Lecture 14: Basic number theory

Nitin Saxena ⋆

IIT Kanpur

1 Euler's totient function ϕ

The case when n is not a prime is slightly more complicated. We can still do modular arithmetic with division if we only consider numbers coprime to n.

For $n \geq 2$, let us define the set,

$$\mathbb{Z}_n^* := \{k \mid \ 0 \leq k < n, \gcd(k,n) = 1\}\,.$$

The cardinality of this set is known as *Euler's totient function* $\phi(n)$, i.e., $\phi(n) = |\mathbb{Z}_n^*|$. Also, define $\phi(1) = 1$.

Exercise 1. What are $\phi(5),\ \phi(10),\ \phi(19)$?

Exercise 2. Show that $\phi(n) = 1$ iff $n \in [2]$.

Show that $\phi(n) = n - 1$ iff n is prime.

Clearly, for a prime p, $\phi(p) = p - 1$. What about a prime power $n = p^k$? There are p^{k-1} numbers less than n which are NOT coprime to n (Why?). This implies $\phi(p^k) = p^k - p^{k-1}$. How about a general number n?

We can actually show that $\phi(n)$ is an almost *multiplicative* function. In the context of number theory, it means,

Theorem 1 (Multiplicative). *If m and n are coprime to each other, then $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$.*

Proof. Define $S := \mathbb{Z}_m^* \times \mathbb{Z}_n^* = \{(a,b) : \ \ a \in \mathbb{Z}_m^*,\ b \in \mathbb{Z}_n^*\}$. We will show a bijection between $\mathbb{Z}_{mn}^*$ and $S = \mathbb{Z}_m^* \times \mathbb{Z}_n^*$. Then, the theorem follows from the observation that $\phi(mn) = |\mathbb{Z}_{mn}^*| = |S| = |\mathbb{Z}_m^*||\mathbb{Z}_n^*| = \phi(m)\phi(n)$.

The bijection $\psi : S \to \mathbb{Z}_{mn}^*$ is given by the map $\psi : (a,b) \mapsto bm + an \mod mn$. We need to prove that ψ is a bijection. That amounts to proving these three things.

- The mapping is valid, i.e., if $a \in \mathbb{Z}_m^*$ and $b \in \mathbb{Z}_n^*$ then $bm + an \in \mathbb{Z}_{mn}^*$. This follows from the fact that bm is coprime to n implies $bm + an$ is coprime to n. Similarly $bm + an$ is coprime to m. So $bm + an$ is coprime to mn (and we use its residue representative in $[mn-1]$).
- Mapping ψ is injective (one to one). Why?
  If $bm + an = b'm + a'n \mod mn$ implies $(b - b')m + (a - a')n = 0 \mod mn$. The latter implies, using coprimality of m, n, that $n|(b - b')$ and $m|(a - a')$. Thus, $(a,b) = (a',b')$ in S.
- Mapping ψ is surjective (onto). Why?
  Consider $t \in \mathbb{Z}_{mn}^*$. Compute $k := tm^{-1} \mod n$. (Note: $k \in \mathbb{Z}_n^*$.) Since $t = km \mod n$ we can write $t = km + \ell n$. If need be, reduce ℓ to $\ell' \mod m$. This achieves both $t = km + \ell' n \mod mn$ and $\ell' \in \mathbb{Z}_m^*$.

These three properties of ψ finish the proof.

□

Exercise 3. Find numbers m, n such that $\phi(mn) \neq \phi(m)\phi(n)$.

⋆ Edited from Rajat Mittal's notes.

Fundamental theorem of arithmetic implies that we can express any number as a product of prime powers. By using Thm 1, we can calculate $\phi(mn)$, when $\phi(m)$ and $\phi(n)$ are given to us (m and n are coprime).

Theorem 2. *If $n = p_1^{k_1} p_2^{k_2} \cdots p_\ell^{k_\ell}$ is a natural number. Then,*

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_\ell}\right).$$

Exercise 4. Prove the above theorem using the argument above.

2 Inclusion-Exclusion vs. Möbius Inversion

There is another way to look at Thm. 2. We are interested in finding out the number of elements between 0 and $n-1$ which do not share a factor with $n = p_1^{k_1} p_2^{k_2} \cdots p_\ell^{k_\ell}$. Let us consider all the elements $\{0, 1, \cdots, n-1\}$.

Define A_i to be the set of elements which are divisible by p_i. For any $I \subseteq [\ell]$, define A_I to be the set of elements which are divisible by all p_i where $i \in I$. You can see that we are interested in the event when none of the p_i's, where $i \in [\ell]$, divide an element. This is a straightforward application of *inclusion-exclusion*,

$$\phi(n) = \sum_{I \subseteq [\ell]} (-1)^{|I|} \cdot |A_I|.$$

Notice that the number of elements which are divisible by $p_1 p_2 \cdots p_j$ is just $\frac{n}{p_1 p_2 \cdots p_j}$. This gives us,

$$|A_I| = \frac{n}{\prod_{i \in I} p_i}.$$

So,

$$\phi(n) = \sum_{I \subseteq [\ell]} (-1)^{|I|} \frac{n}{\Pi_{i \in I} p_i}. \tag{1}$$

Exercise 5. Prove that the above expression is the same as the one in Thm. 2.

In Eqn. 1, the sum is taken over all *square-free* (i.e. of the form $p_1 p_2 \cdots p_i$ with distinct primes) divisors of n. Define a function, $\mu(k)$,

$$\mu(k) := \begin{cases} 1, & \text{if } k = 1 \\ 0, & \text{if } a^2 \mid k \text{ for some } a \geq 2 \\ (-1)^r, & \text{if } k \text{ is square-free with } r \text{ primes.} \end{cases}$$

This function $\mu(k)$ is called the *Möbius function*. Then Eqn. 1 can be rewritten as,

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

Exercise 6. For an integer $n \geq 2$ show that, $\sum_{d|n} \mu(d) = 0$.

$\mu(k)$ is a *multiplicative* function, i.e. for coprime a, b, $\mu(a) \cdot \mu(b) = \mu(ab)$. This can be used to deduce that $\sum_{d|n} \mu(p) = \prod_{i \in [\ell]} (1 + \mu(p_i)) = \mu(p_1) + \mu(p_2) + \cdots + \mu(p_1^{k_1}) = \prod_{i \in [\ell]} (1 + \mu(p_i^2)) = 0$.

Möbius function is really useful in number theory, and combinatorics. One of the main reasons is the "inversion property" (for special functions f).

Theorem 3 (Möbius inversion). *Let f and g be functions defined on natural numbers. Then,*

$$f(n) = \sum_{d \mid n} g(d) \quad \textit{implies} \quad g(n) = \sum_{d \mid n} \mu(d) f\left(\frac{n}{d}\right).$$

Proof. Let us look at RHS of the expression for $g(n)$:

$$\begin{aligned}\sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) &= \sum_{d|n} \mu(d) \sum_{c|n/d} g(c) \\ &= \sum_{c|n} g(c) \left(\sum_{d|n/c} \mu(d) \right) \\ &= g(n)\mu(1) = g(n)\,.\end{aligned}$$

The third equality follows from the fact that $\sum_{d|n} \mu(d)$ is 0 for $n \geq 2$ (is 1 for $n = 1$). The second equality is sum-swapping.

Exercise 7. Prove the second equality by considering the pairs (c, d) s.t. $d \mid n$ and $c \mid n/d$.

□

Functions f and g are called *Möbius transforms* of each other. Eg. n and $\phi(n)$ are Möbius transforms of each other!

Exercise 8. Finite fields are routinely used in computer science. Read up on how to use Möbius inversion to count the number of irreducible polynomials, of degree d, over a finite field.

References

1. N. L. Biggs. Discrete Mathematics. *Oxford University Press*, 2003.
2. P. J. Cameron. Combinatorics: Topics, Techniques and Algorithms. *Cambridge University Press*, 1994.
3. K. H. Rosen. Discrete Mathematics and Its Applications. *McGraw-Hill*, 1999.