Math 220 Fall 2021, Lecture 21: Number theory I

1. Number theory I

1.1. Division with remainder (cont'd)

Last time, we haven't finished proving the following proposition:

Proposition 1.1.1. Let $n \in \mathbb{Z}$ and let d be a positive integer. Then:
(a) We have $n\%d \in \{0, 1, \ldots, d-1\}$ and $n\%d \equiv n \mod d$.
(b) We have $d \mid n$ if and only if $n\%d = 0$.
(c) If $c \in \{0, 1, \ldots, d-1\}$ satisfies $c \equiv n \mod d$, then $c = n\%d$.
(d) We have $n = (n//d)\, d + (n\%d)$.

We proved parts **(d)** and **(a)**; let us now prove **(b)** and **(c)**:

Proof. We set

$$q := n//d \qquad \text{and} \qquad r := n\%d.$$

Then, $n = qd + r$ and $q \in \mathbb{Z}$ and $r \in \{0, 1, \ldots, n-1\}$.

(b) Again, this is an "if and only if" statement, and we shall prove its "$\Longrightarrow$" and "$\Longleftarrow$" directions separately:

$\Longrightarrow$: Assume that $d \mid n$. We must prove that $n\%d = 0$. In other words, we must prove that $r = 0$.

Indeed, $d \mid n$ yields that there is some $c \in \mathbb{Z}$ such that $n = dc$. Consider this c. Therefore, $(c, 0)$ is a quo-rem pair of n and d (since $n = dc = dc + 0$). However, (q, r) is also a quo-rem pair of n and d (by its definition). Since there is only one quo-rem pair of n and d (by the theorem from last time), this shows that $(c, 0) = (q, r)$. In particular, $0 = r$, so that $0 = r$. In other words, $r = 0$. This proves the "$\Longrightarrow$" direction (i.e., it proves that if $d \mid n$, then $n\%d = 0$).

$\Longleftarrow$: If $n\%d = 0$, then $d \mid n$ because

$$n = qd + \underbrace{r}_{=n\%d=0} = qd.$$

This proves the "$\Longleftarrow$" direction. Thus, both directions are proved, so that part **(b)** of the proposition holds.

(c) Let $c \in \{0, 1, \ldots, d-1\}$ satisfy $c \equiv n \mod d$. We must show that $c = n\%d$.

From $c \equiv n \mod d$, we obtain $d \mid c - n$. In other words, $c - n = de$ for some $e \in \mathbb{Z}$. Consider this e. From $c - n = de$, we obtain $c = n + de$, so that $n = c - de = (-e)\, d + c$. This (combined with $c \in \{0, 1, \ldots, d-1\}$) shows that $(-e, c)$ is a quo-rem pair of n and d. However, (q, r) is also a quo-rem pair of n and d (by its definition). Since there is only one quo-rem pair of n and d (by the theorem from last time), this shows that $(-e, c) = (q, r)$. Hence, $c = r = n\%d$. So we are done. $\square$

1.2. Greatest common divisors

Definition 1.2.1. Let a and b be two integers. Then:

(a) The **common divisors** of a and b are the integers that divide a and simultaneously divide b.

(b) The **greatest common divisor** of a and b is the largest among the common divisors of a and b, unless $a = b = 0$. In the latter case, it is defined to be 0.

We denote the greatest common divisor of a and b as $\gcd(a, b)$, and we refer to it as the **gcd** of a and b.

Remark 1.2.2. Why is this well-defined (i.e., why **is** there a largest among the common divisors of a and b ?), and why do we need the exception for $a = b = 0$?

The exception for $a = b = 0$ is necessary, because **every integer** is a common divisor of 0 and 0 (and therefore there is no largest among these common divisors).

As to the first question, consider the case when not both a and b are 0. For example, let's assume $a \neq 0$. Then, any common divisor of a and b divides a and therefore is at most $|a|$. Hence, there is a largest among these common divisors (because 1 is always a common divisor). What we are using here is the fact that any nonempty set of integers that is bounded from above has a largest element.

We collect some basic properties of gcds in the following proposition:

Proposition 1.2.3. **(a)** We have $\gcd(a, b) \in \mathbb{N}$ for any $a, b \in \mathbb{Z}$.

(b) We have $\gcd(a, 0) = \gcd(0, a) = |a|$ for any $a \in \mathbb{Z}$.

(c) We have $\gcd(a, b) = \gcd(b, a)$ for any $a, b \in \mathbb{Z}$.

(d) If $a, b, c \in \mathbb{Z}$ satisfy $b \equiv c \mod a$, then $\gcd(a, b) = \gcd(a, c)$.

(e) We have $\gcd(a, b) = \gcd(a, ua + b)$ for any $a, b, u \in \mathbb{Z}$.

(f) We have $\gcd(a, b) = \gcd(a, b\%a)$ for any positive integer a and any $b \in \mathbb{Z}$.

(g) We have $\gcd(a, b) \mid a$ and $\gcd(a, b) \mid b$ for any $a, b \in \mathbb{Z}$.

(h) We have $\gcd(-a, b) = \gcd(a, b)$ and $\gcd(a, -b) = \gcd(a, b)$ for any $a, b \in \mathbb{Z}$.

(i) If $a, b \in \mathbb{Z}$ satisfy $a \mid b$, then $\gcd(a, b) = |a|$.

Proof. **(a)** Let $a, b \in \mathbb{Z}$. We must prove that $\gcd(a, b) \in \mathbb{N}$.

Indeed, otherwise, $\gcd(a, b)$ would be negative, so that $-\gcd(a, b)$ would be a larger common divisor of a and b, which would contradict the definition of $\gcd(a, b)$.

(b) Let $a \in \mathbb{Z}$. The common divisors of a and 0 are just the divisors of a (since every integer divides 0). Thus, the largest of them is $|a|$ (unless $a = 0$). This proves part **(b)**.

(c) Let $a, b \in \mathbb{Z}$. The common divisors of a and b are exactly the common divisors of b and a. From this, part **(c)** quickly follows.

(d) Let $a, b, c \in \mathbb{Z}$ satisfy $b \equiv c \mod a$. We must prove that $\gcd(a, b) = \gcd(a, c)$.

Let d be a common divisor of a and b. Thus, $d \mid a$ and $d \mid b$. In other words, $a = dx$ and $b = dy$ for some integers x and y. Consider these x and y.

Now, $b \equiv c \mod a$. In other words, $a \mid b - c$. In other words, $b - c = am$ for some $m \in \mathbb{Z}$. Consider this m.

Now, solving the equation $b - c = am$ for c, we obtain

$$c = \underbrace{b}_{=dy} - \underbrace{a}_{=dx} m = dy - dxm = d(y - xm).$$

Thus, $d \mid c$. Therefore, d is a common divisor of a and c.

So we have shown that any common divisor of a and b must also be a common divisor of a and c. In other words,

$$\{\text{common divisors of } a \text{ and } b\} \subseteq \{\text{common divisors of } a \text{ and } c\}.$$

However, the same argument can be made with the roles of b and c swapped (because the relation $b \equiv c \mod a$ is symmetric in b and c). As a result, we obtain

$$\{\text{common divisors of } a \text{ and } c\} \subseteq \{\text{common divisors of } a \text{ and } b\}.$$

Combining this with

$$\{\text{common divisors of } a \text{ and } b\} \subseteq \{\text{common divisors of } a \text{ and } c\},$$

we obtain

$$\{\text{common divisors of } a \text{ and } b\} = \{\text{common divisors of } a \text{ and } c\}.$$

In other words, the common divisors of a and b are precisely the common divisors of a and c. Hence, the largest among the former divisors equals the largest among the latter divisors. In other words, $\gcd(a, b) = \gcd(a, c)$.

[Strictly speaking, the case $a = 0$ should be handled separately[1]. However, this case is trivial, because in this case the assumption $b \equiv c \mod a$ yields $b = c$.]

So part **(d)** is proved.

Part **(e)** follows from **(d)** because $b \equiv ua + b \mod a$.

Part **(f)** follows from **(d)** because $b \equiv b\%a \mod a$.

The remaining parts of the proposition are easy. □

Note that parts **(b)**, **(c)** and **(f)** of Proposition 1.2.3 yield a pretty fast way of

[1]because $\gcd(0, 0)$ is not literally the largest among the common divisors of 0 and 0

computing gcds: For example,

$$\begin{aligned}
\gcd(93,18) &= \gcd(18,93) && \text{(by part } \textbf{(c)}\text{)} \\
&= \gcd\left(18, \underbrace{93\%18}_{=3}\right) && \text{(by part } \textbf{(f)}\text{)} \\
&= \gcd(18,3) \\
&= \gcd(3,18) && \text{(by part } \textbf{(c)}\text{)} \\
&= \gcd\left(3, \underbrace{18\%3}_{=0}\right) && \text{(by part } \textbf{(f)}\text{)} \\
&= \gcd(3,0) = |3| && \text{(by part } \textbf{(b)}\text{)} \\
&= 3.
\end{aligned}$$

This method for computing $\gcd(a,b)$ is known as the **Euclidean algorithm**. In general, it proceeds as follows:

- If $a > b$, then swap a and b.
- If $a \leq b$, then replace b by its remainder $b\%a$.
- If $b = 0$, then the gcd is $|a|$.

Strictly speaking, this only covers the case when $a, b \in \mathbb{N}$. If a or b is negative, we start out by replacing a by $-a$ or b by $-b$ or both.

This algorithm (and the proposition that it relies on) can be used not just to compute $\gcd(a,b)$ quickly, but also to prove some properties of the gcd. The most important of these properties is the following theorem:

Theorem 1.2.4 (Bezout's theorem)**.** Let a and b be two integers. Then, there exist integers x and y such that

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

We will soon prove this theorem. First, a notation:

Definition 1.2.5. Let a and b be two integers. Then, a **Bezout pair** for (a,b) means a pair (x,y) of two integers such that $\gcd(a,b) = xa + yb$.

So Bezout's theorem says that for any two integers a and b, there exists a Bezout pair for (a,b).

> **Example 1.2.6.** What is a Bezout pair for $(2,3)$? It is a pair (x,y) of two integers such that $\gcd(2,3) = x \cdot 2 + y \cdot 3$. Since $\gcd(2,3) = 1$, this simply means a pair (x,y) of two integers such that $1 = x \cdot 2 + y \cdot 3$. For example, $(2,-1)$ is such a pair, because $1 = 2 \cdot 2 + (-1) \cdot 3$. There are many other such pairs, for example $(5,-3)$, since $1 = 5 \cdot 2 + (-3) \cdot 3$.

Proof of Bezout's theorem. We must show that for any $a, b \in \mathbb{Z}$, there exists a Bezout pair for (a,b).

We will prove this by strong induction on $a + b$. Unfortunately, this doesn't work right away, since $a + b$ can be arbitrarily small (keep in mind that a and b can be negative). Thus, we can only use induction to prove the theorem for **nonnegative** a and b. Once this is done, we will have to extend it to the case of arbitrary a and b (possibly negative).

So let us first prove the theorem for nonnegative a, b. In other words, we will prove the following claim:

> *Claim 1:* Let $n \in \mathbb{N}$. Then, for any two integers $a, b \in \mathbb{N}$ satisfying $a + b = n$, there is a Bezout pair for (a,b).

[*Proof of Claim 1:* Apply strong induction on n:

Induction step: Let $n \in \mathbb{N}$. Assume that Claim 1 holds for all smaller nonnegative integers instead of n; in other words, we assume that for any integers $a, b \in \mathbb{N}$ satisfying $a + b < n$, there is a Bezout pair for (a,b). This is our induction hypothesis.

We now need to prove that for any two integers $a, b \in \mathbb{N}$ satisfying $a + b = n$, there is a Bezout pair for (a,b).

So let us fix two such integers $a, b \in \mathbb{N}$ satisfying $a + b = n$.

Now, we have three cases:

Case 1: We have $a = 0$.

Case 2: We have $0 < a \leq b$.

Case 3: We have $a > b$.

Let us first consider Case 1. In this case, $a = 0$, so that $\gcd(a,b) = \gcd(0,b) = |b| = b$ (since $b \geq 0$). We are looking for a Bezout pair for (a,b). In other words, we are looking for a pair (x,y) of integers satisfying

$$\underbrace{\gcd(a,b)}_{=b} = x \underbrace{a}_{=0} + yb.$$

This equation simplifies to

$$b = x \cdot 0 + yb.$$

This is easily solved: e.g., take $(x,y) = (0,1)$. So we are done in Case 1.

Let us consider Case 2. In this case, $0 < a \leq b$. Hence,

$$\gcd(a,b) = \gcd(a, b-a)$$

(by Proposition 1.2.3 **(d)**, since $b \equiv b - a \mod a$). However, $b - a \in \mathbb{N}$ (since $a \leq b$) and

$$a + (b - a) = b < a + b = n.$$

Thus, we can apply the induction hypothesis to the pair $(a, b - a)$. So we conclude that there exists a Bezout pair (u, v) for $(a, b - a)$. Thus, u and v are two integers such that

$$\gcd(a, b - a) = ua + v(b - a).$$

Since $\gcd(a, b) = \gcd(a, b - a)$, we can rewrite this as

$$\gcd(a, b) = ua + v(b - a) = ua + vb - va = (u - v)a + vb.$$

This shows that $(u - v, v)$ is a Bezout pair for (a, b). Thus, such a Bezout pair exists, so we are done in Case 2.

Finally, we need to consider Case 3. Fortunately, the claim we are proving (namely, that there exists a Bezout pair for (a, b)) is symmetric in a and b: In fact, if (u, v) is a Bezout pair for (a, b), then (v, u) is a Bezout pair for (b, a) (because Proposition 1.2.3 **(c)** yields $\gcd(a, b) = \gcd(b, a)$). Thus, by swapping a with b, we can turn $a > b$ into $b > a$, that is, into $a < b$. (The sum $a + b$ does not change when we swap a and b, so it still remains n.) Hence, after this swap, we are either in Case 1 or in Case 2. So we are done in Case 3 as well.

Thus, in all three cases, we have shown that there exists a Bezout pair for (a, b); this completes the induction step. Thus, Claim 1 is proved.]

Claim 1 shows that Bezout's theorem holds when $a, b \in \mathbb{N}$. (Indeed, if $a, b \in \mathbb{N}$, then we can set $n = a + b$ and apply Claim 1.)

We need to prove the theorem for arbitrary $a, b \in \mathbb{Z}$. But this is easy: Replacing a by $-a$ (and x by $-x$), we can allow a to be negative; likewise, we can allow b to be negative.

So Bezout's theorem is proved. $\square$

This proof of Bezout's theorem encodes an algorithm for computing a Bezout pair for (a, b) – in other words, not only for computing $\gcd(a, b)$ but also for writing $\gcd(a, b)$ as a sum $xa + yb$ for some integers x and y. This is called the **extended Euclidean algorithm**.