PartII Number Theory

zc231

This is based on the lecture notes given by Dr.T.A.Fisher, with some other topics in number theory (possibly not covered in the lecture). Some of the theorems here are non-examinable. I put those here just in case someone is interested. Solutions to the exercises are put in a separate file.

Contents

1 Division **3**
1.1 Division Algorithm . . . 3
1.2 Greatest common divisor . . . 3
1.3 Euclidean Algorithm . . . 4
1.4 Fundamental theorem of arithmetic . . . 4
1.5 Exercises . . . 5

2 Arithmetical functions **7**
2.1 Binomial coefficients . . . 7
2.2 The function $\tau(n)$ and Multiplicative functions . . . 7
2.3 Euler's (totient) function $\phi(n)$ . . . 8
2.4 The function $\sigma(n)$ . . . 10
2.5 The Mobius function $\mu(n)$ . . . 10
2.6 Estimate . . . 12
2.7 Dirichlet series . . . 13
2.8 Exercises . . . 14

3 Congruences **16**
3.1 Definition . . . 16
3.2 Chinese remainder theorem . . . 17
3.3 Wilson's theorem . . . 17
3.4 Lagrange's theorem . . . 18
3.5 Primitive roots . . . 19
3.6 Chevalley's theorem . . . 20
3.7 Exercises . . . 21

4 Quadratic Residues **23**
4.1 Legendre's symbol . . . 23
4.2 Euler's criterion . . . 23
4.3 Gauss's lemma . . . 25
4.4 Law of quadratic reciprocity . . . 25
4.5 Jacobi's symbol . . . 27
4.6 Hensel's lemma . . . 28
4.7 Exercises . . . 28

5 Binary quadratic forms **30**
5.1 Sum of two squares . . . 30
5.2 Definition and equivalence . . . 30
5.3 Reduction . . . 31
5.4 Representations by binary quadratic forms . . . 33
5.5 Exercises . . . 34

6 Distribution of primes **35**
6.1 The sum $\sum_p p^{-1}$ and the product $\prod_p (1-p^{-1})^{-1}$ . . . 35
6.2 Legendre's formula . . . 36
6.3 Bertrand's postulate . . . 36
6.4 Partial summation formula . . . 38
6.5 Merten's results . . . 38
6.6 Riemann zeta function . . . 40
6.7 Gamma function and the functional equation . . . 42
6.8 Riemann Hypothesis . . . 43
6.9 Bernoulli numbers . . . 44
6.10 Exercises . . . 46

7 Continued fraction **48**
7.1 Dirichlet's theorem . . . 48
7.2 Convergents . . . 48
7.3 Period . . . 52
7.4 Pell's equation . . . 53
7.5 A set of real numbers modulo 1 . . . 55
7.6 Exercises . . . 58

8 Primality testing and factoring **60**
8.1 Fermat pseudoprime . . . 60
8.2 Euler pseudoprime . . . 60
8.3 Strong pseudoprime . . . 61
8.4 Fermat factorisation . . . 65
8.5 Factor bases . . . 66
8.6 The Continued fraction method . . . 67
8.7 Pollard's $p-1$ method . . . 67
8.8 Exercises . . . 68

1 Division

1.1 Division Algorithm

Definition 1.1. *Let $a, b \in \mathbb{Z}$. We say b divides a (written $b|a$) if there exists an integer c such that $a = bc$. b is called a factor (or divisor) of a.*

Lemma 1.2. *For all $a, b \in \mathbb{Z}$, $b > 0$, there exists $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < b$.*

Proof. Let $S = \{a - nb : n \in \mathbb{Z}\}$. If $0 \in S$ then there exists q such that $a - bq = 0$. If $0 \notin S$, then clearly S contains some positive integer. Let r be the smallest positive integer in S. For any $x \in S$, $x - b \in S$. Therefore, if $r \geq b$ then $r - b$ is another positive integer in S and $r - b < r$ which is a contradiction. □

1.2 Greatest common divisor

Definition 1.3. *Let $a_1, \ldots, a_n \in \mathbb{Z}$. The greatest common divisor d of $a_1, \ldots, a_n$ (written $(a_1, \ldots, a_n)$) is a positive integer d such that $d|a_i$ for all i, and every common divisor of $a_1, \ldots, a_n$ also divides d. $a_1, \ldots, a_n$ are called coprime if $(a_1, \ldots, a_n) = 1$.*

Lemma 1.4. *Given $a_1, \ldots, a_n \in \mathbb{Z}$, not all zero, let $I = \{\sum_i b_i a_i : b_i \in \mathbb{Z}\}$. Then $I = d\mathbb{Z}$ for some I.*

Proof. Let d be the smallest positive integer in I. Then clearly $d\mathbb{Z} \subset I$. Let $a \in I$, then by lemma 1.2 there exist q and r such that $a = qd + r$ where $0 \leq r < d$. Since d is the smallest integer in I, so $r = 0$. Therefore $d|a$ and so $I \subset d\mathbb{Z}$. □

Corollary 1.5. *Let $a_1, \ldots, a_n \in \mathbb{Z}$, not all zero. Then the greatest common divisor of $a_1, \ldots, a_n$ is d where*

$$d\mathbb{Z} = \{\sum_i b_i a_i : b_i \in \mathbb{Z}\}.$$

Proof. Let $I = \{\sum_i b_i a_i : b_i \in \mathbb{Z}\} = d\mathbb{Z}$ for some d by previous lemma. Since $a_i \in I$ for all i so $d|a_i$ for all i. Let d' be a common factor of $a_1, \ldots, a_n$, then $a_i \in d'\mathbb{Z}$ for all i and so $d\mathbb{Z} = I \subset d'\mathbb{Z}$. Therefore $d'|d$. □

Corollary 1.6. *Let $a_1, \ldots, a_n \in \mathbb{Z}$, not all zero. Then there exist $b_1, \ldots, b_n \in \mathbb{Z}$ such that $\sum_i a_i b_i = c$ if and only if $d|c$ where d is the greatest common divisor of $a_1, \ldots, a_n$.*

Proof. By previous corollary, d is the positive integer such that

$$d\mathbb{Z} = \{\sum_i a_i b_i : b_i \in \mathbb{Z}\}.$$

So there exist integer $b_1, \ldots, b_n$ such that $\sum_i a_i b_i = d$, and so

$$\sum_i a_i (b_i \frac{c}{d}) = c$$

if $d|c$. Conversely, if there exist $b_1, \ldots, b_n \in \mathbb{Z}$ such that $\sum_i a_i b_i = c$. Then $c \in \{\sum_i a_i b_i : b_i \in \mathbb{Z}\} = d\mathbb{Z}$ and so $d|c$. □

Corollary 1.7. *If $(a, b) = 1$ then there exists $x, y \in \mathbb{Z}$ such that $ax + by = 1$.*

1.3 Euclidean Algorithm

We now give an algorithm to compute the greatest common divisor of two positive integers a, b. Since $(a, b, c) = ((a, b), c)$ so this can be used to compute the greatest common divisor of $a_1, \ldots, a_n$.

If $a = b$ then $(a, b) = a$. So we may assume $a > b > 0$. Let $a = r_0$ and $b = r_1$. For each $i \geq 1$, by Lemma 1.2, take q_i, r_{i+1} to be positive integers such that

$$r_{i-1} = r_i q_i + r_{i+1}, 0 \leq r_{i+1} < r_i$$

until $r_{k+1} = 0$ for some k. So we have

$$\begin{aligned}
&r_0 = r_1 q_1 + r_2, && 0 < r_2 < r_1;\\
&r_1 = r_2 q_2 + r_3, && 0 < r_3 < r_2;\\
&\cdots\\
&r_{k-2} = r_{k-1} q_{k-1} + r_k, && 0 < r_k < r_{k-1};\\
&r_{k-1} = r_k q_k;
\end{aligned}$$

We claim that $r_k = (a, b)$. Indeed,

$$(a, b) = (r_0, r_1) = (r_1, r_2) = \cdots = (r_{k-1}, r_k) = r_k.$$

Moreover, by Corollary 1.6 there exist x, y such that $ax + by = d$ where $d = (a, b)$. Euclidean algorithm gives a way to compute the integers x, y. We simply work backwards:

$$d = r_k = r_{k-2} - r_{k-1} q_{k-1} = r_{k-2} - q_{k-1}(r_{k-3} - r_{k-2} q_{k-2}) = \cdots .$$

Example 1.8. *Compute x and y such that $20x + 12y = 4$. We have*

$$20 = 12 + 8, 12 = 8 + 4, 8 = 4 \cdot 2$$

and so $4 = 12 - 8 = 12 - (20 - 12) = 2 \cdot 12 - 20$.

1.4 Fundamental theorem of arithmetic

Definition 1.9. *A positive integer $n > 1$ is called a prime if whenever $b|n$, $b = 1$ or $b = n$. Otherwise n is called composite.*

Lemma 1.10. *Let p be a prime. If $p|ab$ then $p|a$ or $p|b$.*

Proof. If $p|ab$ and $p \nmid a$, then $(p, a) = 1$. By Corollary 1.7, there exists x, y such that $px + ay = 1$. Therefore, $pxb + aby = b$. Since $p|ab$ and $p|pxb$ so $p|b$. □

Similarly,

Lemma 1.11. *Let n be a positive integer. If $n|ab$ then $(n, a) > 1$ or $n|b$.*

Proof. If $(n, a) = 1$, then there exist x, y such that $nx + ay = 1$. Therefore, $nxb + aby = b$. Since $n|nxb, n|ab$ so $n|b$. □

Theorem 1.12 (Fundamental Theorem of Arithmetic). *Every integer $n > 1$ can be written as a product of primes. The representation is unique up to order.*

Proof. Existence is clear: If n is a prime, then we are done. Otherwise there exists a factor m of n such that $1 < m < n$. Let m be the smallest such factor between 1 and n. Then m must be a prime. Now repeat this with $\frac{n}{m}$. For uniqueness, suppose

$$n = p_1 \cdots p_r = q_1 \cdots q_k.$$

Since $p_1|n$ so $p_1|q_1 \cdots q_k$. Apply the previous lemma repeatedly we conclude $p_1|q_i$ for some i. We may relabel $q_1, \ldots, q_k$ so that $p_1|q_1$. Then we have

$$\frac{n}{p_1} = p_2 \cdots p_r = q_2 \cdots q_k.$$

Repeat the above so we conclude $r = k$ and $p_i = q_i$ after relabeling $q_1, \ldots, q_k$. □

Definition 1.13. *Let $a_1, \ldots, a_n$ be positive integers. m is a common multiple of $a_1, \ldots, a_n$ if $a_i|c$ for all i. m is called the least common multiple of $a_1, \ldots, a_n$ (written $\{a_1, \ldots, a_n\}$) m is a common multiple of $a_1, \ldots, a_n$ and $m|m'$ for any other common multiple m' of $a_1, \ldots, a_n$.*

Remark 1.14. *If $a = \prod_{i=1}^r p_i^{a_i}$ and $b = \prod_{i=1}^r p_i^{b_i}$ where $p_1, \ldots, p_r$ are distinct primes and $a_i, b_i \geq 0$. Then $(a, b) = \prod_{i=1}^r p_i^{c_i}$ and $\{a, b\} = \prod_{i=1}^r p_i^{d_i}$ where $c_i = \min\{a_i, b_i\}$ and $d_i = \max\{a_i, b_i\}$. Note that $a_i + b_i = c_i + d_i$ so*

$$(a, b)\{a, b\} = ab.$$

Therefore we can compute $\{a, b\}$ by computing (a, b).

One of the important topics in number theory is to study the distribution of prime numbers.

Definition 1.15. *The function $\pi(x)$ is defined to be*

$$\pi(x) = \{p : p \leq x, p \text{ is a prime}\}.$$

Theorem 1.16 (Euclid). *There are infinitely many primes. In other words, $\pi(x) \to \infty$ as $x \to \infty$.*

Proof. Suppose there are only finitely many primes $p_1, \ldots, p_n$. Let $N = \prod_{i=1}^n p_i + 1$ and let q be a prime factor of N. Then $(q, p_i) = 1$ for all i because $p_i \nmid N$. So $q \neq p_i$ for all i and this gives a contradiction. □

Definition 1.17. *A prime p is called a Mersenne prime if $p = 2^n - 1$ for some n.*

All the largest knowing primes are Mersenne primes.

1.5 Exercises

1. (i) Find integers x, y such that $6x + 10y = 2$. (ii) Find integers $6x + 10y + 15z = 1$.

2. For each $n > 1$, let $S_n = \sum_{i=2}^n \frac{1}{i}$. Show that S_n is not an integer.

3. Let n be a positive integer, prove that n can be written as a sum of (at least two) consecutive positive integers if and only if $n \neq 2^k$ for some k.

4. Prove that if $g_1, g_2, \ldots, g_k$ are integers > 1, then every natural number can be expressed uniquely in the form

$$a_0 + a_1 g_1 + a_2 g_1 g_2 + \cdots + a_k g_1 g_2 \cdots g_k$$

where the a_j are integers satisfying $0 \leq a_j < g_{j+1}$. In particular, if $g_i = k$ for all k then we recover the decimal expansion in base k.

5. Given $a \geq b \geq 1$, let $\lambda(a,b)$ be the number of steps of finding (a,b) by Euclidean algorithm. Show that

$$\lambda(a,b) \leq 2\left[\frac{\log b}{\log 2}\right].$$

6. (i) By considering the factorisation of the form $n = a^2 b$ where b is square free, show that $\pi(x) \geq \frac{\log x}{2\log 2}$ for $x \geq 2$. (ii) By using Fundamental theorem of arithmetic, show that in fact $\pi(x) \geq \frac{\log x}{2\log\log x}$ for x large enough.

7. Show that there exist infinitely many primes of the form $4n+3$.

2 Arithmetical functions

2.1 Binomial coefficients

Definition 2.1. *Let x be a real number. $[x] = \max\{n \in \mathbb{Z} : n \leq x\}$. The fractional part of x, written $\{x\}$ is defined to be $x - [x]$.*

For each n, we use the notation $n! = \prod_{i=1}^{n} i$.

Lemma 2.2. *Let p be a prime and n be a positive integer. The largest l such that p^l divides $n!$ can be expressed as*

$$l = \sum_{k=1}^{\infty} [n/p^k].$$

Proof. For each $k \geq 0$, let a_k be the size of the set

$$\{m \in \mathbb{Z} : 1 \leq m \leq n, p^k | m, p^{k+1} \nmid m\}.$$

Each number in the above set has exact power k dividing $n!$, so $l = \sum_{k=0}^{\infty} k a_k$. But $a_k = [n/p^k] - [n/p^{k+1}]$. So

$$l = \sum_{k=0}^{\infty} k([n/p^k] - [n/p^{k+1}]) = \sum_{k=0}^{\infty} (k+1)[n/p^{k+1}] - \sum_{k=0}^{\infty} k[n/p^{k+1}] = \sum_{k=0}^{\infty} [n/p^k].$$

□

Definition 2.3. *Given two positive integers $m \geq n > 0$, the binomial coefficient $\binom{m}{n}$ is defined to be*

$$\binom{m}{n} = \frac{m!}{n!(m-n)!}.$$

Proposition 2.4. *For all $m \geq n > 0$, $\binom{m}{n}$ is an integer.*

Proof. Let p be a prime number. If $p | n!(m-n)!$ then $p | m!$ because $p < m$. By the previous lemma, if $l_i, i = 1, 2, 3$ are the largest integers such that $p^{l_1} | n!, p^{l_2} | (m-n)!, p^{l_3} | m!$, then

$$l_1 = \sum_{k=1}^{\infty} [n/p^k], l_2 = \sum_{k=1}^{\infty} [(m-n)/p^k], l_3 = \sum_{k=1}^{\infty} [m/p^k].$$

For each $k \geq 0$, we have

$$[m/p^k] \geq [n/p^k] + [(m-n)/p^k]$$

and so $l_3 \geq l_1 + l_2$. This shows that if $p^k | n!(m-n)!$ then $p^k | m!$ for any prime p and so by Fundamental Theorem of Arithmetic, $\binom{m}{n}$ is an integer. □

2.2 The function $\tau(n)$ and Multiplicative functions

Definition 2.5. *A real function f defined on the positive integer is said to be multiplicative if $f(mn) = f(m)f(n)$ for all m, n with $(m, n) = 1$. It is said to be completely multiplicative if $f(mn) = f(m)f(n)$ for all positive integers m, n. In particular, if $n = \prod_i p_i^{a_i}$ then*

$$f(n) = \prod_i f(p_i^{a_i}).$$

Definition 2.6. *The function $\tau(n)$ is the number of all positive factors of n. That is,*

$$\tau(n) = \sum_{d|n} 1.$$

Lemma 2.7. *For all $(m,n) = 1$, there is a bijection*

$$\{(d_1, d_2) \in \mathbb{N}^2 : d_1|m, d_2|n\} \to \{d \in \mathbb{N} : d|mn\}, \quad (d_1, d_2) \mapsto d_1 d_2.$$

In particular, σ is multiplicative.

Proof. Indeed, $d_1 d_2 | mn$ so the map is well-defined. It is injective: Suppose $d_1 d_2 = d_3 d_4$ where $d_1, d_3 | m, d_2, d_4 | n$. Then $d_1 | d_3 d_4$. But $(d_1, d_4) = 1$ so $d_1 | d_3$ by Lemma 1.11. Similarly, $d_3 | d_1$ and so $d_1 = d_3$ and $d_2 = d_4$. It is surjective: By Fundamental Theorem of Arithmetic we have $m = \prod_i p_i^{a_i}$ and $n = \prod_j q_j^{b_j}$ where $p_i \neq q_j$ for all i, j. Then $mn = \prod_{i,j} p_i^{a_i} q_j^{b_j}$. For any $d|mn$ we have $d = \prod_{i,j} p_i^{a'_i} q_j^{b'_j}$ where $a'_i \leq a_i, b'_j \leq b_j$. Let $d_1 = \prod_i p_i^{a'_i}$ and $d_2 = \prod_j q_j^{b'_j}$, then $d_1 | m$ and $d_2 | n$. So the map is a bijection. By comparing the sizes of the two sets we conclude that $\sigma(mn) = \sigma(m)\sigma(n)$. □

Corollary 2.8. *Let $n = \prod_i p_i^{a_i}$. Then*

$$\tau(n) = \prod_i (a_i + 1).$$

Proof. It suffices to show that

$$\tau(p^a) = a + 1$$

for all prime a. Indeed, the factors of p^a are $p^i, i = 0, 1, \ldots, a$. □

Lemma 2.9. *If f is multiplicative and if $g(n) = \sum_{d|n} f(d)$. Then the function g is also multiplicative.*

Proof. By the previous lemma, we have a bijection

$$\{(d_1, d_2) \in \mathbb{N}^2 : d_1|m, d_2|n\} \to \{d \in \mathbb{N} : d|mn\}, \quad (d_1, d_2) \mapsto d_1 d_2$$

for any $(m,n) = 1$. Therefore,

$$g(mn) = \sum_{d|mn} f(d) = \sum_{d_1|m, d_2|n} f(d_1 d_2) = \sum_{d_1|m} f(d_1) \sum_{d_2|n} f(d_2) = g(m)g(n).$$

□

2.3 Euler's (totient) function $\phi(n)$

Definition 2.10. *The Euler's (totient) function $\phi(n)$ is defined to be the size of the set*

$$\{m \in \mathbb{N} : m \leq n : (m,n) = 1\}.$$

By convention, $\phi(1) = 1$.

Lemma 2.11. *There is a bijection*

$$\{d \in \mathbb{N} : d \leq mn, (d, mn) = 1\} \to \{(d_1, d_2) \in \mathbb{N}^2 : d_1 \leq m, (d_1, m) = 1, d_2 \leq n, (d_2, n) = 1\}$$

by $d \mapsto (d_1, d_2)$ where $0 \leq d_1 < m, 0 \leq d_2 < n$ such that

$$d = q_1 m + d_1, \quad d = q_2 n + d_2$$

for some integers q_1, q_2. In particular, ϕ is multiplicative.

Proof. $(d, mn) = 1$ and since

$$d = q_1 m + d_1, \quad d = q_2 n + d_2,$$

we conclude that $(d_1, m) = 1$ and $(d_2, n) = 1$. So the map is well-defined. It is injective: Suppose $d = q_1 m + d_1, d = q_2 n + d_2$ and $d' = q_3 m + d_1, d' = q_4 n + d_2$. Then

$$m|(q_1 - q_3)m|d - d' \text{ and } n|(q_2 - q_4)n|d - d'.$$

Since $(m, n) = 1$ so $mn|d - d'$ and so $d - d' = 0$ because $0 < d, d' \leq mn$.

It is surjective: Given d_1, d_2 with $d_1 \leq m, (d_1, m) = 1$ and $d_2 \leq n, (d_2, n) = 1$, let $d = d_1 ny + d_2 mx + zmn$ where $mx + ny = 1$ and z is an integer such that $0 \leq d < mn$. Writing $ny = 1 - mx$ we have $d = d_1 + (d_2 - d_1)mx + zmn$ and so

$$d = ((d_2 - d_1)x + zn)m + d_1$$

and similarly by writing $mx = 1 - ny$ we have

$$d = (d_1 - d_2)y + zm)n + d_2.$$

So $d \mapsto (d_1, d_2)$. Finally,

$$(d, m) = (d_1 ny, m) = (d_1 - d_1 mx, m) = (d_1, m) = 1$$

and

$$(d, n) = (d_2 mx, n) = (d_2 - d_2 ny, n) = (d_2, n) = 1$$

so $(d, mn) = 1$. So d is the preimage of (d_1, d_2). By comparing the sizes of the two sets we conclude that ϕ is multiplicative. □

Corollary 2.12. *Let $n = \prod_i p_i^{a_i}$. Then*

$$\phi(n) = \prod_i p^{a_i - 1}(p_i - 1).$$

Proof. Since ϕ is multiplicative, it suffices to show that $\phi(p^a) = p^{a-1}(p-1)$ for any prime p. Indeed, for any n, $(n, p^a) = 1$ if and only if $(n, p) = 1$. Since the number of positive integers less than p^a which are divisible by p is p^{a-1}, so

$$\phi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1).$$

□

Note that this also shows $\phi(n)$ is always even for all $n > 2$. Indeed, $(a, n) = 1$ if and only if $(n - a, n) = 1$.

Corollary 2.13. *We have an identity*

$$\sum_{d|n} \phi(d) = n.$$

Proof. Since ϕ is multiplicative, then $\sum_{d|n} \phi(d)$ is also multiplicative and so it suffices to show that

$$\sum_{d|p^a} \phi(d) = p^a$$

for any prime p. Indeed,

$$\sum_{d|p^a} \phi(d) = \sum_{i=0}^{a} \phi(p^i) = 1 + \sum_{i=1} (p^i - p^{i-1}) = p^a.$$

□

Remark 2.14. *One can show the above identity directly by considering the bijection*

$$\{c \in \mathbb{N} : c \leq d, (c, d) = 1\} \to \{c \in \mathbb{N} : c \leq n, (c, n) = \frac{n}{d}\}, \quad c \mapsto c\frac{n}{d}$$

and $\sum_{d|n} \phi(d) = \sum_{d|n} \phi\left(\frac{n}{d}\right)$.

2.4 The function $\sigma(n)$

Definition 2.15. *The function $\sigma(n)$ is defined to be the sum of all positive factors of n. In other words, $\sigma(n) = \sum_{d|n} d$.*

Lemma 2.16. *$\sigma(n)$ is multiplicative.*

Proof. By Lemma 2.7, for all $(m, n) = 1$ we have

$$\sigma(mn) = \sum_{d|mn} d = \sum_{d_1|m, d_2|n} d_1 d_2 = \sum_{d_1|m} d_1 \sum_{d_2|n} d_2 = \sigma(m)\sigma(n).$$

□

Corollary 2.17. *Let $n = \prod_i p_i^{a_i}$. Then*

$$\sigma(n) = \prod_i (p_i^{a_i+1} - 1)/(p_i - 1).$$

Proof. It suffices to show that

$$\sigma(p^a) = (p^{a+1} - 1)/(p - 1)$$

for all primes p. Indeed,

$$\sigma(p^a) = \sum_{i=0}^{a} p^i = (p^{a+1} - 1)/(p - 1).$$

□

2.5 The Mobius function $\mu(n)$

Definition 2.18. *The Mobius function $\mu(n)$ is defined to be 1 if $n = 1$, 0 if n is divisible by p^2 for some prime p, and $(-1)^k$ if $n = p_1 \cdots p_k$ where $p_1, \ldots, p_k$ are distinct primes.*

Lemma 2.19. *$\mu(n)$ is multiplicative.*

Proof. For all $(m, n) = 1$ if one of m, n is divisible by p^2 for some p, so is mn. If m, n are both square free, (i.e. not divisible by p^2 for any prime) then mn is also square free. Since $(-1)^{k_1+k_2} = (-1)^{k_1}(-1)^{k_2}$ so μ is multiplicative. □

Corollary 2.20. *Let $\nu(n) = \sum_{d|n} \mu(d)$. Then ν is multiplicative and $\nu(n) = 1$ if $n = 1$ and $\nu(n) = 0$ for all $n \geq 2$.*

Proof. By the previous lemma and Lemma 2.9, ν is multiplicative. If $n = 1$ then $\nu(1) = \mu(1) = 1$. For any prime p,

$$\nu(p^a) = \sum_{d|p^a} \mu(d) = 1 - 1 + 0 + 0 + \cdots = 0.$$

Therefore $\nu(n) = 0$ for all $n \geq 2$. □

Definition 2.21. *Let f, g be real functions defined on positive integers. The convolution of f and g, written $f * g$ is defined to be*

$$f * g(n) = \sum_{d|n} f(d)g(n/d).$$

By convention, the function $1(n)$ is defined to be $1(n) = 1$ for all n. Therefore, $\sum_{d|n} f(d)$ can be written as $f * 1$.

Lemma 2.22. *$f * g = g * f$ for any f and g. Further, $(f * g) * h = f * (g * h)$ for any f, g and h.*

Proof. For any f and g,

$$f * g = \sum_{d|n} f(d)g(n/d) = \sum_{d|n} f(n/d)g(d) = g * f.$$

For any f, g and h, we have

$$\begin{aligned}
(f * g) * h &= \sum_{d|n} (f * g)(d)h(n/d) = \sum_{d|n} \sum_{e|d} f(e)g(d/e)h(n/d) \\
&= \sum_{dd'=n} \sum_{ee'=d} f(e)g(e')h(d') \\
&= \sum_{ee'd'=n} f(e)g(e')h(d').
\end{aligned}$$

Since $f * (g * h) = (g * h) * f$, by symmetry

$$(g * h) * f = \sum_{ee'd'=n} f(e)g(e')h(d')$$

and so $(f * g) * h = f * (g * h)$. □

Theorem 2.23 (**Mobius Inversion Formula**). *Let f be any real function defined on positive integers (not necessarily multiplicative), and let $g = f * 1$. Then $f = g * \mu$. Conversely, if $f = g * \mu$ then $g = f * 1$.*

Proof. We have

$$\begin{aligned}
g * \mu &= \sum_{d|n} g(n/d)\mu(d) = \sum_{d|n} \sum_{e|n/d} f(e)\mu(d) \\
&= \sum_{dd'=n} \sum_{e|d'} f(e)\mu(d) \\
&= \sum_{dee'=n} f(e)\mu(d) \\
&= \sum_{e|n} f(e) \sum_{d|n/e} \mu(d) = \sum_{e|n} f(e)\nu(n/e) = f(n).
\end{aligned}$$

Conversely, if $f = g * \mu$ then

$$\begin{aligned}
f * 1 &= \sum_{d|n} f(d) = \sum_{d|n} \sum_{e|d} g(e)\mu(d/e) \\
&= \sum_{dee'=n} g(e)\mu(e') \\
&= \sum_{e|n} g(e)\nu(n/e) = g(n).
\end{aligned}$$

□

The following is the multiplicative version of Mobius inversion.

Corollary 2.24. *If $F(n) = \prod_{d|n} f(d)$, then $f(n) = \prod_{d|n} F(d)^{\mu(n/d)}$.*

Proof. Let $G(n) = \log F(n)$ and $g(n) = \log f(n)$. Then

$$G(n) = \sum_{d|n} g(d)$$

and so by Mobius inversion formula

$$g(n) = \sum_{d|n} G(d)\mu(n/d).$$

Therefore,

$$f(n) = \exp g(n) = \prod_{d|n} F(d)^{\mu(n/d)}.$$

□

2.6 Estimate

Often we want to estimate $\sum_{n\le x} f(n)$, where $x \in \mathbb{R}$.

Definition 2.25. *For any real function $f(x)$, $g(x) = O(f(x))$ is a quantity such that there exist positive constants c, M such that*

$$|g(x)| \le c|f(x)| \text{ for all } x \ge M.$$

In other words, $|g(x)/f(x)|$ is bounded. The little o notation $h(x) = o(f(x))$ means that $h(x)/f(x) \to 0$ as $x \to \infty$. The asymptotic notation $r(x) \sim f(x)$ means that $r(x)/f(x) \to 1$ as $x \to \infty$.

We shall give several examples.

Proposition 2.26. $\sum_{n\le x} \tau(n) = x\log x + O(x)$.

Proof. We have

$$\sum_{n\le x} \tau(x) = \sum_{n\le x}\sum_{d|n} 1 = \sum_{dm\le x} 1 = \sum_{d\le x}[x/d] = \sum_{d\le x} x/d + O(x).$$

But $\sum_{d\le x} 1/d = \log x + O(1)$ by using integral approximation so

$$\sum_{n\le x} \tau(n) = x\log x + O(x).$$

□

Therefore the average order of τ is about $\log x$.

Proposition 2.27. $\sum_{n\le x} \sigma(n) = \frac{\pi^2}{12}x^2 + O(x\log x)$.

Proof. We observe that

$$\sum_{n\le x} \sigma(n) = \sum_{n\le x}\sum_{d|n} d = \sum_{dm\le x} d = \sum_{m\le x}\sum_{d\le x/m} d.$$

Since

$$\sum_{d\le x/m} d = \frac{1}{2}[x/m]([x/m]+1) = \frac{1}{2}(x/m)^2 + O(x/m),$$

we have

$$\sum_{m\le x}\sum_{d\le x/m} d = \sum_{m\le x}(\frac{1}{2}(x/m)^2 + O(x/m))\frac{x^2}{2}\sum_{m\le x}\frac{1}{m^2} + \sum_{m\le x} O(x/m).$$

We have seen in the previous proposition $\sum_{m\le x} O(x/m) = O(x\log x)$. Finally we use the fact that

$$\sum_{m\le x}\frac{1}{m^2} = \sum_{m=1}^{\infty}\frac{1}{m^2} + O(1/x)$$

and the result follows by the identity $\sum_{m=1}^{\infty}\frac{1}{m^2} = \pi^2/6$. □

Proposition 2.28. $\sum_{n\le x}\phi(x) = \frac{3}{\pi^2}x^2 + O(x\log x)$.

Proof. We have

$$\sum_{n\le x}\phi(n) = \sum_{n\le x}\sum_{d|n}\mu(d)(n/d) = \sum_{de\le x}\mu(d)e = \sum_{d\le x}\mu(d)\sum_{e\le x/d} e.$$

Since we have seen that $\sum_{e\le x/d} e = \frac{1}{2}(x/d)^2 + O(x/d)$, so

$$\sum_{d\le x}\mu(d)\sum_{e\le x/d} e = x^2/2\sum_{d\le x}\mu(d)(1/d)^2 + x\sum_{d\le x}\mu(d)O(1/d).$$

But $\sum_{d\le x}\mu(d)/d^2 = \sum_{d=1}^{\infty}\mu(d)/d^2 + O(1/x)$. We wil show later that $\sum_{d=1}^{\infty}\mu(d)/d^2 = 6/\pi^2$. So we conclude that

$$\sum_{n\le x}\phi(n) = \frac{3}{\pi^2}x^2 + O(x\log x).$$

□

Corollary 2.29. *The probability of two randomly selected positive integers being coprime is* $\frac{6}{\pi^2}$.

Proof. For each positive integer x, the sum $\sum_{n\le x}\phi(n)$ is the number of unordered pairs of coprime integers a, b with $0 < a, b \le x$. There are $\binom{x}{2}$ ways to select two positive integers a, b with $0 < a, b \le x$. So the probability that two randomly selected integers less than or equal to x being coprime is $\frac{\sum_{n\le x}\phi(n)}{\binom{x}{2}}$. By the previous proposition and let $x\to\infty$ we conclude that

$$\lim_{x\to\infty}\frac{\sum_{n\le x}\phi(n)}{\binom{x}{2}} = \frac{6}{\pi^2}.$$

□

2.7 Dirichlet series

We introduce Dirichlet series of the form $\sum_{n=1}^{\infty}\frac{f(n)}{n^s}$ where $f(n)\in\mathbb{Z}$ for each n and $s\in\mathbb{C}$. For convention, we write $s = \sigma + it$ with $\sigma, t\in\mathbb{R}$.

Definition 2.30. *The Riemann zeta-function* $\zeta(s)$ *is defined to be*

$$\zeta(s) = \sum_{n=1}^{\infty}\frac{1}{n^s}.$$

It converges absolutely for $\sigma > 1$.

Proposition 2.31. *Given Dirichlet series* $F(s) = \sum_n f(n)/n^s$ *and* $G(s) = \sum_n g(n)/n^s$, *if* $F(s), G(s)$ *both converge absolutely for* $s\in S$ *for some* S. *Then* $F(s)G(s) = \sum_n (f*g)(n)/n^s$ *for* $s\in S$.

Proof. Since F, G both converge absolutely so we are free to rearrange the sum. Indeed, we have

$$F(s)G(s) = \sum_k f(k)/k^s \sum_m g(m)/m^s = \sum_{m,k} f(k)g(m)/(km)^s = \sum_n \sum_{k|n} f(k)g(n/k)/n^s.$$

□

Corollary 2.32. $\frac{1}{\zeta(s)} = \sum_n \mu(n)/n^s$ *for* $\sigma > 1$. *In particular,* $\sum_n \mu(n)/n^2 = 6/\pi^2$.

Proof. It suffices to prove that $\zeta(s)\sum_n \mu(n)/n^s = 1$. Since $\zeta(s)$ and $\sum_n \mu(n)/n^s$ both converge absolutely for $\sigma > 1$ and so

$$\zeta(s)\sum_n \mu(n)/n^s = \sum_n (1 * \mu)(n)/n^s = \sum_n \nu(n)/n^s = 1.$$

□

2.8 Exercises

1. Show that the number of ordered pairs of positive integers whose least common multiple is n equals $\tau(n^2)$.

2. Show that $\sum_{d^2|n} \mu(d) = |\mu(n)|$.

3. Show that if $\sigma(n)$ is odd then n is a square or twice a square.

4. For each $n \geq 2$, show that
$$\sigma(n) + \phi(n) = n\tau(n)$$
if and only if n is a prime.

5. For each $n \geq 2$, let
$$T(n) = \{a : 1 \leq a \leq n, (a, n) = 1\}$$
and $f(n) = \frac{1}{n}\sum_{a \in T(n)} a$. (i) Show that $f(n) = \frac{1}{2}\phi(n)$.
(ii) By evaluating $\prod_{a \leq n} \frac{a}{n}$ in two different ways, show also that
$$\prod_{a \in T(n)} a = n^{\phi(n)} \prod_{d|n} (d!/d^d)^{\mu(n/d)}.$$

6. If n has k distinct prime factors then $\sum_{d|n} |\mu(d)| = 2^k$.

7. Find all positive integers n such that (i) $\phi(n)|n$ (ii) $\phi(n) = \frac{1}{2}n$ (iii) $\phi(n) = \phi(2n)$.

8. For $\Re(s) > 1$, compute the Dirichlet series of (i) $\zeta(s)^2$ (ii) $1/\zeta(s)$ (iii) $\zeta(s-1)/\zeta(s)$.

9. Let A be the matrix with $A_{ij} = (i, j)$. (i) Let $g(i, j) = 1$ if $j|i$ and 0 otherwise. Show that
$$A_{ij} = \sum_{d \leq n} g(i, d)g(j, d)\phi(d).$$
(ii) By considering the matrices B, C where
$$B_{ij} = g(i, j) \text{ and } C_{ij} = g(j, i)\phi(i)$$
Show that
$$\det A = \prod_{k=1}^{n} \phi(k).$$

10. (i) Prove the following generalised version of Mobius inversion formula. Let f, g be functions defined over $\mathbb{R}_{\geq 1}$. Show that if

$$g(x) = \sum_{n \leq x} f(x/n),$$

then

$$f(x) = \sum_{n \leq x} \mu(n) g(x/n).$$

(ii) Show that $\sum_{n \leq x} \mu(n)[x/n] = 1$. Hence prove that

$$|\sum_{n \leq x} \mu(n)/n| \leq 1.$$

3 Congruences

In this chapter we will introduce the concept of congruences. We shall assume $n \geq 2$.

3.1 Definition

Definition 3.1. *We say a is congruent to b mod n, written*

$$a \equiv b \ mod \ n$$

if $n|a-b$. It is easy to check that this is an equivalence relation.

Lemma 3.2. *If $a \equiv a'$ mod n and $b \equiv b'$ mod n then $a+b \equiv a'+b'$ mod n and $ab \equiv a'b'$ mod n. For any integer c, $ca \equiv ca'$ mod n. Conversely, if $ca \equiv ca'$ mod n and $(c,n)=1$, then $a \equiv a'$ mod n.*

Further, if f is a polynomial with integer coefficients, then $f(a) \equiv f(a')$ mod n.

Proof. The first statement is clear because if $n|a-a', n|b-b'$ then $n|(a+b)-(a'+b')$. Now $ab-a'b' = ab-ab'+ab'-a'b' = a(b-b')+(a-a')b'$ so $n|ab-a'b'$. It is clear that if $n|a-a'$ then $n|ca-ca'$ for any c. Conversely, if $n|c(a-a')$ and $(c,n)=1$ then $n|a-a'$. Finally, $n|a-a'|f(a)-f(a')$ for any polynomial f with integer coefficients. □

Definition 3.3. *Let $n \geq 1$ be a positive integer. $\mathbb{Z}/n\mathbb{Z}$ is the quotient ring so that addition and multiplication can be understood in terms of modular arithmetic. That is,*

$$(a+n\mathbb{Z})+(b+n\mathbb{Z}) = (a+b)+n\mathbb{Z}, (a+n\mathbb{Z})(b+n\mathbb{Z}) = ab+n\mathbb{Z}.$$

Lemma 3.4. *The followings are equivalent. (i) $(a,n)=1$. (ii) There exists x such that $ax \equiv 1$ mod n. (iii) a is a generator for the additive group $\mathbb{Z}/n\mathbb{Z}$.*

Proof. We shall prove (i) implies (ii), (ii) implies (iii) and (iii) implies (i). If $(a,n)=1$ then there exist x,y such that $ax+ny=1$ and so $ax \equiv 1$ mod n. Suppose there exists x such that $ax \equiv 1$ mod n and so there exists y such that

$$ax+ny=1.$$

Let d be the order of a in $\mathbb{Z}/n\mathbb{Z}$ and so $n|ad$. Since $axd+nyd=d$ and $n|axd, n|nyd$ so $n|d$. Therefore $d=n$. Finally, if a generates $\mathbb{Z}/n\mathbb{Z}$ and $(a,n)=d>1$. Then $n|\frac{n}{d}a$ and so the order of a is at most $\frac{n}{d}<n$ which is a contradiction. □

Lemma 3.5. *The multiplicative group of the quotient ring $\mathbb{Z}/n\mathbb{Z}$, written $(\mathbb{Z}/n\mathbb{Z})^\times$, has size $\phi(n)$.*

Proof. $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ if and only if there exists x such that $ax \equiv 1$ mod n, if and only if $(a,n)=1$ by the previous lemma. □

Corollary 3.6. *$\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is prime.*

Proof. $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if every non-zero element is a unit, if and only if $\phi(n)=n-1$, if and only if n is a prime. □

Corollary 3.7 (Fermat Euler theorem). *For any $(a,n)=1$, we have*

$$a^{\phi(n)} \equiv 1 \ mod \ n.$$

In particular, if $p \nmid a$, then $a^{p-1} \equiv 1$ mod p.

Proof. Since $(\mathbb{Z}/n\mathbb{Z})^\times$ has size $\phi(n)$, so $a^{\phi(n)} \equiv 1$ mod n. □

3.2 Chinese remainder theorem

Lemma 3.8. *The linear congruence $ax = b \bmod n$ is soluble for some integer x if and only if $(a, n)|b$.*

Proof. Suppose such x exists, then $n|ax - b$ and so $(a, n)|n|ax - b$. Since $(a, n)|ax$ so $(a, n)|b$. Conversely, if $(a, n)|b$ then there exist x, y such that $ax + ny = (a, n)$ and so

$$ax\frac{b}{(a,n)} + ny\frac{b}{(a,n)} = b$$

and so $ax\frac{b}{(a,n)} \equiv b \bmod n$. □

We now turn to simultaneous linear congruences.

Theorem 3.9 (Chinese remainder theorem). *Let $n_1, \ldots, n_k$ be natural numbers and suppose that they are pairwise coprime, that is $(n_i, n_j) = 1$ for all $i \neq j$. Then, for any $c_1, \ldots, c_k$, the congruences $x \equiv c_j \bmod n_j$ with $1 \leq j \leq k$ are soluble simultaneously for some integer x. The solution is unique modulo $n = \prod_i n_i$.*

Proof. Existence: Let $n = \prod_i n_i$ and $m_j = n/n_j$. Then $n_i|m_j$ for all $i \neq j$ and m_j is coprime to n_j. So there exists x_j such that $m_j x_j \equiv c_j \bmod n_j$ by the previous lemma. Let

$$x = \sum_j x_j m_j.$$

Then $x \equiv c_j x_j m_j \equiv c_j \bmod n_j$.

Uniqueness: Suppose x, y both satisfy the condition. Then $n_j|x - y$ for all j and so $n|x - y$. □

Here is another version of Chinese remainder theorem.

Corollary 3.10. *Let $n = m_1 \cdots m_k$ where $m_1, \ldots, m_k$ are pairwise coprime. Then we have a ring isomorphism*

$$\mathbb{Z}/n\mathbb{Z} \cong \prod_i \mathbb{Z}/m_i\mathbb{Z}, \quad a + n\mathbb{Z} \mapsto \prod_i a + m_i\mathbb{Z}.$$

In particular, we have a group isomorphism

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \prod_i (\mathbb{Z}/m_i\mathbb{Z})^\times$$

and this gives another proof that ϕ is multiplicative by comparing the sizes of the groups.

Proof. It is clearly a well-defined ring homomorphism. Injectivity follows from the uniqueness of Chinese remainder theorem and surjectivity follows from the existence of Chinese remainder theorem. □

3.3 Wilson's theorem

Theorem 3.11. *For any prime p, $(p - 1)! \equiv -1 \bmod p$.*

Proof. For each a, $a^2 \equiv 1 \bmod p$ if and only if $p|(a-1)(a+1)$, if and only if $a \equiv \pm 1 \bmod p$. Therefore, if $a \not\equiv \pm 1 \bmod p$, then there exists $b \not\equiv a \bmod p$ such that $ab \equiv 1 \bmod p$. So

$$(p - 1)! \equiv 1 \cdot (p - 1) \equiv -1 \bmod p.$$

□

Corollary 3.12. *Let p be an odd prime. There exists x such that*

$$x^2 \equiv -1 \ mod\ p$$

if and only if $p \equiv 1 \ mod\ 4$.

Proof. Suppose there exists x such that

$$x^2 \equiv -1 \bmod p.$$

Then

$$1 \equiv x^{p-1} = (x^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \bmod p.$$

This implies that $\frac{p-1}{2}$ is even and so $p \equiv 1 \bmod 4$. Conversely, suppose $p \equiv 1 \bmod 4$. Let $r = \frac{p-1}{2}$ and so r is even. Then

$$-1 \equiv (p-1)! \equiv (r!)^2(-1)^r \equiv (r!)^2 \bmod p$$

where we write every integer i between $r+1$ and $p-1$ as $p-j$ for some $j \leq r$. □

3.4 Lagrange's theorem

Definition 3.13. *Let R be a (commutative) ring. We write $R[X]$ to be the polynomial ring consisting polynomials of the form*

$$a_0 + a_1X + \cdots a_nX^n, n \in \mathbb{Z}_{\geq 0}, a_i \in R.$$

Remark 3.14. *The map*

$$R[X] \to \{functionsR \to R\}, \quad f \mapsto (\alpha \mapsto f(\alpha))$$

is not always surjective. For example, $R = \mathbb{Z}/p\mathbb{Z}$ and $f = X^p - X$. Then $f(\alpha) = 0$ for all $\alpha \in R$ by Fermat Euler theorem. But $f \neq 0$ in $R[X]$.

Lemma 3.15 (Division Algorithm). *Let $f, g \in R[X]$. Suppose the leading coefficient of g is a unit in R, then there exist $q, r \in R[X]$ with $\deg(r) < \deg(g)$ such that $f = gq + r$.*

Proof. If $\deg f < \deg g$ then the result is obvious. Let $\deg f \geq \deg g$ and let $n = \deg f - \deg g$. Let a be the leading coefficient of f and b be the leading coefficient of g. Since b is a unit, there exists $c \in R$ such that $bc = a$. Then $f_1 = f - cgX^n$ has degree less than f. Now repeat the above for $f1$ and g. Thus, we obtain a sequence

$$\begin{aligned}
&f = gq_1 + f_1, && \deg f_1 \geq \deg f \\
&f_1 = gq_2 + f_2, && \deg f_2 \geq \deg g \\
&\cdots \\
&f_{k-1} = gq_k + f_k, && \deg f_k < \deg g.
\end{aligned}$$

Therefore, $f = g(\sum_i q_i) + f_k$. □

Corollary 3.16. *If $f \in R[X]$ has a root $\alpha \in R$. Then $f(X) = (X - \alpha)q(X)$ for some $q(X) \in R[X]$.*

Proof. Apply division algorithm for f and $X - \alpha$ so

$$f(X) = (X - \alpha)q(X) + r(X), \deg r(X) < \deg X - \alpha.$$

Therefore $r(X)$ has degree 0 and so $r(X)$ is a constant in R. Since $f(\alpha) = 0$ so $r(\alpha) = 0$ and so $r(X) = 0$. □

Theorem 3.17 (Lagrange's theorem). *Let R be an integral domain (that is, $ab = 0$ if and only if $a = 0$ or $b = 0$) and $f \in R[X]$ of degree n and $f \neq 0$. Then f has at most n roots in R.*

Proof. We prove the theorem by induction on $n = \deg f$. If $n = 1$, then $f = aX - b$ for some $a, b \in R$ and so either f has no root of $x = b/a$ is the only root. Suppose the statement is true for n. Now let $\deg f = n + 1$. If f has a root α then by the previous corollary, there exists $q(X)$ such that

$$f(X) = (X - \alpha)q(X).$$

Then $\deg q(X) = n$ and so it has at most n roots. Therefore, f has at most $n + 1$ roots. □

Remark 3.18. *By considering $R = \mathbb{Z}/p\mathbb{Z}$, $f(X) = X^{p-1} - 1 - \prod_{i=1}^{p-1}(X - i)$, we have another proof of Wilson's theorem by using Lagrange's theorem. Indeed, f has degree at most $p-2$ but $X = 1, \ldots, p-1$ are roots of f. Therefore, $f = 0$ by Lagrange's theorem. By considering the constant term we have $-1 \equiv (p - 1)!$ mod p.*

3.5 Primitive roots

We will show that $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is cyclic for all odd prime p.

Lemma 3.19. *For each prime p, $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic.*

Proof. Each element $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ satisfies $a^{p-1} = 1$. So the order of a is d for some $d|p - 1$. Let S_d be the set of elements with order d.

Suppose $S_d \neq$. Let $a \in S_d$ and let G_d be the subgroup generated by a. Then $G_d = \{1, a, \ldots, a^{d-1}\}$. Let $R = \mathbb{Z}/p\mathbb{Z}$ and $f(X) = X^d - 1$. Every element of order d is a root of f. By Lagrange's theorem f has at most d roots. But each element in G_d is a root of f and so these are all the roots of f. Therefore each element of order d is a^i for some $i < d$.

Since $G_d \cong \mathbb{Z}/d\mathbb{Z}$ via $a^i \mapsto i$. By Lemma 3.4, we conclude that $(i, d) = 1$. So $|S_d| = \phi(d)$. Therefore $|S_d| = 0$ or $\phi(d)$. Recall that $\sum_{d|p-1} \phi(d) = p - 1$, so

$$\sum_{d|p-1} \phi(d) = p - 1 = \sum_{d|p-1} |S_d|.$$

This shows that $|S_d| = \phi(d)$ for all d and so in particular $|S_{p-1}| = \phi(p - 1) \geq 1$, which means there exists an element of order $p - 1$. □

Theorem 3.20. $(\mathbb{Z}/p^n\mathbb{Z})^\times$ *is cyclic for all odd prime p.*

We will prove this by several lemmas.

Lemma 3.21. *For each $n \geq 2$, g generates $(\mathbb{Z}/p^n\mathbb{Z})^\times$ if and only if g generates $(\mathbb{Z}/p\mathbb{Z})^\times$ and $g^{p^{n-2}(p-1)} \not\equiv 1$ mod p^n.*

Proof. Suppose g generates $(\mathbb{Z}/p^n\mathbb{Z})^\times$, then clearly $g^{p^{n-2}(p-1)} \not\equiv 1 \bmod p^n$. Let d be the order of g in $(\mathbb{Z}/p\mathbb{Z})^\times$ and so $g^d = 1 + pz$ for some z. Then

$$g^{dp^{n-1}} \equiv 1 \bmod p^n$$

and so the order of g in $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is less than dp^{n-1} which is a contradiction.

Conversely, let g be a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$ and $g^{p^{n-2}(p-1)} \not\equiv 1 \bmod p^n$. Let d be the order of g in $(\mathbb{Z}/p^n\mathbb{Z})^\times$. Since $\phi(p^n) = p^{n-1}(p - 1)$, so $d|p^{n-1}(p - 1)$. Also $g^d \equiv 1$ mod p^n implies that $g^d \equiv 1$ mod p. So $p - 1|d$ and so $d = (p - 1)p^k$ for some k. But $g^{p^{n-2}(p-1)} \not\equiv 1$ mod p^n so $k > n - 2$ and so $k = n - 1$. Therefore $d = \phi(p^n)$. □

Lemma 3.22. *For each odd prime p, $(\mathbb{Z}/p^2\mathbb{Z})^\times$ is cyclic. In particular, g generates $(\mathbb{Z}/p\mathbb{Z})^\times$ and $g^{p-1} \not\equiv 1$ mod p^2, if and only if g is a generator for $(\mathbb{Z}/p^2\mathbb{Z})^\times$.*

Proof. Consider the natural reduction

$$(\mathbb{Z}/p^2\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times, \quad a + p^2\mathbb{Z} \mapsto a + p\mathbb{Z}.$$

It is clearly surjective. By considering the sizes of the groups, the kernel is a subgroup of order p and so it must be cyclic. Therefore, we have an element of order p and an element of order $p-1$, so we obtain an element of order $p(p-1)$. □

We now prove Theorem 3.20.

Proof. Let g be a generator of $(\mathbb{Z}p^2\mathbb{Z})^\times$. So g is a generator of $(\mathbb{Z}p\mathbb{Z})^\times$ and $g^{p-1} \not\equiv 1$ mod p^2. Let $g^{p-1} = 1 + pz$ where $(z, p) = 1$. Then for each k,

$$g^{p^k(p-1)} = (1 + pz)^{p^k} \equiv 1 + p^{k+1}z \text{ mod } p^{k+2}.$$

In particular, $g^{p^k(p-1)} \not\equiv 1$ mod p^{k+2}. Let $k = n - 2$ and apply Lemma 3.21. □

Remark 3.23. *The proof of the theorem implies that g is a generator of $(\mathbb{Z}/p^n\mathbb{Z})^\times$ if and only if g is a generator of $(\mathbb{Z}/p^2\mathbb{Z})^\times$, if and only if g is a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$ and $g^{p-1} = 1 + pz$ where $(z, p) = 1$.*

Remark 3.24. *Theorem 3.20 is not true for $p = 2$. For example, $(\mathbb{Z}/2^3\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z})^2$.*

3.6 Chevalley's theorem

We briefly discuss the congruence of general polynomials mod p. Throughout, let p be a prime and $R = \mathbb{Z}/p\mathbb{Z}$.

Definition 3.25. *For any $f, g \in R[X_1, \ldots, X_n]$, we say f is equivalent to g, (written $f \sim g$) if*

$$f(a_1, \ldots, a_n) = g(a_1, \ldots, a_n)$$

for all $(a_1, \ldots, a_n) \in R^n$.

Example 3.26. *Note that $f \sim g$ does not imply $f = g$. For example, $X^p - X \sim X^{p+1} - X^2$ but $X^p - X \neq X^{p+1} - X^2$.*

Definition 3.27. *For any $f \in R[X_1, \ldots, X_n]$, f is called reduced if f has degree less than p in each variable X_i.*

Lemma 3.28. *For each polynomial $f \in R[X_1, \ldots, X_n]$ there exists a reduced polynomial f' such that $f' \sim f$.*

Proof. Replace $X_i^{d_i}$ by r_i in f where $d_i = q_i p + r_i$, $0 \leq r_i < p$. and let f' be the polynomial after this reduction. Then f' is reduced and $f' \sim f$. □

Lemma 3.29. *For any $f, g \in R[X_1, \ldots, X_n]$, if f and g are both reduced and $f \sim g$, then $f = g$.*

Proof. By considering $f - g$, we can assume that $g = 0$ and so it suffices to prove that if f is reduced and $f \sim 0$ then $f = 0$.

When $n = 1$ the result follows by Lagrange's theorem. Suppose this is true for n. Then for $n+1$, consider f as a polynomial in $R[X_1, \ldots, X_n][X_{n+1}]$. Write

$$f = b_m X_{n+1}^m + \cdots + b_0, \text{ where } b_i \in R[X_1, \ldots, X_n].$$

Suppose $b_i \not\sim 0$, then there exists $a_1, \ldots, a_n$ such that $b_i(a_1, \ldots, a_n) \neq 0$ and so for this $(a_1, \ldots, a_n)$, the polynomial

$$f(a_1, \ldots, a_n, X_{n+1}) = b_m(a_1, \ldots, a_n)X_{n+1}^m + \cdots + b_0(a_1, \ldots, a_n)$$

is a non-zero polynomial in $R[X_{n+1}$ of degree less than p. But every element in R is a root of the above polynomial by assumption because $f \sim 0$, so this gives a contradiction. Therefore, $b_i \sim 0$ for all i. By inductive hypothesis, $b_i = 0$ for each i and so $f = 0$. □

Theorem 3.30 (Chevalley's theorem). *Let $f \in R[X_1, \ldots, X_n]$ and $\deg f < n$. (i) If f has a solution, then f has at least two solutions. (ii)If f is homogenous, (that means, each monomial in f has the same degree) then f has a non-trivial solution.*

Proof. (i) Let $r = \deg f < n$ and $h = 1 - f^{p-1}$. If $X_i = a_i, i = 1, \ldots, n$ is a solution of f then $h(a_1, \ldots, a_n) = 1$. Suppose f has no other root, then for any other values $x_1, \ldots, x_n \in R$,

$$f^{p-1}(x_1, \ldots, x_n) = 1$$

and so $h(x_1, \ldots, x_n) = 0$.

By Lemma 3.28, there exists a reduced polynomial h' such that $h \sim h'$. Define a reduced polynomial

$$h''(X_1, \ldots, X_n) = \prod_{i=1}^{n}(1 - (X_i - a_i)^{p-1}).$$

Then clearly $h'' \sim h$ and so $h'' \sim h'$. Since h', h'' are reduced, then by the previous lemma, we conclude that $h'' = h'$. Now h has degree $r(p-1)$. Since $h' \sim h$ and h' is reduced so

$$\deg h' \leq r(p-1) < n(p-1) = \deg h''$$

which gives a contradiction. Therefore f has at least two solutions.

(ii) Since f is homogenous then $(0, \ldots, 0)$ is a solution and so by (i), f has a non-trivial solution. □

3.7 Exercises

1. Prove that if $(a, m) = (a - 1, m) = 1$, then

$$\sum_{i=0}^{\phi(m)-1} a^i \equiv 0 \bmod m.$$

   Let $S_1 = \{1, 11, 111, \ldots\}$ and p is a prime $p \neq 2, 5$. Show that there are infinitely many elements in S_1 which are divisible by p

2. Show that $a^{kp-k+1} \equiv a \bmod p$ for all primes p, integers a and positive integers k. Deduce that 798 divides $a^{19} - a$ for all integers a.

3. Show that if $m > 4$ then $(m-1)! \equiv -1 \bmod m$ if and only if m is a prime. Show further that if p is an odd prime and $0 < k < p$ then

$$(p-k)!(k-1)! \equiv (-1)^k \bmod p.$$

4. Show that if $(m, n) = 1$ then $m^{\phi(n)} + n^{\phi(m)} \equiv 1 \bmod mn$.

5. (i) Prove that for a prime $p > 3$ then product of all the distinct primitive roots mod p is congruent to 1 mod p. (ii) Prove that for any prime p, the sum of all the distinct primitive roots mod p is congruent to $\mu(p-1)$ mod p.

6. Find a counter example for Lagrange's theorem when R is not an integral domain.

7. For each odd prime p and $n \geq 2$, show that the kernel of the natural reduction

$$(\mathbb{Z}/p^n\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$$

is cyclic. This gives another proof that $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is cyclic.

By considering the natural reduction

$$(\mathbb{Z}/2^n\mathbb{Z})^\times \to (\mathbb{Z}/4\mathbb{Z})^\times$$

where $n \geq 2$, show that

$$(\mathbb{Z}/2^n\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{n-2}\mathbb{Z}).$$

8. Let a and n be integers greater than 1, and put $N = a^n - 1$. Show that the order of $a + N\mathbb{Z}$ in $(\mathbb{Z}/N\mathbb{Z})^\times$ is exactly n and deduce that $n|\phi(N)$. If n is a prime, deduce that there are infinitely many primes q such that $q \equiv 1$ mod n.

9. Show that for any odd prime p,

$$1^2 \cdot 3^2 \cdot 5^2 \cdots (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \bmod p.$$

10. Let p be a prime > 3, by considering $\frac{1}{i} + \frac{1}{p-i}$ for each $i \leq (p-1)/2$, show that the numerator of $u_p = 1 + \frac{1}{2} + \cdots + \frac{1}{p-1}$ is divisible by p^2.

4 Quadratic Residues

We shall study the quadratic congruences $x^2 \equiv a \bmod n$.

4.1 Legendre's symbol

Definition 4.1. *Let $a \in \mathbb{Z}$ and $n \in \mathbb{N}$ such that $(a, n) = 1$. a is called a quadratic residue (QR) mod n if the congruence $x^2 \equiv a$ mod n has a solution. Otherwise a is called a quadratic non-residue (QNR). Note that if $a|n$ then $x^2 \equiv a$ mod n is also soluble (though in this case a is not a QR mod n by definition).*

Definition 4.2. *Let p be a prime. The Legendres' symbol $\left(\frac{a}{p}\right)$ is defined as 1 if a is a QR mod p, -1 if a is a QNR mod p, and 0 if $p|a$. Clearly, if $a \equiv b$ mod p, then*

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

Lemma 4.3. *For each n, the set of QR mod n forms a group under multiplication.*

Proof. 1 is a QR mod p because $1 \equiv 1^2 \bmod p$. If $x^2 \equiv a \bmod n$ and $y^2 \equiv b \bmod n$ then

$$(xy)^2 \equiv ab \bmod n.$$

If $x^2 \equiv a \bmod n$ then $x^{-2} \equiv a^{-1} \bmod n$. □

Lemma 4.4. *For each $n > 2$, the set of QR mod n has size $\phi(n)/t(n)$ where $t(n)$ is number of elements $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that $x^2 \equiv 1$ mod n. In particular, the set of QR mod p has size $(p-1)/2$ for any odd prime p.*

Proof. The map

$$(\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^\times, \quad x \mapsto x^2$$

is a group homomorphism and the image is the set of QR. The kernel is the set of elements x such that $x^2 \equiv 1 \bmod n$. The result follows from isomorphism theorem. □

4.2 Euler's criterion

Theorem 4.5 (Euler's criterion). *Let p be an odd prime and $a \in \mathbb{Z}$. Then*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \text{ mod } p.$$

Proof. Let g be a generator for $(\mathbb{Z}/p\mathbb{Z})^\times$. Then $g^{2k}, k = 1, \ldots, (p-1)/2$ are QR mod p. Since there are $(p-1)/2$ QR mod p so these are all the QR mod p and so every QNR has the form g^{2k+1} for some k. If a is a QR mod p then $a = g^{2k}$ and so

$$\left(\frac{a}{p}\right) = 1 \equiv g^{k(p-1)} = a^{(p-1)/2} \bmod p.$$

Since $x^2 \equiv 1 \bmod p$ if and only if $x \equiv \pm 1 \bmod p$, so $g^{(p-1)/2} \equiv -1 \bmod p$. Therefore, if a is a QNR and $a = g^{2k+1}$ for some k, then

$$\left(\frac{a}{p}\right) = -1 \equiv g^{k(p-1)+(p-1)/2} = a^{(p-1)/2} \bmod p.$$

□

Corollary 4.6. *For all integers a, b and odd prime p,*

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

In particular, the map

$$\chi : (\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}, \quad a \mapsto \left(\frac{a}{p}\right)$$

is a group homomorphism with kernel the set of QR mod p.

Proof. By Euler's criterion,

$$\left(\frac{ab}{p}\right) \equiv ab^{(p-1)/2} \equiv a^{(p-1)/2} b^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \mod p.$$

Since they are both ± 1 so $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. □

Corollary 4.7. *-1 is a square mod p if and only if $p \equiv 1$ mod 4.*

Proof. Apply Euler's criterion with $a = -1$. □

We give some applications of the above corollary.

Proposition 4.8. *Let p be an odd prime. Then*

(i) $\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0$.

(ii) $\sum_{a=1}^{p-1} a \left(\frac{a}{p}\right) \equiv 0$ *mod p if $p > 3$.*

(iii) $\sum_{a=1}^{p-1} \left(\frac{a(a+1)}{p}\right) = -1$.

Proof. (i) Let b be a QNR mod p (which exists as $p > 2$). Then

$$(\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times, \quad a \mapsto ab$$

is a bijection. So

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = \sum_{a=1}^{p-1} \left(\frac{ab}{p}\right) = \left(\frac{b}{p}\right) \sum_{a=1}^{p-1} \left(\frac{a}{p}\right)$$

and so $\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0$.

(ii) Since $p > 3$, we pick $b \not\equiv \pm 1, 0$ mod p, and by the above bijection we have

$$\sum_{a=1}^{p-1} a \left(\frac{a}{p}\right) \equiv \sum_{a=1}^{p-1} ab \left(\frac{ab}{p}\right) \equiv \pm b \sum_{a=1}^{p-1} a \left(\frac{a}{p}\right) \mod p$$

and so

$$\sum_{a=1}^{p-1} a \left(\frac{a}{p}\right)(1 \pm b) \equiv 0 \mod p.$$

Therefore, $\sum_{a=1}^{p-1} a \left(\frac{a}{p}\right) \equiv 0$.

(iii) There is a bijection

$$(\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times, \quad a \mapsto a^{-1}.$$

So we have

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

where in the last step we set $b = 1 + a^{-1}$. Then by (i)

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

□

4.3 Gauss's lemma

Lemma 4.9 (Gauss's lemma). *Let p be an odd prime and $a \in \mathbb{Z}$ such that $(a,p)=1$. Let a_j be the integer such that $a_j \equiv aj \mod p$ and $-(p-1)/2 \le a_j \le (p-1)/2$. Then*

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

where ν is the size of $\{j : 1 \le j \le (p-1)/2, a_j < 0\}$.

Proof. For each $1 \le i, j \le (p-1)/2$, if $a_i = \pm a_j$, then

$$(j \pm i)a \equiv 0 \mod p.$$

Since $-p < j \pm i < p$ and $(a,p)=1$, so $j \pm i \equiv 0 \mod p$. Therefore, for all $1 \le i \ne j \le (p-1)/2$, $a_i \ne a_j$. So

$$\{|a_1|, \dots, |a_{(p-1)/2}|\} = \{1, 2, \dots, (p-1)/2\}.$$

Therefore,

$$a^{(p-1)/2}\left(\frac{p-1}{2}\right)! = \prod_j a_j = \left(\frac{p-1}{2}\right)!(-1)^\nu$$

where ν is the size of $\{j : 1 \le j \le (p-1)/2, a_j < 0\}$ and so the result follows by Euler's criterion. □

Corollary 4.10. $\left(\frac{2}{p}\right) = 1$ *if and only if* $p \equiv \pm 1$ *mod* 8.

Proof. Let $a = 2$ and so $a_j = 2j$ for $1 \le j \le [\frac{1}{4}p]$ and $a_j = 2j - p$ for $[\frac{1}{4}p] < j \le (p-1)/2$. So $\nu = (p-1)/2 - [\frac{1}{4}p]$ and so ν is even if and only if $p \equiv \pm 1 \mod 8$. □

4.4 Law of quadratic reciprocity

We shall study the relation between $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ for odd primes p and q.

Theorem 4.11. *Let p, q be distinct odd primes. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

We give a proof using Gauss's lemma. An alternative proof can be found in the Exercises. The first step is to interpret the number ν as in Gauss's lemma in another way.

Lemma 4.12. *Let a, p, ν be the numbers as in Gauss's lemma. Then*

$$\nu = \sum_{i=1}^{2m} (-1)^i \left[\frac{ip}{2a}\right], \text{ where } m = \left[\frac{a}{2}\right].$$

Proof. In Gauss's lemma, ν is the number of j such that aj is inside one of the intervals

$$[p/2, p], [3p/3, 2p], \dots, [(n-1/2)p, np].$$

Therefore it is the number of j such that j is in one of the intervals

$$\left[\frac{p}{2a}, \frac{2p}{2a}\right], \left[\frac{3p}{2a}, \frac{4p}{2a}\right], \dots, \left[\frac{(2n-1)p}{2a}, \frac{2np}{2a}\right].$$

The end points are not integers because $(a,p)=1$. Since the number of integers inside an interval $[\alpha, \beta]$ with $\alpha, \beta \notin \mathbb{Z}$ is $[\beta] - [\alpha]$, this proves the statement. □

Lemma 4.13. *Let p, q be distinct odd primes and $a \in \mathbb{Z}$ such that $(a, p) = (a, q) = 1$. Let ν_1, ν_2 be the numbers for p, q respectively as in Gauss's lemma. If $p \equiv \pm q$ mod $4a$, then $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.*

Proof. By Gauss's lemma, it suffices to prove that ν_1 and ν_2 have the same parity. Suppose $p \equiv q$ mod $4a$, then $\left[\frac{ip}{2a}\right]$ and $\left[\frac{iq}{2a}\right]$ have the same parity for all i. Then by the previous lemma, ν_1, ν_2 have the same parity.

Suppose $p \equiv -q$ mod $4a$, then $\left[\frac{ip}{2a}\right]$ and $\left[\frac{-iq}{2a}\right]$ have the same parity. Since $[-\alpha] = -[\alpha] - 1$ for all real number α and so $\left[\frac{ip}{2a}\right]$ and $\left[\frac{iq}{2a}\right]$ have different parity. Therefore again by the previous lemma, ν_1 and ν_2 have the same parity. □

We now prove law of quadratic reciprocity.

Proof. Suppose $p \neq q$ mod 4 then $4|p+q$ and let $p+q = 4a$ for some a. Then

$$\left(\frac{p}{q}\right) = \left(\frac{4a-q}{q}\right) = \left(\frac{a}{q}\right)$$

and

$$\left(\frac{q}{p}\right) = \left(\frac{4a-p}{p}\right) = \left(\frac{a}{p}\right)$$

By the previous lemma, since $p \equiv -q$ mod $4a$, so

$$\left(\frac{p}{q}\right) = \left(\frac{a}{q}\right) = \left(\frac{a}{p}\right) = \left(\frac{q}{p}\right).$$

So $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1$ if $p + q \equiv 0$ mod 4.

Suppose now $p \equiv q$ mod 4, then $4|p-q$ and let $p - q = 4a$ for some a. Then

$$\left(\frac{p}{q}\right) = \left(\frac{4a+q}{q}\right) = \left(\frac{a}{q}\right)$$

and

$$\left(\frac{q}{p}\right) = \left(\frac{p-4a}{p}\right) = \left(\frac{-a}{p}\right)$$

By the previous lemma, since $p \equiv q$ mod $4a$ so

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

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

Corollary 4.14. *-3 is a quadratic residue mod p if and only if $p \equiv 1$ mod 3.*

Proof. By law of quadratic reciprocity, we have

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{(p-1)/2}(-1)^{(p-1)/2}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right).$$

Therefore $\left(\frac{-3}{p}\right) = 1$ if and only if $\left(\frac{p}{3}\right) = 1$, if and only if $p \equiv 1$ mod 3. □

4.5 Jacobi's symbol

This is a generalisation of Legendre's symbol.

Definition 4.15. *Let $n > 1$ be a positive odd integer and $n = \prod_i p_i$ as a product of primes, not necessarily distinct. Then for any integer a, the Jacobi's symbol $\left(\frac{a}{n}\right)$ is*

$$\left(\frac{a}{n}\right) = \prod_i \left(\frac{a}{p_i}\right).$$

Remark 4.16. *The above definition implies that $\left(\frac{a}{n}\right) = 0$ if $(a, n) > 1$. Also by convention we define $\left(\frac{a}{n}\right) = 1$ if $n = 1$. It is clear that if $a \equiv b$ mod n then*

$$\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right).$$

Remark 4.17. *$\left(\frac{a}{n}\right) = 1$ does not imply a is a square mod n. For example, if $a = 2$ and $n = 15$ then*

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1.$$

But if 2 is a square mod 15 then 2 is a square mod 3, which is a contradiction. But if $\left(\frac{a}{n}\right) = -1$ then a is a QNR mod n because by definition, $\left(\frac{a}{n}\right) = -1$ implies $\left(\frac{a}{p}\right) = -1$ for some prime $p|n$. So a is a QNR mod p and hence a QNR mod n.

Proposition 4.18. *Let n be a positive odd integer. $\left(\frac{2}{n}\right) = 1$ if and only if $n \equiv \pm 1$ mod 8.*

Proof. Let $n = \prod_i p_i$ and so

$$\left(\frac{2}{n}\right) = \prod_i \left(\frac{2}{p_i}\right) = (-1)^t$$

where t is the number of p_i such that $p_i \equiv \pm 3$ mod 8. So t is even if and only if $n \equiv \pm 1$ mod 8. □

Theorem 4.19 (Law of quadratic reciprocity for Jacobi's symbol). *Let m, n be odd positive integers such that $(m, n) = 1$. Then*

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}.$$

Proof. Let $n = \prod_i p_i$ and $m = \prod_j q_j$ where $p_i \neq q_j$ for all i, j. Then

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \prod_i \prod_j \left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right) = \prod_i \prod_j (-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}} = \prod_i \prod_j (-1)^{a_{ij}}$$

where $a_{ij} = -1$ if $p_i \equiv q_j \equiv 3$ mod 4 and $a_{ij} = 1$ otherwise.

Therefore, $\prod_i \prod_j (-1)^{a_{ij}} = (-1)^{uv}$ where u is the number of p_i such that $p_i \equiv 3$ mod 4 and v is the number of q_j such that $q_j \equiv 3$ mod 4. Note that u is even if and only if $n \equiv 1$ mod 4 and v is even if and only if $m \equiv 1$ mod 4. So uv has the same parity as $\frac{m-1}{2}\frac{n-1}{2}$. □

4.6 Hensel's lemma

We want to determine whether a is a QR mod n for given integers a and n. By Chinese remainder theorem, if $n = \prod_i p_i^{a_i}$ then a is a QR mod n if and only if a is a QR mod $p_i^{a_i}$ for each i.

Theorem 4.20 (Hensel's lemma). *For each odd prime p, x is a QR mod p if and only if x is a QR mod p^n for all $n \geq 1$.*

Proof. If x is a QR mod p^n for all $n \geq 1$ then x is a QR mod p. Conversely, if x is a QR mod p, then we prove by induction that x is a QR mod p^n for all $n \geq 1$. This is true for $n = 1$. Suppose x is a QR mod p^{n-1} where $n \geq 2$, then there exists y, k such that

$$y^2 = x + p^{n-1}k$$

where $(y, p) = 1$ because $(x, p) = 1$.

We search for an element of the form $y + p^{n-1}b$ such that $(y + p^{n-1}b)^2 \equiv 1 \bmod p^n$. Then we must have

$$(y + p^{n-1}b)^2 = x + p^{n-1}(k + 2by) + p^{2n-2}b^2 \equiv x \bmod p^n.$$

Since $2n - 2 \geq n$ so we need to pick b such that

$$k + 2by \equiv 0 \bmod p$$

and so $b \equiv -2^{-1}y^{-1}k$. Such b exists because $(2, p) = 1$ and so 2^{-1} exists. □

Proposition 4.21. *Let x be an odd integer. Then x is a QR mod 2^n for all $n \geq 1$ if and only if $x \equiv 1$ mod 8.*

Proof. If x is a QR mod 2^n for all $n \geq 1$ then $x \equiv 1 \bmod 8$ because

$$1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \bmod 8.$$

Conversely, let $x \equiv 1 \bmod 8$. Clearly, x is a QR mod $2, 4$ and we prove by induction that x is a QR mod 2^n for all $n \geq 3$. It is clearly true for $n = 3$. Suppose x is a QR mod 2^{n-1} where $n \geq 4$, then there exist integers y, k such that

$$y^2 = x + 2^{n-1}k$$

where y is odd. We search for an element of the form $y + 2^{n-2}b$ such that $(y + 2^{n-2}b)^2 \equiv x \bmod 2^n$. Then we must have

$$y^2 + 2^{n-1}by + 2^{2n-4}b^2 = x + 2^{n-1}(k + by) + 2^{2n-4}b^2 \equiv x \bmod 2^n.$$

So it suffices to pick b such that k and b have the same parity. □

4.7 Exercises

1. Show that if p is a prime $\equiv 3 \bmod 4$ and if $p' = 2p + 1$ is a prime then $2^p \equiv 1 \bmod p'$. Deduce that $2^{251} - 1$ is not a Mersenne prime.

2. Show that if $p \equiv 1 \bmod 4$, then

$$\sum_{a \in \mathrm{QR}} a = \frac{1}{4}p(p-1) = \sum_{a \in \mathrm{QNR}} a.$$

   Give a counter example when $p \equiv 3 \bmod 4$.

3. Let p be a prime of the form $2^n + 1$. Show that a is a quadratic non-residue mod p if and only if a is a primitive root mod p.

4. By considering integers of the form n^2+4, show that there are infinitely many primes congruent to 5 mod 8. By considering $n^2 + 2$ and $n^2 - 2$, show further that there are infinitely many primes congruent to 3 or 7 mod 8.

5. Let $f(x) = ax^2 + bx + c$ where a, b, c are integers, and let p be an odd prime which does not divide a. Prove that the number of solutions of the congruence $f(x) \equiv 0 \bmod p$ is $1 + \left(\frac{d}{p}\right)$ where $d = b^2 - 4ac$.

6. Show that an integer a is a square if and only if the congruence $x^2 \equiv a \bmod p$ is soluble for every prime p.

7. Let $f(x) = ax^2 + bx + c$ where a, b, c are integers. Let p be an odd prime which does not divide a. Further let $d = b^2 - 4ac$. Show that if $p \nmid d$ then
$$\sum_{x=1}^{p} \left(\frac{f(x)}{p}\right) = -\left(\frac{a}{p}\right).$$
Evaluate the sum when $p|d$.

8. Let p be a prime with $p \equiv 3 \bmod 8$. Show that
$$\sum_{a=1}^{p-1} a\left(\frac{a}{p}\right) = \sum_{a=1}^{(p-1)/2} (2a - p)\left(\frac{a}{p}\right) = \sum_{a=1}^{(p-1)/2} (p - 4a)\left(\frac{a}{p}\right).$$
Deduce that if $p > 3$ then
$$\sum_{a=1}^{(p-1)/2} \left(\frac{a}{p}\right) \equiv 0 \bmod 3.$$

9. Let p be an odd prime and $\zeta = e^{2\pi i/p}$. (i) Let
$$\tau = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta^a.$$
Show that $\tau^2 = p'$ where $p' = (-1)^{(p-1)/2}p$.

(ii) Let q be an odd prime and $q \neq p$. Show that $\left(\frac{p'}{q}\right) = 1$ if and only if
$$\tau^{q-1} \equiv 1 \bmod q.$$

(iii) Show that $\tau^{q-1} \equiv \left(\frac{q}{p}\right) \bmod q$. Hence give an alternative proof for law of quadratic reciprocity.

10. Prove the following general version of Hensel's lemma. Suppose $f(x)$ is a polynomial with integer coefficient and m, k are positive integers such that $m \leq k$. If r is an integer such that
$$f(r) \equiv 0 \bmod p^k \text{ and} f'(r) \not\equiv 0 \bmod p$$
then (by considering Taylor expansion) there exists an integer s such that
$$f(s) \equiv 0 \bmod p^{k+m} \text{ and } r \equiv s \bmod p^k.$$
In particular, setting $f(x) = x^2 - a$ and apply this repeatedly gives the Hensel's lemma in the last section.

5 Binary quadratic forms

5.1 Sum of two squares

Which positive integers can be written as sum of two squares? By studying the Gaussian integers $\mathbb{Z}[i]$, we know that a prime p is a sum of squares if and only if $p \equiv 1 \bmod 4$ or $p = 2$. What about composite numbers? $21 \equiv 1 \bmod 4$, but it cannot be written as sum of two squares. So we might need some more condition for composite numbers.

Theorem 5.1. *Let n be a positive integer. n is the sum of two squares if and only if every prime number $p|n$ with $p \equiv 3$ mod 4 divides n to an even power.*

Proof. Suppose $n = x^2 + y^2$ for some x, y and $p|n$ where $p \equiv 3 \bmod 4$. Then $x^2 \equiv -y^2 \bmod p$. Since -1 is not a square mod p, so we must have

$$x \equiv y \equiv 0 \bmod p.$$

This means $p|x, y$ and so $p^2|x^2 + y^2$. Then n^2/p^2 is a sum of two squares and we repeat the above until $p \nmid n$. Therefore p divides n to an even power.

Conversely, let $n = mb^2$ where m is square free. It suffices to prove that m can be written as a sum of two squares. If $p|n$ where $p \equiv 3 \bmod 4$ then p divides n to an even power. Therefore, $p \nmid m$ and so if $p|m$ then $p = 2$ or $p \equiv 1 \bmod 4$. Each such p can be written as sum of two squares, and since

$$(x^2 + y^2)(x'^2 + y'^2) = (xx' + yy')^2 + (xy' - yx')^2$$

so m can be written as a sum of two squares. □

5.2 Definition and equivalence

Definition 5.2. *$f(x, y)$ is called a binary quadratic form if*

$$f(x, y) = ax^2 + bxy + cy^2, \text{ where } a, b, c \in \mathbb{Z}.$$

The discriminant of f is $d = b^2 - 4ac$. An integer n is represented by f if there exist integers x and y such that $f(x, y) = n$. An integer n is properly represented by f if there exist integers x and y where $(x, y) = 1$ such that $f(x, y) = n$.

Remark 5.3. *The discriminant d of a binary quadratic form is congruent to either 0 or 1 mod 4 and d has the same parity as b.*

Definition 5.4. *The forms $x^2 - \frac{1}{4}dy$ for $d \equiv 0$ mod 4 and $x^2 + xy + \frac{1}{4}(1 - d)y^2$ for $d \equiv 1$ mod 4 are called the principal forms with discriminant d. Therefore for each $d \equiv 0, 1$ mod 4 there exist a binary quadratic form with discriminant d.*

Note that $4af(x, y) = (2ax + by)^2 - dy^2$ and so if $d < 0$ the values taken by f are of the same sign and if $d > 0$ then f takes values of both signs. Indeed $4af(1, 0) > 0$ and $4af(b, -2a) = -4a^2y^2 < 0$.

Definition 5.5. *A binary quadratic form is called positive definite if $a > 0, d < 0$ and negative definite if $a < 0, d < 0$. It is called indefinite if $d > 0$.*

We will mainly focus on positive definite binary quadratic forms in this chapter.

Remark 5.6. *We can write f as (a, b, c) or in matrix notation as*

$$M_f = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

Then the discriminant d is $-4 \det M_f$

When do two binary quadratic forms f and g represent the same numbers?

Definition 5.7. *A unimodular substitution is one of the form*

$$X = \alpha x + \gamma y, \quad Y = \beta x + \delta y$$

where $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ *and* $\alpha\delta - \beta\gamma = 1$.

Definition 5.8. *Two binary quadratic forms* f, g *are equivalent (written* $f \sim g$*) if they are related by a unimodular substitution. It is not hard to check that* $\sim$ *is an equivalence relation.*

Lemma 5.9. *In matrix notation, if* $f(x, y) = ax^2 + bxy + cy^2$ *and*

$$g(x, y) = g(\alpha x + \gamma y, \beta x + \delta y) = Ax^2 + Bxy + Cy^2$$

where $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ *and* $\alpha\delta - \beta\gamma = 1$. *Then*

$$\begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix} = T^t \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} T$$

where $T = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}$.

Proof. Write $\begin{pmatrix} X & Y \end{pmatrix} = T \begin{pmatrix} x \\ y \end{pmatrix}$. □

Corollary 5.10. *Equivalent binary quadratic forms have the same discriminant and they represent the same set of integers.*

Proof. Let M_f and M_g be the matrices for f and g respectively. Then $M_g = U^t M_f U$ for some $U \in \mathrm{SL}_2(\mathbb{Z})$. Therefore $\det M_g = \det M_f$. Since U is invertible so $M_f = (U^t)^{-1} M_g U^{-1}$ so f and g represent the same set of integers. □

Remark 5.11. *The converse of the above corollary is not true. For example,* $f = (1, 0, 6)$ *and* $g = (2, 0, 3)$ *have the same discriminant but they are not equivalent. Indeed,* f *represents* 1 *but* $g(x, y) = 2x^2 + 3y^2 \geq 2$.

5.3 Reduction

We have an equivalence relation for binary quadratic forms. It will help to study the equivalence classes if we specify a 'special' form in each equivalence class. We begin with several examples.

Example 5.12. *If* $f(x, y) = ax^2 + bxy + cy^2$. *Then*

$$g(x, y) = f(x + ty, y) = a(x + ty)^2 + b(x + ty)y + cy^2 = ax^2 + (2at + b) + (at^2 + bt + c)y^2.$$

It is clear that $f \sim g$ *and by picking* $t = \pm 1$, *we have*

$$(a, b, c) \sim (a, b \pm a, a \pm b + c).$$

We can also try the unimodular substitution

$$g(x, y) = f(y, -x) = ay^2 - bxy + cx^2$$

and so $(a, b, c) \sim (c, -b, a)$.

The above example shows that

Lemma 5.13. *Every equivalence class of binary quadratic forms consists of a binary quadratic form (a, b, c) with $|b| \leq a$ and a binary quadratic form with $a \leq c$.*

Definition 5.14. *A positive definite binary quadratic form is reduced if either $-a < b \leq a < c$ or $0 \leq b \leq a = c$.*

For example, $(2, \pm 1, 3)$ are both reduced. $(2, 1, 2)$ is reduced but $(2, -1, 2)$ is not reduced.

Lemma 5.15. *Every binary quadratic form is equivalent to a reduced form.*

Proof. Define the unimodular operations

$$S : (a, b, c) \mapsto (c, -b, a), \quad T_{\pm}(a, b \pm 2a, a \pm b, c).$$

If $a > c$, apply S to decrease a, while leaving $|b|$ fixed. If $a < c$ and $|b| > a$ then apply $T_{\pm}$ to decrease $|b|$ while leaving a fixed. Repeat these steps so we eventually obtain a form with

$$|b| \leq a \leq c.$$

If $b = -a$, then apply $T+$ to replace $(a, -a, c)$ by (a, a, c). If $a = c$ then apply S (if necessary) to ensure $b > 0$. □

The following lemma gives a useful algorithm to find reduced forms of discriminant d.

Lemma 5.16. *Let $f = (a, b, c)$ be a reduced binary quadratic form of discriminant d. Then*

$$|b| \leq a < \sqrt{\frac{|d|}{3}}$$

and $b \equiv d$ mod 2.

Proof. We have $|b| \leq a \leq c$ and so

$$d = b^2 - 4ac \leq ac - 4ac \leq -3a^2.$$

Therefore $a^2 \leq \frac{|d|}{3}$. Since $d = b^2 - 4ac$ so b and d have the same parity. □

Example 5.17. *If $d = -4$, then $a \leq 1$ and so $a = 1$. $b = 0$ and $c = 1$ so the only reduced form of discriminant -4 is $x^2 + y^2$.*

Reduced forms can be used to study integers represented by binary quadratic forms.

Corollary 5.18. *A prime p is a sum of two squares if and only if $p = 2$ or $p \equiv 1$ mod 4.*

Proof. If $p = 2$ then $p = 1^2 + 1^2$. If $p \equiv 1$ mod 4 then -1 is a square mod 4 and so there exists u, v such that $u^2 = -1 + pv$. Let $f(x, y) = (p, 2u, v)$ then $d_f = -4$. Since there is only one reduced form of discriminant -4, so $f \sim (1, 0, 1)$ and so they represent the same set of integers. In particular, p is represented by f and hence p is represented by $(1, 0, 1)$. □

Here is a useful fact of reduced form.

Lemma 5.19. *The smallest three positive integers properly represented by a reduced form $f = (a, b, c)$ are $a, b, a + c - |b|$.*

Proof. If x, y are non-zero integers with $|x| \geq |y|$ then

$$\begin{aligned} f(x,y) &\geq |x|(a|x| - |b||y|) + c|y|^2 \\ &\geq |x|^2(a - |b|) + c|y|^2 \geq a - |b| + c. \end{aligned}$$

Similarly, if $|y| \geq |x| > 0$ then

$$\begin{aligned} f(x,y) &\geq a|x|^2 + |y|(-|b||x| + c|y|) \\ &\geq a|x|^2 + (c - |b|)|y|^2 \geq a - |b| + c. \end{aligned}$$

□

Remark 5.20. *Note these are the smallest integers properly represented by f. For example, if $f = x^2 + 5y^2$ then the smallest three positive integers properly represented by f are $1, 5, 5$ but f also represents 4 (not properly represent).*

Can reduced forms be equivalent?

Theorem 5.21. *Let f, g be two reduced forms. Then f is not equivalent to g.*

Proof. Let

$$f = (a, b, c), \quad g = (a', b', c')$$

be reduced forms. Suppose f, g are equivalent. Then f, g represent the same set of integers. In particular, the smallest three positive integers properly represented by f and g are the same. So $a = a', c = c'$ and $a + c - |b| = a' + c' - |b'|$. So $b = \pm b'$. It remains to check that $b = b'$.

If $b = a$ then $b = a'$ and so $a' = \pm b'$. But g is reduced so $b' = a' = b$. If $a = c$ then $a' = c'$ so $b, b' \geq 0$ and so $b = b'$. So we may assume that $-a < b < a < c$. Then by the previous lemma, for all non-zero integers x, y,

$$f(x,y) \geq a - |b| + c > c > a.$$

So $f(x,y) = a$ if and only if $(x,y) = (\pm 1, 0)$ and $g(x,y) = a'$ if and only if $(x,y) = (\pm 1, 0)$. Since $f \sim g$, so $g(x,y) = f(X,Y) = f(\alpha x + \gamma y, \beta x + \delta y)$. Therefore

$$a = a' = g(\pm 1, 0) = f(\pm\alpha, \pm\beta) = f(\pm 1, 0)$$

and so $\beta = 0$ and $\alpha = \pm 1$. Since $\alpha\delta - \beta\gamma = 1$ so $\delta = \pm 1$ and the sign of δ is the same as the sign of α. Since $c = c'$ so $\beta = 0$ and so the only possible substitutions are $g(x,y) = f(x,y)$ or $g(x,y) = f(-x,-y)$. Therefore $b = b'$. □

Therefore each binary quadratic form is equivalent to a unique reduced form.

Definition 5.22. *Let $d < 0$ be an integer. The class number of d, (written $h(d)$) is the number of reduced forms of discriminant d.*

Definition 5.23. *An integer $d \equiv 0, 1$ mod 4 is called a fundamental discriminant if it is not of the form $d = k^2 d'$ for some integer $k > 1$ and $d' \equiv 0, 1$ mod 4.*

5.4 Representations by binary quadratic forms

We study the set of integers represented by a binary quadratic form.

Lemma 5.24. *Let $f = (a, b, c)$ and $n \in \mathbb{Z}$. n is properly represented by f if and only if f is equivalent to a binary quadratic form with first coefficient n.*

Proof. Suppose $f \sim (n, p, q)$ for some p, q then n is represented by (n, p, q) and so represented by f. Conversely, if $f(\alpha, \beta) = n$ where $(\alpha, \beta) = 1$, then there exists $\gamma, \delta \in \mathbb{Z}$ such that $\alpha\delta - \beta\gamma = 1$. Let

$$g(x, y) = f(\alpha x + \gamma y, \beta x + \delta y)$$

and so $g(1, 0) = f(\alpha, \beta) = n$. Therefore $g \sim (n, p, q)$ for some p, q. □

Theorem 5.25. *Let n be a positive integer and $d < 0$ a discriminant. n is properly represented by a binary quadratic form of discriminant d if and only if the congruence*

$$x^2 \equiv d \ mod \ 4n$$

is soluble.

Proof. Suppose n is represented by (a, b, c) with $b^2 - 4ac = d$. By the previous lemma, $(a, b, c) \sim (n, p, q)$ for some p, q and since equivalent forms have the same discriminant, so $p^2 - 4qn = d$. Therefore,

$$p^2 \equiv d \bmod 4n.$$

Conversely, if there exists x such that $x^2 \equiv d \bmod 4n$, then there exists y such that $x^2 = d + 4ny$. Take $f = (n, x, y)$ and so f has discriminant d, and n is represented by f. □

5.5 Exercises

1. Determine all odd positive integers that can be expressed in the form (i) $x^2 + 2y^2$ (ii) $x^2 + 3y^2$ (iii) $x^2 - y^2$.

2. Which primes are represented by $x^2 + 5y^2$? Which primes are represented by $2x^2 + 2xy + 3y^2$.

3. Prove that n and $2n$, where n is any positive integer, have the same number of representations as the sum of two squares.

4. Is there a positive definite binary quadratic form that represents 2 and the primes congruent to 1 or 3 modulo 8, but no other primes? Is there such a form representing the primes congruent to 1 modulo 4 only?

5. (i) Let p be an odd prime. Show that there exist x, y such that

$$x^2 \equiv -1 - y^2 \bmod p.$$

Hence show that there exist x_0, y_0, u_0, v_0 and k such that

$$x_0^2 + y_0^2 + u_0^2 + v_0^2 = kp.$$

(ii) If $x_0^2 + y_0^2 + u_0^2 + v_0^2 = 2mp$, then show that there exist x_1, y_1, u_1, v_1 such that

$$x_1^2 + y_1^2 + u_1^2 + v_1^2 = mp.$$

(iii) If $x_0^2 + y_0^2 + u_0^2 + v_0^2 = kp$ where k is odd, then show that there exist x_1, y_1, u_1, v_1 such that

$$x_1^2 + y_1^2 + u_1^2 + v_1^2 = k'p, \text{ for some } k' < k.$$

You may use the identity

$$\begin{aligned}(x^2 + y^2 + z^2 + w^2)(x'^2 + y'^2 + z'^2 + w'^2) &= (xx' + yy' + zz' + ww')^2 + (xy' - yx' + wz' - zw')^2 \\ &+ (xz' - zx' + yw' - wy')^2 + (xw' - wx' + zy' - yz')^2.\end{aligned}$$

(iv) Hence show that every prime can be written as a sum of four squares.

(v) Finally show that every positive integer can be written as a sum of four squares.

6 Distribution of primes

6.1 The sum $\sum_p p^{-1}$ and the product $\prod_p (1-p^{-1})^{-1}$

Theorem 6.1. *The sum $\sum_p p^{-1}$ and the product $\prod_p (1-p^{-1})^{-1}$ both diverge.*

Proof. Let $S(x) = \sum_{p \le x} p^{-1}$ and $P(x) = \prod_{p \le x}(1-p^{-1})^{-1}$ for $x \ge 2$. We have

$$P(x) = \prod_{p \le x}(1-p^{-1})^{-1} = \prod_{p \le x}\sum_{i=0}^{\infty} p^{-i} \ge \sum_{n=1}^{[x]} n^{-1} \to \infty$$

as $x \to \infty$.

Now using the taylor expansion of $\log(1-t)$ for $|t| < 1$, we have

$$\log P(x) = -\sum_{p \le x}\log(1-p^{-1}) = \sum_{p \le x}\sum_{i=1}^{\infty}\frac{p^{-i}}{i} = S(x) + \sum_{p \le x}\sum_{i=2}^{\infty}\frac{p^{-i}}{i}.$$

For any $p \le x$,

$$\sum_{i=2}^{\infty}\frac{p^{-i}}{i} \le \frac{1}{2}\sum_{i=1}^{\infty} p^{-i} = \frac{1}{2}\frac{1}{p(p-1)}.$$

Therefore,

$$0 \le \log P(x) - S(x) \le \sum_{p \le x}\frac{1}{2}\frac{1}{p(p-1)} \le \sum_{n=1}^{\infty}\frac{1}{2}\frac{1}{n(n-1)} = \frac{1}{2}$$

and so $S(x) \to \infty$ as $x \to \infty$. □

In particular, this gives another proof of the following statement.

Corollary 6.2. *There are infinitely many primes.*

Moreover,

Corollary 6.3. *For each $x \ge 2$, we have*

$$P(x) \ge \log x, \quad S(x) \ge \log\log x - \frac{1}{2}.$$

Proof. We have seen that $P(x) \ge \sum_{n=1}^{[x]} \frac{1}{n}$ and by integral approximation, we have

$$P(x) \ge \sum_{n=1}^{[x]}\frac{1}{n} > \int_1^{[x]}\frac{1}{t}dt = \log([x]+1) > \log x.$$

For each $0 < u < 1$ we have

$$-\log(1-u) - u = \frac{u^2}{2}\left(1 + \frac{u}{\frac{3}{2}} + \cdots\right) < \frac{u^2}{2}(1 + u + u^2 + \cdots) = \frac{u^2}{2(1-u)}.$$

Let $u = \frac{1}{p}$ and sum over all primes $p \le x$, we conclude that

$$0 \le \log P(x) - S(x) \le \frac{1}{2}\sum_{p \le x}\frac{1}{p(p-1)} < \frac{1}{2}\sum_{n=2}^{\infty}\frac{1}{n(n-1)} = \frac{1}{2}$$

and so $S(x) \ge \log\log x - \frac{1}{2}$. □

We will give explicit approximations of $\sum_{p \le x} p^{-1}$ later.

6.2 Legendre's formula

Recall that $\pi(x)$ is the number of primes less than or equal to x. We give a method to compute $\pi(x)$ effectively.

Definition 6.4. *Let p_n be the nth prime. For $x \geq 2, r \geq 1$, define $N_r(x)$ to be the size of*

$$\{n : 1 \leq n \leq x, p_i \nmid n \text{ for all } i \leq r\}.$$

Lemma 6.5. *For each $x \geq 2, r \geq 1$, we have*

$$N_r(x) = [x] - \sum_{i=1}^{r} [x/p_i] + \sum_{i \neq j \leq r} [x/p_i p_j] + \cdots + (-1)^r [x/p_1 \cdots p_r].$$

Proof. Apply inclusion-exclusion formula to compute $[x] - N_r(x)$. □

Corollary 6.6. *Let $r = \pi(\sqrt{x})$. Then*

$$N_r(x) = \pi(x) - \pi(\sqrt{x}) + 1$$

and hence

$$1 + \pi(x) = \pi(\sqrt{x}) + [x] - \sum_{i=1}^{r} [x/p_i] + \sum_{i \neq j \leq r} [x/p_i p_j] + \cdots + (-1)^r [x/p_1 \cdots p_r].$$

Proof. Each composite number in $[2, x]$ must be divisible by some prime $p_1, \ldots, p_r$ where $r = \pi(\sqrt{x})$. Therefore, the set

$$\{n : 1 \leq n \leq x, p_i \nmid n \text{ for all } i \leq r\}$$

contains 1 and the primes bigger than $\sqrt{x}$. So

$$N_r(x) + \pi(\sqrt{x}) = \pi(x) + 1.$$

□

6.3 Bertrand's postulate

Lemma 6.7. *Let $C = \binom{2n}{n}$, then*

$$2n \log 2 - \log(2n+1) \leq \log C \leq 2n \log 2.$$

Proof. Consider $2^{2n} = (1+1)^{2n}$ and the largest term in the binomial expansion of this is $C = \binom{2n}{n}$. Since there are $2n+1$ terms in the expansion,

$$\frac{2^{2n}}{2n+1} \leq C \leq 2^{2n}.$$

Taking logarithm gives the required inequalities. □

Lemma 6.8. *Let $C = \binom{2n}{n}$, then*

$$(\pi(2n) - \pi(n)) \log n \leq \log C \leq \pi(2n) \log(2n).$$

Proof. Let $r(p)$ be the integer such that

$$p^{r(p)} \leq 2n < p^{r(p)+1}.$$

Recall from 2.2, the exponent to which any prime p divides $n!$ is $\sum_{j=1}^{\infty}[n/p^j]$. So the exponent to which p divides C is

$$\sum_{j=1}^{\infty}\left([2n/p^j] - 2[n/p^j]\right) = \sum_{j=1}^{r(p)}\left([2n/p^j] - 2[n/p^j]\right) \leq \sum_{j=1}^{r(p)} 1 = r(p)$$

because $[2n/p^j] - 2[n/p^j] = 0$ or 1 for each j; Indeed, if the fractional part of n/p^j is less than $1/2$ then $[2n/p^j] - 2[n/p^j] = 0$ and $[2n/p^j] - 2[n/p^j] = 1$ otherwise. Since this is true for all $p|2n$, so

$$C = \binom{2n}{n} \leq \prod_{p\leq 2n} p^{r(p)} \leq \prod_{p\leq 2n} 2n = 2n^{\pi(2n)}$$

and so $\log C \leq \pi(2n)\log(2n)$. It is also clear that $p|C$ for each p with $n < p \leq 2n$ and so

$$n^{\pi(2n)-\pi(n)} = \prod_{n<p\leq 2n} n < \prod_{n<p\leq 2n} p|\binom{2n}{n} = C$$

and so $(\pi(2n) - \pi(n))\log n \leq \log C$. □

Theorem 6.9 (**Chebychev's estimate**). *There exist constants $a, b > 0$ such that for all $x \geq 2$, we have*

$$\frac{ax}{\log x} < \pi(x) < \frac{bx}{\log x}.$$

Proof. By the previous two lemmas, we conclude that

$$\pi(2n) \geq (2n\log 2 - \log(2n+1))/\log(2n)$$

and

$$\pi(2n) - \pi(n) \leq 2n\log 2/\log n.$$

The first inequality implies that there exists $a > 0$ such that

$$\pi(x) > \frac{ax}{\log x}$$

and the second inequality implies that there exists $c > 0$ such that

$$\pi(2x) - \pi(x) < \frac{cx}{\log x}.$$

Since $\pi(x) = \sum_{j=1}^{\infty}[\pi(x/2^{j-1}) - \pi(x/2^j)]$ so we estimate $\pi(x/2^{j-1}) - \pi(x/2^j)$ for each j. Replacing x by $x/2^j$ we conclude that for each j,

$$\pi(x/2^{j-1}) - \pi(x/2^j) \leq \frac{cx}{2^j\log(x/2^j)}.$$

If $2^j \leq x^{1/2}$ then $x/2^j \geq x^{1/2}$ and so

$$\pi(x/2^{j-1}) - \pi(x/2^j) \leq \frac{cx}{2^{j-1}\log(x)}.$$

If $2^j > x^{1/2}$ then

$$\pi(x/2^{j-1}) - \pi(x/2^j) < \pi(x/2^{j-1}) < x/2^{j-1} < 2\sqrt{x}.$$

Since there are at most $\frac{\log x}{\log 2}$ non-zero terms, we conclude that

$$\pi(x) \leq \sum_{j=1}^{\log x/\log 2} [\pi(x/2^{j-1}) - \pi(x/2^j)] < \frac{cx}{\log x} \sum_{j=1}^{\infty} \frac{1}{2^{j-1}} + 2\sqrt{x}\frac{\log x}{\log 2} < bx/\log x$$

for some $b > 0$. □

Remark 6.10. *In fact Chebychev showed that one can take $a = 0.9219\ldots$ and $b = 1.1055\ldots$ if $x \geq 30$.*

Corollary 6.11 (Bertrand's postulate). *For all integer x, there exists a prime p such that $x < p \leq 2x$.*

Proof. By the above remark, we have

$$\pi(x) < \frac{bx}{\log x} < \frac{2ax}{\log 2x} < \pi(2x)$$

for $a = 0.92129\ldots, b = 1.1055\ldots$ and $x \geq 30$. Therefore, $\pi(2x) - \pi(x) \geq 1$ and so there exists a prime between x and $2x$. It is easy to check that the theorem holds for $2 \leq x < 30$. □

6.4 Partial summation formula

We give the following theorem in real analysis.

Theorem 6.12 (Partial summation formula). *Let $a_1, \ldots, a_n$ be any real sequence and let $s(x) = \sum_{n \leq x} a_n$. Further, let $f(x)$ be a real function with continuous derivative $f'(x)$ for all real $x > 0$. Then*

$$\sum_{n \leq x} a_n f(n) = s(x)f(x) - \int_1^x s(u)f'(u)du.$$

Proof. By convention we write $s(0) = 0$. Write $a_n = s(n) - s(n-1)$ so we have

$$\begin{aligned}
\sum_{n \leq x} a_n f(n) &= \sum_{n \leq x} (s(n) - s(n-1))f(n) = \sum_{n \leq x} s(n)f(n) - \sum_{n \leq x} s(n-1)f(n) \\
&= \sum_{n \leq x} s(n)f(n) - \sum_{n \leq x-1} s(n)f(n+1) \\
&= \sum_{n \leq x-1} s(n)(f(n) - f(n+1)) + s(x)f([x]).
\end{aligned}$$

Further, since $s(x)$ is constant in any interval $[n, n+1]$, so

$$\sum_{n=1}^{[x]-1} s(n)(f(n) - f(n+1)) = -\sum_{n=1}^{[x]-1} \int_n^{n+1} s(y)f'(y)dy.$$

Finally, write $s(x)f([x]) = \int_{[x]}^x s(y)f'(y)dy + s(x)f(x)$ and so the result follows. □

6.5 Merten's results

We now give explicit approximations of $\sum_{p \leq x} p^{-1}$ and $\prod_p (1 - p^{-1})^{-1}$.

Theorem 6.13. *We have*

$$\sum_{p \leq x} \frac{\log p}{p} = \log x + O(1).$$

Proof. We have

$$\sum_{n\le x}\log n=\log[x]!=\sum_{p\le x}\sum_{j=1}^{\infty}[x/p^j]\log p$$

because the exponent to which a prime p divides $[x]!$ is $\sum_{j=1}^{\infty}[x/p^j]$ by Lemma 2.2. The contribution from the term $j=1$ is

$$\sum_{p\le x}[x/p]\log p=\sum_{p\le x}(x/p)\log p+O(\pi(x)\log x).$$

Since $\pi(x)<bx/\log x$ by Chebychev's inequality, so $O(\pi(x)\log x)=O(x)$. Since

$$\sum_{j=2}^{\infty}\frac{1}{p^j}=\frac{1}{p(p-1)}$$

and so

$$\sum_{p\le x}\sum_{j=2}^{\infty}x\log p\frac{1}{p(p-1)}\le\sum_{2\le n\le x}\frac{\log n}{n(n-1)}\le x\sum_{n=2}^{\infty}\frac{\log n}{n(n-1)}$$

which is $O(x)$. Therefore,

$$\sum_{n\le x}\log n=x\sum_{p\le x}\frac{\log p}{p}+O(x).$$

Finally, it's an easy exercise (see Exercises) that

$$\sum_{n\le x}\log x=x\log x+O(x)$$

and so the result follows. □

Theorem 6.14. *For some constant c we have*

$$S(x)=\sum_{p\le x}\frac{1}{p}=\log\log x+c+O\left(\frac{1}{\log x}\right).$$

Proof. Apply partial summation formula with $f(x)=\frac{1}{\log x}$,

$$a_n=\frac{\log n}{n}\text{ if }n\text{ is a prime }p\text{ and 0 otherwise.}$$

Then $\sum_{n\le x}a_nf(n)=\sum_{p\le x}\frac{1}{p}$. $f(x)$ has continuous derivative only for $x>1$. But $a_1=0$ so the theorem still applies

$$\sum_{2\le n\le x}a_nf(n)=s(x)f(x)-\int_2^x s(y)f'(y)dy.$$

By the previous theorem, we have

$$s(x)=\sum_{p\le x}\frac{\log p}{p}=\log x+r(x)$$

where $r(x)=O(1)$ and so $s(x)f(x)=1+O\left(\frac{1}{\log x}\right)$. Since $f'(y)=-\frac{1}{x(\log x)^2}$, we have

$$-\int_2^x s(y)f'(y)dy=\int_2^x\frac{s(y)}{y(\log y)^2}dy=\int_2^x\frac{dy}{y\log y}+\int_2^x\frac{r(y)}{y(\log y)^2}dy.$$

Since $\int_2^x\frac{dy}{y\log y}=[\log\log x]_2^x$ and

$$\int_2^x\frac{r(y)}{y(\log y)^2}dy=\int_2^{\infty}\frac{r(y)}{y(\log y)^2}dy-\int_x^{\infty}\frac{r(y)}{y(\log y)^2}dy=c+O\left(\frac{1}{\log x}\right)$$

the result follows by taking the constant to be $c+1-\log\log 2$. □

Theorem 6.15. *For some constant $b > 0$, we have*

$$\prod_{p \le x} (1 - p^{-1})^{-1} = b \log x + O(1).$$

Proof. We have

$$\prod_{p \le x} (1 - p^{-1})^{-1} = \prod_{p \le x} \exp(-\log(1 - p^{-1})) = \exp(\sum_{p \le x} -\log(1 - p^{-1})).$$

By using

$$-\sum_{p \le x} \log(1 - p^{-1}) = \sum_{p \le x} \sum_{i=1}^{\infty} \frac{p^{-i}}{i} = S(x) + \sum_{p \le x} r(p)$$

where $r(p) = \sum_{i=2}^{\infty} \frac{p^{-i}}{i}$. Since

$$r(p) \le \frac{1}{2} \sum_{i=2}^{\infty} p^{-i} \le \frac{1}{2} \frac{1}{p(p-1)}$$

so

$$\sum_{p > x} r(p) \le \sum_{n > x} r(n) \le \sum_{n > x} \frac{1}{n(n-1)} = O\left(\frac{1}{x}\right).$$

Therefore,

$$\sum_{p \le x} r(p) = c' + O\left(\frac{1}{x}\right)$$

where $c' = \sum_p r(p)$ is a constant. Therefore, by the previous theorem

$$S(x) + \sum_p r(p) = \log \log x + c + O(1/\log x) + c' + O(1/x) = \log \log x + b + O(1/\log x)$$

for some $b > 0$. The theorem follows by taking exponentials:

$$P(x) = \exp(S(x) + \sum_p r(p)) = e^b \log x \exp(O(1/\log x))$$

and use the fact $\exp(O(1/\log x)) = 1 + O(1/\log x)$. □

6.6 Riemann zeta function

Recall from chapter 2 that the Riemann zeta function is $\zeta(s) = \sum_n n^{-s}$ where $s \in \mathbb{C}$. We again write $s = \sigma + it$ where $\sigma, t \in \mathbb{R}$.

Lemma 6.16. *For $\sigma > 1$, the series $\sum_{n=1}^{\infty} n^{-s}$ converges absolutely.*

Proof. $|n^{-s}| = |\exp(-s \log n)| = |\exp(-\sigma \log n - it \log n)|$. Since $|e^{i\theta}| = 1$ for all $\theta \in \mathbb{R}$, so $|n^{-s}| = |\exp(-\sigma \log n)| = n^{-\sigma}$. Therefore

$$\sum_{n=1}^{\infty} |n^{-s}| = \sum_{n=1}^{\infty} n^{-\sigma} < \infty.$$

□

Proposition 6.17 (Euler's product). *For $\sigma > 1$, we have*

$$\zeta(s) = \prod_p (1 - p^{-s})^{-1}.$$

Proof. Let $T(N,s) = \prod_{p\le N}(1-p^{-s})^{-1}$ and we will show that $\zeta(s) - T(N,s) \to 0$ as $N \to \infty$ for any s with $\sigma > 1$. We have

$$T(N,s) = \prod_{p\le N}(1-p^{-s})^{-1} = \prod_{p\le N}\sum_{i=0}^{\infty} p^{-is}.$$

Since $T(N,s)$ consists of terms of the form n^{-s} for $n \le N$, so

$$|\zeta(s) - T(N,s)| \le \sum_{n\ge N+1} |n^{-s}| = \sum_{n\ge N+1} n^{-\sigma} \le \int_N^{\infty} \frac{dy}{y^{\sigma}} = \frac{1}{\sigma-1}N^{1-\sigma}.$$

Therefore $|\zeta(s) - T(N,s)| \to 0$ as $N \to \infty$ when $\sigma > 1$. □

Corollary 6.18. *For $\sigma > 1$, $\zeta(s) \ne 0$.*

Proof. By using Euler's product, we have

$$\prod_{p\le x}(1-p^{-s})\zeta(s) = \prod_{p>x}(1-p^{-s})^{-1} = \prod_{p>x}(1+\sum_{i=1}^{\infty} p^{-is})$$

and so

$$\left|\prod_{p\le x}(1-p^{-s})\zeta(s)\right| \le 1 - \sum_{n>x} n^{-\sigma}.$$

For each $\sigma > 1$, the sum $\sum_{n=1}^{\infty} n^{-\sigma}$ converges and so by taking x large enough, we conclude that $1 - \sum_{n>x} n^{-\sigma} \le \frac{1}{2}$ and so $\zeta(s) \ne 0$. □

Theorem 6.19. *$\zeta(s) - \frac{1}{s-1}$ has an analytic continuation to $\sigma > 0$.*

Proof. Writing $1 = n - (n-1)$ we have

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

Then

$$\zeta(s) = s\sum_{n=1}^{\infty}\int_n^{n+1} nx^{-s-1}dx = s\int_1^{\infty}[x]x^{-s-1}dx$$

because $n = [x]$ for $x \in [n, n+1]$. But $[x] = x - \{x\}$ where $\{x\}$ is the fractional part of x and so

$$\zeta(s) = s\int_1^{\infty}(x - \{x\})x^{-s-1} = \frac{s}{s-1} - s\int_1^{\infty}\{x\}x^{-s-1}dx.$$

Since $|\{x\}| \le 1$ for all x, the integral above converges for $\sigma > 0$ and so

$$\zeta(s) - \frac{1}{s-1} = 1 - s\int_1^{\infty}\{x\}x^{-s-1}dx$$

converges to an analytic function on $\sigma > 0$. □

Using a similar method (and integration by part) one can show

Theorem 6.20. *$\zeta(s) - \frac{1}{s-1}$ has an analytic continuation to $\sigma > -1$.*

6.7 Gamma function and the functional equation

Let $s = \sigma + it$ as usual.

Definition 6.21. *For $\sigma > 0$, the Gamma function is defined by*

$$\Gamma(s) = \int_0^\infty e^{-x} x^{s-1} dx.$$

Using integration by part we conclude that

Lemma 6.22. *$s\Gamma = \Gamma(s+1)$ for all s. In particular, for each natural number $s > 0$, we have $\Gamma(s) = s!$.*

Lemma 6.23. *$\int_0^\infty \frac{\sin y}{y^{s+1}} dy = -\sin(\frac{1}{2}s\pi)\Gamma(-s)$ for all $\sigma < 0$.*

Proof. Write $\sin y = \frac{1}{2i}(e^{iy} - e^{-iy})$ and we will compute $\int_0^\infty e^{\pm iy} y^{s+1}$.

Let C be the boundary of the region

$$\{z \in \mathbb{C} : \Re(z) \geq 0, \Im(z) \geq 0, |z| \leq R\, |z| \geq r\}$$

where $r < R$. Then

$$\int_C \frac{e^{iz}}{z^{s+1}} dz = \int_0^R \frac{e^{iy}}{y^{s+1}} dy - i \int_r^R \frac{e^{-t}}{(it)^{s+1}} dt + \int_0^{\frac{\pi}{2}} \frac{e^{iRe^{i\theta}}}{(Re^{i\theta})^{s+1}} iRe^{i\theta} d\theta - \int_0^{\frac{\pi}{2}} \frac{e^{ire^{i\theta}}}{(re^{i\theta})^{s+1}} ire^{i\theta} d\theta.$$

When $R \to \infty$, we have $int_0^{\frac{\pi}{2}} \frac{e^{iRe^{i\theta}}}{(Re^{i\theta})^{s+1}} iRe^{i\theta} d\theta \to 0$ by Jordan's lemma. When $r \to 0$, $e^{ire^{i\theta}} = 1 + O(r)$ and so

$$\int_0^{\frac{\pi}{2}} \frac{e^{ire^{i\theta}}}{(re^{i\theta})^{s+1}} ire^{i\theta} d\theta = \int_0^{\frac{\pi}{2}} \frac{1 + O(r)}{(re^{i\theta})^s} id\theta \to 0$$

because $\sigma < 0$. Therefore, we can write

$$\int_C \frac{e^{iz}}{z^{s+1}} = \int_r^R \frac{e^{iy}}{y^{s+1}} dy - i \int_0^R \frac{e^{-t}}{(it)^{s+1}} dt + f(r, R)$$

where $f(r, R) \to 0$ as $r \to 0, R \to \infty$.

Similarly, by considering the contour C' which is the reflection of C about the origin, we have

$$\int_{C'} \frac{e^{-iz}}{z^{s+1}} dz = \int_0^R \frac{e^{-iy}}{y^{s+1}} dy + i \int_0^R \frac{e^{-t}}{(-it)^{s+1}} dt + g(r, R)$$

where $g(r, R) \to 0$ as $r \to 0, R \to \infty$.

By Cauchy's integral theorem, we take the difference of the above integrals and let $r \to 0, R \to \infty$, so

$$\int_0^\infty \frac{\sin y}{y^{s+1}} dy = \frac{1}{2}\left(\int_0^\infty \frac{e^{-t}}{(it)^{s+1}} dt + \int_0^\infty \frac{e^{-t}}{(-it)^{s+1}} dt\right) = \frac{1}{2i}(i^{-s} - (-i)^{-s})\Gamma(-s) = -\sin(\frac{1}{2}s\pi)\Gamma(-s).$$

□

The following lemma is an exercise of integration and we omit the proof.

Lemma 6.24. *For all $s \in \mathbb{C}$,*

$$\Gamma(\frac{1}{2} - \frac{1}{2}s)/\Gamma(\frac{1}{2}s) = \pi^{-1/2} 2^s \sin(\frac{1}{2}s\pi)\Gamma(1 - s).$$

Theorem 6.25 (The functional equation). *Let $\Xi(s) = \pi^{-\frac{1}{2}s}\Gamma(s)\zeta(s)$. Then $\Xi(s) = \Xi(1-s)$.*

Proof. Assume $-1 < \sigma < 0$. Recall that we can write

$$\zeta(s) = s\int_1^\infty [x]x^{-s-1}dx$$

and now we write $f(x) = [x] - x + \frac{1}{2}$ so that

$$\zeta(s) = s\int_1^\infty f(x)x^{-s-1} + s\int_1^\infty (x - \frac{1}{2})x^{-s-1}dx = s\int_1^\infty f(x)x^{-s-1}dx + \frac{1}{s-1} + \frac{1}{2}.$$

If $\sigma < 0$, then

$$s\int_0^1 f(x)x^{-s-1}dx = s\int_0^1 (-x + \frac{1}{2})x^{-s-1}dx = \frac{1}{s-1} + \frac{1}{2}$$

and so

$$\zeta(s) = s\int_0^\infty f(x)x^{-s-1}dx.$$

Using the Fourier expansion

$$f(x) = \sum_{n=1}^\infty \frac{\sin(2n\pi x)}{n\pi}$$

so we have

$$\zeta(s) = \frac{s}{\pi}\sum_{n=1}^\infty \frac{1}{n}\int_0^\infty \sin(2n\pi x)x^{-s-1}dx = \frac{s}{\pi}\sum_{n=1}^\infty \frac{(2\pi n)^s}{n}\int_0^\infty \frac{\sin y}{y^{s+1}}dy.$$

By Lemma 6.23 we conclude that

$$\zeta(s) = -\frac{s}{\pi}(2\pi)^s\Gamma(-s)\sin(\frac{1}{2}s\pi)\sum_{n=1}^\infty n^{s-1} = -\frac{s}{\pi}(2\pi)^s\Gamma(-s)\sin(\frac{1}{2}s\pi)\zeta(1-s).$$

But $-s\Gamma(-s) = \Gamma(1-s)$ so we have

$$\zeta(s) = 2^s\pi^{s-1}\sin(\frac{1}{2}s\pi)\Gamma(1-s)\zeta(1-s).$$

Finally, since $\Xi(s) = \pi^{-\frac{1}{2}s}\Gamma(\frac{1}{2}s)\zeta(s)$, we conclude $\Xi(s) = \Xi(1-s)$ by using Lemma 6.24.

We have proved the theorem for $-1 < \sigma < 0$. Since $\Xi(1-s)$ is analytic for $\sigma < 0$, therefore the equation above implies that $\zeta(s)$ extends to an analytic function for $\sigma \leq -1$ and so $\zeta(s)$ extends to a meromorphic function on $\mathbb{C}$. Therefore it is true for all s. □

Remark 6.26. *The functional equation shows that $\zeta(s)$ is analytic throughout the complex plane except for a simple pole at $s = 1$ with residue 1. It also shows that $\zeta(s) \neq 0$ for $\sigma < 0$ by using Corollary 6.18.*

6.8 Riemann Hypothesis

There are many interesting results on the Riemann zeta function. For example, it is known that $\zeta(s)$ has infinitely many zeroes on the line $\sigma = \frac{1}{2}$ (Hardy). At least 10^9 zeroes (ordered by t) satisfy $\sigma = \frac{1}{2}$. The Riemann hypothesis asserts that in fact all zeroes of ζ lie on the line $\sigma = \frac{1}{2}$.

Definition 6.27. *The logarithmic integral function is defined by*

$$li(x) = \int_2^x \frac{dt}{\log t}.$$

It is well-known that the Riemann hypothesis is equivalent to the assertion $\pi(x) = \mathrm{li}(x) + O(\sqrt{x}\log x)$. It is knownt hat

$$\pi(x) = \mathrm{li}(x) + O(xe^{-c\sqrt{\log x}})$$

for some constant $c > 0$.

Another assertion known to be equivalent to the Riemann hypothesis is

$$\sum_{n\le x} \mu(n) = O(x^{\frac{1}{2}+\epsilon})$$

for any $\epsilon > 0$.

Proposition 6.28. *$li(x) \sim \frac{x}{\log x}$ as $x \to \infty$.*

Proof. Using integration by part, we have

$$\mathrm{li}(x) = \int_2^x \frac{dt}{\log t} = \left[\frac{t}{\log t}\right]_2^x + \int_2^x \frac{dt}{(\log t)^2} = \frac{x}{\log x} - \frac{2}{\log 2} + \int_2^x \frac{dt}{(\log t)^2}.$$

But

$$\int_2^x \frac{dt}{(\log t)^2} = \int_2^{\sqrt{x}} \frac{dt}{(\log t)^2} + \int_{\sqrt{x}}^x \frac{dt}{(\log t)^2} \le \frac{\sqrt{x}}{(\log 2)^2} + \frac{x}{(\log\sqrt{x})^2}.$$

Therefore $\mathrm{li}(x) \sim \frac{x}{\log x}$ as $x \to \infty$. □

6.9 Bernoulli numbers

We will study the values $\zeta(2t)$ where t is a positive integer.

Definition 6.29. *The nth Bernoulli number, B_n is defined by*

$$B_0 = 1, \quad (m+1)B_m = -\sum_{j=0}^{m-1} \binom{m+1}{j} B_j \text{ for all } m > 0.$$

For example, $2B_1 = -1, 3B_2 = -3B_1 - 1, \ldots$.

Lemma 6.30. *If we expand $\frac{t}{e^t-1}$ as a power series in t, then*

$$\frac{t}{e^t-1} = \sum_{n=0}^{\infty} \frac{B_n t^n}{n!}.$$

Proof. Let $\frac{t}{e^t-1} = \sum_{n=0}^{\infty} \frac{b_n t^n}{n!}$. Using $e^t = \sum_{m=0}^{\infty} \frac{t^m}{m!}$, so

$$t = \sum_{m=1}^{\infty} \frac{t^m}{m!} \sum_{n=0}^{\infty} \frac{b_n t^n}{n!}.$$

Compare coefficients of t on both sides, we conclude that $b_0 = 1$. Now compare the coefficients of t^{k+1} on both sides for $k > 0$, we conclude that

$$\sum_{j=0}^{k+1} \binom{k+1}{j} \frac{1}{(k+1)!} b_j = 0.$$

Therefore $b_k(k+1) = -\sum_{j=0}^{k} \binom{k+1}{j} b_j$ and so $b_k = B_k$ for each k. □

Corollary 6.31. *$B_{2n+1} = 0$ for each $n > 0$.*

Proof. Since $B_0 = 1$ and $B_1 = -\frac{1}{2}$, so

$$\frac{t}{e^t - 1} + \frac{t}{2} = 1 + \sum_{n=2}^{\infty} \frac{B_n t^n}{n!}.$$

But

$$\frac{t}{e^t - 1} + \frac{t}{2} = \frac{t(e^t + 1)}{2(e^t - 1)}$$

which is an even function of t. Therefore $B_{2n+1} = 0$. □

The following theorem gives a method to compute $\zeta(2t)$.

Theorem 6.32 (Euler). *Let t be a positive integer. Then*

$$2(2t)!\zeta(2t) = (-1)^{t+1}(2\pi)^{2t} B_{2t}.$$

Proof. We quote a standard result from analysis

$$\sin x = x \prod_{n=1}^{\infty} \left(1 - \frac{x^2}{n^2\pi^2}\right)$$

and so

$$\log \sin x = \log x + \sum_{n=1}^{\infty} \log\left(1 - \frac{x^2}{n^2\pi^2}\right).$$

Differentiating both sides we have

$$\cot x = \frac{1}{x} - 2\sum_{n=1}^{\infty} \frac{x}{n^2\pi^2 - x^2}$$

and so

$$x \cot x = 1 - 2\sum_{n=1}^{\infty} \frac{x^2}{n^2\pi^2 - x^2}.$$

Now for each n, write

$$\frac{x^2}{n^2\pi^2 - x^2} = \frac{x^2}{n^2\pi^2} \frac{1}{1 - (x/n\pi)^2} = \sum_{t=1}^{\infty} \left(\frac{x}{n\pi}\right)^{2t}.$$

Therefore,

$$x \cot x = 1 - 2\sum_{n=1}^{\infty}\sum_{t=1}^{\infty} \left(\frac{x}{n\pi}\right)^{2t} = 1 - 2\sum_{t=1}^{\infty} \zeta(2t) \left(\frac{x}{\pi}\right)^{2t}.$$

Now write $\cot x = i\frac{e^{ix}+e^{-ix}}{e^{ix}-e^{-ix}}$, so

$$x \cot x = ix\frac{e^{2ix} + 1}{e^{2ix} - 1} = ix + \frac{2ix}{e^{2ix} - 1} = ix + \sum_{t=0}^{\infty} \frac{B_t (2ix)^t}{t!} = 1 + \sum_{t=2}^{\infty} \frac{B_t (2ix)^t}{t!}$$

by Lemma 6.30. Now compare both expressions of $x \cot x$, we conclude that

$$-\frac{2\zeta(2t)}{\pi^{2t}} = (-1)^t 2^{2t} \frac{B_{2t}}{(2t)!}.$$

□

As a simple application, we substitute $t = 1$ into the identity above so we have

Corollary 6.33. $\zeta(2) = \frac{\pi^2}{6}$.

6.10 Exercises

1. Define the von Mangoldt function as

$$\Lambda(n) = \begin{cases} \log p & \text{if } n \text{ is a power of prime } p \\ 0 & \text{otherwise} \end{cases}$$

(i) Compute $\sum_{d|n} \Lambda(d)$. (ii) Show that

$$\sum_{n=0}^{\infty} \frac{\Lambda(n)}{n^s} = -\frac{\zeta'(s)}{\zeta(s)}.$$

2. Define the Liouville function as $\lambda(n) = (-1)^{\omega(n)}$ where $\omega(n)$ is the number of (not necessarily distinct) prime factors of n. Show that

$$\sum_{n=1}^{\infty} \frac{\lambda(n)}{n^s} = \frac{\zeta(2s)}{\zeta(s)}.$$

3. Show that every integer $N > 6$ can be written as a sum of distinct primes.

4. By considering the cases $k < n$ and $k \geq n$ separately, show that

$$\frac{1}{n} + \frac{1}{n+1} + \cdots + \frac{1}{n+k} = m$$

is not soluble for any integer $n > 1$.

5. (i) Show that $\sum_{n \leq x} \log n = x \log x - x + O(\log x)$.

(ii) Show also that $\sum_{n \leq x} \log^2 n = x \log^2 x - 2x \log x + 2x + O(\log^2 x)$.

6. (i) Show that the number of primes q that divides an integer $n > 3$ and exceed $\log n$ is at most $\frac{\log n}{\log \log n}$.

(ii) By considering the product $\prod_{q|n}(1 - q^{-1})$, deduce that

$$\phi(n) > \frac{cn}{\log \log n}$$

for some constant c.

7. Use the functional equation to calculate $\zeta(0)$.

8. Show that

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

Show further that if $\frac{\pi(x) \log x}{x}$ tends to a limit as $x \to \infty$, then the limit must be 1.

9. Show that $\zeta(-2n) = 0$ where n is a positive integer.

10. Let

$$f(t) = \sum_{n=0}^{\infty} \frac{a_n t^n}{n!} \text{ and } g(t) = \sum_{n=0}^{\infty} \frac{b_n t^n}{n!}.$$

We say f is integral if $a_n \in \mathbb{Z}$ for all n. For each $m \geq 2$, we say $f \equiv g \bmod m$ if $a_n \equiv b_n \bmod m$ for all n.

(i) Suppose f is integral and $f(0) = 0$, then $\frac{f^m}{m!}$ is integral.

(ii) Deduce that if $m > 4$ is a composite number, then

$$(e^t - 1)^{m-1} \equiv 0 \bmod m$$

and

$$(e^t - 1)^3 \equiv 2 \sum_{k=1}^{\infty} \frac{t^{2k+1}}{(2k+1)!} \bmod 4.$$

If p is an odd prime, show that

$$(e^t - 1)^{p-1} \equiv -\sum_{k=1}^{\infty} \frac{t^{kp-k}}{(kp-k)!} \bmod p.$$

(iii) Write $t = \log(1 + (e^t - 1))$ and expand $\frac{t}{e^t - 1}$ as a power series in $e^t - 1$. Show that

$$\sum_{p-1|2n} \frac{1}{p} + B_{2n}$$

is an integer (where the sum is taken over all primes p such that $p - 1|2n$).

(iv) Deduce that the denominator of B_{2n} is divisible by 6.

7 Continued fraction

The continued fraction algorithm systematically produce the best rational approximation to a given real number.

7.1 Dirichlet's theorem

We begin by introducing a simple result in diophantine approximation.

Theorem 7.1 (Dirichlet's theorem). *For any $\theta \in \mathbb{R}$ and any integer $Q > 1$, there exist integers p, q with $0 < q < Q$ such that*

$$|q\theta - p| \leq \frac{1}{Q}.$$

Proof. Consider the numbers $0, 1, \{k\theta\}$ where $k = 1, 2, \ldots, Q-1$ where $\{k\theta\}$ is the fractional part of $k\theta$. These numbers are between 0 and 1 and there are $Q+1$ numbers in total. So if we divide $[0, 1]$ into Q intervals with equal size, then two of the above numbers must be in the same interval, and hence the difference of them is less than $1/Q$. Write $\{k\theta\} = k\theta - a_k$ for some integer a_k and so there exist p, q such that

$$|q\theta - p| \leq \frac{1}{Q}.$$

□

Corollary 7.2. *For any $\theta, Q \in \mathbb{R}$, there exist integers p, q with $0 < q < Q$ such that*

$$|p\theta - q| < \frac{1}{Q}.$$

Proof. Consider $[Q] + 1$ and repeat the above proof. □

7.2 Convergents

Fix $\theta \in \mathbb{R}_{>0}$. Intuitively we want to write

$$\theta = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \cdots}}.$$

Definition 7.3. *Let $\theta_0 = \theta$. For each $i \geq 0$, define $a_i = [\theta_i]$. If $a_i = \theta_i$ then stop; otherwise let $\theta_{i+1} = \frac{1}{\theta_i - a_i}$. The numbers $a_0, a_1, \ldots$ are called partial quotients and the numbers $\theta_0, \ldots$ are called the complete quotients. For each $n \geq 0$ we write*

$$[a_0, a_1, \ldots, a_n] = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\cdots + \frac{1}{a_n}}}}.$$

We say the continued fraction of θ is finite if there exists n and $a_0, \ldots, a_n$ such that $\theta = [a_0, \ldots, a_n]$; otherwise we say the continued fraction of θ is infinite.

Lemma 7.4. *The continued fraction of θ is finite if and only if $\theta \in \mathbb{Q}$.*

Proof. Suppose the continued fraction of θ is finite, then clearly θ is rational. Conversely, if $\theta = \frac{a}{b}$, $a, b \in \mathbb{Z}_{>0}$. Run the Euclidean algorithm for a, b and so we have

$$a = a_0 b + r_1, \quad b = a_1 r_1 + r_2, \cdots, r_{n-1} = a_n r_n.$$

Then $\theta = \frac{a}{b} = a_0 + \frac{r_1}{b}$ and so

$$\theta_1 = \frac{b}{r_1} = a_1 + \frac{r_1}{r_2}.$$

Since $r_{n-1} = a_n r_n$ so eventually this stops and so we obtain a finite continued fraction. □

Definition 7.5. *The convergents* $\frac{p_n}{q_n}$ *of* θ *are defined by*

$$p_0 = a_0, \quad p_1 = a_0 a_1 + 1, \quad p_n = a_n p_{n-1} + p_{n-2}, \text{ for all } n \geq 2$$

and

$$q_0 = 1, \quad q_1 = a_1, \quad q_n = a_n q_{n-1} + q_{n-2}, \text{ for all } n \geq 2.$$

Remark 7.6. $(p_n)_{n=1}^{\infty}, (q_n)_{n=1}^{\infty}$ *are strictly increasing sequences and so* $p_n, q_n \to \infty$ *as* $n \to \infty$.

Lemma 7.7. *(i) Let* $\beta \in \mathbb{R}$ *and* $n \geq 2$*, we have*

$$\frac{\beta p_{n-1} + p_{n-2}}{\beta q_{n-1} + q_{n-2}} = [a_0, \ldots, a_{n-1}, \beta].$$

(ii) For each $n \geq 0$*,* $[a_0, \ldots, a_n] = \frac{p_n}{q_n}$.

Proof. (i) Induction on n. If $n = 2$, then

$$[a_0, a_1, \beta] = a_0 + \frac{1}{a_1 + \frac{1}{\beta}} = \frac{(a_0 a_1 + 1)\beta + a_0}{a_1 \beta + 1} = \frac{\beta p_1 + p_0}{\beta q_1 + q_0}.$$

Suppose this is true for n, then for $n+1$, observe that

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

and so by inductive hypothesis

$$[a_0, \ldots, a_n, \beta] = \frac{(a_n + \frac{1}{\beta})p_{n-1} + p_{n-2}}{(a_n + \frac{1}{\beta})q_{n-1} + q_{n-2}} = \frac{a_n p_{n-1} + p_{n-2} + \frac{1}{\beta} p_{n-1}}{a_n q_{n-1} + q_{n-2} + \frac{1}{\beta} q_{n-1}} = \frac{\beta p_n + p_{n-1}}{\beta q_n + q_{n-1}}.$$

(ii) For $n \leq 1$ we check that $[a_0] = \frac{p_0}{q_0}$ and $[a_0, a_1] = \frac{a_0 a_1 + 1}{a_1} = \frac{p_1}{q_1}$. For $n \geq 2$, let $\beta = a_n$ in (i) and we have

$$[a_0, \ldots, a_n] = \frac{a_n p_{n-1} + p_{n-2}}{a_n q_{n-1} + q_{n-2}} = \frac{p_n}{q_n}.$$

□

Lemma 7.8. *(i) For each* $n \geq 1$ *we have*

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}.$$

(ii) For each $n \geq 2$ *we have*

$$p_n q_{n-2} - p_{n-2} q_n = (-1)^n a_n.$$

(iii) p_n, q_n *are coprime for all* n.

Proof. (i) Induction on n. When $n = 1$ we have

$$p_1 q_0 - p_0 q_1 = (a_0 a_1 + 1) - a_0 a_1 = 1.$$

Suppose this is true for n, then

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

(ii) We have

$$p_n q_{n-2} - p_{n-2} q_n = (a_n p_{n-1} + p_{n-2}) q_{n-2} - p_{n-2}(a_n q_{n-1} + q_{n-2}) = a_n (p_{n-1} q_{n-2} - p_{n-2} q_{n-1}) = (-1)^n a_n.$$

(iii) use (i). □

Corollary 7.9. $\lim_{n\to\infty} \frac{p_n}{q_n}$ *exists.*

Proof. By (i) of the previous lemma we have

$$\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n-1}}{q_n q_{n-1}} \to 0$$

as $n \to \infty$. By (ii) of the previous lemma we have

$$\frac{p_n}{q_n} - \frac{p_{n-2}}{q_{n-2}} = \frac{(-1)^n a_n}{q_n q_{n-2}}.$$

Therefore, if $c_n = \frac{p_n}{q_n}$, then

$$c_0 < c_2 < \cdots < c_3 < c_1$$

and since $c_n - c_{n-1} \to 0$ as $n \to \infty$ so c_n tends to a limit. □

Theorem 7.10. *Let $\theta \in \mathbb{R}\backslash\mathbb{Q}$, then for all $n \geq 0$, we have*

$$\left|\theta - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}} < \frac{1}{q_n^2}.$$

Proof. Since $\theta \notin \mathbb{Q}$ so the continued fraction is infinite. By definition of continued fraction, we have

$$\theta = [a_0, a_1, \ldots, a_n, \theta_{n+1}]$$

and $a_{n+1} = [\theta_{n+1}]$. Then we have

$$\theta - \frac{p_n}{q_n} = \frac{\theta_{n+1}p_n + p_{n-1}}{\theta_{n+1}q_n + q_{n-1}} - \frac{p_n}{q_n} = \frac{p_{n-1}q_n - p_n q_{n-1}}{q_n(\theta_{n+1}q_n + q_{n-1})} = \frac{(-1)^n}{q_n(\theta_{n+1}q_n + q_{n-1})}.$$

Since $\theta_{n+1}q_n + q_{n-1} > a_{n+1}q_n + q_{n-1} = q_{n+1}$ so the result follows. □

Corollary 7.11. $\lim_{n\to\infty} \frac{p_n}{q_n} = \theta$.

Proof. The above theorem shows that

$$\lim_{n\to\infty} \frac{p_n}{q_n} - \theta = 0$$

because $q_n \to \infty$ as $n \to \infty$. □

Theorem 7.12. *Let $\theta \in \mathbb{R}\backslash\mathbb{Q}$ and $p, q \in \mathbb{Z}$ with $0 < q < q_{n+1}$. Then*

$$|q\theta - p| \geq |q_n\theta - p_n|.$$

Proof. Since $p_{n+1}q_n - p_n q_{n+1} = \pm 1$ for all n and so there exist $u, v \in \mathbb{Z}$ such that

$$p = up_n + vp_{n+1}, \quad q = uq_n + vq_{n+1}$$

because

$$\begin{pmatrix} p_{n+1} & p_n \\ q_{n+1} & q_n \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}).$$

If $v = 0$ then

$$|q\theta - p| = u|q_n\theta - p_n| \geq |q_n\theta - p_n|.$$

Suppose $v \neq 0$. Since $0 < q < q_{n+1}$, so $u \neq 0$ and u, v have opposite signs. But $q_n\theta - p_n$ and $q_{n+1}\theta - p_{n+1}$ have opposite sign as in the proof of 7.10, so $u(q_n\theta - p_n)$ and $v(q_{n+1}\theta - p_{n+1})$ have the same sign. Therefore

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

□

Corollary 7.13. *If $p, q \in \mathbb{Z}$, $q > 0$ and*

$$|\theta - \frac{p}{q}| \geq |\theta - \frac{p_n}{q_n}|,$$

then $q > q_n$.

Proof. Suppose $q \leq q_n < q_{n+1}$, then by the previous theorem

$$|\theta - \frac{p}{q}| \geq \frac{q_n}{q}|\theta - \frac{p_n}{q_n}| \geq |\theta - \frac{p_n}{q_n}|$$

which is a contradiction. □

Theorem 7.14. *Let $\theta \in \mathbb{R}\backslash\mathbb{Q}$. (i) At least one of any two successive convergents satisfy*

$$|\theta - \frac{p}{q}| < \frac{1}{2q^2}.$$

(ii) Conversely, if $p, q \in \mathbb{Z}$ with $q > 0$ and

$$|\theta - \frac{p}{q}| < \frac{1}{2q^2},$$

then $\frac{p}{q} = \frac{p_n}{q_n}$ for some n.

Proof. (i) Since $\theta - \frac{p_n}{q_n}$ and $\theta - \frac{p_{n+1}}{q_{n+1}}$ have opposite signs. So

$$\left|\theta - \frac{p_n}{q_n}\right| + \left|\theta - \frac{p_{n+1}}{q_{n+1}}\right| = \left|\frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}}\right| \frac{1}{q_n q_{n+1}}$$

by Lemma 7.8. Since $q_n^2 - q_{n+1}^2 \geq 2q_n q_{n+1}$, so

$$\left|\theta - \frac{p_n}{q_n}\right| \leq \frac{1}{2}\left(\frac{1}{q_n^2} + \frac{1}{q_{n+1}^2}\right)$$

and so the result follows.

(ii)Assume $\left|\theta - \frac{p}{q}\right| < \frac{1}{2q^2}$. Since $q_0 = 1$ and $q_n \to \infty$, there exists n such that $q_n \leq q < q_{n+1}$. Then

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

Since $q_n < q_{n+1}$, by Theorem 7.12, we have

$$|q\theta - p| \geq |q_n\theta - p_n|$$

and so

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

Since $q_n \leq q$, we have $\left|\frac{p}{q} - \frac{p_n}{q_n}\right| < \frac{1}{qq_n}$. Finally, we have

$$\left|\frac{p}{q} - \frac{p_n}{q_n}\right| = \left|\frac{pq_n - qp_n}{qq_n}\right|$$

and so if this is not zero, then it is at least $\frac{1}{qq_n}$ because the numerator is an integer. This gives a contradiction and so $\frac{p}{q} = \frac{p_n}{q_n}$. □

7.3 Period

We give an example to compute the partial quotients of θ.

Example 7.15. *$\theta = \sqrt{14}$. Then $a_0 = 3$ and $\theta_1 = \frac{1}{\sqrt{14}-3} = \frac{\sqrt{14}+3}{5}$. So $a_1 = 1$ and $\theta_2 = \frac{5}{\sqrt{14}-2} = \frac{\sqrt{14}+2}{2}$. Then $a_2 = 2$ and so $\theta_3 = \frac{2}{\sqrt{14}-2} = \frac{\sqrt{14}+2}{5}$. Then $a_3 = 1$ and so $\theta_4 = \sqrt{14}+3$. Finally, $a_4 = 6$ and so $\theta_5 = \frac{\sqrt{14}+3}{5} = \theta_1$. Since $\theta_5 = \theta_1$ so $a_5 = a_1$ etc. and so we have*

$$\theta_{i+4} = \theta_i, \quad a_{i+4} = a_i$$

for all $i \geq 1$.

We have seen that the continued fraction of $\sqrt{14}$ is 'periodic' and so we wonder if this is true in general.

Definition 7.16. *A continued fraction is called eventually periodic if it is of the form*

$$[a_0, a_1, \ldots, a_m, \overline{a_{m+1}, \ldots, a_{m+n-1}}]$$

and purely periodic if $m = 0$.

Definition 7.17. *ϕ is said to be a quadratic irrational if ϕ is a root of $ax^2 + bx + c = 0$ for some $a, b, c, \in \mathbb{Z}$ and $\phi \notin \mathbb{Q}$.*

Lemma 7.18. *Let θ be eventually periodic. Then there exist integers a, b, c, d such that $\frac{a\alpha+b}{c\alpha+d}$ is purely periodic.*

Proof. Suppose ϕ is eventually periodic and

$$\phi = [a_0, a_1, \ldots, a_m, \overline{a_{m+1}, \ldots, a_{m+n-1}}].$$

Let $\theta_{m+1} = [\overline{a_{m+1}, \ldots, a_{m+n-1}}]$ which is purely periodic. Since $a_0, \ldots, a_m$ are integers, so there exist integers a, b, c, d such that $\frac{a\theta+b}{c\theta+d} = \theta_{m+1}$. □

Theorem 7.19 (Lagrange). *Let $\theta \in \mathbb{R}$. Then θ is a quadratic irrational if and only if the continued fraction of θ is eventually periodic.*

Proof. Suppose θ is periodic. By the previous lemma, take $a, b, c, d \in \mathbb{Z}$ so that $\alpha = \frac{a\theta+b}{c\theta+d}$ is purely periodic. Then

$$\alpha = [\overline{a_0, a_1, \ldots, a_m}] = [a_0, \ldots, a_m, \alpha] = \frac{\alpha p_m + p_{m-1}}{\alpha q_m + q_{m-1}}.$$

Therefore α satisfies a quadratic polynomial and since α has infinite continued fraction so $\alpha \notin \mathbb{Q}$. Then θ satisfies a quadratic equation.

Conversely, assume α is a root of $ax^2+bx+c = 0$. Let $f(x, y) = ax^2+bxy+cy^2$. Then $f(\theta, 1) = 0$. Write

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

Then $f(p_n\theta_{n+1} + p_{n-1}, q_n\theta_{n+1} + q_{n-1}) = 0$. So θ_{n+1} is a root of $A_nx^2 + B_nx + C_n = 0$ for some $A_n, B_n, C_n \in \mathbb{Z}$. Explicitly, we have

$$A_n = ap_n^2+bp_nq_n+cq_n^2, \quad B_n = 2ap_np_{n-1}+bp_{n-1}q_n+bp_nq_{n-1}+2cq_nq_{n-1}, \quad C_n = ap_{n-1}^2+bp_{n-1}q_{n-1}+cq_{n-1}^2$$

and so

$$A_n = f(p_n, q_n), \quad C_n = f(p_{n-1}, q_{n-1}), \quad B^2 - 4AC = b^2 - 4ac$$

because $p_nq_{n-1} - q_np_{n-1} = \pm 1$.

Since $f(\theta, 1) = 0$, so

$$f\left(\frac{p_n}{q_n}, 1\right) = f\left(\frac{p_n}{q_n}, 1\right) - f(\theta, 1) = a\left(\left(\frac{p_n}{q_n}\right)^2 - \theta^2\right) + b\left(\frac{p_n}{q_n} - \theta\right) = \left(\frac{ap_n}{q_n} + a\theta + b\right)\left(\frac{p_n}{q_n} - \theta\right).$$

As $n \to \infty$, $a\frac{p_n}{q_n} + a\theta + b \to 2a\theta + b$ and so it is bounded above by some constant c. Since

$$\left|\frac{p_n}{q_n} - \theta\right| < \frac{1}{q_n^2}$$

by Theorem 7.10. So $f\left(\frac{p_n}{q_n}, 1\right) < \frac{c}{q_n^2}$ and so $f(p_n, q_n) < c$ for all n. This means that the coefficients A_n, C_n are bounded. Since $B_n^2 - 4A_nC_n = b^2 - 4ac$ is constant, so there are only finitely many triples (A_n, B_n, C_n) for all n. Therefore, there exists $n \neq m$ such that $(A_n, B_n, C_n) = (A_m, B_m, C_m)$ and so $\theta_{m+1} = \theta_{n+1}$. □

7.4 Pell's equation

We study the integer solutions of $x^2 - dy^2 = 1$ where $d > 0$ is a square-free integer. The trivial solutions are $(x, y) = (\pm 1, 0)$. It suffices to study the solutions x, y with $x, y > 0$.

Lemma 7.20. *Suppose $x, y \in \mathbb{Z}_{>0}$ satisfy $x^2 - dy^2 = 1$. Then $\frac{x}{y}$ is a convergent of $\sqrt{d}$.*

Proof. $1 = x^2 - dy^2 = (x - \sqrt{d}y)(x + \sqrt{d}y)$ and since $x + \sqrt{d}y > 0$, so $x - \sqrt{d}y > 0$. Therefore

$$0 < x - \sqrt{d}y = \frac{1}{x + \sqrt{d}y} < \frac{1}{2\sqrt{d}y} < \frac{1}{2y}$$

and so $\left|\frac{x}{y} - \sqrt{d}\right| < \frac{1}{2y^2}$. Then apply Theorem 7.14 (ii). □

We leave the following lemma as an exercise.

Lemma 7.21. *Let θ be a quadratic irrational with conjugate θ' (which has the same quadratic minimal polynomial as θ). Then θ has purely periodic continued fraction if and only if $\theta > 1$ and $-1 < \theta' < 0$.*

Corollary 7.22. *Let $d > 0$ be a square free integer. Then*

$$\sqrt{d} = [a_0, \overline{a_1, \ldots, a_n}].$$

Proof. Consider $\sqrt{d} = [a_0, \theta_1]$. Then $\theta_1 = \frac{1}{\sqrt{d} - a_0} > 0$ and the conjugate

$$0 > \theta_1' = \frac{1}{-\sqrt{d} - a_0} > -1$$

and so by the previous lemma we conclude that θ_1 is purely periodic. □

Theorem 7.23. *Let $d \in \mathbb{Z}_{>0}$ which is square free. Then $x^2 - dy^2 = 1$ has a non-trivial solution.*

Proof. Write $\sqrt{d} = [a_0, \theta_1]$ where θ_1 is purely periodic. Since $\sqrt{d} = a_0 + \frac{1}{\theta_1}$ and so $\theta_1 = \frac{1}{\sqrt{d} - a_0}$. Let

$$\theta_1 = [\overline{a_1, \ldots, a_n}]$$

so we have

$$\sqrt{d} = \frac{\theta_1 p_n + p_{n-1}}{\theta_1 q_n + q_{n-1}} = \frac{p_n + p_{n-1}(\sqrt{d} - a_0)}{q_n + q_{n-1}(\sqrt{d} - a_0)}.$$

This shows that

$$q_{n-1}d + (q_n - a_0 q_{n-1})\sqrt{d} = (p_n - a_0 p_{n-1}) + p_{n-1}\sqrt{d}.$$

Since $\sqrt{d} \notin \mathbb{Q}$, so we must have

$$q_{n-1}d = p_n - a_0 p_{n-1} \text{ and } q_n - a_0 q_{n-1} = p_{n-1}.$$

Therefore,

$$p_{n-1}^2 - dq_{n-1}^2 = p_{n-1}q_n - a_0 q_{n-1}p_{n-1} - (p_n q_{n-1} - a_0 p_{n-1}q_{n-1}) = (-1)^n.$$

So we get solution (p_{n-1}, q_{n-1}) is a solution if n is even and (p_{2n-1}, q_{2n-1}) is a solution if n is odd. □

Remark 7.24. *The above proof also shows that $x^2 - dy^2 = -1$ has a solution when the period of d is odd.*

Corollary 7.25. *Let $d > 0$ be a square free integer and $G = \{x + y\sqrt{d} : x, y \in \mathbb{Z}, x^2 - dy^2 = 1\}$. Then (i) G is a subgroup of $\mathbb{R}^\times$. In particular, the set of solutions to $x^2 - dy^2$ is a group isomorphic to G*

(ii) For any $0 < a < b$, $G \cap [a, b]$ is finite.

(iii) $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$.

Proof. (i) It is easy to see that G is closed under multiplication, and the inverse of $x+\sqrt{d}y$ is $x-\sqrt{d}y$. Therefore G is a subgroup of $\mathbb{R}^\times$. The map $(x, y) \mapsto x + \sqrt{d}y$ gives a bijection between the set of solutions to $x^2 - dy^2 = 1$ and G. Define the group operation on the set of solutions by the group operation of G.

(ii) If $a < x + \sqrt{d}y < b$ then using $x - \sqrt{d}y = \frac{1}{x+\sqrt{d}y}$ we have

$$\frac{1}{b} < x - \sqrt{d}y < \frac{1}{a}.$$

If $y > 0$ then $\frac{1}{b} < x < b$ then there are only finitely many integers x and so there are only finitely many y because $a < x + \sqrt{d}y < b$. If $y < 0$ then $a < x < \frac{1}{a}$ then again we only have finitely many x and hence finitely many y.

(iii) Since there is a non-trivial solution to $x^2 - dy^2 = 1$ with $x, y > 0$, so by (ii) we take the solution x, y with $x + \sqrt{d}y$ smallest and $x + \sqrt{d}y > 1$ (let $a = 1$ and keep increasing b until we have a solution). Let $u + \sqrt{d}v > 1$ such that $u^2 - dv^2 = 1$. Then there exists n such that

$$(x + \sqrt{d}y)^n \leq u + \sqrt{d}y < (x + \sqrt{d}y)^{n+1}$$

and so

$$1 \leq (u + \sqrt{d}y)(x - \sqrt{d}y)^n < x + \sqrt{d}y.$$

By the choice of $x + \sqrt{d}y$, we conclude that

$$(u + \sqrt{d}y)(x - \sqrt{d}y)^n = 1$$

and so $u + \sqrt{d}y = (x + \sqrt{d}y)^n$. This means that every $u + \sqrt{d}v > 1$ with $u^2 - dv^2 = 1$ is a power of $x + \sqrt{d}y$.

Therefore, every $0 < u - \sqrt{d}v < 1$ is a (negative) power of $x + \sqrt{d}y$. So $G = \{\pm(x + \sqrt{d}y)^n : n \in \mathbb{Z}\}$ and so

$$G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}, \quad \pm(x + \sqrt{d})^n \mapsto (\pm, n).$$

□

Remark 7.26. *The above theorem helps to generate solutions to $x^2 - dy^2 = 1$. For example, if x, y is a solution then so is $x' = x^2 + dy^2, y' = 2xy$ because*

$$x' + \sqrt{d}y' = (x + \sqrt{d}y)^2 = x^2 + dy^2 + 2xy\sqrt{d}.$$

7.5 A set of real numbers modulo 1

Let θ be an irrational number. We will study the distribution of $\{\{n\theta\} : n \in \mathbb{N}\}$ where $\{n\theta\}$ is the fractional part of $n\theta$. Intuitively we would expect that these fractional parts are uniformly distributed in $[0, 1]$. We now formally define uniform distribution.

Definition 7.27. *Let $R = \{a_1, a_2, \ldots\}$ be a set of real numbers in the interval $[0, 1]$ and let $0 \leq \beta_1 < \beta_2 \leq 1$. Let $T(n, \beta_1, \beta_2)$ be the size of*

$$\{a_i : i \leq n, \beta_1 \leq a_i \leq \beta_2\}.$$

R is said to be uniformly distributed in the unit interval $[0, 1]$ if

$$\lim_{n\to\infty} \frac{T(n, \beta_1, \beta_2)}{n} = \beta_2 - \beta_1$$

for all β_1, β_2 with $0 \leq \beta_1 < \beta_2 \leq 1$.

We leave the following theorem as an exercise.

Theorem 7.28 (Hurwitz). *There are infinitely many convergents of θ such that*

$$\left|\theta - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2\sqrt{5}}.$$

We firstly prove a theorem which shows that the the set $\{\{i\theta\} : i \in \mathbb{N}\}$ is dense in $[0, 1]$.

Theorem 7.29. *Let θ be an irrational number and $\beta \in \mathbb{R}$. Then there exist infinitely many pairs of integers x and y such that*

$$|x\theta - y - \beta| < \frac{3}{x}.$$

In particular, take $\beta \in [0, 1]$ and then $y = [x\theta]$, so we have infinitely many x such that $|\{x\theta\} - \beta| < \frac{3}{x}$.

Proof. By Hurwitz theorem, there exist infinitely many positive integers a, b with $(a, b) = 1$ such that

$$\theta = \frac{a}{b} + \frac{\gamma}{b^2}, \text{ where } |\gamma| \leq 1.$$

For each b, let c be the integer such that $|c - b\beta|$ is smallest and so

$$\beta = \frac{c}{b} + \frac{\delta}{2b}, \text{ where } |\delta| \leq 1.$$

Since $(a, b) = 1$ there exist integers x, y such that

$$ax - by = c$$

and we can take x with $b \leq 2x < 3b$ because we can replace x by $x + kb$ and y by $y + ka$. Therefore

$$|x\theta - y - \beta| = \left|\frac{xa}{b} + \frac{x\gamma}{b^2} - y - \frac{c}{b} - \frac{\delta}{2b}\right| = \left|\frac{x\gamma}{b^2} - \frac{\delta}{2b}\right| < \frac{x}{b^2} + \frac{1}{2b} < \frac{3}{x}$$

because $b > \frac{2x}{3}$. Since we have infinitely many such b and so we have infinitely many x and y. $\square$

We now prove the set is uniformly distributed.

Lemma 7.30. *Let a, b be integers such that $b > 0$, $(a, b) = 1$ and*

$$\theta = \frac{a}{b} + \frac{\delta}{b^2}, \qquad \text{where } |\delta| < 1.$$

For each j, let $J_j = \{jb + k : k = 0, 1, \ldots, b-1\}$ and

$$K_j = \{\{i\theta\} : i \in J_j\}.$$

Then

$$K_j = \left\{ \left\{ \frac{k + \gamma_j}{b} \right\} : k = 0, 1, \ldots, b-1 \right\}.$$

Proof. We have

$$\alpha(jb + k) = \left(\frac{a}{b} + \frac{\delta}{b^2} \right) (jb + k) = ja + \frac{ka + j\delta}{b} + \frac{k\delta}{b^2}.$$

Since ja is an integer, so

$$\{\alpha(jb + k)\} = \left\{ \frac{ka + j\delta}{b} + \frac{k\delta}{b} \right\} = \left\{ \frac{ka + [j\delta]}{b} + \frac{\gamma_j}{b} \right\}$$

where

$$\gamma = \frac{k\delta}{b} + \{j\delta\}.$$

Since $k < b$, so $|\gamma| < 2$. Since k ranges over a complete system of residues modulo b, $ka + [jb]$ ranges over a complete system modulo b for all because $(a, b) = 1$. Therefore,

$$K_j = \left\{ \left\{ \frac{k + \gamma}{b} \right\} : k = 0, 1, \ldots, b-1 \right\}.$$

□

Lemma 7.31. *For each subinterval $[\beta_1, \beta_2] \subset [0, 1]$ and sufficiently large b so that we can choose integers v, w to satisfy*

$$v - 1 < b\beta_1 \leq v < w \leq b\beta_2 < w + 1,$$

if W_j is the size of

$$\{x \in K_j : x \in [\beta_1, \beta_2]\},$$

then $w - v - 2 \leq W_j \leq w - v + 2$.

Proof. $[\beta_1, \beta_2] \supset [v/b, w/b]$. So W_j is bounded below by the number of elements in K_j in the interval $[v/b, w/b]$. By the previous lemma,

$$K_j = \left\{ \left\{ \frac{k + \gamma}{b} \right\} : k = 0, 1, \ldots, b-1 \right\}$$

and so W_j is bounded below by the number of integers $0 \leq k < b$ such that

$$v \leq k + \gamma \leq w$$

and so $W_j \geq w - v - 2$ because $|\gamma| < 2$. Similarly, W_j is bounded above by the number of integers $0 \leq k < b$ such that

$$v - 1 < k + \gamma < w + 1$$

and so $W_j \leq w - v + 2$. □

Theorem 7.32. *Let θ be an irrational number. Then the set*

$$R = \{\{i\theta\} : i \in \mathbb{N}\}$$

is uniformly distributed in $[0, 1]$.

Proof. By Hurwitz theorem, there exist infinitely many integers a, b with $(a, b) = 1$ and $b > 0$ such that

$$\theta = \frac{a}{b} + \frac{\delta}{b^2}, \qquad \text{where } |\delta| < 1.$$

For each subinterval $[\beta_1, \beta_2] \subset [0, 1]$, and $\epsilon > 0$, pick b large enough so that $b > \frac{1}{\epsilon}$ and we can choose integers v, w to satisfy

$$v - 1 < b\beta_1 \leq v < w \leq b\beta_2 < w + 1.$$

Then pick $n > b$ such that $\frac{b(\beta_2 - \beta_1)}{n} < \epsilon$ and so we have

$$\frac{1}{n} \leq \frac{w - v}{n} < \epsilon$$

and so $1 = O(n\epsilon)$.

Write $n = rb + s$ where $0 \leq s < b$. By definition of W_j in the previous lemma, we have

$$\sum_{j=0}^{r-1} W_j \leq T(n, \beta_1, \beta_2) \leq \sum_{j=0}^{r} W_j$$

and so by the previous lemma,

$$r(w - v - 2) \leq T(n, \beta_1, \beta_2) \leq (r + 1)(w - v + 2).$$

Since $r = \frac{n-s}{b}$ and

$$w - v < b(\beta_2 - \beta_1) \leq w - v + 2$$

we conclude that

$$\frac{n - s}{b}(b(\beta_2 - \beta_1) - 4) \leq T(n, \beta_1, \beta_2) \leq \frac{n - s + b}{b}(b(\beta_2 - \beta_1) + 2).$$

But $s < b$ and so we have the following approximation

$$n(\beta_2 - \beta_1) + O(n\epsilon) \leq T(n, \beta_1, \beta_2) \leq n(\beta_2 - \beta_1) + O(n\epsilon)$$

and so

$$\left| \frac{T(n, \beta_1, \beta_2)}{n} - (\beta_2 - \beta_) \right| < O(\epsilon).$$

Now let $\epsilon \to 0$ and so $n \to \infty$, then

$$\lim_{n \to \infty} \frac{T(n, \beta_1, \beta_2)}{n} = \beta_2 - \beta_1.$$

□

7.6 Exercises

1. (i) Let d and m be positive integers such that d is not a square and such that $m \leq \sqrt{d}$. Prove that if x and y are positive integers satisfying $x^2 - dy^2 = m$ then x/y is a convergent of $\sqrt{d}$.

   (ii) Let d and m be positive integers such that d is not a cube. If x, y are integers satisfying $x^3 - dy^3 = m$ and $3d^{\frac{2}{3}}y > 8m$, then x/y is a convergent of $d^{\frac{1}{3}}$.

2. Let d be a positive integer that is not a square. Let $\theta_n, p_n/q_n$ be the complete quotients and convergents for $\theta = \sqrt{d}$. Show that for all $n \geq 1$ we have

$$p_{n-1} - q_{n-1}\sqrt{d} = (-1)^n / \prod_{i=1}^{n} \theta_i.$$

3. Let u_n be the nth Fibonacci number, i.e.

$$u_1 = 1, u_2 = 1 \text{ and } u_{n+2} = u_{n+1} + u_n, n \geq 0.$$

   Let $\alpha = \frac{1+\sqrt{5}}{2}$ and let p_n/q_n be the nth convergent. (i) Show that $\frac{p_n}{q_n} = \frac{u_{n+2}}{u_{n+1}}$. (ii) It is known that if $\alpha' = \frac{1-\sqrt{5}}{2}$, then

$$u_n = \frac{\alpha^n - \alpha'^n}{\sqrt{5}}.$$

   Use this fact to show that $p|u_{p-1}$ if $p \equiv \pm 1 \bmod 5$ and $p|u_{p+1}$ if $p \equiv \pm 2 \bmod 5$.

4. Write $\beta_n = \frac{q_{n-1}}{q_{n-2}}$ where $\frac{p_n}{q_n}$ are convergents of θ. Let θ_n be the nth complete quotient. Show that if $\theta_n + \beta_n \leq \sqrt{5}$ for three consecutive convergents, then $\beta_n + \frac{1}{\beta_n} < \sqrt{5}$. Prove Hurwitz theorem.

5. Assume that θ is a quadratic irrational which satisfies $\theta > 1$ and $-1 < \theta' < 0$ where θ' is the conjugate of θ. Show that (i) $-1 < \theta'_n < 0$ where

$$\theta = [a_0, a_1, \ldots, a_{n-1}, \theta_n].$$

   (ii) $a_n = \left[\frac{-1}{\theta'_{n+1}}\right]$.

   (iii) θ has purely periodic continued fraction.

   (iv) Show further that if

$$\theta = [\overline{a_0, \ldots, a_n}]$$

   then

$$-\frac{1}{\theta'} = [\overline{a_n, a_{n-1}, \ldots, a_1, a_0}].$$

6. Assume $\theta > 1$ is irrational and has purely periodic continued fraction with convergents $\frac{p_n}{q_n}$. Show that for some suitably chosen n, $f(\theta) = 0$ where

$$f(x) = x^2 q_{n-1} + x(q_{n-1} - p_{n-1}) - p_{n-2}.$$

   Hence show that $-1 < \theta' < 0$. Together with the previous question, we conclude that an irrational number $\theta > 1$ has purely periodic continued fraction if and only if $-1 < \theta' < 0$, which proves Lemma 7.21.

7. Show that there exist infinitely many n such that $\sum_{i=1}^{n} i$ is a square.

8. Let d be a rational number which is not a square. Then

$$\sqrt{d} = [a_0, \overline{a_1, a_2, \ldots, a_{n-1}, 2a_0}]$$

for some $n \geq 1$ where $a_{n-1} = a_i$ for $1 \leq i < n$. Conversely, any continued fraction of this form is the square root of a rational number.

8 Primality testing and factoring

We discuss the following questions in this chapter: (i) Given a large N, can we effectively determine whether N is prime? (ii) Given a large composite integer N, can we find a non-trivial factor of N? We may assume N is odd in both questions.

For (i) the trial division up to $\sqrt{N}$ is not effective. However, small factors are easily found by trial division. For (ii) we can sometimes use Fermat Euler theorem to determine whether N is a prime, for if N is a prime, then

$$a^{N-1} \equiv 1 \bmod N$$

for all $(a, N) = 1$. For example, 9 is not a prime because

$$2^8 = (16)^2 \equiv (-2)^2 \equiv 4 \bmod 9.$$

8.1 Fermat pseudoprime

Definition 8.1. *We say b is a base for N if $(b, N) = 1$. We usually take $b \in \{1, 2, \ldots, N-1\}$.*

Definition 8.2. *An odd composite number N is a (Fermat) pseudoprime to the base b if $b^{N-1} \equiv 1$ mod N.*

Theorem 8.3. *For every integer $b > 1$, there exist infinitely many pseudoprimes to the base b.*

Proof. Let p be an odd prime which does not divide any of $b, b+1, b-1$ and let $N = \frac{b^{2p}-1}{b^2-1}$. It is clear that N is an integer. Moreover,

$$N = \frac{b^p - 1}{b-1}\frac{b^p+1}{b+1}$$

and since p is odd so N is a product of two integers, and so it is composite.

$N - 1 = \frac{b^{2p}-b^2}{b^2-1}$. By Fermat Euler, $b^p \equiv b \bmod p$ and so $b^{2p} \equiv b^2 \bmod p$. So $N - 1 = kp$ for some k. But

$$N - 1 = b^2\frac{b^{p-1}-1}{b-1}\frac{b^{p-1}+1}{b+1} = b^2(1 + p + \cdots + b^{p-2})(b^{p-2} - b^{p-1} + \cdots)$$

and so N is even because $1 + p + \cdots + b^{p-2}$ is even. Therefore k is even and so $k = 2m$ for some m.

On the other hand, $b^{2p} - 1 = (b^2 - 1)N$ and so $b^{2p} \equiv 1 \bmod N$. So

$$b^{N-1} = b^{2mp} = (b^{2p})^m \equiv 1 \bmod N.$$

□

Definition 8.4. *Let N be an composite number. N is called a Carmichael number if N is a pseudoprime to all bases b.*

A result of Alford, Granville and Pomerance of 1992 gives the existence of infinitely many Carmichael numbers.

8.2 Euler pseudoprime

Recall that Euler's criterion states that

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \bmod p.$$

Definition 8.5. *An odd composite integer N is called an Euler pseudoprime to the base b if*

$$b^{\frac{N-1}{2}} \equiv \left(\frac{b}{N}\right) \ mod\ N.$$

Note that $b^{N-1} \equiv 1$ mod N and so every Euler pseudoprime is a Fermat pseudoprime.

Using Euler's criterion we have the following conclusion.

Proposition 8.6. *The set*

$$\{b \in (\mathbb{Z}/N\mathbb{Z})^\times : N \text{ is an Euler pseudoprime to } b\}$$

is a subgroup of $(\mathbb{Z}N/\mathbb{Z})^\times$.

Theorem 8.7. *Let N be an odd composite integer. Then there exists b such that N is not an Euler pseudoprime to the base b.*

Proof. If N is square free, then $N = pm$ where $(p, m) = 1$, p is a prime and $m \geq 3$. Pick u such that $\left(\frac{u}{p}\right) = -1$. Then take b such that

$$b \equiv u \bmod p, \quad b \equiv 1 \bmod m.$$

Then $\left(\frac{b}{N}\right) = -1$. If $b^{\frac{N-1}{2}} \equiv -1 \bmod N$ then $b^{\frac{N-1}{2}} \equiv -1 \bmod m$. But $b \equiv 1 \bmod m$.

If N is not square free, then $N = p^r m$ where $r \geq 2$ and $(p, m) = 1$. So $(1+p)^{N-1} \equiv 1 + (N-1)p$ mod p^2 and so

$$(1+p)^{N-1} \not\equiv 1 \bmod p^r.$$

Take b such that

$$b \equiv 1 + p \bmod p^2, \quad b \equiv 1 \bmod m.$$

Then $(b, N) = 1$ and $b^{N-1} \not\equiv 1 \bmod N$. So N is not a Fermat pseudoprime to the base b and hence not an Euler pseudoprime to the base b. □

Using the above theorem, we have the following primality test: Given an odd integer N, test whether

$$b^{\frac{N-1}{2}} \equiv \left(\frac{b}{N}\right) \bmod N$$

for several randomly chosen b. If any of these fail then N is composite.

8.3 Strong pseudoprime

Definition 8.8. *Let N be an odd integer and write $N - 1 = 2^s t$ where $s \geq 1$ and t is odd. N is called a strong pseudoprime prime to the base b if either $b^t \equiv 1$ mod N or*

$$b^{2^r t} \equiv -1 \ mod\ N, \qquad \text{for some } 0 \leq r < s.$$

Remark 8.9. *If N is a prime, then N is a strong pseudoprime to the base b for all bases b. Indeed, either $b^t \equiv 1$ mod N, or $b^t \not\equiv 1$ mod N. By Fermat Euler,*

$$b^{2^s t} \equiv b^{N-1} \equiv 1 \ mod\ N.$$

Let k be the largest integer such that $b^{2^k t} \not\equiv 1$ mod N. Then

$$b^{2^{k+1} t} \equiv 1 \ mod\ N.$$

But N is prime and so $b^{2^k t} \equiv -1$ mod N.

We now give a theorem which gives an upper bound of

$$S(N) = \{b : 1 \leq b < N, (b, N) = 1, N \text{ is a strong pseudoprime to the base } b\}.$$

Theorem 8.10 (Mercer). *Assume N is an odd integer and $N > 9$. Then $|S(N)| \leq \frac{1}{4}\phi(N)$.*

The idea is to estimate the size of the following set.

Definition 8.11. *For each N, let $u(N)$ be the largest integer such that $2^{u(N)}$ divides $p-1$ for every prime factor p of N and let*

$$U(N) = \{b : 1 \leq b < N, (b, N) = 1, b^{2^{u(N)-1}t} \equiv \pm 1 \ mod \ N\}.$$

Lemma 8.12. *$S(N) \subset U(N)$ and so $|S(N)| \leq |U(N)|$.*

Proof. Let $b \in S(N)$. So either (i) $b^t \equiv 1 \bmod N$ or (ii) there exists $0 \leq r < s$ such that

$$b^{2^r t} \equiv -1 \bmod N.$$

If (i) holds then clearly $b \in U(N)$. Assume (ii) holds. Take $p|N$ and let k_p be the order of b in $(\mathbb{Z}/p\mathbb{Z})^\times$. Since

$$b^{2^{r+1}t} = (b^{2^r t})^2 \equiv 1 \bmod N$$

and so $b^{2^{r+1}t} \equiv 1 \bmod p$. So $k_p | 2^{r+1}t$. But $k_p \nmid 2^r t$, so k_p must be divisible by 2^{r+1}. On the other hand, $k_p | p-1$ by Fermat Euler. Therefore,

$$2^{r+1} | k_p | p-1$$

and so $r+1 \leq u(N)$.

Suppose $r+1 = u(N)$, then $u(N) - 1 = r$ and so $b^{2^{u(N)-1}t} \equiv -1 \bmod N$. Suppose $r+1 < u(N)$, then $u(N) - 1 \geq r+1$ and so $b^{2^{u(N)-1}} \equiv 1 \bmod N$. So $b \in U(N)$. □

Theorem 8.13. *For each N, let $w(N)$ be the number of distinct prime factors of N. Write $N - 1 = 2^s t$, then*

$$|U(N)| = 2 \cdot 2^{(u(N)-1)w(N)} \prod_{p|N} (t, p-1).$$

Proof. Let $m = 2^{u(N)-1}$ and we count the number of solutions of

$$x^m \equiv \pm 1 \bmod N.$$

Let $N = p_1^{a_1} \cdots p_k^{a_k}, a_i \geq 1$ and so $w(N) = k$.

We firstly count the number of solutions of $x^m \equiv 1 \bmod N$ by counting the number of solutions of $x^m \equiv 1 \bmod p_i^{a_i}$ for each i. Since $(\mathbb{Z}/p_i^{a_i}\mathbb{Z})^\times$ is a cyclic group of order $p_i^{a_i-1}(p_i - 1)$, so we have d solutions where $d = (m, p_i^{a_i-1}(p_i - 1))$. Since $p_i | N$ and $(2, N) = (t, N) = 1$, so $(m, p_i^{a_i-1}) = 1$. Therefore, $d = (m, p_i - 1)$. But $2^{u(N)} | p_i - 1$ and so

$$(m, p_i - 1) = 2^{u(N)-1}(t, p_i - 1).$$

Since this is true for each i, then by Chinese remainder theorem, we have

$$2^{(u(N)-1)w(N)} \prod_{p|N} (t, p-1)$$

solutions for $x^m \equiv 1 \bmod N$.

Now we count the number of solutions of $x^m \equiv -1 \bmod N$. We again consider the number of solutions of $x^m \equiv -1 \bmod p_i^{a_i}$ for each i. The number of solutions for

$$x^{2m} \equiv 1 \bmod p_i^{a_i}$$

is

$$(2m, p_i^{a_i-1}(p-1)) = (2m, p_i - 1) = 2^{u(N)}(t, p-1)$$

by using the same argument above. Therefore the number of solutions of

$$x^m \equiv -1 \bmod p_i^{a_i}$$

is $2^{u(N)-1}(t, p-1)$ because $(x^m - 1, x^m + 1) = 1$ and so $x^{2m} \equiv 1 \bmod p_i^{a_i}$ if and only if

$$x^m \equiv \pm 1 \bmod p_i^{a_i}.$$

Therefore the number of solutions of $x^m \equiv \pm 1 \bmod N$ is $2 \cdot 2^{(u(N)-1)w(N)} \prod_{p|N}(t, p-1)$. □

We now prove the result of Mercer.

Proof. Let $\delta(N) = \frac{\phi(N)}{|U(N)|}$ and we shall prove $\delta(N) \geq 4$. Then $\frac{\phi(N)}{|S(N)|} \geq 4$ because we have shown that $|S(N)| \leq |U(N)|$. Let $N = \prod_i p_i^{a_i-1}(p_i - 1)$ and so

$$\phi(N) = \prod_i p_i^{a_i-1}(p_i - 1).$$

Then by the previous theorem, we have

$$\delta(N) = \frac{1}{2} \prod_i \frac{p_i^{a_i}(p_i - 1)}{2^{u(N)-1}(t, p-1)}.$$

It is clear that $\frac{p-1}{2^{u(N)-1}(t,p-1)} \geq 2$. If $i \geq 2$ and $a_i \geq 2$ for some i, then

$$\delta(N) \geq \frac{1}{2} 2^2 \cdot 3 = 6.$$

Similarly if $i \geq 3$ then

$$\delta(N) \geq \frac{1}{2} 2^3 = 4.$$

So the theorem follows in these cases.

It remains to check the theorem for the following cases: (i) $i = 2, a_i = 1$ for all i, i.e. $N = pq$, $p < q$. (ii) $i = 1$. In the first case, we have

$$\delta(N) = \frac{1}{2} \frac{(p-1)(q-1)}{2^{2u(N)-2}(t, p-1)(t, q-1)}$$

where $2^{u(N)} | p-1, q-1$. If $2^{u(N)+1} | q-1$ then

$$\frac{q-1}{2^{u(N)-1}(t, q-1)} \geq 4$$

and so the result follows. If not, since

$$N - 1 = pq - 1 \equiv p - 1 \bmod q - 1$$

so $2^{u(N)} | N - 1$. But $q - 1 \nmid N - 1$, so there must be some odd factor $r | q - 1$ such that $r \nmid N - 1$ because $2^{u(N)+1} \nmid q - 1$. Then

$$\frac{q-1}{(t, q-1)} \geq r \geq 3$$

and so $\delta(N) \geq 6$.

In the second case, since N is composite, we have $N = p^j, j \geq 2$. Then

$$\delta(N) = \frac{p^{j-1}(p-1)}{2^{u(N)}(t, p-1)} \geq p^{j-1}.$$

p is odd and so $p \geq 3$. If $p = 3$ then $j \geq 3$ because we assume $N > 9$ and so $\delta(N) \geq 9$. If $p > 3$ then $\delta(N) \geq 4$.

□

Remark 8.14. *Mercer's result shows that the strong pseudoprime test is much more efficient than the Euler pseudoprime test.*

Finally, we show that every strong pseudoprime is an Euler pseudoprime.

Lemma 8.15. *Let N be a composite number and $N - 1 = 2^s t$. Suppose*

$$b^{2^r t} \equiv -1 \text{ mod } N, \text{ for some } 0 \leq r < s - 1.$$

Then for each prime $p|N$, if $p - 1 = 2^{s'} t'$, then $s' \geq s$ and

$$\left(\frac{b}{p}\right) = -1 \text{ if } s' = r + 1, \quad \text{and } \left(\frac{b}{p}\right) = 1 \text{ if } s' > r + 1.$$

Proof. The fact $s' \geq r + 1$ can be deduced by a similar argument as in the proof of Lemma 8.12: Indeed if k_p is the order of b in $(\mathbb{Z}/p\mathbb{Z})^\times$, we have shown that

$$2^{r+1} | k_p | p - 1$$

and so $r + 1 \leq s'$.

Since t' is odd, we have

$$b^{2^r tt'} \equiv -1 \text{ mod } p.$$

By Euler's criterion, we have

$$\left(\frac{b}{p}\right)^t \equiv b^{(p-1)t/2} = b^{2^{s'-1}tt'} \text{ mod } p.$$

If $s' = r + 1$ then $\left(\frac{b}{p}\right)^t \equiv -1 \text{ mod } p$ and if $s' > r + 1$ then $\left(\frac{b}{p}\right)^t \equiv 1 \text{ mod } p$. The result follows because t is odd. □

Theorem 8.16. *Let N be a composite number. If N is a strong pseudoprime to the base b, then N is an Euler pseudoprime to the base b.*

Proof. Let $N - 1 = 2^s t$. Suppose $b^t \equiv 1 \text{ mod } N$, then

$$1 \equiv b^{\frac{N-1}{2}} \equiv b^t \equiv \left(\frac{b^t}{N}\right) = \left(\frac{b}{N}\right)^t \text{ mod } N.$$

Since t is odd, so $b^{\frac{N-1}{2}} \equiv \left(\frac{b}{N}\right)^t \text{ mod } N$.

Now suppose $b^{2^{s-1}t} \equiv -1 \text{ mod } N$. Since $\frac{N-1}{2} = 2^{s-1}t$, so we need to show that $\left(\frac{b}{N}\right) = -1$. By the previous lemma, if $N = \prod_{p|N} p$ (not necessarily distinct), then

$$\left(\frac{b}{N}\right) = \prod_{p|N} \left(\frac{b}{p}\right) = (-1)^k$$

where k is the number of p with $s' = s$. For those p with $s' \geq s+1$, we have $p \equiv 1 \bmod 2^{s+1}$ and for those p with $s' = s$ we have

$$p \equiv 1 + 2^s t' \equiv 1 + 2^s \bmod 2^{s+1}$$

because t' is odd. Similarly, $N \equiv 1 + 2^s t \bmod 2^{s+1}$. So

$$1 + 2^s \equiv N \equiv \prod_{p|N} p \equiv (1+2^s)^k \equiv 1 + k2^s \bmod 2^{s+1}$$

and so k must be odd. This shows that $\left(\frac{b}{N}\right) = -1$.

Finally, suppose $b^{2^r t} \equiv -1 \bmod N$ where $0 \leq r < s-1$. Then $\frac{N-1}{2} = 2^{s-1}t$ and so

$$b^{\frac{N-1}{2}} \equiv 1 \bmod N.$$

So we need to show that $\left(\frac{b}{N}\right) = 1$. By the previous lemma, if $N = \prod_{p|N} p$ (not necessarily distinct), then

$$\left(\frac{b}{N}\right) = \prod_{p|N} \left(\frac{b}{p}\right) = (-1)^k$$

where k is the number of p with $s' = r+1$.

For those p with $s' \geq r+2$, we have $p \equiv 1 \bmod 2^{r+2}$ and for those p with $s' = r+1$, we have

$$p \equiv 1 + 2^{r+1}t' \equiv 1 + 2^{r+1} \bmod 2^{r+2}$$

because t' is odd. Since $r \leq s-2$, so $r+2 \leq s$ and we have

$$N = 1 + 2^s t \equiv 1 \bmod 2^{r+2}.$$

So

$$1 \equiv N \equiv \prod_{p|N} p \equiv (1+2^{r+1})^k \equiv 1 + k2^{r+1} \bmod 2^{r+2}.$$

This shows that k must be even and so $\left(\frac{b}{N}\right) = 1$. □

8.4 Fermat factorisation

The idea of Fermat factorisation is to write a composite number N as a difference of two perfect squares.

Lemma 8.17. *Let N be an odd integer. There is a bijection*

$$\{(a,b) \in \mathbb{N}^2 : a > b, ab = N\} \to \{(r,s) \in \mathbb{N}^2 : r^2 - s^2 = N\}, \quad (a,b) \mapsto \left(\frac{a+b}{2}, \frac{a-b}{2}\right).$$

Proof. Let $r = \frac{a+b}{2}, s = \frac{a-b}{2}$ then clearly $r^2 - s^2 = N$ and $r, s \in \mathbb{N}$ because a, b are both odd. The inverse is given by $a = r+s, b = r-s$. □

Fermat factorisation is described by the following algorithm. For each $i \geq 1$, let $r_i = [\sqrt{N}] + 1$. If $r_i^2 - N$ is a perfect square, then stop. This will eventually stop if we assume N is a composite odd number.

Example 8.18. *$N = 15$. $r_1 = 4$, and $4^2 - 15 = 1^2$ so $r = 4$ and $s = 1$.*

Remark 8.19. *In general this method is no better than trial division. But it is efficient if has a factor close to $\sqrt{N}$.*

Here are some possible improvements. Suppose we want to factorise $200819 = r^2 - s^2$. Since $200819 \equiv 2 \bmod 3$, so we must have $r \equiv 0 \bmod 3$ and $s \equiv 1 \bmod 3$.

We can also try to factorise kN for some integer k, and consider $r_i = [\sqrt{kN}] + i$. If $N = ab$ and $\frac{a}{b}$ is approximately $\frac{u}{v}$ for some small u, v. Then let $k = uv$ and we have

$$kN = uvab = \left(\frac{av + bu}{2}\right)^2 - \left(\frac{av - bu}{2}\right)^2$$

where $\frac{av-bu}{2}$ is much smaller than $\frac{a-b}{2}$.

8.5 Factor bases

The factor base method is one application of linear algebra in factorisation. We generalise the Fermat factorisation in the following way: find integers r, s such that $r^2 \equiv s^2 \bmod N$. Then $(r - s, N)$ is a proper divisor of n unless $r \equiv s \bmod N$. Similarly, $(r + s, N)$ is a proper divisor of N unless $r \equiv -s \bmod N$.

Definition 8.20. *A factor base B is a set $\{p_1, \ldots, p_k\}$ of distinct primes where we allow p_1 to be -1. For a given odd composite N, the square of an integer b is called a B-number if b' can be expressed as a product of powers of elements of B, where $b' \equiv b^2 \bmod N$ and $|b'| < \frac{1}{2}N$.*

The following algorithm describes the factor base method:

(i) Choose a suitable factor base B.

(ii) Find some B-numbers $b_1, \ldots, b_m$ and record $b'_1, \ldots, b'_m$ where $b'_i \equiv b_i^2 \bmod N$ and $|b'_i| < \frac{1}{2}N$.

(iii) Find some $I \subset \{1, \ldots, m\}$ such that $\prod_{i \in I} b'_i$ is a square, say c^2.

(iv) Let $b = \prod_{i \in I} b'_i$ and so $b^2 \equiv c^2 \bmod N$.

(iv) Compute $(N, b - c)$ and $(N, b + c)$ and hope to get a non-trivial factor of N.

Example 8.21. $N = 4633$. *We have*

$$67^2 \equiv -144, \quad 68^2 \equiv -9 \text{ mod } 4633$$

and so we take $B = \{-1, 2, 3\}$. Then $(67 \cdot 68)^2 \equiv (12 \cdot 3)^2$ and so we have

$$b = 67 \cdot 68 = 4556 \equiv -77 \text{ mod } 4633$$

and $c = 12 \cdot 3 = 36$. We have $(4633, -41) = 41$ and so $4633 = 41 \cdot 113$.

Remark 8.22. *In step (ii), let $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$ and write $B = \{r_1, \ldots, r_k\}$. Let $S(N, B)$ be the set of B-numbers mod N. So if $b \in S(N, B)$ then $b' = r_1^{a_1} \cdots r_k^{a_k}$ for some a_i. Define*

$$\lambda : S(N, B) \to \mathbb{F}_2^k, \quad b \mapsto (\bar{a}_1, \ldots, \bar{a}_k)$$

where $\bar{a}_i$ is a_i mod 2. Then in step (iii) we only need to seek $I \subset \{1, 2, \ldots, m\}$ such that $\sum_{i \in I} \lambda(b_i) = 0$. So we seek a linear independent relation satisfied by the m elements $\lambda(b_1), \ldots, \lambda(b_m)$ in the k-dimensional vector space $\mathbb{F}_2^k$. If $m \geq k + 1$ then we are guaranteed to find such a relation. It is the same as finding the kernel of the matrix whose i^{th} row is $\lambda(b_i)$.

8.6 The Continued fraction method

As we can see, the important thing in the factor base method is to pick a 'good' factor base B. We want number b such that b' is a product of small primes. One approach is to try integers close to $\sqrt{kN}$. Another approach is to use continued fraction. We assume N is not a square so $\sqrt{N}$ is an irrational number.

Lemma 8.23. *Let $\frac{p_n}{q_n}$ be convergents of $\sqrt{N}$. Then*

$$|p_n^2 - Nq_n^2| \leq 2\sqrt{N}.$$

Proof. Recall that $|\sqrt{N} - \frac{p_n}{q_n}| < \frac{1}{q_n q_{n+1}}$ by Theorem 7.10. So $|\sqrt{N} + \frac{p_n}{q_n}| < \frac{1}{q_n q_{n+1}} + 2\sqrt{N}$ by triangle inequality and so

$$|p_n^2 - Nq_n^2| = q_n^2|\sqrt{N} - \frac{p_n}{q_n}||\sqrt{N} + \frac{p_n}{q_n}| < q_n^2 \frac{1}{q_n q_{n+1}}(2\sqrt{N} + \frac{1}{q_n q_{n+1}}) = \frac{1}{q_{n+1}}(2q_n\sqrt{N} + \frac{1}{q_{n+1}}).$$

Since $q_n < q_{n+1}$, so

$$2q_n\sqrt{N} + \frac{1}{q_{n+1}} - 2q_{n+1}\sqrt{N} = \frac{2q_{n+1}(q_n - q_{n+1})\sqrt{N} + 1}{q_{n+1}} < 0.$$

So

$$|p_n^2 - Nq_n^2| < \frac{1}{q_{n+1}} 2q_{n+1}\sqrt{N} = 2\sqrt{N}.$$

□

Remark 8.24. *For all $N \geq 16$, $2\sqrt{N} \leq \frac{1}{2}N$ and so the above lemma actually shows that, if $p'_n \equiv p_n^2$ mod N and $|p'_n| < \frac{1}{2}N$, then $p'_n = p_n^2 - Nq_n^2$. For large N, $2\sqrt{N}$ is much smaller than $\frac{1}{2}N$ and so this gives a clue why this method is efficient. Also we only need to record p_n mod N instead of p_n itself.*

Example 8.25. *$N = 12403$ and try $B = \{-1, 2, 3, 5, 7, 11, 13\}$. We compute the convergents for $\sqrt{N}$,*

$$p_0 \equiv 111, \quad p_1 \equiv 223, \quad p_2 \equiv 334, \quad p_3 \equiv 891, \quad p_4 \equiv 2116, \quad p_5 = 3300, \quad p_6 \equiv 5416 \text{ mod } N$$

and so

$$p'_0 \equiv -82, \quad p'_1 \equiv 117, \quad p'_2 \equiv -71, \quad p'_3 \equiv 89, \quad p'_4 \equiv -27, \quad p'_5 = 166, \quad p'_6 \equiv -39 \text{ mod } N.$$

Then we see

$$(p_1 p_4 p_6)^2 \equiv 117 \cdot (-27) \cdot -39 = (3^3 \cdot 13)^2 \text{ mod } N$$

and we have $p_1 p_4 p_6 \equiv -1062$ mod N. Therefore, $b = 1062$ and $c = 351$. We try $(N, 711) = 79$ and so $N = 79 \cdot 157$.

8.7 Pollard's $p - 1$ method

The Pollard's $p - 1$ method works well when N has a prime factor p such that $p - 1$ is a product of small primes. It is described by the following algorithm

(i) Choose k which is lots of small prime powers. For example, $k = m!$ or k is the least common multiple of $1, 2, \ldots, m$..

(ii) Choose at random a small integer a, coprime to N.

(iii) Compute a^k mod N via repeated squaring.

(iv) Compute $(a^k - 1, N)$ and hope this is a non-trivial factor of N.

(v) If not, repeat for other chices of a and k.

The theory behind the algorithm is the following. If $p|N$ is a prime and $p-1|k$. Then $a^k \equiv 1 \bmod p$ by Euler Fermat. Then $p|(N, a^k - 1)$ in which case we get a non-trivial factor, unless it so happens that $a^k \equiv 1 \bmod N$.

Example 8.26. *$N = 540143$. Try $m = 8$ and $a = 2$. Then $k = lcm(1, 2, \ldots, 8) = 840$. We compute that*

$$a^{840} \equiv 53047 \ mod\ N$$

and we find that $(53047, 540143) = 421$. So $N = 421 \cdot 1283$.

8.8 Exercises

1. Show that if p is a prime, then p^2 is a pseudoprime with respect to a base b if and only if $b^{p-1} \equiv 1 \bmod p^2$. What about p^3?

2. Show that if n is a pseudoprime to the base 2, then so is $N = 2^n - 1$. Show further that N is a strong pseudoprime to the base 2.

3. Show that if n is a strong pseudoprime to the base b, then it is also a strong pseudoprime to the base b^k.

4. Let n be an odd composite integer. (i) Show that n is a Carmichael number if and only if n is square free and $p - 1|n - 1$ for all $p|n$.

   (ii) Show that if n is a Carmichael number, then n is the product of at least three distinct primes.

   (iii) Show that $N = (6t+1)(12t+1)(18t+1)$ is a Carmichael number where $6t+1, 12t+1, 18t+1$ are all prime numbers.

   (iv) Find all Carmichael numbers of the form $91p$ where p is a prime.

5. Let p be a prime > 5. Prove that $N = (4^p + 1)/5$ is a composite integer. Prove that N is a strong pseudoprime to the base 2.

6. Let $N > 1$ be a positive odd integer. Show that the congruence

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{N}\right) \bmod N$$

   fails to hold for at least half of the bases.

7. If $n \equiv 3 \bmod 4$ then n is a strong pseudoprime to the base b if and only if it is an Euler pseudoprime to the base b. Show also the same holds if $\left(\frac{b}{n}\right) = -1$.

8. Prove that if N has a factor which is within $\sqrt[4]{N}$ of $\sqrt{N}$, then Fermat factorisation must work on the first try.