Lecture 13: Basic number theory

Nitin Saxena *

IIT Kanpur

1 Inverse modulo n: or how to solve linear equations

We noticed before that $ab = ac \mod n$ need not imply $b = c \mod n$. This is because $n \mid a(b - c)$ implies $n \mid b - c$ only when $\gcd(a, n) = 1$.

But if a and n are coprime to each other then there exists an integer k, s.t., $ka = 1 \mod n$ (ref. Bézout's identity). The number k (more precisely the residue class of k modulo n) is called the *inverse of a modulo n* and is denoted as $a^{-1} \mod n$.

If inverse of a exist, then,

$$ab = ac \mod n \Rightarrow a^{-1}ab = a^{-1}ac \mod n \Rightarrow b = c \mod n\,.$$

When n is a prime, then any $0 < a < n$ has GCD 1 with n. In this case, inverse exist for all a not divisible by n. Hence, while computing modulo a prime p, we can divide (or cancel) freely.

Exercise 1. Find the following quantities,

1. $2^{-1} \mod 11$.
2. $16^{-1} \mod 13$.
3. $92^{-1} \mod 23$.

Exercise 2. Give an algorithm to find $a^{-1} \mod n$. What previous algorithm can you use?

Exercise 3. Give an algorithm to solve the linear equation $aX = b \mod n$, to find the unknown X.

Let us look at one of the oldest theorems in number theory, whose proof inspires several other proofs in mathematics.

Theorem 1 (Fermat's little theorem, 1640). *Given a prime number p and an integer a coprime to p,*

$$a^{p-1} = 1 \mod p\,.$$

Proof. We will look at the set $S = \{a, 2a, 3a, \cdots, (p-1)a\}$. Since a is coprime to p, no element $ka = 0 \mod p$ if $k \neq 0 \mod p$.

Exercise 4. Show that $\nexists s \neq t \in S : s = t \mod p$.

The previous exercise shows that S has $p - 1$ distinct entries all ranging from 1 to $p - 1$. So S is just a permutation of the set $T = \{1, 2, \cdots, p-1\}$. Taking product of all entries in S and T modulo p, we get,

$$a \cdot 2a \cdots (p-1)a \;=\; 1 \cdot 2 \cdots (p-1) \mod p\,.$$

Cancelling the $(p-1)!$ term from both sides,

$$a^{p-1} = 1 \mod p\,.$$

□

* Edited from Rajat Mittal's notes.

Exercise 5. Prove that $a^p = a \mod p$ for any prime p and any integer a.

This shows that exponentiation in prime modulus is very special!

Exercise 6. For a composite n, and any a, what can you say about $a^n \mod n$?

Nothing special. However, we can prove an alternate statement. For coprime a, n modify the above proof to deduce that $a^{\phi(n)} = 1 \mod n$, where $\phi(n)$ is the number of elements in $[n-1]$ that are coprime to n. When a, n share a factor then there is no good property.

2 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 7. What are $\phi(5),\ \phi(10),\ \phi(19)$?

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

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.