Theorem (Gauss)

Let p be a prime number. Then there are exactly $\varphi(p-1)$ many primitive roots.

e.g. $p=7$, $\varphi(7-1)=\varphi(6)=2$. we have seen they are 3 & 5.

$\Phi(6)=\{1,5\}$

Proof (Incomplete): For $a\in\Phi(p)$,

Notations: $\ell(a)$ = length of each cycle in the dynamics of $\boxed{\cdot a \bmod p}$

$c(a)$ = number of cycles in the dynamics of $\boxed{\cdot a \bmod p}$

$$\ell(a)\cdot c(a)=\varphi(p)=p-1$$

Hence, $\ell(a)\in\mathcal{D}(p-1)$.

Conversely, for each $\ell\in\mathcal{D}(p-1)$, define

$$\Phi_\ell(p):=\{a\in\Phi(p)\mid \ell(a)=\ell\}.$$

In particular, $\Phi_{p-1}(p) = \{\text{primitive roots}\}$.

Want to show: each $\Phi_\ell(p)$ is nonempty.

- For $\ell_1 \neq \ell_2$, we necessarily have $\Phi_{\ell_1}(p) \cap \Phi_{\ell_2}(p) = \emptyset$.

  Hence,

$$p-1 = \#\Phi(p) = \sum_{\ell \mid p-1} \#\Phi_\ell(p)$$

- We will show that:

$$\sum_{\ell \mid p-1} \varphi(\ell) = p-1.$$

- and that:

$$\#\Phi_\ell(p) \leq \varphi(\ell)$$

$$\#\Phi_\ell(p) = \varphi(\ell) > 0.$$

Properties of $\varphi(-)$

1) $\varphi(-)$ is multiplicative.

Namely, $\varphi(mn) = \varphi(m)\varphi(n)$ whenever $GCD(m,n)=1$.

2) $\varphi(p^e) = p^{e-1}(p-1)$

3) $\sum_{d|n} \varphi(d) = n$

$$(f \star g)(n) = \sum_{d|n} f(d)\, g\left(\frac{n}{d}\right)$$

Rmk: ALL of above can be deduced from

*) $\varphi = \mu \star id$

But we haven't proven it.

1): By HW3 S.(e)

"Suppose f and g are multiplicative. Then so is $f \star g$".

2): $$\varphi(p^e) = \sum_{k=0}^{e} \mu(p^k)\, p^{e-k}$$ $\mathcal{D}(p^e) = \{p^k \mid 0 \le k \le e\}$

$$= \underbrace{p^e}_{k=0} - \underbrace{p^{e-1}}_{k=1} + 0 = p^{e-1}(p-1).$$

3): $$\sum_{d \mid n} \varphi(d) = (\varphi \star \mathbb{1})(n)$$ constant function $\mathbb{1}(n) = 1$.

(Möbius inversion formula) $f = \mu \star g \iff g = \mathbb{1} \star f$

Apply it to φ and id, we see that

$$*) \iff 3)$$

But we haven't proven it.

Plan: Prove *) by analyzing $\Phi(n)$. Then 1) & 2) follows.

Then prove 3) by a different analysis. We'll not use Möbius inversion.

$$\Phi(n) = \{ x \in \mathbb{N} \mid 0 \leq x < n,\ GCD(x, n) = 1 \}.$$

$$A = \{0, 1, \cdots, n-1\} \qquad B_d = \{ a \in A \mid d \text{ is a divisor of } a \}$$

Then:

$$\Phi(n) = A \setminus \bigcup_{\substack{d>1 \\ d \mid n}} B_d$$

but this is NOT a disjoint union.

- $\# B_d = \frac{n}{d}$

  0, 1, ⋯, d−1
  d, d+1, ⋯, 2d−1
  ⋯ ⋯

- If $d_1 \mid d_2$, then $B_{d_1} \supset B_{d_2}$

So we can focus on B_p, where p is a prime factor of n.

$$\Phi(n) = A \setminus \bigcup_{\substack{p \mid n \\ p \text{ is prime}}} B_p$$

Still overlap ...

Lemma (Inclusion-Exculsion Principal)

$$\# \bigcup_{i \in I} S_i = \sum_{i \in I} \# S_i - \sum_{i_1, i_2 \in I} \#(S_{i_1} \cap S_{i_2}) + \cdots + \sum_{i_1, \cdots, i_k \in I} (-1)^{k+1} \#(S_{i_1} \cap \cdots \cap S_{i_k}) + \cdots$$

Proof. See Math100.

Apply it to B_p, we have : $I = \{\text{prime divisors of } n\}$

$$\# \bigcup_{p \in I} B_p = \sum_{k \geq 1} \sum_{p_1, \cdots, p_k \in I} (-1)^{k+1} \#(B_{p_1} \cap \cdots \cap B_{p_k})$$

Now,

$$B_{p_1} \cap \cdots \cap B_{p_k} = \{ a \in A \mid a \text{ is divided by } p_1, \cdots, p_k \}$$

$$= \{ a \in A \mid a \text{ is divided by } p_1 \cdots p_k \} = B_{p_1 \cdots p_k}$$

So we have :

$$\underset{\Phi(n)}{\varphi(n)} = \overset{A}{n} - \sum_{k \geq 1} (-1)^{k+1} \sum_{p_1, \cdots, p_k \in I} \# B_{p_1 \cdots p_k}$$

(option 1)
$$= n - \sum_{k \geq 1} (-1)^{k+1} \sum_{p_1, \cdots, p_k \in I} \frac{n}{p_1 \cdots p_k}$$

$$= n \left(1 - \sum_{p \in I} \frac{1}{p} + \sum_{p_1, p_2 \in I} \frac{1}{p_1 p_2} + \cdots \right)$$

$$= n \prod_{p \in I} \left(1 - \frac{1}{p} \right)$$

(option 2) $$= n + \sum_{k\geq 1} (-1)^k \sum_{p_1,\cdots,p_k \in I} \# B_{p_1\cdots p_k}$$

But what is the set $\{ a \mid a = p_1 \cdots p_k$ for some k and some $p_1,\cdots,p_k \in I \}$?

It is exactly the set of square-free divisors of n !

Moreover,
$$\mu(p_1\cdots p_k) = (-1)^k .$$

$$\mu(N) = \begin{cases} 1 & \text{if } N=1 \\ 0 & \text{if } N \text{ is NOT s.f.} \\ (-1)^t & \text{if } N = p_1\cdots p_t \end{cases}$$

So $$\varphi(n) = n + \sum_{\substack{d>1 \\ \text{is a sfd. of } n}} \mu(d)\frac{n}{d}$$

$$= \sum_{d\mid n} \mu(d)\frac{n}{d} = (\mu * \mathrm{id})(n)$$

$\boxed{\text{证}}$

Proof of 3): Want to show $\sum_{d|n} \varphi(d) = n$

$$\Phi(n) = \{ x \in \mathbb{N} \mid 0 \leq x < n,\ GCD(x, n) = 1 \}$$

$A = \{0, 1, \cdots, n-1\}$ $\quad$ $C_d = \{ a \in A \mid GCD(a, n) = d \}$

In particular, $C_1 = \Phi(n)$.

Note that $\begin{cases} C_d \cap C_{d'} = \emptyset \text{ whenever } d \neq d'. \\ A = \bigcup_{d|n} C_d \end{cases}$

Therefore, $n = \sum_{d|n} \# C_d$

$$C_d \underset{g}{\overset{f}{\rightleftarrows}} \Phi\left(\frac{n}{d}\right) \qquad \text{Hence } \# C_d = \varphi\left(\frac{n}{d}\right).$$

$$f: a \in C_d \rightsquigarrow f(a) := \frac{a}{d}.$$

$$\left.\begin{array}{l} \text{Then } 0 \le a < n \Rightarrow 0 \le \frac{a}{d} < \frac{n}{d} \\ \mathrm{GCD}(a, n) = d \Rightarrow \mathrm{GCD}\left(\frac{a}{d}, \frac{n}{d}\right) = 1. \end{array}\right\} \Rightarrow \frac{a}{d} \in \Phi\left(\frac{n}{d}\right)$$

$$g: b \in \Phi\left(\frac{n}{d}\right) \rightsquigarrow g(b) := bd.$$

$$\left.\begin{array}{l} \text{Then } 0 \le b < \frac{n}{d} \Rightarrow 0 \le bd < n \\ \mathrm{GCD}\left(b, \frac{n}{d}\right) = 1 \Rightarrow \mathrm{GCD}(bd, n) = d \end{array}\right\} \Rightarrow bd \in C_d$$

One can verify that $f \circ g = \mathrm{id}_{\Phi(\frac{n}{d})}$ and $g \circ f = \mathrm{id}_{C_d}$.

$\blacksquare$

Next: Study $\Phi_\ell(p) := \{ a \in \Phi(p) \mid \ell(a) = \ell \}$.

Want To Show : $\# \Phi_\ell(p) \leqslant \varphi(\ell)$

Suppose $\Phi_\ell(p) \neq \emptyset$ and $a \in \Phi_\ell(p)$.

For $e = 0, 1, \cdots, \ell - 1$, we have $(a^e)^\ell \equiv (a^\ell)^e \equiv 1 \mod p$

Since $\ell(a) = \ell$, $\bar{a}^0, \bar{a}^1, \cdots, \bar{a}^{\ell-1}$ are distinct. (They are exactly the classes in the cycle.)

sols to "$X^\ell \equiv 1 \mod p$"

will prove later.

By the knowledge of polynomials, $\# \Phi_\ell(p) \leq \# \text{sols} \leq \ell$

Hence, $\Phi_\ell(p) \subseteq \{ \bar{a}^0, \bar{a}^1, \cdots, \bar{a}^{\ell-1} \}$

Q: Among them, which are contained in $\Phi_\ell(p)$?

For any $k>0$,

$$(a^e)^k \equiv 1 \bmod p \Leftrightarrow \ell \mid ek \overset{*}{\Leftrightarrow} \frac{\ell}{GCD(e,\ell)} \mid k$$

proof of $*$: By Bézout Identity, $\exists\, x, y \in \mathbb{Z}$ s.t. $ex+\ell y = GCD(e,\ell)$. So

$$exk + \ell yk = GCD(e,\ell)\cdot k$$

$(\Rightarrow)$ $\ell \mid ek \rightsquigarrow \exists\, z \in \mathbb{Z}$ s.t. $ek = z\ell$. So $k = \frac{\ell}{GCD(e,\ell)}(yk+xz)$

$(\Leftarrow)$ $\frac{\ell}{GCD(e,\ell)} \mid k \rightsquigarrow \exists\, z \in \mathbb{Z}$ s.t. $k\cdot GCD(e,\ell) = \ell z$. So $\ell \mid k\cdot GCD(e,\ell) \mid ke$.

Hence, $\ell(a^e) = \frac{\ell}{GCD(e,\ell)}$. So $a^e \in \Phi_\ell(p) \Leftrightarrow GCD(e,\ell)=1$.

Hence, $\Phi_\ell(p) = \{\bar{a}^e \mid GCD(e,\ell)=1\} \xrightarrow{\sim} \Phi(\ell)$

Consequently, $\#\Phi_\ell(p) = \varphi(\ell)$ if it is not empty.

Nov. 2

After-class reading

- This webpage provides an animated illustration of modular dynamics.
- If you are not familiar with the *inclusion-exclusion principal*, you can read 3.7 of the textbook **Book of Proofs** (Third Edition) by Richard Hammack.
- I encourage you to prove the formula

$$\prod_{p\in I}(1-\frac{1}{p}) = 1 + \sum_{p\in I}\frac{(-1)^1}{p} + \sum_{p_1,p_2\in I}\frac{(-1)^2}{p_1p_2} + \cdots + \sum_{p_1,\cdots,p_k\in I}\frac{(-1)^k}{p_1\cdots p_k} + \cdots .$$

- We will discuss polynomials over $\mathbb{F}_p$ next time. Please read pp. 140–146 for preparing.