COL202: Discrete Mathematical Structures **Spring 2024**

Tutorial Sheet 5

Announced on: Jan 31 (Wed)

1. Based on Problem 9.60 in [LLM17].

   In this problem , we will prove the *Chinese remainder theorem* which says that if one knows the remainders obtained by dividing an integer x by several integers, then one can determine uniquely the remainder of the division of x by the product of these integers under the condition that the divisors are pairwise coprime.[1]

   Formally, let $a > 1$ and $b > 1$ be coprime. The *Chinese remainder theorem* states that for all integers m and n, there is an integer x such that

   $$x \equiv m \pmod{a} \tag{1}$$

   $$x \equiv n \pmod{b} \tag{2}$$

   and x is unique up to congruence modulo ab. That is, any x' that satisfies Equations (1) and (2) must also satisfy

   $$x' \equiv x \pmod{ab}.$$

   a) Prove that for any integers m and n, there exists some x that simultaneously satisfies Equations (1) and (2).

   b) Prove that

   $$x \equiv 0 \pmod{a} \wedge x \equiv 0 \pmod{b} \implies x \equiv 0 \pmod{ab}.$$

   c) Prove that

   $$x \equiv x' \pmod{a} \wedge x \equiv x' \pmod{b} \implies x \equiv x' \pmod{ab}.$$

   d) With the help of parts (a), (b), and (c), prove the statement of Chinese remainder theorem.

2. Based on Problem 9.82 in [LLM17].

   In this problem, we will implement the RSA scheme on a small scale.

   a) Generating the public and private keys.

      - Choose two distinct primes numbers p and q in the range $10 - 40$, and let $n = pq$.
      - Choose a small odd number e that is relatively prime to $\phi(n)$.

[1] The problem appears in the work of Chinese mathematician Sun-tzu, who asked "There are certain things whose number is unknown. If we count them by threes, we have two left over; by fives, we have three left over; and by sevens, two are left over. How many things are there?" [Wik].

- Find d, the inverse of e modulo $\phi(n)$. Explain the method you used to compute d.

b) Encode each of the numbers in the set $\{2, 7, 11, 13\}$ separately as your message m (thus, you will send four different messages).

c) In each case, decrypt the message and verify whether or not you received the original message m.

References

[LLM17] Eric Lehman, Tom Leighton, and Albert R Meyer. *Mathematics for Computer Science*. 2017. URL: https://courses.csail.mit.edu/6.042/spring18/mcs.pdf.

[Wik] Wikipedia article on "Chinese Remainder Theorem" (Accessed: Feb 2023). URL: https://en.wikipedia.org/wiki/Chinese_remainder_theorem.