

4.4 Solving Congruences

Definition 4.4.1 (Inverse of a Modulo m). Let $a \in \mathbb{Z}$, $m \in \mathbb{Z}^+$. We say $\bar{a}$ is the inverse of a modulo m if $a \cdot \bar{a} \equiv 1 \pmod{m}$.

Example 4.4.1. The inverse of 3 modulo 7 is 5.

$$\boxed{3} \cdot \boxed{5} \equiv 1 \pmod{7} \quad 1 = \boxed{5} \times 3 + \boxed{-2} \times 7$$

The existence of the inverse of a modulo m is guaranteed if a and m are relatively prime:

Theorem 4.4.1. If $\gcd(a, m) = 1$ and $m > 1$ then $\bar{a}$ exists. That is, there exists a number $\bar{a}$ such that $a\bar{a} \equiv 1 \pmod{m}$.

Proof. By Bézout's theorem, since $\gcd(a, m) = 1$, $\exists s, t \in \mathbb{Z}$:

$$sa + tm = 1. \quad \text{Let } \bar{a} = s, \text{ we have}$$

$$\bar{a} \cdot a + tm = 1 \quad \Rightarrow \quad a \cdot \bar{a} - 1 = (-t) \cdot m. \quad \text{Since } -t \in \mathbb{Z}:$$

$$m \mid a\bar{a} - 1 \quad \therefore \quad a\bar{a} \equiv 1 \pmod{m}. \quad \square$$

Finding the inverse of a modulo m :

If $\gcd(a, m) = 1$, use Euclidean algorithm to find the Bézout's coefficient s, t so that $sa + tm = 1$ and then

s is the inverse of a modulo m .

↖ the coefficient of a

Example 4.4.2. Using Euclidean algorithm, find the inverse of 3 of modulo 7.

$$7 = 3 \cdot \boxed{2} + \boxed{1} \quad \Rightarrow \quad 1 = \boxed{1} \cdot 7 + \boxed{-2} \cdot 3$$

$$3 = 1 \cdot \boxed{3} + 0 \leftarrow \text{stop}$$

↖ the coefficient of 3

$\therefore -2$ is the inverse of 3 modulo 7.

and note that $-2 + 7 = 5 \quad \therefore -2 \equiv 5 \pmod{7}$

$\therefore$ One may also say 5 is the inverse of 3 modulo 7.

Definition 4.4.2 (Linear Congruence). An equation of the form $ax \equiv b \pmod{m}$ where $a, b \in \mathbb{Z}$, $m \in \mathbb{Z}^+$ are constants is called a linear congruence.

(To solve a linear congruence, we need to find x that satisfies $ax \equiv b \pmod{m}$)

Two Methods for Finding the Solution of Linear Congruences:

- ① If the inverse of a modulo m , say $\bar{a}$, exists then multiply both sides by $\bar{a}$: $\bar{a} \cdot ax \equiv \bar{a} \cdot b \pmod{m}$, but since $a \cdot \bar{a} \equiv 1 \pmod{m} \therefore x \equiv \bar{a} \cdot b \pmod{m}$.
(if $\bar{a}$ does not exist, there may or may not be any solutions)

- ② Add a multiple of m to b so that it becomes divisible by a . If $\gcd(a, m) = 1$, divide both sides by a to get the answer.

Example 4.4.3. Solve the congruence $5x \equiv 6 \pmod{9}$.

Method ①: Using Euclidean algorithm, or by guessing, find the inverse of 5 modulo 9 : $5 \cdot \underline{2} \equiv 1 \pmod{9}$

Multiply both sides of $5x \equiv 6 \pmod{9}$ by 2:

$$10x \equiv 12 \pmod{9}$$

$$\therefore 1 \cdot x \equiv 3 \pmod{9}$$

$$\therefore \boxed{x \equiv 3 \pmod{9}}$$

That is $x \in \{\dots, -15, -6, 3, 12, 21, 30, 39, \dots\}$ or you may say all numbers of the form $x = 9k + 3$ (where $k \in \mathbb{Z}$) are solutions.

Method ②: $5x \equiv 6 + \underline{1 \cdot 9} \pmod{9}$ (added a multiple 9 so that the R.H.S. becomes divisible by 5. because $1 \cdot 9 \equiv 0 \pmod{9}$)
 $\therefore 5x \equiv 15 \pmod{9}$

Since $\frac{5}{5} \in \mathbb{Z}$, $\frac{15}{5} \in \mathbb{Z}$, $\gcd(5, 9) = 1 \therefore \frac{5x}{5} = \frac{15}{5} \pmod{9}$

$$\boxed{x \equiv 3 \pmod{9}}$$

There is a second method, called Back Substitution, to solve a system of linear congruences. We explain this method in the example below:

Example 4.4.8. Solve the system using Back Substitution:

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$

Since $x \equiv 2 \pmod{3} \therefore 3 \mid x-2 \therefore \exists k \in \mathbb{Z}: 3k = x-2$

$\therefore \boxed{x = 3k+2}$. Substitute this back into the second congruence:

$$x \equiv 3 \pmod{5} \therefore 3k+2 \equiv 3 \pmod{5}$$

$$\therefore 3k+2-2 \equiv 3-2 \pmod{5}$$

$$\text{Need inverse of } 3 \pmod{5}: \therefore 3k \equiv 1 \pmod{5}$$

$$3 \cdot \boxed{2} \equiv 1 \pmod{5} \quad \leftarrow \therefore 2(3k) \equiv 2(1) \pmod{5}$$

$$\therefore 6k \equiv 2 \pmod{5}$$

$$\therefore k \equiv 2 \pmod{5}$$

$$\therefore \exists u \in \mathbb{Z}: \underline{k = 5u+2}$$

$$\therefore \underline{x = 3(5u+2) + 2} = 15u + 8$$

Substitute $x = 15u+8$ back into the next congruence:

$$x \equiv 2 \pmod{7} \text{ to get } 15u+8 \equiv 2 \pmod{7}$$

Since $x = 15u+8$, we get

$$x = 15(7w+1) + 8$$

$$\therefore \boxed{x = 105w + 23 \quad (w \in \mathbb{Z})}$$

$$\therefore x \in \{ \dots, -82, 23, 128, 233, \dots \}$$

Since $15 \equiv 1 \pmod{7}$

$$-6 \equiv 1 \pmod{7}$$

$$15u+8-8 \equiv 2-8 \pmod{7}$$

$$15u \equiv -6 \pmod{7}$$

$$\therefore 1 \cdot u \equiv 1 \pmod{7}$$

$$\therefore u \equiv 1 \pmod{7}$$

$$\therefore \exists w \in \mathbb{Z}: u = 7w + 1$$

$$\gcd(a, m) = 1$$

$$\therefore \exists \bar{a} \in \mathbb{Z} \quad a\bar{a} \equiv 1 \pmod{m}$$

The proof of the following theorem gives a method for solving a system of linear congruences.

Theorem 4.4.2 (The Chinese Remainder Theorem). Let $m_1, m_2, \dots, m_k$ be pairwise relatively prime integers greater than 1. Let $a_1, a_2, \dots, a_k \in \mathbb{Z}$. Then the system

$$M_3 = \underbrace{m_1 m_2 m_4 m_5 \dots}_{m_3} = \frac{M}{m_3} \begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

$$m_1 = 3, m_2 = 5, m_3 = 7$$

$$M_1 = 5 \times 7 = 35$$

$$y_1 \downarrow$$

$$35 \square \equiv 1 \pmod{3}$$

has a unique solution modulo $M = m_1 m_2 \dots m_k$. That is, there is a unique solution x with $0 \leq x \leq M - 1$ and all other solutions are congruent to this x modulo M .

Proof. For every $i = 1, 2, \dots, k$, let $M_i = \frac{M}{m_i}$. Note $M_i \in \mathbb{Z}$,

$$\gcd(M_i, m_i) = 1 \quad \text{Since } m_1, m_2, \dots, m_k \text{ are relatively prime.}$$

$$\text{Therefore } \exists y_i \in \mathbb{Z} \text{ s.t. } M_i y_i \equiv 1 \pmod{m_i}$$

Claim: $x = a_1 M_1 y_1 + a_2 M_2 y_2 + \dots + a_k M_k y_k$ is a solution to the system.

Proof of claim: For every $i = 1, 2, \dots, k$, we have

$$\boxed{a_i M_i y_i} \equiv a_i \cdot 1 \equiv \boxed{a_i} \pmod{m_i}$$

$$\text{and } \forall j \neq i : \boxed{a_j M_j y_j} \equiv a_j \underbrace{m_1 m_2 \dots m_k}_{\text{this is a multiple of } m_i} \cdot y_j \equiv \boxed{0} \pmod{m_i}$$

$$\begin{aligned} \therefore x &\equiv a_1 y_1 M_1 + a_2 M_2 y_2 + \dots + \boxed{a_i M_i y_i} + \dots + a_k M_k y_k \pmod{m_i} \\ &\equiv 0 + 0 + \dots + 0 + \boxed{a_i} + 0 + \dots + 0 \pmod{m_i} \\ &\equiv a_i \end{aligned}$$

This shows $x \equiv a_1 \pmod{m_1}$, $x \equiv a_2 \pmod{m_2}$, and so on.
(We are skipping the proof of the "uniqueness")

Example 4.4.7. Solve the system using the Chinese Remainder Theorem:

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$

Here: $a_1 = 2$ $m_1 = 3$
 $a_2 = 3$ $m_2 = 5$
 $a_3 = 2$ $m_3 = 7$

Let $M = m_1 m_2 m_3 = 3 \cdot 5 \cdot 7 = 105$

$$M_1 = \frac{M}{m_1} = \frac{3 \cdot 5 \cdot 7}{3} = 35$$

$$M_2 = \frac{3 \cdot 5 \cdot 7}{5} = 21$$

$$M_3 = \frac{3 \cdot 5 \cdot 7}{7} = 15$$

Let $y_1 =$ the inverse of $M_1 = 35 \pmod{m_1 = 3}$: $35y_1 \equiv 1 \pmod{3}$

$$\therefore 2y_1 \equiv 1 \pmod{3}$$

$$\boxed{y_1 = 2} \text{ works}$$

$$M_2 y_2 \equiv 1 \pmod{m_2}$$

$$21 y_2 \equiv 1 \pmod{5}$$

$$1 \cdot y_2 \equiv 1 \pmod{5}$$

$$\boxed{y_2 = 1} \text{ works}$$

$$M_3 y_3 \equiv 1 \pmod{m_3}$$

$$15 y_3 \equiv 1 \pmod{7}$$

$$1 \cdot y_3 \equiv 1 \pmod{7}$$

$$\boxed{y_3 = 1} \text{ works}$$

$$\therefore x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3$$

$$= 2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1$$

$$= 140 + 63 + 30$$

$$= 233$$

must be a solution by Chinese Remainder-Thm

and all other solutions must be congruent to 233 mod 105 :

$$\{ \dots, 23, 128, \underline{233}, 338, \dots \}$$

There is a second method, called Back Substitution, to solve a system of linear congruences. We explain this method in the example below:

Example 4.4.8. Solve the system using Back Substitution:

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$

Since $x \equiv 2 \pmod{3} \therefore 3 \mid x-2 \therefore \exists k \in \mathbb{Z} : 3k = x-2$

$\therefore \boxed{x = 3k+2}$. Substitute this back into the second congruence:

$$x \equiv 3 \pmod{5} \therefore 3k+2 \equiv 3 \pmod{5}$$

$$\therefore 3k+2-2 \equiv 3-2 \pmod{5}$$

Need inverse of 3 mod 5: $\therefore 3k \equiv 1 \pmod{5}$

$$3 \cdot \boxed{2} \equiv 1 \pmod{5} \quad \leftarrow \therefore 2(3k) \equiv 2(1) \pmod{5}$$

$$\therefore 6k \equiv 2 \pmod{5}$$

$$\therefore k \equiv 2 \pmod{5}$$

$$\therefore \exists u \in \mathbb{Z} : \underline{k = 5u+2}$$

$$\therefore \underline{x = 3(5u+2) + 2} = 15u + 8$$

Substitute $x = 15u+8$ back into the next congruence:

$$x \equiv 2 \pmod{7} \text{ to get } 15u+8 \equiv 2 \pmod{7}$$

$$15u+8-8 \equiv 2-8 \pmod{7}$$

$$15u \equiv -6 \pmod{7}$$

$$\therefore 1 \cdot u \equiv 1 \pmod{7}$$

$$\therefore u \equiv 1 \pmod{7}$$

$$\therefore \exists w \in \mathbb{Z} : u = 7w + 1$$

Since $x = 15u+8$, we get

$$x = 15(7w+1) + 8$$

$$\therefore \boxed{x = 105w + 23 \quad (w \in \mathbb{Z})}$$

$$\therefore x \in \{ \dots, -82, 23, 128, 233, \dots \}$$

Since $15 \equiv 1 \pmod{7}$

$$-6 \equiv 1 \pmod{7}$$

The following theorem enables us to evaluate a^y modulo a prime number p efficiently.

Theorem 4.4.3 (Fermat's Little Theorem). Let p be prime and assume $a \in \mathbb{Z}$ is not a multiple of p . Then $a^{p-1} \equiv 1 \pmod{p}$. Furthermore, if a is any integer then $a^p \equiv a \pmod{p}$.

skip the proof now

we prove here

If a is not a multiple of p , $a^{p-1} \equiv 1 \pmod{p} \therefore a^{p-1} \cdot a \equiv 1 \cdot a \pmod{p}$

If a is a multiple of p then $a \equiv 0 \pmod{p} \therefore a^p \equiv a \pmod{p}$

Example 4.4.9. Find 7^{222} modulo 11. $\therefore a^p \equiv 0^p \equiv 0 \pmod{p} \therefore a^p \equiv a \pmod{p}$

By Fermat's Little Theorem, since $p=11$ is prime and $a=7$ is not a multiple of 11 , we have $7^{11-1} \equiv 1 \pmod{11}$

$$\therefore 7^{10} \equiv 1 \pmod{11}$$

$$\therefore (7^{10})^{22} \equiv 1^{22} \pmod{11}$$

$$7^{220} \equiv 1 \pmod{11}$$

then by multiplying both sides by 7^2 :

$$7^{222} \equiv 7^2 \pmod{11}$$

$$\equiv 49 \pmod{11}$$

$$\equiv 5 \pmod{11}$$

Definition 4.4.3 (Pseudo Prime Base a).

We call a number n "pseudo prime base a " if $a^{n-1} \equiv 1 \pmod{n}$.

$$\therefore \exists w \in \mathbb{Z} : u = 1w + 1$$

4.4. SOLVING CONGRUENCES

CHAPTER 4.

The following theorem enables us to evaluate a^p modulo a prime number p efficiently.

Theorem 4.4.3 (Fermat's Little Theorem). Let p be prime and assume $a \in \mathbb{Z}$ is not a multiple of p . Then $a^{p-1} \equiv 1 \pmod{p}$. Furthermore, if a is any integer then $a^p \equiv a \pmod{p}$.

skip the proof now

we prove here

- If a is not a multiple of p , $a^{p-1} \equiv 1 \pmod{p} \therefore a^{p-1} \cdot a \equiv 1 \cdot a \pmod{p}$
 - If a is a multiple of p then $a \equiv 0 \pmod{p} \therefore a^p \equiv 0 \pmod{p}$
- Example 4.4.9. Find 7^{222} modulo 11. $a^p \equiv 0^p \equiv 0 \pmod{p} \therefore a^p \equiv a \pmod{p}$

By Fermat's Little Theorem, since $p=11$ is prime and $a=7$ is not a multiple of 11, we have $7^{11-1} \equiv 1 \pmod{11}$

$$\therefore 7^{10} \equiv 1 \pmod{11}$$

$$\therefore (7^{10})^{22} \equiv 1^{22} \pmod{11}$$

$$7^{220} \equiv 1 \pmod{11}$$

then by multiplying both sides by 7^2 :

$$7^{222} \equiv 7^2 \pmod{11}$$

$$\equiv 49 \pmod{11}$$

$$\equiv 5 \pmod{11}$$

Definition 4.4.3 (Pseudo Prime Base a).

We call a number n "pseudo prime base a " if $a^{n-1} \equiv 1 \pmod{n}$.

$$2^{n-1} \equiv 1 \pmod{n}$$

By Fermat's Little Theorem, if p is prime and a is not a multiple of p then

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

$\therefore p$ is a pseudo prime base a .

Question. Is there a number n and a number a so that n is pseudo prime base a , but n is not prime?



Proof of Fermat's Little Theorem:

p : prime a is not a multiple of p

Consider $a, 2a, 3a, 4a, \dots, (p-1)a$

Claim. No pair ^{of numbers} from the list above are congruent
Proof of each other modulo p :

^{Proof of claim} If $ra \equiv sa \pmod{p}$ then

$$ra - sa \equiv 0 \pmod{p}$$

$$a(r-s) \equiv 0 \pmod{p}$$

Since a is not a multiple of p , p is prime:

$$\gcd(a, p) = 1$$

$$\therefore \frac{a(r-s)}{a} \equiv \frac{0}{a} \pmod{p}$$

$$\therefore r \equiv s \pmod{p}$$

But $1 \leq r, s \leq p-1$, therefore $r=s$.

Since none of the numbers $a, 2a, 3a, \dots, (p-1)a$ is divisible by p and no two will have the same remainder when divided by p ,

therefore $a \cdot 2a \cdot 3a \cdot \dots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1) \pmod{p}$

p is prime

$$\gcd(2, p) = 1$$

$$\gcd(3, p) = 1$$

$$\vdots$$

$$\gcd(p-1, p) = 1$$

$$\begin{aligned} a^{p-1} \cdot \cancel{1} \cdot \cancel{2} \cdot \cancel{3} \cdot \dots \cdot \cancel{(p-1)} &\equiv \cancel{1} \cdot \cancel{2} \cdot \cancel{3} \cdot \dots \cdot \cancel{(p-1)} \pmod{p} \\ a^{p-1} &\equiv 1 \pmod{p} \end{aligned}$$

Fermat's Little Theorem also gives an efficient method to determine whether a given number n is not prime:

Given a number n , pick a number a that is not a multiple of n . Calculate $a^{n-1} \bmod n$. If $a^{n-1} \not\equiv 1 \pmod{n}$, by Fermat's Little theorem, n cannot be prime.

If one a doesn't work, pick another one.

If for all a , you keep getting $a^{n-1} \equiv 1 \pmod{n}$, then most probably n is prime.

Definition 4.4.4 (Primitive Roots of $\mathbb{Z}_p$). Let p be a prime.

An integer $r \in \mathbb{Z}_p = \{0, 1, \dots, p-1\}$ is called a primitive root modulo p if every non-zero element in $\mathbb{Z}_p$ can be written as a power of r modulo p . (recall that $\cdot$ and $+$ in $\mathbb{Z}_p$ are done modulo p).

Example 4.4.10. Show that 2 is a primitive root of $\mathbb{Z}_{11}$, but 3 is not a primitive root of $\mathbb{Z}_{11}$.

All calculations below are done modulo 11:

$$\rightarrow 2^1 \equiv 2$$

$$2^2 \equiv 4$$

$$2^3 \equiv 8$$

$$\rightarrow 2^4 \equiv 5$$

$$2^5 \equiv 10$$

$$2^6 \equiv 9$$

$$2^7 \equiv 7$$

$$2^8 \equiv 3$$

$$2^9 \equiv 6$$

$$2^{10} \equiv 1$$

$$\therefore \{2^1, 2^2, \dots, 2^{10}\} = \{1, \dots, 10\}$$

$\therefore 2$ is a primitive root of $\mathbb{Z}_{11}$

$$3^1 \equiv 3 \equiv 3^6 \equiv 3^{11}$$

$$3^2 \equiv 9 \equiv 3^7$$

$$3^3 \equiv 5 \equiv 3^8$$

$$3^4 \equiv 4 \equiv 3^9$$

$$3^5 \equiv 1 \equiv 3^{10}$$

$$\therefore \{3^k : k \in \mathbb{N}\} = \{1, 3, 4, 5, 9\}$$

$\uparrow$
mod 11 $\neq \{1, \dots, 10\}$

$\therefore 3$ is not a primitive root of $\mathbb{Z}_{11}$

$$\begin{aligned} 2^1 &\equiv 2 \\ 2^8 &\equiv 3 \\ 2^9 &\equiv 6 \\ 2^{10} &\equiv 1 \end{aligned}$$

74

$\not\equiv \{1, \dots, 10\}$
 $\therefore 3$ is not a primitive root of $\mathbb{Z}_{11}$

4.4. SOLVING CONGRUENCES

CHAPTER 4.

Definition 4.4.5 (Discrete Logarithm of n base r (modulo p)).

Suppose p is prime, r is a primitive root in $\mathbb{Z}_p$.

We know that for every $n \in \mathbb{Z}_p \setminus \{0\}$, $\exists e$ so that $r^e \equiv n \pmod{p}$. We define e to be the discrete logarithm of n base r (modulo p) and we write $e = \log_r n$ (where p is understood)

Example 4.4.11. Find the discrete logarithm of 9 base 2 (modulo 11).

$$\text{In } \mathbb{Z}_{11}: \log_2 9 = ? \iff 2^? \equiv 9 \pmod{11}$$

From previous example, we saw $? = 6$ works.

Answer: 6

