Number Theory ①

Terminology

Natural Numbers $\mathbb{N} = \{1, 2, \dots\}$

Non-negative integers $\mathbb{N}_0 = \{0, 1, 2, \dots\}$

Integers $\mathbb{Z} = \{\dots, -1, 0, 1, \dots\}$

Assume induction or the well-ordering principle.

H. Davenport – The Higher Arithmetic 6th + Edition

G.A and J.M. Jones – Elementary Number Theory (Springer)

Chapter 1 : Divisibility

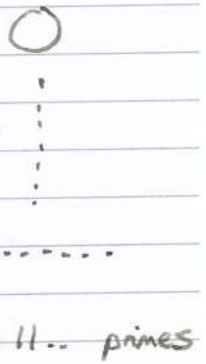
1.1 Definitions

a divides b, $a \mid b \Leftrightarrow \exists c : ac = b$

Clearly $a \mid a$, and $a \mid b \mid c \Rightarrow a \mid c$

Also, $a \mid b$ and $b \mid a \Rightarrow a = \pm b$

So $\mid$ is a partial order on $\mathbb{N}_0$, shown to the right.



We say that p is prime $\Leftrightarrow$ p has exactly two divisors, 1, and p, with $1 \neq p$. Note that for $a, b \in \mathbb{N}$, $a \mid b \Rightarrow a \leq b$, so we can do induction and recursion over $\mid$.

1.2 Euclid's Algorithm

Suppose that $a, b \in \mathbb{N}$. Then there are (unique) $q, r \in \mathbb{N}_0$ with $a = qb + r$, and $0 \leq r < b$.

Proof

$\{a - kb \mid k \in \mathbb{N}_0\}$ has elements ≥ 0 and so we can take

$a - q_0 b \geq 0$ to be the least of these. Then $a = q_0 b + r$, $r \geq 0$. If $r \geq b$, then $r = b + r'$, say, with $r' \geq 0$, and then $a - (q_0+1)b = r'$, contradicting our choice of a least element ✱

Suppose that $a = qb + r = q'b + r'$, $0 \leq r, r' < b$

Then $(q - q')b + (r - r') = 0$. If $q \neq q'$, we have $b \mid r - r'$, but $-b < r - r' < b$ ✱ So $q = q'$, thus $r = r'$, and we have uniqueness.

Euclid's Algorithm

Given $a, b \in \mathbb{N}$, we set successively

$$a = q_0 b + r_0 \qquad 0 \leq r_0 < b$$
$$b = q_1 r_0 + r_1 \qquad 0 \leq r_1 < r_0$$
$$\cdots\cdots$$
$$r_{k-1} = q_{k+1} r_k + r_{k+1} \qquad 0 \leq r_{k+1} < r_k$$
$$\cdots\cdots$$
$$r_{n-1} = q_{n+1} r_n + 0$$

} By tradition, this has $n+1$ lines

Since $b > r_0 > r_1 > \ldots > 0$, the process terminates, by the Well-Ordering Principle. Since $r_{k-1} = q_{k+1} r_k + r_{k+1}$, $d \mid r_{k-1}$ and r_k if $d \mid r_k$ and r_{k+1}, so inductively, $d \mid a, b \Leftrightarrow d \mid r_n$ (and 0). Thus, $h = r_n$ has the properties

i) $h \mid a$ and $h \mid b$ ii) If $d \mid a$, $d \mid b$, then $d \mid h$

and h is the highest common factor of a and b.

Observation

What happens if we replace a, b by a/h and b/h ?

Number Theory ①

The quotients q_i are the same, but the remainders are r_i/h.

Bezout's Theorem

Let $a, b, c \in \mathbb{N}$. Then

$c = xa + yb$ for some $x, y \in \mathbb{Z} \iff d = hcf(a,b) \mid c$

Proof

The only real point is to show that (a,b) can be written in the form given. Inductively, we see that every remainder can be so written.

Aside

The ring-theoretic proof of the existence of (a,b) takes the least positive element of $\{xa + yb \mid x, y \in \mathbb{Z}\}$ and shows (by the division lemma) that it divides all elements.

Extended Algorithm

a	1	0	Each row, r_i satisfies
b	0	1	$r_i = r_{i-2} - q_i r_{i-1}$, and so
r_0	1	$-q_0$	does the entire row.
r_1	$-q_1$	$1+q_0q_1$	

This is because $\begin{pmatrix} 0 & 1 \\ 1 & -q_0 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} b \\ r_0 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \\ 1 & -q_0 \end{pmatrix}\begin{pmatrix} b \\ r_0 \end{pmatrix} = \begin{pmatrix} r_0 \\ r_1 \end{pmatrix}, \ldots$

We see this again in continued fractions:

$$a/b = [q_0, q_1, q_2, \ldots] = q_0 + \cfrac{1}{q_1 + \cfrac{1}{\ldots}} = q_0 + \frac{1}{q_1 + \ldots} + \frac{1}{q_2 + \ldots} + \ldots$$

1.3 The Fundamental Theorem of Arithmetic

Simple Observation

If $n > 1$, then n has a prime factor. We argue inductively. Either n is prime, or there is $1 | m | n$ with $1 < m < n$. By induction, m has a prime factor, so n has.

Corollary

There are an infinite number of primes.

Proof

Suppose that $p_1, \ldots, p_k$ is a finite sequence of primes, and consider $N = p_1 p_2 \ldots p_k + 1$. Let p be a prime factor of N. Then $(p, N) = p$, while $(p_i, N) = 1$. So p is distinct from the p_i. Thus, no finite list contains all of the primes.

Corollary

Any $n \in \mathbb{N}$ has a prime factorisation. Again we argue inductively. 1 is the product of the empty set of primes. Then if $n > 1$, then n has a prime factor p, say, so $n = pm$. Now $1 \leq m < n$, so by induction, m has a prime factorisation. Hence so does n.

Lemma

Let p be a primes.

Then $p | ab \Rightarrow p | a$ or $p | b$.

Number Theory ①

Proof

If $p \nmid a$ then $(a, p) = 1$, so we can take x, y with

$xa + yp = 1$. $xab + ypb = b$.

$p \mid ab$, so $p \mid xab + ypb$, hence $p \mid b$

Fundamental Theorem of Arithmetic

The prime factorisation of a number $n \in \mathbb{N}$ is unique up to order.

That is, if $n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_l$, two 'different' prime factorisations, then in fact $k = l$, and after reordering, $p_i = q_i$.

□

Number Theory ②

Fundamental Theorem of Arithmetic

Prime factorisations are unique up to order. That is, if $n = p_1 \dots p_k = q_1 \dots q_l$ are prime factorisations, then $k = l$ and we can reorder the q_js so that $p_i = q_i$. The proofs is inductive. $n = 1$ has a unique trivial factorisation.

Inductive step: The prime $p_1 \mid q_1 \dots q_l$ and so by our lemma, p_1 divides some q_j. Reorder so that $p_1 \mid q_1$. Thus $p_1 = q_1$, and we cancel to obtain $p_2 \dots p_k = q_2 \dots q_l$. The result follows.

If we write $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ with $p_1 < p_2 < \dots < p_k$ and $\alpha_i > 0$ then the expression is unique. But we can allow expressions with $\alpha_i = 0$ to display all relevant primes.

Observations

1. $a = p_1^{\alpha_1} \dots p_k^{\alpha_k} \mid b = p_1^{\beta_1} \dots p_k^{\beta_k} \iff \alpha_i \leq \beta_i \quad \forall i$.
2. $(a, b) = p_1^{\min(\alpha_1, \beta_1)} \dots p_k^{\min(\alpha_k, \beta_k)}$
3. We have the Lcm $[a, b] = p_1^{\max(\alpha_1, \beta_1)} \dots p_k^{\max(\alpha_k, \beta_k)}$

   Clearly $[a, b] \mid c \iff a \mid c$ and $b \mid c$.

Further Observations

Suppose that $(n, m) = 1$ and $d \mid nm$. Then $e = (d, n)$, $f = (d, m)$ are unique such that $e \mid n$, $f \mid m$, and $ef = d$

Why?

Suppose that $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, $m = q_1^{\beta_1} \dots q_l^{\beta_l}$, p_i, q_j distinct

$d = p_1^{r_1} \cdots p_k^{r_k} q_1^{\delta_1} \cdots q_l^{\delta_l}$ with $r_i \leq \alpha_i$, $\delta_j \leq \beta_j$

Then $e = p_1^{r_1} \cdots p_k^{r_k}$, $f = q_1^{\delta_1} \cdots q_l^{\delta_l}$ are unique as required.

Chapter 2: Congruences

2.1 Basics

For $n \in \mathbb{N}$ we write $a \equiv b \ (n)$ for $n \mid a-b$. Arithmetic mod n is arithmetic in $\mathbb{Z}/n\mathbb{Z}$. For number theory, we can think of it as an arithmetic on the set of least residues $\{0, 1, \ldots, n-1\}$ or least absolute residues $\{-\frac{n}{2} \leq a \leq \frac{n}{2}\}$

Lemma

a is invertible mod $n \iff (a, n) = 1$

Proof:

If $(a, n) = 1$ take $xa + yn = 1$, then $xa \equiv 1 \ (n)$ so x is the inverse of a mod n.

Conversely, if $xa \equiv 1 \ (n)$, then $xa = 1 + zn$ for some z, and then $xa - zn = 1$, so $(a, n) = 1$.

The number of units (invertible elements) mod n is $\varphi(n)$, Euler's totient function. Also, $\varphi(n)$ is the number of generators in the cyclic group $C_n \cong (\mathbb{Z}/n\mathbb{Z}, +)$

Easy Observations

1. If p is prime, then $1, 2, \ldots, p-1$ are coprime to p, so $\varphi(p) = p - 1$
2. If we take p^k, the numbers not coprime are multiples of p,

and there are p^{k-1} of these. So $\varphi(p^k) = p^k - p^{k-1} = (p-1)p^{k-1}$

Proposition

i) (Fermat) If p is prime, then $a^{p-1} \equiv 1 \ (p)$ for all a with $(a,p)=1$

ii) (Euler) For any n, $a^{\varphi(n)} \equiv 1 \ (n)$ for all a with $(a,n)=1$.

Proofs

Either: The units mod n form a multiplicative group of order $\varphi(n)$, and the order of the elements divides the order of the group.

Or: Let $x_1, \dots, x_{\varphi(n)}$ be distinct residues mod n, each with $(x_i, n) = 1$. If $(a,n)=1$, then $ax_1, \dots, ax_{\varphi(n)}$ must be the same list, probably in some other order.

Therefore, $\prod_1^{\varphi(n)} x_i = \prod_1^{\varphi(n)} ax_i = a^{\varphi(n)} \prod_1^{\varphi(n)} x_i \quad (n)$.

But $(\prod_1^{\varphi(n)} x_i)$ is a unit, so cancelling gives $a^{\varphi(n)} \equiv 1 \ (n)$

2·2 The Chinese Remainder Theory

Let $n_1, \dots, n_k$ be coprime in pairs. Then, for any $a_1, \dots, a_k$, there is a solution to the congruences $x \equiv a_i \ (n_i)$, $1 \le i \le k$, and this solution is unique mod $n = n_1 n_2 \dots n_k$

Proofs

Let $n_i m_i = n$ so that $m_i = \prod_{j \neq i} n_j$. Take $\bar{m}_i m_i \equiv 1 \ (n_i)$

Set $x = \sum_{i=1}^{k} a_i \bar{m}_i m_i$. Then mod n_j we have

$x \equiv a_j \bar{m}_j m_j \equiv a_j \ (n_j)$

Uniqueness: If $x \equiv y \equiv a_i \ (n_i)$, then each $n_i \mid x-y$.

So $n \mid x-y$ and then $x \equiv y \ (n)$.

Note that this says that the endiant homomorphism $\mathbb{Z}/n\mathbb{Z} \to \prod_{i=1}^{k} \mathbb{Z}/n_i\mathbb{Z}$ is an isomorphism. But its kernel is the a such that $n_i \mid a \ \forall i$, hence the a such that $n \mid a$. So the homomorphism is injective and so bijective by counting.

2·3 Remarks on $\varphi(n)$

From CRT we see that $(a_1, \dots, a_k)$ is invertible in $\prod_{i=1}^{k} \mathbb{Z}/n_i\mathbb{Z}$ $\Leftrightarrow$ each a_i is invertible mod n_i, so $\varphi(n) = \varphi(n_1) \dots \varphi(n_k)$

φ is an example of a multiplicative function:

If $(a,b) = 1$, then $\varphi(ab) = \varphi(a)\varphi(b)$

Recall from IA that a cyclic group of order n, say $(\mathbb{Z}/n\mathbb{Z}, +)$ has for every $d \mid n$ $(n = de)$ a unique subgroup of order d (namely $\{0, e, 2e, \dots, (d-1)e\}$), and so it has exactly $\varphi(d)$ elements of order $d \mid n$. It follows that $\sum_{d \mid n} \varphi(d) = n$.

Number Theoretic Proof

Set $F(n) = \sum_{d \mid n} \varphi(d)$. Suppose that $(n, m) = 1$. Then

$$F(nm) = \sum_{d \mid mn} \varphi(d) = \sum_{e \mid n, f \mid m} \varphi(ef) = \sum_{e \mid n} \varphi(e) \sum_{f \mid m} \varphi(f)$$
$$= F(n)F(m)$$

Now $F(p^k) = 1 + (p-1) + (p-1)p + \dots + (p-1)p^{k-1} = p^k$

Thus $F(n) = n \ \forall n \in \mathbb{N}$.

10/10/12

Number Theory ③

2.4 "Lagrange's Theorem"

We consider polynomials with coefficients mod p : i.e. in $\mathbb{Z}/p\mathbb{Z}[X]$. A polynomial f has degree n if and only if $f(x) = a_n X^n +$ lower terms with $a_n \not\equiv 0 \ (p)$

Theorem

A polynomial of degree n has at most n roots (mod p)

Proof (By induction)

A polynomial of degree 0 has 0 roots.

Suppose α is a root of f. Then, by the Remainder Theorem, $f(x) = (X-\alpha)g(x)$ where $g(x) = a_n X^{n-1} + \dots$ is of degree $n-1$. Now let β be some other root of f. Then $0 \equiv f(\beta) = (\beta-\alpha)g(\beta)$, $(\beta-\alpha) \not\equiv 0 \ (p)$. So $g(\beta) = 0$ and β is a root of g. By the induction hypothesis g has at most $n-1$ roots. So f has at most n roots.

Example

$X^{p-1} - 1$ has $p-1$ roots, viz. $1, 2, \dots, p-1$. So by our proof, $(X^{p-1} - 1) \equiv (X-1)(X-2)\dots(X-(p-1)) \bmod p$

So $-1 \equiv (p-1)!\,(-1)^{p-1} \ (p)$

So $(p-1)! \equiv -1 \ (p)$ for all odd primes (but also for 2)

Alternative thought: An element x in $(\mathbb{Z}/p\mathbb{Z})^\times$ is its own inverse $\Leftrightarrow x^2 \equiv 1 \ (p) \Leftrightarrow x \equiv \pm 1 \ (p)$

So in the other product $(p-1)!$ all the elements cancel with their inverses and $(p-1)! \equiv -1 \ (p)$

Note : $X^p - X$ has p roots mod p. $a^p \equiv a \ (p)$

2.5 Primitive Element Theorem

Theorem

$(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic. (A generator i.e. an element g such that $g^d \not\equiv 1 \ (p)$ for any d properly dividing $(p-1)$ is called a primitive element. This just says that primitive elements exist)

Special Case $(\mathbb{Z}/7\mathbb{Z})^\times$

1	order	1	2	order	3
3	order	6	4	order	6
5	order	3	6	order	2

Proof Idea

If true, then we expect there to be a unique subgroup of order d $\forall d \mid (p-1)$ and so exactly $\phi(d)$ elements of order d.

Proof

Let $\psi(d)$ be the number of elements of order d. Then $\sum_{d \mid p-1} \psi(d) = p-1$. But $\sum_{d \mid p-1} \phi(d) = p-1$. So it suffices to show that $\psi(d) \leq \phi(d)$. Take any $d \mid p-1$. Either there are no elements of order d, in which case $\psi(d) = 0 \leq \phi(d)$. Or, there is an element a of order d. In this case, the elements $1, a, a^2, \ldots, a^{d-1}$ are all roots of $X^d - 1$. So there are no more such roots by Lagrange, and so ~~the number of~~ all elements of order d are here in the list i.e. there are exactly $\phi(d)$ of them and again $\psi(d) \leq \phi(d)$

10/10/12

Number Theory ③

Note that now, $\Psi(p-1) = \phi(p-1)$ and there are primitive roots.

Alternative View

Any finite subgroup G of the multiplicative group $F^\times$ of a field is cyclic. Let n be the order of the group, and let m be the least common multiple of the orders of the elements. $m \mid n$.

But there are n roots of $X^m - 1$, and so by Lagrange $m = n$

So it suffices to show that in any finite abelian group, there is an element of order lcm m of the order of the elements.

Let $m = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. For each i, there is an element h_i say of order $p_i^{\alpha_i} m_i$ and so an element $g_i = h_i^{m_i}$ of order exactly $p_i^{\alpha_i}$. Then the order of $g_1 \dots g_k$ is m.

2·6 Primitive Elements mod p^k

ASIDE

$(\mathbb{Z}/2\mathbb{Z})^\times$ is trivial. $(\mathbb{Z}/4\mathbb{Z})^\times$ is $\{1, 3\}$ (4), cyclic order 2.

$(\mathbb{Z}/8\mathbb{Z})^\times$ is $\{1, 3, 5, 7\}$ (8) is $C_2 \times C_2$, not cyclic.

It follows that no $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is cyclic for $n \geq 3$

(Because $(\mathbb{Z}/2^n\mathbb{Z})^\times \to (\mathbb{Z}/8\mathbb{Z})^\times$)

For all odd primes, the group $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is in fact cyclic.

In fact, if we find a generator for $(\mathbb{Z}/p^2\mathbb{Z})^\times$ it will be a generator for all such.

Proof

Take g to be a primitive element mod p : then $g^d \not\equiv 1 \ (p)$ for d a proper divisor of $p-1$, and $g^{p-1} \equiv 1 \ (p)$, so $g^{p-1} = 1 + ap$ for some a. If $a \equiv 0 \ (p)$ then $g^{p-1} \equiv 1 \ (p^2)$ and g is not a primitive element mod p^2.

But if that is the case, consider instead $h = g + p$.

Note that $h^p = (g+p)^p = g^p + p \cdot pg^{p-1} + \binom{p}{2} p^2 g^{p-2} + \ldots = g^p \ (\text{mod } p^2)$

So $h^p - h = g^p - h \ (p^2) = g^p - g - p \ (p^2)$

But $g^p = g \ (p^2)$ by nasty assumption.

Thus $h^p - h \equiv -p \ (p^2)$ and so $h^{p-1} \not\equiv 1 \ (p^2)$

So $h^{p-1} = 1 + bp$ with $(b, p) = 1$.

This shows that we can find an element g with

$$g^{p-1} = 1 + ap \quad , \quad (a, p) = 1$$

Such an element is primitive mod p^2.

12/10/12

Number Theory ④

Idea: We show (for an odd prime p) that

- There are primitive roots g mod p with $g^{p-1} = 1 + ap$, $(a,p)=1$
- Any such g is a primitive root mod p^k $\forall k \geq 1$.

Lemma

Suppose $x \equiv y \bmod p^t$ $\quad t \geq 1$.

Then $x^p \equiv y^p \bmod p^{t+1}$

Proof

$2t \geq t+1$

$x = y + kp^t$ and so $x^p = y^p + py^{p-1}kp^t + p^{2t}(\dots)$

$x^p \equiv y^p \ (p^{t+1})$

Now, for our first point, supposed that we picked g^{p-1}, primitive root mod p but with $g^{p-1} \equiv 1 \ (p^2)$. Take any $h \equiv g \ (p)$ (so that it is still a primitive root) but $h \neq g \ (p^2)$. Then $h^p = g^p \ (p^2)$ (by the above), $g^p \equiv g \ (p^2)$ by assumption. Now if $h^{p-1} \equiv 1 \ (p^2)$ then $h^p \equiv h \ (p^2)$ and we would deduce $g \equiv h \ (p^2)$ ⚡ So $h^{p-1} \not\equiv 1 \ (p^2)$

Now, suppose that g is a primitive root mod p with $g^{p-1} = 1 + ap$ $(a,p) = 1$. What is the order of g mod p^k?

- First, it divides $\phi(p^k) = (p-1)p^{k-1}$
- Second, because $(\mathbb{Z}/p^k\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$, $(p-1)$ divides it

So it is of the form $(p-1)p^r$ for some $r \leq k-1$

Then, it suffices to show that $g^{(p-1)p^{k-2}} \not\equiv 1 \ (p^k)$

Lemma'

Suppose $x = 1 + ap^r \ (p^{r+1})$. Then $x^p = 1 + ap^{r+1} \ (p^{r+2})$

Proof

By the above $x^p = (1+ap^r)^p \ (p^{r+2})$

and $(1+ap^r)^p = 1 + pap^r + \binom{p}{2} a^2 p^{2r} + p^{3r}(\dots)$

$= 1 + ap^{r+1} \ (p^{r+2})$

So it follows that $g^{(p-1)p^{k-2}} = 1 + ap^{k-1} \ (p^k) \not\equiv 1 \ (p^k)$

Thus, our g is a primitive root mod p^k $\forall k$.

Note: There are primitive roots mod $2, 4, p^k, 2p^k$, and no others.

Chapter 3 : Quadratic Reciprocity

3.1 Definitions

Let $(a, n) = 1$. Then a is a quadratic residue mod n $\Leftrightarrow x^2 \equiv a \ (n)$ is solvable. Otherwise, a is a non-residue.

We focus on the case mod p for an odd prime p.

Write $p = 2P + 1$ i.e. $P = \frac{p-1}{2}$

The residues mod p are $\{\pm 1, \pm 2, \dots, \pm P\}$

As $a^2 = b^2 \ (p) \Leftrightarrow (a-b)(a+b) \equiv 0 \ (p) \Leftrightarrow a \equiv \pm b \ (p)$

it follows that there are exactly P squares

viz $1^2 = (-1)^2, 2^2 = (-2)^2, \dots, P^2 = (-P)^2$

and so there are exactly P non-squares.

For $(a, p) = 1$, the Legendre Symbol $\left(\frac{a}{p}\right)$ is defined by $\left(\frac{a}{p}\right) = +1$ if a is square, -1 if a is not a square.

Note that the squares $S \subset (\mathbb{Z}/p\mathbb{Z})^\times$ forms a multiplicative subgroup of index 2. Hence we have a homomorphism

$$(\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times / S = \{\pm 1\}$$

$a \mapsto \left(\frac{a}{p}\right)$ is this homomorphism. In particular

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

3.2 Euler's Criterion

Let p be an odd prime and $(a,p) = 1$. Then,

$$\left(\frac{a}{p}\right) = a^{\frac{p}{2}} \ (p) \quad = a^{\frac{p-1}{2}} \ (p)$$

Proof 1

The set of residues $[1, \ldots, p-1]$ are the roots of

$$(X^{p-1} - 1) \equiv (X^{\frac{p}{2}} - 1)(X^{\frac{p}{2}} + 1)$$

Observe that if $a = b^2 \ (p)$ is a quadratic residue then $a^{\frac{p}{2}} = b^{2\frac{p}{2}} = b^{p-1} = 1 \ (p)$ and a is a root of $X^{\frac{p}{2}} - 1$.

There are $\frac{p}{2}$ such and so the $\frac{p}{2}$ non-residues must be roots of $X^{\frac{p}{2}} + 1$ i.e. they satisfy $a^{\frac{p}{2}} \equiv -1 \ (p)$

Proof 2

Let g be a primitive element so that

$1, g, g^2, \ldots, g^{p-2}$ is a complete set of residues in $(\mathbb{Z}/p\mathbb{Z})^\times$

Consider g^r. If r is even then g^r is a square, and

$(p-1) \mid r\frac{p}{2} = r\frac{p-1}{2}$ so $g^{r\frac{p}{2}} \equiv 1 \ (p)$

There are $\frac{p}{2}$ of these and so the g^r with r odd are all non-squares. For them, $(p-1) \nmid r\frac{p}{2} = r\frac{p-1}{2}$ so $g^{r\frac{p}{2}} \not\equiv 1 \ (p)$

On the other hand $(g^{r\frac{p}{2}})^2 = g^{r(p-1)} \equiv 1\ (p)$ and so $g^{r\frac{p}{2}} \equiv -1\ (p)$.

One immediate consequence: If p is an odd prime then -1 is a square mod $p \iff p \equiv 1\ (4)$

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p}{2}} = \begin{cases} +1 & \frac{p}{2} \text{ even} \quad p = 4k+1 \\ -1 & \frac{p}{2} \text{ odd} \quad p = 4k+3 \end{cases}$$

Remark

$$\left(\frac{2}{p}\right) = \begin{cases} +1 & \text{when } p = \pm 1\ (8) \\ -1 & \pm 3\ (8) \end{cases}$$

Main Result

Quadratic Reciprocity, $p \neq q$ odd primes

Then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ except in the case when both $p, q \equiv 3\ (4$

in which case $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$

$$[\mathbb{F}_q[\mu_N] : \mathbb{F}_q] = \text{order}(q) \text{ in } \left(\frac{\mathbb{Z}}{N\mathbb{Z}}\right)^*$$

$$\left(\frac{\mathbb{Z}}{8\mathbb{Z}}\right)^* = \{1, 3, 5, 7\} \cong C_2 \times C_2$$

$p \equiv 1\ (8)$, $p \equiv 1\ (4)$, -1 a square already, $[\mathbb{F}_p(\mu_8) : \mathbb{F}_p] = 1$ $\quad \left(\frac{2}{p}\right) = +1$

$p \equiv -3\ (8)$, $p \equiv 1\ (4)$, -1 a square already, $[\mathbb{F}_p(\mu_8) : \mathbb{F}_p] = 2$ $\quad \left(\frac{2}{p}\right) = -1$

$p \equiv 3\ (8)$, $p \equiv 3\ (4)$, -1 not a square, $[\mathbb{F}_p(\mu_8) : \mathbb{F}_p] = 2$

$p \equiv -1\ (8)$ $\quad p \equiv 3\ (4)$, -1 not a square, $[\mathbb{F}_p(\mu_8) : \mathbb{F}_p] = 2$

15/10/12

3.3 Gauss' Lemma

Let p be an odd prime with $P = \frac{1}{2}(p-1)$. Consider the list of residues $1, 2, \ldots, P$. For no two in the list do we have $i = \pm j$. So if $(a, p) = 1$, the same is true of the list $a\cdot 1, a\cdot 2, \ldots, a\cdot P$ and so mod p this must be the list $\pm 1, \pm 2, \ldots, \pm P$, in some order with some choice of signs.

Assume that there are $k+$ signs and $L-$ signs

Gauss Lemma

$$\left(\frac{a}{p}\right) = (-1)^L$$

Proof

We have $(a\cdot 1)(a\cdot 2)\ldots(a\cdot P) \equiv (-1)^L 1 \ldots P \ (p)$

i.e. $a^P \cdot P! \equiv (-1)^L P! \ (p)$. So $a^P \equiv (-1)^L$ and we conclude by Euler's Criterion. □

Observe that for $a = -1$, L is P and we get

$$\left(\frac{-1}{p}\right) \equiv (-1)^P$$

Remark

If $p = 4k+1$ so that P is even, then

$$P! \equiv (-1)^P P! \equiv (P+1)(P+2)\ldots(p-1)$$

So $(P!)^2 \equiv (p-1)! \equiv -1 \ (p)$

Application to the prime 2

Consider $2\cdot 1, 2\cdot 2, \ldots, 2\cdot P = (p-1)$ and we need to know how many of these are $> P$ ($[P/2]$) and how many $\leq P$ ($[P/2]$)

In case $p = 8k+1$, so that $P = 4k$, we get
$2k$ large residues $(-1)^{2k} = 1$ and 2 is a square.

$p = 8k+3$; $P = 4k+1$ gives $2k+1$ large, $(-1)^{2k+1} \equiv -1$, 2 not square

$p = 8k+5$; $P = 4k+2$ $2k+1$ large, $\equiv -1$, 2 not square

$p = 8k+7$, $P = 4k+3$ $2k+2$ large, $(-1)^{2k+2} \equiv 1$, 2 a square

3.4 Quadratic Reciprocity

Let p, q be odd primes. Then if at least one of p, q $\equiv 1\ (4)$ we have $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ and if $p \equiv q \equiv 3\ (4)$ then $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$. We can express this as

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{PQ}$$

Proofs

For $(a,p) = 1$ and $x \in \{1, \dots, P\}$ write

$$ax = p \cdot \left[\frac{ax}{p}\right] + r_x \quad \text{with} \quad 0 \le r_x < p.$$

So summing over x:

$$a \cdot \tfrac{1}{2} P(P+1) = p\left(\left[\frac{a\cdot 1}{p}\right] + \left[\frac{a\cdot 2}{p}\right] + \dots + \left[\frac{a\cdot P}{p}\right]\right) + \sum_{\text{small}} r_x + \sum_{\text{large}} r_x$$

(M = the bracketed sum)

Note that $\{r_x \mid \text{small}\} \cup \{p - r_x \mid r_x \text{ large}\}$ is just the set $\{1, \dots, P\}$

Summing, $\tfrac{1}{2}P(P+1) = Lp + \sum_{\text{small}} r_x - \sum_{\text{large}} r_x$

Subtracting: $(a-1)\cdot\tfrac{1}{2}P(P+1) = (M-L)p + 2\sum_{\text{large}} r_x$

From which it follows that $M \equiv L\ (2)$ when a is odd.

$\left(\frac{a}{p}\right) = (-1)^M$ for a odd.

15/10/12

Number Theory ⑤

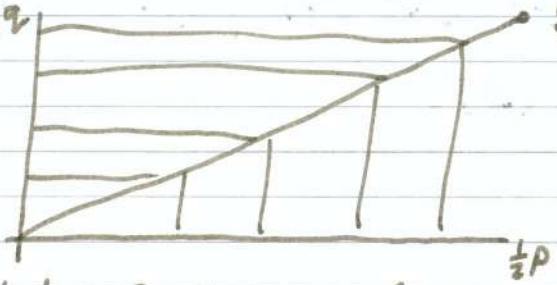
We now specialise to the theorem:

$$\left(\frac{q}{p}\right) = (-1)^M, \quad M = \left(\left\lfloor \frac{q}{p} \right\rfloor + \left\lfloor \frac{q\cdot 2}{p} \right\rfloor + \ldots + \left\lfloor \frac{q\cdot \frac{p}{2}}{p} \right\rfloor\right)$$

$$\left(\frac{p}{q}\right) = (-1)^N, \quad N = \left(\left\lfloor \frac{p}{q} \right\rfloor + \left\lfloor \frac{p\cdot 2}{q} \right\rfloor + \ldots + \left\lfloor \frac{p\cdot Q}{q} \right\rfloor\right)$$

So $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{M+N}$

Consider the integer points.



None of $\{1, \ldots, P\} \times \{1, \ldots, Q\}$ lies on the line.

How many below? Answer M.

How many above? Answer N. So $(-1)^{M+N} = (-1)^{PQ}$

3.5 Illustration

The primes 3 and -3.

① For which primes p is 3 a square?

In the case $p \equiv 1\ (4)$, this holds $\Leftrightarrow$ p^2 is a square mod 3.

$\Leftrightarrow$ $p \equiv 1\ (3)$

One good case is $p \equiv 1\ (12)$

In the case $p \equiv 3\ (4)$ this holds $\Leftrightarrow$ p is not a square mod 3

$\Leftrightarrow$ $p \equiv 2\ (3)$. Another good case is $p \equiv 11\ (12)$

② The rules still hold for negative numbers.

For which p is -3 a square mod p?

$-3 \equiv 1\ (4)$ and so this holds $\Leftrightarrow$ p is a square mod -3

$\Leftrightarrow$ p is a square mod 3 $\Leftrightarrow$ $p \equiv 1\ (3)$

(B) Another take when -3 is a square mod p.

Consider the polynomial $(X^3-1) \equiv (X-1)(X^2+X+1)$

$= (X-1)(X-\frac{1}{2}(-1+\sqrt{-3}))(X-\frac{1}{2}(-1-\sqrt{-3}))$

if $\sqrt{-3}$ exists.

This happens $\Leftrightarrow (X^3-1) \mid (X^{p-1}-1)$

i.e. $\Leftrightarrow p = 1 \ (3)$

$p=23$
$1 \le i \le 22$
when is
i a square
mod 23?

17/10/12

Number Theory ⑥

3.6 The Jacobi Symbol

Suppose n is odd. $n = p_1 \dots p_k$ not necessarily distinct prime factors. Take $(a, n) = 1$. Then the Jacobi Symbol is defined as $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\dots\left(\frac{a}{p_k}\right)$

Note that if a is a square mod p_i then it is a square mod n and so $\left(\frac{a}{n}\right) = 1$. But not vice-versa e.g.

$\left(\frac{2}{5}\right) = -1$, $\left(\frac{2}{11}\right) = -1$ but $\left(\frac{2}{55}\right) = +1$

$\left(\frac{a}{n}\right) = 1 \not\Rightarrow a$ a square

Usually sold as a computation device.

Observations

1. For any odd n, m, $(a, nm) = 1 \Leftrightarrow (a, n) = 1, (a, m) = 1$ and by the definition $\left(\frac{a}{nm}\right) = \left(\frac{a}{n}\right)\left(\frac{a}{m}\right)$
2. Recall $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, p prime, $(ab, p) = 1$.

So if $(ab, n) = 1$ with $n = p_1 \dots p_k$ then

$$\left(\frac{ab}{n}\right) = \left(\frac{ab}{p_1}\right)\dots\left(\frac{ab}{p_k}\right) = \left(\frac{a}{p_1}\right)\left(\frac{b}{p_1}\right)\dots\left(\frac{a}{p_k}\right)\left(\frac{b}{p_k}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$$

3. $\left(\frac{-1}{n}\right) = \left(\frac{-1}{p_1}\right)\dots\left(\frac{-1}{p_k}\right) = \begin{cases} +1 & \text{if } \exists \text{ even \# of primes} \equiv 3(4) \Leftrightarrow n \equiv 1(4) \\ -1 & \text{" " odd " " " " } \Leftrightarrow n \equiv 3(4) \end{cases}$

$= (-1)^{\frac{n-1}{2}}$

4. $\left(\frac{2}{n}\right) = \begin{cases} +1 & \text{if } \exists \text{ even \# primes} \equiv \pm 3(8) \Leftrightarrow n \equiv \pm 1(8) \\ -1 & \text{" " odd " " } \equiv \pm 3(8) \Leftrightarrow n \equiv \pm 3(8) \end{cases}$

and because $3^2 = 5^2 = 1\ (8)$, $3 \times 5 \equiv -1\ (8)$

5. Take m, n odd. $m = p_1 \dots p_k$, $n = q_1 \dots q_l$

Then $\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = \prod\left(\frac{p_i}{q_j}\right)\prod\left(\frac{q_j}{p_i}\right) = \prod\prod\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right)$

$$= \begin{cases} +1 & \text{even number of pairs } (i,j) \text{ with } p_i, q_j \equiv 3(4) \\ -1 & \text{odd " " " " " " " " } \end{cases}$$

$$= (-1)^{\#\{(i,j) \mid p_i, q_j \equiv 3(4)\}} = (-1)^{\#\, i\ p_i \equiv 3(4) \quad \#\, j\ q_j \equiv 3(4)}$$

$$= (-1)^{\frac{n-1}{2}\frac{m-1}{2}} \quad \text{i.e.} \quad \begin{cases} +1 & \text{if } n, m \equiv 1(4) \\ & n, m \equiv 3(4) \end{cases}$$

Remark (n odd)

$\left(\frac{a}{n}\right)$ is the sum of the permutation of $(\mathbb{Z}/n\mathbb{Z})^\times$ given by multiplication by a.

Chapter 4 : Quadratic Forms

4.1 Some results of Fermat

1. A prime p is of the form $x^2+y^2 \Leftrightarrow p \equiv 1\ (4)$ (or $p=2$)
2. A prime p is of the form $x^2+2y^2 \Leftrightarrow p \equiv 1,3\ (8)$ (or $p=2$)
3. A prime p is of the form $x^2+3y^2 \Leftrightarrow p \equiv 1\ (3)$ (or $p=3$)
4. Clearly x^2+4y^2 is a bit subsumed (see 1). What about x^2+5y^2 ? He found : — NOT respectively

If a, b are primes of the form $3, 7\ (20)$ then their product ab is of the form x^2+5y^2.

$3 \cdot 7 = 21 = 4 + 5 \cdot 1^2 = 1^2 + 5 \cdot 2^2$

$3 \cdot 23 = 69 = 7^2 + 5 \cdot 2^2$

Euler conjectured that :

If $p \equiv 1, 9\ (20)$ then p is of the form x^2+5y^2

If $p \equiv 3, 7\ (20)$ then $2p$ is of the form x^2+5y^2.

The issue is this.

We shall consider quadratic forms $ax^2+bxy+cy^2$, $a, b, c \in \mathbb{Z}$. The discriminant of a form is $d = b^2-4ac$

Observe, for example, that the form $(x+y)^2+y^2$ $= x^2+2xy+2y^2$ has to give the same numbers as x^2+y^2.

17/10/12 Number Theory ⑥

By good fortune, all forms of discriminant -4, -8, -12 are equivalent, and the same for -8, -12. But this is not true for -20, which has $2x^2+2xy+3y^2$, x^2+5y^2.

How would Fermat have proved 1. ?

- We know $kp = x^2+1$ as -1 is a square mod p.
- Take $mp = a^2+b^2$ with $|a||b| \leq \frac{1}{2}p$ so that $m < p$.
- Choose $\begin{matrix} u=a \\ v=b \end{matrix}$ mod m with $\begin{matrix} |u| \\ |v| \end{matrix} \leq \frac{1}{2}m$ so that

$lm = u^2+v^2$ with $l < m$

Then $lm^2p = (a^2+b^2)(u^2+v^2) = (au+bv)^2 + (av-bu)^2$

But $m \mid au+bv = a^2+b^2 \ (m)$, $m \mid av-bu = ab-ba \ (m)$

So $lp = A^2+B^2$ and $l < m$.

We continue this until l becomes 1.

Note

The general formula

$(x^2+cy^2)(u^2+cv^2) = (xu-cyv)^2 + c(xv+uy)^2$

(Brahmagupta)

31/10/12 Number Theory (12)

6.5 Dirichlet Series

Any arithmetic function $f: \mathbb{N} \to \mathbb{C}$ has a corresponding Dirichlet series $F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$, $s = \sigma + it \in \mathbb{C}$.

$a \wedge b$ $(a,b) \neq 1$ $b \neq 1$

Suppose that for $s_0 = \sigma_0 + it_0$ this converges absolutely.

Then for any s with $\mathrm{Re}(s) \geq \sigma_0 = \mathrm{Re}(s_0)$ we have $\left|\frac{f(n)}{n^s}\right| \leq \left|\frac{f(n)}{n^{s_0}}\right|$ and so $F(s)$ converges absolutely.

It follows that there is an abscissa of convergence $-\infty \leq a \leq +\infty$ such that if $\mathrm{Re}(s) > a$ then $F(s)$ converges absolutely, and if $\mathrm{Re}(s) < a$ $F(s)$ diverges

Now take $b > a$. Then for $\mathrm{Re}(s) \geq b$ we have $\left|\frac{f(n)}{n^s}\right| \leq \left|\frac{f(n)}{n^b}\right|$ and so $F(s)$ converges absolutely uniformly on $\mathrm{Re}(s) \geq b$. So $F(s)$ is analytic on $\mathrm{Re}(s) > a$ and we can differentiate term by term to get $F'(s) = \sum -\frac{\log n \, f(n)}{n^s}$

Suppose $F(s) = \sum_n \frac{f(n)}{n^s}$, $G(s) = \sum_n \frac{g(n)}{n^s}$ both absolutely convergent in some region. Then we can multiply out and we get $F(s)G(s) = \sum_d \frac{f(d)}{d^s} \sum_e \frac{g(e)}{e^s} = \sum_n \left(\sum_{de=n} f(d)g(e) \right) \frac{1}{n^s}$

$$= \sum_n \left(\sum_{d \mid n} f(d) g\left(\tfrac{n}{d}\right) \right) \frac{1}{n^s}$$

Recall $\zeta(s) = \sum_n \frac{1}{n^s}$ is the Dirichlet series for $f(n) \equiv 1$.

Note that $F(s)\zeta(s) = \sum_n \left(\sum_{d \mid n} f(d) \right) \frac{1}{n^s}$

Recall that we found the inverse to $\zeta(s)$ viz. $\sum_n \frac{\mu(n)}{n^s}$

So we have $1 = \sum \frac{\mu(n)}{n^s} = \sum_n \left(\sum_{d \mid n} \mu(d) \right) \frac{1}{n^s}$

So we think that in fact $\sum_{d|n} \mu(d) = \begin{cases} 1 & n=1 \\ 0 & \text{otherwise} \end{cases}$

Uniqueness Theorem for Dirichlet Series

If $F(s) = \sum_n \frac{f(n)}{n^s}$ is zero in some $\mathrm{Re}(s) > a$, then $f(n) = 0 \ \forall n \in \mathbb{N}$.

Proof

Otherwise, take $f(n_0)$, the first non-zero coefficient.

$$F(s) = \frac{f(n_0)}{n_0^s}\left(1 + \sum_{n>n_0} \frac{f(n)}{f(n_0)} \frac{n_0^s}{n^s}\right) = \frac{f(n_0)}{n_0^s}\left(1 + \sum_k \frac{f(n_0+k)}{f(n_0)} \frac{n_0^s}{(n_0+k)^s}\right)$$

Take $b > a$. Then for $s > b$,

$$\frac{n_0^s}{(n_0+k)^s} = \frac{n_0^b}{(n_0+k)^b} \frac{n_0^{s-b}}{(n_0+k)^{s-b}} \le \frac{n_0^b}{(n_0+k)^b} \frac{n_0^{s-b}}{(n_0+1)^{s-b}}$$

So $(*) \left|\sum_k \frac{f(n_0+k)}{f(n_0)} \frac{n_0^s}{(n_0+k)^s}\right| \le \left(\frac{n_0}{n_0+1}\right)^{s-b} \frac{n_0^b}{|f(n_0)|} \sum_k \frac{|f(n_0+b)|}{|n_0+k|^b}$ → const

So for s sufficiently large, the sum $(*)$ is $\le \frac{1}{2}$ and so

$$|F(s)| \ge \frac{1}{2}\left|\frac{f(n_0)}{n^s}\right| > 0 \quad \not\!\!\not$$

6.6 Calculations

Recall that $\zeta(s)$ is the Dirichlet series for $f(n) = 1$.

The Dirichlet series for $f(n) = n$ is $\sum \frac{n}{n^s} = \sum \frac{1}{n^{s-1}} = \zeta(s-$ $\mathrm{Re}(s) >$

① Recall that $\sum_{d|n} \phi(d) = n$. So

$$\left(\sum \frac{\phi(n)}{n^s}\right)\zeta(s) = \sum_n \left(\sum_{d|n} \phi(d)\right) \frac{1}{n^s} = \zeta(s-1)$$

So $\sum \frac{\phi(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)}$

② What is $(\zeta(s))^2$?

$$(\zeta(s))^2 = \sum_n \left(\sum_{d|n} 1\right) \frac{1}{n^s} = \sum \frac{\tau(n)}{n^s}$$

where $\tau(n) = \#$ divisors of n.

(3) What is $\zeta(s-1)\zeta(s)$?

$$\zeta(s-1)\zeta(s) = \sum_n \left(\sum_{d|n} d\right) \frac{1}{n^s} = \sum_n \frac{\sigma(n)}{n^s}$$ where $\sigma(n)$ is the sum of the divisors of n.

(4) von Mangoldt's Function

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k,\ k \geq 1,\ p \text{ prime} \\ 0 & \text{otherwise} \end{cases}$$

What is $\sum_{d|n} \Lambda(d)$? $(= \log n)$

So $\sum \frac{\Lambda(n)}{n^s} \zeta(s) = \sum \frac{\log n}{n^s} = -\zeta'(s)$

So $\sum \frac{\Lambda(n)}{n^s} = -\frac{\zeta'(s)}{\zeta(s)}$

18/10/12

Number Theory (7)

4.2 Basic Definitions

We consider binary quadratic forms $f(x,y) = ax^2 + bxy + cy^2$ with $a, b, c \in \mathbb{Z}$. An integer n is represented by f when $n = f(x,y)$ for some $x, y \in \mathbb{Z}$ and properly represented when $n = f(x,y)$ for $(x,y) = 1 \in \mathbb{Z}$ and f has a matrix $\begin{pmatrix} a & \frac{1}{2}b \\ \frac{1}{2}b & c \end{pmatrix}$, the matrix of the symmetric bilinear form.

The discriminant of f is $d = b^2 - 4ac$. Evidently

$d = -4 \det(\text{matrix})$

$4a\, f(x,y) = (2ax + by)^2 - dy^2$

So assuming $a \neq 0$, f is degenerate when $d = 0$
indefinite $d > 0$
definite $d < 0$

Note that $d = b^2 - 4ac = \begin{cases} \square & (4) \ b \text{ odd} \\ \square & (4) \ b \text{ even} \end{cases}$

If $d = 4k$ then $x^2 - ky^2$ has discriminant d.

If $d = 4k+1$ then $x^2 \pm xy - ky^2$ has discriminant d.

(Principal Forms of discriminant d)

4.3 Equivalence of Forms

Two forms $f(x,y)$ and $f'(x',y')$ are equivalent $\Leftrightarrow$ there is a matrix $Q = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in SL_2(\mathbb{Z}) = \{Q \in M_2(\mathbb{Z}) \mid \det Q = \}$ such that $f'(x',y') = f(px' + qy', rx' + sy')$

$= a(px' + qy')^2 + b(px' + qy')(rx' + sy') + c(rx' + sy')$

$= (ap^2 + bpr + cr^2)x'^2 + (2apq + b(ps + qr) + 2crs)x'y'$

$+ (aq^2 + bqs + cs^2)y'^2$

What does this mean?

$$f'(x',y') = (x' \; y') \begin{pmatrix} p & q \\ q & s \end{pmatrix} \begin{pmatrix} a & \frac{1}{2}b \\ \frac{1}{2}b & c \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}$$

or, the matrix B' for f' is $Q^T B Q$ where B is the matrix for f.

So you can think of f, f' as representations of the same quadratic forms with respect to different bases.

If $Q \in SL_2(\mathbb{Z})$ then Q gives a bijection

$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto Q \begin{pmatrix} x \\ y \end{pmatrix}$, $\mathbb{Z}^2 \to \mathbb{Z}^2$ with inverse $\begin{pmatrix} x \\ y \end{pmatrix} \mapsto Q^{-1} \begin{pmatrix} x \\ y \end{pmatrix}$

$Q = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$, $Q^{-1} = \begin{pmatrix} s & -q \\ -r & p \end{pmatrix}$

Evidently then equivalent quadratic forms represent the same numbers $f'(x',y') = f\left(Q \begin{pmatrix} x' \\ y' \end{pmatrix}\right)$

Get this learned

Remark

f, f' are improperly equivalent if we allow $\det Q = -1$, still the same property would hold.

In fact, we will only need to use:

$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & \pm 1 \\ 0 & 1 \end{pmatrix}$ and their inverses.

Take $f(x,y) = ax^2 + bxy + cy^2$

$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ gives $cx^2 - bxy + ay^2$

$\begin{pmatrix} 1 & \pm 1 \\ 0 & 1 \end{pmatrix}$ gives $a(x \pm y)^2 + b(x+y)y + cy^2$

$= ax^2 + (b \pm 2a)xy + (a \pm b + c)y^2$

Proposition

An integer n is properly represented by some quadratic form of discriminant $d \iff$ the congruence $x^2 \equiv d \pmod{4n}$ is solvable

18/10/12 Number Theory (7)

Proof

($\Leftarrow$) Take $b^2 \equiv d \ (4n)$, say $b^2 - 4nc = d$. Then the quadratic form $f = nx^2 + bxy + cy^2$ has discriminant d, and $f(1,0) = n$. (N.B. $\text{if } f(1,0) = 1$)

($\Rightarrow$) Suppose that f of discriminant d has $f(p,r) = n$ with $(p,r) =$
Take $q, s \in \mathbb{Z}$ such that $ps - qr = 1$.
Let f' be the form such that $f'(x,y) = f(px+qy, rx+sy)$
f' is equivalent to f and so has discriminant d. But $f'(1,0) = f(p,r) = n$
So f' is of the form $nx^2 + b'xy + c'y^2$ and so $d = b'^2 - 4nc'$
and $x^2 \equiv d \ (4n)$ is soluble.

We used the following lemma:

Lemma

If f, F' are equivalent then they have the same discriminant

Proof

The matrix for f' is $Q^T B Q = B'$ where B is the matrix for f
$\text{disc}(F') = -4 \det B' = -4 \det Q \det B \det Q = \text{disc } f$

22/10/12

Number Theory (8)

S.4 Reduction for positive definite binary quadratic forms

Write a binary quadratic form $f(x,y) = ax^2+bxy+cy^2$ as (a,b,c) in the course of calculations.

We consider positive definite forms (a,b,c) with $a>0$, $c>0$, and $d = b^2-4ac < 0$.

Note that a, c, $a \pm b \pm c$ are all properly representable.

Lemma

Suppose $a \leq c \leq a-|b|+c$ (or equivalently $|b| \leq a \leq c$).

Then, for all $|x|, |y| \geq 1$, $f(x,y) = ax^2+bxy+cy^2$, $f(x,y) \geq a-|b|+c$.

Proof

Suppose $|x| \geq |y| \geq 1$

Then $f(x,y) = ax^2+bxy+cy^2 \geq a|x|^2 - b|x||y| + c|y|^2$

$\geq (a-|b|)|x|^2 + c|y|^2 \geq (a-|b|)+c$

Similarly, this works for $|x| \leq |y|$. □

We say that (a,b,c) is semi-reduced $\Leftrightarrow |b| \leq a \leq c$.

Observation

If a form f is equivalent to a reduced form (a,b,c), then $a \leq c \leq a-|b|+c$ are the least positive integers with the property that there are $\underline{e_1}, \underline{e_2} \in \mathbb{Z}^2$, linearly independent such that $f(\underline{e_1}) = a$, $f(\underline{e_2}) = c$, $f(\underline{e_1}+\underline{e_2}) = a-|b|+c$.

Recall that the $SL_2(\mathbb{Z})$ operations act as follows:

① $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} : (a, b\ c) \mapsto (c, -b, a)$

② $\begin{pmatrix} 1 & \pm 1 \\ 0 & 1 \end{pmatrix} : (a, b, c) \mapsto (a, b \pm 2a, a \pm b + c)$

Lemma

Any positive definite form is equivalent to a semi-reduced form.

Proof

Take (a, b, c), and if it is not semi-reduced, then:

- If $a > c$ apply ①
- If $a \leq c$ but $|b| > a$, apply ② in the form that ensures that $a \pm b + c < c$.

This process terminates, since we don't do ① twice in a row, ① leaves $a+c$ fixed and ② reduces it.

53 Example

$53x^2 + 68xy + 22y^2$

22	-68	53
22	-24	7
7	24	22
7	10	5
5	-10	7
5	0	2
2	0	5

$2x^2 + 5y^2$

22/10/12

Number Theory ⑧

In two special cases, $SL_2(\mathbb{Z})$ enables us to do more.

Fist, suppose $a = c$, so the form is (a, b, a) with $|b| \leq$

$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} : (a, b, a) \longleftrightarrow (a, -b, a) : \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

So we can arrange that $b \geq 0$.

Second, suppose $|b| = a$, so the form is $(a, \pm a, c)$ with $a \leq$

$\begin{pmatrix} 1 & \pm 1 \\ 0 & 1 \end{pmatrix} : (a, -a, c) \longleftrightarrow (a, a, c) : \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$

So again we can take $b = +a$.

A positive definite binary quadratic form (a, b, c) is reduced

$\Leftrightarrow$ Either it is semi-reduced: $|b| \leq a \leq c$ and

if $a = c$ then $b \geq 0$, if $|b| = a$, then $b = a$.

Or $a \leq c$, $-a < b \leq a$, if $a = c$ then $b \geq 0$

Proposition

Any positive definite binary quadratic form is equivalent to a unique reduced form.

Proof

We know that it is equivalent to a semi-reduced form and saw that a semi-reduced is equivalent to a reduced form.

So the issue is uniqueness.

The numbers a, c, $a - |b| + c$ are determined by the form so the only ambiguity is $\pm b$.

There is no ambiguity in the special cases.

So it remains to show that if $|b| < a < c$ then the two forms $ax^2 + bxy + cy^2$ and $ax^2 - bxy + cy^2$ are not (*) equivalent.

Recall that if $f'(x', y') = a'x'^2 + bx'y' + c'y'^2$ is equivalent to $f(x, y) = ax^2 + bxy + cy^2$ via $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in SL_2$ so that $f'\begin{pmatrix} x' \\ y' \end{pmatrix} = f\left(\begin{pmatrix} p & q \\ r & s \end{pmatrix}\begin{pmatrix} x' \\ y' \end{pmatrix}\right)$, then

$a' = f(p, r)$, $c' = f(q, s)$

Suppose the two forms in (*) are equivalent via $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$

Then $a = f(p, r) = ap^2 + bpr + cr^2$ must mean

$p = \pm 1$, $r = 0$. $(\because s = \pm 1)$ (Use $|x|, |y| \geq 1 \Rightarrow f(x, y) \geq a - |b| + c$)

$c = f(q, s) = aq^2 + bqs + cs^2$ must mean $s = \pm 1$, $q = 0$

So the only possibilities are $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$; $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. But they transform (a, b, c) to (a, b, c).

24/10/12

Number Theory ⑨

S·S Reduced Forms

Suppose that (a, b, c) is a semi-reduced form of discriminant d. We have $|b| \leq a \leq c$

Now $-d = 4ac - b^2 \geq 4ac - ac = 3ac$

So it follows that $c \leq \frac{1}{3}|d|$. So we have

$|b| \leq a \leq c \leq \frac{1}{3}|d|$

Proposition

There are only finitely many (semi-) reduced forms of discriminant $d < 0$.

Proof.

Each of $|b|, a, c \leq \frac{1}{3}|d|$ so there are only finitely many choices for each.

Note for computations

$a^2 \leq ac \leq \frac{1}{3}d$, so in fact $a \leq \sqrt{\frac{|d|}{3}}$

Examples

$|b| \leq a \leq c$

$d = -31$. $a \leq \sqrt{\frac{31}{3}}$: $a \leq 3$. $4ac = b^2 + 31$.

$a = 1$ $x^2 + xy + 8y^2$ (we only get the principal form)

$a = 2$, $|b| = 0, 1, 2$ $8c = b^2 + 31$

$2x^2 \pm xy + 4y^2$

$a = 3$, $|b| = 0, 1, 2, 3$ $12c = b^2 + 31$

Nothing works.

$d = -32$ $\quad a \leq \sqrt{\frac{|d|}{3}}$, $a \leq 3$ $\quad |b| \leq a \leq c$ $\quad 4ac = b^2 + 32$

$a = 1$ $\quad x^2 + 8y^2$

$a = 2$ $\quad |b| = 0, 1, 2$ $\quad 8c = b^2 + 32$

$2x^2 + 4y^2$

$a = 3$ $\quad |b| = 0, 1, 2, 3$ $\quad 12c = b^2 + 32$

$3x^2 + 2xy + 3y^2$ (no $-2xy$, since $a = c$)

$d = -35$ $\quad x^2 + xy + 9y^2$, $3x^2 + xy + 3y^2$ (Check

5.6 Standard Applications

Recall that a number n is properly represented by a form of discriminant $d \iff x^2 \equiv d \ (4n)$ is soluble

Note that there are two cases for n odd :

① $d \equiv 1 \ (4)$. Then $x^2 \equiv d \ (4n)$ is soluble

$\iff x^2 \equiv d \ (4)$, $x^2 \equiv d \ (n)$ are soluble (CRT)

$\iff x^2 \equiv d \ (n)$ soluble.

② $d \equiv 0 \ (4)$. Then $4n \mid x^2 - d \Rightarrow x = 2y$ is even,

$4n \mid 4y^2 - d$ so this is equivalent to $n \mid y^2 - \frac{d}{4}$. So in this case the condition is $y^2 \equiv \frac{d}{4} \ (n)$ soluble.

Example

Which primes are represented by a form of discriminant -31 ?

$x^2 + xy + 8y^2$, $2x^2 \pm xy + 4y^2$

Warning : Remember the primes dividing d !!

N.b $(-1)^2 + (-1) \times 2 + 8 \times 2^2 = 31$

Number Theory ⑨

For other p we have p representable $\Leftrightarrow x^2 \equiv -31 \pmod{4p}$ soluble

$\Leftrightarrow x^2 \equiv -31 \pmod{p}$ is soluble.

$\Leftrightarrow \left(\frac{-31}{p}\right) = 1 \Leftrightarrow \left(\frac{p}{-31}\right) = \left(\frac{p}{31}\right) = 1$

So now, we write down the squares mod 31

1, 4, 9, 16, 25, 5, 18, ... and the primes congruent to these numbers mod 31 are representable and the others not.

Example

Which primes are represented by a form of $d = -32$?

(*) $x^2 + 8y^2$, $3x^2 + 2xy + 3y^2$ (don't worry about $2x^2 + 2y^2$, but note that this represents 2)

For $p \neq 2$ we have p represented by one or other of (*)

$\Leftrightarrow x^2 \equiv -32 \pmod{4p}$ is soluble $\Leftrightarrow y^2 \equiv -8 \pmod{p}$ is soluble

That holds $\Leftrightarrow -2$ is a square mod p.

N.B. $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv 1, 3 \pmod 8 \\ -1 & p \equiv 5, 7 \pmod 8 \end{cases}$

Example

Which primes are represented by a form of discriminant -35 ?

$x^2 + xy + 9y^2$, $3x^2 + xy + 3y^2$

$5, 7 \mid d$, represented by $3x^2 + xy + 3y^2$

For other p, look at $x^2 \equiv -35 \pmod{4p}$ (Think, $p = 2$?)

$$x^2 \equiv -35 \pmod{p}$$

$$\left(\frac{-35}{p}\right) = \left(\frac{-7}{p}\right)\left(\frac{5}{p}\right) = \left(\frac{p}{-7}\right)\left(\frac{p}{5}\right) = \left(\frac{p}{7}\right)\left(\frac{p}{5}\right)$$

Write out the squares mod 5, 7 :

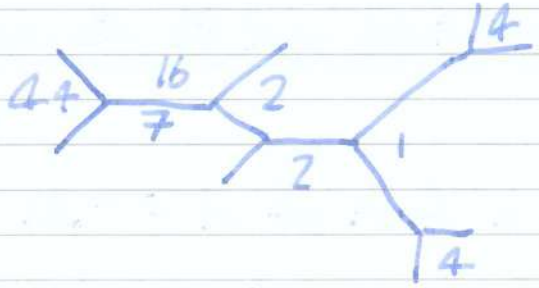
	squares	non-squares
5	1, 4	2, 3
7	1, 2, 4	3, 5, 6

Now we get 12 cases using CRT.

5.7 Conway's Topograph

$$ax^2 + bxy + cy^2$$

$$16x^2 + 21xy + 7y^2$$



26/10/12

Number Theory (10)

Chapter 6: The Riemann Zeta Function

6.1 Remarks on Infinite Products

The infinite product $\prod_1^\infty u_n$ converges to a limit L iff $\prod_1^N u_n \to L$ as $N \to \infty$. This makes sense for $u_n \in \mathbb{C}$.

Suppose for a moment that $u_n \in \mathbb{R}_{>0}$, $\forall n$. We can write $u_n = \exp(\log(u_n))$ and then

$$\prod_1^N u_n = \exp\left(\sum_1^N \log u_n\right)$$

If $\sum_1^N \log(u_n)$ converges, say to L, then $\prod_1^N u_n$ converges to $\exp(L) = e^L \in (0, \infty)$. If $\sum_1^N \log(u_n) \to \infty$ as $N \to \infty$, then $\prod_1^N u_n \to \infty$ as $N \to \infty$. If $\sum_1^N \log(u_n) \to -\infty$ as $N \to \infty$ then $\prod_1^N u_n \to 0$ as $N \to \infty$

Consider a_n with $0 < a_n < 1$. There are two cases for u_n.

$$u_n = 1 + a_n, \quad u_n = \frac{1}{1 - a_n}$$

Proposition

1. If $\sum_1^\infty a_n$ converges, then both $\prod_1^\infty (1+a_n)$ and $\prod_1^\infty (1-a_n)^{-1}$ converge to a positive real i.e. $\in (0, \infty)$.
2. If $\sum_1^\infty a_n$ diverges then $\prod_1^N (1+a_n)$ and $\prod_1^N (1-a_n)^{-1} \to \infty$ as $N \to \infty$.

Proof:

Consider first $1 + a_n$. Note that $0 < \log(1+a_n) < a_n$. So if $\sum_1^\infty a_n$ is convergent then $\sum_1^\infty \log(1+a_n)$ is convergent. So $\prod_1^\infty (1+a_n)$ is convergent to a positive real.

Conversely, note that $\prod_1^N (1+a_n) \geq 1 + \sum_1^N a_n$, and so if $\sum_1^\infty a_n$ diverges then $\prod_1^N (1+a_n) \to \infty$ as $N \to \infty$

Now consider $\frac{1}{1-a_n}$. Note that $0 < \log \frac{1}{1-a_n} = a_n + \frac{a_n^2}{2} + \frac{a_n^3}{3} + \ldots$

$$< a_n + a_n^2 + a_n^3 + \ldots = \frac{a_n}{1 - a_n}$$

Suppose $\sum_1^\infty a_n$ is convergent. Then in particular $a_n \to 0$ and so for n sufficiently large, $\log \frac{1}{1-a_n} < 2a_n$. So we deduce from $\sum a_n$ convergent that $\sum \log \frac{1}{1-a_n}$ convergent. So we get $\prod \frac{1}{1-a_n}$ converges to a positive real.

Conversely, note that $\frac{1}{1-a_n} > 1+a_n$ and so from $\sum_1^\infty a_n$ divergent we deduce $\prod_1^N (1+a_n) \to \infty$ as $N \to \infty$ and so $\prod_1^N \frac{1}{1-a_n} \to \infty$ as $N \to \infty$.

6.2 $\sum_{p \text{ prime}} \frac{1}{p}$ is divergent

Let p_n be the n^{th} prime. $p_1 = 2$, $p_2 = 3$, ... We claim that $\sum_1^\infty \frac{1}{p_n}$ is divergent.

Proof: Suppose $\sum_1^\infty \frac{1}{p_n}$ is convergent. Then $\prod_1^\infty \frac{1}{1-\frac{1}{p_n}}$ is convergent.

Consider $\prod_1^\infty \frac{1}{1-p_n^{-1}} = \prod_1^\infty \left(1 + \frac{1}{p_n} + \frac{1}{p_n^2} + \dots\right)$ is a finite product of sums of geometric series all converging absolutely, so we can rearrange. By the Fundamental Theorem of Arithmetic, this is $\sum_{n \in S_N} \frac{1}{n}$ where $S_N = \{n \mid \text{all prime factors of } n \text{ lie in } \{p_1, p_2, \dots, p_N\}\}$

$\geq \sum_1^N \frac{1}{n} \to \infty$ as $N \to \infty$ ✗

So it follows that $\prod_1^\infty \frac{1}{1-p_n^{-1}}$ and so $\sum_1^\infty \frac{1}{p_n}$ are divergent.

$a_n \geq 0$ decreasing

$\sum_1^\infty a_n$ converges $\Leftrightarrow$ $\sum_1^\infty 2^n a_{2^n}$ converges

Alternatively, suppose $\sum_1^\infty \frac{1}{p_n}$ converges, and take N such that $\sum_{n=1}^\infty \frac{1}{p_n} < \frac{1}{2}$. Let $M = p_1 p_2 \dots p_N$ and consider the numbers $rM+1$, $r \geq 1$.

$\sum_1^\infty \frac{1}{rM+1} \leq \sum_{k=1}^\infty \left(\sum_{n=1}^\infty \frac{1}{p_n}\right)^k \leq 1$. So $\sum_1^\infty \frac{1}{rM+1}$ converges ✗

Recall

$\sum_1^\infty \frac{1}{n}$ diverges but $\sum_1^\infty \frac{1}{n^\alpha}$ converges for $\alpha > 1$.

$\sum_1^\infty \frac{1}{n \log n}$ diverges but $\sum_1^\infty \frac{1}{n (\log n)^\alpha}$ converges for $\alpha > 1$

(and so on. Cauchy's Condensation Test)

Why? $\int \frac{dx}{x(\log x)^\alpha} = \int \frac{dy}{y^\alpha}$

Fact: p_n fits into this picture. It is relatively elementary that p_n is of order $n \log n$. The Prime Number Theorem says that $p_n \sim n \log n$, $\frac{p_n}{n \log n} \to 1$ as $n \to \infty$.

Equivalent form: $\pi(x) = \#$ primes $\leq x$ and then the Prime Number Theorem says that $\pi(x) \sim \frac{x}{\log x}$

Number Theory (11)

5.3 The Riemann-Zeta Function

Set $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ for $s = \sigma + it \in \mathbb{C}$.

Note that $\frac{1}{n^s} = \exp(s \log(\frac{1}{n}))$ and so $\frac{1}{n^{it}}$ has modulus 1

i.e. $\left|\frac{1}{n^s}\right| = \left|\frac{1}{n^\sigma}\right|$

For s real, $\zeta(s)$ is absolutely convergent on $(1, \infty)$. So for $Re(s) > 1$, $\zeta(s)$ is absolutely convergent, and therefore convergent.

Take $\delta > 0$. For real $s \in [1+\delta, \infty)$, $\zeta(s)$ is absolutely uniformly convergent. So for $Re(s) \geq 1+\delta$, $\zeta(s)$ is absolutely uniformly convergent, so it converges to an analytic function on $Re(s) > 1$.

Note that uniform convergence means that we can differentiate term by term. So:

$$\zeta'(s) = \sum_{n=1}^{\infty} -\frac{\log n}{n^s}$$

Elementary estimates for $s \in \mathbb{R}$:

i) $$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \int_1^{\infty} \frac{dx}{x^s} + \sum_{n=1}^{\infty} \int_n^{n+1} \left(\frac{1}{n^s} - \frac{1}{x^s}\right) dx$$

$$= \frac{1}{s-1} + \text{remainder}$$

On $[n, n+1]$, $\left|\frac{1}{n^s} - \frac{1}{x^s}\right| \leq s \cdot \frac{1}{n^{s+1}} \leq s\frac{1}{n^2}$ for $s \geq 1$

So $\left|\zeta(s) - \frac{1}{s-1}\right| \leq s \sum_{n=1}^{\infty} \frac{1}{n^2}$ and so as $s \to 1$ we have

$$\zeta(s) = \frac{1}{s-1} + O(1)$$

Similarly:

$$\zeta'(s) = -\frac{1}{(s-1)^2} + O(1) \text{ as } s \to 1$$

ii) Consider $\sum_{n=1}^{\infty} \frac{2}{(2n)^s} = \sum_{n=1}^{\infty} \frac{2}{2^s} \cdot \frac{1}{n^s} = 2^{1-s}\zeta(s)$

Now, $(2^{1-s}-1)\zeta(s) = 2\sum_{n=1}^{\infty} \frac{1}{(2n)^s} - \sum_{n=1}^{\infty} \frac{1}{n^s}$ | By absolute convergence of the series, we can rearrange terms

$= \sum_{n=1}^{\infty} (-1)^n/n^s = -1 + \frac{1}{2^s} - \frac{1}{3^s} + \ldots$

think about even and odd terms

So $-1 < \sum_{n=1}^{\infty} \frac{(-1)^n}{n^s} < -1 + \frac{1}{2^s} \leq -1 + \frac{1}{2} = -\frac{1}{2}$

and so $\frac{1}{2} < (1 - 2^{1-s})\zeta(s) < 1$

In particular $1 < \zeta(s) < \frac{1}{1-2^{1-s}} \to 1$ as $s \to \infty$

So $\zeta(s) \to 1$ as $s \to \infty$

Fact

$\zeta(s)$ extends by analytic continuation to $\mathbb{C} \setminus \{1\}$ with a simple pole at $s=1$. It has zeroes at $-2, -4, \ldots$ and no other zeroes outside the critical strip $0 \leq \mathrm{Re}(s) \leq 1$.

The Riemann Hypothesis

All zeroes of $\zeta(s)$ in $0 \leq \mathrm{Re}(s) \leq 1$ lie on the line $\mathrm{Re}(s) = \frac{1}{2}$

5.4 Euler's Identity

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1-p^{-s}}$$

$$= \prod_{p \text{ prime}} (1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \ldots)$$

This is formally evident by the Fundamental Theorem of ~~Algebra~~ Arithmetic, so the question is one of convergence.

Consider $\prod_{\substack{p \text{ prime} \\ p \leq N}} \left(\frac{1}{1-p^{-s}}\right) = \prod_{\substack{p \text{ prime} \\ p \leq N}} (1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \ldots)$

This is a finite product of an absolutely convergent series, so we can multiply out to get $\sum_{n \in S_N} \frac{1}{n^s}$ (by the Fundamental Theorem of Arithmetic)

Number Theory II

Here, S_N is the set of numbers with no prime factor $> N$.

Hence $\left|\zeta(s) - \prod_{p \le N} \frac{1}{1-p^{-s}}\right| = \left|\sum_{n \notin S_N} \frac{1}{n^s}\right| \le \sum_{n \notin S_N} \left|\frac{1}{n^s}\right|$

$\le \sum_{n=N+1}^{\infty} \left|\frac{1}{n^s}\right| \to 0$ as $N \to \infty$.

So $\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1-p^{-s}}$

We guess that $(\zeta(s))^{-1} = \prod_{p \text{ prime}} (1-p^{-s})$. Is this true?

Consider the Möbius function $\mu(n) = \begin{cases} (-1)^k & \text{if } n \text{ is a product of } k \text{ distinct primes} \\ 0 & \text{otherwise} \end{cases}$

Claim: $\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \prod_{p \text{ prime}} (1-p^{-s})$ for $\mathrm{Re}(s) > 1$

Consider $\prod_{p \le N} (1-p^{-s}) = \sum_{n \in S_N} \frac{\mu(n)}{n^s}$

As before, we see that

$\left|\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} - \prod_{p \le N} (1-p^{-s})\right| = \left|\sum_{n \notin S_N} \frac{\mu(n)}{n^s}\right| \le \sum_{n \notin S_N} \left|\frac{\mu(n)}{n^s}\right|$

$\le \sum_{n=N+1}^{\infty} \left|\frac{1}{n^s}\right| \to 0$ as $N \to \infty$

We have $\prod_{p \le N} \frac{1}{1-p^{-s}} \to \zeta(s)$

and $\prod_{p \le N} (1-p^{-s}) \to \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$ as $N \to \infty$

Multiplying, we obtain $1 \to \zeta(s) \cdot \sum_{n=1}^{N} \frac{\mu(n)}{n^s}$ as $N \to \infty$

So $\zeta(s) \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = 1$, and

$$\zeta(s) = 1 \Big/ \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$$

In particular, $\zeta(s)$ has no zeroes in $\mathrm{Re}(s) > 1$.

Remarks

i) $\zeta(s) = \prod_p \frac{1}{1-p^{-s}}$ tells us that there are infinitely many primes in a strong way. Otherwise, the right hand side is a finite product, so has a finite value at $s=1$. But we know that $\zeta(s) \to \infty$ as $s \to 1^+$.

ii) Warning:

Letting $s \to 1$ in $\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \prod_p (1-p^{-s})$

is not a trivial matter.

The fact that $\prod_p (1 - \frac{1}{p})$ converges to 0 is elementary.

But $\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = 0$ is not.

02/11/12 Number Theory (13)

6.7 Arithmetic Functions

On functions $f: \mathbb{N} \to \mathbb{C}$ we can define the convolution product

$$f * g(n) = \sum_{d|n} f(d)\, g\left(\frac{n}{d}\right)$$

This is associative, commutative and with unit

$$I(n) = \begin{cases} 1 & \text{if } n=1 \\ 0 & \text{otherwise} \end{cases}$$

Let $u(n) = 1$. We saw that

$$u * \mu(n) = \sum_{d|n} \mu(d) = \begin{cases} 1 & n=1 \\ 0 & \text{otherwise} \end{cases} \quad \text{i.e. } u * \mu = I$$

This is purely combinatorial.

If $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, $\alpha_i \geq 1$ then for $S \subseteq \{1, \dots, k\}$

$\mu\left(\prod_{i \in S} p_i\right) = (-1)^{\text{sgn}(S)}$ and μ is 0 otherwise

So $\sum_{d|n} \mu(d) = \sum_{S \subseteq [1,\dots,k]} (-1)^{\text{sgn}(S)} = \begin{cases} 1 & n=1 \text{ or } \{1,\dots,k\} = \emptyset \\ 0 & \text{for } k \geq 1 \end{cases}$

For # of even subsets of a finite set

$$- \text{\# odd subsets of the set} = \begin{cases} 1 & \text{set is } \emptyset \\ 0 & \text{otherwise} \end{cases}$$

Because $(1-1)^n = \begin{cases} 1 & n=0 \\ 0 & \text{otherwise} \end{cases}$

Remark

$f(n)$ is invertible if and only if $f(1)$ is invertible.

Möbius Inversion Formula

Let f, g be arithmetic functions.

Then $g(n) = \sum_{d|n} f(d)$ iff $f(n) = \sum_{d|n} g(n)\, \mu\left(\frac{n}{d}\right)$

Because:

$$LHS \iff g = f * u \iff f = g * \mu \iff RHS$$

An arithmetic function is multiplicative iff

$f(n \times m) = f(n) f(m)$ for $(n, m) = 1$

For example, ϕ is multiplicative.

Suppose that f, g are multiplicative. Take $(n, m) = 1$

Then $f * g(nm) = \sum_{d \mid nm} f(d)\, g\left(\frac{nm}{d}\right)$

$$= \sum_{a \mid n,\, b \mid m} f(ab)\, g\left(\left(\frac{n}{a}\right)\left(\frac{m}{b}\right)\right)$$

$$= \sum_{a \mid n,\, b \mid m} f(a) f(b)\, g\left(\frac{n}{a}\right) g\left(\frac{m}{b}\right)$$

$$= \sum_{a \mid n} f(a)\, g\left(\frac{n}{a}\right) \sum_{b \mid m} f(b)\, g\left(\frac{m}{b}\right)$$

$$= (f * g)(n)\, (f * g)(m)$$

Thus $f * g$ is multiplicative.

Note

A multiplicative function f is determined by the values $f(p^k)$, p prime.

If f is multiplicative then the Dirichlet series (assuming absolute convergence) has a product expansion $F(s) = \prod_{p \text{ prime}} \left(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \dots\right)$

with argument as before.

f is completely multiplicative iff $f(nm) = f(n) f(m)$. In that case f is determined by $f(p)$, p prime, and the Dirichlet series has the product expansion

$$F(s) = \prod_{p \text{ prime}} \left(\frac{1}{1 - f(p)/p^s}\right)$$

02/11/12 Number Theory (13)

7.1 Legendre's Formula

Prelude

We have $\sum_{p \text{ prime}} \frac{1}{p} = \infty$ so "there are a lot of primes" e.g more than squares since $\sum_n \frac{1}{n^2} < \infty$.

The Prime Number Theorem says that $\pi(x) \sim \frac{x}{\log(x)}$ and in particular, $\frac{\pi(x)}{x} \to 0$ as $x \to \infty$, $\pi(x) = o(x)$

We give an old proof of this.

Fact

Suppose $a_1, \ldots, a_k$ are coprime numbers. Then the number $\phi(x, \underline{a})$ of the integer $\leq x$ and not divisible by $a_1, \ldots, a_k$ is

$$\phi(x, \underline{a}) = \lfloor x \rfloor - \sum_i \left\lfloor \frac{x}{a_i} \right\rfloor + \sum_{i \neq j} \left\lfloor \frac{x}{a_i a_j} \right\rfloor - \ldots$$

(Inclusion - Exclusion Principle)

Aside

Let $p_1, \ldots, p_k$ be the primes dividing n.

Then $\phi(n) = n - \sum_i \frac{n}{p_i} + \sum_{i \neq j} \frac{n}{p_i p_j} + \ldots$

$$= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_k}\right)$$

In particular $\phi(x, N) = \#$ of +ve integers $\leq x$ not divisible by the first N primes

then $\phi(x, N) = \lfloor x \rfloor - \sum_{i \in N} \left\lfloor \frac{x}{p_i} \right\rfloor + \sum_{i,j \in N} \left\lfloor \frac{x}{p_i p_j} \right\rfloor - \ldots$

Note also the following. A number $\leq x$ is composite iff it is divisible by a prime $\leq \sqrt{x}$. So the numbers contributing to $\phi(x, \pi\sqrt{x})$ are 1 together with primes $\leq x$ but $> \sqrt{x}$

So $\phi(x, \pi(\sqrt{x})) = 1 + \pi(x) - \pi(\sqrt{x})$

We have $\phi(x, N) = \lfloor x \rfloor - \sum \lfloor \frac{x}{p_i} \rfloor + \sum \lfloor \frac{x}{p_i p_j} \rfloor - \ldots$

$\pi(x) \leq N + \phi(x, N)$

[For the primes $\leq N$ are either among the first N primes or not divisible by any of the first N primes]

We deduce $\pi(x) \leq N + (x - \sum \frac{x}{p_i} + \sum \frac{x}{p_i p_j} - \ldots) + 2^N$

[Because removing $\lfloor \cdot \rfloor$ changes the value by at most 1 each time and there are 2^N $\lfloor \cdot \rfloor$ in the expression]

So $\pi(x) \leq 2^{N+1} + x \tilde{\prod_1^N} (1 - \frac{1}{p_i})$

But $\tilde{\prod_1^N} (1 - \frac{1}{p_i})$ diverges to 0 as $N \to \infty$ (ζ function)

Take $\varepsilon > 0$. Choose N so that $\tilde{\prod_1^N} (1 - \frac{1}{p_i}) < \varepsilon$.

Then $\pi(x) < 2^{N+1} + \varepsilon x$. Now take $x > 2^{N+1}/\varepsilon$.

Then $\pi(x) < \varepsilon x + \varepsilon x = 2\varepsilon x$

Thus we can make $\frac{\pi(x)}{x}$ arbitrarily small and

$\frac{\pi(x)}{x} \to 0$ as $x \to \infty$.

7.2 Primes in Binomial Coefficients

What power of a prime p divides $n!$?

$\lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \lfloor \frac{n}{p^3} \rfloor + \cdots$

Aside: $n! = \prod_p p^{\sum_r \lfloor n/p^r \rfloor}$ and taking logs,

$\log n! = \sum_p \left(\sum_r \lfloor \frac{n}{p^r} \rfloor \right) \log p \leq n \sum_p \frac{\log p}{p-1}$

It follows that the power of p dividing $\binom{2n}{n} = \frac{(2n)!}{(n!)(n!)}$

is $\sum_r \lfloor \frac{2n}{p^r} \rfloor - 2\lfloor \frac{n}{p^r} \rfloor$

Observe that $\lfloor \frac{2n}{p^r} \rfloor - 2\lfloor \frac{n}{p^r} \rfloor = \begin{cases} 0 \text{ if } k \leq \frac{n}{p^r} < k+\frac{1}{2} \\ 1 \text{ if } k+\frac{1}{2} \leq \frac{n}{p^r} < k+1 \end{cases}$ some $k \in \mathbb{Z}$

Also, we can take the sum from $r=1$ to R, where R is the largest number such that $p^R \leq 2n$.

(*) It follows that the contribution of a power of p to $\binom{2n}{n}$ is $p^{R'}$ with $R' \leq R$, and so is $\leq 2n$.

Aside

Observe that $\therefore \binom{2n}{n} \mid u(2n)$ where $u(x)$ is the least common multiple of all the integers $\leq x$.

Let $\psi(x) = \log u(x) = \sum_{p^r \leq x} \log p = \sum_{m \leq x} \Lambda(m)$

Note that $\binom{2n}{n} = \frac{2n}{n} \cdot \frac{2n-1}{n-1} \cdots \frac{n+1}{1} > 2^n$

and $n \log 2 < \log \binom{2n}{n} < \psi(2n)$

We also have $\vartheta(x) = \sum_{p \leq x} \log p$

Facts:

$\vartheta(x) \sim \psi(x)$ and $\pi(x) \sim \frac{\vartheta(x)}{\log x} \sim \frac{\psi(x)}{\log x}$

Back to $\sum_r \left\lfloor \frac{2n}{p^r} \right\rfloor - 2\left\lfloor \frac{n}{p^r} \right\rfloor$

Two Special Cases

① $n \le p \le 2n$. Then we have $\left\lfloor \frac{2n}{p} \right\rfloor - 2\left\lfloor \frac{n}{p} \right\rfloor = 1$.

which is in any case evident.

② $\frac{2}{3}n < p \le n$. Then, $p, 2p \le 2n$ but $3p \not\le 2n$ and $p \le n$ but $2p \not\le n$. (the important case)

Then we have $\left\lfloor \frac{2n}{p} \right\rfloor - 2\left\lfloor \frac{n}{p} \right\rfloor = 2 - 2 \cdot 1 = 0$

7.3 Upper Bound on Product of Primes

Proposition

For $n \ge 1$, $\prod_{p \le n} p < 4^n$

Proof

True for $n=1$, $n=2$, by inspection. Now we argue inductively.

Suppose $n = 2m+1$ is odd and > 1. Then,

$$\prod_{p \le n} p = \prod_{p \le m+1} p \cdot \prod_{m+1 < p \le 2m+1} p$$

Each p in $m+1 < p \le 2m+1$ appears (just once) in $\binom{2m+1}{m+1} = \binom{2m+1}{m}$. Now $\binom{2m+1}{0} + \binom{2m+1}{1} + \cdots + \binom{2m+1}{m+1} + \binom{2m+1}{m} = 2^{2m+1}$

and so $2\binom{2m+1}{m+1} < 2^{2m+1}$ and so $\binom{2m+1}{m+1} < 4^m \ (= 2^{2m})$

Now $\prod_{p \le n} p < 4^{m+1} \cdot 4^m = 4^{2m+1} = 4^n$

In the case $n = 2m > 2$ even,

$$\prod_{p \le n} p = \prod_{p \le n-1} p < 4^{n-1} < 4^n$$

(Aside $\vartheta(n) < n \log 4$)

05/11/12 Number Theory (14)

7.4 Bertrand's Postulate

For every $n \geq 1$, there is a prime p with $n < p \leq 2n$.

Idea: otherwise $\binom{2n}{n}$ is too small. Note that in $\binom{2n}{0} + \binom{2n}{2n} + \binom{2n}{1} + \dots + \binom{2n}{2n-1} = 2^{2n}$, $\binom{2n}{n}$ is the largest of $2n$ terms so $\binom{2n}{n} > \frac{1}{2n} 2^{2n} = \frac{1}{2n} 4^n$

Suppose there is no p in $(n, 2n]$. Then the p appearing in $\binom{2n}{n}$ are all $\leq \frac{2}{3}n$.

Take the $p \leq \sqrt{2n}$: there are $\leq \sqrt{2n}$ such and each contributes at most $2n$. The $p > \sqrt{2n}$ contribute at most 1.

It follows that $\binom{2n}{n} < (2n)^{\sqrt{2n}} \prod_{p \leq \frac{2}{3}n} p < (2n)^{\sqrt{2n}} 4^{\frac{2}{3}n}$

$\frac{1}{2n} 4^n < (2n)^{\sqrt{2n}} 4^{\frac{2}{3}n}$

In other words $4^{\frac{1}{3}n} < (2n)^{\sqrt{2n}+1}$

But as n increases this must fail as the LHS increases quicker. Consider e.g. $\frac{1}{3} n \log 4 < (\sqrt{2n}+1) \log 2n$

When the inequality fails, it will stay false.

Try $n = 2^{11}$ and take $\log_2$

$\frac{1}{3} 2^{12} < (2^6+1) 12$ false

So Bertrand is true for sufficiently large $n \geq 2^{11}$.

Check small values.

2, 3, 5, 7, 13, 23, 43, ...

07/11/12 Number Theory (15)

Chapter 8 : Continued Fractions

8.1 Example of Euclid's Algorithm

$89 = 3 \times 26 + 11$ $\quad 1 \quad -3$

$26 = 2 \times 11 + 4$ $\quad -2 \quad 7$

$11 = 2 \times 4 + 3$ $\quad 5 \quad -17$

$4 = 1 \times 3 + 1$ $\quad -7 \quad 24$

$3 = 3 \times 1 + 0$ $\quad 26 \quad -89$

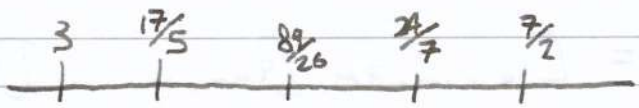
$\frac{89}{26} = 3 + \frac{11}{26}$ $\quad 1 \quad 3$ $\quad 3 = \frac{3}{1}$

$\frac{26}{11} = 2 + \frac{4}{11}$ $\quad 2 \quad 7$ $\quad 3 + \frac{1}{2} = \frac{7}{2}$

$\frac{11}{4} = 2 + \frac{3}{4}$ $\quad 5 \quad 17$ $\quad 3 + \frac{1}{2 + \frac{1}{2}} = \frac{17}{5}$

$\frac{4}{3} = 1 + \frac{1}{3}$ $\quad 7 \quad 24$ $\quad 3 + \frac{1}{2 + \frac{1}{1}} = \frac{24}{7}$

$\frac{3}{1} = 3$ $\quad 26 \quad 89$ $\quad 3 + \frac{1}{2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{3}}}} = \frac{89}{26}$



8.2 Continued Fraction Expansion of a Real

Let θ be real. We can write $\theta_0 = \theta = \lfloor \theta_0 \rfloor + \{\theta_0\}$ $\quad 0 \le \{\theta_0\} < 1$

$$\theta_0 = \begin{cases} a_0 \text{ if } \theta_0 \text{ is an integer, so we stop.} \\ a_0 + \frac{1}{\theta_1} \text{ where } \theta_1 = \frac{1}{\{\theta_0\}} \text{ otherwise} \end{cases}$$

Continue, writing $\theta_1 = \begin{cases} a_1 \text{ if } \theta_1 \text{ an integer, so we stop} \\ a_1 + \frac{1}{\theta_2}, \ \theta_2 = \frac{1}{\{\theta_1\}} \end{cases}$

We get, so long as we continue:

$$\theta = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \cfrac{1}{a_{n-1} + \frac{1}{\theta_n}}}}} = a_0 + \frac{1}{a_1 + \dots} + \frac{1}{a_2 + \dots} + \frac{1}{a_3 + \dots} + \dots + \frac{1}{\theta_n}$$

The returned numbers, $[a_0] = a_0$, $[a_0, a_1] = a_0 + \frac{1}{a_1}, \dots$ are convergents to θ.

If we stop with $\theta = [a_0, a_1, a_2, \ldots, a_n]$ then clearly θ is rational. Is the converse evident? (Euclid's Algorithm)

Note

a_0 can be any integer, but for $i \geq 2$, $a_i \geq 1$.

$\theta_0 = \sqrt{2} = 1 + \frac{1}{\theta_1}$, where $\theta_1 (\sqrt{2} - 1) = 1$, $\theta_1 = \sqrt{2} + 1$

$\theta_1 = \sqrt{2} + 1 = 2 + \frac{1}{\theta_2}$, where $\theta_2 = \sqrt{2} + 1$

So $\sqrt{2} = 1 + \frac{1}{2 + \ldots} + \frac{1}{2 + \ldots} + \ldots$ as a continued fraction.

8.3 Order Properties

We have finite continued fractions

$$[a_0, a_1, a_2, \ldots, a_n] = a_0 + \frac{1}{a_1 + \ldots} + \frac{1}{a_2 + \ldots} + \ldots + \frac{1}{a_{n-1} + \frac{1}{a_n}}$$

Note that $[a_0, a_1, \ldots, a_n] = [a_0, [a_1, a_2, \ldots, a_n]]$

$= [a_0, a_1, \ldots, a_{n-2}, [a_{n-1}, a_n]]$

Equally $[a_0, \ldots, a_n] = [a_0, \ldots, a_m, [a_{m+1}, \ldots, a_n]]$

for any $1 < m < n$. Note the following:

① $[a_0]$ is order preserving in its last argument

② $[a_0, a_1] = a_0 + \frac{1}{a_1}$ is order reversing in its last argument.

Inductively, it follows that $[a_0, \ldots, a_n]$ is order preserving / order reversing in its last argument if n even / n odd.

For, if n is even, $[a_0, \ldots, a_n] = [a_0, \ldots, a_{n-2}, [a_{n-1}, a_n]]$ is an order reversing function of an order reversing function in the last argument.

Similarly, if n is odd, $[a_0, \dots, a_n] = [a_0, \dots, a_{n-2}, [a_{n-1}, a_n]]$ is an order preserving function of an order reversing function.

Note that $[a_0] < [a_0, a_1]$, So

$$[a_0, \dots, a_{2m}, a_{2m+1}] = [a_0, \dots, a_{2m-1}, [a_{2m}, a_{2m+1}]]$$
$$> [a_0, \dots, a_{2m-1}, a_{2m}]$$

$$[a_0, \dots, a_{2m+1}, a_{2m+2}] = [a_0, \dots, a_{2m}, [a_{2m+1}, a_{2m+2}]]$$
$$< [a_0, \dots, a_{2m}, a_{2m+1}]$$

Also, $[a_0] = a_0 < [a_0, a_1, a_2] = a_0 + \frac{1}{a_1 + \dots} + \frac{1}{a_2}$

So $[a_0, \dots, a_{2m}] < [a_0, \dots, a_{2m-1}, [a_{2m}, a_{2m+1}, a_{2m+2}]] = [a_0, \dots, a_{2m+2}]$

and $[a_0, \dots, a_{2m+1}] > [a_0, \dots, a_{2m}, [a_{2m+1}, a_{2m+2}, a_{2m+3}]] = [a_0, \dots, a_{2m+3}]$

So the even convergents are always less than the odd.

8.4 Algebraic Properties

Given $[a_0, \dots, a_n]$ we have the initial convergents:

$$[a_0] = a_0 = \frac{a_0}{1}$$

$$[a_0, a_1] = a_0 + \frac{1}{a_1} = \frac{a_1 a_0 + 1}{a_1}$$

$$[a_0, a_1, a_2] = a_0 + \frac{a_2}{a_1 a_2 + 1} = \frac{a_2 a_1 a_0 + a_0 + a_2}{a_2 a_1 + 1}$$

(Next time) Write $[a_0, \dots, a_n] = \frac{p_n}{q_n}$

Two ways to think:

- $a_0, a_1, \dots, a_n$ are values, and the question might be 'Is $\frac{p_n}{q_n}$ in lowest terms?'
- $a_0, a_1, \dots, a_n$ are indeterminates and the question might be 'Are the polynomials p_n, q_n relatively prime?'

29/11/12 Number Theory (16)

We have $p_0 = a_0$, $q_0 = 1$

$p_1 = a_1 a_0 + 1$, $q_1 = a_1$

$p_2 = a_2 a_1 a_0 + a_0 + a_2$, $q_2 = a_2 a_1 + 1$

Note that $p_2 = a_2 p_1 + p_0$, $q_2 = a_2 q_1 + q_0$

Claim

$p_{n+2} = a_{n+2} p_{n+1} + p_n$, $q_{n+2} = a_{n+2} q_{n+1} + q_n$

for all $n \geq 0$ (†)

Proof (By induction)

The case $n = 0$ is above.

For $n > 0$, assume $p_{n+1} = a_{n+1} p_n + p_{n-1}$, $q_{n+1} = a_{n+1} q_n + q_{n-1}$

and we prove (†)

1) $[a_0, \dots, a_{n+2}] = [a_0, \dots, a_n, [a_{n+1}, a_{n+2}]]$

$= [a_0, \dots, a_n, a_{n+1} + \frac{1}{a_{n+2}}]$

By the inductive hypothesis, this is

$$\frac{(a_{n+1} + \frac{1}{a_{n+2}}) p_n + p_{n-1}}{(a_{n+1} + \frac{1}{a_{n+2}}) q_n + q_{n-1}} = \frac{a_{n+2} a_{n+1} p_n + p_n + a_{n+2} p_{n-1}}{a_{n+2} a_{n+1} q_n + q_n + a_{n+2} q_{n-1}}$$

$$= \frac{a_{n+2}(a_{n+1} p_n + p_{n-1}) + p_n}{a_{n+2}(a_{n+1} q_n + q_{n-1}) + q_n} = \frac{a_{n+2} p_{n+1} + p_n}{a_{n+2} q_{n+1} + q_n} = \frac{p_{n+2}}{q_{n+2}}$$

as desired

2) $[a_0, \dots, a_{n+2}] = [a_0, [a_1, \dots, a_{n+2}]] = [a_0, \frac{p_{n+1}^+}{q_{n+1}^+}]$

where $(\cdot)^+$ denotes the same polynomial but with the variables $a_0, a_1, \dots$ replaced by $a_1, a_2, \dots$

So $[a_0, \ldots, a_{n+2}] = a_0 + \frac{q_{n+1}^+}{p_{n+1}^+} = \frac{a_0 p_{n+1}^+ + q_{n+1}^+}{p_{n+1}^+}$

Note generally that $p_{n+1} = a_0 p_n^+ + q_n^+$, $q_{n+1} = p_n^+$

So $[a_0, \ldots, a_{n+2}] = \frac{a_0 (a_{n+2} p_n^+ + p_{n-1}^+) + a_{n+2} q_n^+ + q_{n-1}^+}{a_{n+2} p_n^+ + p_{n-1}^+}$

$= \frac{a_{n+2} (a_0 p_n^+ + q_n^+) + a_0 p_{n-1}^+ + q_{n-1}^+}{a_{n+2} p_n^+ + p_{n-1}^+} = \frac{a_{n+2} p_{n+1} + p_n}{a_{n+2} q_{n+1} + q_n} = \frac{p_{n+2}}{q_{n+2}}$

as desired. □

Let us rewrite (†) as follows:

$$\begin{pmatrix} p_{n+1} & p_{n+2} \\ q_{n+1} & q_{n+2} \end{pmatrix} = \begin{pmatrix} p_n & p_{n+1} \\ q_n & q_{n+1} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & a_{n+2} \end{pmatrix}$$

Observe that $\begin{pmatrix} p_0 & p_1 \\ q_0 & q_1 \end{pmatrix} = \begin{pmatrix} a_0 & a_1 a_0 + 1 \\ 1 & a_1 \end{pmatrix}$

so $\det \begin{pmatrix} p_0 & p_1 \\ q_0 & q_1 \end{pmatrix} = -1$

Also $\det \begin{pmatrix} 0 & 1 \\ 1 & a_{n+2} \end{pmatrix} = -1$, so it follows that

$$\det \begin{pmatrix} p_{n+1} & p_{n+2} \\ q_{n+1} & q_{n+2} \end{pmatrix} = (-1)^{n+1}$$

Multiplying out, we get $p_n q_{n+1} - p_{n+1} q_n = (-1)^{n+1}$

So we have $\frac{p_n}{q_n}$ as a polynomial in lowest terms. If we insert integer values we get a fraction in lowest terms i.e. $(p_n, q_n) = 1$.

Aside: $\begin{pmatrix} p_n & p_{n+2} \\ q_n & q_{n+2} \end{pmatrix} = \begin{pmatrix} p_n & p_{n+2} \\ q_n & q_{n+2} \end{pmatrix} \begin{pmatrix} 1 & \bullet \\ 0 & a_{n+2} \end{pmatrix}$

and so $p_n q_{n+2} - p_{n+2} q_n = (-1)^{n+1} a_{n+2}$

7.5 Convergence of Continued Fractions

From $p_n q_{n+1} - p_{n+1} q_n = (-1)^{n+1}$ we deduce

$$\left| \frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}} \right| = \frac{1}{q_n q_{n+1}} \quad \left(< \frac{1}{q_n^2} \text{ when } n \geq 1 \right)$$

Note that from $q_{n+2} = a_{n+2} q_{n+1} + q_n$ we get $q_{n+2} \geq q_{n+1} + q_n$ and so (bounded below by Fibonacci), $q_{n+2} \to \infty$ as $n \to \infty$

Recall that we have the even convergents $\leq$ odd convergents.

The evens are increasing, and the odds are decreasing.

So, since the difference between successive convergents tends to zero, we deduce that an infinite continued fraction converges.

Also, if θ has continued fraction $[a_0, a_1, \ldots]$, then we have $\theta = [a_0, \ldots, a_{n-1}, \theta_n]$, with $a_n = [\theta_n] \leq \theta_n$, and so by the order properties

$$\frac{p_n}{q_n} = [a_0, a_1, \ldots, a_n] \lesseqgtr \theta, \text{ for } n \overset{\text{even}}{\underset{\text{odd}}{}}.$$

So the continued fraction converges to θ.

Suppose continued fractions $[a_0, a_1, \ldots] = [a_0', a_1', \ldots]$ where both continue beyond $i = 0$. Then

$$[a_0, \theta_1] = [a_0', \theta_1']$$

$$a_0 + \frac{1}{\theta_1} = a_0' + \frac{1}{\theta_1'}, \quad a_0 - a_0' = \frac{1}{\theta_1'} - \frac{1}{\theta_1}$$

with $\theta_1, \theta_1' \geq 1$.

This is impossible unless $a_0 = a_0'$ when $\theta_1 = \theta_1'$

Inductively, it follows that two infinite continued fractions converging to the same real number must be identical.

Hence we have a uniqueness of a continued fraction expansion.

What if one of them doesn't continue?

i.e. $[\theta_0] = [a_0', \theta_1']$

$a_0 = a_1' + \frac{1}{\theta_1'}$, $\theta_1' \geq 1$

The only way that this can happen is if $\theta_1' = 1$ and we have $[a_0] = [a_0 - 1, 1]$.

It follows inductively that the only equality between distinct continued fractions is of the form:

$[a_0, \ldots, a_n] = [a_0, \ldots, a_n - 1, 1]$

8.5 Rational Approximation

Dirichlet

Let θ be a real. For any integer $Q \geq 1$, $\exists\, p, q$ with $0 < q < Q$ such that $|\theta - \frac{p}{q}| \leq \frac{1}{qQ}$ i.e. $|q\theta - p| \leq \frac{1}{Q}$

Proof

$\{\ \}$ — fractional part

The numbers $0, 1, \{q\theta\}$ for $0 < q < Q$ are $Q+1$ numbers in $[0, 1]$ which we can divide into Q intervals of the form $[0, \frac{1}{Q}], [\frac{1}{Q}, \frac{2}{Q}], \ldots$. So there is some interval containing two of them (pigeonhole principle).

In the case $|\{q\theta\} - 0| \leq \frac{1}{Q}$ we have $|q\theta - \lfloor q\theta \rfloor| \leq \frac{1}{Q}$

In the case $|\{q\theta\} - 1| \leq \frac{1}{Q}$ we have $|q\theta - (\lfloor q\theta \rfloor + 1)| \leq \frac{1}{Q}$

Otherwise $|\{q_1\theta\} - \{q_2\theta\}| \leq \frac{1}{Q}$ with $q_1 > q_2$ say.

Then $|(q_1 - q_2)\theta - (\lfloor q_1\theta \rfloor - \lfloor q_2\theta \rfloor)| \leq \frac{1}{Q}$

Remark

Last time we saw that $|\frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}}| = \frac{1}{q_n q_{n+1}}$. So this is an example when $q_n < q_{n+1}$. Moreover, as θ lies between the two convergents, we have $|\theta - \frac{p_n}{q_n}| \leq \frac{1}{q_n q_{n+1}}$, $|q_n\theta - p_n| \leq \frac{1}{q_{n+1}}$

Observation

For θ real, the sequence $|q_n\theta - p_n|$ is strictly decreasing.

(N.B. we have an infinite sequence if θ is irrational, and a sequence which stops at 0 if θ is rational)

Why? We have

$$\theta = [a_0, a_1, \ldots, a_n, \theta_{n+1}] = \frac{\theta_{n+1} p_n + p_{n-1}}{\theta_{n+1} q_n + q_{n-1}}$$

So $q_n\theta - p_n = \dfrac{\theta_{n+1} p_n q_n + p_{n-1} q_n - \theta_{n+1} p_n q_n - p_n q_{n-1}}{\theta_{n+1} q_n + q_{n-1}} = \dfrac{(-1)^k}{\theta_{n+1} q_n + q_{n-1}}$

$$|q_n\theta - p_n| = \frac{1}{\theta_{n+1} q_n + q_{n-1}}$$

But note that $\theta_{n+1} q_n + q_{n-1} \geq q_n + q_{n-1} = a_n q_{n-1} + q_{n-2} + q_{n-1}$

$= (a_n + 1) q_{n-1} + q_{n-2} > \theta_n q_{n-1} + q_{n-2}$

How good an approximation is $\frac{p}{q}$ to θ? The good measure is $|q\theta - p|$. We say that $\frac{p}{q}$ is a best approximation to θ just when $q > 0$, $|q\theta - p|$ is the minimal distance from $q\theta$ to an integer, and if whenever $0 < q' < q$, p' arbitrary, then $|q'\theta - p'| > |q\theta - p|$ i.e. the approximation is worse.

There is a best approximation with $q = 1$. Either this is an equality, or there is some difference, so there is a better one, by Dirichlet, and we take the best such. We repeat this process.

This is the continued fraction algorithm except perhaps at the very begining. The "trivial" point is this:

$\theta = a_0 + \frac{1}{\theta_1}$. If $\theta_1 \geq 2$, then $a_0 = \frac{p_0}{q_0}$ is a best approximation, but if not $\theta = a_0 + \dfrac{1}{1 + \frac{1}{\theta_2}}$ and $a_0 + 1 = \frac{p_1}{q_1}$ is a best approximation.

Fact

If $\frac{p_n}{q_n}$ is a best approximation to θ, then $\frac{p_{n+1}}{q_{n+1}}$ is the subsequent best approximation.

Proposition

Let $q_n < q < q_{n+1}$, p arbitrary. Then $|q\theta - p| \geq |q_n\theta - p_n|$

Proof

Recall that $\begin{pmatrix} p_n & p_{n+1} \\ q_n & q_{n+1} \end{pmatrix}$ has determinant $(-1)^{n+1}$ so its inverse in the integers exists. Therefore we can uniquely solve $\begin{pmatrix} p_n & p_{n+1} \\ q_n & q_{n+1} \end{pmatrix}\begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} p \\ q \end{pmatrix}$

Note that $u \neq 0$ or $q = vq_{n+1}$ (contradicting $q < q_{n+1}$). Also if $v \neq 0$, then u, v have opposite signs, otherwise $q = uq_n + vq_{n+1}$.

Consider $|q\theta - p| = |u(q_n\theta - p_n) + v(q_{n+1}\theta - p_{n+1})|$

($u(q_n\theta - p_n)$ and $v(q_{n+1}\theta - p_{n+1})$ opposite signs)

$u(q_n\theta - p_n)$ and $v(q_{n+1}\theta - p_{n+1})$ have the same signs.

$$\geq |u(q_n\theta - p_n)| \geq |q_n\theta - p_n|$$

Corollary

Suppose $\frac{p}{q}$ is such that $|\theta - \frac{p}{q}| < \frac{1}{2q^2}$

i.e such that $|q\theta - p| < \frac{1}{2q}$

Then $\frac{p}{q}$ is one of the approximants to θ.

Proof

Let $q_n \leq q \leq q_{n+1}$.

$$\left|\frac{p}{q} - \frac{p_n}{q_n}\right| \leq \left|\theta - \frac{p}{q}\right| + \left|\theta - \frac{p_n}{q_n}\right| = \frac{1}{q}|q\theta - p| + \frac{1}{q_n}|q_n\theta - p_n|$$

$$\leq \left(\frac{1}{q} + \frac{1}{q_n}\right)|q\theta - p| \leq \frac{2}{q_n}\frac{1}{2q} = \frac{1}{q_n q}$$

So $\left|\frac{pq_n - p_n q}{q_n q}\right| < \frac{1}{q_n q}$ which cannot occur in integers unless the left hand side is zero.

18/11/12 Number Theory (18)

8.6 Pell's Equation

$x^2 - dy^2 = 1$. Take $d > 1$ and not a perfect square.

Observation

We have the norm $N : \mathbb{Q}[\sqrt{d}] \to \mathbb{Q} : x + y\sqrt{d} \mapsto x^2 - dy^2$

and this function is multiplicative. $N(zw) = N(z)N(w)$

So solutions in rationals are the kernel of

$N : \mathbb{Q}[\sqrt{d}]^\times \to \mathbb{Q}^\times$

We seek solutions in integers. Consider $\mathbb{Z}[\sqrt{d}] \to \mathbb{Z}$

It is easy to see that the units in $\mathbb{Z}[\sqrt{d}]$ are solutions of

$p^2 - dq^2 = \pm 1$.

More Observations

i) Suppose that $\eta \in \mathbb{Z}[\sqrt{d}]$ is a non-trivial ($\neq \pm 1$) solution to Pell's Equation. Then, so are $\pm\eta$, $\pm\frac{1}{\eta}$, so there is a solution > 1

ii) Suppose $\eta = p + q\sqrt{d}$ is a solution > 1. Then

$0 < \eta^{-1} = p - q\sqrt{d} < 1 < p + q\sqrt{d}$. So $p > q\sqrt{d} > 0$

and so p, q are both positive.

iii) It follows that there is a least solution $\varepsilon > 1$. Take $\eta > 1$ any solution, and then choose k such that $\varepsilon^k \leq \eta < \varepsilon^{k+1}$

Then η/ε^k is a solution $1 \leq \eta/\varepsilon^k < \varepsilon$ and so $\eta/\varepsilon^k = 1$,

$\eta = \varepsilon^k$. Thus the complete set of solutions is $\pm\varepsilon^n$, $n \in \mathbb{Z}$

iv) Similarly, the units in $\mathbb{Z}[\sqrt{d}]$ are of the form $\pm\delta^n$, $n \in \mathbb{Z}$ with $\delta > 1$ the least unit > 1.

Two Possibilities

- $N(\delta) = -1$ in which case $\varepsilon = \delta^2$
- $N(\delta) = 1$, $\delta = \varepsilon$, and there are no solutions to $x^2 - dy^2 = -1$ in integers

Both of these occur.

v) Take $p + q\sqrt{d}$, a solution to Pell, and note that p, q positive, $p > q\sqrt{d}$. Then $|q\sqrt{d} - p| = p - q\sqrt{d} = \frac{1}{p+q\sqrt{d}} < \frac{1}{2q\sqrt{d}}$

So $|q\sqrt{d} - p| < \frac{1}{2q}$. Thus $\frac{p}{q}$ is a convergent to $\sqrt{d}$.

Plan

① We shall show that non-trivial solutions exist

② Characterise where the solutions arise in the continued fraction expansion

③ Deduce some facts about the continued fraction expansion.

① Let us consider for given Q the rationals $\frac{p}{q}$ such that $|\sqrt{d} - \frac{p}{q}| \leq \frac{1}{qQ}$ i.e. such that $|p - q\sqrt{d}| \leq \frac{1}{Q}$.

$|p + q\sqrt{d}| \leq \frac{1}{Q} + 2q\sqrt{d} < 3Q\sqrt{d}$

So $|p^2 - dq^2| < 3\sqrt{d}$, a bound independent of Q.

It follows that there infinitely many p, q with $|p^2 - q^2 d| < 3\sqrt{d}$

(Because we take Q, have $0 < |p - q\sqrt{d}| < \frac{1}{Q}$, take Q_1 such that $\frac{1}{Q_1} < |p - q\sqrt{d}|$, take p_1, q_1 such that $|p_1 - q_1\sqrt{d}| < \frac{1}{Q_1}$, and so on).

Thus there is an M, $|M| < 3\sqrt{d}$ and with infinitely many p, q with $N(p + q\sqrt{d}) = p^2 - dq^2 = M$

Choose p_1, q_1 and p_2, q_2 from this set so that

$p_1 \equiv p_2 \ (M)$ and $q_1 \equiv q_2 \ (M)$.

(We can do this easily as there are only a finite number of possibilities for the residues of p, q mod M).

Now consider $\eta = \frac{p_1 + q_1\sqrt{d}}{p_2 + q_2\sqrt{d}}$. It has norm $\frac{M}{M} = 1$.

$$\eta = \frac{(p_1 + q_1\sqrt{d})(p_2 - q_2\sqrt{d})}{p_2^2 - q_2^2 d} = \frac{(p_1p_2 - q_1q_2d) + (p_2q_1 - p_1q_2)\sqrt{d}}{M}$$

but mod M, $p_2q_1 - p_1q_2 \equiv p_2q_2 - p_2q_2 = 0 \ (M)$

$p_1p_2 - q_1q_2 d \equiv p_2^2 - q_2^2 d \equiv M \equiv 0 \ (M)$

So M divides the coefficients within the numerator.

Thus $\eta = p + q\sqrt{d}$, $p, q \in \mathbb{Z}$

Aside

The continued fraction expansion of $\sqrt{d}$ is of the form

$\sqrt{d} = [a_0, a_1, \ldots, a_k, 2a_0, a_1, \ldots, a_k, 2a_0, a_1, \ldots]$

Guess where the convergents to $\sqrt{d}$ give solutions to

$p^2 - dq^2 = \pm 1$ lie.

$\sqrt{7}$ or larger is instructive.

16/11/12 Number Theory (9)

2. Let $\sqrt{d} = [a_0, a_1, \dots] = [a_0, a_1, \dots, a_n, \theta_{n+1}]$

Then we have $\sqrt{d} = \frac{\theta_{n+1} p_n + p_{n-1}}{\theta_{n+1} q_n + q_{n-1}}$

We invert this to get $\theta_{n+1} = -\frac{p_{n-1} - q_{n-1}\sqrt{d}}{p_n - q_n\sqrt{d}}$ (†)

So $\theta_{n+1} = -\frac{(p_{n-1} - q_{n-1}\sqrt{d})(p_n + q_n\sqrt{d})}{p_n^2 - d q_n^2} = -\frac{(p_{n-1}p_n - q_{n-1}q_n d) + (p_{n-1}q_n - p_n q_{n-1})\sqrt{d}}{p_n^2 - d q_n^2}$ (*)

$(-1)^n$

Suppose that p_n, q_n is a solution to $p^2 - dq^2 = \pm 1$.

In the case that n is odd then $\frac{p_n}{q_n} > \sqrt{d}$ and so $p_n^2 - d q_n^2 = +1$

In the even case, $\frac{p_n}{q_n} < \sqrt{d}$, $p_n^2 - d q_n^2 = -1$.

In either case, $\theta_{n+1} = c + \sqrt{d}$. Now $\theta_{n+1} = a_{n+1} + \frac{1}{\theta_{n+2}}$

$c + \sqrt{d} = c + a_0 + \frac{1}{\theta_1}$. So $\theta_{n+2} = \theta_1$.

Take now p_n, q_n to be the first solution as above. We see that the continued fraction expansion is

$\sqrt{d} = [a_0, a_1, a_2, \dots, a_{n+1}, a_1, \dots, a_{n+1}, \dots] = [a_0, \overline{a_1, \dots, a_{n+1}}]$

Can there be some smaller period inside this period?

Set $m = n+1$, so we have $[a_0, a_1, \dots, a_m, a_1, \dots, a_m]$

Suppose that we had a smaller period, $[a_0, \overline{a_1, \dots, a_r}]$, $r < m$.

Then $\theta_{r+1} = \theta_1$, and so $\theta_1 = \tilde{c} + \sqrt{d}$. By (*), this can only happen if $p_{r-1}^2 - d q_{r-1}^2 = \pm 1$ ✗ (We chose p_n, q_n as the first solution

[As written, $n \geq 1$, but we can extend (†) by setting

$(p_{-2}, q_{-2}) = (0, 1)$, $(p_{-1}, q_{-1}) = (1, 0)$]

The solutions to $p^2 - dq^2 = \pm 1$ occur at the points $k = m-1, 2m-1, 3m-$

We have two cases. If n is even, we start with a solution to $p^2 - dq^2 = +1$, then there are no solutions of $p^2 - dq^2 = -1$.

If n is odd, we start with a solution to $p^2 - dq^2 = -1$, then alternately $+1, -1, +1, \ldots$

These are $1 < \delta, \delta^2, \delta^3$, identified at the start.

Fact:

$$\sqrt{d} = [a_0, \underbrace{a_1, \ldots, a_n}_{\text{symmetric}}, 2a_0, a_1, \ldots, a_n, 2a_0, \ldots]$$

Case of $\sqrt{2}$

$\sqrt{2} = [1, 2, 2, \ldots]$, convergents $\frac{1}{1}, \frac{3}{2}, \frac{7}{5}$

$1 - 2 \cdot 1^2 = -1$ $\qquad$ $3^2 - 2 \cdot 2^2 = 1$

$7^2 - 2 \cdot 5^2 = -1$

Case of $\sqrt{3}$

$\sqrt{3} = [1, 1, 2, 1, 2, \ldots]$, convergents $\frac{1}{1}, \frac{2}{1}, \frac{5}{3}, \frac{7}{4}, \ldots$

$2^2 - 3 \cdot 1^2 = 1$ $\qquad$ $7^2 - 3 \cdot 4^2 = 1$

19/11/12 Number Theory (20)

Chapter 9: Primes and Factoring

9.1 How do we test whether a number n is prime?

Trial Division: Divide by all numbers $m \leq \sqrt{n}$

Wilson's Theorem: $(n-1)! \equiv -1 \ (n) \iff n$ is prime

Idea: If p is prime then $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p-1$.

If $n = p_1^{a_1} \dots p_k^{a_k}$ composite then $(\mathbb{Z}/n\mathbb{Z})^\times$ is isomorphic to $(\mathbb{Z}/p_1^{a_1}\mathbb{Z})^\times \times \dots \times (\mathbb{Z}/p_k^{a_k}\mathbb{Z})^\times$, a product of cyclic groups of orders $(p_i - 1)p_i^{\alpha_i - 1}$. Generally, the groups feel very different.

Order of the group? Not useful, too much computation.

Neither is finding the orders of all elements (too much computation).

9.2 Fermat Pseudoprimes and Carmichael Numbers

If p is prime then the order of $(b, p) = 1$ must divide $(p-1)$.

Definition

A number n is a (Fermat) pseudoprime to base b with $(b, n) = 1$ if and only if $b^{n-1} = 1 \ (n)$, but n is in fact composite.

The traditional choice for b is 2.

The first ψ-prime (pseudoprime) for base 2 is $341 = 11 \times 31$

mod 11: $2, 4, 8, 5, 2^5 = -1, \dots, 2^{10} = 1$

mod 31: $2^5 = 1$, so $2^{10} = 1 \ (341)$

and so $2^{340} = (2^{10})^{34} = 1 \ (341)$

Remarks

1. Any composite number is a pseudoprime to base 1.
2. Any odd composite number is a Ψ-prime to base -1.
3. If we choose different bases, we can find smaller pseudoprimes

Example

① $91 = 7 \times 13$ is a Ψ-prime to base 3.

mod 7 $\quad 3,\ 3^2 = 2,\ 3^3 = 6 = -1,\ 3^6 = 1$

mod 13 $\quad 3^3 = 1$

So 3 has order 6 mod 91 and $6 \mid 90$.

② $25 = 5 \times 5$ is a Ψ-prime to base 7.

$7^2 = -1\ (25)$, so $7^4 = 1\ (25)$ and $4 \mid 24$.

4. Fermat's Little Theorem has a "sort of converse" which is no use.

If $(a, n) = 1$, and $a^{n-1} = 1\ (n)$, and $a^k \neq 1\ (n)$ for any $1 \leq k < n-1$ then n is prime. Because $a^{\varphi(n)} = 1\ (n)$ and this says that $\varphi(n) = n-1$, so n is prime.

Suppose that $n = p_1^{a_1} \dots p_k^{a_k}$ is a pseudoprime to base b. What can we say about the order of $b\ (\text{mod } n)$?

- Fist, it divides $(n-1)$.
- Secondly, it divides the least common multiple of $(p_i - 1)p_i^{a_i - 1}$

If the order had a factor p_i, than that contradicts the first point, so it divides the least common multiple of the $(p_i - 1)$

Note that if $b_1^{n-1} = 1 \ (n)$ and $b_2^{n-1} = 1 \ (n)$ then $(b_1 b_2)^{n-1} = 1 \ (n)$ and similarly for inverses. So the bases b with respect to which n is Ψ-prime form a multiplicative subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$.

Consider the $d_i = (p_i - 1, n-1)$. Then we are really considering the product of the subgroups corresponding to the d_i.

Example

$341 = 11 \times 31$

$(10, 340) = 10 \quad , \quad (30, 340) = 10$

$$\left(\frac{\mathbb{Z}}{341\mathbb{Z}}\right)^\times = \left(\frac{\mathbb{Z}}{11\mathbb{Z}}\right)^\times \times \left(\frac{\mathbb{Z}}{31\mathbb{Z}}\right)^\times$$

both contain a cyclic group of order 10, giving the subgroup with respect to which n is Ψ-prime.

Carmichael Numbers

A composite number n such that n is a Ψ-prime to all bases $(b, n) = 1$ is a Carmichael number.

Observe that if $n = p_1^{a_1} \dots p_k^{a_k}$ is a Carmichael number then the a_i are all 1, i.e. n is squarefree.

Suppose that $n = pq$ is a product of distinct primes.

Suppose $p > q$. Then $(p-1)q = pq - q < pq - 1 = n - 1$

$(p-1)(q+1) = pq + (p-q) - 1 > pq = n$

and so $(p-1) \nmid (n-1)$. So n is not Carmichael.

Example

$561 = 3 \times 11 \times 17$

$3-1 = 2 \mid 560$

$11-1 = 10 \mid 560$

$17-1 = 16 \mid 560$

} So 561 is a Carmichael number. (Why?)

9.3 Strong-pseudoprimes

Suppose that p is prime and $(b,p)=1$, $\langle b \rangle \leq (\mathbb{Z}/p\mathbb{Z})^*$ and we can ask questions about it.

A good question is: Is -1 in $\langle b \rangle$?

Recall that a composite n is a Ψ-prime to base b iff the order of $\langle b \rangle$ divides $n-1$.

For p prime, consider $\langle b \rangle \leq (\mathbb{Z}/p\mathbb{Z})^\times$ and ask when $-1 \in \langle b \rangle$.

Since $\{\pm 1\}$ is the unique subgroup of order 2, it follows that this holds iff $|\langle b \rangle|$ is even.

So if $p-1 = 2^s m$, with m odd, we have the following possibilities

1. The order of $|\langle b \rangle|$ is odd, so it divides m, and so $b^m \equiv 1 \ (p)$
2. The order of $|\langle b \rangle|$ is even so it is of the form $2^t d$ with $1 \leq t \leq s$ and $d \mid m$, and then as $(b^{2^{t-1}d})^2 = 1$ we have $b^{2^{t-1}d} = -1 \ (p)$ and so $b^{2^{t-1}m} = -1 \ (p)$

<u>Definition</u>

An odd composite n is a strong pseudoprime to base b iff for $n-1 = 2^s m$ we have

EITHER $b^m = 1 \ (n)$

OR $b^{2^{t-1}m} = -1 \ (n)$ for some $1 \leq t \leq s$

<u>Remarks</u>

1. Odd composite n are strong Ψ-primes to bases ± 1 but otherwise they have no evident multiplicative properties.
2. 341 is not a strong Ψ-prime to base 2.

   $2^{10} = 1 \ (341)$ but $2^5 = 32 \neq -1 \ (341)$

(Or strictly speaking $2^{170} = 1 (341)$ but $2^{85} \neq -1 (341)$)

Similarly, 91 is not a strong Ψ-prime to base 3.

3. 2047 is the least strong Ψ-prime to base 2.

121 is a strong Ψ-prime to base 3.

$120 = 8 \times 15$, and $3^5 = 243 = 1 (11^2)$ and so $3^{15} = 1 (11^2)$

Also, 91 is a strong Ψ-prime to base 10.

$90 = 2 \times 45$, and $10^3 = 90 = -1 (91)$

$10^{45} = (10^3)^{15} = -1 (91)$

4. Suppose $n = p_1^{a_1} \dots p_k^{a_k}$ and is a Ψ-prime to base b.

We already know that the order of b mod $p_i^{a_i}$ divides $(p_i - 1)$.

Set $n-1 = 2^s m$, $p_i - 1 = 2^{u_i} l_i$

If n is a strong Ψ-prime, then

- either $b^m = 1 (n)$, so mod $p_i^{a_i}$, and so the orders of b mod $p_i^{a_i}$ all divide the relevant d_i
- or $b^{2^{t-1} m} = -1 (n)$ and then the orders of b mod $p_i^{a_i}$ are of the forms $2^t l_i'$ with $l_i' | l_i$ (the same t for all i)

Recall that if we have $n = p_1^{a_1} \dots p_k^{a_k}$ with some $a_i > 1$ (so that n is not squarefree) then there are bases b with n not Ψ-prime to base b.

(e.g. if you choose $b = g$. primitive element mod $p_i^{a_i}$ which gives order $(p_i - 1) p^{a_i - 1}$

But now, even if n is squarefree we can find b such that n is not a strong Ψ-prime to base b.

e.g. take $n = pn'$, p prime, $(p, n') = 1$

Solve $b = g \ (p)$, g the primitive element

$b = 1 \ (n')$

Then if we had $b^{2^{t-1}m} = -1 \ (n) = -1 \ (n')$

but clearly this $= 1 \ (n')$ ⊗

Equally, if we had $b^m = 1 \ (n)$, $b^m = 1 \ (p)$ and so the order of g would be odd (p). But the order is $p-1$, even.

Fact

If n is odd composite then at most $\frac{1}{4}$ of the possible bases have n a strong Ψ-prime. This suggests a probabilistic test.

9.4 Euler Pseudoprimes

(Euler) If p is prime then for $(b, p) = 1$ we have

$b^{\frac{p-1}{2}} = \left(\frac{b}{p}\right) \bmod p$

Definition

An odd composite n is Euler pseudoprime to base b iff

$b^{\frac{n-1}{2}} = \left(\frac{b}{n}\right) \ (n) \pmod n$ ← Jacobi Symbol

Remark

1. If n is odd composite it is Euler Ψ-prime to bases ± 1 and the bases to which it is Euler Ψ-prime form a subgroup.

2. 561 is Euler Ψ-prime to base 2. $561 = 3 \times 11 \times 17$

$2^2 = 1 \ (3)$, $2^{10} = 1 \ (11)$, $2^8 = 1 \ (17)$

$2^{40} = 1 \ (561)$ so $2^{280} = 1 \ (561)$

and also $\left(\frac{2}{561}\right) = 1$ as $561 = 1 \ (8)$

Fact

If n is a strong Ψ prime to base b then it is an Euler Ψ-prime to base b.

Note that if $n = 3 \ (4)$ so that $n-1 = 2m$, m odd, then n an Euler-Ψ-prime to base $b \Rightarrow b^m = \pm 1 \ (n)$ and so n is a strong Ψ-prime.

9.5 Fermat Factorisation

For an odd n, then if n has a non-trivial factorisation ab then $n = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$ is a difference of two squares.

Conversely, if $n = u^2 - v^2$, a difference of two squares with $u \neq \pm v$ then $n = (u+v)(u-v)$ is a factorisation.

If the factors a, b are closed in value then $v = \frac{a-b}{2}$ is small and $u^2 = \left(\frac{a+b}{2}\right)^2$ is close to n. So if we are in this case, we consider $u = \lfloor \sqrt{n} \rfloor + 1$, $\lfloor \sqrt{n} \rfloor + 2$ and so on, and hope for a good outcome, i.e. $u^2 - n$ is square.

Simple Examples

We try to factorise 1147, 1189, 1081 :

$34^2 = 1156$, $1156 - 1147 = 9 = 3^2$, $1147 = 37 \times 31$

$35^2 = 1225$, $1225 - 1189 = 36 = 6^2$, $1189 = 41 \times 29$

$33^2 = 1089$, $1089 - 1081 = 8$

$1156 - 1081 = 75$, $1225 - 1081 = 144 = 12^2$

$1081 = 47 \times 23$

Simple Variant

Suppose that for small k we have $k \times n = u^2 - v^2 = (u+v)(u-v)$

Then with luck $(u+v, n)$ will be a non-trivial factor of n, and the same for $(u-v, n)$

(The difficulty would be $(u+v) = n$, $(u-v) = k$)

Example

Suppose that we want to factorise 793

$29^2 = 821$, $821 - 793 = 28$	$793 \times 3 = 2379$
$30^2 = 900$, $900 - 793 = 107$	$49^2 = 2401$, $2401 - 2374 = 22$
.....	$50^2 = 2500$, $2500 - 2379 = 121 = 11^2$

$(61, 793) = 61$, $(39, 793) = 13$

$793 = 61 \times 13$

More generally, if we can find $u^2 \equiv v^2 \ (n)$ but $u \not\equiv \pm v \ (n)$ then $(u+v, n)$, $(u-v, n)$ provide factors for n.

9.6 Factor bases

A factor base B is some set of primes together with -1. $B = \{p_1, \dots, p_k\}$. We say that b is a B-number iff b^2 has least absolute value mod n i.e. in $[-\frac{n}{2}, \frac{n}{2}]$ a product of numbers from B.

Suppose we find a B-number b such that in $b^2 = p_1^{a_1} \dots p_k^{a_k} \ (n)$, all the a_i are even. Then $b^2 = c^2 \ (n)$ and unless $b = \pm c$ we shall get a factorisation of n.

Suppose that we are not so lucky. We get a B-number $b^2 = p_1^{a_1} \dots p_k^{a_k} \ (n)$: we record $(a_1, \dots, a_k) \bmod 2 \in \mathbb{F}_2^k$

then we get another one $b'^2 = p_1^{a_1'} \dots p_k^{a_k'}$ and record

$(a_1', \dots, a_k') \bmod 2 \in \mathbb{F}_2^k$

We continue until we have a linear dependence $\sum \varepsilon_i \underline{a}^{(i)} = \underline{0}$

If we have $k+1$ vectors this is certain.

Then $d = \prod b_\bullet^{(i)\,\varepsilon_i}$ is a B-number, and it has d^2 a perfect square mod n

How to find B-numbers:

Strategy 1

Pick B to be -1 together with all small primes and take b at random

Strategy 2

Collect some b's, and hold onto this with small prime factors, constructing B accordingly.

To find good b's we want $b^2(n)$ with small prime factors so it is best to make $b^2(n)$ small itself.

9-7 Continued Fractions

Recall that the convergents $\frac{p_k}{q_k}$ to $\sqrt{n}$ are good approximations.

That is, $\left|\frac{p_k}{q_k} - \sqrt{n}\right|$ is small, and so $|p_k - q_k\sqrt{n}|$ is small.

So there is a chance that $|p_k^2 - q_k^2 n|$ is small i.e. p_k^2 is small mod n.

Generally, the convergents $\frac{p_k}{q_k}$ to θ satisfy

$|p_k^2 - q_k^2\theta^2| < 2|\theta|$ (for $k \geq 2$, $|\theta| \geq 1$. Why?)

$|p_k - q_k\theta|\,|p_k + q_k\theta| < 3|\theta|$

by similar method to $p^2 - dq^2$ + Dirichlet

Illustration

$\sqrt{33} = [5, \overline{12, 1, 10}]$

Convergents are $\frac{5}{1}, \frac{6}{1}, \frac{17}{3}, \frac{23}{4}, \frac{247}{43}$

$5^2 = -8 \ (33)$, $6^2 = 36 = 3 \ (33)$, $17^2 = 289 = 25 = -8 \ (33)$

So $85^2 = 8^2 \ (33)$ $\quad (85 = 5 \times 17)$

hcf $(93, 33) = 3$, hcf $(77, 33) = 11$

$33 = 11 \times 3$

9.5 Pollard's p-1 Method

Suppose that we have an odd composite n with a prime factor p with the property that it is a product of 'not too many' instances of a collection of small primes, so that in fact $p-1 \mid k$ which we happen to have chosen in advance.

Pick any $(a, n) = 1$ and consider that $a^{p-1} \equiv 1 \ (p)$, and so $a^k \equiv 1 \ (p)$. So $p \mid a^k - 1$, and $p \mid n$. So $p \mid (a^k - 1, n)$. So $(a^k - 1, n)$ is a factor of n.

Remarks

1. It is possible that $(a^k - 1, n) = n$ i.e. $a^k \equiv 1 \ (n)$. This happens iff $a^k \equiv 1 \ (p_i^{a_i})$ for all the primes in the prime decomposition $n = p_1^{a_1} \dots p_k^{a_k}$. This will not happen for most a unless all the primes are like p, so it is unlikely.
2. Obviously, for computation, we don't compute a^k but rather $a^k \ (n)$.
3. Typically we take k to be the least common multiple of an initial segment of the integers. For example:

$\text{Lcm}\{1, 2, \dots, 8\} = 2^3 \times 3 \times 5 \times 7 = 840$

$\text{Lcm}\{1, 2, \dots, 10\} = 2^3 \times 3^2 \times 5 \times 7 = 2520$

For $k = 2520$:

Primes detected:	Primes not detected
3, 5, 7, 11, 13, 19, 29, 31, 37, 41, 43, 61, 67, 71, 73	17, 23, 42, 53, 59

Example

Factorise 713 using $k = 60$.

Take $a = 2$. $2^{10} = 1024 = 311\ (713)$, $2^{20} = 46,721 = 466\ (713)$

$2^{40} = 217156 = 404\ (713)$, $2^{60} = 32\ (713)$

So $2^{60} - 1 \equiv 31\ (713)$, and $(31, 713) = 31$.

Observe that all of $(310, 713)$, $(465, 713)$, $(403, 713) = 31$.

For in fact $2^5 = 32$ and $(2^5 - 1, 713) = 31$

So strongly, we profit from the fact that 2 is far from being a primitive element mod 31. In fact, in implementations it is worth checking this systematically.

Take $a = 3$. $3^6 = 729 \equiv 16\ (713)$. So $3^{60} = 404\ (713)$

and again we would have $(403, 713) = 31$.

Appendix : Sums of Squares

Recall that a number n is a sum of 2 squares iff it is a square $\times$ a product of primes $= 2$ or $\equiv 1\ (4)$. This is essentially given by prime factorisation in $\mathbb{Z}[i]$.

The sum of 4 squares is related "in a similar * way" to the 'integral quaternions'.

Consider $x = x_0 + x_1 i + x_2 j + x_3 k$ with the usual quaternion multiplication i.e. $i^2 = j^2 = k^2 = ijk = -1$

We have $\bar{x} = x_0 - x_1 i - x_2 j - x_3 k$.

Then $\bar{x}y = (x_0 - x_1 i - x_2 j - x_3 k)(y_0 + y_1 i + y_2 j + y_3 k$

$= (x_0y_0 + x_1y_1 + x_2y_2 + x_3y_3) + (x_0y_1 - x_1y_0 + x_3y_2 - x_2y_3)$

$+ (x_0y_2 - x_2y_0 + x_1y_3 - x_3y_1)j$

$+ (x_0y_3 - x_3y_1 + x_2y_1 - x_1y_2)k$

We have $N(x) = \bar{x}x = x_0^2 + x_1^2 + x_2^2 + x_3^2$

Also, by inspection, we have $\overline{\bar{x}y} = \bar{y}x$

So $N(xy) = \overline{xy}\,xy = \bar{y}\bar{x}xy = N(x)\bar{y}y = N(x)N(y)$

Thus there is a formula giving the ~~sum of 4~~ product of 2 sums of 4 squares as a sum of 4 squares.

Note $1 = 1^2$, $2 = 1^2 + 1^2$, so to show that all numbers can be written as the sum of 4 squares it is enough to show it for all odd primes.

Lemma

Let p be an odd prime. Then there are $0 < m \leq p$, and a, b such that $mp = 1 + a^2 + b^2$

Proof

Consider the numbers $\{a \mid 0 \leq a \leq \frac{1}{2}(p-1) = \underline{P}\}$ and the numbers $\{-1 - b^2 \mid 0 \leq b \leq \frac{1}{2}(p-1) = \underline{P}\}$

Observe that if $a^2 = a'^2 \ (p)$, then $a = \pm a' \ (p)$ so $a = a'$.

Similarly, $-1 - b^2 = -1 - b'^2 \ (p) \Rightarrow b = b'$.

So mod p we have two sets of exactly $\frac{p+1}{2} = \underline{P} + 1$ elements.

So we must have some $a^2 = -1 - b^2 \bmod p$. Then we have

$mp = 1 + a^2 + b^2$

But also $a^2 \leq \frac{1}{4}(p-1)^2$, $b^2 \leq \frac{1}{4}(p-1)^2$.

So $1 + a^2 + b^2 \leq \frac{1}{2}(p-1)^2 < p^2$ and so $0 < m < p$.

Corollary

If p is an odd prime then there is $0 < m < p$ with

$$mp = x_0^2 + x_1^2 + x_2^2 + x_3^2 = N(x)$$

It suffices to show now that the least such m is 1.

Lemma

Suppose p, $mp = N(x)$ are as above with m even.

Then an even number of the x_i are odd, and so we can rearrange so that $x_0 \pm x_1$, $x_2 \pm x_3$ are even. Then

$$mp = 2\left(\left(\frac{x_0+x_1}{2}\right)^2 + \left(\frac{x_0-x_1}{2}\right)^2 + \left(\frac{x_2+x_3}{2}\right)^2 + \left(\frac{x_2-x_3}{2}\right)^2\right)$$

and we may cancel a 2.

Corollary

The least m will be odd.

Lemma

Suppose that p is odd, $mp = N(x)$, $0 < m < p$, m odd.

Then clearly $m \nmid$ all the x_i. For otherwise, $m^2 \mid N(x) = mp$ and $m \mid p$ ✗

Take $y_i = x_i \bmod m$, the least absolute residues so that $|y_i| < \frac{1}{2}m$

1. $N(y) = y_0^2 + y_1^2 + y_2^2 + y_3^2 = N(x) \pmod m$ and $N(x) \equiv 0 \pmod m$, So $m \mid N(y)$.
2. $N(y) < \frac{1}{4}m^2 + \frac{1}{4}m^2 + \frac{1}{4}m^2 + \frac{1}{4}m^2 = m^2$. Thus $N(y) = km$ for some $k < m$.

Now let $z = \bar{x}y$.

Then $N(z) = N(\bar{x}y) = N(x)N(y) = mp \cdot km = kp\,m^2$

But modulo m, $z = \bar{x}y = \bar{x}x = N(x) = x_0^2 + x_1^2 + x_2^2 + x_3^2 + 0i + 0j + 0k$

So $m \mid z_0, z_1, z_2, z_3$. Set $w_i = \frac{z_i}{m} \in \mathbb{Z}$.

$N(w) = kp$ with $k < m$.

Therefore, the least n must be 1.

So every integer can be expressed as a sum of four squares.

Congruent Numbers

Consider right-angled triangles with rational sides.

$\left(\frac{a}{d}\right)^2 + \left(\frac{b}{d}\right)^2 = \left(\frac{c}{d}\right)^2$

A number n is a congruent number iff it is the area of such a triangle i.e. $n = \frac{1}{2}\frac{ab}{d^2}$

Alternatively, n is congruent when we can find solutions in integers to $a^2 + b^2 = c^2$ and $ab = 2nd^2$ in integers a, b, c, d.

Example

3, 4, 5 shows that 6 is congruent.

9, 40, 41 shows that 180 is congruent.

$\frac{9}{6}, \frac{40}{6}, \frac{41}{6}$ shows that 5 is congruent.

Fibonacci found that 7 is congruent.

Terminology

$\frac{b-a}{2}, \frac{c}{2}, \frac{b+a}{2}$

$\left(\frac{c}{2}\right)^2 - \left(\frac{b-a}{2}\right)^2$ is square.

$\left(\frac{b+a}{2}\right)^2 - \left(\frac{c}{2}\right)^2$ is square.

There is a connection with elliptic curves: n is congruent if and only if $y^2 = x^3 - n^2x$ is soluble in rationals.

Facts

Some weak form of the Birch and Swinerton-Dyer Conjecture $\Rightarrow$ All numbers of the form $8k+5$, $8k+6$, $8k+7$, are congruent.

(Ye Tian) There are infinitely many congruent numbers as above which are squarefree, and the product of r (distinct) primes, for all $r \neq 1$

(Fermat) 1 is not a congruent number.

Suppose that we have $a^2+b^2 = c^2$ and $ab = 2d^2$.

We may as well assume that a, b are coprime, for any factor of a and b is a factor of c and d and we could cancel.

1. As $(a,b) = 1$, we can assume that $a = 2x^2$, $b = y^2$.
2. $4x^4 = c^2 - b^2$ i.e. $x^4 = \frac{c+b}{2} \cdot \frac{c-b}{2}$

   Also, b is odd, so c is odd, so $\frac{c \pm b}{2}$ are integers. Also, they are coprime because any factor | their sum $= c$, their difference $= b$, and so divides a, contradicting $(a,b) = 1$.

   So $\frac{c+b}{2} = u^4$, $\frac{c-b}{2} = v^4$
3. $b = y^2 = u^4 - v^4 = (u^2+v^2)(u^2-v^2)$

   If u^2+v^2, u^2-v^2 have a common factor, it is odd, since b is odd, and divides $2u^2$, $2v^2$, so divides u^2, v^2, so divides $\frac{c+b}{2}$, $\frac{c-b}{2}$, which are coprime.

So $(u^2+v^2), (u^2-v^2)$ are coprime. So $u^2+v^2=s^2$, $u^2-v^2=t^2$

Then $n^2 = \frac{s^2+t^2}{2} = \left(\frac{s+t}{2}\right)^2 + \left(\frac{s-t}{2}\right)^2$

and $\frac{s+t}{2}, \frac{s-t}{2} \in \mathbb{Z}$.

s, t odd
$u^2+v^2, u^2-v^2 \equiv 1 \ (4)$
$u^2 \equiv 1 (4), \ v^2 \equiv 0 (4)$

Also, $\frac{s+t}{2} \cdot \frac{s-t}{2} = \frac{s^2-t^2}{4} = \frac{v^2}{2} = 2\left(\frac{v}{2}\right)^2 \cdot \frac{v}{2} \in \mathbb{Z}$.

But $u \leq u^4 < u^4+v^4 = c$