ALGEBRA

CHRISTIAN REMLING

1. Some elementary number theory

1.1. **Primes and divisibility.** We denote the collection of integers by $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, \ldots\}$. Given $a, b \in \mathbb{Z}$, we write $a|b$ if $b = ac$ for some $c \in \mathbb{Z}$. We then say that a *divides* b or that a is a *divisor* of b. For example, $3|21$ or $-5|100$, but $2 \nmid -3$.

Exercise 1.1. Show that divisibility has the following general properties: (1) if $a|b$ and $b|c$, then $a|c$; (2) if $a|b$ and $b|a$, then $a = \pm b$; (3) if $a|b$ and $a|c$, then also $a|(bx + cy)$ for arbitrary $x, y \in \mathbb{Z}$; (4) if $1 \le b < a$, then $a \nmid b$; (5) $a|x$ for all $x \in \mathbb{Z}$ precisely if $a = \pm 1$; (6) a and $-a$ have the same divisors; (7) $a|0$ for all $a \in \mathbb{Z}$.

An integer $p \ge 2$ is called a *prime* if it has no divisors other than ± 1, $\pm p$. The first few primes are $2, 3, 5, 7, 11, 13, 17, 19, \ldots$. The key tool for studying divisibility in $\mathbb{Z}$ is division with remainder: given $a, b \in \mathbb{Z}$, $b \ge 1$, there are unique integers m, r, with $0 \le r < b$, such that $a = mb + r$. To see that this is true, just consider the integers $a - xb$, for fixed $a, b \in \mathbb{Z}$ and with x varying over $\mathbb{Z}$. These are equally spaced, with distance b between consecutive numbers, so exactly one choice of x produces an integer in $\{0, 1, \ldots, b - 1\}$.

For example, if we divide 23 by 6, with remainder, then we obtain $23 = 3 \cdot 6 + 5$. Or let's divide -6 by 23: this gives $-6 = (-1) \cdot 23 + 17$.

Let $a, b \in \mathbb{Z}$, not both equal to zero. The *greatest common divisor* of a and b is defined as the greatest integer d that divides both a and b. We denote it by $\gcd(a, b)$ or just by (a, b). For example, $(6, 10) = 2$. If $(a, b) = 1$, then we call a, b *relatively prime.* If a and b are distinct primes, they will be relatively prime: there aren't any individual divisors, let alone common divisors. However, this sufficient condition for two integers to be relatively prime is certainly not necessary: for example, $a = 6$ and $b = 25$ are also relatively prime, but neither a nor b is a prime.

The *Euclidean algorithm* finds (a, b) by repeated division with remainder. By Exercise 1.1, sign changes do not affect divisors; in particular, they leave the gcd unchanged, and thus it's enough to be able to handle (a, b) in the case $a, b \geq 1$. It will be convenient to assume this when running the Euclidean algorithm (by the way, what is $(a, 0)$?).

We put $r_{-1} = a$, $r_0 = b$ and then define a sequence $r_1, r_2, \ldots, r_N$ recursively by

$$r_{n-2} = m_n r_{n-1} + r_n;$$

in other words, in the nth step, we take the two previous members of the sequence r_{n-2}, r_{n-1} and divide the former by the latter, to produce the new remainder r_n. Since the remainders decrease strictly (why is that true?), we must eventually reach $r_N = 0$, after N steps. When this happens, the algorithm stops and outputs $r_{N-1} = (a, b)$ as the desired gcd.

I'll give a general proof that this works in a moment, but let's first work an example. Let $a = 4620$, $b = 126$. We start out by dividing a by b:

$$4620 = 36 \cdot 126 + 84,$$

so $r_1 = 84$. Next, we divide $r_0 = b$ by r_1. Since $126 = 84 + 42$, this gives the new remainder $r_2 = 42$. We continue in this way and divide 84 by 42. Since this doesn't leave a remainder, we have that $r_3 = 0$ and thus $N = 3$ and $(4620, 126) = r_2 = 42$.

Exercise 1.2. Find $(4680, 756)$ and $(81, 210)$ by running the Euclidean algorithm by hand.

Exercise 1.3. Show that if $a < b$, then $r_1 = a$ (in other words, the first step just swaps a and b if they originally appeared in the "wrong" order).

Let's now discuss the general theory.

Theorem 1.1. *The Euclidean algorithm, as described above, computes* $r_{N-1} = (a, b)$.

Proof. Since $r_N = 0$, we have that $r_{N-2} = m_{N-1} r_{N-1}$, so $r_{N-1} | r_{N-2}$, and then $r_{N-3} = m_{N-2} r_{N-2} + r_{N-1}$, so also $r_{N-1} | r_{N-3}$. We can continue in this way to see that $r_{N-1} | r_n$ for all $n \leq N-1$, and since the algorithm started with $r_{-1} = a$ and $r_0 = b$ in the first two steps, we arrive at the conclusion that $r_{N-1} | a$, $r_{N-1} | b$.

It remains to be shown that r_{N-1} is the *largest* number that divides both a and b. To see this, let c be any common divisor of a and b. I claim that then $c | r_n$ for all $n \geq -1$. This again follows by just keeping track of what the algorithm does, step by step. Clearly, since $a = m_1 b + r_1$, we have that $c | r_1$. Next, from $b = m_2 r_1 + r_2$, we then see that $c | r_2$, and we can continue until the algorithm stops to establish my claim. In particular, $d = (a, b)$ must satisfy $d | r_{N-1}$, so $d \leq r_{N-1}$ and it follows that $d = r_{N-1}$, as claimed. □

From the Euclidean algorithm, we obtain a very useful decription of the gcd:

Theorem 1.2. *The gcd of a, b can be characterized as the smallest positive integer of the form $ax + by$, $x, y \in \mathbb{Z}$.*

Corollary 1.3. *The integers a, b are relatively prime precisely if there are $x, y \in \mathbb{Z}$ so that $ax + by = 1$.*

Proof of Theorem 1.2. Write $d = (a, b)$. We first show that there are $x, y \in \mathbb{Z}$ with $d = ax + by$. In fact, x, y can also be extracted from the Euclidean algorithm. Starting at the end again, we first observe that

$$d = r_{N-1} = r_{N-3} - m_{N-1} r_{N-2}. \tag{1.1}$$

In fact, it is true in general that $r_n = r_{n-2} - m_n r_{n-1}$, that is, each remainder is a linear combination of the previous two remainders. We can now successively plug these linear combinations into (1.1) to (eventually) express $d = r_{N-1}$ as a linear combination of $a = r_{-1}$ and $b = r_0$.

To conclude the proof, we must now show that the set of numbers $ax + by$, $x, y \in \mathbb{Z}$, does not contain positive integers that are smaller than d. That is clear, however, because d divides any such linear combination $ax + by$, so $ax + by \geq d$ if $ax + by$ is positive. □

Exercise 1.4. We defined the Euclidean algorithm only for $a, b \geq 1$. Convince yourself that Theorem 1.2 and its Corollary hold for arbitrary $a, b \in \mathbb{Z}$, not both zero.

Example 1.1. We saw above that $(4620, 126) = 42$, so by the Theorem, there are $x, y \in \mathbb{Z}$ so that $4620x + 126y = 42$. Moreover, by the proof, we can systematically find x, y from the Euclidean algorithm. Let us do this here; I'll make use of the divisions with remainder we did above, when we ran the Euclidean algorithm. We must start at the end. The algorithm terminated in $N = 3$ steps, and we obtained $d = r_2 = 42$ from $126 = 84 + 42$ or, equivalently, $42 = 126 - 84$. Working our way from the bottom up towards the top, we recall that we obtained $r_1 = 84$ from the division $4620 = 36 \cdot 126 + 84$, so $84 = 4620 - 36 \cdot 126$. Plug this into the previous equation to obtain that

$$42 = 126 - (4260 - 36 \cdot 126) = -4260 + 37 \cdot 126,$$

which is the desired representation of the gcd, with $x = -1$ and $y = 37$.

Lemma 1.4. *If $(a, b) = (a, c) = 1$, then also $(a, bc) = 1$.*

Proof. By the Corollary, $ax+by = au+cv = 1$ for suitable $u, v, x, y \in \mathbb{Z}$. It follows that $bcvy = (1 - ax)(1 - au) = 1 - az$ for some $z \in \mathbb{Z}$, by multiplying out the RHS. This says that $(a, bc) = 1$, as desired. □

Proposition 1.5. *(a) If $(a,b)=1$ and $a|c$, $b|c$, then also $ab|c$.*
(b) If p is a prime and $p|ab$, then $p|a$ or $p|b$.

Exercise 1.5. Give (simple) examples that show that both parts fail if the assumptions ($(a,b)=1$ and p prime, respectively) are dropped.

Proof. (a) By assumption, $c=ad=be$ and also $ax+by=1$ for suitable $x,y\in\mathbb{Z}$, so

$$c=c\cdot ax+c\cdot by=beax+adby,$$

and it is now clear that $ab|c$, as desired.

(b) A prime has no divisors ≥ 2 other than itself, so $(p,a)=1$ unless $p|a$. So if what we are trying to show were false, then p would be relatively prime to both a and b, but then also to ab, by Lemma 1.4. This contradicts our assumption that $p|ab$, that is, $(p,ab)=p$. □

With these preparations out of the way, we can now give a proof, from scratch, of the *fundamental theorem of arithmetic:*

Theorem 1.6. *Every integer $a\geq 1$ can be written as a product of primes $a=p_1p_2\cdots p_n$. Moreover, this factorization is essentially unique in the sense that if also $a=p'_1p'_2\cdots p'_m$, then $m=n$ and, after relabeling suitably, $p_j=p'_j$.*

Proof. We first establish the existence of such a factorization into primes. If a is itself a prime, then there's nothing to show: take $n=1$, $p_1=a$. (Also, in the trivial case $a=1$, we take $n=0$, which works formally because the empty product is, by definition, equal to 1.) If $a\geq 2$ is not a prime, then $a=bc$ with $1<b,c<a$, and now either b,c are both primes and we're done, with $n=2$, $p_1=b$, $p_2=c$, or at least one of them has non-trivial divisors, which again must be smaller than the original number. We then factorize further, and since the numbers keep getting smaller as long as we still have divisors, this must stop at some point, and we obtain the desired factorization.

Exercise 1.6. Give a more formal version of this very simple argument; more precisely, prove the existence of a factorization into primes by an induction on a.

We now prove the uniqueness claim, by induction on n. If $n=0$, then $a=1$, and we must have that $m=0$ also, since $p'_j\geq 2$. Now suppose that $n\geq 1$ and that the claim holds for $n-1$. Clearly, $p_1|a$, and by repeatedly applying Proposition 1.5(b), we see that $p_1|p'_j$ for some j; for convenience, let's assume that $j=1$. Since p_1,p'_1 are both primes, this can only happen if $p_1=p'_1$. It follows that $p_2\cdots p_n=p'_2\cdots p'_m$, and since the product on the LHS has $n-1$ prime factors, the induction hypothesis now gives that $n-1 = m-1$ and the primes in both products agree, after relabeling. □

In the factorization from Theorem 1.6, repeated primes are of course possible, for example $12 = 2 \cdot 2 \cdot 3$. We usually reorganize slightly and write prime factorizations in the form

$$a = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n},$$

with exponents $e_j \geq 0$.

Theorem 1.7 (Euclid)**.** *There are infinitely many primes.*

Proof. Given primes $p_1, \ldots p_N$, consider $a = p_1 p_2 \cdots p_N + 1$. Then $a > 1$, so some prime at least must occur in its factorization (a itself could be prime), but clearly none of $p_1, \ldots, p_N$ divides a, so there must be an additional prime. □

1.2. **Congruences.**

Definition 1.8. An *equivalence relation* on a set A is a binary relation $\sim$ that is: (1) *reflexive:* $a \sim a$ for all $a \in A$; (2) *symmetric:* if $a \sim b$, then $b \sim a$; (3) *transitive:* if $a \sim b$ and $b \sim c$, then $a \sim c$.

For example, equality $=$ is an equivalence relation on any set A, and so is the relation defined by letting $a \sim b$ hold for any two $a, b \in A$. We will see a more interesting example in a moment.

In general, equivalence relations are essentially the same thing as *partitions.* Here, we call a collection of non-empty subsets $A_\alpha \subseteq A$ (finitely or infinitely many, and the sets themselves may be finite or infinite) a partition of A if $A_\alpha \cap A_\beta = \emptyset$ for $\alpha \neq \beta$ and $\bigcup_\alpha A_\alpha = A$.

Exercise 1.7. Elaborate on the claim made above. More specifically, show the following: (a) If $\sim$ is an equivalence relation on A and we define $A_a = \{b \in A : b \sim a\}$, for $a \in A$, then, for any two $a, b \in A$, either $A_a \cap A_b = \emptyset$ or $A_a = A_b$. Moreover, $\bigcup_{a \in A} A_a = A$, so if we view the $\{A_a : a \in A\}$ as a collection of sets, then we have a partition (which is not indexed by $a \in A$).

(b) Conversely, given a partition $\{A_\alpha\}$, define a relation by declaring $a \sim b$ precisely if $a, b \in A_\alpha$ for some α (note that a, b are required to lie in the *same* set). Show that $\sim$ is an equivalence relation on A.

(c) Parts (a) and (b) provide operations that produce a partition from a given equivalence relation and vice versa. Show that these operations are inverses of each other. Maybe you want to set up some notation to formulate this clearly: for an equivalence relation R, let $F(R)$ be the partition defined in part (a). Similarly, given a partition

P, let $G(P)$ be the equivalence relation defined in part (b). Then you want to show that $G(F(R)) = R$ and $F(G(P)) = P$.

General comment: Everything in this problem is completely straightforward, you should be able to do it in your head. Just make sure you don't get intimidated by the notation.

In the sequel, we will pass freely between equivalence relations and partitions, as spelled out in this Exercise. Given an equivalence relation, we call $A_a = \{b \in A : b \sim a\}$ the *equivalence class* of a; also, it is common to denote this by $A_a = (a)$ or by $\overline{a}$. A member $b \in (a)$ is called a *representative* of the equivalence class of a; in other words, a representative is just a b with $b \sim a$. Finally, we will often want to consider the set $\{(a) : a \in A\}$ of equivalence classes; it is common to denote this by $A/\sim$.

Now fix an integer $k \geq 1$. A particularly important equivalence relation on $\mathbb{Z}$ is obtained by defining

$$m \equiv n \mod k \quad \text{if } k|m - n.$$

If this holds, we say that m, n are *congruent* modulo k.

Exercise 1.8. Show that congruence modulo k indeed is an equivalence relation.

Exercise 1.9. What is the equivalence class of an $n \in \mathbb{Z}$ with respect to congruence modulo k?

Congruence is an important equivalence relation because it respects the algebraic structure of $\mathbb{Z}$. Let's make this more precise. I claim that if $m \equiv m' \mod k$ and $n \equiv n' \mod k$, then also $m + n \equiv m' + n' \mod k$ and $mn \equiv m'n' \mod k$. Let's verify the second claim: we know that $m' = m + kx$ and $n' = n + ky$ for some $x, y \in \mathbb{Z}$. Thus $m'n' = mn + k(nx + my + kxy)$, and this shows that $m'n' \equiv mn$, as desired.

Exercise 1.10. Prove the claim about addition in the same way.

These properties allow us to define addition and multiplication on the equivalence classes, as follows: $(m) + (n) := (m + n)$, $(m)(n) := (mn)$. Here, $m+n$ and mn on the right-hand sides will depend on the choice of representatives; recall in this context that m is *not* determined by its equivalence class. Rather, we have that $(m') = (m)$ if (and only if) $m' \in (m)$. However, the argument from the preceding paragraph and the Exercise show that this will not cause problems here: while m, n are not uniquely determined by their equivalence classes, and thus $m + n$ isn't either, the *equivalence class* $(m + n)$ of $m + n$ is independent of these choices, and of course all the same remarks apply to the product (mn).

This collection of equivalence classes $\mod k$ is denoted by $\mathbb{Z}_k$ or (for reasons that will become clear later) by $\mathbb{Z}/(k)$. The equivalence classes themselves are also called *residue classes* in this context. We will later develop a more abstract view of these matters. For now, let me just present one result (Fermat's little theorem) as a teaser.

Exercise 1.11. Show that $+, \cdot$ in $\mathbb{Z}_k$ obey (most of) the usual rules. More precisely, let $x, y, z \in \mathbb{Z}_k$. Show that: (1) $x + y = y + x$ and $xy = yx$; (2) $(x + y) + z = x + (y + z)$ and $(xy)z = x(yz)$; (3) $x + 0 = x$ and $x \cdot 1 = x$; (4) there is an additive inverse $-x \in \mathbb{Z}_k$ such that $x + (-x) = 0$; in fact, we can obtain $-x$ as $-x = (-1)x$; (5) $x(y + z) = xy + xz$.

We have followed the usual practice of blurring the distinction between equivalence classes (= members of $\mathbb{Z}_k$) and their representatives (which are integers, from $\mathbb{Z}$): 0 in part (3) really stands for the equivalence class $(0) \in \mathbb{Z}_k$ of $0 \in \mathbb{Z}$, and similar remarks apply to parts (4), (5).

By and large this says that we can just manipulate algebraic expressions in $\mathbb{Z}_k$ the way we are used to. Some care must definitely be exercised, however. For example, $2 \cdot 3 \equiv 0 \mod 6$ even though $2 \not\equiv 0, 3 \not\equiv 0 \mod 6$, so $\mathbb{Z}_6$ (unlike $\mathbb{Z}$) has the property that zero may be written as a product of non-zero factors: $0 = 2 \cdot 3$

Proposition 1.9. *Let $k \geq 1$ and $a \in \mathbb{Z}$ be given. Then the congruence*

$$ax \equiv 1 \mod k$$

has a solution x precisely if a and k are relatively prime. In particular, this holds if $k = p$ is a prime and $a \not\equiv 0 \mod p$.

Proof. When written out, the congruence requires us to find $x, y \in \mathbb{Z}$ so that $ax + ky = 1$, and such x, y exist precisely if a, k are relatively prime, by Corollary 1.3. □

Theorem 1.10 (Fermat)**.** *If p is a prime and $a \not\equiv 0 \mod p$, then $a^{p-1} \equiv 1 \mod p$.*

Proof. In this proof, I am again not going to carefully distinguish between residue classes and their representatives in the notation.

Observe that there are exactly p residue classes modulo p: more specifically, by division by p with remainder, we see that each $n \in \mathbb{Z}$ is congruent to exactly one of $0, 1, \ldots, p - 1$. Now multiply the non-zero residue classes by a to obtain $a, 2a, \ldots, (p - 1)a$. I claim that these are still the residue classes $1, 2, \ldots, p-1$, possibly in a different order. Indeed, Proposition 1.9 guarantees that any $1 \le n \le p-1$ can be written as $n \equiv ax \mod p$, for some $1 \le x \le p-1$; note also that $x = 0$ can not be the solution that the Proposition says exists because $a0 \equiv 0$. So the list $a, 2a, \ldots, (p-1)a$ contains all non-zero residue classes, and this implies that there can't be repetitions because there are $p-1$ entries in the list and also $p-1$ residue classes that we know are listed.

In particular, this implies that

$$1 \cdot 2 \cdots (p-1) \equiv a \cdot (2a) \cdots ((p-1)a) \mod p$$

because on both sides, we are multiplying the same residue classes, only in a different order (perhaps). Manipulating the RHS further, we see that

$$A \equiv Aa^{p-1} \mod p, \qquad A \equiv 1 \cdot 2 \cdots (p-1);$$

in these steps, I've made repeated use of the properties from Exercise 1.11. With the help of Proposition 1.9 again, we can now successively "divide through" by $1, 2, \ldots, p-1$ to conclude that $1 \equiv a^{p-1}$, as claimed (more precisely, for each $n = 1, 2 \ldots, p-1$, I multiply both sides by an x with $nx \equiv 1$). □

Exercise 1.12. Compute $2^5 \mod 6$. So Fermat's little theorem may fail if p is not a prime. Where in the proof did I use this assumption? (I really used it twice, find both instances please.)

Exercise 1.13. As a by-product of this proof we saw that if $ax \equiv ay \mod p$, $a \not\equiv 0 \mod p$, then $x \equiv y \mod p$ (for combinatorial reasons). Show this directly.