Melbourne High School
Maths Extension Group 2023
Term 1 Week 10 Handout

§1. Problems relating to combinatorial games

1. A pile of a stones is given. Two players play the following game: each of them in turns takes 1,2 or 3 stones. The player who takes the last stone wins. Determine, in terms of a, who has a winning strategy.

2. In the game *DoubleChess*, the rules of chess are changed so that White and Black alternately make two legal moves at a time. Show that Black doesn't have a winning strategy

3. Two players start with the number 1 and take turns to multiply it by an integer from 2 to 9. The winner is the first player to obtain a number greater than or equal to 1000. Which player has a winning strategy?

4. All cells of a 4×4 table are painted white. In turn two players paint a white cell black. If a player makes a move, after which there is a black square 2×2, the player loses. Who has a winning strategy?

5. Two players in turn write S or O in an empty cell of a 1×2000 table. The first player who produces three consecutive boxes that spell SOS wins. If all boxes are filled without producing SOS then the game is a draw. Prove that the second player has a winning strategy.

§2. Modular arithmetic and congruences

§2.1 Theory and notation

Our previous exploration of Euclid's algorithm has left us perfectly poised on the precipice of the most important theorem in elementary number theory, the Fundamental Theorem of Arithmetic. However, to increase the suspense, we shall delay our study of this theorem until next term. For now, we settle for another core pillar of number theory: modular arithmetic and congruence.

Think of modular arithmetic as cyclic counting, or a system of doing arithmetic in which numbers "wrap" around at a certain value. For example, when we consider the hour of the day on a twelve-hour clock, 13 is the same as 1, 14 is the same as 2, 15 is the same as 3, and so on. In this case the hours wrap around when they get to the number 12. The power of this lies in how we can take an infinity (the positive integers) and reduce it to a finite set of 12 numbers. To illustrate, suppose we start at midnight and add 147 hours. To find the hour of the day at that time, we only need to know how much bigger 147 is than a multiple of 12, because the hours reset every 12 hours. We see that 147 is 3 more than a multiple of 12, so we are at 3 o'clock. Note how this works for an arbitrarily large hour. By subtracting a multiple of 12, we can always reduce the hour to one between 0 and 11; the 12th hour wraps around to 0. Also note how this is the same as finding the remainder after division by 12. The only possible remainders are the numbers $0, 1, 2, \ldots, 11$.

This idea of "wrapping around" is so useful it has its own notation. Given two integers a and b and a third positive integer greater than unity m called the *modulus*, we say that *a is congruent to b modulo m* if b can be obtained by subtracting from a a multiple of m. This relation is denoted

$$a \equiv b \pmod{m}.$$

Another way of saying it is that $a - b$ is a multiple of m. We call a and b *residues* of each other.

The preceding algebraic definition is not intuitive. A more intuitive way to think about it is if a and b are congruent modulo m, then a and b are essentially the same number when viewed from the perspective of divisibility by m; that is, they leave the same remainder when divided by m. That remainder is always a number between 0 and $m - 1$ inclusive, and is called the *least residue* of a and b. Relative to a modulus m, every number is congruent to one number in the set $\{0, 1, 2, \ldots, m-1\}$. This set is called a *complete set of residues*. Any set of m elements in which all elements are incongruent to one another is also called a complete set of residues. For example, relative to the modulus 5, the set $\{-2, -1, 0, 1, 2\}$ is a complete set of residues. Every number is congruent to one of those numbers modulo 5.

The definition of congruence extends naturally to negative integers. For example, $2 \equiv -5 \pmod{7}$ because $2 - (-5)$ is divisible by 7. The main algebraic picture to keep in mind is that of $a - b$ being divisible by m if $a \equiv b \pmod{m}$. This relation can be written

$$a - b = mk$$

for some integer k. Rearranging yields

$$a = mk + b.$$

Recognise that this is Euclidean division of a and m; this proves there exists some $b = b'$ such that $0 \leq b' \leq m - 1$, and hence any number a is congruent to a number in that range, as already mentioned.

The true power of congruence reveals itself when we being treating the congruence symbol $\equiv$ like an equals sign. Here are some of the basic properties of congruences. Assuming that $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$, then:

- $a + b \equiv a' + b' \pmod{m}$;
- $a - b \equiv a' - b' \pmod{m}$;
- $ab \equiv a'b' \pmod{m}$;
- $ka \equiv ka' \pmod{m}$ for any integer k (this is a special case of the preceding property).

These are fairly simple to prove using the algebraic definition of congruence.

The preceding properties show that congruences are compatible with equations in at least addition, subtraction, and multiplication. We can deduce from this that congruences are also compatible with polynomial evaluation, as long as the polynomial has integer coefficients. For example, if $a \equiv 1 \pmod{4}$, then

$$\begin{aligned} a^2 + 7a + 5 &\equiv 1^2 + 7 + 5 \pmod{4} \\ &\equiv 13 \pmod{4} \\ &\equiv 1 \pmod{4} \end{aligned}$$

Even though the only thing we know about a is that it is 1 more than a multiple of 4, we can tell that $a^2 + 7a + 5$ will also be 1 more than a multiple of 4, regardless of what a actually is. More generally, if $P(x)$ is a polynomial with integer coefficients, then

$$P(a) \equiv P(b) \pmod{m}$$

if $a \equiv b \pmod{m}$.

We have seen that addition, subtraction, and multiplication work with congruences the same way they work with equations. How about division?

A common factor can only be cancelled from both sides of a congruence if it is coprime with the modulus. For example, in the congruence $42 \equiv 12 \pmod{10}$, the factor 3 may be cancelled from both sides to yield the correct congruence $14 \equiv 4 \pmod{10}$ because 3 is coprime with 10. However, dividing both sides by 6 yields the incorrect congruence $7 \equiv 2 \pmod{10}$.

To demonstrate why this is the case, suppose $ax \equiv ay \pmod{m}$. Then, by definition, $a(x-y)$ is divisible by m. By cancelling a from both sides, we assert that $x-y$ is divisible by m, but this might not be the case, because m could divide a and not $(x-y)$. The only way to ensure that m divides $(x-y)$ and not a is if a and m are coprime; hence cancelling a factor from both sides of a congruence is valid only if that factor is relatively prime with the modulus.

What if the two sides of a congruence don't share a common factor? In other words, are fractions allowed in congruences? The answer to this question is slightly more complicated, relating to solving linear congruences. This will be explored in the next section.

§2.2 Exercises

1. Prove the following two properties of congruences (symmetry and transitivity).
   - If $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$.
   - If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$.
2. Use modular arithmetic to prove the divisibility test for 3 and 9.
3. Use modular arithmetic to prove the divisibility test for 11. (That is, a number written in decimal notation is divisible by 11 if the alternating sum of its digits is divisible by 11.)
4. Show that if $a \equiv b \pmod{2m}$, then $a^2 \equiv b^2 \pmod{4m}$. If you can, prove the more general statement that if $a \equiv b \pmod{km}$, then $a^k \equiv b^k \pmod{k^2 m}$.

§2.3 Linear congruences

As with normal equations, we can solve congruences. The simplest type is the linear congruence

$$ax \equiv b \pmod{m}.$$

The above equation is soluble for x when a and m are relatively prime. To see why, let's go back to the definition of congruence. If $ax \equiv b \pmod{m}$, then $ax-b$ is divisible by m. Hence let $ax-b = my$ for some integer y. Rearrange to get the equation $ax-my = b$. This is the linear equation we considered when discussing the Euclidean algorithm, and we know that it always has natural number solutions when a and m are coprime. Hence our linear congruence has a solution in x too, since we just need to solve the linear equation and reduce the value of x to its least residue.

To illustrate, let us solve the congruence

$$7x \equiv 5 \pmod{13}.$$

Since 7 and 13 are prime, they are coprime, so this equation has a solution. We use the definition of congruence and let $7x - 5 = 13y$ for some integer y; rearranging we get $7x - 13y = 5$. To solve this equation, we first solve the equation $7x' - 13y' = 1$ using the Euclidean algorithm, which gives us the solution $(x', y') = (2, 1)$. Multiply x' and y' by 5 to get the solution to the desired equation: $(x, y) = (10, 5)$. Since 10 cannot be reduced further modulo 13, we have solved the congruence by obtaining the solution $x \equiv 10 \pmod{13}$.

There are two things to note in our preceding example. Firstly, by finding one solution, we have actually found infinitely many solutions, because any number congruent to 10 modulo 13 is also a solution. However, in finding solutions to congruences, we consider the number of solutions to be the number of incongruent solutions; hence this equation has only one solution. Secondly, solving the congruence gives us an answer as to what the fraction $5/7$ means modulo 13; it is congruent to 10. In general, fractions are allowed in congruences as long as the denominator is coprime with the modulus because they are just symbolic of a solution to a linear congruence. The fraction b/a relative to the modulus m represents the solution to the linear equation $ax \equiv b \pmod{m}$, and hence only exists when a and m are coprime because otherwise such a solution would not exist, as we have shown. An interesting parallel between congruences and equations is evident when we consider prime moduli. If m is prime, the only condition is that b is not a multiple of m, as that guarantees b and m are coprime. But that just means $b \not\equiv 0 \pmod{m}$, which is analogous to how dividing both sides of an equation by 0 is not allowed.

Now it is time to generalise. Consider the equation

$$ax \equiv b \pmod{m} \tag{1}$$

where a and m are not necessarily coprime. Let $g = \gcd(a, m)$. If $g = 1$ we have the case described above. So what happens if $g \neq 1$?

As is often the case in mathematics, we start with the definitions. Performing a similar algebraic manipulation as before, we get the equation

$$ax - my = b \tag{2}$$

for some integer y. We know the LHS will always be a multiple of g, and therefore the equation only

has positive integer solutions when b is a multiple of g. This immediately answers our question as to when the congruence (1) has any solutions.

Now the goal is to find how many solutions there are and what they are. As before, the next step is to solve equation (2) for x and y. If we let the solution to $ax' - my' = g$ be $(x', y') = (u, v)$, we obtain a solution to equation (2) by multiplying by b/g, which we know to be an integer because g divides b. Hence the solution we get for equation (2) is

$$(x, y) = \left(\frac{ub}{g}, \frac{vb}{g}\right).$$

Having found one solution, $x \equiv ub/g \pmod{m}$, the natural question is whether there are any more. A key technique that we use here is to assume another solution exists; if we prove that this second solution is congruent to the first, then there are no more solutions. Otherwise, we have found a way of generating all other solutions.

Let's label our first solution x_1 and suppose there is another solution x_2. By definition, $ax_2 \equiv b \pmod{m}$. Using the properties of transitivity and symmetry, we deduce that $ax_2 \equiv ax_1 \pmod{m}$. Now we use the definition of congruence to find that $a(x_2 - x_1)$ is divisible by m, which further implies that $(a/g)(x_2 - x_1)$ is divisible by m/g.

Here is where we use the definition of g. Since $g = \gcd(a, m)$, then a/g and m/g cannot share any common factors, since otherwise we would derive a contradiction in the definition of g. Hence the number m/g cannot divide a/g; it must divide $x_2 - x_1$. From this we conclude there is some integer k for which

$$x_2 - x_1 = k \cdot \frac{m}{g}.$$

Rearranging for our new solution x_2, we get

$$x_2 = x_1 + k \cdot \frac{m}{g}.$$

We have therefore found another solution to our original congruence:

$$x_2 \equiv x_1 + k \cdot \frac{m}{g} \pmod{m}.$$

Since m/g is not congruent to 0 modulo m, the two solutions x_2 and x_1 will be incongruent as long as k takes one of the values $1, 2, \ldots, g-1$. We need not consider $k \geq g$ because those values of k do not yield a new solution. For example, if $k = g + 1$, we get $x_2 = x_1 + m + g/m$, which is the same solution modulo m as if we took $k = 1$.

We get all solutions to the congruence (1) by running k through the values $0, 1, 2, \ldots, g-1$; hence there are exactly g incongruent solutions.

The result of this rather arduous journey is a most exciting theorem about the solubility of linear congruences. Here is a concise summary. If a and b are integers, m is a positive integer greater than 1, and $g = \gcd(a, m)$, the congruence

$$ax \equiv b \pmod{m}$$

has exactly g incongruent solutions. To find these solutions, first solve the equation $ax - my = g$. Let the solution to this equation be $(x, y) = (u, v)$. Then all g solutions can be found by computing

$$x_k = \frac{bu}{g} + k \cdot \frac{m}{g}$$

for $k = 0, 1, 2 \ldots, g-1$.

Linear congruences are the tip of the iceberg when it comes to solving congruences. In the future we shall consider congruences of higher degree, in which there are many interesting theorems. In particular, the study of quadratic congruences has led to a theorem that Gauss considered the "golden theorem" and is no doubt one of the most beautiful theorems in all of mathematics. But more on this exciting topic at another time.

§2.4 Problems

1. I have invited 118 people to my party, but unfortunately 13 of them can't make it. Therefore at the end of my party, after everyone eats the same number of cupcakes, I would like 13 cupcakes left for them. However, each person at my party can eat a maximum of 50 cupcakes; anyone who eats more than that will become seriously ill, and that's not good. If my cupcake vendor only sells in batches of 97 cupcakes, am I able to satisfy the needs of my party?

2. Given an integer a and a modulus m, the *multiplicative inverse of a modulo m* is another integer denoted by a^{-1} such that $aa^{-1} \equiv 1 \pmod{m}$. Show that if a and m are coprime, then there always exists a multiplicative inverse of a modulo m.

3. Hence, or otherwise, prove that

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

   for any prime p. (This is known as *Wilson's Theorem.*)

4. Let a and m be coprime integers with $m > 1$. Show that if each element of the set

   $$\{0a, a, 2a, \ldots, (m-1)a\}$$

   is reduced modulo m, the resulting set is equal to the set

   $$\{0, 1, 2, \ldots, m-1\}.$$

   Hence find a second proof that the equation $ax \equiv b \pmod{m}$ is soluble when $\gcd(a, b) = 1$.