Primitive root theorem

Recall that a primitive root modulo p is an element of $\Phi(p)$ such that the dynamic of $\boxed{\cdot a \pmod{m}}$ consists of only one circle.

Theorem 4.9.1 (Gauss)

If p is prime, then $\Phi(p)$ contains exactly $\varphi(\varphi(p))$ primitive roots.

Recall that a primitive root modulo p is an element of $\Phi(p)$ such that the dynamic of $\boxed{\cdot a \pmod{m}}$ consists of only one circle.

Theorem 4.9.1 (Gauss)

If p is prime, then $\Phi(p)$ contains exactly $\varphi(\varphi(p))$ primitive roots.

Example 4.9.2

For the prime 7, we have $\varphi(\varphi(7)) = \varphi(6) = 2.$ Indeed, we have exactly two primitive roots 3 and 5.

Proof. For $a \in \Phi(p)$, theorem 4.4.5 tells us the dynamic of $\boxed{\cdot a \pmod{p}}$ consists of cycles of the same length $\ell(a)$. Let $c(a)$ be the number of cycles. Then we have

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

In particular, $\ell(a) \mid p - 1$.

Proof. For $a \in \Phi(p)$, theorem 4.4.5 tells us the dynamic of $\boxed{\cdot a \pmod{p}}$ consists of cycles of the same length $\ell(a)$. Let $c(a)$ be the number of cycles. Then we have

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

In particular, $\ell(a) \mid p - 1$.

Conversly, for each divisor ℓ of $p - 1$, define

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

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

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

1. For distinct divisors $\ell_1 \neq \ell_2$ of $p-1$, we necessarily have $\Phi_{\ell_1}(p) \cap \Phi_{\ell_1}(p) = \varnothing$. Therefore,

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

Proof of the theorem

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

1. For distinct divisors $\ell_1 \neq \ell_2$ of $p-1$, we necessarily have $\Phi_{\ell_1}(p) \cap \Phi_{\ell_1}(p) = \varnothing$. Therefore,

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

2. We will show that

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

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

1. For distinct divisors $\ell_1 \neq \ell_2$ of $p-1$, we necessarily have $\Phi_{\ell_1}(p) \cap \Phi_{\ell_1}(p) = \varnothing$. Therefore,

$$p - 1 = |\Phi(p)| = \sum_{\ell | p-1} |\Phi_\ell(p)|.$$

2. We will show that

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

3. But for each divisor ℓ of $p-1$, we will see that

$$|\Phi_\ell(p)| \leqslant \varphi(\ell).$$

Proof of the theorem

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

1. For distinct divisors $\ell_1 \neq \ell_2$ of $p-1$, we necessarily have $\Phi_{\ell_1}(p) \cap \Phi_{\ell_1}(p) = \varnothing$. Therefore,

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

2. We will show that

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

3. But for each divisor ℓ of $p-1$, we will see that

$$|\Phi_\ell(p)| \leqslant \varphi(\ell).$$

4. Hence, combining 1–3, we must have $|\Phi_\ell(p)| = \varphi(\ell) > 0$. $\square$

$\left|\{\text{primitive roots}\}\right| = \varphi(\varphi(p))$

Properties of $\varphi(\cdot)$

Theorem 4.9.3

Let m *be a positive integer. Then*

$$\varphi(m) = m \prod_{\substack{p \mid m \\ p \in \mathbb{P}}} \left(1 - \frac{1}{p}\right).$$

Theorem 4.9.3

Let m be a positive integer. Then

$$\varphi(m) = m \prod_{\substack{p \mid m \\ p \in \mathbb{P}}} \left(1 - \frac{1}{p}\right).$$

Corollary 4.9.4

The function $\varphi(\,\cdot\,)$ is multiplicative and $\varphi(p^e) = p^{e-1}(p-1)$ for any prime p.

Proof. The formula follows from careful study of the following sets:

$$A := \{0, 1, \cdots, m-1\}, \qquad B_d := \left\{a \in A \,\middle|\, a \text{ is a multiple of } d\right\}.$$

Proof. The formula follows from careful study of the following sets:

$$A := \{0, 1, \cdots, m-1\}, \qquad B_d := \left\{a \in A \,\middle|\, a \text{ is a multiple of } d\right\}.$$

First note that

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

Proof. The formula follows from careful study of the following sets:

$$A := \{0, 1, \cdots, m-1\}, \qquad B_d := \left\{a \in A \,\middle|\, a \text{ is a multiple of } d\right\}.$$

First note that

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

Note that: whenever $d_1 \mid d_2$, we must have $B_{d_1} \supseteq B_{d_2}$. Therefore, we may only focus on B_p with p being a prime divisor of m:

$$\Phi(m) = A \setminus \bigcup_{\substack{p \mid m \\ p \in \mathbb{P}}} B_p.$$

But there are still overlaps.

We need the following result from combinatorics:

Lemma 4.9.5 (Inclusion - exclusion principle)

$$\left|\bigcup_{i\in I} S_i\right| = \sum_{k\geqslant 1}(-1)^{k-1} \sum_{i_1,\cdots,i_k\in I} \left|S_{i_1}\cap\cdots\cap S_{i_k}\right|.$$

We need the following result from combinatorics:

Lemma 4.9.5 (Inclusion - exclusion principle)

$$\left|\bigcup_{i\in I} S_i\right| = \sum_{k\geqslant 1}(-1)^{k-1} \sum_{i_1,\cdots,i_k\in I} \left|S_{i_1}\cap\cdots\cap S_{i_k}\right|.$$

Note that if $p_1,\cdots,p_k$ are distinct primes, then $\operatorname{lcm}(p_1,\cdots,p_k) = p_1\cdots p_k$. Hence,

$$B_{p_1}\cap\cdots\cap B_{p_k} = B_{p_1\cdots p_k}$$

Properties of $\varphi(\,\cdot\,)$

We need the following result from combinatorics:

Lemma 4.9.5 (Inclusion - exclusion principle)

$$\left|\bigcup_{i\in I} S_i\right| = \sum_{k\geqslant 1}(-1)^{k-1}\sum_{i_1,\cdots,i_k\in I}\left|S_{i_1}\cap\cdots\cap S_{i_k}\right|.$$

Note that if $p_1,\cdots,p_k$ are distinct primes, then $\mathrm{lcm}(p_1,\cdots,p_k) = p_1\cdots p_k$. Hence,

$$B_{p_1}\cap\cdots\cap B_{p_k} = B_{p_1\cdots p_k}$$

Apply the inclusion - exclusion principle to the sets B_p, where p ranges over prime divisors of m (let's denote this set by I):

$$|\Phi(m)| = |A| - \sum_{k\geqslant 1}(-1)^{k-1}\sum_{p_1,\cdots,p_k\in I}\left|B_{p_1\cdots p_k}\right|$$

On the other hand, it is clear that $|B_d| = \frac{m}{d}$ whenever $d \mid m$. Thus, we obtain from the previous identity that

$$\varphi(m) = m - \sum_{k \geqslant 1} (-1)^{k-1} \sum_{p_1, \cdots, p_k \in I} \frac{m}{p_1 \cdots p_k}$$

On the other hand, it is clear that $|B_d| = \frac{m}{d}$ whenever $d \mid m$. Thus, we obtain from the previous identity that

$$\begin{aligned}\varphi(m) &= m - \sum_{k\geqslant 1}(-1)^{k-1}\sum_{p_1,\cdots,p_k\in I}\frac{m}{p_1\cdots p_k}\\ &= m\left(1-\sum_{k\geqslant 1}(-1)^{k-1}\sum_{p_1,\cdots,p_k\in I}\frac{1}{p_1\cdots p_k}\right)\end{aligned}$$

On the other hand, it is clear that $|B_d| = \frac{m}{d}$ whenever $d \mid m$. Thus, we obtain from the previous identity that

$$\begin{aligned}
\varphi(m) &= m - \sum_{k \geqslant 1} (-1)^{k-1} \sum_{p_1, \cdots, p_k \in I} \frac{m}{p_1 \cdots p_k} \\
&= m \left(1 - \sum_{k \geqslant 1} (-1)^{k-1} \sum_{p_1, \cdots, p_k \in I} \frac{1}{p_1 \cdots p_k} \right) \\
&= m \prod_{p \in I} \left(1 - \frac{1}{p} \right).
\end{aligned}$$

$\square$

Theorem 4.9.6

$$\sum_{d \mid m} \varphi(d) = m.$$

Theorem 4.9.6

$$\sum_{d \mid m} \varphi(d) = m.$$

Proof. Consider the following sets:

$$A := \{0, 1, \cdots, m-1\}, \qquad C_d := \{a \in A \mid \gcd(a, m) = d\}.$$

Theorem 4.9.6

$$\sum_{d \mid m} \varphi(d) = m.$$

Proof. Consider the following sets:

$$A := \{0, 1, \cdots, m-1\}, \qquad C_d := \{a \in A \mid \gcd(a, m) = d\}.$$

Note that whenever $d_1 \neq d_2$, we must have $C_{d_1} \cap C_{d_2} = \varnothing$. Therefore,

$$|A| = \sum_{d \mid m} |C_d|.$$

It remains to relate $|C_d|$ and $\varphi(d)$.

We finish the proof by showing that C_d is bijective to $\Phi(\frac{m}{d})$.

We finish the proof by showing that C_d is bijective to $\Phi(\frac{m}{d})$.

For any $a \in C_d$, we have

- Since $0 \leqslant a < m$, we have $0 \leqslant \frac{a}{d} < \frac{m}{d}$.
- Since $\gcd(a, m) = d$, we have $\gcd(\frac{a}{d}, \frac{m}{d}) = 1$.

Therefore, $\frac{a}{d} \in \Phi(\frac{m}{d})$.

We finish the proof by showing that C_d is bijective to $\Phi(\frac{m}{d})$.

For any $a \in C_d$, we have

- Since $0 \leqslant a < m$, we have $0 \leqslant \frac{a}{d} < \frac{m}{d}$.
- Since $\gcd(a, m) = d$, we have $\gcd(\frac{a}{d}, \frac{m}{d}) = 1$.

Therefore, $\frac{a}{d} \in \Phi(\frac{m}{d})$. In this way, we obtain a map from C_d is to $\Phi(\frac{m}{d})$. It is not difficult to verify that it is bijective. $\square$

Dirichlet convolution

Definition 4.9.7

Let f and g be two arithmetic functions. Then their *Dirichlet convolution* $f \star g$ is the arithmetic function

$$f \star g \colon m \longmapsto \sum_{d \mid m} f(d) g\left(\frac{m}{d}\right).$$

Definition 4.9.7

Let f and g be two arithmetic functions. Then their *Dirichlet convolution* $f \star g$ is the arithmetic function

$$f \star g \colon m \longmapsto \sum_{d \mid m} f(d) g\left(\frac{m}{d}\right).$$

The set of arithmetic functions equipped with the Dirichlet convolution (and the neural element for $\star$) is an abelian monoid. Moreover, it becomes a ring after equipped with addition of functions (see supplementary notes for more details).

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

Theorem 4.9.6 can be interpreted as:

$$\varphi \star \mathbf{1} = \mathrm{id},$$

where $\mathbf{1}$ is the constant function mapping any positive integer to 1, id is the identity function mapping any positive number to itself.

Theorem 4.9.6 can be interpreted as:

$$\varphi \star \mathbf{1} = \mathrm{id},$$

where $\mathbf{1}$ is the constant function mapping any positive integer to 1, id is the identity function mapping any positive number to itself.

The *Möbius inversion formula* says that

$$f = g \star \mu \iff g = f \star \mathbf{1}\,.$$

Hence, theorem 4.9.6 is equivalent to the following one:

$$\varphi = \mathrm{id} \star \mu = \mu \star \mathrm{id}\,.$$

Dirichlet convolution

Let's spell out $\mu \star \mathrm{id}$.

Let's spell out $\mu \star \mathrm{id}$.

For any positive integer m, we have

$$(\mu \star \mathrm{id})(m) = \sum_{d \mid m} \mu(d) \frac{m}{d}$$

Recall that

$$\mu(x) := \begin{cases} 1 & \text{if } x = 1, \\ 0 & \text{if } x \text{ is NOT sqaure-free,} \\ (-1)^k & \text{if } x \text{ is sqaure-free and has exactly } k \text{ prime divisors.} \end{cases}$$

Therefore,

$$(\mu \star \mathrm{id})(m) = m + \sum_{k \geqslant 1} (-1)^k \sum_{p_1, \cdots, p_k \in I} \frac{m}{p_1 \cdots p_k},$$

Therefore,

$$(\mu \star \mathrm{id})(m) = m + \sum_{k \geqslant 1} (-1)^k \sum_{p_1, \cdots, p_k \in I} \frac{m}{p_1 \cdots p_k},$$

which we have seen equal to

$$m \prod_{\substack{p \mid m \\ p \in \mathbb{P}}} \left(1 - \frac{1}{p}\right).$$

So theorems 4.9.3 and 4.9.6 are equivalent through the *Möbius inversion formula*.

Some remarks:

- Without spelling out $\mu \star \mathrm{id}$, the identity $\varphi = \mu \star \mathrm{id}$ itself already implies that φ is multiplicative since both μ and id are multiplicative.

Some remarks:

- Without spelling out $\mu \star \mathrm{id}$, the identity $\varphi = \mu \star \mathrm{id}$ itself already implies that φ is multiplicative since both μ and id are multiplicative.
- So we can only spell out $(\mu \star \mathrm{id})(p^e)$, where p is a prime. But this is clear since we know $\mathscr{D}(p^e) = \{1, p, \cdots, p^e\}$, and among them, only 1 and p are square-free.

$$\varphi(p^e) = \sum_{\substack{p^k \\ 0 \le k \le e}} \mu(p^k)\, p^{e-k} = 1 \cdot p^e + (-1) \cdot p^{e-1}$$
$$= p^{e-1} \cdot (p-1).$$