1 Integers and Divisibility

In this course we primarily want to study the factorization properties of integers. So we should probably start by reminding ourselves how integers and factorization work.

Much of this material was covered in Math 210, but we shall review it so we can use it during the rest of the course, as well as perhaps putting it on a somewhat firmer foundation.

1.1 The integers and the rationals

For further reading on the material in this subsection, consult **Rosen 1.1–1.3; PMF 1.1–1.2, 2.1–2.2**.

Definition 1.1. The *integers* are elements of the set $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$.

The *natural numbers* are elements of the set $\mathbb{N} = \{1, 2, \dots\}$ of positive integers.

The *rational numbers* are elements of the set $\mathbb{Q} = \{p/q : p, q \in \mathbb{Z}\}$.

Remark 1.2.

1. Some sources include 0 as a natural number; in this course we will not, and none of the four suggested texts do so.

2. You may feel like these aren't really definitions, and you're not entirely wrong. A rigorous definition of the natural numbers is an extremely tedious exercise in mathematical logic; famously, Russell and Whitehead feature the proposition that "$1 + 1 = 2$" on page 379 of *Principia Mathematica*.

   We will simply trust that everyone in this course understands how to count.

The natural numbers have two very important properties.

Fact 1.3 (The Well-Ordering Property)**.** *Every subset of the natural numbers has a least element.*

This may seem obviously true, but is important for proving a number of results. (Compare the integers, the rationals, and the reals, all of which lack this property).

Fact 1.4 (The Successor Property)**.** *Every natural number n has a* successor $n + 1$*. Every natural number except 1 is the successor of some natural number. In particular there is no greatest natural number.*

This successor property underlies the principle of induction, which should be familiar to you from Math 210. It has two different but equivalent formulations:

Fact 1.5 (The Principle of Weak Induction)**.** *Let $P(n)$ be some statement about the natural number n. Then if $P(1)$ is true, and if $P(k)$ implies $P(k+1)$, then $P(n)$ is true for every natural number n.*

Fact 1.6 (The Principle of Strong Induction)**.** *Let $P(n)$ be some statement about the natural number n. Then if $P(n)$ is true whenever $P(k)$ is true for all $k < n$, then $P(n)$ is true for every natural number n.*

Remark 1.7. As stated, the principle of strong induction doesn't separately require a base case (i.e. it does not single out the case $n = 1$). Why not?

1.2 Divisibility

For further reading on the material in this subsection, consult **Rosen 1.5; PMF 3.1**.

Definition 1.8. If a and b are integers, we say that a *divides* b and write $a|b$ if there is an integer m such that $am = b$. We say a is a *divisor* or *factor* of b.

If there is no such integer, we may say that a does not divide b, and write $a \nmid b$.

Remark 1.9. The requirement that m is an integer is very important; if we allowed m to be a rational number, every integer would divide every other.

Note that if $a|b$ then $a \neq 0$. Rosen includes this in the definition but it is in fact implied by the rest of the definition.

Example 1.10.

- $2|6$
- $-2|6$
- $4 \nmid 6$
- $13|221$
- $3 \nmid 221$
- $17|0$
- $24 \nmid 12$

Much of this course will be spent studying properties related to divisibility; for now we'll prove a few basic facts about divisibility.

Lemma 1.11. *If a, b, c are integers with $a|b$ and $b|c$, then $a|c$. (In other words, the relationship $|$ is transitive).*

Proof. $a|b$ so there is some integer m with $am = b$. And $b|c$ so there is integer n with $bn = c$. Thus $amn = c$, and since mn is an integer, we have $a|c$ by definition. □

Lemma 1.12. *If a, b are natural numbers and $a|b$, then $1 \leq a \leq b$.*

Proof. Since a is a natural number, we know that $1 \leq a$. So we just need to show that $a \leq b$.

We know $a = mb$ for some integer m; since $a, b \geq 0$ we must have $m \geq 0$, and thus $1 \leq m$ (since clearly $m \neq 0$ if $a \neq 0$). Multiplying this inequality by a we have $a \leq am = b$. □

Lemma 1.13 (Linear Combinations)**.** *If a, b, c, m, n are integers, and $a|b$ and $a|c$, then $a|mb+nc$. We can say that if a divides b and c then it divides any integer linear combination of them.*

Proof. We know there are integers p and q so that $ap = b$ and $aq = c$. Then we can see $a(pm + qn) = apm + aqn = bm + cn$, and since $pm + qn$ is an integer, we have $a|mb + nc$ by definition of "divides". □

1.3 The Greatest Common Divisor

For further reading on the material in this subsection, consult **Rosen 3.3, PMF 3.4, Stein 1.1.2**.

A useful tool for studying the divisibility and factorization properties of integers is the concept of the greatest common divisor.

Definition 1.14. If a and b are integers, then the *greatest common divisor* of a and b, written $\gcd(a, b)$ or just (a, b), is the largest (positive) integer d that divides both a and b.

We can similarly define $\gcd(a_1, a_2, \ldots, a_n)$ to be the largest (positive) integer that divides each a_i.

Remark 1.15. The notations $\gcd(a, b)$ and (a, b) are interchangeable. We'll mostly use (a, b) since it is shorter and easy to write; when we're worried about ambiguity we'll write out the full expression.

Example 1.16.

- $(4, 6) = 2$
- $(4, 8) = 4$
- $(2, 3) = 1$
- $(23, 47) = 1$
- $(-81, 36) = 9$
- $(-4, 4) = 4$
- $(1, a) = \gcd(a, 1) = 1$ for any integer a.
- $(0, a) = (a, 0) = |a|$ for any integer a.

Remark 1.17. We define $(0,0) = 0$ for boring technical reasons. This will almost never come up. (If you're familiar with the concept of an ideal, notice that the ideal generated by a and b is also the ideal generated by (a,b)–and the notation itself is suggestive.)

Fact 1.18. *For any integers a, b, $(a,b) = (b,a)$.*

Exercise 1.19. *Prove that if a and b are integers, then (a,b) exists and is unique.*

The greatest common divisor, as the name suggests, tells us how much two integers have in common (with respect to factorization). Sometimes integers have nothing in common:

Definition 1.20. If $(a,b) = 1$ then we say a and b are *relatively prime* or *coprime*.

Example 1.21.
- 2 and 3 are relatively prime. 4 and 7 are relatively prime. 12 and 35 are relatively prime.
- 4 and 6 are not relatively prime. 12 and 34 are not relatively prime. 1000 and 18 are not relatively prime.

We would like to split a pair of numbers into "the bit they have in common" and "the bit that's different." (We do this intuitively, really; we can look at 4 and 6 and see they have a 2 in common, and then factors of 2 and 3 respectively that they don't share). But we can be a bit more precise here:

Proposition 1.22. *If a, b are integers with $(a,b) = d$, then $(a/d, b/d) = 1$.*

Proof. Let a, b be integers and $(a,b) = d$. Both a/d and b/d are integers; suppose there is a positive integer e that divides both of them. Then we have integers m, n with

$$em = a/d \qquad en = b/d$$
$$dem = a \qquad den = b$$

and thus de divides both a and b.

But d is the greatest common divisor of a and b, so $d \geq de$, and since $e \geq 1$ we must have $e = 1$. So the only positive integer that divides both a/d and b/d is 1, and so $(a/d, b/d) = 1$ as desired. □

Thus given two integers a, b, we have split them into the common part (a,b), and the relatively prime parts a/d, b/d.

Corollary 1.23. *If a and $b \neq 0$ are integers, then $a/b = p/q$ for some integers p, q with $(p,q) = 1$.*

Proof. Let $d = (a, b)$ and set $p = a/d, q = b/d$. Then $(p, q) = 1$ by 1.22, and $p/q = (a/d)/(b/d) = a/b$. □

This allows us to talk about fractions being in lowest terms.

1.4 The GCD and linear combinations

For further reading on the material in this subsection, consult **Rosen 3.3, PMF 3.4–3.5, Stein 1.1.2, Shoup 1.1**.

Now that we understand how the greatest common divisor works, we want to see how it interacts with arithmetic–addition and multiplication.

Lemma 1.24. *Let a, b, c be integers. $(a + cb, b) = (a, b)$.*

Proof. Let a, b, c be integers. Suppose d is a divisor of both a and b. Then by lemma 1.13 on linear combinations we know that d divides $a + cb$. Thus d is a common divisor of a and $a + cb$.

Conversely suppose d divides both b and $a + cb$. We can see that $a = (a + cb) - c(b)$ is a linear combination of b and $a + cb$, and thus again by lemma 1.13 we see that d divides b. Thus d is a common divisor of a and b.

So we have proven that the set of common divisors of a and b is exactly the same as the set of common divisors of a and $a + cb$. Thus the greatest common divisor must be the same. □

This tells us that if we know the gcd of two numbers, we can add a multiple of the second number to the first without changing anything.

Example 1.25.

- We know that $(2, 3) = 1$. Thus we also have $(5, 3) = (8, 3) = (11, 3) = (30002, 3) = 1$.
- We know that $(8, 6) = 2$. Thus $(14, 6) = (68, 6) = 2$, and also $(8, 14) = (8, 86) = 2$.
- But note we can only change one thing at a time. $(15, 20) = 5$ but $(15 + 20, 20 + 15) = (35, 35) = 35$.

If we want to talk about addition and multiplication, it is useful to use the idea of a linear combination (which was already referenced in Lemma 1.13).

Definition 1.26. If a and b are integers, then an *integer linear combination* of a and b is a sum of the form $ma + nb$ where m, n are both integers.

Example 1.27. What are the linear combinations of 4 and 6? We clearly can get 4 and 6, as well as $8 = 2 \cdot 4$, $10 = 4 + 6$, $12 = 2 \cdot 6$. Linear combinations are not unique, as in $24 = 3 \cdot 4 + 2 \cdot 6 = 6 \cdot 4 = 4 \cdot 6$.

We can also get smaller numbers: $(-1)\cdot 4 + 6 = 2$, $(-3)\cdot 4 + 2\cdot 6 = 0$, and $(-3)\cdot 4 + (-5)\cdot 6 = -42$.

Example 1.28. What are some linear combinations of 5 and 7? We can get $10, 12, 14$ and so on. We can get $7 - 5 = 2$. So we can get $2 \cdot 7 - 2 \cdot 5 = 4$, and 6 and 8.

Is this the smallest postive result we can get? No! We see that $3 \cdot 5 - 2 \cdot 7 = 15 - 14 = 1$. Thus we can always get $3n \cdot 5 - 2n \cdot 7 = n$ and we can get any integer as a linear combination of 5 and 7.

You might notice that in both of these cases, the smallest result we can get is the greatest common denominator. This is in fact a general theorem, but we need an important (and familiar!) result first.

Lemma 1.29 (Division Algorithm)**.** *If a and b are integers and $b > 0$, then there are* unique *integers q and r such that $a = bq + r$ with $0 \leq r < b$.*

Remark 1.30. I describe this as familiar because this is just the division-with-remainder that we all learned in grade school. When we do the division b/a, then q is the quotient and r is the remainder.

Though this is traditionally called an "algorithm", the theorem itself doesn't give an algorithm. There is an algorithm presented in the proof, which is in essense division by repeated subtraction.

Proof. We use the well-ordering property.

Consider the set S of non-negative integers of the form $a - bk$ for k an integer. S is nonempty because when k is sufficiently small (possibly negative)–in particular when $k < a/b$–we will have $a - bk \geq 0$.

Since S is a set of non-negative integers, by the well-ordering property it has a least element $r = a - bq$. We will take these values as the values of r, q given in the theorem. By construction $r \geq 0$.

Suppose $r \geq b$. Then $r - b \geq 0$ and thus $r - b = a - b(q + 1)$ is an element of S which is smaller than r, contradicting minimality. Thus $0 \leq r < b$. This proves that the pair q, r exists.

(You can think of this process as conducting division by repeated subtraction. The last step is observing that if $r \geq b$ we can conduct one additional subtraction).

Now let us prove this pair is unique. Suppose we can write $a = q_1 b + r_1 = q_2 b + r_2$, giving us two representations of a as quotient and remainder. By subtracting these two equations we get

$$\begin{aligned} q_1 b + r_1 - (q_2 b + r_2) &= 0 \\ b(q_1 - q_2) &= r_2 - r_1 \end{aligned}$$

and thus b divides $r_2 - r_1$.

But since $0 \leq r_1, r_2 < b$, we know that $-b < r_2 - r_1 < b$. Since b cannot divide a number between 0 and b, we must have $r_2 - r_1 = 0$ and thus $r_2 = r_1$. Consequently $q_2 = q_1$ as well, and the quotient and remainder pair is unique. □

Proposition 1.31. *If a and b are integers and at least one is nonzero, then (a, b) is the least positive integer that is an integer linear combination of a and b.*

Proof. By the well ordering property there is a least positive integer that is a linear combination of a and b; call it $d = ma + nb$. We first wish to show that d is a common divisor of a and b—that is, that $d|a$ and $d|b$.

By the division algorithm, we can write $a = dq + r$ for $0 \leq r < d$. But then we can write $r = a - dq$ as a linear combination of a and q; since d is a linear combination of a and b, this means that r is a linear combination of a and b. In particular

$$r = a - dq = a - (ma + nb)q = (1 - mq)a - (nq)b.$$

Thus r is a linear combination of a and b but $0 \leq r < d$. Since d is the least positive linear combination, we must have $r = 0$

Thus $a = dq$ and so d divides a. An identical argument shows that d divides b, so g is a common divisor of a and b.

Now we much show that d is the *greatest* common divisor. Suppose c is some integer such that $c|a$ and $c|b$. Then by lemma 1.13 on linear combinations, $c|ma + nb = d$, and thus $c \leq d$. Therefore $d = (a, b)$. □

Note that the argument at the end of this proof generalizes:

Proposition 1.32. *If a and b are non-zero integers, then a positive integer d is equal to (a, b) if and only if*

- *$d|a$ and $d|b$, and*

- *If $c|a$ and $c|b$, then $c|d$.*

Proof. Let $d = (a, b)$. Then clearly $d|a$ and $d|b$. Suppose $c|a$ and $c|b$; then by the previous result $d = ma + nb$ and $c|ma + nb = d$.

Conversely, suppose $d|a$ and $d|b$, and that whenever $c|a$ and $c|b$ then $c|d$. Then d is a common divisor of a and b. In particular set $c = (a, b)$. Then we know that $c|d$, and thus $c \leq d$. But since d is a common divisor we also know that $c \geq d$, so $c = d$. □

Remark 1.33. This gives an alternate characterization of the greatest common divisor that does not depend on the usual notion of "less than" or "greater than."

In fact, we can think of divisibility as giving a partial order on the integers; then the greatest common denominator is the greatest common divisor under this partial order as well.

Corollary 1.34. *Integers a and b are relatively prime if and only if there are integers m and n such that $ma + nb = 1$.*

Proposition 1.35. *If a and b are integers, then the set of linear combinations of a and b is the set of integer multiples of (a, b).*

Proof. Set $d = (a, b)$. We first show that every linear combination of a and b is a multiple of d: since $d|a$ and $d|b$, then d divides any linear combination of them (by lemma 1.13).

Now let us show that every multiple of d is a linear combination of a and b. We know that d is a linear combination of a and b, so write $d = ma + nb$. Let kd be some multiple of d. Then $kd = k(ma + nb) = (km)a + (kn)b$ is a linear combination of a and b. □

Corollary 1.36 (Bezout's theorem)**.** *If a and b are integers, then there are integers m and n such that $ma + nb = (a, b)$.*

Remark 1.37. Bezout's theorem is actually a much more general theorem in algebraic geometry about solutions of polynomial equations (alternatively, about the intersections of curves). It was named for Étienne Bézout, and first proved by Claude Bachet.

(Stigler's Law of Eponymy, attributed to Robert Merton, says that no scientific discovery is named after its actual discoverer).

1.5 The Euclidean Algorithm

For further reading on the material in this subsection, consult **Rosen 3.4, PMF 4.1–4.2, Stein 1.1.2**.

In the previous subsection we saw that the greatest common divisor of two numbers is the least positive linear combination of them. But this doesn't quite tell us how to find it. Fortunately, there is a simple algorithm that allows us to find the greatest common denominator of any pair of numbers quite easily.

Unlike the "division algorithm" this is actually an algorithm–which means it gives a set of steps that, when followed, reliably returns an answer. However, it uses the division algorithm to make its steps work.

The basic idea is to repeatedly subtract copies of the smaller number from the larger number, switching repeatedly, until we get to zero. Because linear combinations don't change divisibility, this won't ever change the greatest common denominator, and so we can change our starting (large) problem into a smaller, easier problem. Repeating this step gives us an answer.

To make that argument more rigorous, we need to recall the following lemma:

Lemma 1.38. *If a, b are integers and $a = bq + r$, then $(a, b) = (b, r)$*

Proof. This is precisely Lemma 1.24. □

This allows us to compute gcds easily by reducing big gcd computations to smaller ones.

Example 1.39. Suppose we want to compute $(36, 56)$. Then $56 = 1 \cdot 36 + 20$ so $(56, 36) = (20, 36)$. Now we can see that $36 = 1 \cdot 20 + 16$ and thus $(20, 36) = (20, 16)$. Then $20 = 1 \cdot 16 + 4$ so $(20, 16) = (4, 16) = 4$. Thus $(36, 56) = 4$.

Theorem 1.40 (Euclidean Algorithm)**.** *Let a, b be integers with $a \geq b > 0$. Set $r_0 = a, r_1 = b$, and inductively define r_n by the division algorithm, setting $r + n02 = r_{n-1}q_{n-1} + r_n$. We have $r_1 > r_2 > \ldots r_k > 0$, and if r_k is the last nonzero remainder obtained this way, then $r_k = (a, b)$.*

Sketch of proof: By lemma 1.38 we know that each step doesn't change the gcd. Thus the gcd at the end is the gcd at the beginning. If we repeat our step we will eventually get one value to 0, and then the gcd of the two will be the other value. □

Example 1.41. Let us compute $(20, 78)$. We have $78 = 3 \cdot 20 + 18$ so $(20, 78) = (20, 18)$. Then $20 = 1 \cdot 18 + 2$ so $(20, 18) = (2, 18)$.

We can easily see that this is 2, but if we want to keep using the algorithm we compute that $18 = 9 \cdot 2 + 0$ so $(2, 18) = (2, 0) = 2$.

In the language of the algorithm, we have $r_0 = 78, r_1 = 20, r_2 = 18, r_3 = 0 = (20, 78)$.

This might seem overly difficult–isn't it easier to just list all the factors? (Or, for those of you who are sneaking ahead, to break the numbers into their prime factors?)

And indeed for small problems this is easier; most of you could probably compute $(20, 78)$ in your heads. But as the numbers in question get larger—much larger—factorization gets much harder. And Euclid's algorithm does not.

Fact 1.42 (Lamé)**.** *For any pair of natural numbers a, b, the Euclidean algorithm takes at most $\log_2(ab)$ steps to find (a, b).*

For any pair of natural numbers $a > b$, the Euclidean algorithm takes at most $5 \log_{10}(b)$ steps to find (a, b).