

## Notes on number theory

Basic fact about division:

**Exercise 62** in Chapter 1. Let  $a, b, c, m$ , and  $n$  be integers. Prove that if  $a$  divides each of  $b$  and  $c$ , then  $a$  divides  $nb + mc$ .

*Proof.* Suppose  $a$  divides each of  $b$  and  $c$ . Then there exist  $k, \ell \in \mathbb{Z}$  such that

$$\begin{aligned}b &= ka \\c &= \ell a.\end{aligned}$$

Then for any  $n, m \in \mathbb{Z}$

$$nb + mc = (nk + m\ell) a.$$

Hence  $a$  divides  $nb + mc$ .

gcd and the division algorithm:

**Exercise 92** in Chapter 3. Let  $b$  be a nonzero integer and let  $a, q$ , and  $r$  be integers such that

$$a = bq + r.$$

Prove that

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

*Proof.* Let  $d = \gcd(b, r)$ . Since  $d|b$  and  $d|r$ , by Exercise 62,  $d$  divides  $bq + r$ . That is,  $d|a$ . Since  $d|a$  and  $d|b$ , we have  $d|\gcd(a, b)$ . That is,  $\gcd(b, r) |\gcd(a, b)$ . Since  $\gcd(a, b) > 0$ , we conclude

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

Similarly, using  $r = b(-q) + a$ , we can prove

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

Application of the division algorithm:  $\gcd(a, b)$  is a combination of  $a$  and  $b$ :

**Theorem 1.** Let  $a$  and  $b$  be nonzero integers and let  $d = \gcd(a, b)$ . Then there exist integers  $m$  and  $n$  such that

$$d = ma + nb.$$

*Proof (sketch).* This follows from the Euclidean algorithm. Without loss of generality, assume  $0 < b < a$ . By the division algorithm there are  $q$  and  $r$  such that

$$\begin{aligned} a &= qb + r \\ 0 &\leq r < b. \end{aligned}$$

Thus

$$r = 1 \cdot a + (-q)b.$$

(1) If  $r = 0$ , then  $b$  divides  $a$  and  $d = b$ .

(2) If  $r > 0$ , then we consider  $0 < r < b$  and apply the division algorithm. Eventually we get a remainder which is  $d = \gcd(a, b)$  and we can express  $d$  as a combination of  $a$  and  $b$ .

Characterization of  $\gcd(a, b)$  as the least natural number which is a combination of  $a$  and  $b$ :

**Theorem 2 (Theorem 3.10).**  $d = \gcd(a, b)$  is the smallest number in the set

$$S = \{ma + nb : m, n \in \mathbb{Z}\} \cap \mathbb{N}.$$

*Proof.* By Theorem 1,  $d \in S$ . On the other hand, given any  $ma + nb \in S$ , we have

$$d \mid (ma + nb)$$

since  $d \mid a$  and  $d \mid b$ . Hence  $d \leq ma + nb$ .

$\gcd$  after dividing by  $\gcd$  (the following two corollaries comprise **Exercise 103** in Chapter 3):

**Corollary 3.** If  $d = \gcd(a, b)$ , then

$$\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

*Proof.* By Theorem 1, there exist integers  $m$  and  $n$  such that

$$d = ma + nb.$$

Hence

$$1 = m\frac{a}{d} + n\frac{b}{d}.$$

By Theorem 2,  $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ .

Conversely,

**Corollary 4.** If  $d \in \mathbb{N}$  is a divisor of both  $a$  and  $b$  such that  $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ , then  $d = \gcd(a, b)$ .

*Proof.* Reverse the argument above: If  $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ , then there exist integers  $m$  and  $n$  such that

$$1 = m\frac{a}{d} + n\frac{b}{d},$$

which implies

$$d = ma + nb.$$

Since  $\gcd(a, b)$  divides  $a$  and  $b$ , we have that  $\gcd(a, b)$  divides  $d$ . Thus  $\gcd(a, b) = d$ .

gcd times lcm:

**Exercise 96** in Chapter 3. If  $a, b \in \mathbb{N}$ , then prove that

$$\gcd(a, b) \cdot \text{lcm}(a, b) = ab.$$

*Proof.* Let  $d = \gcd(a, b)$  and let  $m = \text{lcm}(a, b)$ . We want to show  $dm = ab$ . Since  $d|a$  and  $d|b$ , there are integers  $e$  and  $f$  such that

$$a = de$$

$$b = df.$$

Since  $d = \gcd(a, b)$ , by Corollary 3 we have

$$\gcd(e, f) = \gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

We want to show that

$$m = def,$$

for then we would have

$$\gcd(a, b) \cdot \text{lcm}(a, b) = dm = d^2ef = ab.$$

Now  $a|def$  and  $b|def$ , so that  $def$  is a multiple of both  $a$  and  $b$ .

Suppose that  $n$  is a multiple of both  $a$  and  $b$ . We want to show that  $def \leq n$ . Since  $\gcd(e, f) = 1$ , there are integers  $p$  and  $q$  such that

$$pe + qf = 1.$$

Hence

$$pne + qnf = n.$$

Since  $b = df$  divides  $n$ , we have  $def$  divides  $ne$ . Similarly, since  $a = de$  divides  $n$ , we have  $def$  divides  $nf$ . Hence  $def$  divides  $pne + qnf = n$ . We conclude  $def \leq n$ . That is,  $def$  is equal to the least common multiple  $m = \text{lcm}(a, b)$ .

dividing two numbers and being relatively prime to one of them:

**Corollary 3.11 (Exercise 98).** If  $a, b$ , and  $c$  are integers such that  $a$  and  $b$  are relatively prime and  $a|bc$ , then  $a|c$ .

*Proof.* Since  $\text{gcd}(a, b) = 1$ , there exists  $m, n \in \mathbb{Z}$  such that

$$ma + nb = 1.$$

Then

$$mac + nbc = c.$$

Since  $a$  divides  $mac$  and  $a$  divides  $bc$ , by Exercise 62,  $a$  divides  $mac + nbc$ . That is,  $a$  divides  $c$ .

properties of prime numbers:

**Theorem 3.12 (Exercise 99).** If  $p$  is a prime and  $a$  is an integer such that  $p$  does not divide  $a$ , then  $a$  and  $p$  are relatively prime.

*Proof.* Since  $\text{gcd}(a, p)$  is a divisor of  $p$  and  $p$  is prime, we have  $\text{gcd}(a, p) = 1$  or  $\text{gcd}(a, p) = p$ . If  $\text{gcd}(a, p) = p$ , then  $p$  divides  $a$  since  $\text{gcd}(a, p)$  divides  $a$ . We have proved that  $\text{gcd}(a, p) = 1$  or  $p|a$ . Hence, if  $p$  does not divide  $a$ , then  $a$  and  $p$  are relatively prime.

**Corollary 3.13 (Exercise 100).** Let  $a$  and  $b$  be integers and let  $p$  be a prime number. If  $p$  divides  $ab$ , then  $p$  divides  $a$  or  $p$  divides  $b$ .

*Proof.* Suppose  $p$  does not divide  $a$ . Then by Theorem 3.12,  $a$  and  $p$  are relatively prime. By Corollary 3.11, since  $p$  and  $a$  are relatively prime and  $p$  divides  $ab$ , we have  $p$  divides  $b$ . We have proved that  $p$  divides  $a$  or  $p$  divides  $b$ .

congruence:

Let  $n \in \mathbb{N}$  and  $a, b \in \mathbb{Z}$ . We  $a$  is congruent to  $b$  modulo  $n$  if  $a - b$  is divisible by  $n$ . We write  $a \equiv b \pmod{n}$ .

Congruence modulo  $n$  is an equivalence relation on the set of integers  $\mathbb{Z}$ .

Define

$$[x] = [x]_n = \{y \in \mathbb{Z} : y \equiv x \pmod{n}\}.$$

**Example.** Take  $n = 5$ . We have

$$[3]_5 = \{\dots, -12, -7, -2, 3, 8, 13, 18, \dots\}.$$

**Theorem 4.9.** If  $n \in \mathbb{N}$ , then each integer is congruent, modulo  $n$ , to precisely one of the integers  $0, 1, 2, \dots, n - 1$ .

*Proof.* Division algorithm. See p. 130.

Fix  $n \in \mathbb{N}$  and denote as before  $[x] = [x]_n$ . Thus the only congruence classes (modulo  $n$ ) are

$$[0], [1], [2], \dots, [n - 1].$$

Adding and multiplying congruence classes. Define

$$[x] \oplus [y] = [x + y]$$

$$[x] \odot [y] = [xy].$$

Not difficult exercise: show that the operations  $\oplus$  and  $\odot$  are well defined. Why is this an issue? Because when we write  $[x]$ , the  $x$  is not unique. For example,  $[x + n] = [x]$ . Hint to solution:

**Theorem 4.10.** Let  $n \in \mathbb{N}$  and let  $a, b, c, d \in \mathbb{Z}$ . If  $a \equiv b \pmod{n}$  and  $c \equiv d \pmod{n}$ , then

$$(a) \quad a + c \equiv b + d \pmod{n}$$

$$(b) \quad ac \equiv bd \pmod{n}.$$

*Proof of Part (a).* Suppose  $a \equiv b \pmod{n}$  and  $c \equiv d \pmod{n}$ . Then there are integers  $k$  and  $\ell$  such that

$$a - b = kn$$

$$c - d = \ell n.$$

(You may use the above for part (b) too.) Then

$$a + c - (b + d) = (a - b) + (c - d) = (k + \ell)n.$$

Hence  $a + c \equiv b + d \pmod{n}$ .

Part (b) is **Exercise 64** in Chapter 4.

Hint for **Exercise 70**: The main step uses the identity (something similar is also possible)

$$\begin{aligned} a^m - b^m &= a^{m-1}a - a^{m-1}b + a^{m-1}b - b^m \\ &= a^{m-1}(a - b) + (a^{m-1} - b^{m-1})b. \end{aligned}$$

Hint for **Exercise 66**: Let

$$S = \{[1], [2], \dots, [p-1]\}$$

be the set of nonzero equivalence classes mod  $p$ .

(a) Suppose  $[a] \in S$  and  $[a] = [-a]$ . Since  $[a] = [b]$  says that  $p$  divides  $a - b$ , we have ...

(b) Suppose  $[ab] \notin S$ . How do you obtain a contradiction?

(c)

$$a^2 - b^2 = (a - b)(a + b).$$

**Theorem 4.12.** Let  $n \in \mathbb{N}$ , let  $a, b, c \in \mathbb{Z}$ , and let  $d = \gcd(c, n)$ , and suppose that

$$ac \equiv bc \pmod{n}.$$

Then

$$a \equiv b \pmod{\frac{n}{d}}.$$

*Proof.* Assume  $ac - bc = (a - b)c$  is divisible by  $n$ . We need to show that  $a - b$  is divisible by  $\frac{n}{d}$ . By assumption, there is a  $k \in \mathbb{Z}$  such that

$$(a - b)c = kn.$$

Then

$$(a - b)\frac{c}{d} = k\frac{n}{d}$$

On the other hand, since  $d = \gcd(c, n)$ , by Corollary 3 we have

$$\gcd\left(\frac{c}{d}, \frac{n}{d}\right) = 1.$$

Thus, since  $\frac{n}{d}$  divides  $(a - b)\frac{c}{d}$ , by Corollary 3.11 we have  $\frac{n}{d}$  divides  $a - b$ . That is,  $a \equiv b \pmod{\frac{n}{d}}$ .

**Fermat's Little Theorem.** Let  $p$  be a prime, and let  $a \in \mathbb{N}$  such that  $p$  does not divide  $a$ . Then

$$a^{p-1} \equiv 1 \pmod{p}.$$

*Proof* of FLT (tricky). Suppose  $p$  divides  $ja$  for some  $j = 1, 2, \dots, p - 1$ . Then since  $\gcd(p, a) = 1$ , by Corollary 3.11 we have  $p$  divides  $j$ , a contradiction.

We conclude for all  $j = 1, 2, \dots, p - 1$  that  $p$  does not divide  $ja$ . That is, none of  $a, 2a, \dots, (p - 1)a$  is divisible by  $p$ .

Furthermore, no two of the integers  $a, 2a, \dots, (p-1)a$  is congruent modulo  $p$ . This is easy since if  $1 \leq i < j \leq p-1$  then  $ja - ia = (j-i)a$  is not divisible by  $p$ .

Tricky (but simple) idea: we have

$$\{[a], [2a], \dots, [(p-1)a]\} = \{[1], [2], \dots, [p-1]\}$$

because there are exactly  $p-1$  *nonzero* (i.e., not congruent to  $[0]$ ) congruence classes modulo  $p$  (the  $p-1$  congruence classes  $[a], [2a], \dots, [(p-1)a]$  are distinct and nonzero).

Conclusion

$$a \cdot 2a \cdots (p-1)a \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}.$$

That is,

$$(p-1)!a^{p-1} \equiv (p-1)! \pmod{p}.$$

That is,  $p$  divides  $(p-1)!a^{p-1} - (p-1)! = (p-1)!(a^{p-1} - 1)$ . On the other hand,  $\gcd(p, (p-1)!) = 1$ , so that  $p$  divides  $a^{p-1} - 1$ . That is,  $a^{p-1} \equiv 1 \pmod{p}$ .

**Corollary (Exercise 81 in Chapter 4).** Let  $p$  be a prime, and let  $a \in \mathbb{N}$ . Then

$$a^p \equiv a \pmod{p}.$$

*Proof.* (1) Suppose  $p$  does not divide  $a$ . Then by Fermat's Little Theorem,

$$a^{p-1} \equiv 1 \pmod{p},$$

so that  $a^p \equiv a \pmod{p}$  follows from multiplying by  $a$ .

(2) Suppose  $p$  divides  $a$ . Then  $a^p \equiv 0 \pmod{p}$  and  $a \equiv 0 \pmod{p}$ , which implies  $a^p \equiv a \pmod{p}$ .

**Wilson's Theorem: Theorem 4.16.** Let  $p$  be a prime. Then

$$(p-1)! \equiv -1 \pmod{p}.$$

**Exercise 83** (Big hint).

$$(p-1)! \equiv -(p-2)! \equiv 2(p-3)! \pmod{p}.$$

Why? Need to explain.

**Chinese Remainder Theorem.** To be discussed on Monday, May 12.  
**Theorem 4.14.**

**Example 9.** Solve the system of congruences:

$$\begin{aligned}x &\equiv 1 \pmod{3} \\x &\equiv 3 \pmod{7} \\x &\equiv 5 \pmod{11}.\end{aligned}$$

Any two of the moduli 3, 7, and 11 are relatively prime.

The Chinese Remainder Theorem says to solve

$$\begin{aligned}7 \cdot 11 \cdot y_1 &\equiv 1 \pmod{3} \\3 \cdot 11 \cdot y_2 &\equiv 1 \pmod{7} \\3 \cdot 7 \cdot y_3 &\equiv 1 \pmod{11}.\end{aligned}$$

Solutions are

$$\begin{aligned}y_1 &= -1 \\y_2 &= 3 \\y_3 &= -1.\end{aligned}$$

Then the Chinese Remainder Theorem says that

$$x = 1 \cdot 77y_1 + 3 \cdot 33y_2 + 5 \cdot 21y_3 = 115$$

is a solution to the original system of congruences.

### Notes on equivalence relations

An equivalence relation  $\simeq$  on a set  $X$  is a relation which is reflexive, symmetric and transitive:

1.  $x \simeq x$  for all  $x \in X$
2. if  $x \simeq y$ , then  $y \simeq x$
3. if  $x \simeq y$  and  $y \simeq z$ , then  $x \simeq z$ .

Equivalence class is a set of the form

$$[x] = \{y \in X : x \simeq y\}.$$

**Theorem.** For any  $x, y \in X$  either

$$[x] = [y] \quad \text{or} \quad [x] \cap [y] = \emptyset.$$

*Proof.* (1) Suppose  $x \simeq y$ . If  $z \in [x]$ , then  $z \simeq x$ . By transitivity,  $z \simeq y$ , that is  $z \in [y]$ . We have proved  $[x] \subseteq [y]$ . Similarly, one may prove that  $[y] \subseteq [x]$ .

(2) Suppose  $x \not\simeq y$ . Let  $z \in [x]$ . Then  $z \simeq x$ .

Suppose  $z \in [y]$  (we will get a contradiction to this assumption). Then  $z \simeq y$ . Hence by transitivity,  $x \simeq y$ , which contradicts  $x \not\simeq y$ . Hence  $z \notin [y]$ .

We have proved if  $z \in [x]$ , then  $z \notin [y]$ . Thus  $[x] \cap [y] = \emptyset$ .

Furthermore,

$$\bigcup_{x \in X} [x] = X.$$

Thus the equivalence classes  $[x]$  are disjoint and their union is the whole set  $X$ .

The set of all equivalence classes on  $X$  is denoted by

$$X / \simeq .$$

**Example 1.** Consider the set of integers  $\mathbb{Z}$  with the equivalence relation  $x \simeq y$  if  $x - y$  is an even integer, i.e.,  $x - y$  is divisible by 2. There are only two equivalence classes:

$[0]$  = the set of even integers

$[1]$  = the set of odd integers.

These two equivalence classes are disjoint and their union is the whole set  $\mathbb{Z}$ . And  $\mathbb{Z} / \simeq = \{[0], [1]\}$  is a two element set.

**Example 2.** Consider the set of real numbers  $\mathbb{R}$  with the equivalence relation  $x \simeq y$  if  $x - y$  is an integer.

The set  $\mathbb{R} / \simeq$  may be identified with the circle

$$\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}.$$

To see this, note that every real number is equivalent to a real number between 0 and 1. That is, if  $x \in \mathbb{R}$ , then there exists  $y \in [0, 1]$  such that  $x \simeq y$ . Moreover, in the subset  $[0, 1]$  the only two numbers which are equivalent are the endpoints 0 and 1. Identifying them gives a circle, like tying two ends of a string to get a loop.

A concrete way to see this is to define the function

$$F : \mathbb{R} \rightarrow \mathbb{R}^2$$

by

$$F(x) = (\cos 2\pi x, \sin 2\pi x).$$

Since

$$\cos^2 2\pi x + \sin^2 2\pi x = 1,$$

we have  $F(x)$  is in the circle for all  $x \in \mathbb{R}$ . Furthermore,

$$F(x) = F(y)$$

if and only if  $x - y$  is an integer, that is, if and only if  $x \simeq y$ . This means that one gets a map

$$\bar{F} : \mathbb{R}/\simeq \rightarrow \text{circle}$$

defined by

$$\bar{F}([x]) = F(x)$$

which is well-defined and actually a one-to-one correspondence. We have established (modulo checking some details) that there is a one-to-one correspondence between  $\mathbb{R}/\simeq$  and the unit circle.

**Example 3.** We can add a dimension to the previous example. Consider the plane  $\mathbb{R}^2 = \{(x, y) : x, y \in \mathbb{R}\}$  with the equivalence relation  $(x_1, y_1) \simeq (x_2, y_2)$  if  $x_1 - x_2$  and  $y_1 - y_2$  are both integers. It turns out that  $\mathbb{R}^2/\simeq$  may be identified with the surface of a donut (called a torus)!

relations which are not equivalence relations:

**Exercise 30abc** in Chapter 4.

(a) Let  $R = \{(1, 1), (2, 2), (3, 3), (4, 4), (1, 2), (2, 3)\}$ .

(b) Let  $R = \{(1, 2), (2, 1)\}$ .

(c) Let  $R = \{(1, 2), (2, 3), (1, 3)\}$ .

matrices:

**Exercise 45** in Chapter 4 (background). Assume  $n > 1$ . Let  $S$  denote the set of  $n \times n$  matrices with real coefficients. Let  $T$  denote the set of invertible  $n \times n$  matrices with real coefficients.

The identity matrix  $I$  is the matrix with 1's along the diagonal and 0's off the diagonal. It has the property that for any matrix  $N$ ,

$$N \cdot I = I \cdot N = N.$$

If  $M \in T$ , i.e., if  $M$  is invertible, then there is a unique  $n \times n$  matrix  $M^{-1}$  such that

$$M \cdot M^{-1} = M^{-1} \cdot M = I.$$

Note that  $I^{-1} = I$ .