

Dis 3A: Modular Arithmetic II

Monday, 6 July 2020 10:10 PM

Let's race – use **any** technique:

$$\begin{array}{c} x \equiv 7 \pmod{13} \\ x \equiv 4 \pmod{17} \end{array} \quad | \quad \begin{array}{l} -a) \\ -b) \end{array}$$

What's $x \pmod{13 \cdot 17} = 221$?

[3 mins] Type your solution in the chat.

$$\begin{aligned} ① \quad & x = 20, 23, 26, \dots \quad \leftarrow \\ ② \quad & x - 7 = 13k, k \in \mathbb{Z} \\ & x = 13k + 7 \quad (\text{mod } 17) \\ & 13k + 7 \equiv 4 \pmod{17} \\ & 13k \equiv -3 \pmod{17} \\ & 13k \equiv 14 \pmod{17} \\ & (k \equiv 13^{-1} \pmod{17}) \quad \leftarrow \\ & k \equiv 14 \pmod{17} \quad \leftarrow \\ & \dots \end{aligned}$$

Thm (The Chinese Remainder Theorem)

Let $1 < m_1, m_2, \dots, m_n \in \mathbb{Z}^+$ be pairwise relatively prime. $\gcd(m_i, m_j) = 1, i \neq j$

Let $a_1, a_2, \dots, a_n \in \mathbb{Z}$. Then the system

$$x \equiv a_1 \pmod{m_1}$$

:

$$x \equiv a_n \pmod{m_n}$$

has a solution.

$$x \equiv \prod_{i=1}^k a_i \left(\frac{M}{m_i} \right) \left(\frac{M}{m_i} \right)^{-1} \pmod{M}$$

$$\text{where } M = \prod_{i=1}^n m_i$$

Where does this come from? [5mins]

WT find d_1, d_2 :

$$\begin{gathered} \text{Bezout's identity} \\ \gcd(m_1, m_2) = c_1 m_1 + c_2 m_2 = 1 \end{gathered}$$

$$x = d_1 m_1 + d_2 m_2$$

$$\begin{gathered} d_1 = 2 \\ \Rightarrow d_1 \equiv 2 \pmod{4} \end{gathered}$$

$$d_1 \equiv \boxed{1} \pmod{m_1}$$

$$d_2 \equiv \boxed{2} \pmod{m_2}$$

$$\begin{aligned} & \text{2 moduli case:} \\ & \begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases} \quad \leftarrow \quad M = m_1 m_2 \\ & \text{Show } x \equiv a_1 \left(\frac{M}{m_1} \right) \cdot \left(\frac{M}{m_1} \right)^{-1} + a_2 \left(\frac{M}{m_2} \right) \cdot \left(\frac{M}{m_2} \right)^{-1} \pmod{M} \end{aligned}$$

$$\begin{gathered} \exists d_1, d_2 \in \mathbb{Z}, \text{ s.t.} \\ x = d_1 m_1 + d_2 m_2 \quad \leftarrow \quad \boxed{0} \quad \leftarrow \quad \dots \\ \leftarrow \quad \leftarrow \quad \leftarrow \quad \leftarrow \quad \leftarrow \end{gathered}$$

$$\begin{gathered} \text{normally} \rightarrow d_2 = 0 \pmod{9} \\ d_2 \equiv \boxed{4} \pmod{4} \end{gathered}$$

$\forall \exists a_1, a_2 \in \mathbb{Z}, \text{ s.t. } (x) = (d_1)m_1 + (d_2)m_2 \not\equiv 0$

WT find d_1, d_2 :

$$\begin{cases} d_1m_1 + d_2m_2 \equiv a_1 \pmod{m_1} \\ d_1m_1 + d_2m_2 \equiv a_2 \pmod{m_2} \end{cases}$$

$m_2 = \frac{M}{m_1}$

$$x \equiv a_1 \left(m_2^{-1} \right)_{m_1} m_2 + a_2 \left(m_1^{-1} \right)_{m_2} m_1 \pmod{m_1 m_2}$$

$$x \equiv a_1 \left(\frac{M}{m_1} \right)^{-1}_{m_1} \left(\frac{M}{m_1} \right) + a_2 \left(\frac{M}{m_2} \right)^{-1}_{m_2} \left(\frac{M}{m_2} \right) \pmod{M}$$

$d_2 \equiv 4 \pmod{4}$
 $x \not\equiv \text{not always}$
 $d_2 \equiv 4 \pmod{8}$

$$d_1m_1 + d_2m_2 \not\equiv a_1 \pmod{m_1}$$

$$d_2m_2 \equiv a_1 \pmod{m_1}$$

$$d_2 \equiv \left(m_2^{-1} \right)_{m_1} a_1 \pmod{m_1}$$

let b
 $d_2 \equiv [a_1 + b] \pmod{m_1}$
 have not "applied"

$$(mod m_1)$$

2 When/Why can we use CRT?

Let $a_1, \dots, a_n, m_1, \dots, m_n \in \mathbb{Z}$ where $m_i > 1$ and pairwise relatively prime. In lecture, you've constructed a solution to

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases} A$$

$$M = m_1 \cdot m_2 \cdots m_n$$

- Show the solution is unique modulo M . (Recall that a solution is unique modulo m means given two solutions $x, x' \in \mathbb{Z}$, we must have $x \equiv x' \pmod{m}$)
- Suppose m_i 's are not pairwise relatively prime. Is it guaranteed that a solution exists? Prove or give a counterexample.
- Suppose m_i 's are not pairwise relatively prime and a solution exists. Is it guaranteed that the solution is unique modulo M ? Prove or give a counterexample.

[8 mins]

suppose $\exists x'$ that's also a soln
 WTS: $x - x' \equiv 0 \pmod{M}$
 $x - x' \equiv 0 \pmod{m_i} \quad \forall i \in [n]$

Contradiction:

assume $\exists x'$
 satisfying A, where
 $x' - x \equiv b \pmod{M}$

$b \neq 0 \pmod{M}$
 by def'n of x, x' (so $\exists k$)
 $\Rightarrow x' - x \equiv 0 \pmod{m_j}, \forall j \in [n]$
 subtracting

$$x \equiv a_1 + a_2 M_1$$

$$x = a_1 m_2 + a_2$$

$$(mod m_1) \text{ to}$$

$$a_1 \times b$$

direct proof

1 Modular Practice

Solve the following modular arithmetic equations for x and y .

(a) $9x + 5 \equiv 7 \pmod{11}$.

$$x = 10 \quad 90 \equiv 2 \pmod{11}$$

(b) Show that $3x + 15 \equiv 4 \pmod{21}$ does not have a solution.

(c) The system of simultaneous equations $3x + 2y \equiv 0 \pmod{7}$ and $2x + y \equiv 4 \pmod{7}$.

(d) $13^{2019} \equiv x \pmod{12}$.

$$x = 13^{2019} \pmod{12}$$

(e) $7^{21} \equiv x \pmod{11}$

$$x \equiv 1 \pmod{12}$$

[5 mins + 5 mins]

$7^1 \equiv 7 \pmod{11}$
 $7^2 \equiv 56 \pmod{11}$
 $7^3 \equiv 3 \pmod{11}$
 $7^4 \equiv 9 \pmod{11}$
 $7^5 \equiv 4 \pmod{11}$
 $7^{21} = 7^4 \cdot 7^4 \cdot 7^4 \equiv 7 \times 3 \times 4 \pmod{11}$
 $7^{21} \equiv 84 \pmod{11}$

$$7^{21} = \overline{7^6 \cdot 7^4 \cdot 7^1} \equiv 7 \times 3 \times 1 \pmod{11}$$

$$\boxed{x \equiv 7 \pmod{11}}$$

3 Mechanical Chinese Remainder Theorem (practice)

Solve for $x \in \mathbb{Z}$ where:

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 4 \pmod{7} \end{cases} \quad M = m_1 m_2 m_3$$

Skip ('plug and chug')

$$x \equiv a_1 \left(\frac{M}{m_1} \right) \left(\frac{M}{m_1} \right)^{-1} + \dots$$

Bridge to homework Q:

Prove that for each positive integer n , there are pairwise relatively prime integers k_0, k_1, \dots, k_n all strictly greater than 1, such that $k_0 k_1 \dots k_n - 1$ is the product of two consecutive integers.

~~[...]~~ + end] \rightarrow Names

WTS: $\exists n \in \mathbb{Z}^+, \exists k_0, \dots, k_n > 1$ s.t.

$$\rightarrow k_0 k_1 \dots k_n - 1 = t(t+1)$$

W.T.: Find $k_0, \dots, k_n \in \mathbb{Z}$

$$P(t) = t^2 + t + 1 = K$$

$$P(t) = t^2 + t + 1$$

Find $t \in \mathbb{Z}$

$$\begin{aligned} t &\equiv 0 \pmod{k_0} \\ t &\equiv 1 \pmod{k_1} \\ &\vdots \\ t &\equiv n \pmod{k_n} \end{aligned}$$

$$(P(t) \equiv 0 \pmod{K})$$

If $\exists t \in \mathbb{Z}$ s.t. $P(t) \equiv 0 \pmod{K}$ $\Leftrightarrow \gcd(k_i, k_j) = 1 \forall i, j$

$$\downarrow P(t) \equiv 0 \pmod{K}$$

What if $\exists t_i, i \in \{0, n\}$ s.t.

$$\text{and } P(t) \equiv P(t_i) \equiv 0 \pmod{k_i}$$

find t_i 's s.t.

$$\uparrow \uparrow \rightarrow P(t) \equiv P(t_i) \pmod{k_i}, \forall i \in \{0, n\}$$

are there "n" #s of the form $t^2 + t + 1$ s.t. yes

