Mod Continued

Quick Tips

① → use inverse for solving x

$3x \equiv 1 \mod n$

$(3^{-1})3x \equiv (3^{-1})1 \mod n$

$x \equiv$

② → when $a \equiv b \mod m$ then $[a-b] \equiv 0 \mod m$ or $m \mid (a-b)$ $\Rightarrow$ $\Rightarrow [d \mid a-b]$ $\Rightarrow [a \equiv b \mod d]$

m not prime → but divisors → any divisors of m also divide $a-b$

③ All arithmetic except (division) holds

④ [Simplify]! first under mod m ex $(n > m)$ $n \equiv (b) \mod m$ → exponents → [repeated squaring]

[⑤ $a \equiv b + a \mod m$ apply to all operations]

Questions

[CRT] Chinese remainder thm

↳ the "linear algebra" connection to mod

↳ thing is on [basis] — First def

↳ $a_1 \cdots a_n$ → range

↳ $m_1 \cdots m_n$ → [pairwise coprime] → 3, 5, 7

says $[x \equiv a_1 \mod m_1, \ \vdots, \ x \equiv a_n \mod m_n]$

$M = \prod m_i$ excluded

$x = [(a_1 \cdot b_1) \cdots a_n \cdot b_n] \mod M$ → mod m_1

x · x^{-1} = 1

$\prod m_i$ if 1 · $[\prod m_i]^{-1}$ if 1 · m_1

3, [5, 7]

5, 7 = 0 mod m_i → m_i

① $b_1 \equiv 0 \mod m_i$, $i \neq 1$ → $m_i \mid \prod m_i$ if $i \neq 1$

$[b_1 \equiv 1 \mod m_1]$

$x \cdot x^{-1}$

$X \equiv a_1 \cdot [b_i] \mod m_1$

$X \equiv a_1$

↳ after constructing basis ⇒ linear combination to retrieve x

↳ trick for large mod calc → (split into two primes)

⇒ perform comp on parts

⇒ combine back

basis → (g^3) mod

$g^{100} \mod (77)$

↳ $g^{100} \equiv (a_1) \mod 7$

$g^{100} \equiv (a_2) \mod 11$

↳ $[a_1 \equiv 1]$

$[a_2 \equiv 64^{50} \equiv 9^{50}$

↳ 81^{25}

$\equiv \vdots$

combine with (b_i)

a_1 a_2

find b_1 b_2

$x = a_1 b_1 + a_2 b_2$

1 Modular Practice

Solve the following modular arithmetic equations for x and y.

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

$9x \equiv 7-5$

$9x \equiv 2 \pmod{11}$

$9^{-1} \equiv$

$9 \cdot a \equiv 1 \pmod{11}$

45 (5) $\rightarrow 9^{-1} \pmod{11}$

$(9 \cdot 5)x \equiv 2 \cdot 5 \pmod{11}$

$1 \quad x \equiv 10 \pmod{11}$

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

$3x + 15 \equiv 4 \pmod{21}$

$\gcd(21,3) \neq 1$

[can't have inverse]

$-21 \qquad -11$

$-11 = -21 + 10$

$[3x \equiv [-11] \pmod{21}]$

10

$3x \equiv 10 \pmod{21}$

$(3x \equiv 10 \pmod{3})$

[3 divisor of 21]

$3x \not\equiv 1 \pmod{3}$

$\equiv 0 \qquad 0$

proof contra

$2 \qquad 8-0$

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

$[2(2x+y) - 3x + 2y] \equiv x \equiv 8-0 \pmod{7}$

1

$3 + 2y \equiv 0 \pmod{7} \qquad x \equiv 1$

$y = 2$

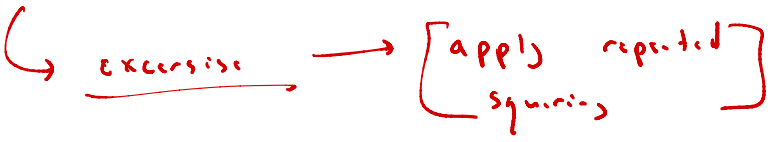
(d) $13^{2019} \equiv x \pmod{12}$.

simplify

$13^1 \equiv 1 \pmod{12} \qquad 13^2 \equiv 1 \quad \ldots$

$13^{2019} \equiv 1 \pmod{12}$

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



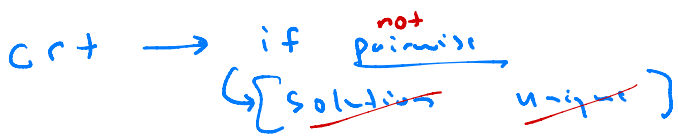
2 When/Why can we use CRT?

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

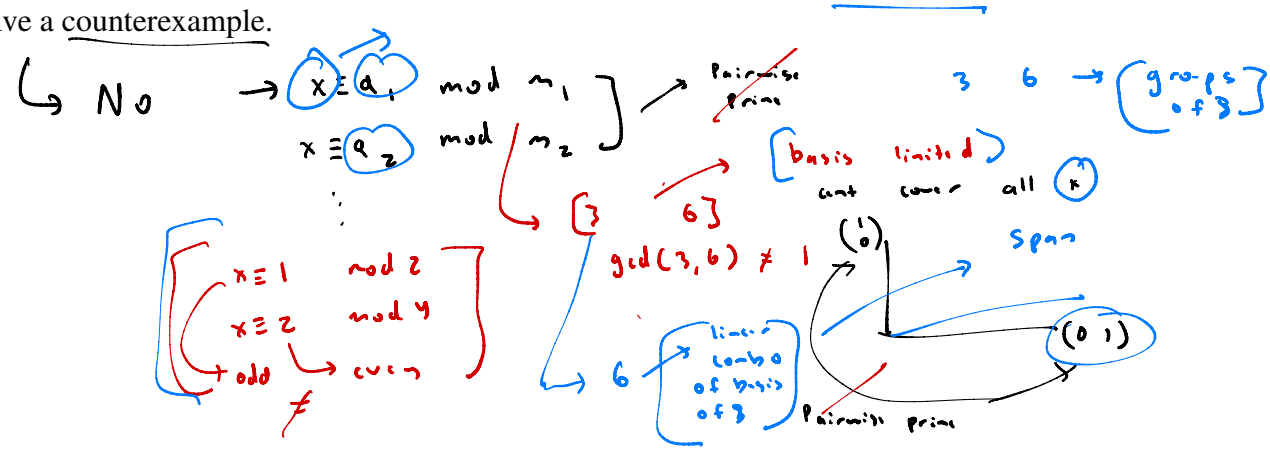
$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ &\vdots \\ x &\equiv a_n \pmod{m_n}. \end{aligned}$$

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

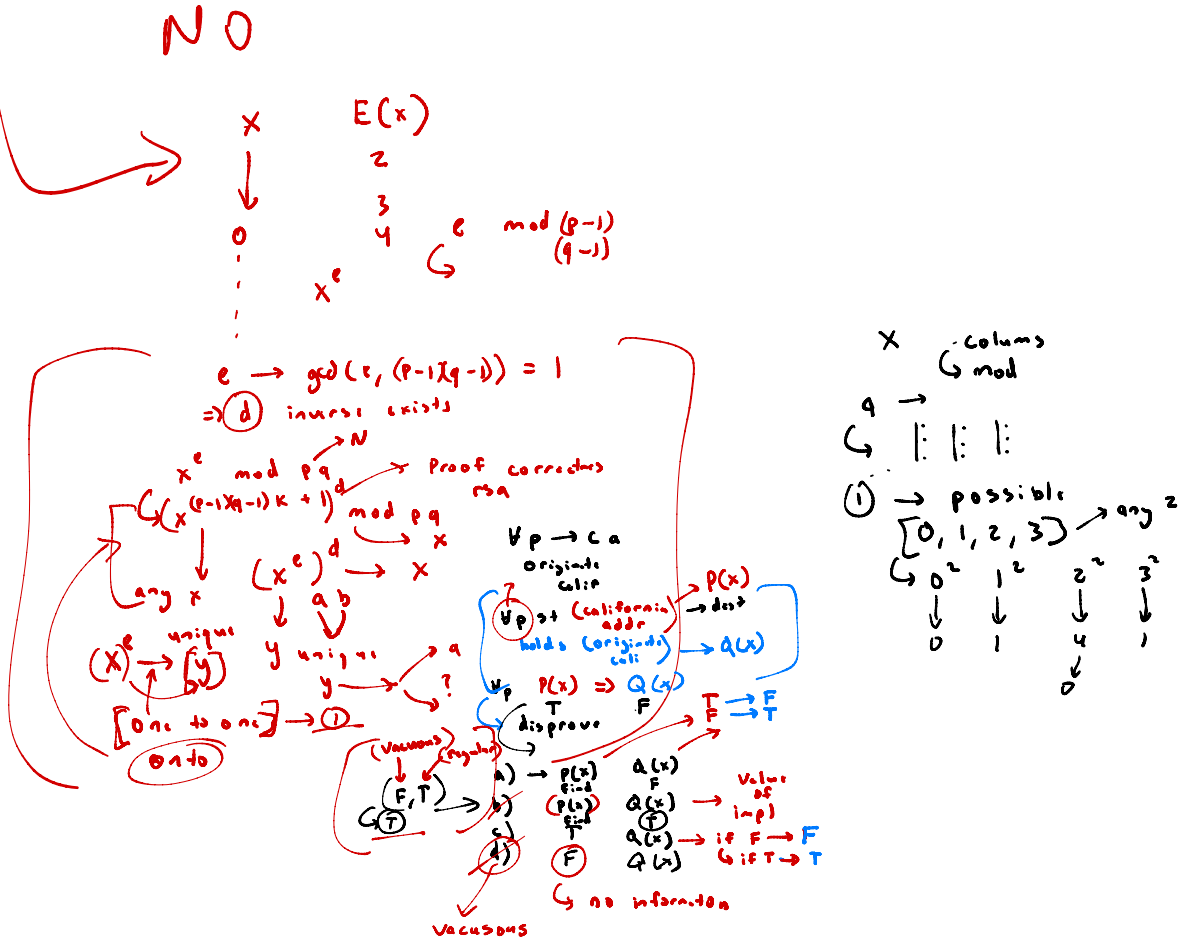
1. Show the solution is unique modulo m. (Recall that a solution is unique modulo m means given two solutions $x, x' \in \mathbb{Z}$, we must have $x \equiv x' \pmod{m}$.)



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.



3 Mechanical Chinese Remainder Theorem

In this problem, we will solve for x such that

$$\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \end{aligned}$$

(a) Find a number $0 \leq b_2 < 30$ such that $b_2 \equiv 1 \pmod 2$, $b_2 \equiv 0 \pmod 3$, and $b_2 \equiv 0 \pmod 5$.

(b) Find a number $0 \leq b_3 < 30$ such that $b_3 \equiv 0 \pmod 2$, $b_3 \equiv 1 \pmod 3$, and $b_3 \equiv 0 \pmod 5$.

(c) Find a number $0 \leq b_5 < 30$ such that $b_5 \equiv 0 \pmod 2$, $b_5 \equiv 0 \pmod 3$, and $b_5 \equiv 1 \pmod 5$.

(d) What is x in terms of b_2, b_3, and b_5? Evaluate this to get a numerical value for x.