and the other elements have none.

In  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  are quadratic residues.

**Proof**

The multiplicative group  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  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 . Then  is a quadratic residue if and only if  (and a non-residue if ).

**Proof**

If *a* is an *even* power of the generator *r* then  since 2*q* is the order of the group. 

**Application**

When does the equation  have a solution modulo an odd prime?

That is, when is –1 a quadratic residue?

Answer: ⇔  *q* is even ⇔ *p* is of the form 4*k* + 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 . Then the **Legendre symbol**  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 (mod *p*)).

**Remarks**

1) We can now interpret the above corollaries as:

a) 

b) If  then  mod *p*. In particular .

2) If *r* is a primitive root and  for  then .

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

**Theorem** (Gauss's Lemma)

Let *p* be an odd prime and . Consider the numbers *a*, 2*a*, 3*a*, ... , *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*, 2*a*, ... , *qa* must be distinct mod *p* (since *a* is invertible in ) and if we take these numbers to lie in the range [–*q*, *q*] and we were to have (say)  then  which can't happen since  is in the range [1, *q*].

Multiplying  with the appropriate choice of signs on the right and this is  Thus  and the result follows from Euler's criterion. 

**Application**

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

Take  and we get a list: 2, 4, ... , 2*q* = *p* – 1.

Put *p* = 8*k* + *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 .

**§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  being a quadratic residue modulo a prime  in terms of  being a quadratic residue modulo .

We can state it most conveniently using Legendre symbols.

**Theorem** (The Law of Quadratic Reciprocity)

Let  and  be distinct odd primes. Put .

Then .

This can be phrased as:

*The quadratic character of  and  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 .

Write  and subtract a suitable multiple of  so that each is in the range .

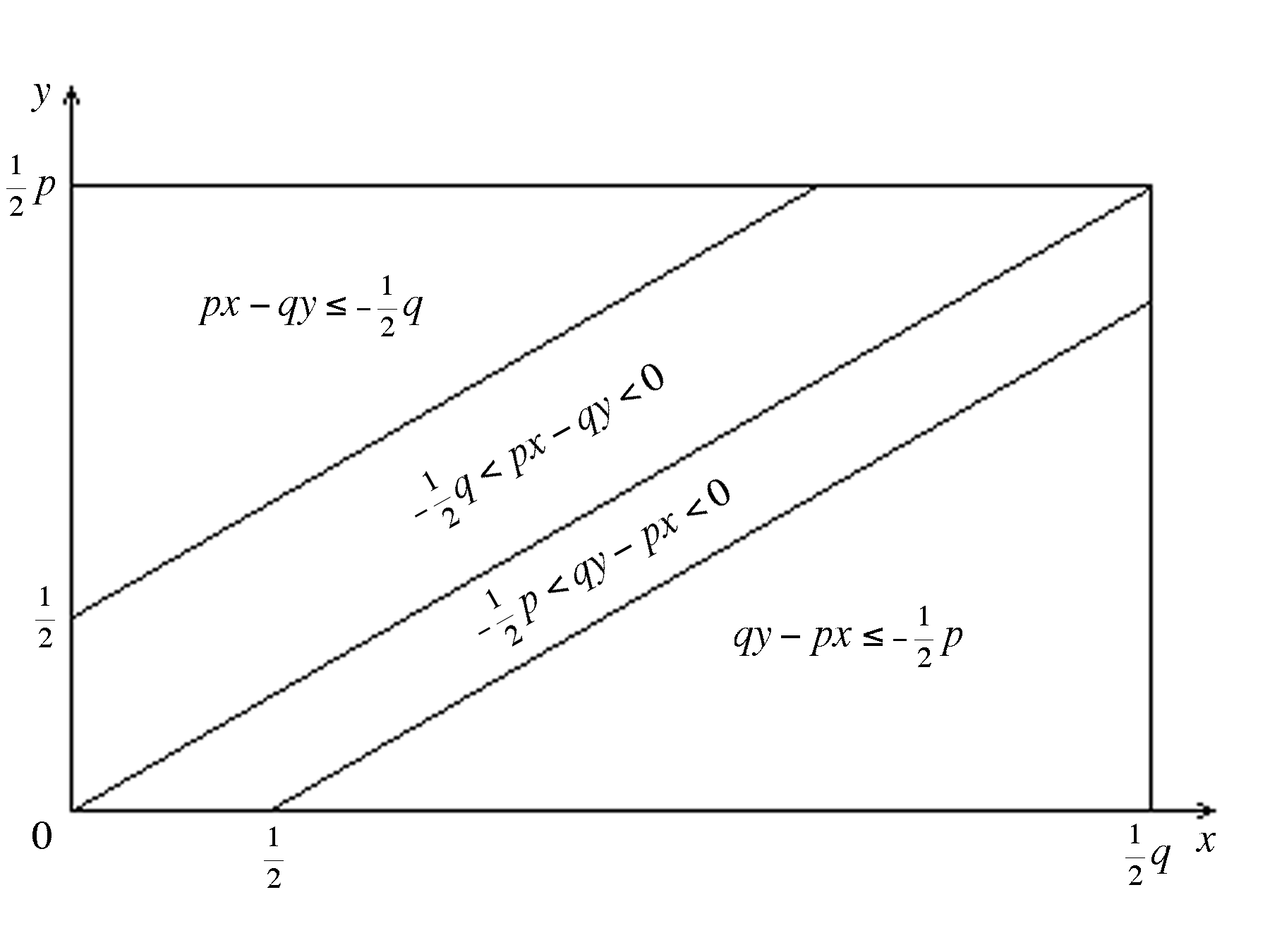
Then the number of minuses we get is the number of pairs  which lie in  for *x* lying in the range  (*x, y* integers).

 and this is < since *y* is an integer. Thus .

So the number *l* of (*x, y*)s to count are the number of lattice points in the rectangle  which satisfy . Then . Similarly  where m is the number of lattice points in the rectangle satisfying 

We are trying to show that  or equivalently that  is even.

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



The map  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)  so 15 is a qr mod 71

(in fact √15 = ±21 mod 71)

2) 

\*: since we can always take out squared factors

\*\*: since 97 = 8*k* + 1 \*\*\*: since 

3) When is 3 a quadratic residue mod *p* ?

 if *p* = 1 mod 4 and  if *p* = 3 mod 4.

The only quadratic residue mod 3 is 1 so

 if *p* = 1 (mod 4) and 1 (mod 3) ⇔ *p* = 1 (mod 12)

or if *p* = 3 (mod 4) and 2 (mod 3) ⇔ *p* = 11 (mod 12)

i.e. *p* = ±1 (mod 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  with  a product of distinct prime powers. Then *a* has a square root if and only if *a* has a square root modulo each .

If *a* has  roots modulo  then it has  roots modulo *n*.

**Proof**

Use the Chinese remainder theorem to reduce the problem to one modulo each . 

**Example**

Let *n* = 30 = 2 × 3 × 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* (≠ 0 mod *p*) has a square root modulo  if and only if it has a square root modulo *p*.

**Proof**

If  then clearly .

For the converse, if *a* has a root mod *p* put  and then put  and solve . This is

 or  and we can solve this for *bp* since 2*y* and *p* are coprime.

Similarly we may start with a root modulo  find a root modulo  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  is a product of (not necessarily distinct) odd primes.

Then the **Jacobi symbol** is .

**Remarks**

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

2) If  then it does *not* necessarily follow that *a* has a square root modulo *n*. For example  but 2 has no square root mod 15. However if  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 .

2) If *a* is are coprime to the odd *m*, *n* then .

3)  ; 

4) (*Quadratic reciprocity*)

If *m, n* are coprime then .

**Example**

1)  and so 11 has no square root mod 27

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



Hence (since 2999 is a prime) this Legendre symbol is +1 and so 335 is a quadratic residue ()

**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* ≠ 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*  *of x* \*\*

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

**Example**

For example, if you start with  then you get  which is written  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.

424 = 37 × 11 + 17

37 = 17 × 2 + 3

17 = 3 × 5 + 2

3 = 2 × 1 + 1

2 = 2 × 1 + 0

One can rewrite this as:





In general given  start with  (integer part) and then if  write  and  then if  we take  etc.

**Definition**

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

The argument with the Euclidean algorithm above shows that every *rational number* has a continued fraction expansion  which terminates after a finite number of steps. The expansion is unique except that if the last partial quotient  = 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:

 = 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:

 = 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 ** has a continued fraction expansion  then the rational numbers

 for *n* ≥ 0 are called the **convergents** of **.

We can calculate the convergents recursively.

**Theorem**

The convergents  of  satisfy

 and then

 for *n* ≥ 2.

**Proof**

It is easy to check that  is as claimed for *n* = 0, 1.

Then by induction assume the recurrence holds for *k*.

Then 



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

 It is well-known that the ratios of successive Fibonacci numbers converge to .

2) The convergents of the continued fraction [3; 7, 15, 1, 292, 1, 1, 1, 2, ... ] calculated for *π* are  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  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 ** does indeed converge to **.

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

3) The numbers  increase as *n* increases.

4) What we are considering are sometimes called simple continued fractions to distinguish them from the more general  .

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 ** by a rational  is to divide up the real line into segments of length  and take the nearest multiple of this to **. One can then be sure that .

For example one may approximate π by  to better that .

Dirichlet proved one could do better than this.

**Theorem**

Given any real number ** and integer *Q* one can find a rational  with *q* < *Q* such that .

**Proof**

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

Consider the *Q* + 1 points in the interval [0, 1] given by: 0, {**}, {2**}, ... {(*Q* – 1)**}, 1 where { } means the fractional part.

Divide up the unit interval into *Q* intervals of length  and we deduce that two of these must lie in the same sub-interval.

That is . Hence for some integers *p, q* we must have  and so . 

**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  satisfy .

**Proof**

Using the above recurrence relations for  and  and induction we may prove  .Then divide by . 

From the definition above  with  and so  and ** lies between  and .

Thus ** is closer than  to  as claimed earlier.

**Remarks**

1) Note that from the above corollary, the convergents are alternately larger () and smaller () than ** .

2) In fact one may show that the sequence () is monotonic decreasing and the sequence () is monotonic increasing. (Both of course converge to **.) Thus the sequence of convergents alternately underestimate and overestimate the final limit.

3) In fact one may show that the convergent  approximates ** better than any rational number with a denominator smaller than  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.

 and the process then repeats itself.

In general the continued fraction of a square root of an integer is of the form  which we write as .

**Remarks**

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

2) The periodic part has a very specific symmetrical form. In fact  always has the form .

e.g.  

3) As above, each  reduces to  and in fact the numbers  satisfy  and .

4) More generally any *quadratic irrational* of the form  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**

 We showed earlier that the continued fraction of  is .

 ** = [3; 3, 3, 3, 3, ...]

Then  and so  and so.

3) ** = [0; 3, 2, 3, 2, ...]

Then  and so  and so.

**§4.4 Pell's equation**

This is the equation  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  in  is  and the norm satisfies *N*(*uv*) = *N*(*u*) *N*(*v*). So if (*x, y*) is a solution of Pell's equation then  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  whose square is  giving the next solution. Its cube is  and so on.

2) It follows from the above that if  are the solutions of Pell's equation then the  satisfy a recurrence relation of the form  where . The  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  then the convergent  corresponding to the penultimate term of the first periodic block gives the fundamental solution  of the equation .

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 . 

**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:  =

 and the solutions of  come from the 3rd, 7th, ... convergents and are: (8, 3), (127, 48), ...

Note that  as in Remark 1) above.

Let *d* = 10

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



The 0th convergent gives a solution of  and we need the next (19, 6) to get a solution of Pell's equation.

(117, 37) satisfies  while (721, 228) is a solution of Pell's equation.

Note that 

Brahmagupta's example: *d* = 83

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



giving the solutions mentioned above.

Note that  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 ** (to be solved for *x, y*) has a solution if and only if *d* = hcf(*a, b*) divides *c*.

**Proof**

Since *d* divides *a* and *b* it divides ** and so the condition is necessary.

Conversely, if *c = md* then use the Euclidean algorithm to write

** 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  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 .

We can characterise all such solutions.

**Theorem**

If (*x, y, z*) are coprime integers satisfying  with (say) *y* even, then  for some integers *a, b*.

**Proof**

Note that  and so we get a solution starting with any *a, b*.

To see that such *a, b* exist, write the equation in the form . Since *x, z* are coprime it follows that that  and the other prime factors of *x – z* and *x + z* must be squared. Hence  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:  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 :

If , factorise the LHS:  and use the unique factorisation property in  to prove the result.

Lamé (in 1847) thought he had a proof using  with ** a *p*th root of 1 but unfortunately the proof required this ring to have the unique factorisation property (which it doesn't if *p* ≥ 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 .

**Proof**

If we are given a smallest such solution, then  is a Pythagorean triple with (say) *y* even and so .

Now *b* must be even since if *a* were even and *b* odd then we would have  which is impossible.

Then  is a Pythagorean triple and we have

. Then 

Since  are pairwise coprime we have  for integers *e, f, g*.

Thus  and  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  dates back to (and was solved by) Fermat. Later mathematicians (Euler, Lagrange, Gauss, etc.) investigated (for example) which integers could be written as (say)  or  etc.

**Definitions**

A (binary) **quadratic form** is a (homogeneous) polynomial

 denoted (*a, b, c*).

The **discriminant** of such a form is the integer *d* = .

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

**Remark**

This is the notation used by Lagrange, Kronecker, Dedekind and Davenport. Legendre, Gauss and Dirichlet used the notation  with the discriminant  which is –1 × (the determinant of the matrix).

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

**Example**

If  then put  and then  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.

 with *ps – qr* = 1

That is if we have a matrix  with unit determinant such that

.

**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  and  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* ≤ *a* < *c* or 0 ≤ *b* ≤ *a* = *c*

**Theorem**

Any positive definite form is equivalent to a reduced form.

**Proof**

If *a > c* then apply the unimodular transformations  to swap *a* and *c*. Then use  (which replaces *b* by *b* ± 2*a*) 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  and so *a, c* and *b* ≤  )

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, ... the class number is 2.

For *d* = –23, –31, ... 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 .

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  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 4*n*.

**Proof**

Suppose . Then define  and take *a = n*, Then the form  has discriminant *d* and .

Conversely, suppose that *f* has discriminant *d* and  with . Then for some *q, s* we have  and so *f* is equivalent to a form  with . But  have the same discriminant and so mod *n* the equation  has a solution .

**Application**

Take  so that *d* = –4 and this is the only reduced form with this discriminant.

So *n* can be properly represented as  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 4*k* + 1.

Thus we get the result proved by Fermat: *n* is representable in the form  if and only if all the primes of the form 4*k* + 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 129*x* + 1728*y*.

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 **. Is the number ** always prime? How does this affect Euclid's proof of the infinitude of the primes?

b) What about the number **?

4) *Primes of the form* 4*k* – 1

If ** are primes of the form 4*k* – 1, prove that the number ** cannot have all its factors of the form 4*k* + 1. Imitate Euclid's proof to deduce that there are infinitely many primes of the form 4*k* – 1.

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

5) *Hilbert's example of a system where factorisation is not unique*

Let *H* be the set of numbers of the form 4*k* + 1 for *k* = 0, 1, 2, ... i.e. *H* = {1, 5, 9, 13, ...} 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  to  given by  is an isomorphism of additive groups which is *not* a ring isomorphism.

Prove that the map  is a ring isomorphism.

Use the Euclidean algorithm to define a ring isomorphism from  to  if *m, n* are coprime.

7) *Pseudo-primes*

Show that 210 = 1 modulo 11 and 25 = 1 modulo 31. Deduce that 2340 = 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  13  19]

Show, more generally, that for any integer *t* the number

(6*t* +1)(12*t* +1)(18*t* +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  then *p* is prime.

11) *Applications of Fermat’s Little Theorem*

a) If *p* and *q* are distinct primes, prove that .

b) (Euler 1732) If a prime *p* does not divide *a* or *b*, prove that *p* divides *.*

Does this result still hold if *p* is composite ?

12) *Mersenne numbers*

Use your calculator to find factors of the Mersenne numbers 223 – 1 and 229 – 1.

(The next composite Mersenne number 237 – 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  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  is divisible by *p* for 1 ≤ *k* < *p*.

[Hint: In the quotient ** 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  modulo *p* for 1 ≤ *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

where **[***x***]** is the integer part of *x* and *pt* is the largest power of *p* ≤ *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* ... 2*n*.

The Prime Number Theorem can be used to show that for any  > 0, there is an *N* such that if *n* > *N* there is a prime in any interval *n* ... (1 + **)*n*. Use the PNT to prove it for ** = 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* ... 3*n,* 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

 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  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 **method*

Use Pollard's **-method to factorise the number 391 = 17 × 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



and hence prove that the Fermat number 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 *

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

*n* – **(*n*) = *p* + *q* – 1 and (*p* + *q*)2 = (*p* – *q*)2 + 4*n.*

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

Given that **(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 + 5i, 14 + 10i and 55 + i as products of irreducibles in **Z**[i].

b) Factorise the Gaussian integers *a* = 5 + 3i and *b* = 7 + 8i 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 = 52 × 29 and 20808 = 23 × 32 × 172 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 **Z**[i]. What other integers have fourth roots in **Z**[i] but not in **Z** ? Are there any integers which have cube roots in **Z**[i] but not in **Z** ?

32) *Failure of unique factorisation*.

Prove that the elements 2, 1 ± √–3 are irreducible in **Z**[√–3]. Deduce that the element 4 can be written as a product of irreducibles in **Z**[√–3] in two ways.

Find a number with two distinct factorisations in **Z**[√–5].

33) *Quadratic number fields in* **R**

Let *d* be a *positive* integer not divisible by a square > 1. If the *norm* of an element of the ring **Z**[√*d*] is defined by *N*(*a + b√d*) = show that *N*(*uv*) = *N*(*u*)*N*(*v*) for *u, v* in **Z**[√*d*].

Show that the element 3 is not irreducible in **Z**[√2].

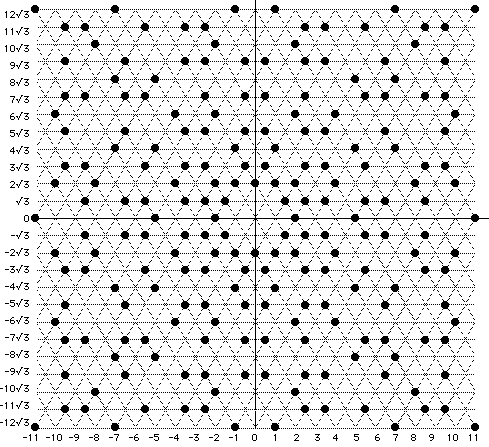
Work modulo 5 to show that there is no element in **Z**[√2] with norm 5 and deduce that the element 5 is irreducible.

34) *Calculations in the Eisenstein integers*

Let ** be the complex cube root of 1 given by .

Prove that the *norm* of *a* + *b* in **Z**[**] is given by *N*(*a* + *b* = *a*2 – *ab* + *b*2.

Show that any unit (an element with a multiplicative inverse) in **Z**[] must have norm 1 and hence find all such units.

If *u* is a unit and *p* is a prime in **Z**[] prove that *up* is also a prime and deduce that the picture of primes in **Z**[**] will have six-fold rotational symmetry.

Prove that if *n* is an integer and is a prime of the form 6*k* + 5 then *n* is also a prime in **Z**[**].

Show that 2 is a prime in **Z**[**] but that 3 is not.

*Primes in* **Z**[**] *are shown here*

35) *Sums of four squares.*

Show that if *n* = 7 (mod 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  *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 4*k* + 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 .

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*1*p*2...*pm*)2 – 2. Prove that 2 is a quadratic residue mod *q* and hence that *q* is of the form 8*k* ± 1.

Prove that *N* cannot have all its divisors of the form 8*k* + 1. Adapt Euclid’s proof of the infinitude of the primes to prove that there are infinitely many primes of the form 8*k* + 7.

d) By considering the number (*p*1*p*2...*pm*)2 + 2, prove that there are infinitely many primes of the form 8*k* + 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  = 1 if *p* = 1 (mod 6) and –1 if *p* = 5 mod 6.

39) *Jacobi symbols*

Calculate the Jacobi symbols .

Prove that if the Jacobi symbol  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 = 216 + 1 is a prime and that hence the group **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 .

b) Use your calculator to investigate the continued fraction expansions of  and .

42) *Convergents*

a) Use the convergents of the continued fraction expansion of *e* in §4.1 to find some good rational approximations to *e*. ( 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 . 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 . Say, .

44) Find the quadratic irrationals whose continued fraction expansions are  and .

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  prove that  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  and (*A,B*) is a solution of the equation  then (*aA + dbB, aB + bA*) is a solution of . Prove this.

46) Prove that  does not have a solution in the integers.

[Hint: Quadratic residues!]

How would you find a solution of ?

Find the general solution to the Diophantine equation .

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.