1st sym. Theorems about Number Thoery

Choi Pooreunhaneul

April 11, 2023

1 Divisibility Theory in the Integers

Theorem 1.1 Division Algorithm. There exists unique q and r satisfying

$$a = qb + r \qquad (0 \leq r < b) \tag{1}$$

Theorem 1.2. Without some trivial properties, given statement hold:

$$(a) \text{ If } a|b \text{ and } a|c, \text{ then } a|(bx + cy) \tag{2}$$
$$(b)\ gcd(a, b) = ax + by \tag{3}$$

Corollary.

$$(a) \text{ If } gcd(a, b) = d, \text{ then } gcd(a/d, b/d) = 1 \tag{4}$$
$$(b) \text{ If } a|c \text{ and } b|c, \text{ with } gcd(a, b) = 1, \text{ then } ab|c \tag{5}$$

Theorem 1.3 Euclid's lemma.

$$\text{If } a|bc, \text{ with } gcd(a, b) = 1, \text{ then } a|c. \tag{6}$$

Lemma.

$$\text{If } a = bq + r, \text{ then } gcd(a, b) = gcd(q, r). \tag{7}$$

Theorem 1.4.

$$gcd(a, b)lcm(a, b) = ab \tag{8}$$

Theorem 1.5. The linear Diophantine eq. *ax+by=c* has a sol. iff $d|c$, where *gcd(a,b)=d.* If x_0, y_0 is one of sol, then

$$x = x_0 + (\frac{b}{d})t \quad y = y_0 - (\frac{a}{d})t. \tag{9}$$

2 Primes and Distribution

Theorem 2.1. If p_n is the nth prime number, then

$$p_n \leq 2^{2^{n-1}}. \tag{10}$$

Corollary. For $n \geq 1$, there are at least *n+1* primes less than 2^{2^n}.

Theorem 2.2. There are an infinite number of primes of the form $4n$+3.

Therem 2.3 Dirichlet. If a and b are relatively prime positive int, then the arithmetic progression

$$a,\ a+b,\ a+2b, \cdots \tag{11}$$

contains infinitely many primes.

Theorem 2.4. If all the n>2 terms of the arithmetic progression

$$p,\ p+d,\ , \cdots,\ p+(n-1)d \tag{12}$$

are prime numbers, then the common difference d is divisible by every prime q<n.

3 The Theory of Conguruences

Theorem 3.1.

$$\text{If } ca \equiv cb\,(mod\,n),\ \text{then } a \equiv b\,(mod\,n/d), \text{where } d = gcd(c,n). \tag{13}$$

Theorem 3.2.

$$\text{Let } P(x) = \sum_{k=0}^{m} c_k x^k \text{ be a polynomial function of } x \text{ with integral coefficients.}$$

$$\text{If } a \equiv b\,(mod\,n), \text{then } P(a) \equiv P(b)\,(mod\,n). \tag{14}$$

Theorem 3.3. For decimal expansion of the positive integer, given statement hold:

$$(a)\ 9|N \text{ iff } 9|S \text{ for } S = N(0) \tag{15}$$

$$(b)\ 11|N \text{ iff } 11|T \text{ for } T = N(-1). \tag{16}$$

Theorem 3.4. The linear conguruence $ax \equiv b\ (mod\,n)$ has a sol. iff $d|b$, where *d=gcd(a,n)*, while it has d mutually incongruent sol. mod n.

Theorem 3.5 Chinese Remainder Theorem. Let $n_1, \cdots, n_r$ be positive int. s.t. $gcd(n_i, nj) = 1$ for $i \neq j$. Then the the system of linear congruences has a simultaneous sol. which is unique mod. the int. $n_1 \cdots n_r$.

Theorem 3.6. The system of linear congruences

$$\begin{aligned} ax + by &\equiv r\,(mod\,n) \\ cx + dy &\equiv s\,(mod\,n) \end{aligned} \tag{17}$$

has a unique sol. mod. n whenever *gcd(ad-bc,n)=1.*

4 Fermat's Theorem

Theorem 4.1 Fermat's Theorem. Let p be a prime and suppose that $p \nmid a$. Then $a^{p-1} \equiv 1\ (mod\ p)$.

Corollary. If p is a prime, then $a^p \equiv a\ (mod\ p)$ for any int. a.

Lemma. If p and q are distinct primes with $a^p \equiv a\ (mod\ p)$ and $a^q \equiv a\ (mod\ q)$, then $a^{pq} \equiv a\ (mod\ pq)$.

Definition. If $n|a^n - a$ holds, then n is called a pseudoprime to the base a.

Theorem 4.2. If n is an odd pseudoprime, then $M_n = 2^n - 1$ is a larger one.

Theorem 4.3. Let n be a composite square-free int, say, $n = p_1 \cdots p_r$, where they are distinct prime. If $p_i - 1|n - 1$, then n is an absolute pseudoprime.

Theorem 4.4 Wilson. If p is a prime, then $(p-1)! \equiv -1\ (mod\ p)$.

Theorem 4.5. The quadratic congruence $x^2 + 1 \equiv 0\ (mod\ p)$, where p is an odd prime, has a sol. iff $p \equiv 1\ (mod\ 4)$.

5 Number-Theoretic Functions

Definition. Given a positive int. n, $\tau(n)$ denote the number of positive divisors of n and $\sigma(n)$ denote the sum of those divisors.

Theorem 5.1. The functions τ, σ are both multiplicative.

Theorem 5.2. If f is a multiplicative function and F is defined by

$$F(n) = \sum_{d|n} f(d) \tag{18}$$

then F is also multiplicative and converse also holds.

Definition. For a positive int. n, define μ by the rules

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } p^2|n \\ (-1)^r & \text{if } n = p_1 \cdots p_r \end{cases} \tag{19}$$

Theorem 5.3. For each positive int. n,

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases} \tag{20}$$

Theorem 5.4 Möbius inversion formula. Let F, f be two number-theoretic functions related by formula

$$F(n) = \sum_{d|n} f(d). \tag{21}$$

Then

$$f(n) = \sum_{d|n} \mu(d) F(\frac{n}{d}) = \sum_{d|n} \mu(\frac{n}{d}) F(d). \tag{22}$$

Theorem 5.5. If n is a positive int, then the exponent of the highest power of p that divides $n!$ is

$$\sum_{k=1}^{\infty} [\frac{n}{p^k}] \tag{23}$$

where the series is finite.

Theorem 5.6. Let F, f be number-theoretic functions s.t.

$$F(n) = \sum_{d|n} f(d) \tag{24}$$

Then, for any positive int. N,

$$\sum_{n=1}^{N} F(n) = \sum_{k=1}^{N} f(k)[\frac{N}{k}] \tag{25}$$

Corollary. Following holds:

$$\sum_{n=1}^{N} \tau(n) = \sum_{n=1}^{N} [\frac{N}{k}] \tag{26}$$

$$\sum_{n=1}^{N} \sigma(n) = \sum_{n=1}^{N} n[\frac{N}{k}] \tag{27}$$

6 Euler's Generalization of Fermat's Theorem

Definition. $\phi(n)$ denote the number of positive int. not exceeding n that are relatively prime to n. Also, it is multiplicative.

Theorem 6.1. If p is a prime and $k > 0$, then

$$\phi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p}) \tag{28}$$

Theorem 6.2.

$$\phi(n) = n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_r}) \tag{29}$$

Lemma. Let $n > 1$ and *gcd(a,n)=1*. If $a_1, \cdots, a_{\phi(n)}$ are the int. less than n and relatively prime to n, then

$$aa_1, \cdots, aa_{\phi(n)} \tag{30}$$

are congruent mod n to $a_1, \cdots, a_{\phi(n)}$ in some order.

Theorem 6.3 Euler. If $n \geq 1$ and *gcd(a,n)=1*, then $a^{\phi(n)} \equiv 1 \ (mod\ n)$.

Theorem 6.4 Gauss. For each positive int,

$$n = \sum_{d|n} \phi(d) \tag{31}$$

the sum being extended over all positive divisors of n.

Theorem 6.5. For $n > 1$, the sum of the positive int. less than n and relatively prime to it is $\frac{1}{2}n\phi(n)$.

Theorem 6.6. For any positive int,

$$\phi(n) = n \sum_{d|n} \frac{\mu(d)}{d} \tag{32}$$

7 Primitive Roots and Indices

Definition. Let $n > 1$ and *gcd(a,n)=1*. The order of a mod n is the smallest positive int. k s.t. $a^k \equiv 1\ (mod\ n)$. If it is $\phi(n)$, then a is a primitive root of n.

Theorem 7.1. Let the integer a have order k mod n. Then $a^h \equiv 1\ (mod\ n)$ iff $k|h$; in particular, $k|\phi(n)$.

Theorem 7.2. If the int. a has order k mod n, then $a^i \equiv a^j\ (mod\ n)$ iff $i \equiv j\ (mod\ k)$.

Corollary. If a has order k mod n, then the int. $a,\ a^2, \cdots, a^k$ are incongrunt mod n.

Theorem 7.3. If a has order k mod n and $h > 0$, then a^h has order $\dfrac{k}{gcd(h,k)}\ (mod\, n)$.

Theorem 7.4. Let *gcd(a,n)=1* and let $a_1, \cdots, a_{\phi(n)}$ be the positive int. less than n and relatively prime to n. If a is a primitive root on n, then

$$a^1, \cdots, a^{\phi(n)} \tag{33}$$

are congruent mod n to $a_1, \cdots, a_{\phi(n)}$ in some order.

Corollary. If n has a primitive root, then it has exactly $\phi(\phi(n))$ of them.

Theorem 7.5 Lagrange. If p is a prime and

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \qquad a_n \not\equiv 0\ (mod\ p) \tag{34}$$

is a poly. with int. coeff, then the congruence

$$f(x) \equiv 0\ (mod\ p) \tag{35}$$

has at most n incongrunet sol. mod p.

Corollary. If p is a pirme and $d|p-1$, then the congruence

$$x^d - 1 \equiv 0\ (mod\ p) \tag{36}$$

has exactly d sol.

Theorem 7.6. If p is a pirme and $d|p-1$, then there are exactly $\phi(d)$ incongruent integers having order d mod p.

Corollary. If p is a prime, then there are exactly $\phi(p-1)$ incongruent primitive roots of p.

Theorem 7.7. For $k \geq 3$, the int. 2^k has no primitive roots.

Theorem 7.8. If *gcd(m,n)=1*, where $m, n > 2$, then the int. mn has no primitive roots.

Lemma. If p is an odd prime, $\exists$ primitive root r of p s.t. $r^{p-1} \not\equiv 1\ (mod\ p^2)$.

Corollary. If p is an odd prime, then p^2 has a primitive root; in fact, for a primitive root r of p, either r, $r+p$ or both is a primitive root of p^2.

Lemma. Let p be an odd prime and let r be a primitive root of p with the property that $r^{p-1} \not\equiv 1\ (mod\ p^2)$. Then for each int. $k \geq 2$,

$$r^{p^{k-2}(p-1)} \not\equiv 1\ (mod\ p^k) \tag{37}$$

Theorem 7.9. If p is an odd prime number and $k \geq 1$, then there exists a primitive root for p^k.

Corollary. There are primitive roots for $2p^k$, where p is an odd prime and $k \geq 1$.

Definition. Let r be a primitive root of n. If *gcd(a,n)=1*, then the smallest positive integer k s.t. $a \equiv r^k\ (mod\ n)$ is called the index of a relative to r.

We denote the index of a relative to r by $\text{ind}_r a$ or just ind a.

Theorem 7.10. If n has a primitive root r and ind a denotes the index of a relative to r, then the following properties hold:

$$(a)\ \text{ind}\ (ab) \equiv \text{ind}\ a + \text{ind}\ b\ (\text{mod}\ \phi(n)). \tag{38}$$

$$(b)\ \text{ind}\ a^k = k\ \text{ind}\ a\ (\text{mod}\ \phi(n)). \tag{39}$$

$$(c)\ \text{ind}\ 1 \equiv 0\ (\text{mod}\ \phi(n)), \text{ind}\ r \equiv 1\ (\text{mod}\ \phi(n)). \tag{40}$$

Theorem 7.11. Let n be an int. possessing a primitive root and let *gcd(a, n)*=1. Then the congruence $x^k \equiv a$ (mod n) has a sol. iff

$$a^{\phi(n)/d} \equiv 1\ (mod\ n) \tag{41}$$

where $d = gcd(k, \phi(n)$; if it has a sol, there are exactly d sol. mod n.

Corollary. Let p be a prime and *gcd(a,p)=1*. Then the congruence $x^k \equiv a\ (mod\ p)$ has a sol. iff $a^{(p-1)/d} \equiv 1\ (mod\ p)$, where *d=gcd(k,p-1)*.

0 Hensel's Lemma

Let p be a prime. Then let

$$P(x) = x^n + \sum_{i=0}^{n-1} c_i x^i \tag{42}$$

be a polynomial with integer coefficient. Assume that $\exists$ int. a_1 s.t.

$$P(a_1) \equiv 0 \ (mod \ p) \qquad and \quad P'(a_1) \not\equiv 0 \ (mod \ p). \tag{43}$$

Then, for all natural number k, $\exists$ int. a_k unique up to $mod \ p^k$ s.t.

$$a_k \equiv a_1 \ (mod \ p) \qquad and \qquad P(a_k) \equiv 0 \ (mod \ p^k) \tag{44}$$

This is done.