Math 220 Fall 2021, Lecture 22: Number theory I

1. Number theory I

1.1. Greatest common divisors (cont'd)

Last time, we proved:

Theorem 1.1.1 (Bezout's theorem)**.** Let a and b be two integers. Then, there exist integers x and y such that

$$\gcd(a, b) = xa + yb.$$

A pair (x, y) of two such integers was called a **Bezout pair** for (a, b).

Bezout's theorem leads to several important properties of gcds. The first one is the so-called **universal property of the gcd**:

Theorem 1.1.2 (universal property of the gcd)**.** Let $a, b, m \in \mathbb{Z}$. Then, we have the equivalence

$$(m \mid a \text{ and } m \mid b) \iff (m \mid \gcd(a, b)).$$

In other words, the common divisors of a and b are precisely the divisors of $\gcd(a, b)$.

Proof of Theorem 1.1.2. We must prove the two implications

$$(m \mid a \text{ and } m \mid b) \implies (m \mid \gcd(a, b))$$

and

$$(m \mid \gcd(a, b)) \implies (m \mid a \text{ and } m \mid b).$$

The second implication is easy: If $m \mid \gcd(a, b)$, then $m \mid a$ (because $m \mid \gcd(a, b) \mid a$) and $m \mid b$ (similarly).

It remains to prove the first implication: i.e., that

$$(m \mid a \text{ and } m \mid b) \implies (m \mid \gcd(a, b)).$$

So let us assume that $m \mid a$ and $m \mid b$. We must prove that $m \mid \gcd(a, b)$.

Bezout's theorem yields that there exist two integers x and y such that $\gcd(a, b) = xa + yb$. Consider these x and y. We have $m \mid a \mid xa$ and $m \mid b \mid yb$, so that $m \mid xa + yb$ (since a sum of two multiples of m is again a multiple of m). Since $xa + yb = \gcd(a, b)$, we can rewrite this as $m \mid \gcd(a, b)$. And so we are done. □

Here is another property of gcds:

Theorem 1.1.3. Let $s, a, b \in \mathbb{Z}$. Then,

$$\gcd(sa, sb) = |s| \cdot \gcd(a, b).$$

Proof. Let $g = \gcd(a, b)$ and $h = \gcd(sa, sb)$. So we must prove that $h = |s| \cdot g$. Note that h and g are nonnegative.

One good way to prove that two nonnegative integers p and q are equal is by showing that $p \mid q$ and $q \mid p$. Indeed, from $p \mid q$ and $q \mid p$, we obtain $|p| = |q|$ (by a proposition we proved back in Lecture 18), and therefore $p = q$ (since p and q are nonnegative).

Thus, in order to prove $h = |s| \cdot g$, it suffices to show that $h \mid |s| \cdot g$ and $|s| \cdot g \mid h$. Equivalently, it suffices to show that $h \mid sg$ and $sg \mid h$ (since signs do not matter in divisibilities).

Let us prove that $sg \mid h$: Indeed, $g = \gcd(a, b) \mid a$, so that $sg \mid sa$. Similarly, $sg \mid sb$. Thus, by Theorem 1.1.2 (applied to sg, sa and sb instead of m, a and b), we conclude that $sg \mid \gcd(sa, sb)$. In other words, $sg \mid h$ (since $h = \gcd(sa, sb)$).

Let us now prove that $h \mid sg$: We have $h = \gcd(sa, sb) \mid sa$ and $h = \gcd(sa, sb) \mid sb$. However, Bezout's theorem says that there exist two integers x and y such that $\gcd(a, b) = xa + yb$. Consider these x and y. So $g = \gcd(a, b) = xa + yb$. Now, from $h \mid sa \mid sxa$ and $h \mid sb \mid syb$, we obtain

$$\begin{aligned} h &\mid sxa + syb && \text{(since a sum of two multiples of } h \text{ is a multiple of } h) \\ &= s \underbrace{(xa + yb)}_{=g} = sg. \end{aligned}$$

So we have shown that $h \mid sg$ and $sg \mid h$. As we already explained, this completes the proof. □

The next theorem will be helpful later on:

Theorem 1.1.4. Let $a, b, c \in \mathbb{Z}$ satisfy $a \mid c$ and $b \mid c$. Then, $ab \mid \gcd(a, b) \cdot c$.

Proof. Bezout's theorem says that there exist two integers x and y such that $\gcd(a, b) = xa + yb$. Consider these x and y.

Now, $b \mid c$, so that $ab \mid ac \mid xac$. Also, $a \mid c$, so that $ab \mid cb = bc \mid ybc$. So both xac and ybc are multiples of ab. Since the sum of two multiples of ab is again a multiple of ab, we thus conclude

$$ab \mid xac + ybc = \underbrace{(xa + yb)}_{=\gcd(a,b)} c = \gcd(a, b) \cdot c,$$

qed. □

1.2. Coprime integers

Now, we shall define an important relation between two integers: coprimality.

Definition 1.2.1. Two integers a and b are said to be **coprime** (or **relatively prime**) if $\gcd(a, b) = 1$.

Remark 1.2.2. This is a symmetric relation: If a and b are coprime, then b and a are coprime (since $\gcd(b, a) = \gcd(a, b)$).

Example 1.2.3. (a) An integer n is coprime to 2 if and only if n is odd. In fact:

- If n is even, then $\gcd(n, 2) = 2$, because 2 is a common divisor of n and 2 (and clearly there cannot be any larger common divisor, since a divisor of 2 cannot be larger than 2).
- If n is odd, then $\gcd(n, 2) = 1$, since 2 is not a common divisor of n and 2 but 1 is.

(b) An integer n is coprime to 3 if and only if n is not divisible by 3.
(c) An integer n is coprime to 4 if and only if n is odd.
(d) An integer n is coprime to 5 if and only if n is not divisible by 5.

The following two theorems are useful properties of coprime integers:

Theorem 1.2.4. Let $a, b, c \in \mathbb{Z}$ satisfy $a \mid c$ and $b \mid c$. Assume that a and b are coprime. Then, $ab \mid c$. (In other words, a product of two coprime divisors of c is again a divisor of c.)

Proof. Theorem 1.1.4 yields $ab \mid \gcd(a, b) \cdot c$. However, since a and b are coprime, we have $\gcd(a, b) = 1$. So this divisibility $ab \mid \gcd(a, b) \cdot c$ becomes $ab \mid 1 \cdot c$. In other words, $ab \mid c$. □

Theorem 1.2.5 (coprime cancellation theorem)**.** Let $a, b, c \in \mathbb{Z}$ satisfy $a \mid bc$. Assume that a is coprime to b. Then, $a \mid c$.

Proof. Bezout's theorem says that there exist two integers x and y such that $\gcd(a, b) = xa + yb$. Consider these x and y. Since a is coprime to b, we have $\gcd(a, b) = 1$, so that $1 = \gcd(a, b) = xa + yb$.

Now,

$$c = c \cdot \underbrace{1}_{=xa+yb} = c \cdot (xa + yb) = cxa + cyb = \underbrace{acx}_{\text{a multiple of } a} + \underbrace{bcy}_{\substack{\text{a multiple of } a \\ \text{because } a \mid bc \mid bcy}}.$$

This is a multiple of a (since a sum of two multiples of a is again a multiple of a). In other words, $a \mid c$. □

1.3. Prime numbers

Recall:

Definition 1.3.1. An integer $n > 1$ is said to be **prime** (or **a prime**) if the only positive divisors of n are 1 and n.

So the numbers $2, 3, 5, 7, 11, 13, 17, \ldots$ are primes. We have proved a while ago that there are infinitely many primes.

We shall now show a simple but important property of primes:

Lemma 1.3.2 (black-or-white lemma)**.** Let p be a prime. Let $n \in \mathbb{Z}$. Then, n is either divisible by p or coprime to p (but not both).

Proof. It is easy to see that n cannot be divisible by p and coprime to p at the same time (because if n is divisible by p, then $\gcd(n, p) = p > 1$, which means that n cannot be coprime to p). Thus, it remains to show that n is always divisible by p or coprime to p.

Assume the contrary. Thus, n is neither divisible by p nor coprime to p. The number $\gcd(n, p)$ must be a positive divisor of p, and thus equals either 1 or p (since p is prime, so the only positive divisors of p are 1 and p). However, it cannot be 1, since n is not coprime to p. So it must be p.

Thus we have $\gcd(n, p) = p$. Therefore, $p = \gcd(n, p) \mid n$. This contradicts the fact that n is not divisible by p. The lemma is thus proved. □

(The name "black-or-white lemma" is my own invention; it refers to the idea that a prime p separates the integers into its "friends" – meaning its multiples – and its "enemies" – meaning the numbers coprime to p.)

As an application of the black-or-white lemma, we can prove a property of Pascal's triangle that you might have already noticed in Lecture 17: All entries in the $n = 7$ row except for the two 1's (i.e., all the binomial coefficients $\binom{7}{1}, \binom{7}{2}, \ldots, \binom{7}{6}$) are divisible by 7; all entries in the $n = 5$ row except for the two 1's are divisible by 5; likewise for the $n = 3$ and $n = 2$ rows. The pattern here can be generalized:

Theorem 1.3.3. Let p be a prime. Let $k \in \{1, 2, \ldots, p - 1\}$. Then, $p \mid \binom{p}{k}$.

Proof. Apply the black-or-white lemma to $n = k$. Thus, we conclude that k is either divisible by p or coprime to p. Since k cannot be divisible by p (because $0 < k < p$), we thus conclude that k is coprime to p. In other words, p is coprime to k.

Next, recall the definition of binomial coefficients (Lecture 17). Thus,

$$\binom{p}{k} = \frac{p\,(p-1)\,(p-2)\cdots(p-k+1)}{k!} = \frac{p\cdot(p-1)\,(p-2)\cdots(p-k+1)}{k\cdot(k-1)!}$$

$$\left(\text{since } k! = \underbrace{1\cdot 2\cdot\cdots\cdot(k-1)}_{=(k-1)!}\cdot k = (k-1)!\cdot k = k\cdot(k-1)!\right)$$

$$= \frac{p}{k}\cdot\underbrace{\frac{(p-1)\,(p-2)\cdots(p-k+1)}{(k-1)!}}_{=\binom{p-1}{k-1}} = \frac{p}{k}\cdot\binom{p-1}{k-1}.$$

Multiplying both sides of this by k, we obtain

$$k\cdot\binom{p}{k} = p\cdot\underbrace{\binom{p-1}{k-1}}_{\in\mathbb{Z}}.$$

This shows that

$$p \mid k\cdot\binom{p}{k}.$$

Since p is coprime to k, we can thus apply the coprime cancellation theorem to $a = p$ and $b = k$ and $c = \binom{p}{k}$. We conclude that $p \mid \binom{p}{k}$, qed. □

Here are some further properties of primes:

Theorem 1.3.4 (prime divisor separation theorem)**.** Let p be a prime. Let $a, b \in \mathbb{Z}$ be such that $p \mid ab$. Then, $p \mid a$ or $p \mid b$.

This is in contrast to the fact that generally, if an integer n divides a product ab, it does not follow automatically that $n \mid a$ or $n \mid b$. (For example, we have $6 \mid 4\cdot 9$ but $6 \nmid 4$ and $6 \nmid 9$.) Theorem 1.3.4 says that primes behave better than that.

Proof of Theorem 1.3.4. Assume the contrary. So $p \nmid a$ and $p \nmid b$.

The black-and-white lemma yields that p either divides a or is coprime to a. Since $p \nmid a$, we thus see that p is coprime to a. Hence, we can use the coprime cancellation theorem to obtain $p \mid b$ from $p \mid ab$. This contradicts $p \nmid b$. □

Corollary 1.3.5 (prime divisor separation theorem for k factors)**.** Let p be a prime. Let $a_1, a_2, \ldots, a_k \in \mathbb{Z}$ be such that $p \mid a_1 a_2 \cdots a_k$. Then, there exists some $i \in \{1, 2, \ldots, k\}$ such that $p \mid a_i$.

(In words: If a prime divides a product of several integers, then it must divide at least one of the factors.)

Proof of Corollary 1.3.5. Induct on k. Use Theorem 1.3.4 in the induction step. □

We are now ready to state what might be the most important property of primes: the fact that each positive integer can be uniquely decomposed into a product of some primes. For instance,

$$200 = 2 \cdot 100 = 2 \cdot 2 \cdot 50 = 2 \cdot 2 \cdot 5 \cdot 10 = \underbrace{2 \cdot 2 \cdot 5 \cdot 2 \cdot 5}_{\text{a product of primes}} .$$

The word "uniquely" means here that any two ways to decompose a given positive integer n as a product of primes are "equal up to reordering the factors". For example, we can also decompose 200 as $5 \cdot 2 \cdot 2 \cdot 5 \cdot 2$.

Let us state this fact in full generality. We first introduce the terminology for it:

Definition 1.3.6. Let n be a positive integer. A **prime factorization** of n means a finite list $(p_1, p_2, \ldots, p_k)$ of primes (not necessarily distinct) such that $n = p_1 p_2 \cdots p_k$.

Theorem 1.3.7 (Fundamental Theorem of Arithmetic)**.** Let n be a positive integer. Then:

(a) There exists a prime factorization of n.

(b) This prime factorization is unique up to reordering its entries. In other words, if $(p_1, p_2, \ldots, p_k)$ and $(q_1, q_2, \ldots, q_\ell)$ are two prime factorizations of n, then $(q_1, q_2, \ldots, q_\ell)$ can be obtained from $(p_1, p_2, \ldots, p_k)$ by reordering the entries.

I will sketch the proof on zoom. (Part **(a)** has already been proved in Lecture 16.)