NTL4 – Order, Arithmetic Functions

Theorem 8.1 (Wilson's Theorem)

Let p be a prime. Then

$$(p-1)! \equiv -1 \ (mod\ p)$$

Alternatively, more generally,

For any integer n, we have

$$(n-1)! \equiv -1 \ (mod\ n)$$

if and only if n is a prime.

Theorem 8.2 (Fermat's Christmas Theorem)

Let p be a prime. Then, there exists an x with $x^2 \equiv -1 (mod\ p)$

if and only if $p = 2$ or $p \equiv 1 (mod\ 4)$.

Example 1. Prove Fermat's Christmas Theorem.

Definition 8.1 (Order)

Let p be a prime and $a \not\equiv 0\ (mod\ p)$. Then the order of a modulo p is defined to be the smallest positive integer n such that $a^n \equiv 1 (mod\ p)$.

We write this as $n = ord_p a$ or sometimes shorthanded to $o_p a$. Order cannot be zero.

$$a^n \equiv 1 (mod\ p) \Leftrightarrow n = ord_p a, \qquad where\ n\ is\ smallest\ positive\ integer$$

For example, the order of 2 mod 9 is 6.

Theorem 8.3 (Fundamental Theorem of Orders)

For a prime p and any integer $a \neq 0\ (mod\ p)$, we have

$$a^m \equiv 1\ (mod\ p) \Leftrightarrow ord_p a \mid m.$$

Corollary 8.3.1

For relatively prime positive integers a and m,

$$order_m a \mid \phi(m)$$

Example 2. For positive integers $a > 1$ and n, find $ord_{a^n-1}(a)$.

Example 3. Prove that if p is prime, then every prime divisor of $2^p - 1$ is greater than p.

Example 4. Let $a > 1$ and n be given positive integers. If p is an odd prime divisor of $a^{2^n} + 1$, prove that $p - 1$ is divisible by 2^{n+1}.

Example 5. (Classical) Let n be an integer with $n \geq 2$. Prove that n doesn't divide $2^n - 1$.

Example 6. Let a and b be relatively prime integers. Prove that any odd divisor of $a^{2^n} + b^{2^n}$ is of the form $2^{n+1}m + 1$.

Definition 8.2 (Primitive Roots)

Let p be a prime. Then a residue $g \neq 1$ is called primitive root mod p if g has order $(p-1)$ mod p.

$$g^{p-1} \equiv 1 \ (mod\ p)$$

Theorem 8.4 (Primitive Roots Generate all Non-zero Residues)

Let g be a primitive root modulo p. Then

$$\{g^1, g^2, g^3, \dots, g^{p-1}\} \equiv \{1,2,3, \dots, p-1\} \ (mod\ p)$$

Theorem 8.5 (Primitive Roots Always Exists modulo p)

Let $p > 2$ be a prime. Then there always exists a primitive root modulo p.

Example 7. (Sum of powers $mod\ p$) Let $p > 2$ be a prime. Then for any integer x,

$$1^x + 2^x + \cdots + (p-1)^x \equiv \begin{cases} -1, & if\ p-1 \mid x \\ 0, & otherwise \end{cases} \ (mod\ p).$$

Theorem 9.1 (Number of Divisors)

Let $n \in \mathbb{N}$ such that its prime factorization is

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

Then, the number of divisors of n,

$$d(n) = (1+\alpha_1)(1+\alpha_2) \dots (1+\alpha_k)$$

Note. The function $d(n)$ is odd if and only if n is a square.

Theorem 9.2 (Sum of Divisors)

Let $n \in \mathbb{N}$ such that its prime factorization is

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

Then, the sum of divisors of n,

$$\sigma(n) = \left(\sum_{\beta_1=0}^{\alpha_1} p_1^{\beta_1}\right) \dots \left(\sum_{\beta_k=0}^{\alpha_k} p_k^{\beta_k}\right) = \left(\frac{p_1^{\alpha_1+1} - 1}{p_1 - 1}\right) \dots \left(\frac{p_k^{\alpha_k+1} - 1}{p_k - 1}\right)$$

Theorem 9.3 (Euler's Totient Function)

Let $n \in \mathbb{N}$ such that its prime factorization is

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

Then, the number of positive integers less than n that are coprime to n are

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_k}\right)$$
$$= p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \dots p_k^{\alpha_k - 1} \cdot (p_1 - 1)(p_2 - 1)\dots(p_k - 1)$$

Theorem 9.4 (Gauss)

For any positive integer n, we have

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

For instance, if $n = 10$, then $\phi(1) + \phi(2) + \phi(5) + \phi(10) = 1 + 1 + 4 + 4 = 10$

Definition 9.1 (Floor Function)

For a real number x, there is a unique integer n such that $n \le x < n + 1$.

We say that n is the greatest integer less than or equal to x.

$$n = \lfloor x \rfloor$$

The difference $x - \lfloor x \rfloor$ is called the fractional part of x and is denoted by $\{x\}$.

$$\{x\} = x - \lfloor x \rfloor$$

The least integer greater than or equal to x is called the ceiling of x and is denoted by $\lceil x \rceil$.

If x is an integer, then $\lfloor x \rfloor = \lceil x \rceil = x, \{x\} = 0$.

If x is not an integer, then $\lceil x \rceil = \lfloor x \rfloor + 1$

Example 8. (Australia 1999) Solve the following system of equations:

$$x + \lfloor y \rfloor + \{z\} = 200.0$$
$$\{x\} + y + \lfloor z \rfloor = 190.1$$
$$\lfloor x \rfloor + \{y\} + z = 178.8.$$

Theorem 9.5 (Properties of Floor and Ceiling Functions)

1. *If a and b are integers with $b > 0$, and q is the quotient and r is the remainder when a is divided by b, then $q = \left\lfloor \frac{b}{a} \right\rfloor$ and $r = \left\{ \frac{a}{b} \right\} \cdot b$.*
2. *For any real number x and any integer n, $\lfloor x + n \rfloor = \lfloor x \rfloor + n$ and $\lceil x \rceil + n = \lceil x \rceil + n$.*
3. *If x is an integer then $\lfloor x \rfloor + \lfloor -x \rfloor = 0$; if x is not an integer, then $\lfloor x \rfloor + \lfloor -x \rfloor = -1$.*

   If x is an integer then $\lceil x \rceil + \lceil -x \rceil = 0$; if x is not an integer, then $\lceil x \rceil + \lceil -x \rceil = 1$.

   If x is an integer then $\{x\} + \{-x\} = 0$; if x is not an integer, then $\{x\} + \{-x\} = 1$.

4. *The floor function is nondecreasing; that is for* $x \leq y, \lfloor x \rfloor \leq \lfloor y \rfloor$.
5. $\left\lfloor x + \frac{1}{2} \right\rfloor$ *rounds* x *to its nearest integer.*
6. $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1$
7. $\lfloor x \rfloor \cdot \lfloor y \rfloor \leq \lfloor xy \rfloor$ *for non-negative real numbers* x *and* y.
8. *For any positive real number* x *and any positive integer* n *the number of positive multiples of* n *not exceeding* x *is* $\left\lfloor \frac{x}{n} \right\rfloor$.
9. *For any real number* x *and any positive integer* n,

$$\left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor = \left\lfloor \frac{x}{n} \right\rfloor.$$

Example 9. (Gauss) Let p and q be relatively prime integers. Prove that

$$\left\lfloor \frac{p}{q} \right\rfloor + \left\lfloor \frac{2p}{q} \right\rfloor + \cdots + \left\lfloor \frac{(q-1)p}{q} \right\rfloor = \frac{(p-1)(q-1)}{2}.$$

Theorem 9.6 (Hermite Identity)

Let x *be a real number, and let* n *be a positive integer. Then*

$$\lfloor x \rfloor + \left\lfloor x + \frac{1}{n} \right\rfloor + \left\lfloor x + \frac{2}{n} \right\rfloor + \cdots + \left\lfloor x + \frac{n-1}{n} \right\rfloor = \lfloor nx \rfloor$$