Lecture 12: Basic number theory

Nitin Saxena ⋆

IIT Kanpur

1 Euclid's GCD (Contd.)

Theorem 1 (Bézout's identity). *For integers $a \geq b > 0$, there exist integers α, β, such that,*

$$\gcd(a,b) = \alpha \cdot a + \beta \cdot b\,.$$

Moreover, the identity is unique *if we assume* $0 \leq \alpha < b/\gcd(a,b)$.

Proof. By hypothesis, the GCD is a positive number. The extended Euclid's gcd algorithm gives us at least one such identity.

For convenience we will work with the *coprime* numbers $a' := a/\gcd(a,b)$ and $b' := b/\gcd(a,b)$. 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, $|\beta b'| = |\alpha a' - 1| \leq |b'a'|$. Thus, $|\beta| \leq a'$.

Finally, suppose that α, β in the above range are not unique. 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 $[0, \ldots, b'-1] \times [-a', \ldots, a']$.

□

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 this basic lemma, we can prove the fundamental theorem.

⋆ Edited from Rajat Mittal's notes.

1.1 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. 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 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 1. 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 2. 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 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 if $a = b \mod n$ then $a = kn + b \mod n$ for any 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 3. Check the consistency for the second relation.

For doing calculations, it generally makes sense to take the smallest nonnegative 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 $\{0, 1, 2, \cdots, n-1\}$.

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 4. 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 5. 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?

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.