Lecture 1

Euler's totient function / φ function

Def: $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$

$$n \longmapsto \#\{k \leq n \mid GCD(k,n) = 1\}$$

i.e. the number of positive integers less than or equal to n that are coprime to n.

coprime $\sim$ GCD = 1

Ex: 1) $\varphi(6) = \#\{k \leq 6 \mid GCD(k,6) = 1\}$

$= \#\{1, 5\} = 2$

2) $\varphi(7) = \#\{1, 2, 3, 4, 5, 6\}$

$= 6$

3) $\varphi(p) = \#\{1, 2, \ldots, p-1\}$

(p ↑ prime)

$= p - 1$

Recall: $\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \ldots, n-1\}$

Def: $(\mathbb{Z}/n\mathbb{Z})^\times := \{ x \in \mathbb{Z}/n\mathbb{Z} : x \text{ has an inverse in } \mathbb{Z}/n\mathbb{Z} \}$

$= \{ x \in \mathbb{Z}/n\mathbb{Z} : \exists\, y \in \mathbb{Z}/n\mathbb{Z} \text{ s.t. } xy \equiv 1 \mod n \}$

Ex: 1) $(\mathbb{Z}/6\mathbb{Z})^\times = \{1, 5\}$

Why is that?

If for $x \in \mathbb{Z}/6\mathbb{Z}$ $\exists\, y \in \mathbb{Z}/6\mathbb{Z}$ s.t. $xy \equiv 1 \mod 6$

$\iff \exists\, q \in \mathbb{Z}$ s.t. $xy + 6q = 1$

$\iff$ (Lecture 1) $\gcd(x, 6) = 1$

Thus $(\mathbb{Z}/6\mathbb{Z})^\times = \{1, 5\}$

2) $\mathbb{Z}/7\mathbb{Z}^\times = \{1, 2, 3, 4, 5, 6\}$

3) $\mathbb{Z}/9\mathbb{Z}^\times = \{1, 2, 4, 5, 7, 8\}$

4) $\mathbb{Z}/b\mathbb{Z}^\times = \{1, \ldots, b-1\}$

Question: Cardinality of $\mathbb{Z}/n\mathbb{Z}^\times$

Answer: $\varphi(n)$. Because

$$\mathbb{Z}/n\mathbb{Z}^\times = \{0 \leq a \leq n-1 : GCD(a,n) = 1\}$$

Exercise: For any $n \in \mathbb{N}$.

$$[0]_n \notin \mathbb{Z}/n\mathbb{Z}^\times$$

Prop: $|\mathbb{Z}/n\mathbb{Z}^\times| = \varphi(n)$

Pf: It suffices to show that if

$x \in \mathbb{Z}/n\mathbb{Z}^\times$ then $GCD(x,n) = 1$

$\Updownarrow$ $\Updownarrow$

$\exists y$ s.t. $xy \equiv 1 \bmod n \iff \exists q$ s.t. $xy + nq = 1$

Theorem (Generalized FLT)

Let $z \in \mathbb{Z}$ and $n \in \mathbb{N}$ with $GCD(z, n) = 1$. Then $z^{\varphi(n)} \equiv 1 \bmod n$

Corollary (FLT)

Let n be a prime $\Leftrightarrow n \nmid z$ $\Leftrightarrow GCD(n, z) = 1$. Then the above say $z^{\varphi(n)} = z^{n-1} \equiv 1 \bmod n$

If n is prime then $\varphi(n) = n-1$

FLT

Question: Let $z \in \mathbb{Z}/n\mathbb{Z}^{\times}$. Then what is the inverse of z?

Answer: $z^{\varphi(n)-1}$, because

$$z \times z^{\varphi(n)-1} = z^{\varphi(n)} \equiv 1 \bmod n$$

Proof: It is quite similar to the proof of the FLT.

Let $\{z_1, \ldots, z_{\varphi(n)}\}$ be the set of positive integers that are coprime to n.

Consider $\{zz_1, \ldots, zz_{\varphi(n)}\}$.

WTS that the above is the same as

$\{z_1, \ldots, z_{\varphi(n)}\} \mod n$

i). Note that $GCD(zz_j, n) = 1, \forall j$.

As $GCD(z, n) = 1 = GCD(z_j, n)$

$\Rightarrow$ n does not share any prime factor with z & z_j, so neither with zz_j. [Equivalently, if $p \mid GCD(n, zz_j)$

$\Rightarrow p \mid n$ & $p \mid zz_j$

$\Leftrightarrow p \mid n$ & $p \mid z$ or $p \mid z_j$

$\Leftrightarrow p \mid GCD(n, z)$ or $p \mid GCD(n, z_j)$]

Thus $\{zz_1, \ldots, zz_{\varphi(n)}\}$

$\subseteq \{z_1, \ldots, z_{\varphi(n)}\}$

2) $zz_i \not\equiv zz_j \mod n$ if $i \neq j$

Indeed, if $zz_i \equiv zz_j \mod n$

then $n \mid z(z_i - z_j)$ $\quad i \neq j$

But $GCD(n, z) = 1 \Rightarrow n \mid z_i - z_j$

which is impossible as $1 \leq z_i, z_j \leq n-1$

Thus we have $\{zz_1, \ldots, zz_{\varphi(n)}\} \mod n$

$= \{z_1, \ldots, z_{\varphi(n)}\}$

Multiplying

$$\Rightarrow z^{\varphi(n)} \underbrace{\prod_{j=0}^{\varphi(n)} z_j}_{Y} \equiv \underbrace{\prod_{j=1}^{\varphi(n)} z_j}_{Y} \mod n$$

$\Rightarrow n \mid (z^{\varphi(n)} - 1)$

But $GCD(z_j, n) = 1 \Rightarrow GCD(Y, n) = 1$

$\Rightarrow n \mid z^{\varphi(n)} - 1 \Rightarrow z^{\varphi(n)} \equiv 1 \mod n.$

□

RMK: The above theorem will not help to find inverse if we don't know how to calculate $\varphi(n)$ efficiently.

Theorem: 1) $\varphi(p^k) = (p-1)p^{k-1}$, p prime, $k \geq 0$ integer
$= p^k\left(1-\frac{1}{p}\right)$

2) $\varphi(mn) = \varphi(m)\varphi(n)$ if $GCD(m,n) = 1$.

RMK: The theorem is very helpful to calculate $\varphi(n)$

Corollary: Let $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ by the FTA where p_i are distinct primes. Then

$$\varphi(n) = n\prod_{j=1}^{r}\left(1-\frac{1}{p_j}\right) = n\prod_{p|n}\left(1-\frac{1}{p}\right)$$

Proof: By the above theorem

$$\varphi(n) = \varphi\left(p_1^{k_1}\cdots p_r^{k_r}\right)$$
$$= \varphi\left(p_1^{k_1}\right)\cdots\varphi\left(p_r^{k_r}\right)$$
AD for $p_i \neq p_j$, $GCD\left(p_i^{k_i}, p_j^{k_j}\right) = 1$
$$= p_1^{k_1}\left(1-\frac{1}{p_1}\right)\cdots p_r^{k_r}\left(1-\frac{1}{p_r}\right)$$
$$= n\prod_{p|n}\left(1-\frac{1}{p}\right)$$

Example: $\varphi(120)$

$$= \varphi(2^3 \times 3 \times 5)$$

$$= 120\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$$

$$= 120 \times \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5} = 32$$

This is much easier than listing numbers up to 120 that are coprime to 120.

Proof of the theorem (Non-examinable)

Exercise: Show that $\varphi(p^k) = p^k\left(1-\frac{1}{p}\right)$.

Proof: $\varphi(p^k) = \#\{n \le p^k \mid GCD(n, p^k) = 1\}$

$= \#\{n \le p^k \mid GCD(n, p) = 1\}$

$= \#\{n \le p^k \mid p \nmid n\}$

$= p^k - \#\{n \le p^k \mid p \mid n\}$

$= p^k - \#\{n = pq \mid q \le p^{k-1}\}$

$= p^k - p^{k-1} = p^k\left(1-\frac{1}{p}\right)$

Prob: Let $d \mid n$. Then

$$\#\{ z \leq n \mid \gcd(z, n) = d \} = \varphi\left(\frac{n}{d}\right)$$

RMK: The above is a generalization of counting coprime numbers.

Ex: $n = 10$

$$\#\{ z \leq 10 \mid \gcd(z, 10) = 2 \} = \varphi(5)$$

$$\#\{2, 4, 6, 8\} = 4$$

Proof: $d \mid n \Rightarrow \exists\, q$ s.t. $n = dq$

Claim $\{ y \leq q \mid \gcd(y, q) = 1 \}$

$\cong$ (bijection) $\{ z \leq n \mid \gcd(z, n) = d \}$

The map is $y \longmapsto yd$.

The map is clearly injective.

To show surjectivity, let $z = d z'$

$$GCD(n, z) = d.$$

$$\Updownarrow$$

$$GCD(dq, dz') = d.$$

$$\Updownarrow$$

$$d\, GCD(q, z') = d$$

$$\Updownarrow$$

$$GCD(q, z') = 1$$

On the other hand, $z' = \frac{z}{d} \leq \frac{n}{d} = q$.

$\square$

Order

Def: Let $n \in \mathbb{Z}$ and $z \in (\mathbb{Z}/n\mathbb{Z})^{\times}$.

We call $e(z)$ to be the order of z if $e(z)$ is the minimum among $e \in \mathbb{N}$ with $z^e \equiv 1 \bmod n$.

RMK: Gen. FLT $\Rightarrow z^{\varphi(n)} \equiv 1 \bmod n$

But $\varphi(n)$ may not be the minimal e s.t. $z^e \equiv 1 \bmod n$.