Number Theory

Benjamin Cosman, Patrick Lin and Mahesh Viswanathan

Fall 2020

TAKE-AWAYS

- $a \mid b$ means there exists an integer k such that $b = ak$. We say that a is a *factor* or *divisor* of b, and b is a *multiple* of a.
- For integers a and b with $a > 0$, there exist unique integers q, r such that $b = qa + r$ and $0 \leq r < a$. $q = \mathsf{quot}(b, a)$ is called the *quotient* and $r = \mathsf{rem}(b, a)$ is called the *remainder*.
- A number greater than 1 is *prime* if its only factors are 1 and itself. Every integer can be written as a product of a unique weakly decreasing sequence of primes.
- $\gcd(a, b)$ is the largest integer dividing both a and b. a and b are *coprime* if $\gcd(a, b) = 1$.
- $a \equiv b \bmod n$ means $n \mid (a - b)$. This equivalence relation splits the integers into *congruence classes* $[a]_n = \{b \mid a \equiv b \bmod n\}$. Any element $b \in [a]_n$ is called a *representative* of the congruence class; the *canonical representative* of $[a]_n$ is $\mathsf{rem}(a, n)$.
- Congruence classes can be added and multiplied.

The idea of divisibility underlies among other things, many techniques in modern cryptography and hashing. The use of prime numbers is so prevalent in cryptography that trying to efficiently factor numbers into their prime factors continues to be a major area of research in cryptography and computer security. Many common hashing schemes used for things like hash tables involve taking an input x and outputting the "congruence class" of some function of x.

Divisibility

Recall that b being even means that there exists some integer k such that $b = 2k$. We can also write this as $2 \mid b$, to be read as "2 is a factor of b" or "b is a multiple by 2." We can make this more general:

Definition 1 (Divisibility)**.** Given integers a and b, $a \mid b$ means there exists integer k such that $b = ak$. In this case we say that a is a *factor* or *divisor* of b, and b is a *multiple* of a.

Some examples:

- $3 \mid 6$
- $-7 \mid 49$
- $83 \mid -11537$
- $\forall a \in \mathbb{Z}$, $a \mid a$
- $\forall a \in \mathbb{Z}$, $a \mid 0$
- $\forall a \in \mathbb{Z} \setminus \{0\}$, $0 \nmid a$ (0 is *not* a factor of a)

You should probably think about the last two examples and figuring out why they are true.

A number of easy but useful facts can be proven about divisibility.

Lemma 2. *For any integers a, b, c, x, y:*

a) If $a \mid b$ and $b \mid c$ then $a \mid c$

b) If $a \mid b$ and $a \mid c$ then $a \mid bx + cy$

c) If $c \neq 0$, then $a \mid b$ if and only if $ca \mid cb$

Proof.

a) By definition, there exist integers k, ℓ such that $b = ak$ and $c = b\ell$. Then $c = a(k\ell)$, so $a \mid c$.

b) By definition, there exist integers k, ℓ such that $b = ak$ and $c = a\ell$. Then $bx + cy = akx + a\ell y = a(kx + \ell y)$, so $a \mid bx + cy$.

c) First suppose that $a \mid b$, then $b = ak$ for some integer k, so $cb = (ca)k$, so $ca \mid cb$. Now suppose $ca \mid cb$, then there exists some integer k so that $cb = cak$. Since $c \neq 0$ we can cancel c from both sides to find $b = ak$, i.e., $a \mid b$. □

It is also useful to know what happens $a \nmid b$. You probably remember exercises where you try to divide some integer b by some other integer a and get some remainder left over. This is formalized in the following theorem:

Theorem 3 (Division Theorem)**.** *Let a, b be integers such that $a > 0$. Then there exist unique integers q, r such that $b = aq + r$ and $0 \leq r < a$.*

Proof. We first prove existence by induction for $b \geq 0$. For $b \geq 0$, let $P(b)$ be the statement "There exist integers q, r such that $b = aq + r$ and $0 \leq r < a$."

The base cases are $P(b)$ for $0 \leq b \leq a - 1$. Well, $b = 0a + b$, so we can set $q = 0$ and $r = b$.

For the inductive case $k \geq a$, assume as our inductive hypothesis that P holds for all i from 0 and $k - 1$. Set $\ell = k - a$. Then since $0 \leq k - a \leq k - 1$, the inductive hypothesis implies $\ell = qa + r$ for

some integers q, r where $0 \leq r < a$. Then

$$\begin{aligned} k &= a + (k - a) \\ &= a + \ell \\ &= a + (qa + r) \\ &= (q + 1)a + r. \end{aligned}$$

Induction complete.

For $b < 0$, then $-b > 0$, so there exist q, r so that $-b = qa + r$ and $0 \leq r < a$. If $r = 0$, then $b = (-q)a$. Otherwise, $b = -qa - r = -(q + 1)a + (a - r)$, and since $0 < r < a$, $0 < a - r < a$ as well.

We now need to show that q, r are unique. Suppose that $b = qa + r = q'a + r'$, where $0 \leq r < a$, $0 \leq r' < a$, and $r' \geq r$. We need to show that $q = q'$ and $r = r'$.[1] Observe that $r' - r = a(q - q')$. But $0 \leq r' - r \leq r' < a$, so $0 \leq q - q' < 1$. Since $q - q'$ is an integer, it must be the case that $q - q' = 0$. But then also $r' - r = 0$, so $q' = q$ and $r' = r$. □

[1] Recall that "there exists exactly one x, $P(x)$" means that there exists at least one x, $P(x)$, and for all x, y, $P(x) = P(y)$ implies $x = y$.

Definition 4. Given integers a, b with $a > 0$, the *quotient* $\mathsf{quot}(b, a)$ and *remainder* $\mathsf{rem}(b, a)$ are the unique integers such that $b = a \cdot \mathsf{quot}(b, a) + \mathsf{rem}(b, a)$ and $0 \leq \mathsf{rem}(b, a) < a$.

(Co)primality

Recall that an integer $p > 1$ is *prime* if the only factors of p are 1 and p, and *composite* otherwise. There are many applications in which we are interested in comparing the common factors of two composite integers a, b.[2] The *greatest common divisor* $\gcd(a, b)$ is the largest integer that is a factor of both a and b. It is easy to see that for primes p, q such that $p \neq q$, $\gcd(p, q) = 1$. More generally, two numbers a, b are said to be *coprime* or *relatively prime* if $\gcd(a, b) = 1$.

[2] Many cryptographic methods, such as the RSA algorithm, are based on the idea that the prime factors are hard to compute.

The following lemma turns out to have far-reaching applications in number theory and in computer algebra in general:

Lemma 5 (Bézout's Lemma)**.** *Let a, b be non-zero integers. Then there exist integers x, y such that $ax + by = \gcd(a, b)$.*

You will be asked to prove Bézout's lemma in your homework. One nice consequence of Bézout's lemma is the following:

Lemma 6 (Euclid's Lemma)**.** *Suppose $a, b_1, b_2, \ldots, b_k$ are integers such that a is prime and $a \mid b_1 b_2 \ldots b_k$. There there exists some i, $1 \leq i \leq k$, such that $a \mid b_i$.*

Proof. We will use Bézout's lemma to show the special case of $k = 2$. The general result follows via induction.[3]

[3] If you can't see how this works right away, you should work out the full induction details for yourself.

If $a \mid b_1$, then we are done. So suppose that $a \nmid b_1$. Since a is prime, $\gcd(a, b_1) = 1$. By Bézout's lemma, there exist integers x, y so that $ax + b_1 y = \gcd(a, b_1) = 1$. Then multiplying both sides by b_2, we get $b_2(ax + b_1 y) = ab_2 x + b_1 b_2 y = b_2$. Since $a \mid b_1 b_2$ by assumption, $a \mid ab_2 x + b_1 b_2 y$ by Lemma 2. So $a \mid b_2$. □

We previously saw (in the unit on Induction) that every integer $n \geq 2$ is a product of one or more primes. This is known as a *prime factorization* of n. It turns out that the prime factorization of every integer $n \geq 2$ is unique up to reordering the factors. In other words, if we rearrange the prime factors in *weakly decreasing* order[4] then n is a *product of a unique weakly decreasing sequence of primes*, or pusp, for short.[5]

[4] A sequence of numbers is weakly decreasing if each number in the sequence is greater than or equal to the numbers after it.

[5] You probably recall a bogus proof of this fact from the Induction Homework.

Theorem 7 (Fundamental Theorem of Arithmetic)**.** *Every integer greater than one is a pusp.*

Proof. By induction.

The base case is $n = 2$: 2 is prime, and by definition there is only one sequence of primes whose product is 2, namely, 2.

For the inductive case, assume as our inductive hypothesis that every number i between 2 and $n - 1$ is a pusp. We will now show that n is a pusp.

We already know that n can be written as a product of primes, $n = p_1 p_2 \dots p_k$. Since multiplication is commutative, we can assume (by reordering if necessary) that $p_1 \geq p_2 \geq \cdots \geq p_k$. Now suppose that n can be written as a product of primes in a different way, $n = q_1 q_2 \dots q_\ell$.

Set $m = p_2 p_3 \dots p_k$, so that $p_1 m = n = q_1 q_2 \dots q_\ell$. Since $m \in \mathbb{Z}$ we know that $p_1 \mid q_1 q_2 \dots q_\ell$. By Euclid's Lemma, $p_1 \mid q_i$ where $1 \leq i \leq \ell$. But since $p_1 \neq 1$ and q_i is prime, we conclude that $p_1 = q_i$. By reordering the factors $q_1, q_2, \dots, q_\ell$, we can assume that $i = 1$ (so $p_1 = q_1$) and that $q_2 \geq q_3 \geq \cdots \geq q_\ell$.

We now have $p_2 \dots p_k = m = q_2 \dots q_\ell$. But since $2 \leq m \leq n - 1$, by the inductive hypothesis, m is a pusp, so the sequences $p_2, \dots, p_k$ and $q_2, \dots, q_\ell$ are the same.

We conclude that any two ways of writing n as a product of a weakly decreasing sequence of primes are actually the same, i.e., n is a pusp. Induction complete. □

Congruence modulo n and modular arithmetic

Recall that there are an infinite number of integers, but computers have finite memory. More generally, we might be working with a very large set of possible numbers, but we would much prefer to do

our computations over a much smaller set.[6] One way to do this is via *modular arithmetic*, which preserves some useful properties of normal arithmetic over the integers.

[6] For example, storing data in a hash table.

Definition 8. For integers a, b, n with $n > 0$, $a \equiv b \bmod n$ (a and b are congruent modulo n) if and only if $n \mid (a - b)$.

Note that $n \mid (a - b)$ if and only if $n \mid (b - a)$, so the definition is symmetric in a and b.

Let us practice using this definition by proving the following useful lemma:

Lemma 9. *Let a, b, c, d, n be integers with $n > 0$ such that $a \equiv c \bmod n$ and $b \equiv d \bmod n$. Then:*

a) $a + b \equiv c + d \bmod n$, *and*

b) $ab \equiv cd \bmod n$.

Proof. Let a, b, c, d, n be integers with $n > 0$ such that $a \equiv c \bmod n$ and $b \equiv d \bmod n$. Then $n \mid (a - c)$ and $n \mid (b - d)$.

For the first part, Lemma 2 tells us that $n \mid ((a - c) + (b - d)) = ((a + b) - (c + d))$. So $a + b \equiv c + d \bmod n$.

The second part is slightly more difficult. From $n \mid (a - c)$, we know that there exists some integer k such that $nk = a - c$, and from $n \mid (b - d)$, we know there exists some integer ℓ such that $n\ell = b - d$. Rearranging, we get $a = c + nk$ and $b = d + n\ell$, so $ab = (c + nk)(d + n\ell) = cd + n(c\ell + dk + nk\ell)$. Since $c\ell + dk + nk\ell \in \mathbb{Z}$, we conclude $n \mid (ab - cd)$, i.e., $ab \equiv cd \bmod n$. □

Definition 10. Given integers a and n, the *congruence class* of a modulo n is the set $[a]_n = \{b \mid a \equiv b \bmod n\}$.[7] Any element $b \in [a]_n$ is called a *representative* of $[a]_n$.

[7] Congruence modulo n is an *equivalence relation* over the integers, and you can verify for yourself that the relation is reflexive, symmetric, and transitive. Equivalence relations over a set A split the set into disjoint *equivalence classes*. Congruence classes are a special case of this more general phenomenon.

Lemma 9 tells us that if $c \in [a]_n$ and $d \in [b]_n$, then $c + d \equiv a + b \bmod n$, i.e., $[c + d]_n = [a + b]_n$, and similarly, $cd \equiv ab \bmod n$, i.e., $[cd]_n = [ab]_n$. In other words, no matter which representatives we choose when adding or multiplying, we end up in the same equivalence class at the end. This justifies the following definition:

Definition 11 (Modular Arithmetic)**.**

a) $[a]_n + [b]_n = [a + b]_n$

b) $[a]_n[b]_n = [ab]_n$

The definition of congruence class implies that if $b \in [a]_n$, then $[a]_n = [b]_n$. One common way to think about modular arithmetic is by thinking of a number a as being "the same" as its remainder when divided by n:

Lemma 12. $a \equiv \mathsf{rem}(a, n) \bmod n$, *i.e.*, $[a]_n = [\mathsf{rem}(a, n)]_n$.

$\mathsf{rem}(a, n)$ is often referred to as the *canonical* representative of $[a]_n$. In particular, doing computations using $\mathsf{rem}(a, n)$ can greatly simplify computations. For example, consider $a = 79$, $b = 102$, and $n = 4$. Then $\mathsf{rem}(a, n) = 3$ and $\mathsf{rem}(b, n) = 2$. Instead of computing $[79 + 102]_4 = [181]_4 = [1]_4$, we can compute $[79]_4 + [102]_4 = [3]_4 + [2]_4 = [3 + 2]_4 = [5]_4 = [1]_4$. Similarly, instead of computing $[79]_4[102]_4 = [79 \cdot 102]_4 = [8058]_4 = [2]_4$, we can compute $[79]_4[102]_4 = [3]_4[2]_4 = [6]_4 = [2]_4$.