CS 70 Discrete Mathematics and Probability Theory
Summer 2017 Hongling Lu, Vrettos Moulos, and Allen Tang **DIS 07B**

1 More Chinese Remainder Theorem

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

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

(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.

2 Count and Prove

(a) Over 1000 students walked out of class and marched to protest the war. To count the exact number of students protesting, the chief organizer lined the students up in columns of different length. If the students are arranged in columns of 3, 5, and 7, then 2, 3, and 4 people are left out, respectively. What is the minimum number of students present? Solve it with Chinese Remainder Theorem.

(b) Prove that for $n \geq 1$, if $935 = 5 \times 11 \times 17$ divides $n^{80} - 1$, then 5, 11, and 17 do not divide n.

3 RSA Practice

Consider the following RSA schemes and solve for asked variables.

(a) Assume for an RSA scheme we pick 2 primes $p = 5$ and $q = 11$ with encryption key $e = 9$, what is the decryption key d? Calculate the exact value.

(b) If the receiver gets 4, what was the original message?

(c) Encode your answer from part (b) to check its correctness.

4 RSA Lite

Woody misunderstood how to use RSA. So he selected prime $P = 101$ and encryption exponent $e = 67$, and encrypted his message m to get $35 = m^e \bmod P$. Unfortunately he forgot his original message m and only stored the encrypted value 35. But Carla thinks she can figure out how to recover m from $35 = m^e \bmod P$, with knowledge only of P and e. Is she right? Can you help her figure out the message m? Show all your work.