Review of Number Theory

1. Preliminary

R : real numbers
$Z = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$: integers
$N = \{1, 2, 3, \cdots\}$: natural numbers, or positive integers
$Q = \{\frac{n}{m} \mid n, m \in Z \text{ and } m \neq 0\}$: rational numbers

Divisibility:
$d \mid n$ means there is an integer k such that $n = dk$. We can say d divides *n*, or d is a divisor of *n*, or *n* is a multiple of *d*.

Division Algorithm:
If a and b are integers and $b > 0$, then there exist unique integers q and r satisfying the two conditions: $a = bq + r$ and $0 \leq r < b$. q is called the quotient and r is called the remainder.

MOD operation:
For $b > 0$, define $a \bmod b = r$ where r is the remainder given by the Division Algorithm when *a* is divided by *b*, that is, $a = bq + r$ and $0 \leq r < b$.

Greatest Common Divisor:
Let $a, b \in Z$. If $a \neq 0$ or $b \neq 0$, we define gcd(*a*, *b*) to be the largest integer *d* such that $d \mid a$ and $d \mid b$. We define gcd(0, 0) = 0.

Bezout's Lemma:
For all integers *a* and *b*, there exist integers *s* and *t* such that gcd(*a*, *b*) = *sa* +*tb*.

2. Prime Numbers

An integer $p > 1$ is a prime number if and only if its only divisors are ± 1 and $\pm p$.

Euclid's Theorem:
There are infinitely many prime numbers.

Prime Number Theorem:

Let $x \in R$, $x > 0$. $\pi(x)$ denotes the number of primes *p* such that $p \leq x$.

$\pi(x) \sim \frac{x}{\ln(x)}$ for all $x > 0$. Or, $\lim_{x \to \infty} \frac{\pi(x)}{x / \ln(x)} = 1$.

$\pi(10^2)=25, \pi(10^3)=168, \pi(10^4)=1229, \pi(10^5)=9592, \pi(10^6)=78498,$
$\pi(10^7)=664579, \pi(10^8)=5761455, \pi(10^9)=50847534$

Prime Factorization:
Any integer $a>1$ can be factored in a unique way as $a=p_1^{a_1}p_2^{a_2}\cdots p_t^{a_t}$ where $p_1<p_2<\cdots p_t$ are prime numbers and where each a_i is a positive integer. Or, $a=\prod_{i=1}^{t} p_i^{a_i}$.
For example: $600=2^3\times 3^1\times 5^2$.

Relatively prime:
We say that *a* and *b* are relatively prime if gcd(*a, b*)=1.

Euclid's Lemma:
If *p* is a prime and *p*|*ab*, then *p*|*a* or *p*|*b*.

3. Congruences

Let $m\geq 0$. We write $a\equiv b(\operatorname{mod} m)$ if $m\,|\,a-b$, and we say that ***a* is congruent to *b* modulo *m***. Here *m* is said to be the **modulus** of the congruence.

Theorem:
For $m>0$ and for all *a*, *b*, *c*:
- $a\equiv b(\operatorname{mod} m)\Leftrightarrow a \operatorname{mod} m = b \operatorname{mod} m$.
- $a\equiv a(\operatorname{mod} m)$ (reflexivity)
- $a\equiv b(\operatorname{mod} m)\Rightarrow b\equiv a(\operatorname{mod} m)$ (symmetry)
- $a\equiv b(\operatorname{mod} m)$ and $b\equiv c(\operatorname{mod} m)\Rightarrow a\equiv c(\operatorname{mod} m)$ (transitivity)

If $a\equiv b(\operatorname{mod} m)$ and $c\equiv d(\operatorname{mod} m)$, then
- $a\pm c\equiv b\pm d(\operatorname{mod} m)$
- $ac\equiv bd(\operatorname{mod} m)$
- $a^n\equiv b^n(\operatorname{mod} m)$ for all $n\geq 1$
- $f(a)\equiv f(b)(\operatorname{mod} m)$ for all polynomials $f(x)$ with integer coefficients.

4. Fermat's and Euler's Theorems

Fermat's Theorem:
If *p* is prime and *a* is a positive integer not divisible by *p*, then $a^{p-1}\equiv 1 \operatorname{mod} p$.

Euler's Totient Function:
$\phi(n)$: the number of positive integers less than *n* and relatively prime to *n*.
For a prime number *p*, $\phi(p)=p-1$.

Euler's Theorem:
For every *a* and *n* that are relatively prime: $a^{\phi(n)} \equiv 1 \bmod n$.

5. Discrete Logarithms

Remark: Discrete logarithms are fundamental to a number of public-key algorithms, including Diffie-Hellman key exchange, ElGamal system, and the Digital Signature algorithm.

Ordinary logarithms:
For base *x* and for a value *y*, if $y = x^i$, then $i = \log_x(y)$, and $y = x^{\log_x(y)}$.
Properties of logarithms:
$\log_x(1) = 0$
$\log_x(x) = 1$
$\log_x(yz) = \log_x(y) + \log_x(z)$
$\log_x(y^r) = r\log_x(y)$

Primitive root:
If *a* is a primitive root of *n*, then its powers $a, a^2, \ldots, a^{\phi(n)}$ are distinct (mod *n*) and are all relatively prime to *n*. In particular, for a prime number p, if *a* is a primitive root of *p*, then $a, a^2, \ldots, a^{p-1}$ are distinct (mod *p*).

Index:
Consider a primitive root *a* for some prime number *p*. It follows that for any integer *b*, we can find a unique exponent *i* such that $b \equiv a^i \bmod p$ where $0 \le i \le p-1$. This exponent i is referred to as **the index of the number *b* for the base *a* (mod *p*)**. We denote this value as $\text{ind}_{a,p}(b)$. Or, $b \equiv a^i \bmod p, 0 \le i \le p-1 \Rightarrow i = \text{ind}_{a,p}(b)$.

Discrete logarithm problem:
Consider the equation $y = g^x \bmod p$. Given *g*, *x*, and *p*, it is very easy to calculate *y*. However, given *y*, *g*, and *p*, it is very difficult to find *x*.