These notes are based on a course of lectures given by Professor Corti during Autumn Term 2007 at Imperial College London. In general the notes follow Prof Corti's lectures very closely and only few changes were made mostly to make the typesetting easier. These notes have not been checked by Prof Corti and should not be regarded as official notes for the course. In particular, all the errors are made by me. However, I don't take any responsibility for their consequences; use at your own risk (and attend lectures, they are fun). Please email me at a$100$@ic.ac.uk with any comments or corrections.

Anton Stefanek
March 2008
## Contents

1. **Introduction**  
   1.1 Primes  
   1.2 Diophantine Equations  
   1.3 Algebraic Number Theory  
   
2. **Euclid's algorithm and The Fundamental Theorem**  
   2.1 Euclid's Algorithm  
   
3. **Congruences**  
   
4. **The Euler's Function $\varphi(n)$**  
   
5. **Chinese Remainder Theorem**  
   
6. **$k$th powers and roots mod $n$**  
   6.1 Successive Squaring  
   6.2 Applications  
   6.3 RSA Cryptography  
   
7. **Arithmetic functions**  
   7.1 Dirichlet Convolution  
   
8. **Perfect Numbers**  
   
9. **Large $n$ averages of arithmetic functions**  
   
10. **Prime Numbers**  
   
11. **Primitive Elements**  
   11.1 Solving linear congruences  
   
12. **Quadratic Reciprocity**  
   
13. **Sums of squares**  
   13.1 Fundamental Theorem in $\mathbb{Z}[i]$  
   13.2 Sums of Three Squares  
   13.3 Sums of Four Squares  
   
14. **Liouville's Theorem**
Chapter 1

Introduction

1.1 Primes

Let \( \mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\} \). Say \( n \in \mathbb{Z} \) divides \( m \in \mathbb{Z} \), write \( n | m \), if there exists \( k \in \mathbb{Z} \) such that \( m = kn \).

**Definition 1.1.** A number \( p \in \mathbb{Z}, p \neq \pm 1 \), is irreducible if \( p = nm \) implies that either \( n = \pm 1 \) or \( m = \pm 1 \).

A number \( p \in \mathbb{Z}, p \neq \pm 1 \), is prime if \( p|ab \) implies \( p|a \) or \( p|b \) for all \( a, b \in \mathbb{Z} \).

It is easy to show that if \( p \) is prime, \( p \) is also an irreducible and harder to show the opposite. This forms the basis of unique factorization.

**Theorem 1.2.** There are infinitely many primes.

**Proof.** Suppose the contrary, i.e. that \( p_1, p_2, \ldots, p_k \) are all the primes. Then apply the unique factorization to \( N = p_1 p_2 \cdots p_k + 1 \): it is clear that no \( p_i \) divides \( N \), hence \( N \) has a unique factorization with new primes appearing. \( \Box \)

The question is: How many primes are there? For example, the following is known: for \( \pi(n) = \# \{ p \mid p \text{ prime, } p \leq n \} \):

**Theorem 1.3.**

\[
\lim_{n \to \infty} \frac{\pi(n) \log(n)}{n} = 1.
\]

1.2 Diophantine Equations

Let \( \mathbb{Z}[x_1, \ldots, x_n] \) be the polynomials in variables \( x_1, \ldots, x_n \) with coefficients in \( \mathbb{Z} \).

Given \( f_1, \ldots, f_m \in \mathbb{Z}[x_1, \ldots, x_n] \), study the system of equations

\[
\begin{align*}
    f_1(x_1, \ldots, x_n) &= 0, \\
    f_2(x_1, \ldots, x_n) &= 0, \\
    &\vdots \\
    f_m(x_1, \ldots, x_n) &= 0
\end{align*}
\]

for \( x_1, \ldots, x_n \in \mathbb{Z} \) (and sometimes \( \mathbb{Q} \)).

**Example 1.4.** Solve \( x^2 + y^2 - z^2 = 0 \) (\( \star \)) for \( x, y, z \in \mathbb{Z} \). A similar question then is: solve \( X^2 + Y^2 = 1 \) (\( \star \star \)) \( (X = \frac{x}{z}, Y = \frac{y}{z}) \) for \( X, Y \in \mathbb{Q} \). This has a geometric interpretation, i.e. find points with coordinates in \( \mathbb{Q} \) on a circle of radius 1. The line of slope \( m \) passing through \( (0, -1) \) has equation...
y = mx − 1. We get

\[ x^2 + (mx - 1)^2 = 1 \]
\[ (1 + m^2)x^2 - 2mx = 0 \]
\[ x((1 + m^2)x - 2m) = 0 \]

If \( x = \frac{2m}{1 + m^2} \) we have

\[ y = m \left( \frac{2m}{1 + m^2} \right) - 1 = \frac{2m^2 - 1 - m^2}{1 + m^2} = \frac{m^2 - 1}{m^2 + 1} \]

Solution of (**) then is

\[ \{ x = \frac{2m}{m^2 + 1}, \ y = \frac{m^2 - 1}{m^2 + 1} \mid m \in \mathbb{Q} \} \]

To get solutions of (**), let \( m = \frac{s}{t} \) and then

\[ x = \frac{2s}{s^2 + 1}, \ y = \frac{s^2 + t^2}{s^2 + t^2} \]

With a bit of thought, we get solutions for (**) to be

\[ x = 2st, \]
\[ y = s^2 - t^2, \]
\[ z = s^2 + t^2 \]

for \( s, t \in \mathbb{Z} \). We can divide by two if both \( s \) and \( t \) are odd.

Other examples could be to solve for \( x, y \in \mathbb{Z} \) \( x^2 + y^2 = a \) with \( a \in \mathbb{Z} \).

1.3 Algebraic Number Theory

Integers in number fields.

Example 1.5. Let \( x \in \mathbb{Z} \) be square free \( (k^2 \) does not divide \( x \) for all \( k \neq \pm 1 \)). Then

\[ \mathbb{Q}(\sqrt{d}) = \{ x + y\sqrt{d} \mid x, y \in \mathbb{Q} \} \]

is an example of a number field. There is a notion of integers in \( \mathbb{Q}(\sqrt{d}) \), e.g. integers in \( \mathbb{Q}(\sqrt{-1}) \) are the things of the form \( a + bi, a, b \in \mathbb{Z} \).
Chapter 2

Euclid’s algorithm and The Fundamental Theorem

Definition 2.1. The highest common factor of two integers \( a, b \) is \( (a, b) = \text{hcf}(a, b) = \text{gcd}(a, b) \), the largest \( d \) such that \( d | a \) and \( d | b \).

2.1 Euclid’s Algorithm

Given integers \( a, b > 0 \), there exist integers \( q, r \) such that \( a = bq + r \) and \( 0 \leq r < b \). Start with \( 0 < a_2 < a_1 \). Then let

\[
\begin{align*}
a_1 &= a_2q_1 + a_3, \\
a_2 &= a_3q_2 + a_4, \\
&\vdots \\
a_{k-1} &= a_kq_{k-1} + a_{k+1}, \\
a_k &= a_{k+1}q_k + 0
\end{align*}
\]

with \( 0 \leq a_{i+1} < a_i \) for all \( i \).

Proposition 2.2. \( a_{k+1} = \text{hcf}(a_1, a_2) \).

Proof. If \( d | a_1 \) and \( d | a_2 \), then \( d | a_2 \) and \( d | a_3, d | a_3 \) and \( d | a_4, \ldots, d | a_{k+1} \). □

Example 2.3. We have \( \text{hcf}(105, 28) = 7 \):

\[
\begin{align*}
105 &= 28 \cdot 3 + 21 \\
28 &= 21 \cdot 1 + 7 \\
21 &= 7 \cdot 3 + 0.
\end{align*}
\]

Corollary 2.4.

(1) There exist integers \( x, y \) such that \( \text{hcf}(a, b) = ax + by \).

(2) If \( d | a \) and \( d | b \), then \( d | \text{hcf}(a, b) \).

(3) The group \( \{ ax + by \mid x, y \in \mathbb{Z} \} \) is a subgroup of \( \mathbb{Z} \) generated by \( \text{hcf}(a, b) \), i.e. \( \text{hcf}(a, b) \mathbb{Z} \).

Proof. For (1), \( \text{hcf}(a, b) \in \langle a, b \rangle \) since \( \text{hcf}(a, b) \in \langle a_{k+1} \rangle = \langle a_{k-1}, a_k \rangle = \cdots = \langle a_1, a_2 \rangle \). This also shows (3). For (2), if \( d | a \) and \( d | b \) then \( d | ax + by = \text{hcf}(a, b) \). □
Example 2.5. Find $x, y$ such that $105x + 28y = 7$. Euclid’s algorithm gives

\[
\begin{align*}
21 & = 105 - 28 \cdot 3 \\
7 & = 28 - 21 \cdot 1 \\
& = 28 - (105 - 28 \cdot 3) - 1 \\
& = 105 \cdot (-1) + 28 \cdot 4.
\end{align*}
\]

Proposition 2.6. An integer $p$ is prime if and only if it is irreducible.

Proof.

$\Rightarrow$ Assume $p$ is prime. Let $p = nm$. Then $p|n$ or $p|m$, say $p|n$. Then $n = kp$ for some $k$. Now $p = pkm$, i.e. $km = 1$. Hence $m = \pm 1$ and so $p$ is irreducible.

$\Leftarrow$ Assume $p$ is irreducible. Say $p|ab$. Assume $p$ does not divide $a$ and show $p$ divides $b$.

Because $p$ is irreducible, $\gcd(p, a) = 1$, so there exist $x, y \in \mathbb{Z}$ such that $px + ay = 1$. Get $pxb + yab = b$. Now $p|ab$ and $p|p$, so $p|pxb + yab$ and so $p|b$. Hence $p$ is prime.

\[\blacksquare\]

Lemma 2.7. Assume $d|ab$, $\gcd(d, a) = 1$. Then $d|b$.

Proof. There exist integers $a, b, c$ such that $dx + ay = 1$ and so $dxb + yab = b$ and so $d|b$.

Theorem 2.8 (The Fundamental Theorem). Every integer $n > 0$ can be uniquely written as a product of primes

\[n = \prod_{p_1 < p_2 < \ldots < p_k} p_i^{e_i}.
\]

Proof. It is immediate that there exists a decomposition into irreducibles (if $n = n_1 n_2$ then both $n_1, n_2 < n$). Now assume we can do this in more than one way, that is

\[n = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r} = q_1^{b_1} q_2^{b_2} \ldots q_s^{b_s}.
\]

Clearly $p_1 | q_1, q_2^{b_2} \ldots q_s^{b_s}$. Because $p_1$ and all $q_i$’s are prime, $p_1$ is $q_i$ for some $i$. We can by induction get unique decomposition of $n/p_1$.

\[\blacksquare\]

Problem – for $x, y \in \mathbb{Z}$, solve $ax + bx = c$ ($\ast$). A solution exists if and only if $\gcd(a, b)|c$.

Example 2.9. Solve $105x + 28y = 14$. We know that $\gcd(105, 28) = 7$ and also that $7|14$ and so a solution exists. Recall that $105 \cdot (-1) + 28 \cdot 4 = 7$ and so $105 \cdot (-2) + 28 \cdot 8 = 14$. So $(x_0, y_0) = (-2, 8)$ is a solution.

Let $(x_0, y_0)$ be a solution. Then $(x, y)$ solves ($\ast$) iff $a(x - x_0) + b(y - y_0) = 0$ that is iff $u = x - x_0, \ v = y - y_0$ solve $au + bv = 0$ ($\ast \ast$). Write $d = \gcd(a, b)$ and $a = da', b = db'$. Then ($\ast \ast$) is equivalent to $a'u + b'v = 0$ where $\gcd(a', b') = 1$. Note that now $a'|v$, i.e. $v = ka'$ and so $u = -kb'$. That is, $u, v$ solves ($\ast \ast$) iff $u = -kb'$ and $v = ka'$ for some $k \in \mathbb{Z}$. Therefore the solutions to ($\ast$) are

\[\{x = x_0 - kb', \ y = y_0 + ka' \mid k \in \mathbb{Z}\}.
\]

For the previous example, this is $\{-2 - 4k, 8 + 15k \mid k \in \mathbb{Z}\}$. 
Chapter 3

Congruences

**Definition 3.1.** We say that \( a \) is congruent to \( b \) modulo \( n \), write \( a \equiv b \mod n \) if and only if \( n | (a - b) \). The **congruence classes modulo** \( n \) are \( \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/n \).

**Note** (Division algorithm). Let \( a = nq + r, 0 \leq r < n \). Then \( a \) is congruent (modulo \( n \)) to a unique \( r, 0 \leq r < n \). Possible to think similar to \( \mathbb{Z}/n = \{0 \leq r < n\} \). In particular, \( \mathbb{Z}/n \) has \( n \) elements.

Also note that \( \mathbb{Z}/n \) is a **ring**.

**Example 3.2.** \( (\mathbb{Z}/n, +) \) is a cyclic abelian group generated by \( 1 \in \mathbb{Z}/n \).

The reason to have congruences is that \( \mathbb{Z}/n \) is finite.

**Example 3.3.** Let \( p \) be an odd prime. Then \( x^2 + y^2 = p \) is soluble for \( x, y \in \mathbb{Z} \) only if \( p \equiv 1 \mod 4 \). The key point is that \( x^2 \equiv 0, 1 \mod 4 \) for all \( x \) and hence \( x^2 + y^2 \equiv 0, 2 \mod 4 \). On the other hand, \( p \equiv 1, 3 \mod 4 \). The converse is also true, but the proof is much harder and will be given later.

**Example 3.4.** Solve \( x^2 + y^2 - 3z^2 = 0 \) for \( x, y, z \in \mathbb{Z} \). This has no solutions (aside from the trivial case \( x = y = z = 0 \)). Consider modulo 3 and assume a non-trivial solution \( x, y, z \). Have

\[
\begin{align*}
x^2 + y^2 - 3z^2 & \equiv 0 \mod 3 \\
y^2 & \equiv 0 \mod 3
\end{align*}
\]

and so \( x, y \equiv 0 \mod 3 \) (since if \( x \equiv 1, 2 \mod 3 \), \( x^2 \equiv 1 \mod 3 \)), i.e. \( x = 3x', y = 3y' \). So we have

\[
\begin{align*}
(3x')^2 + (3y')^2 - 3z'^2 &= 0 \\
9x'^2 + 9y'^2 - 3z'^2 &= 0 \\
z^2 &= 3(x'^2 + y'^2).
\end{align*}
\]

Looking again at modulo 3, we get \( z^2 \equiv 0 \mod 3 \) and hence \( z \equiv 0 \mod 3 \) and so \( z = 3z' \). Hence all three \( x, y, z \) are divisible by 3. Putting these together, we get

\[
\begin{align*}
x^2 + y^2 - 3z^2 &= 0 \\
9x'^2 + 9y'^2 - 27z'^2 &= 0 \\
x'^2 + y'^2 - 3z'^2 &= 0.
\end{align*}
\]

So from \( x, y, z \) we have constructed a smaller solution \( x', y', z' \). We can repeat the same process until we inevitably get to the trivial solution.

**Example 3.5.** Similar to the previous example: \( x^2 - 2y^2 = 0 \) has no solutions for \( x, y \in \mathbb{Z} \). We have \( x^2 - 2y^2 \equiv 0 \mod 2 \) and so \( x^2 \equiv 2y^2 \equiv 0 \mod 2 \) and so \( x = 2x' \). We get

\[
\begin{align*}
(2x')^2 - 2y^2 &= 0 \\
4x'^2 - 2y^2 &= 0 \\
2x'^2 - y^2 &= 0
\end{align*}
\]

and so \( y^2 \equiv 0 \mod 2 \) and hence \( y = 2y' \). We get \( x'^2 - 2y'^2 = 0 \) and can descent to the trivial solution.
A known fact: let \( q(x, y, z) \in \mathbb{Z}[x, y, z] \) be a homogeneous quadratic polynomial. Then \( q(x, y, z) = 0 \) is soluble for \( x, y, z \in \mathbb{Z} \) iff (i) \( q(x, y, z) \equiv 0 \mod p^n \) is soluble for \( x, y, z \in \mathbb{Z}/p^n \) for all \( n \geq 1 \) and \( p \) prime and (ii) \( q(x, y, z) = 0 \) is soluble for \( x, y, z \in \mathbb{R} \). It turns out that (i) can be checked using only finitely many pairs of \( p, n \).

Consider the equation
\[
ax \equiv b \mod n
\]
for \( x \in \mathbb{Z}/n \).

**Theorem 3.6.** The equation \((\star)\) is soluble iff \( \text{hcf}(a, n) | b \) and there exist precisely \( \text{hcf}(a, n) \) solutions modulo \( n \).

**Proof.** Have \( ax \equiv b \mod n \) iff there exists \( y \) such that \( ax - ny = b \). Integers \( x, y \) exist iff \( \text{hcf}(a, n) | b \) (from the previous).

Assume \( ax_0 \equiv b \mod n \). Then \( ax \equiv b \mod n \) iff \( a(x - x_0) \equiv 0 \mod n \). So the solutions of \((\star)\) are \( \{ x_0 + u \mid au \equiv 0 \mod n \} \). We need to solve \( au \equiv 0 \mod n \), that is \( n|au \). Write \( d = \text{hcf}(a, n), a = d' d, \) \( n = n' d \) where \( \text{hcf}(d', n') = 1 \). Then \( n|au \) iff \( n'|d' u \) iff \( n'|u \), so \( u = 0, n', \ldots, (d - 1)n' \).

**Example 3.7.** Solve \( 18x \equiv 8 \mod 22 \) for \( x \in \mathbb{Z}/22\mathbb{Z} \). We have \( \text{hcf}(18, 22) = 2 \) which divides 8, so there exist a solution. We use the Euclidean algorithm to find one solution:

\[
\begin{align*}
22 &= 18 \cdot 1 + 4 \\
18 &= 4 \cdot 4 + 2.
\end{align*}
\]

So \( 2 = 18 - 4 \cdot 4 = 18 - 4(22 - 18) = 18 \cdot 5 - 22 \cdot 4 \) and so \( x_0 = 20 = 5 \cdot 4 \) solves \((\dagger)\).

We have \( 18u \equiv 0 \mod 22 \) iff \( 9u \equiv 0 \mod 11 \), so \( u \equiv 0, 11 \mod 22 \). The solutions of are \( \{ 20, 9 \mod 22 \} \).
Chapter 4

The Euler’s Function $\varphi(n)$

**Definition 4.1.** The Euler’s function $\varphi(n)$ is defined as

$$\varphi(n) = \{0 < k < n \mid \gcd(k, n) = 1\}.$$ 

Equivalently, it is the number of elements of $\mathbb{Z}/n^*$, the multiplicative group of all $a \in \mathbb{Z}/n$ for which there exists a $b \in \mathbb{Z}/n$ such that $ab \equiv 1 \mod n$. Indeed, $ax \equiv 1 \mod n$ is soluble iff $\gcd(a, n)\mid 1$ by the previous theory.

**Theorem 4.2.**

1. If $\gcd(n, m) = 1$ then $\varphi(nm) = \varphi(n)\varphi(m)$.
2. If $p$ is a prime, then $\varphi(p^r) = p^r - p^{r-1}$.
3. 

$$\varphi(n) = n \prod_{\text{prime } p \mid n} \left(1 - \frac{1}{p}\right).$$

We give two proofs of this theorem:

**Proof 1.** We prove (3) and then (1) and (2) follow. The proof will follow the same structure as this example. Calculate $\varphi(12)$. We have $12 = 2^2 \cdot 3$. We can partition $\mathbb{Z}/12$ to a disjoint union of numbers divisible by 2, 3, 6 and the rest. Then

$$\varphi(12) = 12 - \# \{\text{divisible by 2}\} - \# \{\text{divisible by 3}\} + \# \{\text{divisible by 6}\}$$

$$= 12 - \frac{12}{2} - \frac{12}{3} + \frac{12}{6}$$

$$= 4$$

$$= \# \{1, 5, 7, 11\}.$$ 

Slightly more general case arises when we consider $n = p^r q^s$ for $p, q$ prime. We get

$$\varphi(n) = n - \frac{n}{p} - \frac{n}{q} + \frac{n}{pq}$$

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

In general, we can use the following Lemma we state without a proof:

**Lemma 4.3** (Inclusion-exclusion formula). Let $\Omega$ be a finite set and $A_1, \ldots, A_m \subseteq \Omega$ its subsets. Then

$$\left|\Omega \setminus \left(\bigcup_{i=1}^m A_i\right)\right| = |\Omega| + \sum_{k=1}^m (-1)^k \sum_{i_1 < \cdots < i_k} |A_{i_1} \cap \cdots \cap A_{i_k}|.$$
Write \( n = \prod_{i=1}^{m} p_i^{r_i} \) and let \( \Omega = \mathbb{Z}/n \) and \( A_i = \{ l \mod n \mid p_i \mid l \} \). Clearly
\[
A_i \cap A_{i_2} \cap \cdots \cap A_{i_k} = \{ l \mod n \mid p_{i_1}, p_{i_2}, \ldots, p_{i_k} \mid l \}.
\]
Using the above lemma, we get
\[
\varphi(n) = |\Omega \setminus \bigcup_i A_i| = n - \sum_i n/p_i + \sum_{i<j} n/p_{i}p_{j} - \sum_{i<j<k} n/p_{i}p_{j}p_{k} + \cdots
\]
\[
= n \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right).
\]

**Corollary 4.4** (Euler’s Theorem). For integers \( a, n \), if \( \gcd(a, n) = 1 \), \( a^{\varphi(n)} \equiv 1 \mod n \).

**Proof.** \( \mathbb{Z}/n^* \) is an abelian group of order \( \varphi(n) \). Also \( \gcd(a, n) = 1 \) means that \( a \in \mathbb{Z}/n^* \) and so the order of \( a \) divides \( \varphi(n) \), hence \( a^{\varphi(n)} = 1 \) in \( \mathbb{Z}/n^* \).

**Corollary 4.5** (Fermat’s little theorem). For a \( p \) prime and an integer \( a \) not divisible by \( p \), \( a^{p-1} \equiv 1 \mod p \).

**Proof.** This is a special case of the previous corollary with \( n = p \) prime.
Chapter 5

Chinese Remainder Theorem

**Theorem 5.1** (Chinese Remainder Theorem). Let $n, m$ be integers such that $\text{hcf}(n, m) = 1$. Then

1. For all $a, b$ there exists a unique $z$ modulo $nm$ such that
   
   
   
   $z \equiv a \mod n$,
   
   $z \equiv b \mod m$,
   
   2. and $\text{hcf}(z, nm) = 1$ if and only if $\text{hcf}(a, n) = \text{hcf}(b, m) = 1$.

**Proof.** To show the existence of $z$: We have

\[ z = a + nx = b + my \]

\[ nx - my = b - a. \]

Now $x, y$ exist because $\text{hcf}(n, m) = 1$.

To show the uniqueness, consider another solution $z'$. Then $z - z' \equiv 0 \mod n$ and so $n|z - z'$ and similarly $m|z - z'$ and so $mn|z - z'$, that is $z \equiv z' \mod mn$.

**Example 5.2.** Solve for $z$ modulo $7 \cdot 9 = 63$:

\[ z \equiv 3 \mod 7, \]

\[ z \equiv 5 \mod 9. \]

We have $3 + 7x = 5 + 9y$, e.g. $x = -1$ and $y = -1$. So a solution is $3 + 7(-1) = -4 \equiv 59 \mod 63$.

**Theorem 5.3** (Chinese Remainder Theorem, High level view). Assume $\text{hcf}(n, m) = 1$. Then

1. $Z/nm = Z/n \times Z/m$ as a direct product of abelian groups under addition.

   2. $Z/nm^\times = Z/n^\times \times Z/m^\times$ as a direct product of abelian groups under multiplication.
Chapter 6

\( k^{\text{th}} \) powers and roots mod \( n \)

6.1 Successive Squaring

Example 6.1. Calculate \( a^k \mod n \), for example calculate \( 7^{327} \mod 853 \). The idea is to write 327 as a sum of powers of two, that is \( 327 = 256 + 64 + 4 + 2 + 1 \). Then we have

\[
\begin{align*}
7^1 &\equiv 7 \mod 853, \\
7^2 &\equiv 14 \mod 853, \\
7^4 &\equiv (7^2)^2 \equiv 49^2 \equiv 695 \mod 853, \\
7^8 &\equiv (7^4)^2 \equiv 695^2 \equiv 227 \mod 853, \\
7^{16} &\equiv (7^8)^2 \equiv 227^2 \equiv 349 \mod 853, \\
7^{32} &\equiv 675 \mod 853, \\
7^{64} &\equiv 123 \mod 853, \\
7^{128} &\equiv 628 \mod 853, \\
7^{256} &\equiv 298 \mod 853.
\end{align*}
\]

So

\[
7^{327} \equiv 7^{256} \cdot 7^{64} \cdot 7^4 \cdot 7^2 \cdot 7 \\
\equiv 298 \cdot 123 \cdot 695 \cdot 49 \cdot 7 \\
\equiv 286 \mod 853.
\]

To calculate \( a^k \mod n \):

- Write \( k = u_0 + 2u_1 + 4u_2 + \cdots + 2^r u_r \) for \( u_i \in \{0, 1\} \).
- Calculate \( a, a^2, a^4, \ldots, a^{2^r} \mod n \).
- Finally multiply to get \( a^k \mod n \).

6.2 Applications

In primality tests. Recall that if \( p \) is prime, \( a^{p-1} \equiv 1 \mod p \). For example, we can check that \( p = 2279 \) is not a prime by showing that \( 2^{2278} \not\equiv 1 \mod 2279 \).

Proposition 6.2. Assume that \( \gcd(b, n) = 1 \) and \( \gcd(k, \phi(n)) = 1 \). Then there exists a unique \( a \mod n \) such that \( a^k \equiv b \mod n \).
Proof. There exist \( x, y \) such that \( ky - \varphi(n)x = 1 \). The following operations are inverse to each other on \( \mathbb{Z}/n^* - \varphi : a \mapsto a^k \) and \( \psi : b \mapsto b^y \). We need to check that \( \psi \circ \varphi = \psi \circ \phi \) is the identity. We have

\[
\psi \circ \varphi(a) = \left(a^k\right)^y = a^{ky} = a^{\varphi(n)z+1} = a\left(a^{\varphi(n)}\right)^z \equiv a \mod n
\]

by the Euler’s theorem. Similarly \( \phi \circ \psi(b) = (b^y)^k = b^{ky} = b \mod n \).

Example 6.3. Solve for \( x \), \( x^{131} \equiv 758 \mod 1073 \).

- Find \( \varphi(1073) = 1073 = 29 \cdot 37 \), so \( \varphi(1073) = 28 \cdot 36 = 1008 \).
- Find \( z, y \) such that \( 131y - 1008z = 1 \). Take \( y = 731 \) and \( z = 95 \).
- Get \( x = 758^y \cdot 758^{731} \equiv 905 \mod 1073 \).

To solve \( x^k \equiv b \mod n \) is computationally very hard because we need to have a complete factorization of \( n \). This all becomes very easy if somehow \( \varphi(n) \) is known.

### 6.3 RSA Cryptography

Proposition 6.4. Assume \( n \) is square-free (i.e. if \( k^2|n \) then \( k = \pm 1 \) or equivalently, \( n \) is a product of distinct primes) and \( \text{hcf}(k, \varphi(n)) = 1 \). Then \( x^k \equiv b \mod n \) has a unique solution \( x \in \mathbb{Z}/n \) for all \( b \in \mathbb{Z}/n \).

Note. Note that we no longer assume \( \text{hcf}(b, n) = 1 \) and we look at \( \mathbb{Z}/n \) instead of \( \mathbb{Z}/n^* \).

Proof. Similar to the previous proposition. Since \( \text{hcf}(k, \varphi(n)) = 1 \), there exist \( y, z \in \mathbb{Z} \) such that \( ky - \varphi(n)z = 1 \). We show that the following maps are inverse to each other \(- \varphi : \mathbb{Z}/n \rightarrow \mathbb{Z}/n \) such that \( \varphi(a) = a^k \) and \( \psi : \mathbb{Z}/n \rightarrow \mathbb{Z}/n \) such that \( \psi(a) = a^y \) Clearly

\[
\varphi(a) = a^k \equiv a^{\varphi(n)z+1},
\]

\[
\psi(a) = a^y = a^{\varphi(n)z+1}.
\]

We just need to show that \( a^{\varphi(n)z+1} \equiv a \mod n \) for all \( a \). We can write \( n = p_1p_2 \ldots p_r \) with \( p_i \) distinct primes. Then \( \varphi(n) = (p_1 - 1)(p_2 - 1) \ldots (p_r - 1) \). Thinking modulo \( p_i \), we get

\[
a^{\varphi(n)z+1} \equiv a^{1+(p_i-1)-1} \equiv \begin{cases} 0 \equiv a \mod p_i & \text{if } p_i|a, \\ a \mod p_i & \text{if } p_i \nmid a. \end{cases}
\]

Hence \( a^{\varphi(n)z+1} \equiv a \mod p_i \) for all \( i \). By the uniqueness in Chinese Remainder Theorem, we conclude that \( a^{\varphi(n)z+1} \equiv a \mod n \).

How to use this for cryptography? Choose two large primes \( p, q \) with \( p < q \). Let \( n = pq \) and choose \( k \) such that \( \text{gcd}(k, \varphi(n)) = 1 \). Then make \( n, k \) public (these will be used in encryption) and keep \( p, q, \varphi(n) \) secret for decryption. By a message, we mean a string \( a_1a_2 \cdots \) with \( a_i \in \mathbb{Z}/n \). Now:

- The encrypted message is the string \( b_1b_2 \cdots \) where \( b_i \equiv a_i^k \in \mathbb{Z}/n \).
- To decrypt a message, we must find \( z, y \) such that \( ky - \varphi(n)z = 1 \) (existence is assumed by the refined proposition at the start).

Example 6.5. Take \( n = 77 \) and \( k = 7 \) and make them public. We have \( n = 7 \cdot 11 \) and so \( \varphi(n) = 60 \), \( \text{gcd}(k, \varphi(n)) = 1 \) and this is kept secret. We code letters as follows:
Now, we decrypt the message HELLO: The message is code as 18, 15, 22, 22, 25 and the encrypted message is then $18^7, 15^7, 22^7, 22^7, 25^7$ (all mod $n$), that is 39, 71, 22, 22, 53. Note that we only needed the public key ($n$ and $k$) for encryption.

To decrypt, we need the secret information: We get $7 \cdot 43 - 60 \cdot 5 = 1$. We can check that

$$39^{43}, 71^{43}, 22^{43}, 22^{43}, 53^{43} \equiv 18, 15, 22, 22, 25 \text{ mod } 77$$

gives the original message.
Chapter 7

Arithmetic functions

**Definition 7.1.** An arithmetic function is a function $f : \mathbb{N} \to \mathbb{C}$.

Arithmetic function $f$ is multiplicative if for $m, n$ such that $\text{hcf}(m, n) = 1$, $f(nm) = f(n)f(m)$ and completely multiplicative if $f(nm) = f(n)f(m)$ for all $m, n \in \mathbb{N}$.

**Example 7.2.** Define $u$ to be

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

Define 1, $I$ to be

$$1(n) = 1,$$
$$I(n) = n$$

for all $n$. Another example of an arithmetic function is the Euler function $\varphi(n)$. Also the following two functions

$$\sigma_k(n) = \sum_{d|n} d^k \text{ for } k \in \mathbb{N},$$
$$\mu(n) = \begin{cases} (-1)^k & \text{if } n = p_1 \cdots p_k \text{ (distinct primes),} \\ 1 & \text{if } n = 1, \\ 0 & \text{otherwise.} \end{cases}$$

These are both also multiplicative (we will show this later).

### 7.1 Dirichlet Convolution

**Definition 7.3.** The Dirichlet convolution of two arithmetic functions $f, g : \mathbb{N} \to \mathbb{C}$ is the function $f * g : \mathbb{N} \to \mathbb{C}$

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

**Example 7.4.**

$$\sigma_1(n) = \sigma(n) = \sum_{d|n} d = I * 1.$$  

**Proposition 7.5.** For $n \in \mathbb{N}$, $n = \sum_{d|n} \varphi(d)$ or in other words, $I = \varphi * 1$.

**Proof.** The set $\{0, 1, \ldots, n-1\}$ is a disjoint union of sets $A(c)$ for all divisors $c$ of $n$ where

$$A(c) = \{0 < k < n \mid c = \text{hcf}(k, n)\}.$$

We claim that $|A(c)| = \varphi(d)$ where $d = n/c$. We have $\text{hcf}(k, n) = c$ iff $k = hc$ and $n = dc$ for some $h, d$ and $\text{hcf}(h, d) = 1$. This means there is a 1−1 correspondence between $A(c)$ and $\{0 < h < d \mid \text{hcf}(h, d) = 1\}$.

Also for a divisor $c$ of $n$, $n/c$ is also a divisor of $n$ and hence the proposition follows. \[\blacksquare\]
Proposition 7.6 (Properties of Dirichlet convolution). The Dirichlet convolution is \((f, g)\) are arithmetic functions)

1. commutative, i.e. \(f * g = g * f\),
2. associative, i.e. \(f * (g * h) = (f * g) * h\),
3. has an identity \(u\) such that \(f * u = u * f = f\) and
4. is multiplicative for \(f, g\) multiplicative.

Proof. We prove (4). Take \(n, m\) with \(\gcd(n, m) = 1\). Then

\[
f * g(nm) = \sum_{d|m} f(d)g\left(\frac{nm}{d}\right).
\]

Since \(\gcd(n, m) = 1\), every divisor \(d\) of \(nm\) is uniquely of the form \(d = d' d''\) where \(d'|n\) and \(d''|m\) and \(\gcd(d', d'') = 1\). Therefore

\[
f * g(nm) = \sum_{d'|n, d''|m} f(d')g\left(\frac{n}{d'}\right)g\left(\frac{m}{d''}\right)
= \left(\sum_{d'|n} f(d')g\left(\frac{n}{d}\right)\right)\left(\sum_{d''|m} g\left(\frac{m}{d''}\right)\right)
= (f * g(n))(f * g(m)).
\]

Theorem 7.7. The *-inverse of 1 is \(\mu\), i.e. \(1 * \mu = u\).

First proof. Because \(1 * \mu\) is multiplicative (since 1 and \(\mu\) are), we need to check the equality \(1 * \mu(n) = u(n)\) only for \(n = p^r\) for \(p\) prime, \(r \geq 1\). We have

\[
1 * \mu(1) = \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^r)
= 1 - 1 + 0 + \cdots + 0
= 0 = u(p^r).
\]

The case \(n = 1\) can be easily checked.

Second proof. Let \(n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}\). Then

\[
1 * \mu = \sum_{d|n} \mu(d) = \sum_{d|p_1 p_2 \cdots p_k} \mu(d)
= \sum_{i_1 < i_2 < \cdots < i_k} \mu(p_{i_1} p_{i_2} \cdots p_{i_k})
= \sum_{i_1 < i_2 < \cdots < i_k} (-1)^{i_1 + i_2 + \cdots + i_k}
= \sum_{i_1 < i_2 < \cdots < i_k} (-1)^k
= 0 = u(n).
\]

Theorem 7.8. \(\varphi = \mu * I\), that is

\[
\varphi(n) = \sum_{d|n} \mu(d) \cdot \frac{n}{d}.
\]
Proof. We have $\sum_{d|n} \varphi(d) = n$, that is $I = \varphi \ast 1$. Therefore

$$I \ast \mu = (\varphi \ast 1) \ast \mu = \varphi \ast (1 \ast \mu) = \varphi \ast u = \varphi.$$  

Corollary 7.9. The function $\varphi$ is multiplicative.

Proof. By the previous theorem, $\varphi = \mu \ast I$ which is multiplicative since $\mu$ and $I$ are.
Chapter 8

Perfect Numbers

Definition 8.1. Integer \( n \) is perfect if it is equal to the sum of its divisors, i.e.

\[
\sigma(n) = \sum_{d|n, \quad d \neq n} d.
\]

That is also if \( \sigma(n) = 2n \).

Can we find all perfect numbers? For example, numbers 6, 10, 12, 28, 496 are perfect.

Theorem 8.2 (Euclid, Euler). An even number \( n \) is perfect if and only if \( n = 2^{p-1}(2^p - 1) \) where \( p \) and \( 2^p - 1 \) are prime.

Remark 8.3. There are no known odd perfect numbers.

Proof.

\[ \Rightarrow (\text{Euclid}) \quad \text{Let } n = 2^{p-1}q \text{ with } q = 2^p - 1. \quad \text{The divisors of } n \text{ are } 1, 2, 2^2, \ldots, 2^{p-1} \text{ and } q, 2q, \ldots, 2^{p-1}q. \]

Therefore

\[
\sigma(n) = 1 + 2 + 4 + \cdots + 2^{p-1} + q(1 + 2 + \cdots + 2^{p-1})
\]

\[
= 2^p - 1 + q(2^p - 1)
\]

\[
= (2^p - 1)(q + 1)
\]

\[
= 2 \cdot 2^{p-1}q
\]

\[
= 2n.
\]

\[ \Leftarrow (\text{Euler}) \quad \text{Let } n \text{ be even and perfect and let } n = 2^k m \text{ for } k \geq 1 \text{ and } m \text{ odd. We know that } \sigma \text{ is multiplicative and hence}
\]

\[
\sigma(n) = \sigma(2^k)\sigma(m)
\]

\[
2n = 2^{k+1}m = \left(2^{k+1} - 1\right)\sigma(m).
\]

Therefore \( 2^{k+1} - 1|m \) and \( 2^{k+1}|\sigma(m) \) and for \( L = m/(2^{k+1} - 1) \)

\[
\sigma(m) = 2^{k+1}L
\]

\[
m = \left(2^{k+1} - 1\right)L.
\]

We have \( L = 1 \), otherwise

\[
2^{k+1}L = \sigma(m) \geq 1 + L + m = 1 + L + \left(2^{k+1} - 1\right)L
\]

\[
= 2^{k+1}L + 1.
\]
Hence (1) and (2) become

\[ \sigma(m) = 2^{k+1} \]
\[ m = 2^{k+1} - 1. \]

So \( \sigma(m) = m + 1 \) and therefore the only divisors of \( m \) are 1 and \( m \) and so \( m \) is prime. We claim that when \( m = 2^{k+1} - 1 \) is prime, \( k + 1 = p \) is also prime. If \( k + 1 = ab \), then

\[ m = 2^{k+1} - 1 = (2^a - 1) \left( 1 + 2^a + 2^{2a} + \cdots + 2^{(b-1)a} \right) \]

would be a non-trivial factorisation of \( m \), contradicting \( m \) being prime. Hence \( n = 2^k \cdot m = 2^{p-1} (2^p - 1) \) where \( m = 2^p - 1 \) and \( p \) are prime.

\[ \square \]

**Definition 8.4.** A prime \( q \) of the form \( q = 2^p - 1 \) is called a Mersenne prime.

For example 3, 7, 31, 127, 131071 are Mersenne primes but \( 2^{11} - 1 = 2047 \) is not. It is unknown whether there are infinitely many Mersenne primes.
Chapter 9

Large $n$ averages of arithmetic functions

Given some arithmetic function $f(n)$, we want to study the behaviour of $f(n)$ as $n$ goes to infinity. For example the function $\sigma(n)$. For $n$ prime, $\sigma(n) = n + 1$, for $n = 2^k$, $\sigma(n) = 2^{k+1} - 2n$. So it is not going to be possible to say $\sigma(n)$ has a “definitive” behaviour as $n$ goes to infinity. Instead, we will study the average of $\sigma(n)$ as $n \to \infty$.

**Definition 9.1.** We say that a function $f(x)$ is *asymptotic* to $g(x)$ and write $f(x) \sim g(x)$ if and only if

$$\lim_{x \to \infty} \frac{f(x)}{g(x)} = 1.$$ 

**Definition 9.2.** We say that $f(x)$ is “big O” of $g$ and write $f(x) = O(g(x))$ if and only if there exists $c > 0$ and $a \in \mathbb{R}$ such that for all $x \geq a$ implies $f(x) \leq cg(x)$.

Later, we will prove the following theorem.

**Theorem 9.3.** For $d(n) = \sigma_0(n) = \sum_{d|n} 1$

(i) $\sum_{n \leq x} d(n) \sim x \log x$,

(ii) $\sum_{n \leq x} d(n) = x \log x + O(x)$,

(iii) $\sum_{n \leq x} d(n) = x \log x + (2\gamma - 1)x + O(\sqrt{x})$ where $\gamma$ is the Euler’s constant.

We could further prove the following results

**Theorem 9.4.**

- $\sum_{n \leq x} \sigma_a(n) = \frac{\zeta(a+1)}{\alpha+1} x^{\alpha+1} + o(x^\beta)$ if $0 < \alpha, \beta \neq 1$ for $\beta = \max\{1, \alpha\}$.
- $\sum_{n \leq x} \sigma(n) = \frac{1}{2} \zeta(2)x^2 + o(x \log x)$,
- $\sum_{n \leq x} \varphi(n) = \frac{x^2}{\pi^2} x^2 + o(x \log x)$,

where

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

**Definition 9.5.** The *Euler’s constant* $\gamma$ is

$$\gamma = \lim_{n \to \infty} \left( 1 + \frac{1}{2} + \cdots + \frac{1}{n} - \log(n+1) \right).$$

**Remark 9.6.** Usually, $\gamma$ is defined as $\gamma = \lim_{n \to \infty} \left( 1 + \frac{1}{2} + \cdots + \frac{1}{n} - \log(n+1) \right)$. This is an equivalent definition, because $\lim_{n \to \infty} (n + 1) - \log n = 0$. 

---

**Euler’s constant**
**Proposition 9.7.** For \( x > 0 \),

\[
\sum_{n \leq x} \frac{1}{n} = \log x + \gamma + O\left(\frac{1}{x}\right).
\]

**Proof.** First, we shall show that \( \gamma \) exists. The idea is to approximate \( \sum_{k \leq x} \frac{1}{k} \) with \( \int_{1}^{x} \frac{du}{u} \). Let \( A_i = \frac{1}{i} - \int_{i}^{i+1} \frac{du}{u} \). Then for \( n = \lfloor x \rfloor \)

\[
\sum_{k=1}^{n} \frac{1}{k} = \int_{1}^{n+1} \frac{du}{u} + \sum_{k=1}^{n} A_k
\]

\[
= \log(n+1) + \sum_{k=1}^{n} A_k.
\]

On the other hand, we have

\[
\sum_{k=1}^{n} \frac{1}{k} \leq \int_{2}^{n+1} \frac{du}{u-1} \leq 1 + \int_{1}^{n} \frac{du}{u} = 1 + \log n.
\]

Putting together, we get

\[
\gamma_n = 1 + \frac{1}{2} + \cdots + \frac{1}{n} - \log(n+1)
\]

\[
= A_1 + \cdots + A_n \leq 1 + \log n - \log(n+1) \leq 1.
\]

The sequence \( (\gamma_n) \) is bounded from above (by 1) and is increasing. Hence it converges to an existing limit. This limit is \( \gamma \). Now we estimate \( \sum_{k > x} A_k \):

**Lemma 9.8.** \( \sum_{k > x} A_k = O\left(\frac{1}{x}\right) \).

**Proof.** Using the above definition of \( A_k \), observe that \( \sum_{k > n} A_k \) lies in the area enclosed by the curves \( \frac{1}{x} \) and \( \frac{1}{x+1} \) from \( k \) onwards. That is \( \int_{n}^{\infty} \left( \frac{1}{u-1} - \frac{1}{u} \right) du = \int_{n}^{\infty} \frac{du}{u(u-1)} \)

and therefore

\[
\sum_{k > x} A_k = O\left(\int_{x}^{\infty} \frac{du}{u(u-1)} + O\left(\frac{1}{x}\right)\right)
\]

\[
= O\left(\int_{x}^{\infty} \frac{du}{u^2} + O\left(\frac{1}{x}\right)\right)
\]

\[
= O\left(\frac{1}{x}\right) + O\left(\frac{1}{x}\right)
\]

\[
= O\left(\frac{1}{x}\right).
\]

Using the above lemma, we get

\[
\sum_{n \leq x} \frac{1}{n} = \int_{1}^{x} \frac{du}{u} + \sum_{n \leq x} A_n + O\left(\frac{1}{x}\right)
\]

\[
= \int_{1}^{x} \frac{du}{u} + \sum_{n=1}^{\infty} A_n - O\left(\sum_{n > x} A_n\right) + O\left(\frac{1}{x}\right)
\]

\[
= \log x + \gamma + O\left(\frac{1}{x}\right).
\]
**Theorem 9.9.** For \( d(n) = \sigma_0(n) = \sum_{d|n} 1 \)

(i) \( \sum_{n \leq x} d(n) \sim x \log x \),

(ii) \( \sum_{n \leq x} d(n) = x \log x + O(x) \),

(iii) \( \sum_{n \leq x} d(n) = x \log x + (2\gamma - 1)x + O(\sqrt{x}) \) where \( \gamma \) is the Euler’s constant.

**Proof.**

(ii) Observe that \( \sum_{n \leq x} d(n) = \sum_{n \leq x} \sum_{d|n} 1 \). Let \( k = \lfloor x \rfloor \). Also \( d|n \leq x \) if \( n = dq \) where \( q \leq x/d \). Therefore \( \sum_{n \leq x} d(n) \) is the number of integer points in the area under the curve \( dq = k \). This is equal to

\[
\sum_{d \leq x} \sum_{q \leq \frac{x}{d}} 1 = \sum_{d \leq x} \left( \frac{x}{d} + O(1) \right)
= \sum_{d \leq x} \frac{x}{d} + O(x)
= x \sum_{d \leq x} \frac{1}{d} + O(x)
= x \left[ \log x + \gamma + O \left( \frac{1}{x} \right) \right] + O(x)
= x \log x + O(x).
\]

\[\blacksquare\]
Chapter 10

Prime Numbers

We want to test how prime numbers are distributed. The following is surprisingly hard to prove:

**Theorem 10.1** (Dirichlet). Assume that \(\text{hcf}(a,b) = 1\). Then there are infinitely many primes \(p \equiv b \mod a\).

We now look at two special cases.

**Theorem 10.2.** There are infinitely many primes \(p\) of the form \(p \equiv 3 \mod 4\).

*Proof.* Assume \(\{3, p_1, \ldots, p_r \}\) are all the primes of the form \(q \equiv 3 \mod 4\). Let \(N = 4p_2p_3\cdots p_r + 3 \equiv 3 \mod 4\). Now \(N\) has a decomposition into primes \(q_1\cdots q_s\). Since \(N\) is odd, so are all \(q_i\). If all \(q_i \equiv 1 \mod 4\), then \(N \equiv 1 \mod 4\); hence at least one \(q_i\) is 3 mod 4. But \(q_i\) is none of 3, \(p_2, \cdots, p_r\), a contradiction.

**Theorem 10.3.** There are infinitely many primes \(p\) of the form \(p \equiv 1 \mod 4\).

*Proof.* Assume \(\{p_1, p_2, \ldots, p_r\}\) are all the primes congruent to 1 mod 4. Take \(a = 2p_1p_2\cdots p_r\) and \(N = a^2 + 1 \equiv 1 \mod 4\) and its prime factors \(q_1, \ldots, q_s\). All \(q_i\) are odd, hence \(q_i \equiv \pm 1 \mod 4\) for all \(i\). Also, \(a^2 + 1 \equiv 0 \mod q_i\) and so the equation \(x^2 \equiv -1 \mod q_i\) is soluble for all \(q_i\).

**Lemma 10.4.** Let \(q\) be an odd prime. Assume the equation \(x^2 \equiv -1 \mod q\) is soluble. Then \(q \equiv 1 \mod 4\).

*Proof.* Think about the abelian group \((\mathbb{Z}/q\mathbb{Z})^*\) under multiplication. By assumption, there exists \(a \in (\mathbb{Z}/q\mathbb{Z})^*\) such that \(a^2 = -1\) and so \(a\) is of order 4. By Lagrange’s theorem, \(4 = o(a)|o(\mathbb{Z}/q\mathbb{Z})^* = q - 1\), that is \(q \equiv 1 \mod 4\).

From the previous lemma, all \(q_i \equiv 1 \mod 4\). None of them is in \(\{p_1, \ldots, p_r\}\); a contradiction.

**Remark 10.5.** We will later show that for \(q\) odd prime, \(x^2 \equiv -1 \mod q\) is soluble iff \(q \equiv 1 \mod 4\). More generally, we will study \(x^2 \equiv b \mod q\).

**Definition 10.6.** Let \(\pi(x) = \#\{p | p \leq x, p \text{ prime}\}\).

**Example 10.7.** Some values of \(\pi(x)\):

\[
\pi(10) = 4, \\
\pi(100) = 25, \\
\pi(1000) = 168, \\
\pi(10000) = 1229.
\]

**Theorem 10.8** (Prime Number Theorem). \(\lim_{x \to \infty} \frac{\pi(x)\log x}{x} = 1\).
Some of the open questions about primes are: Is every even number a sum of two primes? Are there infinitely many twin primes?

**Definition 10.9.** Let \( p_1 < p_2 < \cdots \) be the list of all primes. Define

\[
\mathcal{N}_r(x) = \{ n \mid 1 \leq n \leq x, \ p_i \nmid n \ \text{for all} \ i = 1, 2, \ldots, r \},
\]

\( N_r(x) = \# \mathcal{N}_r(x) \).

**Theorem 10.10** (Legendre Formula).

\[
N_r(x) = \lfloor x \rfloor - \sum_{i=1}^{r} \left\lfloor \frac{x}{p_i} \right\rfloor + \sum_{i<j} \left\lfloor \frac{x}{p_ip_j} \right\rfloor + \cdots + (-1)^r \left\lfloor \frac{x}{p_1p_2\cdots p_r} \right\rfloor.
\]

**Proof.** Using the inclusion-exclusion principle.

**Definition 10.11.** Let \( \mathcal{P}(x) = \{ p \mid p \text{ prime, } p \leq x \} \) so then \( \pi(x) = \# \mathcal{P}(x) \).

**Lemma 10.12.**

1. For \( r = \pi(\sqrt{x}) \), \( \pi(x) = \pi(\sqrt{x}) + N_r(x) - 1. \)
2. More generally, if \( 0 < \xi < x \) and \( r = \pi(\xi) \), then \( \pi(x) \leq \pi(\xi) + N_r(x) \).

**Proof.**

(2) We have \( \mathcal{P}(x) \subset \mathcal{P}(\xi) \bigcup \mathcal{N}_r(x) \) (that is \( \mathcal{P}(\xi) \cap \mathcal{N}_r(x) = \emptyset \)). Indeed it is obvious that \( \mathcal{P}(x) \subset \mathcal{P}(\xi) \cup \mathcal{N}_r(x) \). It is also clear that \( \mathcal{P}(x) \cap \mathcal{N}_r(x) = \emptyset \) and therefore \( \pi(x) \leq \pi(\xi) + N_r(x) \).

(1) In the case \( \xi = \sqrt{x} \), saying \( \mathcal{P}(x) = \mathcal{P}(\sqrt{x}) \bigcup \mathcal{N}_r(\sqrt{x}) \) just need to show \( \exists \ t \in \mathcal{N}_r(\sqrt{x}) \setminus \{1\} \). If \( n \) is composite then \( n \) is divisible by a prime less than \( \sqrt{x} \), hence \( n \) cannot be in \( \mathcal{N}_r(\sqrt{x}) \setminus \{1\} \) and so \( n \) is prime and \( n \in \mathcal{P}(x) \).

**Note.** Note that \( \sqrt{x} \) in (1) can be replaced by any \( \xi \geq \sqrt{x} \).

**Example 10.13.** Let \( x = 100, \ r = \pi(\sqrt{100}) = 4 \). Then \( \pi(100) = \pi(10) + N_4(100) \). Using the Legendres Formula, we can calculate \( \pi(100) \) only knowing the primes less or equal to 10:

\[
\pi(100) = 4 + N_4(100)
\]

\[
= 4 + 100 - \frac{100}{2} - \frac{100}{3} - \frac{100}{5} - \frac{100}{7} + \frac{100}{2 \cdot 3} + \frac{100}{2 \cdot 5} + \frac{100}{3 \cdot 5} + \frac{100}{2 \cdot 7} + \frac{100}{5 \cdot 7} - \frac{100}{2 \cdot 3 \cdot 5} - \frac{100}{2 \cdot 3 \cdot 7} - \frac{100}{3 \cdot 5 \cdot 7} - \frac{100}{2 \cdot 5 \cdot 7} + \frac{100}{2 \cdot 3 \cdot 5 \cdot 7} - 1
\]

\[
= 4 + 100 - 50 - 33 - 20 - 14 + 16 + 10 + 7 + 6 + 4 + 2 - 3 - 2 - 1 - 0 - 1 = 25.
\]

**Theorem 10.14.**

\[
\lim_{x \to \infty} \frac{\pi(x)}{x} = 0.
\]
Proof. For $0 < \xi < x$ (to be chosen later), $r = \pi(\xi)$,

$$\pi(x) \leq r + N_r(x)$$

$$= r + \left\lfloor \frac{x}{\xi} \right\rfloor + \sum_{1 \leq i_1 < i_2 \leq r} \frac{x}{p_{i_1} p_{i_2}} - \cdots$$

$$\leq r + \left\lfloor \frac{x}{\xi} \right\rfloor + \sum_{1 \leq i_1 < i_2 \leq r} \frac{x}{p_{i_1} p_{i_2}} - \cdots$$

$$+ x - \sum_{i=1}^{\left\lfloor \frac{x}{\xi} \right\rfloor} \frac{x}{p_i} + \sum_{1 \leq i_1 < i_2 \leq r} \frac{x}{p_{i_1} p_{i_2}} - \cdots$$

$$\leq r + 2^r + x \prod_{i=1}^{r} \left( 1 - \frac{1}{p_i} \right).$$

Now we try to estimate $\prod_{p \leq \xi} \left( 1 - \frac{1}{p} \right)$:

**Lemma 10.15.** Let

$$P(x) = \prod_{p \leq x} \left( 1 - \frac{1}{p} \right)^{-1}.$$  

Then $P(x) > \log x$.

**Proof.** For all $m > 0$ we have

$$P(x) > \prod_{n \leq x} \left( 1 + \frac{1}{p} + \frac{1}{p^2} + \cdots + \frac{1}{p^m} \right)$$

$$= \sum_{n \in S} \frac{1}{n}$$

Here $S$ is a set of natural numbers (products of primes $p \leq x$). We want to make sure $S$ contains all $1 \leq n \leq x$: If $n \leq x$, then $n = \prod_{i=1}^{k} p_i^{a_i}$ where all $p_i \leq x$. We need $m$ such that all $a_i \leq m$. We claim that $m$ such that $2^{m+1} > x$ works. Indeed, if $n \leq x$ then $n = \prod_{i=1}^{k} p_i^{a_i}$ with $2 \leq p_i \leq x$ and so $2^{a_i} \leq p_i^{a_i} \leq n \leq x < 2^{m+1}$, i.e. $a_i < m + 1$.

Finally, we get

$$P(x) > \sum_{n \leq x} \frac{1}{n} > \sum_{n \leq x} \frac{1}{n} > \int_{1}^{x} \frac{1}{n} = \log x.$$  

By the Lemma and because clearly $r = \pi(\xi) \leq \xi$, we have

$$\pi(x) \leq \xi + 2^r + \frac{x}{\log \xi}$$

for all $\xi$. Choose $\xi = K \log x$ for $K > 0$ to be chosen later. Then $2^r = x^{K \log 2}$ so we get

$$\pi(x) \leq K \log x + x^{K \log 2} + \frac{x}{\log \log x + \log \log K}$$

so

$$\pi(x) \leq K \log x + x^{K \log 2 - 1} + \frac{1}{\log \log x + \log \log K}.$$  

If $K > 0$ and $K \log 2 - 1 < 0$ (that is we can choose $K < 1/\log 2$) then clearly the right hand side goes to 0 as $x \to \infty$. 

■
Chapter 11

Primitive Elements

Lemma 11.1. Let $F$ be a field and consider an equation for $x \in F$:

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

where $a_i \in F$. This equation has at most $n$ solutions.

Proof. There is Euclid's algorithm in $F[x]$, that is for $f(x), g(x) \in F[x]$, there exists $q(x), r(x) \in F[x]$ such that $f(x) = g(x)q(x) + r(x)$ with $\deg r(x) < \deg g(x)$.
We can show that if $b \in F$ is a root of $f(x)$, then $x - b | f(x)$.

If $f(x) = 0$ has a solution $b$, then $f(x) = (x - b)g(x)$ with $\deg g(x) = \deg f(x) - 1$. We can continue by induction. ■

Theorem 11.2. For $p$ prime, $\mathbb{Z}/p\mathbb{Z}^\times$ is a cyclic group (of order $p - 1$).

Proof. $G = \mathbb{Z}/p\mathbb{Z}^\times$ has order $n = p - 1$. Every element in $G$ satisfies the polynomial equation $x^n - 1 = 0$.

We claim that if $d | n$ then the equation $x^d - 1 = 0$ has exactly $d$ solutions. We have

$$x^n - 1 = (x^d - 1)(1 + x^d + x^{2d} + \cdots + x^{d(d - 1)})$$

where $n = dd'$. The left hand side has $n$ roots. Clearly $x^d - 1$ has at most $d$ roots and $1 + x^d + \cdots + x^{d(d - 1)}$ has at most $d d' - d = n - d$ roots. Hence $x^d - 1$ has exactly $d$ roots.

For $d | n$ denote

$$\psi(d) = \# \{ a \in \mathbb{Z}/p\mathbb{Z}^\times \mid o(a) = d \}.$$

We claim that $\psi(d) = \varphi(d)$. Then since $\varphi(n) \neq 0$, there are elements of order $n$ and hence $\mathbb{Z}/p\mathbb{Z}^\times$ is cyclic and the theorem will follow from this claim. We prove it by induction on $d$: If $d = 1$, then $\psi(1) = 1 = \varphi(1)$. Assume the claim is true for $d' < d$. Then the roots of $x^d - 1$ are the elements of $G$ of order $d' | d$. Hence (by the previous claim)

$$\sum_{d' | d} \psi(d') = d.$$

On the other hand we know that

$$\sum_{d' | d} \varphi(d') = d.$$

Putting these together and using the induction hypothesis, we get

$$d = \psi(d) + \sum_{d' | d, d' \neq d} \psi(d')$$

$$= \psi(d) + \sum_{d' | d, d' \neq d} \varphi(d'),$$

$$d = \varphi(d) + \sum_{d' | d, d' \neq d} \varphi(d').$$

Hence $\varphi(d) = \psi(d)$. ■
Definition 11.3. A number \( g \in \mathbb{Z}/p\mathbb{Z}^\times \) is a **primitive element** if \( g \) is a generator of \( \mathbb{Z}/p\mathbb{Z}^\times \).

Definition 11.4. Let \( a \in \mathbb{Z}/p\mathbb{Z}^\times \) and \( g \) be a primitive element of \( \mathbb{Z}/p\mathbb{Z}^\times \). If \( a = g^k \), then define the **index** of \( a \) \( I_g(a) \) to be \( k \).

**Note.** Note that \( I(a) \) is defined with respect to a specific primitive root. Note also that \( I(a) \) is defined modulo \( p - 1 \). Also note that \( I \) is a homomorphism from \((\mathbb{Z}/p\mathbb{Z}^\times, \times) \) to \((\mathbb{Z}/(p - 1)\mathbb{Z}, +) \); similarly to \( \log \) being a homomorphism from \((\mathbb{R} \setminus \{0\}, \times) \) to \((\mathbb{R}, +) \). Therefore the index is sometimes called the **discrete logarithm**.

Example 11.5. Take \( \mathbb{Z}/13\mathbb{Z}^\times \) and its primitive root \( g = 2 \).

<table>
<thead>
<tr>
<th>( a )</th>
<th>( I_g(a) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>9</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>11</td>
</tr>
<tr>
<td>7</td>
<td>3</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>10</td>
<td>7</td>
</tr>
<tr>
<td>11</td>
<td>6</td>
</tr>
</tbody>
</table>

**Lemma 11.6 (Properties of \( I \)).** For \( a \in \mathbb{Z}/p\mathbb{Z}^\times \)

(i) \( I(ab) = I(a) + I(b) \mod p - 1 \) (i.e. \( I \) is a homomorphism from the multiplicative group mod \( p \) to the additive group mod \( p - 1 \)),

(ii) \( I(a^k) = kI(a) \).

**Proof.** If \( a = g^k \) and \( b = g^l \) with \( g \) a primitive element of \( \mathbb{Z}/p\mathbb{Z}^\times \), then \( I(ab) = kl = I(a)I(b) \). Part (ii) is a special case. ■

### 11.1 Solving linear congruences

We will look at a method to find solutions to equations of the form \( ax \equiv b \mod m \). Recall that this equation has a solution if and only if \( \text{hcf}(a, m) \) divides \( b \).

**Example 11.7.** We want to solve \( 5x \equiv 9 \mod 13 \). We get (with respect to primitive root 2)

\[
I(5) + I(x) \equiv I(9) \mod 12 \\
9 + I(x) \equiv 8 \mod 12 \\
I(x) \equiv 11 \mod 12 \\
x \equiv 7 \mod 12.
\]

**Example 11.8.** We want to solve \( 3x^{30} \equiv 10 \mod 13 \). We have

\[
I(3) + 30I(x) \equiv I(10) \mod 12 \\
4 + 30I(x) \equiv 10 \mod 12 \\
6I(x) \equiv 6 \mod 12.
\]

The solutions for \( I(x) \) are 1, 3, 5, 7, 9, 11 and so \( x \) can be 2, 8, 9, 11, 5, 7.
Chapter 12

Quadratic Reciprocity

Let \( p \) be a prime.

**Definition 12.1.** A number \( a \in \mathbb{Z}/p\mathbb{Z}^\times \), \( p \nmid a \) is a **quadratic residue** mod \( p \) if the equation \( x^2 \equiv a \mod p \) has a solution. Otherwise \( a \) is a **non-residue**.

Consider the field \( \mathbb{Q} \) of rational numbers. We know that \( x^2 = 2 \) and \( x^2 = -1 \) are not soluble in \( \mathbb{Q} \). In any field, it is interesting to ask if a given polynomial equation \( f(x) = 0 \) has a solution. The equation \( x^2 \equiv a \mod p \) is the simplest such equation in \( \mathbb{Z}/p\mathbb{Z} \).

**Definition 12.2.** Let \( p \) be a prime. The **Legendre symbol** is

\[
\left( \frac{a}{p} \right) = \begin{cases} 
+1 & \text{if } p \nmid a \text{ and } a \text{ is a quadratic residue}, \\
-1 & \text{if } p \nmid a \text{ and } a \text{ is a non-residue}, \\
0 & \text{if } p | a.
\end{cases}
\]

Quadratic reciprocity gives an efficient method to calculate the Legendre symbol.

**Proposition 12.3.** The Legendre symbol \( \left( \frac{\cdot}{p} \right) \) as a function \( \mathbb{Z}/p\mathbb{Z}^\times \to \{\pm 1\} \) is a group homomorphism, that is for \( a_1, a_2 \in \mathbb{Z}/p\mathbb{Z}^\times \)

\[
\left( \frac{a_1 a_2}{p} \right) = \left( \frac{a_1}{p} \right) \left( \frac{a_2}{p} \right).
\]

**Proof.** Clearly \( a \) is a quadratic residue (QR) iff \( I(a) \) is even: if \( x^2 \equiv a \mod p \) has a solution \( b \), then \( I(a) = I(b^2) = 2I(b) \). If \( I(a) = 2k \), then \( a = g^{2k} \) for a primitive element \( g \) and so \( b = g^k \) satisfies \( x^2 \equiv a \mod p \). The rest follows easily.

**Remark 12.4.** The proposition holds if \( a_1 \) or \( a_2 \) is divisible by \( p \). In particular, if \( n = a_1^{r_1} a_2^{r_2} \cdots a_k^{r_k} \), then

\[
\left( \frac{n}{p} \right) = \left( \frac{a_1^{r_1}}{p} \right) \cdots \left( \frac{a_k^{r_k}}{p} \right).
\]

**Theorem 12.5** (Euler’s criterion). Let \( p \) be an odd prime. Then

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

**Proof.** If \( a \equiv g^k \) for \( g \) a primitive element of \( \mathbb{Z}/p\mathbb{Z}^\times \) then \( a^{\frac{p-1}{2}} = (-1)^k \).

**Theorem 12.6.** Let \( p \) be an odd prime. Then

\[
\left( \frac{-1}{p} \right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 
1 & \text{if } p \equiv 1 \mod 4, \\
-1 & \text{if } p \equiv 3 \mod 4.
\end{cases}
\]
Proof. An immediate consequence of Euler’s criterion. Let \( g \) be a primitive element of \( \mathbb{Z}/p\mathbb{Z}^\times \). Then \( g^{p-1} = 1 \), so \( I(-1) = \frac{p-1}{2} \).

**Theorem 12.7.** Let \( p \) be an odd prime. Then

\[
\left( \frac{2}{p} \right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 
1 & p \equiv 1,7 \mod 8, \\
-1 & p \equiv 3,5 \mod 8.
\end{cases}
\]

**Proof.** The idea is to calculate \( 2 \cdot 4 \cdot 6 \cdots (p-1) \) in two different ways. The first way: let \( P = \frac{p^2-1}{2} \). Then

\[
2 \cdot 4 \cdots (p-1) = (2 \cdot 1)(2 \cdot 2) \cdots (2 \cdot P)
\]

\[
= 2P P!.
\]

The second way: divide \( 2,4,\ldots,(p-1) \) into two groups of numbers greater than and less or equal to \( P \). The greater ones (\( l \) of them), are all negative odd numbers greater than or equal to \( -P \) modulo \( p \). Hence

\[
2 \cdot 4 \cdot 6 \cdots (p-1) \equiv (-1)^l P! \mod p.
\]

Note also that by Euler’s criterion, \( 2^P \equiv \left( \frac{2}{p} \right) \mod p \). We have

\[
2P P! \equiv (-1)^l P! \mod p \\
\left( \frac{2}{p} \right) \equiv 2^P \equiv (-1)^l \mod p.
\]

We now need to find \( l \). There are 4 cases:

If \( p = 8k+1 \), then the two groups of factors are \( 2,4,\ldots,4k \) and \( (4k+2),\ldots,(8k) \) and so \( l = 2k \) and \( \left( \frac{2}{p} \right) = 1 \).

If \( p = 8k+3 \), then the two groups of factors are \( 2,4,\ldots,4k \) and \( (4k+2),\ldots,(8k+2) \) and so \( l = 2k+1 \) and \( \left( \frac{2}{p} \right) = -1 \).

If \( p = 8k+5 \), then the two groups of factors are \( 2,4,\ldots,4k+2 \) and \( (4k+4),\ldots,(8k+4) \) and so \( l = 2k+1 \) and \( \left( \frac{2}{p} \right) = -1 \).

If \( p = 8k+7 \), then the two groups of factors are \( 2,4,\ldots,4k+2 \) and \( (4k+4),\ldots,(8k+6) \) and so \( l = 2k+2 \) and \( \left( \frac{2}{p} \right) = 1 \).

**Theorem 12.8** (Law of Quadratic Reciprocity, First statement). Let \( p_1, p_2 \) be two primes such that \( p_1 \mid a, p_2 \mid a \) and \( p_1 = 4am_1 + r_1, p_2 = 4am_2 + r_2 \). If \( r_1 = r_2 \) or \( r_1 = 4a - r_2 \) then \( \left( \frac{a}{p_1} \right) = \left( \frac{a}{p_2} \right) \).

**Theorem 12.9** (Law of Quadratic Reciprocity, Second statement). Let \( p, q \) be odd primes. Then

\[
\left( \frac{p}{q} \right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \left( \frac{q}{p} \right) = \begin{cases} 
-\left( \frac{q}{p} \right) & \text{if } p \equiv 3 \mod 4 \text{ and } q \equiv 3 \mod 3, \\
\left( \frac{q}{p} \right) & \text{otherwise.}
\end{cases}
\]

**Proof.** We will show this using the First statement. Assume \( p > q \). If \( p \equiv q \mod 4 \) then \( p = 4a + q \) and

\[
\left( \frac{p}{q} \right) = \left( \frac{4a + q}{q} \right) = \left( \frac{4a}{q} \right) \left( \frac{1}{q} \right) = \left( \frac{a}{q} \right) \left( \frac{1}{q} \right).
\]

Also

\[
\left( \frac{q}{p} \right) = \left( \frac{p-4a}{p} \right) = \left( \frac{-4a}{p} \right) = \left( -1 \right) \left( \frac{a}{p} \right) = (-1)^{\frac{p-1}{2}} \left( \frac{a}{p} \right).
\]

Now \( \left( \frac{q}{p} \right) = \left( \frac{a}{p} \right) \), because \( p \equiv q \mod 4a \) (by the First statement).
If \( p \equiv -q \mod 4 \) then

\[
\left( \frac{p}{q} \right) = \left( \frac{-q + 4a}{q} \right) = \left( \frac{4a}{q} \right) = \left( \frac{a}{q} \right),
\]

\[
\left( \frac{q}{p} \right) = \left( \frac{-p + 4a}{p} \right) = \left( \frac{4a}{p} \right) = \left( \frac{a}{p} \right).
\]

Now \( \left( \frac{a}{p} \right) = \left( \frac{a}{q} \right) \) because \( p \equiv -q \mod 4 \) (from the First statement). ■

**Remark 12.10.** The second statement allows us to calculate \( \left( \frac{a}{p} \right) \) but not efficiently, since it still requires factorization of \( a \).

**Example 12.11.**

\[
\left( \frac{14}{137} \right) = \left( \frac{2}{137} \right) \left( \frac{7}{137} \right) = \left( \frac{137}{7} \right) = \left( \frac{4}{7} \right) = 1
\]

since \( 137 \equiv 1 \mod 8 \).

\[
\left( \frac{299}{397} \right) = \left( \frac{-98}{397} \right) = \left( \frac{-1}{397} \right) \left( \frac{2}{397} \right) \left( \frac{7}{397} \right)^2 = -1.
\]

\[
\left( \frac{55}{179} \right) = \left( \frac{5}{179} \right) \left( \frac{11}{179} \right) = \frac{179}{5} \left( -1 \right) \frac{179}{11} = \left( \frac{4}{5} \right) \left( \frac{3}{11} \right) = \left( \frac{11}{3} \right) \left( \frac{2}{3} \right) = -1
\]

since \( \left( \frac{3}{2} \right) = -1 \frac{3}{1} = -1 \).

**Proof of First statement.** Let \( P = \frac{p - 1}{2} \). We write the product \( a(2a) \cdots (Pa) \) modulo \( p \) in two different ways. First, we need the following lemma.

**Lemma 12.12 (Gauss Lemma).** Let \( p \) be an odd prime and \( a \) an integer, \( p \nmid a \). For \( j = 1, 2, \ldots, P \) let \( a_j \) be the unique integer such that \(-\frac{p}{2} < a_j < \frac{p}{2}\) and \( a_j \equiv j a \mod p \). Let \( l(a) = \# \{ a_j \mid a_j < 0 \} \). Then

\[
\left( \frac{a}{p} \right) = (-1)^{l(a)}.
\]

**Proof.** Note that \( a_{j_1} = a_{j_2} \) means that \( j_1 a \equiv j_2 a \mod p \) and so \( p \mid (j_1 - j_2) a \) and so \( j_1 = j_2 \). If \( a_{j_1} = -a_{j_2}, j_1 a \equiv -j_2 a \mod p \) and so \( p \mid j_1 + j_2 < p \), impossible. Hence each of \( \{ 1, 2, \ldots, p \} \) occurs exactly once in \( \{ a_j \mid j = 1, 2, \ldots, P \} \) and with a unique sign.

Hence \( a(2a)(3a) \cdots (Pa) = a^p P! = (-1)^{l(a)} P! \) and so \( a^P = \left( \frac{a}{p} \right) = (-1)^{l(a)} \).


**Lemma 12.13.**

1. If \( a, \beta \in \mathbb{R}, a \in \mathbb{Z} \), then

   \[
   \text{number of integers in } [a, \beta] = \{ t \in \mathbb{Z} \mid a \leq t \leq \beta \} = |\beta| - |a|.
   \]

2. If \( n_1, n_2 \in \mathbb{Z} \), then the numbers of integers in \([a, \beta]\) and in \([2n_1 + a, 2n_2 + \beta]\) have the same parity.
Now we can study $l(a)$. We only need to know its parity.

We get that $l(a)$ is the number of integers in the intervals $\left[ \frac{r}{2a}, \frac{r}{a} \right]$, $\left[ \frac{3r}{2a}, \frac{2r}{a} \right]$, $\left[ \frac{8r}{2a}, \frac{7r}{a} \right]$, $\left[ \frac{14r}{2a}, \frac{13r}{a} \right]$, ... Now we use the previous lemma on these intervals, since their end points are never integers.

Write $p = 4am + r$. Then $l(a)$ is the number of integers in intervals

$$\left[ 2m + \frac{r}{2a}, 4m + \frac{r}{a} \right], \left[ 6m + \frac{3r}{2a}, 8m + \frac{2r}{a} \right], \ldots, \left[ 2(2b - 1)m + \frac{(2b - 1)r}{2a}, 4bm + \frac{br}{a} \right],$$

which has the same parity, by the Lemma part (2), as the number of integers in the intervals

$$\left[ \frac{r}{2a}, \frac{r}{a} \right], \left[ \frac{3r}{2a}, \frac{2r}{a} \right], \left[ \frac{7r}{2a}, \frac{6r}{a} \right], \ldots, \left[ \frac{2b - 1}{a}, \frac{br}{a} \right].$$

If $p = 4am - r$, then $l(a)$ is the number of integers in the intervals

$$\left[ -\frac{r}{2a}, -\frac{r}{a} \right], \left[ -\frac{3r}{2a}, -\frac{2r}{a} \right], \ldots,$$

which is by the Lemma part (1) (showing only for the first interval)

$$\left[ -\frac{r}{2a} \right] - \left[ -\frac{r}{a} \right] = -\left[ \frac{r}{2a} \right] + \frac{r}{\gcd(r, a)} = \left[ \frac{r}{\gcd(r, a)} \right] + 1 = \frac{r}{\gcd(r, a)} - \frac{r}{2a},$$

the number of integers in $\left[ \frac{r}{2a}, \frac{r}{a} \right]$. Hence the result does not depend on the sign of $r$. ■

**Definition 12.14.** Let $n > 0$ and odd $a \in \mathbb{Z}$. Write $n = \prod p_i^{e_i}$ for $p_i$ prime and $a_i \in \mathbb{Z}$, $a_i \geq 0$. Define the **Jacobi symbol**

$$\left( \frac{a}{n} \right) = \prod \left( \frac{a}{p_i} \right)^{e_i}.$$

**Remark 12.15.**

1. $\left( \frac{a}{n} \right) = 0$ if $\gcd(a, n) > 1$.

2. Assume $\gcd(a, n) = 1$. If $x^2 \equiv a \mod n$ is soluble, then $x^2 \equiv a \mod p_i$ is soluble for all $i$ and so $\left( \frac{a}{n} \right) = 1$.

3. However $\left( \frac{a}{n} \right) = 1$ does not mean that $x^2 \equiv a \mod n$ is soluble. For example consider $\left( \frac{2}{15} \right) = \left( \frac{2}{3} \right) \left( \frac{2}{5} \right) = (-1)(-1) = 1$. But clearly $x^2 \equiv 2 \mod 15$ is not soluble.

**Theorem 12.16** (Properties of the Jacobi Symbol).

1. $\left( \frac{a}{n} \right)$ only depends on $a \mod n$.

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

3. $\left( \frac{a}{nm} \right) = \left( \frac{a}{n} \right) \left( \frac{a}{m} \right)$.

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

5. (Quadratic Reciprocity for Jacobi symbol) If $a, n > 0$ are both odd, then

$$\left( \frac{a}{n} \right) = (-1)^{\frac{n - 1}{2} \cdot \frac{a - 1}{2}} \left( \frac{n}{a} \right) \left( \frac{a}{n} \right) \left( \frac{a}{n} \right)$$

if $n, a \equiv 3 \mod 4$, otherwise.
The key point is that we can calculate \( \left( \frac{a}{n} \right) \) using properties 1 to 5 without having to factorise either \( a \) or \( n \).

**Example 12.17.**

\[
\left( \frac{3421}{5693} \right) = \left( \frac{-2272}{5693} \right) = \left( \frac{-1}{5693} \right) \left( \frac{2272}{5693} \right) = \left( \frac{-1}{5693} \right) \left( \frac{2}{5693} \right)^3 \left( \frac{71}{5693} \right) = \left( \frac{-1}{5693} \right) \left( \frac{13}{71} \right) = \left( \frac{-1}{71} \right) = \left( \frac{-6}{71} \right) = \left( \frac{2}{13} \right) \left( \frac{3}{13} \right) = \left( \frac{3}{13} \right) = \left( \frac{13}{3} \right) = \left( \frac{1}{3} \right) = 1.
\]

**Proof.**

(1) Easy by Chinese Remainder Theorem.

(2) Obvious.

(3) The function \( c(n) = (-1)^{\frac{n-1}{2}} \) is multiplicative; we need to show that \( \frac{nm-1}{2} \equiv \frac{n-1}{2} + \frac{m-1}{2} \) mod 2 for \( n, m \) such that \( \text{hcf}(n, m) = 1 \). That is

- \( nm - 1 \equiv n - 1 + m - 1 \) mod 4
- \( nm - n - m + 1 \equiv 0 \) mod 4
- \( (n-1)(m-1) \equiv 0 \) mod 4.

This is true as \( n, m \) are both odd. Now we check that \( \left( \frac{-1}{n} \right) = c(n) \). Write \( n = \prod p_i^{a_i} \). By definition, \( \left( \frac{-1}{n} \right) = \prod \left( \frac{-1}{p_i} \right)^{a_i} \). The result follows by the properties of Legendre symbol and multiplicativity of \( c(n) \).

(4) Similar to (3). Now choose function \( \gamma(n) = (-1)^{\frac{n^2-1}{8}} \).

(5) Let \( n = q_1 q_2 \cdots q_r \) and \( a = p_1 p_2 \cdots p_s \) with \( q_i, p_i \) not necessarily distinct primes. We have

\[
\left( \frac{a}{n} \right) = \prod \left( \frac{p_i}{q_j} \right),
\]

\[
\left( \frac{n}{a} \right) = \prod \left( \frac{q_i}{p_j} \right).
\]

Applying Quadratic Reciprocity for Legendre symbol, we get

\[
\left( \frac{a}{n} \right) = (-1)^{t} \left( \frac{n}{a} \right)
\]

where \( t = uv \) with \( u, v \) the number of primes within \( p_i, q_j \) respectively equal to 3 mod 4.

We have \( u \) odd iff \( a \equiv 3 \) mod 4 and \( v \) odd iff \( n \equiv 3 \) mod 4.
Chapter 13

Sums of squares

What integers \( n > 0 \) can be written as \( n = a^2 + b^2 \) for \( a, b \in \mathbb{Z} \)?

**Remark 13.1.** For \( u, v, A, B \in \mathbb{R} \), we have

\[
(u^2 + v^2)(A^2 + B^2) = (uA + vB)^2 + (vA - uB)^2.
\]

Using this remark, we can look at a simpler question of what primes can be written as sum of two squares.

**Theorem 13.2.** An odd prime \( p \) can be written as a sum of two squares if and only if \( p \equiv 1 \mod 4 \).

**Proof.**

\(\Rightarrow\) Assume \( a^2 + b^2 \equiv 0 \mod p \). Note that \( p \) does not divide \( a, b \). We get \( (\frac{a}{b})^2 + 1 \equiv 0 \mod p \) and hence \( (\frac{-1}{p}) = 1 \) and so \( p \equiv 1 \mod 4 \).

\(\Leftarrow\) Assume \( p \equiv 1 \mod 4 \). The method of this proof is called Fermat descent. We can write \( A^2 + B^2 = M \) \( p \) with \( 1 \leq M < p \). Because \( (\frac{-1}{p}) = 1 \), there exists \( A \) such that \( A^2 \equiv -1 \mod p \), that is \( A^2 + 1 = Mp (B = 1) \) for some \( M \). We can assume that \( 0 < A < p/2 \) (otherwise we can take \( p - A \)) so that \( A^2 + 1 < \frac{p^2}{4} + 1 < p^2 \).

If \( M = 1 \), we are done. Otherwise we will try to find a solution with smaller \( M \). Choose \( u, v \) with \( -\frac{1}{2} < M < u, v \leq \frac{1}{2} M \) and

\[
\begin{align*}
 u &\equiv A \mod M, \\
 v &\equiv B \mod M.
\end{align*}
\]

Clearly \( u^2 + v^2 \equiv A^2 + B^2 \mod M \). Therefore \( u^2 + v^2 = r M \) for \( r < M \) (since \( u^2 + v^2 \leq \frac{M^2}{4} + \frac{M^2}{4} = \frac{M^2}{2} \)). Multiply to get

\[
(u^2 + v^2)(A^2 + B^2) = (uA + vB)^2 + (vA - uB)^2 = M^2 r p.
\]

Now \( uA + vB \equiv A^2 + B^2 \equiv 0 \mod M \) and also \( vA - uB \equiv BA - AB \equiv 0 \mod M \) and hence

\[
\left(\frac{uA + vB}{M}\right)^2 + \left(\frac{vA - uB}{M}\right)^2 = r p
\]

with \( r < M \). Repeat until \( M = 1 \).

**Example 13.3.** Write \( p = 317 \) as a sum of two squares. We want \( A^2 + B^2 \equiv 0 \mod p \). We know that there exists \( A \) such that \( A^2 \equiv -1 \mod p \), i.e. \( A^2 + 1 = Mp \) for some \( M \). We can check that \( 2^{\frac{p-1}{2}} \) is a square root of \(-1\) modulo 317. We get \( 2^{79} \equiv 203 \mod 317 \). Now \( 203^2 + 1^2 = 130 \times 317 \). We need to
find \( u, v \) such that \(-65 \leq u, v \leq 65\) and \( u \equiv 203 \mod 130\) and \( v \equiv 1 \mod 130\). Get \( u = -57\) and \( v = 1\). Then \( u^2 + v^2 = 25 \cdot 130\) and so

\[
\left(\frac{203 \cdot (-57) + 1}{130}\right)^2 + \left(\frac{1 \cdot 203 + 57}{130}\right)^2 = 25 \cdot 317
\]

Now \( A = 89, B = 2\) and \( M = 25\). We have \( 89 \equiv -11 \mod 25\) and so

\[
\left(\frac{-11 \cdot 89 + 4}{25}\right)^2 + \left(\frac{2 \cdot 89 + 11 \cdot 2}{25}\right)^2 = 5 \cdot 317
\]

Now \( A = 39\) and \( B = 8\), \( u = -1\) and \( v \equiv -2 \mod 5\) and we get

\[
\left(\frac{-39 - 16}{5}\right)^2 + \left(\frac{-2 \cdot 39 + 8}{5}\right)^2 = 317
\]

\[
11^2 + 14^2 = 317.
\]

**Theorem 13.4.** Let \( n > 0 \) be an integer. Then there exist integers \( a, b \) such that \( n = a^2 + b^2 \) iff for prime \( p \) such that \( p \equiv 3 \mod 4\) and \( p | n \), \( p \) divides \( n \) an even number of times.

**Proof.**

\[ \iff \]

\( n = \prod_{i=1}^{r} p_i \) with \( p_i \) distinct and either \( p_i = 2 \) or \( p_i \equiv 1 \mod 4\). Using the equality

\[
(u^2 + v^2)(A^2 + B^2) = (uA + vB)^2 + (vA - uB)^2
\]

\( r \) times and the previous theorem, we get that \( \prod_{i=1}^{r} p_i \) is a sum of two squares, say \( k^2 + m^2 \). Then

\[ n = (kM)^2 + (mM)^2. \]

\[ \Rightarrow \]

Assume \( n = a^2 + b^2 \). Let \( p \) be odd, \( p | n \). Then \( a^2 + b^2 \equiv 0 \mod p \). If \( p \nmid a \), then \( \left(\frac{b}{a}\right)^2 \equiv -1 \mod p \) and so \( p \equiv 1 \mod 4 \). If \( p | a \), then \( p | b \), i.e. \( a = pa', b = pb' \). Then

\[ n = p^2(a^2 + b^2) = p^2a'^2 + p^2b'^2. \]

Therefore \( p^2 | n \) and also for \( m = a^2 + b^2 \), \( m < \frac{n}{p^2} \). We can assume by induction that \( p \) divides \( m \) an even number of times. Then \( p \) divides \( n = p^2m \) an even number of times.

\[ \blacksquare \]

**Example 13.5.** Let \( n = 1105 = 5 \cdot 13 \cdot 17 \). Then

\[ n = 5 \cdot 13 \cdot 17 \]

\[ = (2^2 + 1^2)(3^2 + 2^2)(4^2 + 1^2) \]

\[ = [(3 \cdot 2 + 1)^2 + (3 \cdot 1 - 2 \cdot 2)^2](4^2 + 1^2) \]

\[ = (8^2 + 1^2)(4^2 + 1^2) \]

\[ = (8 \cdot 4 + 1 \cdot 1)^2 + (1 \cdot 4 - 1 \cdot 8)^2 \]

\[ = 33^2 + (-4)^2 \]

\[ = 33^2 + 4^2. \]

**Note.** Let \( p \equiv 1 \mod 4 \). Then \( p = a^2 + b^2 \) for some integers \( a, b \). We can write this in \( \mathbb{C} \) as \( p = (a + ib)(a - ib) \).
13. SUMS OF SQUARES

**Definition 13.6.** Define the ring Gaussian integers \( \mathbb{Z}[i] \) as

\[
\mathbb{Z}[i] = \{a + i\beta \mid a, \beta \in \mathbb{Z}\}.
\]

**Definition 13.7.** Define the norm in \( \mathbb{Z}[i] \) to be \( N(a + i\beta) : \mathbb{Z}[i] \setminus \{0\} \to \mathbb{N} \setminus \{0\} \)

\[
N(a + i\beta) = a^2 + \beta^2.
\]

Note that \( N(ab) = N(a)N(b) \) for all \( a, b \in \mathbb{Z}[i] \setminus \{0\} \).

**Theorem 13.8** (The Euclidean Algorithm in Gaussian integers). For all \( a, b \in \mathbb{Z}[i] \), \( b \neq 0 \), there exist \( q, r \in \mathbb{Z}[i] \) with \( a = bq + r \) and \( N(r) < N(b) \).

**Remark 13.9.** The ring \( \mathbb{Z}[\sqrt{-5}] \) has norm \( N(a + i\sqrt{5}) = a^2 + 5\beta^2 \) but it does not have the Euclidean Algorithm.

**Lemma 13.10.** Let \( \mathbb{Q}(i) = \{a + i\beta \mid a, \beta \in \mathbb{Q}\} \). Given \( \gamma = a + i\beta \in \mathbb{Q}(i) \), there exists \( c = a + ib \in \mathbb{Z}[i] \) such that \( N(\gamma - c) \leq 1/2 \).

**Proof.** Obvious: take \( c \) to be the nearest Gaussian integer to \( \gamma \). Then \( N(\gamma - c) \leq (1/2)^2 + (1/2)^2 = 1/2 \).

**Proof of the Theorem.** Observe that \( \mathbb{Q}(i) \) is a field. If \( x = a + i\beta \in \mathbb{Q}(i) \) and \( y = a + ib \in \mathbb{Q}(i) \setminus \{0\} \) then \( x/y \) makes sense:

\[
\frac{a + i\beta}{a + ib} = \frac{(a + i\beta)(a - ib)}{(a + ib)(a - ib)} = \frac{(aa - \beta b) + i(-ab + \beta a)}{a^2 + b^2} \in \mathbb{Q}(i).
\]

Now let \( a = a_1 + ia_2 \in \mathbb{Z}[i] \) and \( b = \beta_1 + i\beta_2 \neq 0 \in \mathbb{Z}[i] \). Then \( a/b \in \mathbb{Q}(i) \). By the previous Lemma, there exists \( q \) such that \( N(a/b - q) \leq 1/2 \). Now define \( r \in \mathbb{Z}[i] \) such that \( a = bq + r \). We claim that \( N(r) < N(b) \): We have

\[
r = b\left(\frac{a}{b} - q\right)
\]

\[
N(r) = N(b)N\left(\frac{a}{b} - q\right) \leq \frac{1}{2}N(b) < N(b).
\]

**Definition 13.11.** A \( u \in \mathbb{Z}[i] \) is a unit if there exists \( v \in \mathbb{Z}[i] \) such that \( uv = 1 \). Denote the set of all units in \( \mathbb{Z}[i] \) by \( \mathbb{Z}[i]^\times \).

Note that if \( u \) is a unit, from \( uv = 1 \) we have \( N(u)N(v) = N(1) \) and hence \( N(u) = 1 \) and so \( u \) can be \( \pm 1 \) or \( \pm i \) (all are clearly units).

**Example 13.12.** We find \( \text{hcf}(\alpha, \beta) = \text{hcf}(4 + 10i, -1 + 9i) \) using the Euclidean algorithm. We have \( N(4 + 10i) = 116 \) and \( N(-1 + 9i) = 82 \). We first divide in \( \mathbb{Q}(i) \):

\[
\frac{-4 + 10i}{1 - 9i} = \frac{(4 - 90) + (36 + 10)i}{82} = \frac{43 - 23i}{41}.
\]

Now the nearest \( q \) in \( \mathbb{Z}[i] \), i.e. \( q = 1 - i \). Define

\[
r = \alpha - q\beta = 4 + 10i - (1 - i)(-1 + 9i)
= -4.
\]

Euclidean algorithm says that \( \text{hcf}(4 + 10i, -1 + 9i) = \text{hcf}(-1 + 9i, -4) \). Continuing in this fashion, we get \( \text{hcf}(4 + 10i, -1 + 9i) = 1 + i \).
13.1 Fundamental Theorem in \( \mathbb{Z}[i] \)

**Definition 13.13.** Call \( \alpha \in \mathbb{Z}[i] \) an **irreducible** if for all \( \beta \in \mathbb{Z}[i] \), \( \beta|\alpha \) implies either \( \beta = u \in \mathbb{Z}[i]^* \) or \( \frac{\alpha}{\beta} = u \in \mathbb{Z}[i]^* \). A non-unit \( \pi \in \mathbb{Z}[i] \) is a **prime** if \( \pi|\alpha \beta \) implies \( \pi|\alpha \) or \( \pi|\beta \).

The existence of Euclidean algorithm in \( \mathbb{Z}[i] \) implies that all primes in \( \mathbb{Z}[i] \) are also irreducibles.

**Theorem 13.14.** The primes in \( \mathbb{Z}[i] \) are
- \( \pi = 1 + i \),
- integer primes \( p \equiv 3 \mod 4 \),
- of the form \( a + ib \) where \( a^2 + b^2 = p \) is an integer prime, \( p \equiv 1 \mod 4 \).

**Remark 13.15.** In the proof we do not use the fact that \( p \equiv 1 \mod 4 \) implies \( p \) is a sum of two squares. Therefore, in part, we get another proof of this. This new proof will not be explicit as it will not show how to find \( a, b \) such that \( p = a^2 + b^2 \), but it will say that \( a, b \) are “essentially unique” (all other solutions are \( \pm a, \pm b \)).

**Proof.** Let \( p \in \mathbb{Z} \) be an integer prime. Assume \( p \) is not prime in \( \mathbb{Z}[i] \). Then there exists a prime \( \pi \in \mathbb{Z}[i] \) such that \( \pi|p \). Therefore \( N(\pi)|N(p) = p^2 \) and therefore \( N(\pi) = p \). If \( N(\pi) = 1, \pi \) is a unit, a contradiction. If \( N(\pi) = p^2 \), then \( N\left(\frac{\pi}{p}\right) = 1 \) and so \( p \) is a unit, a contradiction.

If \( \pi = a + ib \) then \( N(\pi) = a^2 + b^2 = p \). Hence \( p \) is a sum of two squares and so \( p \equiv 1 \mod 4 \). This shows that if prime \( p \equiv 3 \mod 4 \), then \( p \) is also a prime in \( \mathbb{Z}[i] \).

Now we show that \( \pi = a + ib \) with \( a^2 + b^2 = p \) integer prime \( \mod 4 \) is a prime in \( \mathbb{Z}[i] \). Let \( \rho \in \mathbb{Z}[i] \) be a prime such that \( \rho|\pi \). Then \( N(\rho)|N(\pi) = p \), so \( N(\rho) = p \) (otherwise \( \rho \) is a unit). Therefore \( N\left(\frac{\pi}{\rho}\right) = 1 \) and hence \( \pi = u\rho \) for \( u \) unit and so \( \pi \) is a prime.

\( 1 + i \) is a prime in \( \mathbb{Z}[i] \): \( N(1 + i) = 2 \)

**Theorem 13.16.** Every \( \alpha \in \mathbb{Z}[i] \) can be expressed as a product

\[
\alpha = \prod_{i=1}^{m} \pi_i^{r_i}
\]

where \( \pi_i \) are primes, in a unique way (up to reordering and units).

**Proof.** Let \( \alpha = x + iy \in \mathbb{Z}[i] \). We will show that there exists a prime \( \pi \in \mathbb{Z}[i] \) of one of the forms described in the theorem above such that \( \pi|\alpha \). Since \( N(\alpha) = x^2 + y^2 \in \mathbb{Z} \), there exists an integer prime \( p \) such that \( p|N(\alpha) \). If \( p = 2 \) then \( 2 = (1 + i)(1 - i)|N(\alpha) = a\bar{a} \). Now either \( 1 + i|\alpha \) or \( 1 + i|\bar{a} \) and then \( 1 - i|\alpha \).

If \( p \equiv 3 \mod 4 \), then \( p \) is a prime in \( \mathbb{Z}[i] \). From \( p|a\bar{a} \) we get \( p|a \) or \( p|\bar{a} \) and then \( p = p|a \).

If \( p \equiv 1 \mod 4 \) then since \( \left(\frac{-1}{p}\right) \) there exist \( A, B \in \mathbb{Z} \) such that \( A^2 + B^2 \equiv 0 \mod p \) with \( \text{hcf}(A, p) = \text{hcf}(B, p) = 1 \), i.e. \( p|A^2 + B^2 = (A + iB)(A - iB) \). We claim that \( p \) is not a prime in \( \mathbb{Z}[i] \): If \( p \) was prime, then either \( p|A + iB \) or \( p|A - iB \) and so \( p|A \) and \( p|B \), a contradiction.

Hence there exists a prime \( \pi \in \mathbb{Z}[i] \) such that \( \pi|p \). As before, we can show that \( N(\pi) = p \) and so \( \pi = a + ib \). \( a^2 + b^2 = p \). So \( \pi|a\bar{a} \). Either \( \pi|a \) or \( \pi|\bar{a} \) and then \( \pi|a \).

**Corollary 13.17.** Let \( p \equiv 1 \mod 4 \) be an integer prime. Then \( p = a^2 + b^2 \) in exactly 8 ways.

**Proof.** These are form all the prime factorizations in \( \mathbb{Z}[i] \), that is

\[
p = (\pm a)^2 + (\pm b)^2 = (\pm b)^2 + (\pm a)^2.
\]

■
Theorem 13.18. Let \( n > 0 \) be an integer and

\[
D_1 = \# \{d | n \mid d \equiv 1 \pmod{4}\}, \\
D_2 = \# \{d | n \mid d \equiv 3 \pmod{4}\}.
\]

Then \( n \) is a sum of two squares in \( 4(D_1 - D_2) \) ways.

Example 13.19. Let \( n = 45 = 3^2 \cdot 5 \). Divisors of \( 45 \) mod 4 are 1, 5, 9, 45 and 3 mod 4 are 3, 15. Therefore the theorem 45 is a sum of two squares in \( 4(4 - 2) = 8 \) ways.

Proof. The proofs uses unique factorization in \( \mathbb{Z}[i] \). By the Fundamental Theorem of Arithmetic, that is every \( n \in \mathbb{Z} \) has a unique factorization in \( \mathbb{Z} \):

\[
n = 2^s p_1^{i_1} \cdots p_r^{i_r} q_1^{i_1} \cdots q_s^{i_s},
\]

where \( p_i \) are primes 1 mod 4 and \( q_j \) are primes 3 mod 4. We know that \( n \) is a sum of two squares iff all the \( f_j \) are even.

We will show that

\[
\# \{ \text{ways to write } n = A^2 + B^2 \} = \begin{cases} 
4(e_1 + 1)(e_2 + 1) \cdots (e_r + 1) & \text{if all } f_j \text{ are even}, \\
0 & \text{otherwise}.
\end{cases}
\]

The unique factorization of \( n \in \mathbb{Z}[i] \) is

\[
n = (-1)^k (1 + i)^{2t} (a_1 + ib_1)^{e_1} (a_2 - ib_2)^{e_2} \cdots (a_r - ib_r)^{e_r} (a_r + ib_r)^{e_r} q_1^{f_1} \cdots q_s^{f_s},
\]

where \( p_i = a_i^2 + b_i^2 \). Say \( n = A^2 + B^2 = (A + iB)(A - iB) \). If \( r \in \mathbb{Z}[i] \) is prime and \( r | n \) then either \( r | A + iB \) and then \( r^2 | A - iB \) or \( r^2 | A + iB \) and then \( r^2 | A - iB \). This means that

\[
A + iB = u(1 + i)^t (a_1 + ib_1)^{x_1} (a_2 - ib_2)^{x_2} \cdots (a_r + ib_r)^{x_r} (a_r - ib_r)^{x_r} q_1^{f_1} \cdots q_s^{f_s}
\]

where \( u \) is a unit and where \( 0 \leq x_i \leq e_i \). We say that \( x^t \) properly divides \( y \) if \( x^t \) divides \( y \) and no higher powers of it divide \( y \). Denote this as \( x^t || y \). The key point is that \( (a_1 + ib_1)^{x_1} || A + iB \) then \( (a_1 + ib_1)^{x_1} || A - iB \). But now \( n = (A + iB)(A - iB) \) and therefore \( (a_1 - ib_1)^{x_1 - x_2} || A + iB \).

We now prove by induction on \( s \) that

\[
4(D_1 - D_2) = \begin{cases} 
4(e_1 + 1)(e_2 + 1) \cdots (e_r + 1) & \text{if all } f_j \text{ are even}, \\
0 & \text{otherwise}.
\end{cases}
\]

If \( s = 0 \) then every odd divisor \( d \) of \( n \) is 1 mod 4, that is

\[
(e_1 + 1) \cdots (e_r + 1) = \# \{ \text{odd divisors of } n = D_1 \}.
\]

Now say that \( n = q^f \cdot m \) where \( q \nmid m \) and \( q \equiv 3 \pmod{4} \). Assume the statement holds for \( m \). We will show it holds for \( n \). If \( f \) is odd then

\[
\{ \text{odd divisors of } n \} = \{ q^f d \mid d \text{ is an odd divisor of } m \text{ for } i = 0, 1, \ldots, f \}.
\]

We have

\[
d \equiv 3 \pmod{4} \Leftrightarrow \begin{cases} 
q^f d \equiv 1 \pmod{4} & \text{if } i = 1, 3, \ldots \text{ and } \\
q^f d \equiv 3 \pmod{4} & \text{if } i = 0, 2, \ldots
\end{cases}
\]

Also

\[
d \equiv 1 \pmod{4} \Leftrightarrow \begin{cases} 
q^f d \equiv 3 \pmod{4} & \text{if } i = 1, 3, \ldots \text{ and } \\
q^f d \equiv 1 \pmod{4} & \text{if } i = 0, 2, \ldots
\end{cases}
\]

So \( D_1 = D_3 \) and \( D_1 - D_3 = 0 \).

If \( f \) is even then

\[
D_1(n) - D_3(n) = \# \{ q^f d \equiv 1 \pmod{4} \} - \# \{ q^f d \equiv 3 \pmod{4} \} = \# \{ d \equiv 1 \pmod{4} \} - \# \{ d \equiv 3 \pmod{4} \}
\]

\[
= D_1(m) - D_3(m) = \begin{cases} 
(e_1 + 1) \cdots (e_r + 1) & \text{if all other } f_j \text{'s are even} \\
0 & \text{otherwise}.
\end{cases}
\]

\[\square\]
13.2 Sums of Three Squares

**Theorem 13.20.** A positive integer \( n \) is the sum of 3 squares if and only if \( n \) is not of the form \( n = 4^i(8m + 7) \).

Proof. We will only prove that if \( n = 4^i(8m + 7) \), then \( n \) is not the sum of 3 squares. We adopt the method of Fermat descent.

Assume that \( t > 0 \) and \( n = a^2 + b^2 + c^2 \equiv 0 \mod 4 \). Therefore \( a^2, b^2, c^2 \equiv 0 \mod 4 \) as \( 0, 1 \) are the only squares mod 4. Say \( a = 2a', b = 2b', c = 2c' \). Then \( \frac{n}{4} = a'^2 + b'^2 + c'^2 \). Apply this argument \( t \) times to get \( N = 8m + 7 = A^2 + B^2 + C^2 \).

Now look at things modulo 8. The only squares mod 8 are 0, 1, 4 and clearly no sum of 3 of them gives 7 mod 8.

13.3 Sums of Four Squares

**Definition 13.21.** The *quaternions* \( Q \) are the (non-commutative) ring of elements of the form \( \alpha = a + bi + cj + dk \), \( a, b, c, d \in \mathbb{Z} \), with the following holding for \( i, j, k \):

\[
\begin{align*}
  i^2 &= j^2 = k^2 = 1, \\
i j &= -ji = k, \\
j k &= -kj = i, \\
k i &= -ik = j.
\end{align*}
\]

A quaternion \( \alpha \) has a *conjugate* \( \bar{\alpha} = a - bi - cj - dk \), and \( a \bar{\alpha} = N(\alpha) = a^2 + b^2 + c^2 + d^2 \).

**Lemma 13.22.** For all \( \alpha, \beta \in \mathbb{Q} \), \( N(\alpha \beta) = N(\alpha)N(\beta) \).

Proof. By explicit computation.

**Corollary 13.23.** If \( M, L \in \mathbb{Q} \) are sums of 4 squares then so is \( ML \).

Proof. Let \( M = x^2 + y^2 + z^2 + w^2 = N(\alpha) \), \( \alpha = x + iy + jz + kw \), and \( L = N(\beta) \), \( \beta = x' + iy' + jz' + kw' \). Let \( \gamma = \alpha \beta = x'' + iy'' + jz'' + kw'' \). By the previous lemma, \( N(\gamma) = x'^2 + y'^2 + z'^2 + w'^2 = N(\alpha)N(\beta) \) with

\[
\begin{align*}
x'' &= xx' + yy' + zz' + ww', \\
y'' &= xy' - yx' + wz' - wz, \\
z'' &= zx' - xz' + yw' - wy, \\
w'' &= zw' - wx' + yz' - zy'.
\end{align*}
\]

**Proposition 13.24.** Every prime can be written as a sum of 4 squares.

Proof. First we need the following:

**Lemma 13.25.** For an odd prime \( p \) there exist integers \( x, y, 0 \leq x, y \leq \frac{p-1}{2} \) such that \( x^2 + y^2 + 1 \equiv 0 \mod p \).

Proof. For \( 0 \leq x \leq \frac{p-1}{2} \), the squares \( x^2 \) lie on different residue classes modulo \( p \); \( x^2 \equiv x^2 \mod p \) iff \((x - z)(x + z) \equiv 0 \mod p \) iff \( x = z \) (since \( x, z \leq \frac{p-1}{2} \)). Similarly for \( 0 \leq y \leq \frac{p-1}{2} \), the numbers \(-1 - y^2 \) all lie in distinct residue classes. The number of possible \( x \) and \( y \)'s is \( \frac{p-1}{2} + 1 \), since there is only \( p \) residue classes, there exist \( x, y \) such that \( x^2 \equiv -1 - y^2 \mod p \) and so \( x^2 + y^2 + 1 \equiv 0 \mod p \).
By the lemma, there exist integers $0 \leq x, y \leq \frac{p-1}{2}$ such that $x^2 + y^2 + 1^2 + 0^2 = Mp$ for some integer $M$ with $0 \leq M < p$.

Now let $1 \leq r < p$ be a minimal integer such that there exist integers $x, y, z, w$ with $x^2 + y^2 + z^2 + w^2 = rp$. If $r = 1$, we are done. Otherwise we aim to find a smaller such $r$: Assume that $r$ is even. Then \( \{x, y, z, w\} \) contains an even number of odd and even elements, say $x, y$ and $z, w$ have the same parity. Then

\[
\frac{x^2 + y^2 + z^2 + w^2}{2} = \left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 + \left(\frac{z+w}{2}\right)^2 + \left(\frac{z-w}{2}\right)^2 = \frac{r}{2}p.
\]

Continuing like this, we get $r$ odd.

Define $a, b, c, d, \frac{l}{2} < a, b, c, d < \frac{r}{2}$ as

\[
a \equiv x \mod r, \\
b \equiv y \mod r, \\
c \equiv z \mod r, \\
d \equiv w \mod r.
\]

We have

\[
a^2 + b^2 + c^2 + d^2 \equiv x^2 + y^2 + z^2 + w^2 \equiv 0 \mod p.
\]

So

\[
a^2 + b^2 + c^2 + d^2 = lr \\
< \frac{r^2}{2} + \frac{r^2}{2} + \frac{r^2}{2} = r^2.
\]

Note that $l \neq 0$, since if $l = 0$, then $a, b, c, d = 0$ and so $r|x, y, z, w$ and $r^2|rp$, that is $r|p$ and $r = 1$; a contradiction.

So $1 \leq l < r$ and

\[
lr^2p = (x^2 + y^2 + z^2 + w^2)(a^2 + b^2 + c^2 + d^2) \\
= (xa + yb + zc + wd)^2 + (xb - ya - zd + wc)^2 + (xc + yd - za - wb)^2 + (xd - yc + zb - wc)^2.
\]

Now

\[
xa + yb + zc + wa \equiv x^2 + y^2 + z^2 + w^2 \equiv 0 \mod r, \\
xb - ya - zd + wc \equiv xy - yx - zw + wz \equiv 0 \mod r, \\
xc + yd - za - wb \equiv xz - yw - zx - wy \equiv 0 \mod r, \\
xd - yc + zb - wa \equiv xw - yz + zy + wx \equiv 0 \mod r.
\]

\[
\left(\frac{xa + yb + zc + wd}{r}\right)^2 + \left(\frac{xb - ya - zd + wc}{r}\right)^2 + \left(\frac{xc + yd - za - wb}{r}\right)^2 + \left(\frac{xd - yc + zb - wa}{r}\right)^2 = lr.
\]

We can continue like this until $r = 1$. 

\[\blacksquare\]
Chapter 14

Liouville’s Theorem

Definition 14.1. A real number \( \alpha \in \mathbb{R} \) is algebraic if \( f(\alpha) = 0 \) for some polynomial \( f(x) \) with coefficients in \( \mathbb{Q} \).

Example 14.2. \( \alpha = \sqrt{2} + \sqrt{3} \) is algebraic since we have \( \alpha^2 = 2 + 2\sqrt{6} \) and so \( \left( \frac{\alpha^2 - 5}{2} \right)^6 = 6 \) and then \( \alpha \) is a root of polynomial \( f(x) \)

\[
f(x) = \left( \frac{x^2 - 5}{2} \right)^2 - 6.
\]

It is true that if \( \alpha, \beta \) are algebraic, so are \( \alpha \beta \), \( \alpha + \beta \) and if \( \beta \neq 0 \), so is \( \frac{\alpha}{\beta} \).

Definition 14.3. If \( \alpha \) is algebraic with \( f(\alpha) = 0 \) the polynomial of minimal degree then the degree of \( \alpha \) is the degree of \( f(x) \).

We say \( \alpha \) is transcendental if \( \alpha \) is not algebraic.

Remark 14.4. The set of algebraic numbers in \( \mathbb{R} \) is countable: \( \mathbb{Q} \) is countable so the set of polynomials with coefficients in \( \mathbb{Q} \) is also countable. Therefore the set of transcendental numbers is uncountable.

Can we make a single explicit transcendental number? It is known that \( e, \pi \) are transcendental. The following theorem allows us to construct many transcendental numbers:

Theorem 14.5 (Liouville’s Theorem). If \( \alpha \) is an algebraic number of degree \( d \), then for all \( D > d \), there are only finitely many rational numbers \( p/q \in \mathbb{Q} \) such that

\[
\left| \frac{p}{q} - \alpha \right| < \frac{1}{q^D}.
\]

Proof. Let \( f(x) = c_0 x^d + c_1 x^{d-1} + \cdots + c_d \) for \( c_i \in \mathbb{Z} \) be a polynomial such that \( f(\alpha) = 0 \). Then \( f(x) = (x - \alpha)g(x) \) with \( g(x) \) a polynomial with real coefficients. Choose

\[
K = \max_{x \in [\alpha - 1, \alpha + 1]} |g(x)|.
\]

Assume that \( \beta = p/q \in \mathbb{Q} \) satisfies the given inequality. Evaluate \( f(\beta) \):

\[
f \left( \frac{p}{q} \right) = \frac{c_0 p^d + c_1 p^{d-1} q + \cdots + c_d q^d}{q^d}.
\]

This is clearly non-zero, otherwise \( \alpha \) would be a root of a polynomial \( g(x) = f(x)/(x - p/q) \) of degree smaller than \( d \). Then

\[
\frac{1}{q^d} \leq \left| \frac{c_0 p^d + c_1 p^{d-1} q + \cdots + q^d}{q^d} \right| = \left| f \left( \frac{p}{q} \right) \right| = \left| \frac{p}{q} - \alpha \right| \left| g \left( \frac{p}{q} \right) \right| < \frac{K}{q^D}
\]

and therefore \( q < K^{1/D} \). \( \blacksquare \)