Lecture 7: Number Theory

Rajat Mittal*

IIT Kanpur

We will move on to the next topic in discrete mathematics called *number theory*. Number theory studies the properties of natural numbers and is considered one of the most beautiful branches of mathematics; it is also known as the queen of mathematics.

It is one of the earliest branch of mathematics (another one is Geometry), with ample evidence that it was studied in old civilizations like India, China and Mesopotamia. Most of them developed similar ideas and methods independently, some of which we are going to study.

Many famous mathematician, like Pythagoras, Aryabhatta and Diophantus in the earlier times and Gauss, Tao, Bhargava in the recent times, have worked in this field. We will start with the basics of this field and then see some important concepts: Modular arithmetic, Fermat's little theorem and Chinese remaindering.

In this lecture note, numbers means natural numbers or integers depending upon the context.

1 Basics

We will start with the most basic primitive of division between two numbers. Division algorithm says that given two numbers a and b, we can divide a by b obtaining quotient q and remainder $0 \leq r < b$:

$$a = qb + r\,.$$

Eg. $101 = 7 \cdot 14 + 3$.

Exercise 1. Show that the quotient and the remainder are unique if we assume that the remainder is less than b and greater than equal to 0.

Let $a = qb + r = q'b + r'$, implying that $(q - q')b + (r - r') = 0$. The latter gives $b|(r - r')$, but we had assumed that $0 \leq r, r' < b$.

A number b *divides* a if the remainder is zero. We denote it by $b \mid a$. Similarly, $b \nmid a$ denotes that b does not divide a. If b divides a then a is a *multiple* of b. Eg. $7 \nmid 101$, $7|105$.

With the definition of divisibility, 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 cases is when $\gcd(a, b) = 1$, i.e., there is no common factor between a and b. In this case, we say that a and b are *coprime* to each other.

Exercise 2. How can you calculate the GCD of two numbers?

1.1 Euclid's GCD algorithm (c.300 BC)

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

Suppose we are given two numbers a, b s.t. $a \geq b \geq 0$. The algorithm $\gcd(a, b)$ is given below.

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

Exercise 3. Can you prove this?

$$\gcd(a, b) = \gcd(qb + r, b) = \gcd(r, b)\,.$$

* Thanks to Nitin Saxena for his notes from the previous iteration of the course.

if $b = 0$ **then**
  Output a
end
if $b = 1$ **then**
  Output 1
end
Compute $a = qb + r$ by the division algorithm. Output $\gcd(b, r)$.

Algorithm 1: GCD algorithm

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

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

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

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

In this case $\gcd(a, b)$ will be r_k.

Exercise 4. Show that the remainder at least halves after every two steps of Euclid's algorithm.

Exercise 5. What can you say about the number of steps in Euclid's algorithm?

Hint: It's related to the Fibonacci sequence!

Exercise 6. Write the pseudocode of the other version of Euclid's algorithm in which we halve the smaller number each time, i.e. we use $a = qb + r$ where $|r| \leq b/2$. How many steps will it take?

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 (i.e. by induction), ultimately we can write the $\gcd(a, b) = r_k$ as the integer combination of a, b.

Theorem 1 (Bézout's identity). *For integers a, b, there exist integers α, β, such that,*

$$\gcd(a, b) = \alpha \cdot a + \beta \cdot b\,. \tag{3}$$

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.*

Exercise 7. Show that if α, β satisfy Eqn. 3, then $\alpha + rb, \beta - ra$ also satisfy the same equation for any integer r.

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,

$$1 = ka + \ell b\,.$$

Multiplying both sides by c, we get

$$c = kac + \ell bc\,.$$

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

Using Lem. 1, we can restrict the choice of α and β in Bezout's identity.

Theorem 2. *For integers* $a > b > 1$, *we know that there exist integers* α, β *which satisfy* $\gcd(a, b) = \alpha \cdot a + \beta \cdot b$. *Let* $a' := a/\gcd(a, b)$ *and* $b' := b/\gcd(a, b)$, *then there exists exactly one pair* (α, β), *such that,*

$$0 \leq \alpha \leq b' - 1 \text{ and } -a' + 1 \leq \beta \leq 0\,.$$

Note 1. A similar proof can be given for any two integers a and b. We assumed $a > b > 1$ to simplify the statement and the proof of the theorem.

Proof. Since $a > b > 1$, the GCD is a positive number.

For convenience we will work with the *coprime* numbers $a' := a/\gcd(a, b)$ and $b' := b/\gcd(a, b)$, as defined in the theorem. The above identity can be written as:

$$1 \;=\; \alpha a' + \beta b'\,.$$

We can ensure $0 \leq \alpha < b'$, by dividing α by b' (say $\alpha = qb' + r$), using the remainder (r) and accordingly changing β (to $\beta - qa'$). Then, $|\beta b'| = |\alpha a' - 1| < |b'a'|$. Thus, $|\beta| < a'$.

Exercise 8. Show that β is negative.

α, a, b are positive.

To show the uniqueness, suppose there exist two pairs α_1, β_1 and α_2, β_2 in the above range. Then,

$$(\alpha_1 - \alpha_2) \cdot a' \;=\; (-\beta_1 + \beta_2) \cdot b'\,.$$

By Lemma 1, we get that $b' | (\alpha_1 - \alpha_2)$. Since the difference is smaller than b', we deduce it to be zero. Hence, $(-\beta_1 + \beta_2)$ is also zero. This contradiction implies the uniqueness of (α, β) in the range $[0, \ldots, b' - 1] \times [-a' + 1, \ldots, 0]$.

□

The first goal for us would be to prove that every number has a unique prime factorization (*fundamental theorem of arithmetic*).

1.2 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 $m > 1$ and $m' > 1$, we get that any number n can be written as,

$$n = p_1 p_2 \cdots p_k\,, \text{for some } k, \text{ where } p_i\text{'s are primes.}$$

Collecting the identical primes in one power, we get the factorization,

$$n = p_1^{\ell_1} p_2^{\ell_2} \cdots p_k^{\ell_k}\,, \text{ for some } k.$$

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

Can two different prime factorizations exist? It turns out, this factorization is unique up to the ordering of primes.

For the sake of contradiction, suppose there are two such factorizations $p_1 \cdots p_k$ and $q_1 \cdots q_\ell$. 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 $q = q_1 \cdots q_{\ell-1}$ or q_ℓ (Lemma 1). If it divides $q = q_1 \cdots q_{\ell-1}$, 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. We know that p_1 and q_i are both primes. So, $p_1 = q_i$, which is a contradiction. This gives the theorem,

Theorem 3 (Unique factorization). *Given a number n, it can be written in a unique way as a product of increasing primes,*

$$n = p_1^{\ell_1} p_2^{\ell_2} \cdots p_k^{\ell_k} \text{ , where } p_i\text{'s are primes.}$$

2 Modular arithmetic

What is the day on the 184th day of an year, if it started with a Sunday?

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 whole 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 9. Prove that $r(ab) = r(r(a)r(b))$.

Applying this technique recursively (or iteratively), 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 10. Show that the last digit of 2^{2^n} for any $n \geq 2$ is 6.

The above trick 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 us study modular arithmetic more formally, following Gauß (1801).

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

Note 2. $a = b \mod n$ is read as, a is congruent to b modulo n. Some books also use the notation, $a \equiv b \mod n$.

Exercise 11. Say, a is related to b iff $a = b \mod n$. Show that it is an equivalence relation.

It is clear from the definition that if $a = b \mod n$ then $a = kn + b \mod n$ for an integer k. For a number b, the set $\{b + kn | k \in \mathbb{Z}\}$ is called the *residue class of b modulo n* and is denoted by the same notation $b \mod n$. (*It is a set, technically called a coset.*)

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 $\mathbb{Z}_n$. (Technically, we should use $\mathbb{Z}/n\mathbb{Z}$, but for this course we use the former as a shorthand.)

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 on these modulo classes (in a natural way).

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

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 12. Check the consistency for the second relation.

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

Another way to say the same thing 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 13. What is the last digit of 2^{39} ?

$2^{39} = 2^{32+4+2+1} = 2 \cdot 4 \cdot 6 \cdot 6^8 = 2 \cdot 4 \cdot 6 = 8 \mod 10$.

Though you should be careful not to overuse your intuition of integer operations. For example, if $ab = 0 \mod n$ and $a \neq 0 \mod n$, it does not mean that $b = 0 \mod n$. Take $a = 2, b = 3, n = 6$ as an example.

This property also tells you that, in general, *cancellation rule* fails: $ab = ac \mod n \not\Rightarrow b = c \mod n$.

Exercise 14. 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 $0 < a < p$. What is p?
7. Find the number of integer solutions of $25x + 31y = 6$.
8. Find the number of integer solutions of equation $x^2 + y^2 = 4z - 1$.
9. How do you check if there is a solution to $x^2 = a \mod p$ where p is a prime?

3 Inverse modulo n or how to solve linear equations in $\mathbb{Z}_n$

In the last section, we saw how to add, subtract and multiply elements of $\mathbb{Z}_n$ (calculations modulo n). Let us ask the next question, how to perform division in $\mathbb{Z}_n$? If we want to divide b by a, it is equivalent to solve linear equation $ax = b \mod n$.

Important note: if $b = ac \mod n$ need not imply $x = c \mod n$. This is because $n \mid a(x - c)$ implies $n \mid x - c$ only when $\gcd(a, n) = 1$.

Exercise 15. Let $\gcd(a, n) = 1$, how do we find the solution of $ax = b \mod n$?

But if a and n are coprime to each other then there exists an integer k, s.t., $ka = 1 \mod n$ (Bézout's identity 3). 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 exists, then,

$$ax = b \mod n \Rightarrow a^{-1}ax = a^{-1}b \mod n \Rightarrow x = a^{-1}b \mod n\,.$$

Suppose n is a prime, then for any $0 < a < n$, $\gcd(a, n) = 1$. In this case, inverse exist for all a not divisible by n. In other words, we have inverse of every element except 0 in $\mathbb{Z}_n$. Hence, while computing modulo a prime p, we can divide (or cancel) freely.

Exercise 16. Find the following quantities,

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

Exercise 17. Give an algorithm to find $a^{-1} \mod n$. What previous algorithm can you use?

Exercise 18. Find the inverse of 25 modulo 23 using the algorithm above.

It is clear from previous paragraph that computations modulo a prime p are *nicer* because every element in $\mathbb{Z}_p$ (except 0) is coprime to p. We can prove many interesting properties in $\mathbb{Z}_p$, let us look at one of the important theorems in number theory.

Theorem 4 (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, $ka = 0 \mod p$ if and only if $k \neq 0 \mod p$.

Exercise 19. Show that $\nexists s \neq t : sa = ta \mod p$.

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,

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

□

Exercise 20. 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 21. 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 $a^{\phi(u)} = 1 \mod u$, where $\phi(u)$ is the number of elements in $[u-1]$ that are coprime to u. When a, u share a factor then there is no good property.

4 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 22. 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 5 (Multiplicative). *If m and n are coprime to each other, then $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$.*

Proof. Define $S := \mathbb{Z}_m^* \times \mathbb{Z}_n^* = \{(a, b) : \quad a \in \mathbb{Z}_m^*,\ b \in \mathbb{Z}_n^*\}$. 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 23. Find numbers m, n such that $\phi(mn) \neq \phi(m)\phi(n)$.

Fundamental theorem of arithmetic implies that we can express any number as a product of prime powers. By using Thm 5, we can calculate $\phi(mn)$, when $\phi(m)$ and $\phi(n)$ are given to us (m and n are coprime).

Theorem 6. *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 24. Prove the above theorem using Thm. 5.

For a positive integer n and a coprime a,

$$a^{\phi(n)} = 1 \mod n.$$

This is known as *Euler's theorem* and can be proven in a very similar manner to Fermat's theorem.

5 Chinese remainder theorem

By finding inverses modulo n, we can solve a linear equation (congruence) modulo n. Let us take the next step, how about a system of linear equations?

$$a_1 x = b_1 \mod m \text{ and } a_2 x = b_2 \mod n.$$

If the equations need to have a solution, the $\gcd(a_1, m)$ ($\gcd(a_2, n)$ should divide b_1 (b_2) respectively. Dividing by the GCD's and then multiplying by the inverse of the coefficient of x, we get the equations of type,

$$x = c_1 \mod m \text{ and } x = c_2 \mod n. \tag{4}$$

Exercise 25. Suppose m, n are not coprime to each other. Show that there exist c_1, c_2 such that Eq. 4 have no common solution.

For simplicity, we will assume that m, n are coprime to each other in Eq. 4. The general case is not very difficult. Readers are encouraged to try it once they finish reading the solution of coprime case below.

Exercise 26. Show that if x is a solution of Eq. 4, then $x + r \cdot mn$ is also a solution for any integer r.

The above exercise shows that we are only interested in solutions modulo mn. We saw a mapping from integers modulo m and integers modulo n to integers modulo mn in the last section.

$$(a, b) \to bm + an \mod mn.$$

The number $c_2m + c_1n$ gives c_2m remainder when divided by n and c_1n when divided by m. Since m and n are coprime to each other, $m^{-1} \mod n$ and $n^{-1} \mod m$ exist. This gives us an idea to modify the mapping,

$$(c_1, c_2) \to c_2m(m^{-1} \mod n) + c_1n(n^{-1} \mod m) \mod mn.$$

Exercise 27. Show that the number $c_2m(m^{-1} \mod n) + c_1n(n^{-1} \mod m)$ leaves remainder $c_1 \mod m$ and $c_2 \mod n$.

This gives us one solution modulo mn, can there be two solutions to Eq. 4 distinct modulo mn. Suppose x, y are two distinct solutions. The congruences 4 imply that $x - y$ is divisible by both m and n. Since m and n are coprime, $x - y$ is divisible by mn.

Above discussion shows that if m, n are coprime then Eq. 4 has a unique solution modulo mn. This idea can be generalized to more than 2 equations and is known as *Chinese remainder theorem.*

Theorem 7 (Chinese remainder theorem (CRT)). *Let $n_1, n_2, \cdots, n_k$ be positive integers which are pairwise coprime to each other. Then, the system of congruences,*

$$\begin{aligned} x &= c_1 \mod n_1 \\ x &= c_2 \mod n_2 \\ &\vdots \\ x &= c_k \mod n_k \end{aligned}$$

has a unique solution modulo $n_1n_2 \cdots n_k$ and it can be found efficiently.

Note 3. All other solutions can be found by adding/subtracting multiples of $n_1n_2 \cdots n_k$ to this unique solution.

Proof. We will show that there is a solution of these system of congruences. The uniqueness of this solution and the fact that every other solution is obtained by adding/subtracting a multiple of $n_1n_2 \cdots n_k$, is an easy generalization of the case of two congruences. We leave it as a simple exercise for the reader.

Define $N := n_1n_2 \cdots n_k$ and then $N_i := N/n_i$. We want to find a solution modulo N. Notice that n_1 is coprime to all other n_i's, i.e., n_1 is coprime to N_1. Suppose, thinking of induction, we had a solution r of system of congruences,

$$\begin{aligned} x &= c_2 \mod n_2 \\ &\vdots \\ x &= c_k \mod n_k \end{aligned}$$

Then, to solve the entire system, we needed to find a solution to,

$$x = c_1 \mod n_1 \text{ and } x = r \mod N_1.$$

By the case of two congruences, the solution would have been,

$$x = c_1 N_1 (N_1^{-1} \mod n_1) + r n_1 (n_1^{-1} \mod N_1).$$

The first term is independent of $c_2, \cdots, c_k$. This gives us the idea for the complete solution,

$$x = \sum_i c_i N_i (N_i^{-1} \mod n_i).$$

Exercise 28. Show that the x above satisfies the system of congruences in the theorem.

The only remaining thing is to show that this x can be constructed efficiently. This follows because $N_i^{-1} \mod n_i$ can be found efficiently using Extended Euclidean algorithm (rest are only addition and multiplication).

□

Chinese remainder theorem is very useful in breaking large computation. The idea is, to compute modulo $n = pq$, we can just do computation modulo p and q separately. Those results can be combined to get result modulo n by Chinese remaindering. We will see one such application for speeding up RSA later.

6 Extra reading: Inclusion-Exclusion vs. Möbius Inversion

There is another way to look at Thm. 6. 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,

$$\phi(n) = \sum_{I \subseteq [\ell]} (-1)^{|I|} \frac{n}{\Pi_{i \in I} p_i}. \tag{5}$$

Exercise 29. Prove that the above expression is the same as the one in Thm. 6.

In Eqn. 5, 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. 5 can be rewritten as,

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

Exercise 30. 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, $\mu(a) \cdot \mu(q) = \mu(ab)$. This can be used to deduce that $\sum_{d|n} \mu(p) = \prod_{i \in [j]} (1 + \mu(p_i) + \mu(p_i^2) + \cdots + \mu(p_i^{k_i})) = \prod_{i \in [j]} (1 + \mu(p_i)\mu(d) + \mu(p_i^2)\mu(d) + \cdots + \mu(p_i^{k_i})\mu(d)) = 0$.

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

Theorem 8 (Möbius inversion). *Let f and g be functions defined on natural numbers. Then,*

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

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

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

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 31. 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 32. 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. K. H. Rosen. Discrete Mathematics and Its Applications. *McGraw-Hill*, 1999.
2. N. L. Biggs. Discrete Mathematics. *Oxford University Press*, 2003.