CS 70 Discrete Mathematics and Probability Theory
Summer 2020 Course Notes **DIS 3A**

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

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

$$x' \equiv a_1 \pmod{m_1}$$
$$\vdots$$
$$x' \equiv a_n \pmod{m_n}.$$

$x \equiv 2 \pmod 3$
$x \equiv 4 \pmod 7$

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 $x \equiv x' \pmod{m}$.)

Assume $\exists x' : x \not\equiv x' \pmod{m}$

$m_i \mid (x - x')$ $\quad (x - x') \equiv 0 \mod m_i \ \forall i$

$\hookrightarrow m \mid (x - x')$

$x - x' = km \pmod{m}$

$\Rightarrow x' - x \equiv 0 \mod m$

$x' \equiv x \mod m$

$m_1 \mid x,\ m_2 \mid x,\ m_3 \mid x, \ldots, m_n \mid x$

$\Rightarrow m \mid x$

$12 \equiv 0 \mod 6$

$18 \equiv 0 \mod 6$

$p \mid x,\ q \mid x \ \gcd(p, q) = 1 \Rightarrow pq \mid x$

2. Suppose m_i's are not pairwise relatively prime. Is it guaranteed that a solution exists? Prove or give a counterexample.

$x \equiv 1 \mod 2$

$x \equiv 2 \mod 4$

0 1 2 3 4 5 6 7

0 1 2 3 4 5

$x \equiv 5 \pmod 7$
$x \equiv 2 \pmod 5$
$x \equiv 3 \pmod 9$

$x \equiv 3 \bmod 6$
$x \equiv 6 \bmod 9$

3, 9, 15, 21, 27, 33, 39,
45, 51

① Unique $x \bmod 315$

② $x = a_1 b_1 + a_2 b_2 + a_3 b_3 \bmod (315)$
$= 45(5\times5) + 63(2\times2) + 35(3\times8) \bmod (315)$
$= 2217 \bmod (315) = \boxed{12} \bmod 315$

$45(25) + 63(4) + 35(24) \bmod (315)$

$a_1 = 5, \quad a_2 = 2, \quad a_3 = 3$

$45(25) + \cancel{63(4)} + \cancel{35(24)} \bmod 7$
$= 3\cdot4 = 12 = 5 \bmod 7$

$b_1 = ((5\times9)^{-1} \bmod 7)(5\times9)$
$= 45^{-1} \bmod 7$
$= 3^{-1} \bmod 7$
$= 5 \bmod 7$

$\cancel{45(25)} + 63(4) + \cancel{35(24)} \bmod 5$
$= 63\times4 = 3\times4 = 12 = 2 \bmod 5$

$b_2 = (7\times9)^{-1} \bmod 5 = 3^{-1} \bmod 5 = (2)63$

$b_3 = (7\times5)^{-1} \bmod 9 = 8 \bmod 9 = (8)35$

$\cancel{45(25)} + \cancel{63(4)} + 35(24) \bmod 9$
$= 8\times6 = 48 = 3 \bmod 9$

$m = m_1 \cdot m_2 \cdot m_3 \cdots m_n$

2.1 Assume $\exists x' : x' \not\equiv x \pmod m$
and x' satisfies all congruences.
We have,
$x \equiv a_i \bmod m_i \ \forall i$
$x' \equiv a_i \bmod m_i \ \forall i$

$x \equiv x' \pmod{m_i} \forall i$
$\Rightarrow x \equiv x' \pmod m$
need to prove

Consider
$x - x' \equiv a_i - a_i \equiv 0 \pmod{m_i} \ \forall i$
$\Rightarrow m_i \mid (x - x') \ \forall i$
$\Rightarrow m \mid (x - x')$ ∵ m_i's are pairwise coprime
$\Rightarrow x - x' \equiv 0 \bmod m$
$\Rightarrow x' \equiv x \pmod m$
Contra!

$4 \equiv 0 \bmod 2$
$6 \equiv 0 \bmod 2$

$2 \mid 12 \qquad 2 \mid 4$
$3 \mid 12 \qquad 4 \mid 4$
$6 \mid 12 \qquad 8 \mid 4$

$m_1 = 2$

$m_2 = 5$

$m_3 = 9$

$x = 180$

$2 \mid 180$

$5 \mid 180$

$9 \mid 180$

$90 \mid 180$

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.

$x \equiv 0 \mod 2$

$x \equiv 2 \mod 4$

$2, 6 \mod 8$

3 Mechanical Chinese Remainder Theorem (practice)

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

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 4 \pmod 7$$

(a) Find the multiplicative inverse of 5×7 modulo 3.

(b) What is the smallest $a \in \mathbb{Z}^+$ such that $5 \mid a$, $7 \mid a$, and $a \equiv 2 \pmod 3$?

(c) Find the multiplicative inverse of 3×7 modulo 5.

(d) What is the smallest $b \in \mathbb{Z}^+$ such that $3 \mid b$, $7 \mid b$, and $b \equiv 3 \pmod 5$?

(e) Find the multiplicative inverse of 3×5 modulo 7.

(f) What is the smallest $c \in \mathbb{Z}^+$ such that $3 \mid c$, $5 \mid c$, and $c \equiv 4 \pmod 7$?

(g) Write down the set of solutions for the system of equations.