Lecture 4: Number theory

Rajat Mittal

IIT Kanpur

In the next few classes we will talk about the basics of *number theory*. Number theory studies the properties of natural numbers and is considered one of the most beautiful branches of mathematics. In this lecture note, numbers means natural numbers or integers depending upon the context.

1 Fundamental theorem of arithmetic

The first task for us would be to derive the fact that every number has a unique prime factorization (*fundamental theorem of arithmetic*) from the basic division algorithm.

Division algorithm says that given two numbers a and b, we can divide a by b obtaining quotient q and remainder $r < b$.

$$a = qb + r$$

Since we have put the condition $r < b$, the quotient and remainder are unique.

Exercise 1. Show that the quotient and the remainder are unique if we assume that remainder is less than b.

A number b divides a if the remainder is zero. We denote it by $b \mid a$. $b \nmid a$ denotes that b does not divide a. If b divides a then a is a multiple of b.

Now we can define the *greatest common divisor (GCD)*. The GCD of two numbers a and b is defined as the biggest number which divides both a as well as b. It is also denoted by $gcd(a, b)$.

One of the important case is when $gcd(a, b) = 1$, i.e., there is no common factor between a and b. We say that a and b are *coprime* to each other.

1.1 Euclid's GCD algorithm

Euclid's GCD algorithm is one of the earliest, most elementary and most important algorithm in the world of mathematics. It gives a recursive way to calculate the GCD.

Suppose we are given two numbers a, b, s.t., $a \geq b$. The algorithm $gcd(a, b)$ is given below.

if $b = 0$ **then**
    Output a
end
if $b = 1$ **then**
    Output 1
end
Say $a = qb + r$, then find $gcd(b, r)$

Algorithm 1: GCD algorithm

The correctness of the procedure relies on the fundamental fact that if $a = qb+r$ then $gcd(a, b) = gcd(b, r)$.

Exercise 2. Can you prove this?

To take an example, lets compute the GCD of 64 and 26.

$$\begin{aligned} gcd(64, 26) &\rightarrow 64 = 2 \times 26 + 12 \\ gcd(26, 16) &\rightarrow 26 = 2 \times 12 + 2 \\ gcd(12, 2) &\rightarrow 12 = 6 \times 2 + 0 \\ gcd(2, 0) &\rightarrow 2 \end{aligned} \tag{1}$$

This shows that $gcd(64, 26) = 2$. In general the equation will look like,

$$\begin{aligned} gcd(a, b) &\rightarrow a = q_1 \times b + r_1 \\ gcd(b, r_1) &\rightarrow b = q_2 \times r_1 + r_2 \\ &\vdots \\ gcd(r_{k-2}, r_{k-1}) &\rightarrow r_{k-2} = q_k \times r_{k-1} + r_k \\ gcd(r_{k-1}, r_k) &\rightarrow r_{k-1} = q_{k+1} \times r_k + 0 \\ gcd(r_k, 0) &\rightarrow r_k \end{aligned} \tag{2}$$

In this case $gcd(a, b)$ will be r_k. Notice that r_1 can be written as an integer combination of a, b, i.e., $r_1 = c_1 a + c_2 b$ for some integers c_1, c_2 using the first equation. Similarly r_2 can be written as an integer combination of b, r_1 and hence a, b.

Keeping track of these coefficients, ultimately we can write the $gcd(a, b) = r_k$ as the integer combination of a, b.

Theorem 1. *Given integers $a, b \geq 0$, there exist two integers k, l, such that,*

$$gcd(a, b) = ka + lb$$

It is clear from the argument before that these coefficients can be obtained by keeping track of coefficients in Euclid's algorithm. This is called the *extended Euclidean algorithm*. You will write this extended Euclidean algorithm as part of the assignment.

Exercise 3. What can you say about the size of k and l?

Using Theorem 1, we can prove the following lemma.

Lemma 1. *Let $gcd(a, b) = 1$. If $a \mid bc$ then $a \mid c$.*

Proof. We know that there exist k, l, such that,

$$1 = ka + lb.$$

Multiplying both sides by c,

$$c = kac + lbc$$

Since a divides both the terms on the right hand side, a divides c too. □

Using this basic lemma, we can prove the fundamental theorem.

1.2 Proof of fundamental theorem of arithmetic

From the definition of primes it is clear that we can start finding the factors of any number n. Either n is prime or it can be written as mm'. If we keep applying this procedure to m and m'. We get that any number n can be written as,

$$n = p_1 p_2 \cdots p_k,$$

for some k, where p_i's are primes. Collecting the same primes in one power, we get the factorization,

$$n = p_1^{l_1} p_2^{l_2} \cdots p_k^{l_k},$$

for some k. This is called the prime factorization of n. It is not clear from the method above that this factorization is unique.

Can two such factorizations exist? It turns out, this factorization is unique up to ordering of primes. For the sake of contradiction, suppose there are two such factorizations $p_1 \cdots p_k$ and $q_1 \cdots q_l$. By cancelling the common primes, we can assume that no p_i is equal to any q_j.

We know that since p_1 is a prime, it will divide either $q = q_1 \cdots q_{l-1}$ or q_l (Lemma 1). If it divides $q = q_1 \cdots q_{l-1}$, we can further divide q and ultimately get that p_1 divides q_i for some i.

This implies that p_1 divides some q_i. But p_1 and q_i are both primes. So, $p_1 = q_i$, which is a contradiction. This gives the theorem,

Theorem 2. *Unique factorization: Given a number n, it can be written in a unique way as a product of primes (unique up to ordering).*

$$n = p_1^{l_1} p_2^{l_2} \cdots p_k^{l_k}$$

Where p_i's are all primes.

2 Modular arithmetic

What is the last digit of 2^{64}? This number is too big and it is very difficult to calculate the last digit by computing the number 2^{64}.

But the problem becomes simpler if you realize that the last digit of 2^{64} is the remainder of 2^{64} when divided by 10. Denote the remainder of n when divided by 10 as $r(n)$. Next observation is, $r(2^{64})$ can be calculated by multiplying $r(2^{32})$ and $r(2^{32})$ and then taking the remainder by 10.

Exercise 4. Prove that $r(ab) = r(r(a)r(b))$.

Applying this technique recursively, we get, $r(2^8) = 6 \Rightarrow r(2^{16}) = 6 \Rightarrow r(2^{32}) = 6 \rightarrow r(2^{64}) = 6$. So the last digit of 2^{64} is 6.

Exercise 5. Show that the last digit of 2^{2^n} for any $n \geq 2$ is 6.

Above example of dealing with remainders is called *modular arithmetic*. There are many uses of modular arithmetic in mathematics, computer science and even in chemistry. Please read the Wikipedia article for more applications.

Let's study modular arithmetic more formally.

Definition 1. *We say $a = b \mod n$ iff $a - b$ is divisible by n.*

Note 1. $a = b \mod n$ is read as, a is congruent to b modulo n. Some books also use the notation, $a \equiv b \mod n$

It is clear from the definition that $a = b \mod n$ then $a = kn + b \mod n$ for any integer k. For a number b, the set $\{b + kn\}$ is called the *residue class* of b modulo n and is denoted $b \mod n$. For example, the set $\{\cdots, -10, -7, -4, -1, 2, 5, 8, 11, \cdots\}$ is the residue class of 2 modulo 3.

The set of all residue classes of n is denoted by $\mathbb{Z}_n$.

Notice that any element $c \in a \mod n$ is of the form $a + kn$ for some k. Using this definition, we can define the operations like addition and multiplication between these modulo classes.

1. $a \mod n + b \mod n = a + b \mod n$
2. $(a \mod n)(b \mod n) = ab \mod n$

We can easily check that these definitions are consistent. For the first relation, this means, take any two elements $c \in a \mod n$ and $d \in b \mod n$. Then $c + d = e \mod n$ for any $e \in (a + b) \mod n$.

Exercise 6. Check the consistency for the second relation.

For doing calculations, it generally makes sense to take the smallest number in $a \mod n$ as the representative and do the calculations using that representative. The representatives will be $\{0, 1, 2, \cdots, n-1\}$ and all of them will belong to different residue class. Whenever doing these calculations, we can subtract any number of the form kn to keep the calculation in the range $\{0, 1, 2, \cdots, m-1\}$.

Another way to say the same things is, $\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$. Where it is understood that 0 stands for the residue class of 0 modulo n and so on. You can add and multiply numbers in this set modulo n.

Exercise 7. What is the last digit of 2^{39}?

Though you should be careful not to overuse your intuition of operations on Integers. For example, if $ab = 0 \mod n$ and $a \neq 0 \mod n$, does not imply that $b = 0 \mod n$. Take $a = 2, b = 3, n = 6$ as an example. This property also tells you that $ab = ac \mod n \not\Rightarrow b = c \mod n$.

Exercise 8. Solve the following questions,

1. What is $1235 \mod 25$?
2. Show that $2468 \times 13579 = -3 \mod 25$.
3. Show that $5^n \mod 10 = 5$ for all n.
4. If n has representation $x_r x_{r-1} \cdots x_1 x_0$ in decimal, i.e., $n = x_0 + 10x_1 + \cdots + 10^r x_r$. Then $n = x_0 + x_1 + \cdots + x_r \mod 9$.
5. Show that $9787 \times 1258 \neq 12342046$ by calculating both sides $\mod 9$.
6. Suppose $3a = 0 \mod p$ where p is a prime and $a < p$. What is p?

2.1 Inverse modulo n

We noticed above 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 exist an integer k, s.t., $ka = 1 \mod n$ (Thm. 1). 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}. If inverse of a exist,

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

When n is a prime, then any $0 < a < p$ 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 freely too.

Exercise 9. Find the following quantities.

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

Exercise 10. Give an algorithm to find $a^{-1} \mod n$. What previous algorithm can you use?

Let's look at one of the nice theorems in number theory.

Theorem 3. *Fermat's little theorem: 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 11. Show that $\nexists s, t \in S : s = t \mod p$.

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

$$a.2a.3a.\cdots.(p-1)a = 1.2.\cdots.(p-1) \mod p.$$

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

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

Hence proved. □

Exercise 12. Prove that $a^p = a \mod p$ for any prime p and any integer a.

3 Euler's totient function

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

Let's define the set,

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

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

Exercise 13. 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 *multiplicative*. In the context of the number theory, it means,

Theorem 4. *If m and n are coprime to each other,*

$$\phi(mn) = \phi(m)\phi(n).$$

Proof. Call $S = \mathbb{Z}_m^* \times \mathbb{Z}_n^* = \{(a, b) : \ a \in \mathbb{Z}_m^*, \ b \in \mathbb{Z}_n^*\}$. 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 map, $\psi(a, b) = bm + an$. 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 co-prime to n implies $bm + an$ is coprime to n. Similarly $bm + an$ is coprime to m. So $bm + an$ is coprime to mn.
- Mapping ψ is injective (one to one). You will prove this in the assignment.
- Mapping ψ is surjective (onto).

  Exercise 14. Any member $t \in \mathbb{Z}_{mn}$ can be written as $t = km + ln \mod n$ where k, l are integers.

  To prove that the mapping is surjective, now we only need to show that if $k \notin \mathbb{Z}_n^*$ or $l \notin \mathbb{Z}_m^*$ then $km + ln \notin \mathbb{Z}_{mn}^*$. This is also left as a simple exercise.

□

Exercise 15. Find m, n, s.t., $\phi(mn) \neq \phi(m)\phi(n)$.

Fundamental theorem of arithmetic implies that we can express any number as product of prime powers. By using Thm 4, we can calculate $\phi(mn)$, when $\phi(m)$ and $\phi(n)$ are given to us (m and n are coprime).

Theorem 5. *If $n = p_1^{k_1} p_2^{k_2} \cdots p_l^{k_l}$ is a natural number. Then,*

$$\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k}).$$

Exercise 16. Prove the above theorem using the argument above.

4 Mobious Inversion

There is another way to look at Thm. 5. We are interested in finding out the number of elements between 0 and n which do not divide $n = p_1^{k_1} p_2^{k_2} \cdots p_l^{k_l}$. Lets 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 $I \subseteq [l]$, 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 $i \in [l]$, divide an element. This is a straightforward application of inclusion-exclusion.

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

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,

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

So,

$$\phi(n) = \sum_{I \subseteq [l]} (-1)^{|I|} \frac{n}{\Pi_{i \in I} p_i}. \tag{3}$$

Exercise 17. Prove that the above expression is same as the one in Thm. 5.

In Eqn. 3, the sum is taken over all square-free (numbers of the form $p_1 p_2 \cdots p_i$) divisors of n. Define a function, $\mu(k)$,

$$\mu(k) = \begin{cases} 1 & \text{if } k = 1 \\ 0 & \text{if } a^2 \mid k \text{ for some } a \geq 2 \\ (-1)^r & \text{if } k = p_1 p_2 \cdots p_r \end{cases}$$

This function $\mu(k)$ is called the *Mobious function*. Then,

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

Exercise 18. For an integer $n \geq 2$, show that,

$$\sum_{d|n} \mu(d) = 0.$$

Hint: Look at the prime factorization of n.

Mobious function is really useful in number theory and one of the reasons is its inversion property.

Theorem 6. *Let f and g be functions defined on natural numbers. If*

$$f(n) = \sum_{d|n} g(d)$$

then

$$g(n) = \sum_{d|n} \mu(d) f(\frac{n}{d}).$$

Proof. Let's look at the right hand side of the expression for $g(n)$.

$$\begin{aligned} \sum_{d|n} \mu(d) f(\frac{n}{d}) &= \sum_{d|n} \mu(d) \sum_{c|n/d} g(c) \\ &= \sum_{c|n} g(c) (\sum_{d|n/c} \mu(d)) \\ &= g(n)\mu(1) \end{aligned} \tag{4}$$

The third equality follows from the fact that $\sum_{d|n} \mu(d)$ is 0 for $n \geq 2$. The second equality is given as an exercise.

Exercise 19. Prove the second equality by considering the pairs (c, d), s.t., $d \mid n$ and $c \mid n/d$.

□

5 Assignment

Exercise 20. Prove the correctness of division algorithm.

Exercise 21. Another definition of $g = gcd(a, b)$ is, g is the number which divides both a, b and any number which divides both a, b also divides g. Show that the two definitions are equivalent.

Exercise 22. Write the extended Euclidean algorithm for GCD

Exercise 23. Solve $x^2 = 10 \mod 13$ by trial and error. There are two solutions.

Exercise 24. Suppose $x^2 = a \mod p$ where p is a prime. Show that for any $0 < a < p$, there are exactly two solutions or none.

Exercise 25. Solve the quadratic equation $x^2 + 3x + 11 = 0 \mod 11$

Exercise 26. Show that a number n is prime iff ,

$$1.2.\cdots.(p-1) = -1 \mod n.$$

This is known as *Wilson's theorem.*

Exercise 27. Solve the equation $x^2 + 5x + 8 = 0 \mod 11$.

Exercise 28. Prove that the mapping ψ as defined in the proof of Thm. 4 is injective (one to one).

Exercise 29. Prove the converse of Thm. 6.

References

1. N. L. Biggs. Discrete Mathematics. *Oxford University Press*, 2003.