XM452 Lecture Notes 3

Erdaifu Luo

21 March 2023

§12 Introductory Remarks about Congruences

§12.1 Definition of Congruences

The most simple example of a **congruence** between integers is that of being congruent mod 2: a and b are **congruent mod 2** if they are both even or if they are both odd.

Another example is congruent mod 3, a and b are **congruent 3** if

$$a = 3k_1 + r$$
$$b = 3k_2 + r$$

where r is the same in both equations. Note that this is equivalentto $3 \mid (a - b)$. So there are three **congruence classes** mod $3(r = 0, 1, and 2)$.

Definition 12.1. Let a and b be integers. We say this is **a is congruent to b mod n** if $n \mid (a - b)$, or equivalently, if when one divides n into a and n into b, one gets the same remainder term

$$a = nk_1 + r \quad \text{with} \quad 0 \le r \le n - 1$$
$$b = nk_2 + r \quad \text{with} \quad 0 \le r \le n - 1$$

where r is the same in both equations.

Definition 12.2. If a is congruent to $b \pmod{n}$ we write

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

Similarly,

$$a \not\equiv b \pmod{n}$$

means they are not congruent.

Example 12.3 (a) $5 \equiv 9 \pmod 4$ because $4 \mid (9 - 5)$.

(b) $-6 \equiv 19 \pmod 5$ because $5 \mid 19 - (-6)$.

(c) Clocks measure time mod 12.

(d) Days of the week measure days mod 7.

§13 Basic Properties of Congruences

§13.1 Modular Arithmetic

Remember $a \equiv b \pmod{n}$ if $n \mid (a-b)$.

Theorem 13.1

If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then

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

$$a - c \equiv b - d \pmod{n},$$

and

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

In other words, the basic property of addition, subtraction and multiplication apply to the environment of congruencies. A special case is when $c = d$.

Example 13.2

$$\begin{aligned} 30 &\equiv 2 \pmod{7} \\ 76 &\equiv -1 \pmod{7} \\ 30 \cdot 76 &\equiv 2 \cdot -1 \pmod{7} \\ &\equiv 5 \pmod{7} \end{aligned}$$

Proof. First show that

$$(a + c) - (b + d) = (a - b) + (c - d),$$

which is divisible by n.

Simiarily,

$$(a - c) - (b - d) = (a - b) + (d - c),$$

again divisible by n.

Lastly,

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

again divisible by n, proving all 3. □

§13.2 Division in Congruences

Theorem 13.3 (Modular Division)

If $(a, n) = 1$ and $ab \equiv ac \pmod{n}$, then $b \equiv c \pmod{n}$.

More generally, if $(a, n) = d$ and $ab \equiv ac \pmod{n}$, then $b \equiv c \pmod{\frac{n}{d}}$.

Proof. Suppose $(a,n) = d$ and $ab \equiv ac \pmod{n}$. Therefore, there is an integer k such that

$$ab = ac + kn$$

because

$$n \mid (ab - ac).$$

Let

$$a_1 = \frac{a}{d} \text{ and } n = \frac{n}{d},$$

these are integers because $d = (a,n)$.

Also, $(a_1, n_1) = (\frac{a}{d}, \frac{n}{d}) = 1$. Dividing the above equation by d, we get

$$\frac{a}{d} \cdot b, \frac{n}{d} \cdot c = k \cdot \frac{n}{d}$$

or

$$a_1 b = a_1 c + kn_1,$$

so

$$a_1(b - c) = kn_1.$$

Therefore, we conclude that

$$n_1 \mid a_1(b - c),$$

but since $(a_1, n_1) = 1$, we know

$$n_1 \mid (b - c).$$

That is,

$$b \equiv c \pmod{n_1}$$

or

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

□

§14 Residues, Complete Residue Systems

§14.1 The Notion of Residues

Every integer k is congruent mod n to one of the integers $0, 1, \dots n-1$.

Definition 14.1 (Complete Residue System)**.** A set of n integers $a_1, a_2, \dots, a_n$ is a **complete system of residue mod n** if every integer is congruent mod n to exactly one of the a_j's.

Example 14.2

The set of $0, 1, \dots, n-1$ is a complete system of residues mod n.

Theorem 14.3

Any set of n consecutive integers is a complete residue system mod n.

Proof. Take any set of n consecutive integers $k, k+1, \ldots k+(n-1)$. Let a be any integer. Then by dividing $a-k$ by n, we can write

$$a - k = ln + r$$

where

$$0 \leq r \leq n-1$$

and r is the remainder term.

Therefore,

$$a - k \equiv r \pmod{n}$$

or

$$a \equiv k + r \pmod{n}.$$

Since $0 \leq r \leq n-1$, $k+r$ is in the list $k, k+1, \ldots, k+n-1$.

Next we need to show that a is congruent to only one of the integers $k, k+1, \ldots, k+n-1$. We know

$$a \equiv k + r \pmod{n}$$

so suppose

$$a \equiv k + r' \pmod{n}$$

for some $r' \neq r$ where $0 \leq r' \leq n-1$. If we prove that $r' = r$ and a contradiction exists with our previous claim, we can prove the theorem.

From the previous, we know that

$$k + r \equiv k + r' \pmod{n}.$$

Subtracting,

$$r \equiv r' \pmod{n}$$

or

$$r - r' \equiv 0 \pmod{n}$$

and so

$$n \mid (r - r').$$

But since $0 \leq r' \leq n-1$, this implies $r = r'$, which is a contradiction to our claim that $r \neq r'$ and proves our theorem. □

Since every integer is congruent mod n to one in the list $0, 1, \ldots, n-1$, we can "**add mod n**" or aka do "**modular arithmetic**".

Example 14.4

Mod 5 arithmetic meaning doing arithmetic with integers $0, 1, 2, 3, 4$.

$$3 + 4 \equiv 2 \pmod{5}$$
$$4 + 4 \equiv 3 \pmod{5}$$
$$4 + 1 \equiv 0 \pmod{5}$$

and so on. We can make an addition table mod 4 in that regard.

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

§14.2 Polynomial Congruencies

Recall if $a \equiv b \pmod{n}$, then $ac \equiv bc \pmod{n}$. Therefore, if $a \equiv b \pmod{n}$,

$$a^2 \equiv b^2 \pmod{n}$$

and if $k \geq 0$,

$$a^k \equiv b^k \pmod{n}.$$

Also,

$$ca^k \equiv cb^k \pmod{n}.$$

Theorem 14.5

Let

$$f(x) \equiv a_k x^k + a_{k-1}x^{k-1} + \cdots + a_1 x^1 + a_0$$

be any polynomial with integral coefficients, or $a_0, \ldots, a_k \in \mathbb{Z}$. Then if

$$a \equiv b \pmod{n},$$

then

$$f(a) \equiv f(b) \pmod{n}.$$

Proof. TODO □

Example 14.6 (Casting out Nines)

Observe that every positive integer n is congruent mod 9 to the sum of its digits. Write n in terms of its digits. That is,

$$n = a_k 10^k + a_{k-1}10^{k-1} + \cdots + a_1 10 + a_0$$

where $a_0, \ldots, a_k \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Let

$$f(x) \equiv a_k x^k + a_{k-1}x^{k-1} + \cdots + a_1 x^1 + a_0,$$

so $n = f(10)$.

But

$$1 \equiv 10 \pmod{9},$$

so

$$f(1) \equiv f(10) \pmod{9},$$

and

$$a_0 + a_1 + \cdots + a_k \equiv n \pmod{9}.$$

Since we are adding mod 9, we can neglect, or "cast out", any $a_1 = 9$, or if a pair $a_i + a_j = 9$, we can throw away the pair.

Example 14.7

Using the previous method on 382792, we get

$$\begin{aligned} 382792 &\equiv 3+8+2+7+9+2 \pmod 9 \\ &\equiv 3+8+2 \pmod 9 \\ &\equiv 13 \pmod 9 \\ &\equiv 4 \pmod 9. \end{aligned}$$

§15 Linear Congruence Equations

§15.1 Solving an Equation mod n

We now examine how to solve a linear equation of the form

$$a_1x_1 + \cdots + a_kx_k \equiv b \pmod n$$

where $x_1, \ldots, x_k$ are the unknowns.

We want integers $x_1, \ldots, x_k$ that satisfy the equation. This is equivalent to solving the equation

$$a_1x_1 + \cdots + a_kx_k = nx_{k+1} + b$$

for some integer x_{k+1}. This, then, is equivalent to solving the linear Diophantine equation

$$a_1x_1 + \cdots + a_kx_k - nx_{k+1} = b$$

for integer values $x_1, \ldots, x_k$.

Example 15.1

In the equation

$$x + 2y + z \equiv 1 \pmod 5,$$

$x = 1$, $y = 1$, $z = 3$ is a solution, which is the same solution mod 5 as $x = 6$, $y = 11$, $z = 8$.

However, it is a different solution than $x = 2$, $y = 0$, $z = 4$.

Theorem 15.2

The equation $ax \equiv b \pmod n$ has solutions if, and only if,when $d = (a, n)$, then $d \mid b$.

If $d \mid b$, thenn the solution is unique mod $\frac{n}{d}$. So if $(a, n) = 1$, then there is always a unique solution mod n.

Proof. Since $ax \equiv b \pmod n$ has an integer solution if and only if the linear Diophantine equation in two unknowns

$$ax - ny = b$$

has integral solutions.

By a previous theorem, this has a solution if and only if $d = (a, n) \mid b$. Thus,

$$ax \equiv b \pmod n$$

has a solution if and only if $d \mid b$.

Let (x_0, y_0) be an integral solution to

$$ax - ny = b.$$

Then, every other solution is of the form

$$x = x_0 + t \cdot \frac{n}{d}.$$

Thus, every solution to $ax \equiv b \pmod{n}$ is of the previous form. Since

$$x = x_0 + t \cdot \frac{n}{d} \equiv x_0 \pmod{\frac{n}{d}},$$

all solutions are congruent to $x_0 \pmod{\frac{n}{d}}$ and hence the solution is unique $\pmod{\frac{n}{d}}$. $\square$

When we studied the linear Diophantine equaton in two unknowns, we developed a systematic way of solving $ax - ny = b$ of $d \equiv b$.

Namely, if $d = ar + ns$ since $d = (a, n)$ and $b = de$ since $d \mid b$, then

$$x_0 = re \text{ and } y_0 = se$$

is a solution, and all other solutions is congruent mod $\frac{n}{d}$ to $x_0 = re$.

We can divide the equation $ax \equiv b \pmod{n}$ by d to get

$$\frac{a}{d} \cdot x \equiv e \pmod{\frac{n}{d}}$$

where, if $c = \frac{a}{d}$, we are solving the equation

$$cx \equiv e \pmod{n},$$

where $(c, e) = 1$.

Example 15.3

(1) Assume $11x \equiv 18 \pmod{23}$. Let $d = (a, n) = (11, 23) = 1$. So This has an unique solution mod 23 because $1 = d \mid 23$. If we write $d = 1 = r \cdot 11 + s \cdot 23$, then $x_0 = r \cdot 18$ is the unique solution mod 23. Since

$$1 = -2 \cdot 11 + 1 \cdot 23,$$

$r = -2$, thus $x_0 \equiv -2 \cdot 18 \equiv -36 \equiv 10 \pmod{3}$ is the unique solution.

(2) $14x \equiv 13 \pmod{21}$ has no solutions mod 21 because $d = (14, 21) = 7$ does not divide 13.

(3) $9x \equiv 15 \pmod{21}$, Let $d = (9, 21) = 3$. $3 \mid 15$, so it has solutions. Dividing through by $d = 3$,

$$3x \equiv 5 \pmod{7}.$$

This has an unique solution mod 7, since $(3, 7) = 1$. Namely,

$$x_0 = r \cdot 5.$$

Solving, we get $x_0 \equiv 4 \pmod{7}$.

§16 The Chinese Remainder Theorem

§16.1 Solutions of Systems of Congruences

Example 16.1

Consider the simultaneous equations

$$\begin{aligned} x &\equiv 2 \pmod 4 \\ x &\equiv 1 \pmod 6 \end{aligned}$$

There are no simultaneous solutions. For the first equation, every solution x is even. For the seocnd every solution x is odd.

For another example,

Example 16.2

Consider the simultaneous equations

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 7 \end{aligned}$$

The first has a solution of the form

$$x = 3m + 2$$

while the second has a solution of the form

$$x = 7n + 3.$$

So the simultaneous solution would be when

$$\begin{aligned} 3m + 2 &= 7n + 3 \\ 3m - 1 &= 7n \\ 3m - 7n &= 1 \end{aligned}$$

which, after solving, $m = -2$ and $n = -1$ works.

§16.2 Proof to the CRT

In general, we can determine when there are solutions to two or more general equations to modular arithemetic.

Theorem 16.3 (Chinese Remainder Theorem)
If $(m, n) = 1$, then the equations

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

have a unique solution mod mn.

More generally, if $m_1, \ldots, m_k$ are positive integers that are pairwise relatively prime, then the k equations

$$\begin{aligned} x &\equiv a_1 \pmod{m} \\ x &\equiv a_2 \pmod{n} \\ &\vdots \\ x &\equiv a_k \pmod{m} \end{aligned}$$

have a unique solution mod $m_1, \ldots, m_k$.

Proof. $x \equiv a \pmod{m}$ means that $x = a + mt$ for some $t \in \mathbb{Z}$. This satisfies the second equation if

$$a + mt \equiv b \pmod{n}$$

that is, if

$$mt \equiv (b - a) \pmod{n}.$$

Since $(m, n) = 1$, this has a unique solution mod n, say

$$t \equiv c \pmod{n},$$

that is, there is an integer k such that

$$t = c + nk.$$

Since $x = a + mt$,

$$x = a + m(c + nk),$$

or

$$x = a + mc + mnk.$$

Thus the simultneous equations

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

have solutions exactly of the form

$$x = a + mc + mnk.$$

All of these solutions are congruent mod mn.

In full generality, assume we have $m_1, \ldots, m_k$ pairwise relatively prime. Consider

$$\begin{aligned} x &\equiv a_1 \pmod{m} \\ x &\equiv a_2 \pmod{n} \\ &\vdots \\ x &\equiv a_k \pmod{m} \end{aligned}$$

Show this has a unique solution mod $m_1, \dots, m_k$. By the first part of the theorem,

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

has a unique solution, say $b_2 \pmod{m_1 m_2}$. Consider the two equations

$$\begin{aligned} x &\equiv b_2 \pmod{m_1 m_2} \\ x &\equiv a_3 \pmod{m_3} \end{aligned}$$

where $(m_1 m_2, m_3) = 1$. Since they are relatively prime, by the first part of the theorem, there exists a unique solution mod $m_1 m_2 m_3$, say

$$x \equiv b \pmod{m_1 m_2 m_3}.$$

Continuing, we get a unique solution

$$x \equiv b_k \pmod{m_1 \dots m_k}$$

to the system of equations

$$\begin{aligned} x &\equiv a_1 \pmod{m} \\ x &\equiv a_2 \pmod{n} \\ &\vdots \\ x &\equiv a_k \pmod{m}. \end{aligned}$$

□

.

§17 Linear Congruence Equations in Two Variables

§17.1 The Chinese Remainder Theorem (Continued)

If $a_1, \dots, a_k$ are restricted to integers between 0 and $m_j - 1$ respectively, then this theorem says that if $m_1, \dots, m_k$ are pairwise relatively prime, then there is an integer x such that for each $j = 1, \dots, k$, the quotient $\frac{x}{m_j}$ has remainder a_j.

Theorem 17.1

Consider the system of equations

$$\begin{aligned} cx + ey &\equiv a \pmod{n} \\ dx + fy &\equiv b \pmod{n} \end{aligned}$$

If $(cf - de, n) = 1$, these equations have a unique common solution for x and y mod n.

Proof. Assume there is a solution and try to compute it. Multiplying the first equation by f, the second by e, and subtracting,

$$(cf - de)x \equiv (af - be) \pmod{n}.$$

Since $(cf-de,n)=1$, there is a unique solution x mod n to the equation. Similarly, multiplying the second of the system of equations by c and subtracting d times the first,

$$(cf-de)y \equiv (bc-ad) \pmod{n}.$$

Again, since $(cf-de,n)=1$, there is a unique solution y mod n to the previous.

So there is a number z such that

$$(cf-de)\cdot z \equiv 1 \pmod{n},$$

and z will play the role of $\frac{1}{cf-de}$, which is the modular inverse of $cf-de$, in this modular arithmetic.

Multiplying the first equation by z,

$$z(cf-de)\cdot x \equiv z(af-be) \pmod{n},$$

or

$$x \equiv z(af-be) \pmod{n}.$$

Multiplying the second equation by z,

$$y \equiv z(bc-ad) \pmod{n}.$$

Substituting into the original equations,

$$\begin{aligned} cx+ey &\equiv cz(af-be)+ez(bc-ad) \pmod{n} \\ &\equiv czaf-ezad \pmod{n} \\ &\equiv az(cf-de) \pmod{n} \\ &\equiv a \pmod{n}. \end{aligned}$$

Similarily, $dx+fy\equiv b \pmod{n}$ is also satisfied when the above x and y occurs. This means that unique solutions x and y exists such that the given system of equations have a common solution. □