Math 127: Division

Mary Radcliffe

1 Definitions and the Division Theorem

In this set of notes, we look to develop a sense of division and divisibility in the integers. We begin by refreshing some definitions we may have seen before.

Definition 1. Let $a, b \in \mathbb{Z}$. We say that b *divides* a if there exists an integer k such that $a = kb$. The number b is called a *divisor* or *factor* of a, and the number a is called a *multiple* of b. Notationally, we write $b|a$ to denote that b divides a.

We have already seen some results about division in our early work. For example, we showed the following things (possibly among others):

- If b is even and $b|a$, then a is even.
- If $a, b \in \mathbb{Z}$ and $a \geq 2$, then a does not divide one of b or $b + 1$.
- If ab is even, then one of a or b is even.
- If $a|b$ and $b|c$, then $a|c$.

In addition, in constructing the rational numbers, we at least alluded to the idea that we could think about integer division with remainders, and then we left that alone. Time to revive it! We begin our foray into divisibility with the following theorem.

Theorem 1 (Division Theorem)**.** *Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Then there exist unique integers $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < |b|$.*

Proof. First, note that if $a = 0$, then $q = 0, r = 0$ is the unique solution to the equation given.

We consider all other cases according to the signs of a and b.

Case 1: $b > 0, a > 0$. In order to prove the theorem, there are two parts: first, to show the existence of these integers q, r, and second, to show their uniqueness.

For the existence, for each $n \geq 0$ define $r_n = a - nb$. Let $S = \{r_n \mid r_n \geq 0\}$, that is, S is the set of those r_n that are nonnegative. Note that $r_0 = a > 0$, so S is nonempty. By the Well-Ordering Principle[1], S has a minimum element, say $r_k = a - kb$. Then $a = kb + r_k$, by definition. Moreover, $r_{k+1} = a - (k + 1)b = r_k - b < r_k$, so $r_{k+1} \notin S$, since r_k is the minimum of S. But this implies that $r_{k+1} < 0$, so $r_k - b < 0$, and hence $r_k < b$. Therefore, we have found integers k, r_k such that $a = kb + r_k$ and $0 \leq r_k < |b| = b$, and the existence of such integers is thus established.

For the uniqueness, suppose that $a = qb + r = q'b + r'$, where $q, q', r, r' \in \mathbb{Z}$ and $0 \leq r, r' < b$. By rearranging this equation, we have $qb - q'b = r' - r$, so $b(q - q') = r' - r$. Thus, $b|(r' - r)$. On the other hand, since $0 \leq r, r' < b$, we have that $-b < r' - r < b$. Note, if $q - q' > 0$, then $b(q - q') > b$, which is

[1]Technically, S is not a subset of $\mathbb{N}$ here, since 0 might be in S. However, the set $\mathbb{N} \cup \{0\}$ is also well ordered, so we can still apply the Well-Ordering Principle here.

impossible. If $q - q' < 0$, then $b(q - q') < -b$, which is also impossible. Therefore, it must be the case that $q - q' = 0$, which implies $r' - r = 0$, and thus the representation of a is unique.

Case 2: $b < 0, a > 0$. Note that any presentation of $a = qb + r$ also implies $a = (-q)(-b) + r$. The choice of $-q, r$ are both exist and are unique by Case 1.

Case 3: $b > 0, a < 0$. By Case 1, we have a unique q, r such that $-a = (-q)b + r$, with $0 \leq r < b$. Hence there is a unique q, r such that $a = qb - r$, with $0 \leq r < b$. If $r = 0$, this is sufficient for the problem. If $r \neq 0$, we can write $a = (q - 1)b + (b - r)$, then, and $0 < b - r < b$. Uniqueness will follow by an argument identical to that in Case 1.

Case 4: $b < 0, a < 0$. By Case 2, we have a unique q, r such that $-a = (-q)b + r$, with $0 \leq r < b$. Proceed as in Case 3 to construct a solution for a. □

Definition 2. Let $a, b \in \mathbb{Z}$, with $b \neq 0$ and let q, r be the numbers guaranteed by Theorem 1. We say that q is the *quotient* of a divided by b, and the r is the *remainder* of a divided by b.

So, the division theorem gives us one way to look at two numbers a, b in the case that neither divides the other: we can look at the divisibility in terms of remainders. We will revisit this later and define a structure of arithmetic on remainders, called modular arithmetic.

There is another approach, though, to looking at two numbers that do not have a divisibility relationship. We can look at what divisors they DO have in common.

2 GCDs and the Euclidean Algorithm

Definition 3. Let $a, b \in \mathbb{Z}$. An integer d is called a *greatest common divisor* of a, b, frequently abbreviated as a gcd of a, b if the following two conditions are met:

- $d|a \wedge d|b$
- $q|a \wedge q|b \Rightarrow q|d$.

Example 1. Let $a = 20, b = 10$. Then both 10 and -10 are gcds for a, b.

In general, we will restrict ourselves to considering positive gcds, so that we do not have this kind of thing come up. So we wish to define $\gcd(a, b)$ to be the positive gcd of a and b. One problem, though: we need to ensure that such a number exists. If we think of *gcd* as a function from $\mathbb{Z} \times \mathbb{Z}$ to $\mathbb{N}$, we would like to make sure that the function is well defined, so that the gcd exists and is unique for every choice of a, b.

Theorem 2. *Let $a, b \in \mathbb{Z}$. Then a and b have a gcd.*

Proof. First, if both a and b are 0, then 0 is a gcd for a and b, since 0 is divisible by q for every $q \in \mathbb{Z}$.

If a is negative, we can replace a with $-a$ without impacting the divisibility properties of a. Likewise, if b is negative, we can replace it with $-b$. Hence, we may proceed assuming that both a and b are nonnegative, and at least one of a, b is nonzero. Wolog, suppose that $a \neq 0$.

Define $X = \{n \in \mathbb{N} \mid n = au + bv \text{ for some } u, v \in \mathbb{Z}\}$. Notice that $a = a \cdot 1 + b \cdot 0$ and $a > 0$, so $a \in X$. Therefore, $X \neq \emptyset$, and X is a subset of $\mathbb{N}$, so by the Well Ordering Principle X has a minimum. Let $d = \min(X)$.

Claim 1: $d|a$.

Proof. [Proof of Claim 1.] By Theorem 1, there exist unique $q, r \in \mathbb{Z}$ such that $a = qd + r$, and $0 \leq r < d$. Moreover, as $d \in X$, there exist $u, v \in \mathbb{Z}$ such that $d = au + bv$. Hence, we have

$$\begin{aligned} r &= a - qd \\ &= a - q(au + bv) \\ &= (1 - qu)a + (-qv)b. \end{aligned}$$

Hence, if $r > 0$, we must have $r \in X$. However, since $r < d$, we cannot have $r \in X$, since $d = \min(X)$. Therefore, $r = 0$, so $a = qd$ and $d|a$. □

By the same technique, we can establish the following claim:

Claim 2: $d|b$.

Hence, we have that d is a common divisor to both a and b. It remains to establish the second property for a gcd, namely, that if $q|a$ and $q|b$, we also have $q|d$.

To that end, suppose that q is a common divisor of a and b, so that there exist integers k, ℓ such that $a = kq$ and $b = \ell q$. Then we have

$$d = au + bv = kqu + \ell qv = q(ku + \ell v),$$

and thus $q|d$.

Therefore, d meets the definition of a gcd for a, b, and thus a gcd must exist. □

This gets us half of the way through our conundrum: we know that a, b have a nonnegative gcd. We would also like to establish this gcd is unique, which will be done with the following homework exercise:

Proposition 1. Let $a, b \in \mathbb{Z}$. If d, d' are both gcds for a, b, then $d = \pm d'$.

Hence, we can consistently define $\gcd(a, b)$ to be the unique nonnegative *gcd* for two integers a, b. It will be useful to know, in general, some basic properties of *gcd*, as follows.

Proposition 2. Let $a \in \mathbb{Z}$. Then

- $\gcd(a, 0) = a$.
- $\gcd(a, 1) = 1$.
- For all $k \in \mathbb{Z}$, $\gcd(a, ka) = a$

Ok, but in general, how do we calculate gcds? The answer is through a classic algorithm known as the Euclidean Algorithm. To explain how the algorithm works, we first need a very useful theorem.

Theorem 3. *Let $a, b \in \mathbb{Z}$, with $b \neq 0$, and let q, r be the unique integers guaranteed by Theorem 1 having $a = qb + r$. Then*

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

Before we prove this theorem, let's consider what it buys us. Suppose we wish to find the gcd of two numbers a, b, where wolog $a > b$. This can be tricky, because we would have to consider all the divisors of the two numbers, which is a computationally difficult problem. But Theorem 3 tells us that we don't really have to do all that; we can reduce the problem to a simpler problem by just dividing a by b, and picking out the remainder instead. This is a smaller number than a, so it will end up being easier to deal with. Moreover, we can perform division pretty simply by just looking at $a - b, a - 2b$, etc, until we find a negative number; then we know what the division ought to be. We can even do all this work by hand. For example:

Example 2. Calculate $\gcd(67620, 66234)$.

Solution. This looks atrocious, but it's not really. First, we can write

$$67620 = 66234 * 1 + 1386.$$

Therefore, by Theorem 3, we have that $\gcd(67620, 66234) = \gcd(66234, 1386)$.
Wash, rinse, repeat.

$$66234 = 1386 * 47 + 1092.$$

$$1386 = 1092 * 1 + 294.$$

$$1092 = 294 * 3 + 210.$$

$$294 = 210 * 1 + 84.$$

$$210 = 84 * 2 + 42.$$

$$84 = 42 * 2 + 0.$$

By repeatedly applying Theorem 3, we can say that $\gcd(67620, 66234) = \gcd(42, 0) = 42$ by Proposition 2.

In general, the algorithm can be defined recursively as follows.

Euclidean Algorithm. The Euclidean Algorithm is defined on input a, b, with $|a| > |b|$, and produces output $\gcd(a, b)$. The algorithm proceeds as follows:

- Initialize $r_0 = |a|$, $r_1 = |b|$.
- While $r_n > 0$: define r_{n+1} to be the remainder of r_{n-1} divided by r_n.
- If $r_n = 0$, then $r_{n-1} = \gcd(a, b)$.

It remains only to prove Theorem 3. The proof, actually, is pretty straightforward.

Proof. [Proof of Theorem 3] Let a, b, q, r be as in the statement of the theorem. Let $d = \gcd(a, b)$. Notice that as $r = a - bq$, and both a and b are divisible by d, then r is divisible by d as well.

Moreover, suppose that d' is an integer such that $d'|r$ and $d'|b$. Then since $a = qb + r$, we must also have that $d'|a$. But then as $d = \gcd(a, b)$, we have that $d'|d$. Hence, any divisor of both r and b is also a divisor of d.

Therefore, d meets the definition of gcd for b and r. By uniqueness of the positive gcd, we therefore have that $d = \gcd(b, r)$. □

2.1 Coprime Integers

Definition 4. Let $a, b \in \mathbb{Z}$. We say that a and b are *coprime*, or *relatively prime*, if a and b share no common factors. That is to say, a and b are coprime if $\gcd(a, b) = 1$. We write $a \perp b$ to denote that a and b are coprime.

Coprimality can be useful with thinking about common divisors. In particular, we have the following useful and obvious proposition, whose proof is a homework exercise:

Proposition 3. Let $a, b \in \mathbb{Z}$ be nonzero, and let $d = \gcd(a, b)$. Then

- $\frac{a}{d}$ and $\frac{b}{d}$ are coprime.
- Write $a = dk$ for some $k \in \mathbb{Z}$. Then for $y \in \mathbb{Z}$, if $a|(dy)$, then $k|y$.

3 Linear Diophantine Equations

The previous section gives us an understanding of how to compute $\gcd(a, b)$, and also in the proof of Theorem 2, we show that $\gcd(a, b)$ is the smallest positive number that can be written in the form $au + bv$ for some $u, v \in \mathbb{Z}$.

This leads us to a natural question: what other kind of stuff can be written in the form $au + bv$? That is to say, for what choices of $c \in \mathbb{Z}$ does the equation $au + bv = c$ have a solution $(u, v) \in \mathbb{Z} \times \mathbb{Z}$?

Example 3. The equation $2u + 4v = c$ has a solution $(u, v) \in \mathbb{Z} \times \mathbb{Z}$ if and only if c is even.

Proof. First, suppose that c is even, so that $c = 2k$ for some $k \in \mathbb{Z}$. Take $u = k$, $v = 0$. Then $2u + 4v = 2k = c$, so $2u + 4v = c$ has a solution.
On the other hand, if $2u + 4v = c$ has a solution, then since both $2u$ and $4v$ are even, we must also have that c is even. □

Ok, very good, but how did we know that c had to be even in that example? If you look at the equation, you see that each of the terms $2u$ and $4v$ are divisible by 2, so obviously when you add them together you should get something divisible by 2.

Can we generalize? Sure! What about looking at $au + bv = c$, for a general choice of a, b? If both a and b are divisible by d, then we should obviously also have that c is divisible by d. As in the example, this turns out to be the only rule we need.

Theorem 4 (Bezout's Lemma)**.** *Let $a, b, c \in \mathbb{Z}$, and put $d = \gcd(a, b)$. Then the equation $au + bv = c$ has a solution $(u, v) \in \mathbb{Z} \times \mathbb{Z}$ if and only if $d|c$.*

Proof. The forward direction is trivial: if $au + bv = c$ has a solution $(u, v) \in \mathbb{Z} \times \mathbb{Z}$, then as both au and bv are divisible by d, so too is c.

For the backward direction, suppose that $c \in \mathbb{Z}$ has $d|c$, so that $c = dk$ for some $k \in \mathbb{Z}$. Recall from the proof of Theorem 2 that d can be written as $ax + by$ for some $x, y \in \mathbb{Z}$. Then $c = dk = (ax + by)k = a(xk) + b(yk)$, so taking $u = xk$ and $v = yk$, we have an integer solution to $au + bv = c$. □

Using the definition of coprimality above, we have the following immediate corollary:

Corollary 1. *Let $a, b \in Z$. Then the equation $au + bv = 1$ has a solution $(u, v) \in \mathbb{Z} \times \mathbb{Z}$ if and only if $a \perp b$.*

That is to say, we can solve the equation $au + bv = 1$ over the integers if and only if a and b share no common factors at all.

This is fine, then, but it doesn't seem to actually help us solve real problems. That is, we have an answer to when a solution exists, but not how to actually find one. This is handled by the so-called Reverse Euclidean Algorithm.

Example 4. Find integers u, v so that $1092u + 294v = 42$.

Solution. These numbers were borrowed from Example 2, so we have already seen via the Euclidean Algorithm that $\gcd(1092, 294) = 42$. In particular, the steps of the Euclidean Algorithm to

get there were as follows:

$$1092 = 294 * 3 + 210.$$

$$294 = 210 * 1 + 84.$$

$$210 = 84 * 2 + 42.$$

$$84 = 42 * 2 + 0.$$

We can rewrite each of these things in terms of their remainders, as follows:

$$210 = 1092 - 294 * 3$$

$$84 = 294 - 210 * 1$$

$$42 = 210 - 84 * 2$$

Now, starting from the last equation, we substitute in:

$$\begin{aligned} 42 &= 210 - 84 * 2 \\ &= 210 - (294 - 210 * 1) * 2 = 210 * 3 + 294 * (-2) \\ &= (1092 - 294 * 3) * 3 + 294 * (-2) \\ &= 1092 * 3 + 294 * (-11) \end{aligned}$$

Hence, our solution is $u = 3$ and $v = -11$.

Excellent, that was good! But it isn't the only solution. You can check for yourself that $u = -4$ and $v = 15$ also solve the problem in the above example.

In fact, we could construct all kinds of example, just by making small adjustments to u and v. Indeed, suppose that x and y are integers with $ax + by = 0$. Then we could take $u + x$ and $v + y$, and that should generate more solutions to the equation. So now, if we wish to determine all solutions, we need to think about what kinds of integers there are having $ax + by = 0$.

Theorem 5. *Let $a, b \in \mathbb{Z}$ be nonzero, and let $d = \gcd(a, b)$. Then $ax + by = 0$ if and only if there exists $k \in \mathbb{Z}$ such that $x = \frac{bk}{d}$ and $y = \frac{-ak}{d}$.*

Proof. The backward direction is trivial; clearly any (x, y) taking the described form yields a solution to the equation.

Now, for the forward direction, suppose $ax + by = 0$. Write $a = nd$ and $b = md$, where by Proposition 3 we have that n and d are coprime. We make the following observations:

1. $ax = -by$, and hence $a|(by)$. Since $by = d(my)$, we have that $a|d(my)$, and hence by Proposition 3, $n|my$. Since n and m are relatively prime, $n|y$. Write $y = nt$.
2. Likewise to the above, $m|x$. Write $x = ms$.
3. $x = -\frac{b}{a}y = -\frac{mdnt}{nd} = -mt = \frac{b}{d}(-t)$, since $m = \frac{b}{d}$.

Put $k = -t$, so that $x = \frac{bk}{d}$. Then $y = -\frac{a}{b}x = \frac{-ak}{d}$, as desired. □

This Theorem yields the following immediate consequence:

Theorem 6. *Let $a, b \in \mathbb{Z}$ nonzero, and let $d = gcd(a, b)$. Suppose $c \in \mathbb{Z}$ with $d|c$, and let (u_0, v_0) be one solution to the equation $au + bv = c$. Then the set of all solutions to the equation is*

$$\left\{(u, v) \in \mathbb{Z} \times \mathbb{Z} \mid u = u_0 + \frac{bk}{d},\ v = v_0 - \frac{ak}{d} \text{ for some } k \in \mathbb{Z}\right\}$$