Elementary Number Theory Part 3 (Supplementary)

CRT and DHKE (Supplementary)

MZI

School of Computing
Telkom University

SoC Tel-U

June 2023

Acknowledgements

This slide is composed based on the following materials:

1. *Discrete Mathematics and Its Applications*, 8th Edition, 2019, by K. H. Rosen (main).
2. *Discrete Mathematics with Applications*, 5th Edition, 2018, by S. S. Epp.
3. *Mathematics for Computer Science*. MIT, 2010, by E. Lehman, F. T. Leighton, A. R. Meyer.
4. Slide for Matematika Diskret 2 (2012). Fasilkom UI, by B. H. Widjaja.
5. Slide for Matematika Diskret 2 at Fasilkom UI by Team of Lecturers.
6. Slide for Matematika Diskret. Telkom University, by B. Purnama.

Some of the pictures are taken from the above resources. This slide is intended for academic purpose at FIF Telkom University. If you have any suggestions/comments/questions related to the material on this slide, send an email to `<pleasedontspam>@telkomuniversity.ac.id`.

Contents

Contents

Motivation: Counting The Remainder of Division

Notice the following story.

Problem

An old man who sells mangos wants to count how many mangos remained in the shop. The old man is not sure about the exact amount, but he knows that:

1. if the remaining number of mangos is divided by 3, then the remainder is 2;
2. if the remaining number of mangos is divided by 5, then the remainder is 3;
3. the remaining number of mangos is between 100 and 120.

Can you determine the exact number of remaining mangos?

Mathematical Model of the Problem

Suppose the number of mango is x, then we have the following mathematical model:

1. if the number of mango is divided by 3, then the remainder is 2;

Mathematical Model of the Problem

Suppose the number of mango is x, then we have the following mathematical model:

1. if the number of mango is divided by 3, then the remainder is 2;
   if x is divided by 3, then the remainder is 2; thus we have $x \bmod 3 = 2$, or $x \equiv 2 \pmod 3$;
2. if the number of mango is divided by 5, then the remainder is 3;

Mathematical Model of the Problem

Suppose the number of mango is x, then we have the following mathematical model:

1. if the number of mango is divided by 3, then the remainder is 2;
   if x is divided by 3, then the remainder is 2; thus we have $x \bmod 3 = 2$, or $x \equiv 2 \pmod 3$;
2. if the number of mango is divided by 5, then the remainder is 3;
   if x is divided by 5, then it the remainder is 3; thus we have $x \bmod 5 = 3$, or $x \equiv 3 \pmod 5$;

Mathematical Model of the Problem

Suppose the number of mango is x, then we have the following mathematical model:

1. if the number of mango is divided by 3, then the remainder is 2;
   if x is divided by 3, then the remainder is 2; thus we have $x \bmod 3 = 2$, or $x \equiv 2 \pmod 3$;
2. if the number of mango is divided by 5, then the remainder is 3;
   if x is divided by 5, then it the remainder is 3; thus we have $x \bmod 5 = 3$, or $x \equiv 3 \pmod 5$;
3. the number of mango is between 100 and 120, or $100 \leq x \leq 120$.

As a result, we have to look for x that satisfies:

$$x \equiv 2 \pmod 3 \quad (1)$$
$$x \equiv 3 \pmod 5 \quad (2)$$

with $100 \leq x \leq 120$. Two linear congruences (1 and 2) form a system of linear congruences.

Finding a Solution of a System of Linear Congruences

From (1) we have

$$x \equiv 2 \pmod 3 \text{, then } x = 3s + 2 \text{, for } s \in \mathbb{Z},$$

by substituting this value to (2), that is $x \equiv 3 \pmod 5$, we have

Finding a Solution of a System of Linear Congruences

From (1) we have

$$x \equiv 2 \pmod 3 \text{, then } x = 3s + 2 \text{, for } s \in \mathbb{Z},$$

by substituting this value to (2), that is $x \equiv 3 \pmod 5$, we have

$$3s + 2 \equiv 3 \pmod 5$$

Finding a Solution of a System of Linear Congruences

From (1) we have

$$x \equiv 2 \pmod 3 \text{, then } x = 3s + 2 \text{, for } s \in \mathbb{Z},$$

by substituting this value to (2), that is $x \equiv 3 \pmod 5$, we have

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

Finding a Solution of a System of Linear Congruences

From (1) we have

$$x \equiv 2 \pmod 3 \text{, then } x = 3s + 2, \text{ for } s \in \mathbb{Z},$$

by substituting this value to (2), that is $x \equiv 3 \pmod 5$, we have

$$\begin{aligned} 3s + 2 &\equiv 3 \pmod 5 \\ 3s &\equiv 1 \pmod 5 \\ s &\equiv 2 \pmod 5, \end{aligned}$$

consequently $s = 5t + 2$ for $t \in \mathbb{Z}$. By substituting this value to our original equation, we obtain

$$x =$$

Finding a Solution of a System of Linear Congruences

From (1) we have

$$x \equiv 2 \pmod 3 \text{, then } x = 3s + 2, \text{ for } s \in \mathbb{Z},$$

by substituting this value to (2), that is $x \equiv 3 \pmod 5$, we have

$$\begin{aligned} 3s + 2 &\equiv 3 \pmod 5 \\ 3s &\equiv 1 \pmod 5 \\ s &\equiv 2 \pmod 5, \end{aligned}$$

consequently $s = 5t + 2$ for $t \in \mathbb{Z}$. By substituting this value to our original equation, we obtain

$$x = 3s + 2 =$$

Finding a Solution of a System of Linear Congruences

From (1) we have

$$x \equiv 2 \pmod 3 \text{, then } x = 3s + 2, \text{ for } s \in \mathbb{Z},$$

by substituting this value to (2), that is $x \equiv 3 \pmod 5$, we have

$$\begin{aligned} 3s + 2 &\equiv 3 \pmod 5 \\ 3s &\equiv 1 \pmod 5 \\ s &\equiv 2 \pmod 5, \end{aligned}$$

consequently $s = 5t + 2$ for $t \in \mathbb{Z}$. By substituting this value to our original equation, we obtain

$$x = 3s + 2 = 3(5t + 2) + 2 = 15t + 8,$$

or the solution is $x \equiv 8 \pmod{15}$. Observe $8 \equiv 2 \pmod 3$ and $8 \equiv 3 \pmod 5$. Then, since $105 \equiv 0 \pmod{15}$, we can choose $x =$

Finding a Solution of a System of Linear Congruences

From (1) we have

$$x \equiv 2 \pmod 3 \text{, then } x = 3s + 2, \text{ for } s \in \mathbb{Z},$$

by substituting this value to (2), that is $x \equiv 3 \pmod 5$, we have

$$\begin{aligned} 3s + 2 &\equiv 3 \pmod 5 \\ 3s &\equiv 1 \pmod 5 \\ s &\equiv 2 \pmod 5, \end{aligned}$$

consequently $s = 5t + 2$ for $t \in \mathbb{Z}$. By substituting this value to our original equation, we obtain

$$x = 3s + 2 = 3(5t + 2) + 2 = 15t + 8,$$

or the solution is $x \equiv 8 \pmod{15}$. Observe $8 \equiv 2 \pmod 3$ and $8 \equiv 3 \pmod 5$. Then, since $105 \equiv 0 \pmod{15}$, we can choose $x = 105 + 8 = 113 \equiv 8 \pmod{15}$.

System of Linear Congruences with Three Conditions

The problem of linear congruences with three conditions has been explained since the Ancient Chinese dynasty by Sun-Tsu. In this slide we will discuss on how to solve a system of linear congruences with three or more conditions.

Image taken from img5.epochtimes.com/i6/80118052019l974.jpg.

General Xin Han's Warrior

Problem

General Xin Han lead a force of 1500 warriors. After the battle, between $400 - 500$ of the warriors died. To ensure the number of dead warriors, he asked his warriors to:

1. form a group of 3 warriors; it turns out there are 2 warriors who have no group at all;
2. form a group of 5 warriors; it turns out there are 3 warriors who have no group at all;
3. form a group of 7 warriors; it turns out there are 2 warriors who have no group at all.

Based on the above information, determine the exact number of the warriors left alive.

Mathematical Model

From the previous problem, we can obtain a system of linear congruences as follows

$$x \equiv 2 \pmod 3 \tag{3}$$
$$x \equiv 3 \pmod 5 \tag{4}$$
$$x \equiv 2 \pmod 7, \tag{5}$$

x must satisfy $1000 \leq x \leq 1100$.

Finding x

The integer x that simultaneously satisfies (3), (4), and (5) can be found by *back substitution method* with these following steps:

Finding x

The integer x that simultaneously satisfies (3), (4), and (5) can be found by *back substitution method* with these following steps:

- From (3), we obtain $3 \mid (x-2)$, hence $x = 3s + 2$, for $s \in \mathbb{Z}$.

Finding x

The integer x that simultaneously satisfies (3), (4), and (5) can be found by *back substitution method* with these following steps:

- From (3), we obtain $3 \mid (x-2)$, hence $x = 3s + 2$, for $s \in \mathbb{Z}$.
- By substituting $x = 3s + 2$ to (4), we obtain

$$\begin{aligned} 3s + 2 &\equiv 3 \pmod 5 \\ 3s &\equiv 1 \pmod 5 \\ s &\equiv 2 \pmod 5 \ \text{(since } 3^{-1} \equiv 2 \pmod 5\text{)}. \end{aligned}$$

Finding x

The integer x that simultaneously satisfies (3), (4), and (5) can be found by *back substitution method* with these following steps:

- From (3), we obtain $3 | (x-2)$, hence $x = 3s + 2$, for $s \in \mathbb{Z}$.
- By substituting $x = 3s + 2$ to (4), we obtain

$$\begin{aligned} 3s + 2 &\equiv 3 \pmod 5 \\ 3s &\equiv 1 \pmod 5 \\ s &\equiv 2 \pmod 5 \text{ (since } 3^{-1} \equiv 2 \pmod 5 \text{)}. \end{aligned}$$

- In other words $5 | (s-2)$ or $s = 5t + 2$, for $t \in \mathbb{Z}$.

Finding x

The integer x that simultaneously satisfies (3), (4), and (5) can be found by *back substitution method* with these following steps:

- From (3), we obtain $3 | (x-2)$, hence $x = 3s + 2$, for $s \in \mathbb{Z}$.
- By substituting $x = 3s + 2$ to (4), we obtain

$$\begin{aligned} 3s + 2 &\equiv 3 \pmod 5 \\ 3s &\equiv 1 \pmod 5 \\ s &\equiv 2 \pmod 5 \text{ (since } 3^{-1} \equiv 2 \pmod 5 \text{)}. \end{aligned}$$

- In other words $5 | (s-2)$ or $s = 5t + 2$, for $t \in \mathbb{Z}$.
- As a result, $x = 3s + 2 = 3(5t+2) + 2 = 15t + 8$. By substituting $x = 15t + 8$ to (5) we obtain

$$\begin{aligned} 15t + 8 &\equiv 2 \pmod 7 \text{, since } 15t + 8 \equiv t + 1 \pmod 7 \text{, then} \\ t + 1 &\equiv 2 \pmod 7 \\ t &\equiv 1 \pmod 7 . \end{aligned}$$

Finding x

The integer x that simultaneously satisfies (3), (4), and (5) can be found by *back substitution method* with these following steps:

- From (3), we obtain $3 | (x-2)$, hence $x = 3s + 2$, for $s \in \mathbb{Z}$.
- By substituting $x = 3s + 2$ to (4), we obtain

$$\begin{aligned} 3s + 2 &\equiv 3 \pmod 5 \\ 3s &\equiv 1 \pmod 5 \\ s &\equiv 2 \pmod 5 \text{ (since } 3^{-1} \equiv 2 \pmod 5 \text{)}. \end{aligned}$$

- In other words $5 | (s-2)$ or $s = 5t + 2$, for $t \in \mathbb{Z}$.
- As a result, $x = 3s + 2 = 3(5t+2) + 2 = 15t + 8$. By substituting $x = 15t + 8$ to (5) we obtain

$$\begin{aligned} 15t + 8 &\equiv 2 \pmod 7 \text{, since } 15t + 8 \equiv t + 1 \pmod 7 \text{, then} \\ t + 1 &\equiv 2 \pmod 7 \\ t &\equiv 1 \pmod 7 . \end{aligned}$$

- Hence, $7 | (t-1)$ or $t = 7u + 1$, for $u \in \mathbb{Z}$.

- We obtain $x = 15t + 8 = 15\,(7u + 1) + 8 = 105u + 23$ or $105 \big| \,(x - 23)$, so $x \equiv 23 \,(\mathrm{mod}\, 105)$.

- We obtain $x = 15t + 8 = 15\,(7u + 1) + 8 = 105u + 23$ or $105 \mid (x - 23)$, so $x \equiv 23 \pmod{105}$.
- The solution of x that satisfies (3), (4), and (5) are all $x \in \mathbb{Z}$ such that $x \equiv 23 \pmod{105}$. Notice that $105 = 3 \cdot 5 \cdot 7$.
- $1000 \leq x \leq 1100$, observe

$$\begin{aligned} 1050 &\equiv 0 \pmod{105}, \text{ so} \\ 1073 &\equiv 23 \pmod{105}. \end{aligned}$$

- We obtain $x = 15t + 8 = 15\,(7u + 1) + 8 = 105u + 23$ or $105 \mid (x - 23)$, so $x \equiv 23 \pmod{105}$.
- The solution of x that satisfies (3), (4), and (5) are all $x \in \mathbb{Z}$ such that $x \equiv 23 \pmod{105}$. Notice that $105 = 3 \cdot 5 \cdot 7$.
- $1000 \leq x \leq 1100$, observe

$$\begin{aligned} 1050 &\equiv 0 \pmod{105}, \text{ so} \\ 1073 &\equiv 23 \pmod{105}. \end{aligned}$$

- So, there are 1073 warriors left alive.

The Chinese Remainder Theorem

Theorem (Chinese Remainder Theorem)

Given integers $m_1, m_2, \ldots, m_n$ that are larger than 1 and relatively prime ($\gcd(m_i, m_j) = 1$ for all $i \neq j$), if $a_1, a_2, \ldots, a_n \in \mathbb{Z}$, then the system of linear congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

has a unique solution in modulo $m = m_1 m_2 \cdots m_n$ (on the other words, there is one $x \in \mathbb{Z}_m$ that satisfies the system of linear congruence).

Content

Mutual Password Problem

Problem

Alice and Bob want to make an account whose password can be known only by them. The password consists of six digit of decimal numbers. At first, they want to make the password together somewhere, but they cannot meet because of the distance. When they want to discuss the password by phone/chat, they are afraid that Eve, their enemy, hacks into their conversation. Can Alice and Bob make a password together without any meeting and explicit explanation of the password by phone/text?

Diffie-Hellman Key Exchange

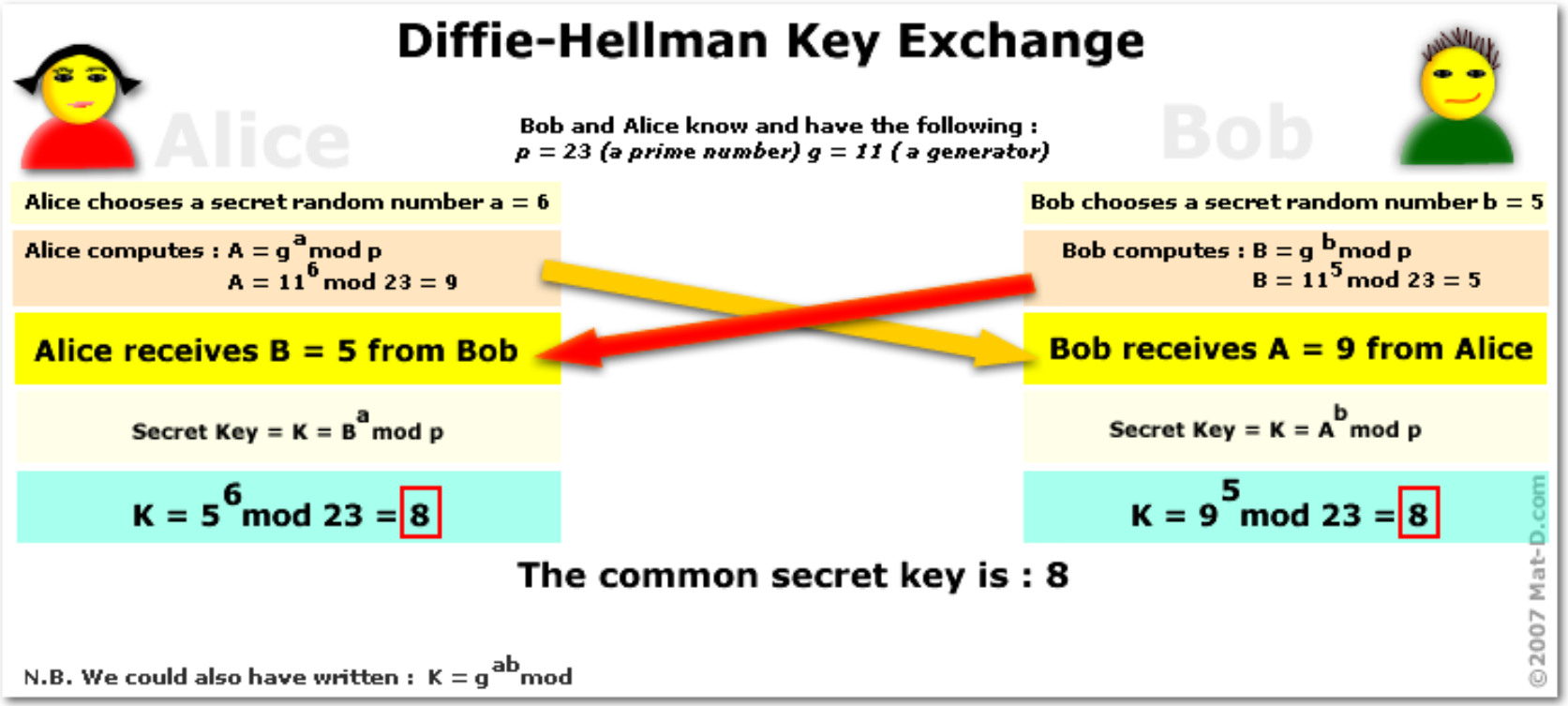

Image taken from http://matdonline.free.fr/img/diffieHellman.png.

Formal Explanation on The Diffie-Hellman Key Exchange

<table>
<tr><th colspan="2">Public Parameters</th></tr>
<tr><td colspan="2">A trusted party chooses and announces:
the set $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$ with p is a prime number
and a number $g \in \mathbb{Z}_p^*$ with: $\forall h \in \mathbb{Z}_p^* \; \exists k \in \mathbb{N}_0 \left(g^k = h\right)$</td></tr>
<tr><th colspan="2">Private Key</th></tr>
<tr><th>Alice</th><th>Bob</th></tr>
<tr><td>Choose number $a \in [0, p-1]$</td><td>Choose number $b \in [0, p-1]$</td></tr>
<tr><th colspan="2">Key Exchange</th></tr>
<tr><td>Alice computes $A = g^a \bmod p$
Alice send A to Bob.</td><td>Bob computes $B = g^b \bmod p$.
Bob send B to Alice.</td></tr>
<tr><th colspan="2">Computation of the mutual key</th></tr>
<tr><th>Alice</th><th>Bob</th></tr>
<tr><td>Alice computes $A' = B^a \bmod p$</td><td>Bob computes $B' = A^b \bmod p$</td></tr>
<tr><td colspan="2">The mutual key is $A' = B'$.</td></tr>
</table>

The Correctness of Diffie-Hellman Key Exchange

Observe that

$$\begin{aligned} A' &= B^a \bmod p = \left(g^b \bmod p\right)^a \bmod p = g^{ba} \bmod p, \\ B' &= A^b \bmod p = \left(g^a \bmod p\right)^b \bmod p = g^{ab} \bmod p, \end{aligned}$$

since $ab = ba$, then $A' = B'$.