Dis 3A: Modular Arithmetic II

Monday, 6 July 2020 10:10 PM

Let's race – use ***any*** technique:

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

What's $x \mod 13 * 17 = 221$?

[3 mins] Type your solution in the chat.

a) 20, 33, 46, ...

b) $x - 7 = 13k, \quad k \in \mathbb{Z}$

$x = 13k + 7$ into b)

$13k + 7 \equiv 4 \pmod{17}$

$13k \equiv -3 \pmod{17}$

$13k \equiv 14 \pmod{17}$

$k \equiv (13^{-1}) * 14 \pmod{17}$ (17 is prime)

$\equiv \ldots$

Thm (The Chinese Remainder Theorem)

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

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

$x \equiv a_1 \pmod{m_1}$

$\vdots$

$x \equiv a_n \pmod{m_n}$

has a solution.

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

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

Where does this come from? [5mins]

Bezout's identity

$\gcd(m_1, m_2) = c_1 m_1 + c_2 m_2 = 1$

c_1 is m_1^{-1} mod m_2; c_2 is m_2^{-1} mod m_1

2 moduli case:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases} \quad M = m_1 m_2$$

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

$\exists \ d_1, d_2 \in \mathbb{Z}$, s.t. $x = d_1 m_1 + d_2 m_2$

WT find d_1, d_2?

$x = d_1 m_1 + d_2 m_2$

$d_1 = 2 \Rightarrow d_1 \equiv 2 \pmod 4$

$d_1 \equiv 1 \mod m_1$

$d_2 \equiv 2 \mod m_2$

normally $d_2 \equiv 0 \pmod 4$

$d_2 \equiv 4 \pmod 4$

2 When/Why can we use CRT?

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

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

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

1. 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 $x \equiv x' \pmod{m}$.)
2. Suppose m_i's are not pairwise relatively prime. Is it guaranteed that a solution exists? Prove or give a counterexample.
3. 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]

1 Modular Practice

Solve the following modular arithmetic equations for x and y.

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

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

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

[5 mins + 5 mins]

$7^{21} = 7^{16} \cdot 7^4 \cdot 7^1 \equiv 7 \times 3 \times 4 \pmod{11}$

$\equiv 84$

$x \equiv 7 \pmod{11}$

3 Mechanical Chinese Remainder Theorem (practice)

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

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 4 \pmod 7 \end{cases}$$

a_1, m_1; a_2, m_2; a_3, m_3

$M = m_1 m_2 m_3 = \ldots$

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

Skip ('plug and chug')

$x \equiv 2\left(35\right)\left(35\right)^{-1}_{3} + 3\left(21\right)\left(21\right)^{-1}_{5} + \ldots$

Bridge to homework Q:

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

$t(t+1)$

[~~Easy~~ + end] Names

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

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

WTS: Find $k_0, \ldots, k_n$ & t

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

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

Find t & Ks

$t \equiv 0 \pmod{k_0}$

$t \equiv \square \pmod{k_1}$

$\vdots$

$t \equiv \square \pmod{k_n}$

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

$\exists t$ s.t. if $P(t) \equiv 0 \pmod{k_i}$, $\gcd(k_i, k_j) = 1$, $i \in [0, n]$

$\Rightarrow k_i \mid P(t)$

$\Rightarrow \prod_{i=0} k_i \mid P(t)$

$P(t) \equiv 0 \pmod k$

What if $\exists\ t_i, i \in [0, n]$ s.t.

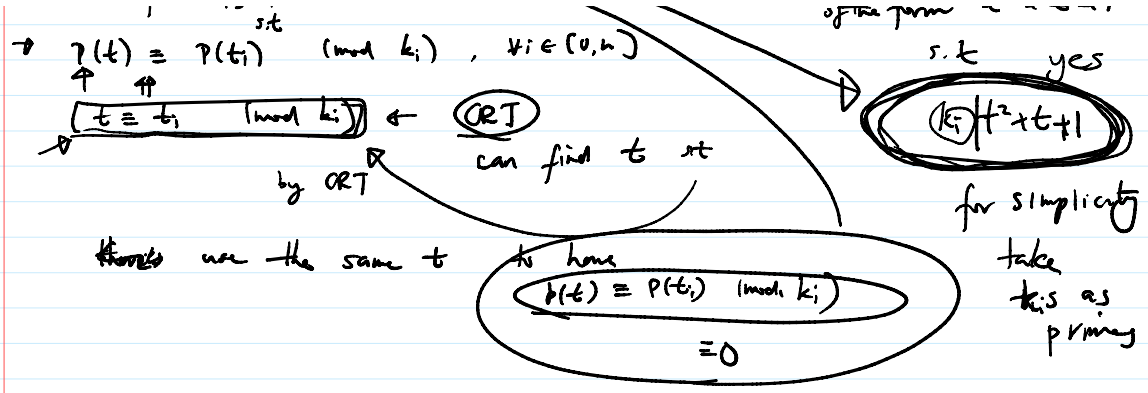
and $P(t) \equiv P(t_i) \equiv 0 \pmod{k_i}$

find t_i's s.t.

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

are there "n" #'s of the form $t^2 + t + 1$ s.t.

yes



$8 \equiv 0 \pmod 4$