3. Math 235 Fall 2021, Worksheet 3: Modular arithmetic

Modular arithmetic was introduced by Gauss, and has since become one of the most fundamental tools in number theory (and, via its generalization to arbitrary ideals in rings, in abstract algebra). We will state its foundational results without proof, as the proofs are both easy and easily found in the literature.

As before, $\mathbb{N}$ means the set $\{0, 1, 2, \ldots\}$.

3.1. Congruence

The fundamental notion of modular arithmetic is *congruence modulo n*:

Definition 3.1.1. Let $n, a, b \in \mathbb{Z}$. We say that *a is congruent to b modulo n* if and only if $n \mid a - b$. We shall use the notation "$a \equiv b \bmod n$" for "a is congruent to b modulo n".

We furthermore shall use the notation "$a \not\equiv b \bmod n$" for "a is not congruent to b modulo n".

For example:

- We have $3 \equiv 7 \bmod 2$, since $2 \mid 3 - 7 = -4$.
- We have $3 \not\equiv 6 \bmod 2$, since $2 \nmid 3 - 6 = -3$.
- Two integers a and b satisfy $a \equiv b \bmod 0$ if and only if $a = b$. (Indeed, $a \equiv b \bmod 0$ is defined to mean $0 \mid a - b$, but the latter divisibility happens only when $a - b = 0$, which is tantamount to saying $a = b$.)
- We have $a \equiv b \bmod 1$ for any two integers a and b.

The relation "$a \equiv b \bmod n$", as a relation between the two integers a and b (for fixed n), is called a *congruence modulo n*.

Here are some basic rules for dealing with congruences (prove them yourself, or see [Grinbe19, §2.3] for the proofs):

Proposition 3.1.2. Let $n \in \mathbb{Z}$ and $a \in \mathbb{Z}$. Then, $a \equiv 0 \bmod n$ if and only if $n \mid a$. (Thus, in particular, $n \equiv 0 \bmod n$ always holds.)

Proposition 3.1.3. Let $a, b, n \in \mathbb{Z}$. Then, $a \equiv b \bmod n$ if and only if there exists some $d \in \mathbb{Z}$ such that $b = a + nd$.

Proposition 3.1.4. Let $a, b, c, n \in \mathbb{Z}$. Then, $a - b \equiv c \bmod n$ if and only if $a \equiv b + c \bmod n$.

Proposition 3.1.5. Let $n \in \mathbb{Z}$.

(a) We have $a \equiv a \bmod n$ for every $a \in \mathbb{Z}$. (This is called the *reflexivity of congruence*.)

(b) If $a, b, c \in \mathbb{Z}$ satisfy $a \equiv b \bmod n$ and $b \equiv c \bmod n$, then $a \equiv c \bmod n$. (This is called the *transitivity of congruence*.)

(c) If $a, b \in \mathbb{Z}$ satisfy $a \equiv b \bmod n$, then $b \equiv a \bmod n$. (This is called the *symmetry of congruence*.)

(d) If $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ satisfy $a_1 \equiv b_1 \bmod n$ and $a_2 \equiv b_2 \bmod n$, then

$$a_1 + a_2 \equiv b_1 + b_2 \bmod n; \tag{1}$$

$$a_1 - a_2 \equiv b_1 - b_2 \bmod n; \tag{2}$$

$$a_1 a_2 \equiv b_1 b_2 \bmod n. \tag{3}$$

(e) Let $m \in \mathbb{Z}$ be such that $m \mid n$. If $a, b \in \mathbb{Z}$ satisfy $a \equiv b \bmod n$, then $a \equiv b \bmod m$.

Proposition 3.1.6. Let $n, a, b \in \mathbb{Z}$ be such that $a \equiv b \bmod n$. Then, $a^k \equiv b^k \bmod n$ for each $k \in \mathbb{N}$.

Proposition 3.1.5 **(b)** allows us to chain congruences together like equalities (as long as they all are congruences modulo the same n). Proposition 3.1.5 **(c)** allows us to turn them around. Combined with Proposition 3.1.5 **(a)** (which says that any equality is a congruence), these two facts reveal that congruence modulo n (for fixed $n \in \mathbb{Z}$) is an equivalence relation. We will often use this implicitly when we chain congruences (modulo the same n) together. For example, we will write

$$a \equiv b \equiv c \equiv d \bmod n$$

to mean that $a \equiv b \bmod n$ and $b \equiv c \bmod n$ and $c \equiv d \bmod n$. Such a chain of congruences then implies that any of the four numbers a, b, c, d is congruent to any other modulo n (since congruence modulo n is an equivalence relation). Equality signs ($=$) can also appear in such a chain, since Proposition 3.1.5 **(a)** says that any equality is a congruence.

Proposition 3.1.5 **(d)** allows us to add, subtract and multiply (but not divide) two congruences together. Finally, Proposition 3.1.6 allows us to take congruences to k-th powers whenever $k \in \mathbb{N}$.

Before stating any more general properties, let us see how the ones above can be used:

Exercise 3.1.1. Let $n \in \mathbb{N}$. Show that $7 \mid 3^{2n+1} + 2^{n+2}$.

Solution to Exercise 3.1.1. We have $3^2 = 9 \equiv 2 \bmod 7$. Thus, Proposition 3.1.6 (applied to 7, 3^2, 2 and n instead of n, a, b and k) yields $\left(3^2\right)^n \equiv 2^n \bmod 7$. Multiplying this congruence[1] by the obvious congruence $3 \equiv 3 \bmod 7$, we obtain $\left(3^2\right)^n \cdot 3 \equiv$

[1] i.e., applying (3)

$2^n \cdot 3 \bmod 7$. Thus, $3^{2n+1} = \left(3^2\right)^n \cdot 3 \equiv 2^n \cdot 3 \bmod 7$. On the other hand, $2^{n+2} = 2^n \cdot 2^2 = 2^n \cdot 4$, so that $2^{n+2} \equiv 2^n \cdot 4 \bmod 7$ (since any equality is a congruence).

Now, adding the two congruences[2] $3^{2n+1} \equiv 2^n \cdot 3 \bmod 7$ and $2^{n+2} \equiv 2^n \cdot 4 \bmod 7$, we obtain

$$3^{2n+1} + 2^{n+2} \equiv 2^n \cdot 3 + 2^n \cdot 4 = 2^n \cdot \underbrace{(3+4)}_{=7} = 2^n \cdot 7 \equiv 0 \bmod 7$$

(since $2^n \cdot 7$ is clearly divisible by 7). In other words, $7 \mid 3^{2n+1} + 2^{n+2}$. This solves Exercise 3.1.1. □

3.2. The substitution principle

Let us state some further general properties of congruences.

We know from Proposition 3.1.5 **(d)** that we can add or subtract any two congruences. Thus, by induction, we can add or multiply any finite number of congruences together:

Proposition 3.2.1. Let n be an integer. Let S be a finite set. For each $s \in S$, let a_s and b_s be two integers. Assume that

$$a_s \equiv b_s \bmod n \qquad \text{for each } s \in S. \tag{4}$$

Then,

$$\sum_{s \in S} a_s \equiv \sum_{s \in S} b_s \bmod n \qquad \text{and} \qquad \prod_{s \in S} a_s \equiv \prod_{s \in S} b_s \bmod n.$$

As a consequence of all the properties stated above, we can *substitute* numbers inside a congruence. That is, the following principle holds:

> *Substitution principle for congruences:* Let a, b, n be three integers satisfying $a \equiv b \bmod n$. Let E be a "reasonable" expression that contains a in it. If we substitute all of the a's in E by b's[3], then the resulting expression F will satisfy $E \equiv F \bmod n$.

For example, if a, b, n are three integers satisfying $a \equiv b \bmod n$, then $a^3 + 7a^2 - 5 \equiv b^3 + 7b^2 - 5 \bmod n$. Informally speaking, this is because the congruence $a \equiv b \bmod n$ allows us to substitute b for a in $a^3 + 7a^2 - 5$ (in the same way as $a = b$ would lead us to $a^3 + 7a^2 - 5 = b^3 + 7b^2 - 5$). Formally speaking, this is a consequence of Proposition 3.1.5 and Proposition 3.1.6 (see [Grinbe20, Example 3.2.13] and [Grinbe19, §2.5] for details).

[2] i.e., applying (1)

[3] More generally, we can replace **some** of the a's in E by b's. For example, we can replace the first two a's in $a^3 + a^2 + a$ by b's, obtaining $b^3 + b^2 + a$.

When I stated the substitution principle for congruences, I did not specify what "reasonable" means. And indeed, there are some limits to the principle: While it is true that $a \equiv b \bmod n$ implies $a^2 \equiv b^2 \bmod n$, it is **not** true that $a \equiv b \bmod n$ implies $2^a \equiv 2^b \bmod n$ (counterexample: $n = 2$, $a = 0$ and $b = 2$). Thus, while we can substitute integers in the base of a power (because of Proposition 3.1.6), we **cannot** substitute integers in the exponent of a power (since there is no analogue of Proposition 3.1.6 that would say that $k^a \equiv k^b \bmod n$ for each $k \in \mathbb{N}$). Likewise, substitution is not allowed in fractions or more complicated functions. It is best to read "reasonable" as "polynomial" in the substitution principle (with the caveat that all coefficients of the polynomial must be integers, and that the exponents are not to be changed).

Using the substitution principle, we can rewrite our above solution to Exercise 3.1.1 to make it much shorter:

Solution to Exercise 3.1.1 (shortened version). We have $3^2 = 9 \equiv 2 \bmod 7$. Thus, $3^{2n+1} = \left(\underbrace{3^2}_{\equiv 2 \bmod 7} \right)^n \cdot 3 \equiv 2^n \cdot 3 \bmod 7$ (here, we have used the substitution principle to substitute 2 for 3^2). Hence, (again using the substitution principle) we have

$$\underbrace{3^{2n+1}}_{\equiv 2^n \cdot 3 \bmod 7} + \underbrace{2^{n+2}}_{=2^n \cdot 2^2 = 2^n \cdot 4} \equiv 2^n \cdot 3 + 2^n \cdot 4 = 2^n \cdot \underbrace{(3+4)}_{=7} = 2^n \cdot 7 \equiv 0 \bmod 7$$

(since $2^n \cdot 7$ is clearly divisible by 7). In other words, $7 \mid 3^{2n+1} + 2^{n+2}$. This solves Exercise 3.1.1. □

3.3. Congruence vs. remainders

When n is a positive integer, congruences modulo n are closely related to remainders upon division by n. We recall how the latter are defined (and introduce some notation for them):

Definition 3.3.1. Let n be a positive integer. Let $u \in \mathbb{Z}$. Then, there exists a unique pair $(q, r) \in \mathbb{Z} \times \{0, 1, \ldots, n-1\}$ such that $u = qn + r$. The entries q and n of this pair are denoted by $u//n$ and $u\%n$, and are called the *quotient* and the *remainder* of the division of u by n.

For instance, $17//5 = 3$ and $17\%5 = 2$.

Here are some basic properties of quotients and remainders (see [Grinbe19, §2.6] for the proofs of the first two propositions):

Proposition 3.3.2. Let n be a positive integer. Let $u \in \mathbb{Z}$.
(a) Then, $u\%n \in \{0, 1, \ldots, n-1\}$ and $u\%n \equiv u \bmod n$.
(b) We have $n \mid u$ if and only if $u\%n = 0$.
(c) If $c \in \{0, 1, \ldots, n-1\}$ is such that $c \equiv u \bmod n$, then $c = u\%n$.
(d) We have $u = (u//n)\, n + (u\%n)$.

Proposition 3.3.3. Let n be a positive integer. Let u and v be integers. Then, $u \equiv v \bmod n$ if and only if $u\%n = v\%n$.

Proposition 3.3.4. Let n be a positive integer. Let $u \in \mathbb{Z}$. Then, $u//n = \left\lfloor \dfrac{u}{n} \right\rfloor$.

Proposition 3.3.3 lets us turn congruences between integers into equalities between their remainders, and vice versa. Here is an example of how this can be useful:

Exercise 3.3.1. What is the last (i.e., least significant) digit of the number 7^{7^7} ? (Recall that a^{b^c} means $a^{(b^c)}$, not $\left(a^b\right)^c$, since the latter could equally well be written a^{bc}.)

Solution idea. With a computer, you could just compute the number (it has 695975 digits) and look at its last digit. But this is clearly not a viable strategy for an exam. (Besides, a modern examiner could equally well ask for $77^{77^{77}}$.) What to do?

For each positive integer m, the last digit of m is the remainder $m\%10$ (why?). So we must compute $7^{7^7}\%10$. To this purpose, it suffices to "simplify 7^{7^7} modulo 10", that is, find some smaller integer m such that $7^{7^7} \equiv m \bmod 10$. (Once such an m is found, we will then be able to apply Proposition 3.3.3 and conclude that $7^{7^7}\%10 = m\%10$. The remainder $m\%10$ should be easier to compute.)

As a warmup, let us first do this with 7^7. To make this task more manageable, we observe that $7^7 = 7^{2\cdot 3+1} = \left(7^2\right)^3 \cdot 7$, so we try to simplify 7^2 first. (This is an instance of "exponentiating by squaring", a well-known computational trick.) This is easy: We have $7^2 = 49 \equiv -1 \bmod 10$. Hence,

$$7^7 = \left(\underbrace{7^2}_{\equiv -1 \bmod 10} \right)^3 \cdot 7 \equiv (-1)^3 \cdot 7 = -7 \equiv 3 \bmod 10.$$

Thus, Proposition 3.3.3 yields $7^7\%10 = 3\%10 = 3$.

Now, let us come back to 7^{7^7}. Knowing that $7^7 \equiv 3 \bmod 10$, it is tempting to conclude that $7^{7^7} \equiv 7^3 \bmod 10$ (by substituting 3 for 7^7 in the exponent). Unfortunately, this is a misuse of the substitution principle, since we are not allowed to substitute in an exponent. (Although it would happen to produce the right answer in this particular case!)

Instead, we look at the first few powers of 7 modulo 10:

$$\begin{aligned}
7^0 &\equiv 1 \bmod 10;\\
7^1 &\equiv 7 \bmod 10;\\
7^2 &\equiv -1 \bmod 10;\\
7^3 &\equiv -7 \bmod 10;\\
7^4 &\equiv 1 \bmod 10;\\
7^5 &\equiv 7 \bmod 10;\\
7^6 &\equiv -1 \bmod 10;\\
&\cdots.
\end{aligned}$$

(We could equally well have used 9 and 3 instead of -1 and -7, since $-1 \equiv 9 \bmod 10$ and $-7 \equiv 3 \bmod 10$. However, the minus signs feel more natural.) A pattern is easily spotted: The right hand sides repeat every 4 lines. That is, we have

$$7^{k+4} \equiv 7^k \bmod 10 \qquad \text{for each } k \in \mathbb{N}. \tag{5}$$

This pattern is easily proved, too (just observe that $7^{k+4} = 7^k \cdot \underbrace{7^4}_{\equiv 1 \bmod 10} \equiv 7^k \cdot 1 = 7^k \bmod 10$).

Using (5), we see (by induction on m) that

$$7^{k+4m} \equiv 7^k \bmod 10 \qquad \text{for each } k \in \mathbb{N} \text{ and } m \in \mathbb{N}.$$

Hence, for each nonnegative integer n, we have

$$7^n \equiv 7^{n\%4} \bmod 10$$

(because $n = n\%4 + 4\,(n//4)$). Applying this to $n = 7^7$, we obtain $7^{7^7} \equiv 7^{7^7\%4} \bmod 10$.

Now we need to find $7^7\%4$. This is no harder than the remainder $7^7\%10$ we computed above; we get $7^7\%4 = 3$. Hence,

$$7^{7^7} \equiv 7^{7^7\%4} = 7^3 \equiv -7 \bmod 10.$$

Thus, Proposition 3.3.3 yields $7^{7^7}\%10 = (-7)\%10 = 3$, and we are done. □

3.4. More example problems

So much for the basics. Here are some more interesting problems:

Exercise 3.4.1. Let $P(x)$ be a univariate polynomial with integer coefficients. That is, there exist constant integers $u_0, u_1, \ldots, u_d$ such that each $x \in \mathbb{Z}$ satisfies $P(x) = \sum_{k=0}^{d} u_k x^k$.

Consider an integer sequence $(s_0, s_1, s_2, \ldots)$ defined recursively by setting

$$s_0 = 0$$

and

$$s_i = P(s_{i-1}) \qquad \text{for each } i \geq 1.$$

Prove the following: If a and b are two nonnegative integers satisfying $a \mid b$, then $s_a \mid s_b$.

[**Example:** If $P(x) = x^2 + 1$, then this sequence has recurrence relation $s_i = P(s_{i-1}) = s_{i-1}^2 + 1$, so its first 7 entries are

$$s_0 = 0, \qquad s_1 = 0^2 + 1 = 1, \qquad s_2 = 1^2 + 1 = 2, \qquad s_3 = 2^2 + 1 = 5,$$
$$s_4 = 5^2 + 1 = 26, \qquad s_5 = 26^2 + 1 = 677, \qquad s_6 = 677^2 + 1 = 458\,330.$$

It is easy to check that s_2 divides s_4 and s_6, and that s_3 divides s_6, as the exercise claims.]

Solution idea. This is similar to a property of the Fibonacci sequence we have seen on worksheet 1 (Exercise 1.1.1 **(e)**). Unfortunately, there is no "addition formula" this time, as our sequence $(s_0, s_1, s_2, \ldots)$ is a lot less "well-behaved" (at least when $P(x)$ has degree > 1). However, its simple recursion offers an advantage to working modulo n. To wit, the following holds:

Claim 1: Let $n \in \mathbb{Z}$, and let $i, j \in \mathbb{N}$ satisfy $s_i \equiv s_j \bmod n$. Then, $s_{i+1} \equiv s_{j+1} \bmod n$.

[*Proof of Claim 1:* We know that $P(x)$ is a polynomial with integer coefficients. Hence, the substitution principle for congruences tells us that $s_i \equiv s_j \bmod n$ entails $P(s_i) \equiv P(s_j) \bmod n$ [4]. In other words, $s_{i+1} \equiv s_{j+1} \bmod n$ (since the recurrence relation of our sequence entails $s_{i+1} = P(s_i)$ and $s_{j+1} = P(s_j)$). Thus, Claim 1 follows.]

Claim 1 can easily be leveraged to "move by multiple steps":

[4] If you don't believe this, just check it by hand: Write the polynomial P as $P(x) = \sum_{k=0}^{d} u_k x^k$ with integer coefficients $u_0, u_1, \ldots, u_d$. Then, $P(s_i) = \sum_{k=0}^{d} u_k s_i^k$ and $P(s_j) = \sum_{k=0}^{d} u_k s_j^k$. However, from $s_i \equiv s_j \bmod n$, we obtain $s_i^k \equiv s_j^k \bmod n$ for each $k \in \mathbb{N}$ (by Proposition 3.1.6). Multiplying this congruence by u_k (that is, by the obvious congruence $u_k \equiv u_k \bmod n$), we obtain $u_k s_i^k \equiv u_k s_j^k \bmod n$. Summing these congruences over all $k \in \{0, 1, \ldots, d\}$ (using Proposition 3.2.1), we obtain $\sum_{k=0}^{d} u_k s_i^k \equiv \sum_{k=0}^{d} u_k s_j^k \bmod n$. In other words, $P(s_i) \equiv P(s_j) \bmod n$ (since $P(s_i) = \sum_{k=0}^{d} u_k s_i^k$ and $P(s_j) = \sum_{k=0}^{d} u_k s_j^k$).

Claim 2: Let $n \in \mathbb{Z}$ and $k \in \mathbb{N}$, and let $i, j \in \mathbb{N}$ satisfy $s_i \equiv s_j \bmod n$. Then, $s_{i+k} \equiv s_{j+k} \bmod n$.

[*Proof of Claim 2:* Induction on k, using Claim 1 in the induction step.]

From Claim 2, in turn, we obtain the following claim, which is essentially a restatement of the exercise:

Claim 3: Let $a \in \mathbb{N}$ and $k \in \mathbb{N}$. Then, $s_{ak} \equiv 0 \bmod s_a$.

[*Proof of Claim 3:* We induct on k. The *base case* ($k = 0$) is obvious, since $s_{a \cdot 0} = s_0 = 0 \equiv 0 \bmod s_a$. For the *induction step*, we fix some $\ell > 0$, and assume (as IH[5]) that Claim 3 holds for $k = \ell - 1$. We must prove that Claim 3 holds for $k = \ell$.

Our IH says that $s_{a(\ell-1)} \equiv 0 \bmod s_a$. This can be rewritten as $s_{a(\ell-1)} \equiv s_0 \bmod s_a$ (since $s_0 = 0$). Hence, Claim 2 (applied to $i = a(\ell - 1)$ and $j = 0$ and $n = s_a$ and $k = a$) yields $s_{a(\ell-1)+a} \equiv s_{0+a} \bmod s_a$. In view of $a(\ell - 1) + a = a\ell$, this rewrites as

$$s_{a\ell} \equiv s_{0+a} = s_a \equiv 0 \bmod s_a.$$

In other words, Claim 3 holds for $k = \ell$. This completes the induction step, so that Claim 3 is proven.]

Now, if a and b are two nonnegative integers satisfying $a \mid b$, then we can write b as $b = ak$ for some $k \in \mathbb{N}$, and therefore Claim 3 yields $s_b \equiv 0 \bmod s_a$; but this says precisely that $s_a \mid s_b$. Thus, the exercise is solved. □

The above solution illustrates a general tactic: that of using congruences as scaffolding to prove divisibilities. Of course, congruences are themselves divisibilities ($a \equiv b \bmod n$ means nothing but $n \mid a - b$), but it is often more convenient to write them as congruences (particularly as this makes the substitution principle available).

There are other ways to use congruences as well. One is by exploiting their "veto power" over equations. The underlying idea is stupid: If a, b, n are integers such that $a \not\equiv b \bmod n$, then $a \neq b$. This turns out to be surprisingly useful:

Exercise 3.4.2. Find all pairs (x, y) of nonnegative integers satisfying $2^x - 1 = 3^y$.

Solution idea. The only such pairs are $(1, 0)$ and $(2, 1)$.

In fact, it is easy to check that $(1, 0)$ and $(2, 1)$ are such pairs; thus, we only need to show that there are no others. So we assume (for the sake of contradiction) that (x, y) is a pair of nonnegative integers satisfying $2^x - 1 = 3^y$ and $(x, y) \neq (1, 0)$ and $(x, y) \neq (2, 1)$. Thus, we can easily see that $x > 2$ (why?), so that 2^x is divisible by 8. That is, $2^x \equiv 0 \bmod 8$. Hence, from $2^x - 1 = 3^y$, we obtain $3^y = \underbrace{2^x}_{\equiv 0 \bmod 8} - 1 \equiv$

[5] Recall: "IH" = "induction hypothesis".

$0 - 1 \equiv 7 \bmod 8$. However, a look at the powers of 3 modulo 8 shows that this is impossible:

$$3^0 \equiv 1 \bmod 8,$$
$$3^1 \equiv 3 \bmod 8,$$
$$3^2 \equiv 1 \bmod 8,$$
$$3^3 \equiv 3 \bmod 8,$$
$$\ldots$$

(it is clear that the right hand sides repeat every 2 lines, and that 7 is not among them). Thus, the exercise is solved. □

3.5. Modular inverses and cancellation

In general, it is not allowed to cancel factors from congruences, even if the factors are nonzero. For instance, it is not true that $6a \equiv 6b \bmod 4$ implies $a \equiv b \bmod 4$; a counterexample is easy to find (for instance, $a = 0$ and $b = 2$). However, cancellation is allowed when the factor being cancelled is coprime to the modulus[6]. To wit, the following holds ([Grinbe20, Lemma 3.5.11]):[7]

Lemma 3.5.1. Let a, b, c, n be integers such that a is coprime to n and such that $ab \equiv ac \bmod n$. Then, $b \equiv c \bmod n$.

Better yet, even some sort of "division" is possible modulo n, as long as we divide by an integer coprime to the modulus:

Theorem 3.5.2. Let a and n be two coprime integers. Then, there exists an $a' \in \mathbb{Z}$ such that $aa' \equiv 1 \bmod n$.

For example, if $a = 2$ and $n = 5$, then we can take $a' = 3$ (since this satisfies $aa' = 2 \cdot 3 = 6 \equiv 1 \bmod 5$).

The integer a' in Theorem 3.5.2 is not unique, but it is "unique modulo n" (that is, any two valid candidates for a' are mutually congruent modulo n). We call such an integer a' a *modular inverse* to a modulo n. It does indeed behave like an inverse for a modulo n, in the sense that multiplication by a' undoes multiplication by a modulo n. Thus, Lemma 3.5.1 follows easily from Theorem 3.5.2 (just pick a modular inverse a' for a modulo n, and multiply both sides of the congruence $ab \equiv ac \bmod n$ with a').

Theorem 3.5.2, in turn, can be proved using the *Bezout theorem*, which says that if a and b are two integers, then $\gcd(a, b)$ can be written in the form $\gcd(a, b) = xa + yb$ for some integers x and y. We refer to [Grinbe20, Theorem 3.5.9 **(b)**] for the

[6] The *modulus* in a congruence $a \equiv b \bmod n$ is defined to be the number n.

[7] Recall that two integers u and v are said to be *coprime* if they satisfy $\gcd(u, v) = 1$. Instead of saying "u and v are coprime", we also say "u is coprime to v".

detailed proof of Theorem 3.5.2 (and to [Grinbe20, Theorem 3.4.5] for the proof of the Bezout theorem[8]).

Here are some applications of modular inverses and Lemma 3.5.1 in particular. The first is a piece of a greater result known as the *Chinese Remainder Theorem*:

Exercise 3.5.1. Let p and q be two coprime integers. Let a and b be any two integers. Prove that there exists some integer x such that

$$x \equiv a \bmod p \qquad \text{and} \qquad x \equiv b \bmod q.$$

Solution idea. We are looking for an integer x satisfying the two congruences $x \equiv a \bmod p$ and $x \equiv b \bmod q$. The first congruence means that $p \mid x - a$; in other words, it means that $x - a = up$ for some integer u. Thus, our x needs to satisfy $x - a = up$ for some integer u; in other words, it needs to have the form $x = a + up$ for some integer u. Now, it remains to find u in such a way that the second congruence $x \equiv b \bmod q$ will be satisfied as well. Upon substituting $a + up$ for x, this congruence $x \equiv b \bmod q$ rewrites as $a + up \equiv b \bmod q$, which is equivalent to $up \equiv b - a \bmod q$. To find u, we thus want to "divide $b - a$ by p" modulo q. Fortunately, we have a tool for this: modular inverses. To wit, Theorem 3.5.2 (applied to p and q instead of a and n) yields that there exists some $p' \in \mathbb{Z}$ such that $pp' \equiv 1 \bmod q$. Multiplying by this p' is like dividing by p. Thus, we set $u = p'(b-a)$, and then we have $up = pu = \underbrace{pp'}_{\equiv 1 \bmod q}(b-a) \equiv b - a \bmod q$, which is precisely what we wanted. Thus, setting $u = p'(b-a)$ and $x = a + up$ gives us the x we were looking for (or, to be precise, one such x).

Incidentally, when writing up a solution like this, you do not need to describe the thought process as I did above; all you need is to describe the x and prove that it works. This allows you to be much shorter. Here is how the above solution will look like when shortened like this:

First solution to Exercise 3.5.1. Theorem 3.5.2 (applied to p and q instead of a and n) yields that there exists some $p' \in \mathbb{Z}$ such that $pp' \equiv 1 \bmod q$. Consider this p'. Set $u := p'(b-a)$, and set $x := a + up$. Then,

$$x = a + u \underbrace{p}_{\equiv 0 \bmod p} \equiv a + u \cdot 0 = a \bmod p$$

and

$$x = a + \underbrace{up}_{=pu} = a + p \underbrace{u}_{=p'(b-a)} = a + \underbrace{pp'}_{\equiv 1 \bmod q}(b-a) \equiv a + 1(b-a) = b \bmod q.$$

Thus, we have found an integer x satisfying $x \equiv a \bmod p$ and $x \equiv b \bmod q$. This solves Exercise 3.5.1. □

[8] Actually, proving the Bezout theorem makes for a nice exercise in strong induction. (Hint: $\gcd(a,b) = \gcd(b,a) = \gcd(a,b-a)$.)

This solution is short and slick, but one thing might be missing: symmetry. This is, of course, a "first-world problem" (there is nothing wrong with a non-symmetric solution), but it is a bit jarring to see the construction of x being "biased towards p" while the conditions that it is meant to satisfy are symmetric. And indeed, there is an even nicer, symmetric solution around, although this one might be harder to come up with:

Second solution to Exercise 3.5.1. Theorem 3.5.2 (applied to p and q instead of a and n) yields that there exists some $p' \in \mathbb{Z}$ such that $pp' \equiv 1 \bmod q$. Theorem 3.5.2 (applied to q and p instead of a and n) yields that there exists some $q' \in \mathbb{Z}$ such that $qq' \equiv 1 \bmod p$. Consider these integers p' and q'. Now, set $x = pp'b + qq'a$. Then,

$$x = \underbrace{p}_{\equiv 0 \bmod p} p'b + \underbrace{qq'}_{\equiv 1 \bmod p} a \equiv 0p'b + 1a = a \bmod p$$

and similarly $x \equiv b \bmod q$. So we have found our x, and rather explicitly in fact. □

□

Here is another application of modular inverses:

Exercise 3.5.2. Let p be a prime number. Let $a, b \in \mathbb{Z}$ and $k \in \{0, 1, \ldots, p-1\}$ be such that $a \equiv b \bmod p$. Prove that

$$\binom{a}{k} \equiv \binom{b}{k} \bmod p.$$

[**Example:** If $p = 3$ and $a = 5$ and $b = 8$ and $k = 2$, then this is saying that $\binom{5}{2} \equiv \binom{8}{2} \bmod 3$. Note how this would be false for $k = 3$. In a way, this is a – somewhat limited – instance of the substitution principle for congruences holding even beyond its "reasonable" assumptions.]

Solution idea. First of all, this all wouldn't make sense if $\binom{a}{k}$ and $\binom{b}{k}$ were not integers. Fortunately, $\binom{a}{k}$ and $\binom{b}{k}$ are indeed integers (see, e.g., [Grinbe18, proof of Theorem 1.3.16] for the reason why).

The definition of binomial coefficients yields

$$\binom{a}{k} = \frac{a\,(a-1)\,(a-2)\cdots(a-k+1)}{k!} \qquad \text{and} \tag{6}$$

$$\binom{b}{k} = \frac{b\,(b-1)\,(b-2)\cdots(b-k+1)}{k!}. \tag{7}$$

Now, the substitution principle for congruences yields

$$a\,(a-1)\,(a-2)\cdots(a-k+1) \equiv b\,(b-1)\,(b-2)\cdots(b-k+1) \bmod p$$

(since $a \equiv b \bmod p$). In view of (6) and (7), we can rewrite this congruence as

$$k! \cdot \binom{a}{k} \equiv k! \cdot \binom{b}{k} \bmod p. \tag{8}$$

If we could cancel $k!$ from this congruence, we would be done.

Fortunately, we can indeed do this. Indeed, if you know some basic number theory, you will recognize that $k \in \{0, 1, \ldots, p-1\}$ entails that the integer $k!$ is coprime to p, and therefore Lemma 3.5.1 allows us to cancel $k!$ from (8). If you don't, you can get to the same conclusion by a step-by-step procedure: After all, $k!$ is the product $1 \cdot 2 \cdot \cdots \cdot k$. Thus, the congruence (8) rewrites as

$$1 \cdot 2 \cdot \cdots \cdot k \cdot \binom{a}{k} \equiv 1 \cdot 2 \cdot \cdots \cdot k \cdot \binom{b}{k} \bmod p. \tag{9}$$

However, each of the k integers $1, 2, \ldots, k$ is coprime to p (since $k \in \{0, 1, \ldots, p-1\}$ and since p is prime) and therefore can be cancelled from a congruence modulo p (by Lemma 3.5.1). Hence, we can cancel all these k integers $1, 2, \ldots, k$ from (9), one after the other. At the end, we obtain $\binom{a}{k} \equiv \binom{b}{k} \bmod p$, so the exercise is solved. □

3.6. Class problems

The following problems are to be discussed during class.

Exercise 3.6.1. Prove that there exist no two rational numbers a and b such that $a^2 + b^2 = 3$.

Exercise 3.6.2. Let $k \in \mathbb{N}$, and let m be a positive integer. Define a sequence $(c_0, c_1, c_2, \ldots)$ of integers by setting

$$c_n = \binom{n}{k} \% m \qquad \text{for each } n \in \mathbb{N}.$$

Prove that this sequence is purely periodic.

[**Example:** If $k = 2$ and $m = 2$, then this sequence is

$$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, \ldots),$$

which is purely periodic with a period of 4 (the entries $0, 0, 1, 1$ repeat endlessly). Note that this period is larger than m, which illustrates that the substitution principle for congruences does not apply to polynomials with non-integer coefficients: For instance, we have $1 \equiv 3 \bmod 2$, but $\binom{1}{2} \not\equiv \binom{3}{2} \bmod 2$.]

Exercise 3.6.3. Prove that there exist infinitely many primes that are congruent to 3 modulo 4.

Exercise 3.6.4. Let p be a prime.

(a) Prove that $p \mid \binom{p}{k}$ for each $k \in \{1, 2, \ldots, p-1\}$.

(b) Prove that $(a+b)^p \equiv a^p + b^p \bmod p$ for any integers a and b.

(c) Prove that $a^p \equiv a \bmod p$ for any integer a.

(d) Prove that $a^{p-1} \equiv 1 \bmod p$ for any integer a that is not divisible by p.

Parts **(c)** and **(d)** of Exercise 3.6.4 are known as *Fermat's Little Theorem*.

Exercise 3.6.5. Let p be a prime. Prove that there exists a positive integer n such that $p \mid 2^n + 3^n + 6^n - 1$.

3.7. Homework exercises

Solve 3 of the 6 exercises below and upload your solutions on gradescope by October 15.

Exercise 3.7.1. Let p be a prime. Let $k \in \mathbb{N}$.

(a) Prove that

$$\binom{k}{p-1} \equiv \begin{cases} 1, & \text{if } k \equiv -1 \bmod p; \\ 0, & \text{if } k \not\equiv -1 \bmod p \end{cases} \bmod p.$$

(b) Prove that

$$\binom{k}{p} \equiv \left\lfloor \frac{k}{p} \right\rfloor \bmod p.$$

Exercise 3.7.2. A polynomial $p(x)$ with rational coefficients is called *integer-valued* if it has the property that $p(a) \in \mathbb{Z}$ for each $a \in \mathbb{Z}$.

An integer-valued polynomial $p(x)$ is called *congruence-preserving* if it has the following additional property: If n, a, b are three integers satisfying $a \equiv b \bmod n$, then $p(a) \equiv p(b) \bmod n$.

The substitution principle for congruences yields that every polynomial with integer coefficients is congruence-preserving.

On the other hand, the polynomial $p(x) = \dfrac{x(x-1)}{2} = \binom{x}{2}$ is integer-valued but not congruence-preserving (because $1 \equiv 3 \bmod 2$ but $p(1) \not\equiv p(3) \bmod 2$).

Prove that the polynomial

$$p(x) = \frac{x^2\left(x^2-1\right)}{2} = \binom{x^2}{2}$$

is integer-valued and congruence-preserving (despite not having integer coefficients). Thus, all inclusions in

$$\begin{aligned}&\{\text{polynomials with integer coefficients}\}\\ &\subseteq \{\text{congruence-preserving integer-valued polynomials}\}\\ &\subseteq \{\text{integer-valued polynomials}\}\end{aligned}$$

are strict.

Exercise 3.7.3. Let m and n be two coprime positive integers. Prove that

$$\sum_{k=0}^{m-1} \left\lfloor \frac{kn}{m} \right\rfloor = \frac{(m-1)(n-1)}{2}.$$

Exercise 3.7.4. Let $P(x)$ and $(s_0, s_1, s_2, \ldots)$ be as in Exercise 3.4.1. Prove that

$$\gcd(s_a, s_b) = \left| s_{\gcd(a,b)} \right| \qquad \text{for any } a, b \in \mathbb{N}.$$

[**Hint:** Show that $\gcd(s_a, s_b) = \gcd(s_a, s_{b-a})$ whenever $a \leq b$; then argue by strong induction as in the proof of the Bezout theorem ([Grinbe20, proof of Theorem 3.4.5]).]

Exercise 3.7.5. Let p be a prime such that $p \equiv 3 \bmod 4$.

(a) Prove that there exists no $c \in \mathbb{Z}$ such that $c^2 \equiv -1 \bmod p$.

(b) Prove that if $a, b \in \mathbb{Z}$ are two integers satisfying $a^2 + b^2 \equiv 0 \bmod p$, then a and b are multiples of p.

(c) Prove that there exist no two rational numbers a and b such that $a^2 + b^2 = p$.

[**Hint:** For part **(a)**, apply Exercise 3.6.4 **(d)** and note that $(p-1)/2$ is odd. For part **(b)**, use modular inverses modulo p. Note that part **(c)** generalizes Exercise 3.6.1.]

Exercise 3.7.6. Prove that there exist infinitely many primes that are congruent to 1 modulo 4.

[**Hint:** You can use Exercise 3.7.5 **(a)**.]

References

[Grinbe18] Darij Grinberg, *Enumerative Combinatorics (Drexel Fall 2019 Math 222 notes)*, 18 September 2020.
`http://www.cip.ifi.lmu.de/~grinberg/t/19fco/n/n.pdf`

[Grinbe19] Darij Grinberg, *Introduction to Modern Algebra (UMN Spring 2019 Math 4281 notes)*, 1 October 2020.
http://www.cip.ifi.lmu.de/~grinberg/t/19s/notes.pdf

[Grinbe20] Darij Grinberg, *Math 235: Mathematical Problem Solving*, 10 August 2021.
https://www.cip.ifi.lmu.de/~grinberg/t/20f/mps.pdf