INTRODUCTION TO NUMBER THEORY

Number Theory is an area of mathematics that studies the properties and relationships of integers. Number theory has fascinated many students and mathematicians because so much of the theory of numbers can be understood without a knowledge of higher mathematics. Number theory has an important applications in information security.

1. Famous Problems in Number Theory

Here are some famous problems in Number Theory:

Goldbach Conjecture: Is every even integer \( n \geq 4 \) a sum of two primes?
Twin Prime Conjecture: Are there infinitely many primes \( p \) such that \( p + 2 \) is also a prime?
Primality Testing: Is there an efficient way to determine whether \( n \) is prime?
Factoring: Given the product of two large primes \( n = p \cdot q \), is there an efficient way to recover the primes \( p \) and \( q \)?

2. Divisibility

Definition 1. Let \( a \) and \( b \) be integers. We say that \( a \) divides \( b \) if there is an integer \( k \) such that \( a \cdot k = b \). The notation for this is \( a | b \).

Example 1. \( 7 | 63 \) because \( 7 \cdot 9 = 63 \).

Note that every number divides zero since \( a \cdot 0 = 0 \) for every integer \( a \).

Definition 2. We say that a number is **perfect** if it equals the sum of its positive integral divisors, excluding itself.

Example 2. \( 6 = 1 + 2 + 3 \) and \( 28 = 1 + 2 + 4 + 7 + 14 \) are perfect numbers.

Lemma 1. The following statements about divisibility hold:

- If \( a | b \), then \( a | b \cdot c \) for all \( c \).
- If \( a | b \) and \( b | c \), then \( a | c \).
- If \( a | b \) and \( a | c \), then \( a | sb + tc \) for all \( s \) and \( t \).
- For all \( c \neq 0 \), \( a | b \) if and only if \( ca | cb \).

3. Greatest Common Divisor

Definition 3. A positive integer \( d \) is called **greatest common divisor** of \( a \) and \( b \) if \( d \) divides both \( a \) and \( b \) and any divisor of \( a \) and \( b \) is also a divisor of \( d \). It is denoted \( \text{gcd}(a, b) \).

Example 3. \( \text{gcd}(18, 24) = 6 \).

Definition 4. If \( \text{gcd}(a, b) = 1 \), then we say that \( a \) and \( b \) are **relatively prime**.
Lemma 2. The following statements about the greatest common divisor hold:

- Every common divisor of $a$ and $b$ divides $\gcd(a, b)$.
- $\gcd(ka, kb) = k \cdot \gcd(a, b)$ for all $k > 0$.
- If $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$, then $\gcd(a, bc) = 1$.
- If $a|bc$ and $\gcd(a, b) = 1$, then $a|c$.
- If $a, b \in \mathbb{N}$ and $b = a \cdot q + r$, then $\gcd(a, b) = \gcd(a, r)$.

4. Euclidean algorithm for finding $\gcd(a, b)$

Example 4. Computing the greatest common divisor of 1147 and 899:

\[ \gcd(1147, 899) = \gcd(899, \underbrace{248}_{1147=1 \cdot 899+248}) \]

\[ = \gcd(248, \underbrace{155}_{899=3 \cdot 248+155}) \]

\[ = \gcd(155, \underbrace{93}_{248=1 \cdot 155+93}) \]

\[ = \gcd(93, \underbrace{62}_{155=1 \cdot 93+62}) \]

\[ = \gcd(62, \underbrace{31}_{93=1 \cdot 62+31}) \]

\[ = \gcd(31, \underbrace{0}_{62=2 \cdot 31+0}) \]

\[ = \gcd(31, 0) \]

\[ = 31. \]
Theorem 3. Given integers $a$ and $b$ not both of which are zero, there exist integers $x$ and $y$ such that $\gcd(a, b) = a \cdot x + b \cdot y$.

5. Prime numbers

Definition 5. A number $p > 1$ with no positive divisors other than itself and 1 is called a prime number.

Theorem 4. There are infinitely many primes.

Proof: Suppose that $p_1 = 2 < p_2 = 3 < \ldots < p_k$ are all of the primes. Let $P = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1$ and let $p$ be a prime dividing $P$. Then $p$ can not be any of the primes listed above, otherwise $p$ would divide the difference $P - p_1 \cdot p_2 \cdot \ldots \cdot p_k = 1$, which is impossible. So this prime $p$ is still another prime, and $p_1, p_2, \ldots, p_k$ would not be all of the primes. \Box

Theorem 5. There are infinitely many primes of the form $4 \cdot n + 1$ and of the form $4 \cdot n + 3$.

Lemma 6. If $p$ is a prime and $p|ab$, then $p|a$ or $p|b$.

The Fundamental Theorem of Arithmetic:

Every positive integer $n$ can be written in a unique way as a product of primes:

$$ n = p_1 \cdot p_2 \cdot \ldots \cdot p_k \quad (p_1 \leq p_2 \leq \ldots \leq p_k) $$

Dirichlet’s theorem:

Let $a, b \in \mathbb{N}$ be relatively prime. Then there exist infinitely many primes of the form $a \cdot n + b$ for $n \in \mathbb{N}$.

Euclid’s theorem:

If $p$ is a prime number and $p$ divides $a \cdot b$, then $p$ divides $a$ or $p$ divides $b$.

The Prime Number theorem:

For each positive integer $n$ there are approximately $n / \ln n$ prime numbers up to $n$.

6. Modular Arithmetic

Modular arithmetic is one of the foundations of number theory, touching on almost every aspect of its study, and providing key examples for group theory, ring theory and abstract algebra. In cryptography, modular arithmetic directly underpins public keysystems such as RSA and Diffie-Hellman, provides finite fields which underlie elliptic curves, and is used in a variety of symmetric key algorithms. Modular arithmetic was introduced by Carl F. Gauss in 1801. He in his paper *Disquisitiones Arithmeticae* introduced the notion of ”congruence”.

Gauss said that $a$ is congruent to $b$ modulo $n$ if $n|(a - b)$. This is denoted $a \equiv b \mod n$.

Example 5. $29 \equiv 15 \mod 7$ because $7|(29 - 15)$.
**Definition 6.** Let $a$, $b$ and $n$ are integers and $n > 0$. We write $a \equiv b \mod n$ if $n$ divides $a - b$.

- $n$ is called the modulus.
- $b$ is called the remainder.

Note that the remainder $b$ is not unique. Here is an example:

- $12 \equiv 3 \mod 9$ ; 3 is a valid remainder since 9 divides $12 - 3$
- $12 \equiv 21 \mod 9$ ; 21 is a valid remainder since 9 divides $12 - 21$
- $12 \equiv -6 \mod 9$ ; $-6$ is a valid remainder since 9 divides $12 - (-6)$

**Question:** Which remainder do we choose?
By agreement, we usually choose:

- $0 \leq b < n$

**Question:** How is the remainder computed?
Any $a \in \mathbb{Z}$ can be written as $a = q \cdot n + b$ where $0 \leq b < n$. Now since $a - b = q \cdot n$ ($n$ divides $a - b$) we can write $a \equiv b \mod n$. Note that $b \in \{0, 1, 2, ..., n - 1\}$.

**Lemma 7.** The following hold for $n \geq 1$:

- $a \equiv a \pmod{n}$
- $a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$
- $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ implies $a \equiv c \pmod{n}$

6.1. **Modular addition and multiplication.**

**Definition 7.** The set $\mathbb{Z}_n = \{0, 1, 2, 3, ..., n - 1\}$ has two operations "+" and "." for all $a, b \in \mathbb{Z}_n$ such that:

- $a + b \equiv c \pmod{n}$ ($c \in \mathbb{Z}_n$)
- $a \cdot b \equiv d \pmod{n}$ ($d \in \mathbb{Z}_n$)

**Example 6.** $17 + 20 \mod 22 = 15$ and $4 \cdot 8 \mod 22 = 10$.

**Lemma 8.** The following hold for $n \geq 1$:

- $a \equiv b \pmod{n}$ implies $a + c \equiv b + c \pmod{n}$
- $a \equiv b \pmod{n}$ implies $ac \equiv bc \pmod{n}$
- $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ imply $a + c \equiv b + d \pmod{n}$
- $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ imply $a \cdot c \equiv b \cdot d \pmod{n}$

The modulo operation can be applied to intermediate results:

- $(a + b) \mod m \equiv (a \mod m) + (b \mod m) \mod m$
- $(a \cdot b) \mod m \equiv (a \mod m) \cdot (b \mod m) \mod m$

**Example 7.** $8^3 \mod 7 \equiv (8 \mod 7) \cdot (8 \mod 7) \cdot (8 \mod 7) \mod 7 \equiv 1 \cdot 1 \cdot 1 \mod 7 \equiv 1$

**Fermat’s Little Theorem:**

Let $p$ be a prime which does not divide the integer $a$, then $a^{p-1} = 1 \mod p$.

**Proof:** Start by listing the first $p - 1$ positive multiples of $a$:

- $a, 2a, 3a, ..., (p - 1)a$
Suppose that \( r \cdot a \) and \( s \cdot a \) are the same modulo \( p \), then we have \( r = s \mod p \), so the \( p - 1 \) multiples of \( a \) above are distinct and nonzero; that is, they must be congruent to \( 1, 2, 3, \ldots, p - 1 \) in some order. Multiply all these congruences together and we find
\[
a \cdot 2a \cdot 3a \cdot \ldots \cdot (p - 1)a = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p - 1) \mod p
\]
or better,
\[
(p - 1)(p - 1)! = (p - 1)! \mod p
\]
Divide both side by \( (p - 1)! \) to complete the proof. \( \diamond \) Sometimes Fermat’s Little Theorem is presented in the following form:

**Corollary 9.** Let \( p \) be a prime and \( a \) any integer, then \( a^p = a \mod p \).

**Proof:** The result is trivial (both sides are zero) if \( p \) divides \( a \). If \( p \) does not divide \( a \), then we need only multiply the congruence in Fermat’s Little Theorem by \( a \) to complete the proof. \( \diamond \)

### 6.2. Linear Equations

There is the following theorem for solving equations of the form \( a \cdot X = b \mod n \):

**Theorem 10.** The equation \( a \cdot X = b \mod n \) has a solution in \( \mathbb{Z}_n \) if, and only if, \( \gcd(a, n) \) divides \( b \).

The Euclidean Algorithm is the main tool for solving such equations. The solution process has the following steps:

1. Compute \( \gcd(a, n) \). If \( b \) is a multiple of it, find \( k \) such that \( b = k \cdot \gcd(a, n) \), and proceed to the next step. Otherwise, stop since the equation has no solution.

2. Using the Euclidean Algorithm, compute \( x \) and \( y \) such that \( a \cdot x + n \cdot y = \gcd(a, n) \) and such that \( x \) is positive. Notice that then \( x \) is a solution for the equation \( a \cdot x = \gcd(a, n) \mod n \).

3. Compute \( k \cdot x \mod n \), where \( k \) is from Step 1 and \( x \) is from Step 2. This is a solution to \( a \cdot X = b \mod n \).

If the equation is solvable, then it has \( \gcd(a, n) \) many solutions. If \( s \) is a solution, then also \( s + k \cdot \frac{p}{\gcd(a, n)} \mod n \) for \( k = 0, 1, 2, 3, \ldots, \gcd(a, n) - 1 \).

### 6.3. Solving several linear equations simultaneously

Sometimes one is confronted by the following sort of problem:

Find the smallest natural number which simultaneously satisfies the following equations:
\[
\begin{align*}
x &= 12 \mod 101 \\
x &= 13 \mod 103
\end{align*}
\]

The main tool used in this context is known as

**The Chinese Remainder Theorem:**

Let \( n_1, n_2, \ldots, n_k \) be natural numbers such that for \( i, j \) distinct indices one has \( \gcd(n_i, n_j) = 1 \). Then the system of equations
\[ x = b_1 \ mod \ n_1 \]
\[ x = b_2 \ mod \ n_2 \]
\[ x = b_3 \ mod \ n_3 \]
\[ \vdots \]
\[ x = b_k \ mod \ n_k \]

has a solution which is unique modulo \( N = n_1 \cdot n_2 \cdot \ldots \cdot n_k \).

Indeed, if for each \( i \) we set \( N_i = N/n_i \), and if \( x_i = \frac{1}{N_i} \ mod \ n_i \), then the number
\[ x = b_1 \cdot N_1 \cdot x_1 + b_2 \cdot N_2 \cdot x_2 + \ldots + b_k \cdot N_k \cdot x_k \mod N \]

is that unique solution.

7. Euler \( \phi \) - function

**Definition 8.** For \( n \geq 1 \), let \( \phi(n) \) denote the number of positive integers not exceeding \( n \) that are relatively prime to \( n \).

The function \( \phi(n) \) is called the Euler phi-function or totient function. If \( n \) is prime number, then every integer less than \( n \) is relatively prime to it. We have that if \( n \) is prime then \( \phi(n) = n - 1 \). We will show that the other direction also holds. Assume that \( \phi(n) = n - 1 \) and \( n \) is a composite number. Then \( n \) has a divisor \( d \) such that \( 1 < d < n \). It follows that there are at least two integers among \( 1, 2, 3, \ldots, n \) which are not relatively prime to \( n \), namely \( d \) and \( n \) itself. As a result, \( \phi(n) \leq n - 2 \). This proves that for \( n > 1 \), \( \phi(n) = n - 1 \) if and only if \( n \) is prime.

**Theorem 11.** If \( p \) is a prime and \( k > 0 \), then
\[
\phi(p^k) = p^k - p^{k-1} = p^k(1 - 1/p).
\]

**Proof:** Claim: \( gcd(n, p^k) = 1 \) if and only if \( p \) does not divide \( n \).

Proof of the Claim:
It is clear that if \( gcd(n, p^k) = 1 \), then \( gcd(n, p) = 1 \). Assume that \( gcd(n, p) = 1 \) and \( gcd(n, p^k) = x \). We will show that \( x = 1 \). Using the Euclidean Algorithm we can find \( m \) and \( n \) such that \( x = m * n + m * p^k \) i.e. \( x = m * n + m * p^{k-1} * p \). From the assumption that \( gcd(n, p^k) = x \) we have that \( x \) divides \( n \) and \( x \) divides \( p^{k-1} * p \) we have that \( x \) must divides \( p \). So \( x \) can be either 1 or \( p \). But \( x \) cannot be \( p \) because \( gcd(n, p) = 1 \). How many integers are divisible by \( p \) in the set \( \{1, 2, 3, \ldots, p^k\} \)? There are \( p^{k-1} \) integers between 1 and \( p^k \) which are divisible by \( p \), namely \( p, 2p, 3p, \ldots, (p^{k-1})p \). Thus, the set \( \{1, 2, 3, \ldots, p^k\} \) contains exactly \( p^k - p^{k-1} \) integers which are relatively prime to \( p^k \) and so, by the definition of \( \phi \)-function \( \phi(p^k) = p^k - p^{k-1} \).

**Theorem 12.** Let \( m \) and \( n \) are positive integers that have no common factor greater than 1 i.e. \( gcd(m, n) = 1 \). Then, \( \phi(m \cdot n) = \phi(m) \cdot \phi(n) \).

**Lemma 13.** Given integers \( a, b, c, gcd(a, bc) = 1 \) if and only if \( gcd(a, b) = 1 \) or \( gcd(a, c) = 1 \).

**Theorem 14.** If the integer \( n > 1 \) has the prime factorization \( n = p_1^{k_1}p_2^{k_2}p_3^{k_3} \ldots p_r^{k_r} \), then
\[
\phi(n) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \ldots (p_r^{k_r} - p_r^{k_r-1}) = n(1 - 1/p_1)(1 - 1/p_2) \ldots (1 - 1/p_r)\]
Proof: We use induction on \( r \), the number of distinct prime factors of \( n \). By the previous theorem, the result is true for \( r = 1 \). Suppose that it holds for \( r = i \). We prove that the statement holds for \( r = i + 1 \). Since
\[
gcd(p_1^{k_1} p_2^{k_2} ... p_i^{k_i} p_{i+1}^{k_{i+1}}) = 1,
\]
by the previous theorem we have
\[
\phi(p_1^{k_1} p_2^{k_2} ... p_i^{k_i} p_{i+1}^{k_{i+1}}) = \phi(p_1^{k_1} p_2^{k_2} ... p_i^{k_i}) \cdot \phi(p_{i+1}^{k_{i+1}}) = \phi(p_1^{k_1} p_2^{k_2} ... p_i^{k_i}) \cdot (p_{i+1}^{k_{i+1}} - p_{i+1}^{k_{i+1} - 1}).
\]
The first factor on the right side becomes
\[
\phi(p_1^{k_1} p_2^{k_2} ... p_i^{k_i}) = (p_1^{k_1} - p_1^{k_1 - 1})(p_2^{k_2} - p_2^{k_2 - 1})...(p_i^{k_i} - p_i^{k_i - 1})
\]
and this completes the proof. \( \Box \)

Theorem 15. For \( n > 2 \), \( \phi(n) \) is an even integer.