Introduction to Number Theory

Math 110 | Winter 2023

Xu Gao

February 17, 2023

What we have seen last time

- Discrete logarithm
- Some cryptography
- Primitive root theorem

Today's topics

- Properties of $\varphi(\,\cdot\,)$
- Dirichlet convolution

Proof of primitive root theorem

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

$\shortparallel$

Proof. 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

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

today

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

next week

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

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

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

Theorem 16.1

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

$= p^{e-1}(p-1)$

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 16.2

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

m, n coprime $\quad \varphi(mn) = mn \prod_{p \mid mn} (1-\frac{1}{p}) = \underbrace{m \prod_{p \mid m} (1-\frac{1}{p})}_{\varphi(m)} \cdot \underbrace{n \prod_{p \mid n} (1-\frac{1}{p})}_{\varphi(n)}$

$\hookrightarrow$ $p \mid m$ or $p \mid n$ but not both

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

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

whenever d has a proper divisor $d' > 1$ then we can drop 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:

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

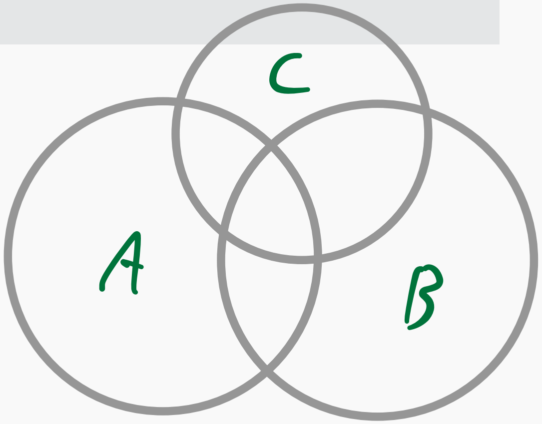
But there are still overlaps. e.g. $B_{pq} \subseteq B_p$ & B_q

We need the following result from combinatorics:

Lemma 16.3 (Inclusion - exclusion principle) $\sum_{i\in I}|S_i| - \sum_{\substack{i,j\in I\\ i\neq j}}|S_i\cap S_j|$

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

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,



$$B_{p_1}\cap\cdots\cap B_{p_k} = \underbrace{B_{p_1\cdots p_k}}_{\{\text{common multiple of } p_1,\cdots,p_k\}}$$

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):

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

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

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

"Euler product" $\square$

Theorem 16.4

$d \mapsto \frac{m}{d}$ is bijective on $\mathcal{D}(m)$

$$\sum_{d|m} \varphi\left(\frac{m}{d}\right) = \sum_{d|m} \varphi(d) = m.$$

Proof. Consider the following sets:

$$A = \bigcup_{d|m} C_d$$

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

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

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

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

Proof. 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

Dirichlet convolution

Definition 16.5

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 HW 5 for more details).

$$\sum_{d \mid n} \varphi(d) \cdot 1 = n$$

Theorem 16.4 can be interpreted as:

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

where **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 16.4 is equivalent to the following one:

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

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

For any positive integer m, we have

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

Recall that

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

m

0

$x = p_1 \cdots p_k$

$(-1)^k \frac{m}{p_1 \cdots p_k}$

Dirichlet convolution

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 16.1 and 16.4 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.
- 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.

$$\varphi(p^e) = \underbrace{\mu(1) \cdot p^e}_{1} + \underbrace{\mu(p) \cdot \frac{p^e}{p}}_{p} = p^e - p^{e-1}$$

Dirichlet convolution

Our argument of

$$\varphi(m) = |\Phi(m)| = \sum_{\ell \mid \varphi(m)} |\Phi_\ell(m)|$$

and

$$\sum_{\ell \mid \varphi(m)} \varphi(\ell) = \varphi(m)$$

works for any modulus m. So why the *primitive root theorem* may fail for general m? This could only because there are cases where

$$|\Phi_\ell(m)| > \varphi(\ell).$$

Exercise 16.1

Let $m = 20$ be the modulus.

1. Compute $\ell(a)$ for all $a \in \Phi(20)$ and conclude that there is no primitive root modulo 20.
2. However, compute $\varphi(\varphi(20))$. In particular, it is nonzero.
3. Find all $\ell \mid \varphi(20)$ such that $|\Phi_\ell(20)| > \varphi(\ell)$.

The following algebraic result is used in the lecture.

Exercise 16.2 "Euler product"

Show that

$$\prod_{i\in I}\left(1-\frac{1}{x_i}\right)=\sum_{k\geqslant 1}(-1)^k\sum_{i_1,\cdots,i_k\in I}\frac{1}{x_{i_1}\cdots x_{i_k}}.$$