Number Theory Homework.

1. Congurences, modular arthmetic, and solving linear congruences.

1.1. **Definition and some basic results and examples.** The following definition was fist given by Carl Friedrich Gauss in his book *Disquisitiones Arithmeticae* which was published in 1801. It is has proven to simplify many computations and proofs in number theory and elsewhere.

Definition 1. Let n be a positive integer. Then for $a, b \in \mathbb{Z}$ we write

$$a \equiv b \mod n$$

to mean

$$n \mid (b - a).$$

In we say that a ***is congruent to*** b ***modulo*** n, or just a ***congruent to*** b ***mod*** n**.**

Proposition 2. *The following hold for all* $a, b, c \in \mathbb{Z}$ *and any positive integer* n*.*
(a) $a \equiv a \mod n$
(b) $a \equiv b \mod n$ *implies* $b \equiv a \mod n$
(c) $a \equiv b \mod n$ *and* $b \equiv c \mod n$ *implies* $a \equiv c \mod d$
(Using terminology you many have seen in other classes, this is saying that $\equiv \mod n$ *is an* ***equivalence relation****.)*

Problem 1. Prove this. *Hint:* These all follow form basic properties of divisibility. For example if $a \equiv b \mod n$ and $b \equiv c \mod n$, then $n \mid (b - a)$ and $n \mid (c - a)$. But if n divides two numbers it divides their sum. Thus $n \mid (c - a) = (c - b) + (b - a)$. $\square$

We now show that congruence mod n plays well with the basic arithmetic operations.

Proposition 3. *If*

$$a \equiv b \mod n \qquad \text{and} \qquad c \equiv d \mod n$$

Then

$$a + c \equiv b + d \mod n, \qquad a - c \equiv b - d \mod n, \qquad ac \equiv bd \mod n.$$

Problem 2. Prove this. *Hint:* The assumption of the hypothesis can be stated as saying that there are q_1 and q_2 such that $(b - a) = q_1 n$ and $(d - c) = q_2 n$. Then $(b + d) - (a + c) = (b - a) + (d - c) = (q_1 + q_2)n$. Slightly trickier is the result for products, where we have to use the trick of adding and subtracting a term:

$$bd - ac = bd - ad + ad - ac = (b - a)d + a(d - c)$$

and now show that an n can be factored out of this. $\square$

This can be extended to more than sums and products of just two terms.

Proposition 4. *If*

$$a_j \equiv b_j \mod n \qquad \textit{for} \qquad j = 1, 2, \ldots, k$$

then

$$(a_1 + a_2 + \cdots + a_k) \equiv (b_1 + b_2 + \cdots + b_k) \mod n$$

and

$$a_1 a_2 \cdots a_k \equiv b_1 b_2 \cdots b_k \mod n.$$

In particular for any nonnegative integer k

$$a \equiv b \mod n \qquad \Longrightarrow \qquad a^k \equiv b^k \mod n.$$

Proof. This is just an easy induction on k. □

Proposition 5. *If $f(x) = c_k x^k + c_{k-1}x^{k-1} + \cdots c_1 x + c_0$ is a polynomial with integer coefficients, then*

$$a \equiv b \mod n \qquad \Longrightarrow \qquad f(a) \equiv f(b) \mod n.$$

Problem 3. Prove this. *Hint:* One way, and maybe the most natural, to do this is just by repeated use of the last couple of propositions. But it is not hard to give an nice proof based on induction on $k = \deg f(x)$. Write

$$f(x) = x(c_k x^{k-1} + c_{k-2}x^{k-1} + \cdots + c_2 x + c_1) + c_0 = xg(x) + c_0.$$

Then $g(x) = c_k x^{k-1} + c_{k-2}x^{k-1} + \cdots + c_2 x + c_1$ is a polynomial with $\deg g(x) = k - 1 = \deg f(x) - 1$. Thus if you have the correct induction hypothesis you will have that $g(a) \equiv g(b) \mod n$. □

The following shows that two numbers are congruent modulo n if any only if they have the same remainder with divided by n.

Theorem 6. *Let n be a positive integer and a_1 and a_2 any integers. Divide n into a_1 and a_2 to get quotients and remainders*

$$a_1 = q_1 n + r_1, \qquad a_2 = q_2 n + r_2 \qquad \textit{with} \qquad 0 \le r_1 < n, \quad 0 \le r_2 < n.$$

Then

$$a_1 \equiv a_2 \mod n \qquad \Longleftrightarrow \qquad r_1 = r_2.$$

Problem 4. Prove this. *Hint:* One way to start is $a_2 - a_1 = (q_2 - q_1)n + (r_2 - r_1)$. Show $0 \le |r_2 - r_1| < n$ and therefore $n \mid (r_2 - r_1)$ if and only if $r_1 = r_2$. □

We can now do "arithmetic modulo n" by adding and multiplying integers and then "reducing mod n", that is replacing the result by the remainder when divided by n. For example working modulo 6 we have

$$2 + 3 = 5, \qquad 2 + 4 = 6 \equiv 0 \mod 6, \qquad 5 \cdot 4 = 20 \equiv 2 \mod 6.$$

The full addition and multiplication tables modulo 6 and 7 are

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

·	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

The addition and multiplication tables modulo 6.

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

·	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

The addition and multiplication tables modulo 7.

Problem 5. If you have never constructed addition and multiplication tables as these make the tables for the integers modulo 4 and the integers modulo 5. □

To give an immediate application of the usefulness of these ideas to give an easy explanation of the method of "casting out nines". What this says is that for any positive decimal integer, for example $n = 986{,}529$, the sum of its digits, in our case $S = 9+8+6+5+2+9 = 39$, have the same remainder when divided by 9. In our example

$$986{,}529 = 109{,}614 \cdot 9 + 3 \qquad \text{and} \qquad 39 = 4 \cdot 9 + 3$$

so in both cases the remainder is 3. The reason this works is that

$$10 \equiv 1 \mod 9.$$

Taking powers

$$10^k \equiv 1 \mod 9.$$

Therefore

$$\begin{aligned} 986{,}529 &= 9 \cdot 10^5 + 8 \cdot 10^4 + 6 \cdot 10^3 + 5 \cdot 10^2 + 2 \cdot 10 + 9 \\ &\equiv 9 \cdot 1 + 8 \cdot 1 + 6 \cdot 1 + 5 \cdot 1 + 2 \cdot 1 + 9 \qquad \mod 9 \\ &= 9 + 8 + 6 + 5 + 2 + 9 \\ &= 39 \end{aligned}$$

This shows

$$986{,}529 \equiv 9 + 8 + 6 + 5 + 2 + 9 \mod 9$$

and thus these numbers have the same remainder when divided by 9.

Problem 6. (a) Based on this example give a precise statement to the fact that a positive integer and the sum of its digits have the same remainder when divided by 9 and prove it. Show this implies that an integer is divisible by 9 if and only of the sum of its digits is divisible by 9.

(b) We also have that $10 \equiv 1 \mod 3$. Use this to state and prove a rule for "casting out threes" and in particular show an integer is divisible by 3 if and only it the sum of its digits is divisible by 3. □

Until recently, when calculators made having to do such checks pointless, casting out nines was used as a check on doing arithmetic calculations. For example in the addition problem:

		Digit sum		Sum mod 9
	8643	8+6+4+3=21		3
	9634	9+6+3+4=22		4
+	5326	5+3+2+6=16	+	7
	23603			$14 \equiv 5 \mod 9$

Casting the nines out of 23603 (that is take the digit sum and reduce modulo 9) gives $2 + 3 + 6 + 0 + 3 = 14 \equiv 5 \mod 9$. That we got 5 both times gives a check that the calculation is correct. This method does not guarantee the answer is right, but does give a check that let people catch enough errors that it was worth doing. The method also works to give checks on substation, multiplication, and division problems.

A related idea comes form the fact $10 \equiv -1 \mod 11$. Thus

$$(10)^k \equiv (-1)^k \mod 11.$$

This can be used as follows:

$$\begin{aligned} 82{,}752 &= 8(10)^4 + 2(10)^3 + 7(10)^2 + 5(10) + 2 \\ &\equiv 8(-1)^4 + 2(-1)^3 + 7(-1)^2 + 5(-1) + 2 \mod 11 \\ &= 8 - 2 + 7 - 5 + 2 \\ &= 10 \end{aligned}$$

and therefore $82{,}752 \equiv 8 - 2 + 7 - 5 + 2 \equiv 10 \mod 11$ and so if 82,752 is divided by 11 the remainder is 10.

Problem 7. Based on this example make precise the statement that a positive integer and the alternating sum of its digits have the same remainder when divided by 11 and prove the result. (Be careful, there is more than one way to define the alternate sum of the digits: i.e. when $n = 1{,}435$ do we want $1 - 4 + 3 - 5$ or $-1 + 4 - 3 + 5$?) Thus an integer is divisible by 11 if and only if the alternating sum of its digits is divisible by 11. □

Hopefully the last problems were straightforward. To get a feel for how much modular arithmetic simplifies arguments about divisibility and remainders, it is worth spending some time and finding your own proof that the method of casting out nines works but that does not use arithmetic mod

9.[1] (Casting out nines was known long before Gauss, so modular arithmetic is not required to prove it.)

Before going on we pause for an aside to discuss how to compute $a^k \mod n$ for a large value of k. Later we will find some better methods in the case $\gcd(a, n) = 1$, and so may not be that important for the mathematical theory, but the trick is pretty and is definitely used by people doing computational number theory and to some extent by computer scientists. To start with an example let's find the remainder when 7^{83} is divided by 13. You definitely do not want to compute[2] 7^{83}, but this can be avoided by repeatedly squaring and reducing modulo 13. The idea is that it is easy to compute powers of the form $7^{2^k} \mod 13$ by repeated squaring:

$$\begin{aligned}
7^2 &= 49 \equiv 10 \mod 13\\
7^4 &= (7^2)^2 \equiv 10^2 \equiv 9 \mod 13\\
7^8 &= (7^4)^2 \equiv 9^2 \equiv 3 \mod 13\\
7^{16} &= (7^8)^2 \equiv 3^2 \equiv 9 \mod 13\\
7^{32} &= (7^{16})^2 \equiv 9^2 \equiv 3 \mod 13\\
7^{64} &= (7^{32})^2 \equiv 3^2 \equiv 9 \mod 13
\end{aligned}$$

Back to 7^{83}, note

$$83 = 64 + 16 + 2 + 1$$

and therefore

$$\begin{aligned}
7^{83} &= 7^{64} \cdot 7^{16} \cdot 7^2 \cdot 7\\
&\equiv 9 \cdot 9 \cdot 10 \cdot 7 && \mod 13\\
&= 81 \cdot 70\\
&\equiv 3 \cdot 5 && \mod 13\\
&\equiv 2 && \mod 13
\end{aligned}$$

Thus the remainder when 7^{83} is divided by 13 is 2.

Problem 8. Use this method to compute (a) the remainder when 10^{45} is divided by 7, (b) the remainder when 37^{39} is divided by 17 (*Hint:* As a first step note $37 \equiv 3 \mod 17$), (c) the remainder when 10^{70} is divided by 24. □

Definition 7. Let n be a positive integer. Two integers a and b are in ***the same residue class*** modulo n iff $a \equiv b \mod n$. A set of n integers $r_1, r_2, \ldots, r_n$ is a ***complete set of residues*** modulo n iff each integer a is in the residue class of exactly one of the numbers $r_1, r_2, \ldots, r_n$. □

---

[1] The Wikipedia article *Casting out nines* has some elementary proofs.

[2] Just in case you really felt the need to know:
7^{83} = 13,903,921,949,820,524,683,398,592,075,392,719,113,700,201,232,097,144,724,944,011,875,664,343.

The following is direct consequence of Theorem 6.

Proposition 8. *For any postive integer n the numbers $0, 1, \ldots, n-1$ are a complete set of residues modulo n.*

Problem 9. Prove this. *Hint:* It $a \in \mathbb{Z}$ use the division algorithm to divide a by n to get $a = qn + r$ with $0 \le r < n$. That is r is one of the numbers $0, 1, \ldots, n-1$ and also $a \equiv r \mod n$. □

Problem 10. (a) Is $1, 2, 3$ a complete set of residues modulo 3?
(b) Is $0, 1, 2$ a complete set of residues modulo 3?
(c) Is $-1, 0, 1$ a complete set of residues modulo 3?
(d) Is $-1, 0, 5$ a complete set of residues modulo 3?
(e) Is $0, 3, 3^2, 3^3, 3^4, 3^5, 3^6$ a complete set of residues modulo 7?
(f) Is $0, 2, 2^2, 2^3, 2^4, 2^5, 2^6$ a complete set of residues modulo 7? □

Proposition 9. *Let n be a positive integer and $r_1, r_2, \ldots, r_n$ integers such that*

$$i \neq j \qquad \Longrightarrow \qquad r_i \not\equiv r_j \mod n$$

then $r_1, r_2, \ldots, r_n$ is a complete set of residues modulo n. (Note the hypothesis could also be stated as $r_i \equiv r_j \mod n \implies i = j$.)

Proof. Use the division algorithm to divide n into r_j to get

$$r_j = q_j n + s_j \qquad \text{and} \qquad s_j \in \{0, 1, \ldots, n-1\}.$$

This implies $r_j \equiv s_j \mod n$. Therefore if $i \neq j$, then $s_i \neq s_j$ for if $s_i = s_j$, then

$$\begin{aligned} r_i &\equiv s_i \mod n \\ &= s_j \\ &\equiv r_j \mod n \end{aligned}$$

which contradicts our assumption that $r_i \not\equiv r_j$ for $i \neq j$. Therefore $s_1, s_2, \ldots, s_n$ are distinct elements of $\{0, 1, \ldots, n-1\}$. As the set $\{0, 1, \ldots, n-1\}$ has exactly n elements, it follows that $s_1, s_2, \ldots, s_n$ and just the numbers $0, 1, \ldots, n-1$ listed in some order. Therefore if $a \in \mathbb{Z}$ we divide n into a to get

$$a = qn + r$$

where $0 \le r < n$. Then $r = s_i$ for some i and thus

$$\begin{aligned} a &\equiv r \mod n \\ &\equiv s_i \mod n \\ &\equiv r_i \mod n. \end{aligned}$$

Thus each $a \in \mathbb{Z}$ is in the residue class modulo n of at least one of the r_i's. But as $r_i \not\equiv r_j$ for $i \neq j$ this implies that a is in the residue class of exactly one of the r_i's. □

The following uses the last result to give an example of a complete set of residues that will be useful to us later.

Proposition 10. *If n is a positive integer and a is an integer with* $\gcd(a, n) = 0$ *then the set* $0, a, 2a, 3a, \ldots, (n-1)a$ *(that is the list of numbers ka for $k = 0, 1, \ldots, n-1$) is a complete set of residues modulo n.*

For example, when $n = 12$ and $a = 5$, this implies

$$0,\ 5,\ 10,\ 15,\ 20,\ 25,\ 30,\ 35,\ 40,\ 45,\ 50,\ 55$$

is a complete set of residues modulo 12.

Problem 11. Prove Proposition 10. *Hint:* Let $r_j = ja$ for $j = 0, 1, \ldots, n-1$. This is a list of n integers. Since there are n of them, by Proposition 9 it is enough to show $r_i \equiv r_j \mod n$ implies $i = j$. That is

$$ia \equiv ja \mod n \qquad \Longrightarrow \qquad i = j.$$

If $ia \equiv ja \mod n$, then $n \mid a(i-j)$. Now use $\gcd(a, n) = 1$ to conclude $n \mid (i-j)$. But $0 \leq i, j < n$ which implies $|i-j| < n$. $\square$

1.2. **Solving a single linear congruence.** Given integers a and b and a positive integer n will find all solutions to

$$ax \equiv b \mod n.$$

when they exist. There are several possible cases. First there are congruences such as

$$5x \equiv 4 \mod 6.$$

With a little trial and error we see $x = 2$ is a solution. But that so are $x = 8$, $x = -2$, and in general $x = 2 + 6t$ where t is any integer and moreover this gives all solutions. As all these solutions are $\equiv 2 \mod 6$ we will say that in this case the congruence has a unique solution.

Next we can have congruences such as

$$2x \equiv 4 \mod 6$$

where both $x = 2$, and $x = 5$ are solutions, but $2 \not\equiv 4 \mod 6$. So in this case the congruence has solutions, but they are not unique modulo $n = 6$. We will see that in this case all solutions are of the form $x = 2 + 6t$, or $x = 5 + 6t$. Reduce modulo 6 we this gives two solutions, so we that the congruence has two solutions (modulo 6).

Finally there are congruences such as

$$2x \equiv 3 \mod 6$$

that have no solutions.

The main idea in understanding this question is to note that $ax \equiv b \mod n$ is to convert it to a linear Diophantine equation.

$$\begin{aligned} x \text{ is a solution to } ax \equiv b \mod n &\iff n \mid (b - ax) \\ &\iff \text{there is } y \in \mathbb{Z} \text{ with } (b - ax) = ny \\ &\iff ax + ny = b \text{ has a solution.} \end{aligned}$$

To be more precise.

Proposition 11. *(a) Let* $(x, y) = (x_1, y_1)$ *be a solution to the linear Diophantine equation* $ax + ny = b$*. Then* $x = x_1$ *is a solution to congruence* $ax \equiv b \mod n$*.*

(b) Conversely, if x_1 *is a solution to the congruence* $ax \equiv b \mod n$*, then there is a* y_1 *such that* $(x, y) = (x_1, y_1)$ *is a solution to* $ax + ny = b$*.*

Problem 12*.* Prove this. □

The last proposition basically says that to solve $ax \equiv b \mod n$, solve $ax + ny = b$ and just use the x values.

Example 12*.* As a first example let us solve

$$5x \equiv 7 \mod 13.$$

This is equivalent to solving

$$5x + 13y = 7.$$

We do the Euclidean algorithm to solve Bézout's equation.

$$\begin{aligned}(3) &= (13) - 2(5)\\ (2) &= (5) - (3)\\ (1) &= (3) - (2).\end{aligned}$$

Now back doing the usual back substitution

$$\begin{aligned}(1) &= (3) - (2) && = (3) - \big((5) - (3)\big)\\ &= -(5) + 2(3) && = -(5) + 2\big((13) - 2(5)\big)\\ &= 2(13) - 5(5).\end{aligned}$$

Therefore

$$5(-5) + 13(2) = (1).$$

Multiply by 7 to get

$$5(-35) + 12(14) = (7).$$

Thus $(x, y) = (-35, 14)$ is a particular solution to $5x + 13y = 7$. So the general solution to this equation is

$$x = -35 + 13t, \qquad y = 14 - 5t.$$

Therefore the general solution to the congruence is

$$x - 35 + 13t.$$

Note that replacing -35 by any integer of the form $-35+13k$ will give same set of solutions. Using $-35 + 3 \cdot 13 = 4$ then gives that we can write the general solution as

$$x = 4 + 13t$$

with t any integer. If we are considering solutions mod 13 the unique solution is the residue class defined by $x \equiv 4 \mod 13$ (which is the same as the residue class $x \equiv -35 \mod 13$). □

Example 13. For a second example let us solve

$$6x \equiv 4 \mod 15.$$

This leads to the Diophantine equation

$$6x + 15y = 9.$$

Going through the usual routine

$$(3) = (15) - 2(6)$$

so we are lucky and it stops after one step and we have

$$6(-2) + 15(1) = (3).$$

Multiply by 3 to get

$$6(-6) + 15(3) = (9)$$

and therefore $(x, y) = (-6, 3)$ is a particular solution to $6x + 15y = 9$. Thus the general solution is

$$x = -6 + \frac{15}{\gcd(6,15)}t = -6 + 5t, \qquad y = 3 - \frac{6}{\gcd(6,15)}t = 3 - 2t.$$

We only need the x values, so the general solution to the congruence is

$$x = -6 + 5t.$$

Unlike the last example these are not all the same mod $n = 15$. Let $t0, 1, 2 \ldots$ solutions

$$-6,\ -1,\ 4,\ 9,\ 14,\ 19$$

which starts to repeat after when we get to 9 (as $9 \equiv -6 \mod 15$, $14 \equiv -1 \mod 15$, $19 \equiv 4 \mod 15$). So $6x \equiv 4 \mod 15$ has three residue classes as solutions:

$$x \equiv 4, 9, 14 \mod 15$$

are all solutions mod 15, they are distinct mod 15, and every residue that solves the congruence solves is congruence to one of these residue classes. So in this case we say the congruence has three residue classes as solutions. Or more briefly that the congruence has 3 solutions mod 15. □

Example 14. As a last example consider

$$8x \equiv 5 \mod 12.$$

This leads to the Diophantine equation

$$8x + 12y = 5$$

which has no solution as $\gcd(8, 12) = 4 \nmid 5$. Thus the congruence has no solution. □

Theorem 15. *The linear congruence*

$$ax \equiv b \mod n$$

has solutions if and only if $\gcd(a, n) \mid b$. *If it does have a solution and* x_0 *is one solution, then the general solution is*

$$x = x_0 + \frac{n}{\gcd(a, n)} t$$

with $t \in \mathbb{Z}$. *Viewed modulo* n, *the number of solutions is* $\gcd(a, n)$ *and are the residue classes of*

$$x = x_0 + \frac{n}{\gcd(a, n)} t \qquad \textit{for} \qquad t = 0, 1, \ldots, \gcd(a, n) - 1.$$

Problem 13. Prove this. □

Problem 14. Solve the following congruences of the form $ax \equiv b \mod n$. Determine how many solutions they have mod n.

(a) $12x \equiv 5 \mod 31$.
(b) $24x \equiv 12 \mod 40$.
(c) $12x \equiv 13 \mod 40$.

1.3. **Inverses modulo n.**

Proposition 16. *Let* n *be a positive integer and* a *an integer with* $\gcd(a, n) = 1$. *Then there is an integer* b *that is the* ***multiplictive inverse of*** a ***modulo*** n *in the sense that*

$$ab \equiv 1 \mod n.$$

This inverse is unique in the sense that if b *and* b' *are both inverse mod* n *to* a, *then* $b \equiv b' \mod n$

Problem 15. Prove this in two ways. First note that it is a direct consequence of Theorem 15 as we are just solving the congruences $ax \equiv 1 \mod n$. For a second proof use $\gcd(a, n) = 1$ to find integers x and y such that $ax + ny = 1$, and this implies $ax \equiv 1 \mod n$. So $b = x$ is the required inverse modulo n. □

In finding finding the inverses modulo n, it is generally easier to use the second method from the last problem. This is because it just involves solving Bézout's equation $ax + ny = 1$ and we have become experts on that.

Example 17. Find the inverse of 31 modulo 73. First use the Euclidean algorithm

$$\begin{aligned} (11) &= (73) - 2(31) \\ (9) &= (31) - 2(11) \\ (2) &= (11) - (9) \\ (1) &= (9) - 4(2). \end{aligned}$$

Thus

$$\begin{aligned} (1) &= (9) - 4(2) & &= (9) - 4\big((11) - (9)\big) \\ &= -4(11) + 5(9) & &= -4(11) + 5\big((31) - 2(11)\big) \\ &= 5(31) - 14(11) & &= 5(31) - 14\big((73) - 2(31)\big) \\ &= -14(73) + 33(31). & & \end{aligned}$$

And, as $-14(73) \equiv 0 \mod 73$,

$$-14(73) + 33(31) = 1$$

clearly implies

$$31 \cdot 33 \equiv 1 \mod 73.$$

Thus 33 is the multiplicative inverse of 31 modulo 73. □

Problem 16. Find the following
(a) The inverse of 19 mod 23.
(b) The inverse of 45 mod 64.
(c) The inverse of 324 mod 79. □

Problem 17. Let $\hat{a}$ be the inverse of a mod n and $\hat{b}$ the inverse of b mod n. Show the product $\hat{a}\hat{b}$ is the inverse of the product ab mod n □

We can use inverses modulo n to prove the following (which also follows form Theorem 15).

Proposition 18. *If* $\gcd(a, n) = 1$, *and* $ax \equiv ay \mod n$, *then* $x \equiv y \mod n$. *That is when* $ax \equiv ay \mod n$ *and* $\gcd(a, n) = 1$, *we can cancel*

That is when $ax \equiv ay \mod n$ and $\gcd(a, n) = 1$, we can cancel a on both sides of the congruence.

Problem 18. Prove this. *Hint:* One way is to let $\widehat{a}$ be an inverse of a modulo n and multiply both sides of $ax \equiv ay \mod n$ by $\widehat{n}$. □

Problem 19. Show that the hypothesis $\gcd(a, n) = 1$ is required in Proposition 18 by giving an example where $\gcd(a, n) \neq 1$ and integers x and y such that $ax \equiv ay \mod n$ but $x \not\equiv y \mod n$. □

1.4. **Solving simultaneous linear congruences: the Chinese remainder theorem.** Consider the system

$$\begin{aligned} x &\equiv b_1 \mod n_1 \\ x &\equiv b_2 \mod n_2 \end{aligned}$$

of two linear congruences. We assume

$$\gcd(n_1, n_2) = 1$$

To find a solution to this system set

$$\begin{aligned} m_1 &= n_2 \\ m_2 &= n_1 \end{aligned}$$

and let

$$\begin{aligned}\widehat{m}_1 &= \text{an inverse of } m_2 \mod n_1\\ \widehat{m}_2 &= \text{an inverse of } m_1 \mod n_2\end{aligned}$$

and let

$$x = m_1\widehat{m}_1 b_1 + m_2\widehat{m}_2 b_2.$$

Then

$$\begin{aligned}x &= m_1\widehat{m}_1 b_1 + m_2\widehat{m}_2 b_2\\ &\equiv m_1\widehat{m}_1 b_1 + 0 && (\text{as } m_2\widehat{m}_2 \equiv 0 \mod n_1)\\ &\equiv b_1 && (\text{as } m_1\widehat{m}_1 \equiv 1 \mod n_1)\end{aligned}$$

with a similar calculation showing

$$x \equiv b_2 \mod n_2.$$

We have therefore proven the existence part of

Theorem 19 (Chinese remainder theorem for two congruences)**.** *If n_1 and n_2 are positive integers with $\gcd(n_1, n_2) = 1$, then for any integers b_1 and b_2 there is a simultaneous solution to the congruences*

$$\begin{aligned}x &\equiv b_1 \mod n_1\\ x &\equiv b_2 \mod n_2\end{aligned}$$

which can be found by the construction above. If $x = x_0$ is one solution, then the general solution is

$$x = x_0 + n_1 n_2 t$$

with $t \in \mathbb{Z}$. (Thus the solution is unique modulo n_1n_2.)

Problem 20. Prove uniqueness part of this. That it that the general solution is of the given form. *Hint:* First check that $x = x_0 + n_1n_2t$ is a solution. Now assume that x is a solution. Then $x \equiv b_1 \equiv x_0 \mod n$, which implies $n_1 \mid (x - x_0)$. Likewise $n_2 \mid (x - x_0)$. Use these facts and that $\gcd(n_1, n_2) = 1$ to show $n_1n_2 \mid (x - x_0)$. $\square$

Example 20. Solve the system

$$\begin{aligned}x &\equiv 5 \mod 8\\ x &\equiv 4 \mod 11\end{aligned}$$

In the notataion above we have

$$m_1 = 11, \qquad m_2 = 9$$

You can check

$$11(3) \equiv \mod 8, \qquad 8(7) \equiv 1 \mod 11$$

so that we can use

$$\widehat{m}_1 = 3, \qquad \widehat{m}_2 = 7.$$

Then a particular solution to our equation is

$$x_0 = m_1\widehat{m}_1 b_1 + m_2\widehat{m}_2 b_2 = 11 \cdot 3 \cdot 5 + 8 \cdot 7 \cdot 4 = 389.$$

Thus the general solution is

$$x = 389 + 8 \cdot 11t = 389 + 88t.$$

Or working $\mod 88$ we have

$$389 \equiv 37 \mod 88$$

so we could also write the general solution as

$$x = 37 + 88t.$$

(As a check note $37 \equiv 5 \mod 8$ and $37 \equiv 4 \mod 11$.) □

Problem 21. Solve the following:

(a) $x \equiv 7 \mod 13$
$x \equiv 3 \mod 21$
(b) $x \equiv 21 \mod 27$
$x \equiv -4 \mod 14$
(c) $3x \equiv 5 \mod 8$
$2x \equiv 6 \mod 15$

Hint: For (c) first find solutions to $3x \equiv 5 \mod 8$ and $2x \equiv 6 \mod 15$ to reduce the system to one of the form $x \equiv b_1 \mod 8$ and $x \equiv b_2 \mod 15$. □

It is only a bit more work to do this for three or more simultaneous congruences. Let n_1, n_2, and n_3 be positive integers with

$$\gcd(n_1, n_2) = \gcd(n_1, n_3) = \gcd(n_2, n_3) = 1.$$

Set

$$\begin{aligned} m &= n_1 n_2 n_3 \\ m_1 &= n_2 n_3 = \frac{m}{n_1} \\ m_2 &= n_1 n_3 = \frac{m}{n_2} \\ m_3 &= n_1 n_2 = \frac{m}{n_3} \end{aligned}$$

Then

$$\gcd(n_1, m_1) = \gcd(n_2, m_2) = \gcd(n_3, m_3) = 1.$$

Thus there are $\widehat{m}_1$, $\widehat{m}_2$, and $\widehat{m}_3$ such that

$$\begin{aligned} \widehat{m}_1 &= \text{an inverse of } m_1 \bmod n_1 \\ \widehat{m}_2 &= \text{an inverse of } m_2 \bmod n_2 \\ \widehat{m}_3 &= \text{an inverse of } m_3 \bmod n_3 \end{aligned}$$

Then

$$\begin{aligned}
m_1\widehat{m}_1 &\equiv 1 \mod n_1 && \text{(definition of inverse mod } n_1\text{)} \\
m_1\widehat{m}_1 &\equiv 0 \mod n_2 && \text{(as } n_1 \mid m_2\text{, and thus } m_2 \equiv 0 \mod n_2\text{)} \\
m_1\widehat{m}_1 &\equiv 0 \mod n_3 && \text{(as } n_1 \mid m_3\text{, and thus } m_3 \equiv 0 \mod n_3\text{)}
\end{aligned}$$

Likewise

$$\begin{aligned}
m_2\widehat{m}_2 &\equiv 0 \mod n_1 & m_2\widehat{m}_2 &\equiv 1 \mod n_2 & m_2\widehat{m}_2 &\equiv 0 \mod n_3 \\
m_3\widehat{m}_3 &\equiv 0 \mod n_1 & m_3\widehat{m}_3 &\equiv 0 \mod n_2 & m_3\widehat{m}_3 &\equiv 1 \mod n_3
\end{aligned}$$

If we introduce the ***Kronecker delta***:

$$\delta_{ij} = \begin{cases} 1, & i = j; \\ 0, & i \neq j. \end{cases}$$

this can all be summarized by

$$m_i\widehat{m}_i \equiv \delta_{ij} \mod n_j.$$

For any integers b_1, b_2, b_3 set

$$x = m_1\widehat{m}_1 b_1 + m_2\widehat{m}_2 b_2 + m_3\widehat{m}_3 b_3$$

Then

$$\begin{aligned}
x &= m_1\widehat{m}_1 b_1 + m_2\widehat{m}_2 b_2 + m_3\widehat{m}_3 b_3 \\
&\equiv 1 \cdot b_1 + 0 \cdot b_2 + 0 \cdot b_3 && \mod n_1 \\
&= b_1.
\end{aligned}$$

Similar calculations yield

$$\begin{aligned}
x &\equiv b_2 \mod n_2 \\
x &\equiv b_3 \mod n_3
\end{aligned}$$

To summarize

Theorem 21. *Let n_1, n_2, and n_3 be positive integers with $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then for any integers b_1, b_2, and b_3 the simultaneous congruences*

$$\begin{aligned}
x &\equiv b_1 \\
x &\equiv b_2 \\
x &\equiv b_3
\end{aligned}$$

have a solution. This solution is unique modulo the product $n_1n_2n_3$. That is if x_0 is one solution, then the general solution is

$$x = x_0 + mt$$

where $m = n_1n_2n_3$ and $t \in \mathbb{Z}$.

Problem 22. We have proven the existence part of this. Prove the uniqueness part. $\square$

Example 22. Solve the system

$$\begin{aligned} x &\equiv 2 \mod 3 \\ x &\equiv 1 \mod 4 \\ x &\equiv 3 \mod 5. \end{aligned}$$

This is just plug and chug.

$$m_1 = 4 \cdot 5 = 20, \qquad m_2 = 3 \cdot 5 = 15, \qquad m_3 = 3 \cdot 4 = 12.$$

Noting that

$$20(2) \equiv 1 \mod 3, \qquad 15(3) \equiv 1 \mod 4, \qquad 12(3) \equiv 1 \mod 5$$

we see we can take

$$\widehat{m}_1 = 2, \qquad \widehat{m}_2 = 3, \qquad widehatm_3 = 3.$$

Then a particular solution to the system is

$$x_0 = m_1\widehat{m}_1 b_1 + m_2\widehat{m}_2 b_2 + m_3\widehat{m}_3 b_3 = 20 \cdot 2 \cdot 2 + 15 \cdot 3 \cdot 1 + 12 \cdot 3 \cdot 3 = 233.$$

This is unique modulo $m = 3 \cdot 4 \cdot 5 = 60$ and

$$233 \equiv 53 \mod 60.$$

Thus we can write

$$x = 53 + 60T$$

for the general solution. Or, and this is probably better, say the solution is $x \equiv 53 \mod 60$. □

Problem 23. Solve the following:

(a) $x \equiv 2 \mod 3$
$x \equiv 3 \mod 5$
$x \equiv 4 \mod 7$

(b) $x \equiv 1 \mod 7$
$x \equiv 1 \mod 9$
$x \equiv 1 \mod 16$
Hint: If you think about this for a while you should be able to write down the solution without doing any calculations.

(c) $x \equiv 21 \mod 22$
$x \equiv 34 \mod 35$
$x \equiv 38 \mod 39$
Hint: Anther one that can be done without calculation (as a start note $21 \equiv -1 \mod 22$). □

We now do the general case, not because there are any new ideas involved, but as practice in using the Kronecker delta and summation notation. Let $n_1, n_2, \ldots, n_k$ be k positive integers such that

$$\gcd(n_i, n_j) = 1 \qquad \text{when} \qquad i \neq j.$$

Let m be the product of these integers:

$$m = n_1 n_2 \cdots n_k.$$

For $i = 1, 2, \ldots, k$ let

$$m_i = \frac{m}{n_i} = \underbrace{n_1 n_2 \cdots n_{i-1} n_{i+1} \cdots n_k}_{\text{Product with } n_i \text{ omitted}}$$

be the product of all the n_j's other than n_i. Note that if $j \neq i$, then n_j is a factor in m_i and therefore

$$m_i \equiv 0 \mod n_j \qquad \text{when} \qquad i \neq j. \tag{1}$$

As $\gcd(n_j, n_i) = 1$ the numbers n_j and n_i have no common prime factors. As m_i is the product of the n_j's other than n_i it will also have no prime factors in common with n_i and therefore

$$\gcd(n_i, m_i) = 1.$$

Thus m_i will have an inverse modulo n_i. So there is an integer $\widehat{m}_i$ with

$$m_i \widehat{m}_i \equiv 1 \mod n_i.$$

Combining this with (1) gives

$$m_j \widehat{m}_j \equiv \delta_{ij} \mod n_i.$$

If $b_1, b_2, \ldots, b_k$ are any integers, set

$$x = \sum_{j=1}^{k} m_j \widehat{m}_j b_j.$$

Then

$$\begin{aligned} x &= \sum_{j=1}^{k} m_j \widehat{m}_j b_j \\ &\equiv \sum_{j=1}^{k} \delta_{ij} b_j \mod n_i \quad && (\text{as } m_j \widehat{m}_j \equiv \delta_{ij} \mod n_i.) \\ &= b_i && (\text{as } \delta_{ij} = 0 \text{ for } j \neq i, \text{ all but one term vanishes.}) \end{aligned}$$

So we have

Theorem 23. *Let $n_1, n_2, \ldots, n_k$ be positive integers with*

$$\gcd(n_i, n_j) = 1 \qquad \textit{for} \qquad i \neq j.$$

Then for any integers $b_1, b_2, \ldots, b_k$ the simultaneous congruences

$$x \equiv b_i \mod n_i \qquad i = 1, 2, \ldots, k$$

have a common solution. This solution is unique modulo the the product $m = n_1 n_2 \cdots n_k$. That is if x_0 is one solution, then the general solution is

$$x = x_0 + mt$$

with $t \in \mathbb{Z}$.

Proof. We have done everything but the uniqueness. If x_0 is one solution and x is anther solution. Then $x - x_0 \equiv b_i - b_i = 0 \mod n_i$ and thus $n_i \mid (x - x_0)$. As $n_1, n_2, \ldots, n_k$ are pairwise relatively prime, this implies $x - x_0$ is divisible by the product $m = n_1 n_2 \cdots n_k$. Therefore for some integer t we have $x - x_0 = mt$, that is $x = x_0 + mt$. $\square$