# Discrete Mathematics Assignment 3

12312706 Zhou Liangyu

1. $\because ac \mid bc$

   $\therefore k \cdot ac = bc.$

   $\therefore k \cdot a = b.$

   $\therefore a \mid b.$

2. (a) $-2024 \div 33 = -62.$

   (b) $(20234 - 2024) \bmod 25 = 18210 \bmod 25 = 10.$

   (c) $94232 \cdot 2982 \bmod 7 = [(94232 \bmod 7)(2982 \bmod 7)] \bmod 7 = (5 \cdot 0) \bmod 7 = 0.$

3. (a) $(11011)_2 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = (27)_{10}.$

   (b) $(101\ 100)_2 = (54)_8.$

   (c) $(AE01F)_{16} = (1010\ 1110\ 0000\ 0001\ 1111)_2.$

   (d) $(720235)_8 = (111\ 010\ 000\ 010\ 011\ 101)_2 = (0011\ 1010\ 0000\ 1001\ 1101)_2 = (3A09D)_{16}.$

4. (a) $8085 = 5 \cdot 1617 = 3 \cdot 5 \cdot 539 = 3 \cdot 5 \cdot 7 \cdot 77 = 3 \cdot 5 \cdot 7 \cdot 7 \cdot 11.$

   (b) $12! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 5 \cdot 5 \cdot 7 \cdot 11.$

5. (a) $267 = 3 \cdot 79 + 30$

   $79 = 2 \cdot 30 + 19$

   $30 = 1 \cdot 19 + 11$

   $19 = 1 \cdot 11 + 8$

   $11 = 1 \cdot 8 + 3$

   $8 = 2 \cdot 3 + 2$

   $3 = 1 \cdot 2 + 1$

   $2 = 2 \cdot 1 + 0$

   $\therefore gcd(267, 79) = 1.$

   (b) $1 = 3 - 1 \cdot 2$

   $= 3 \cdot 3 - 1 \cdot 8$

   $= 3 \cdot 11 - 4 \cdot 8$

   $= 7 \cdot 11 - 4 \cdot 19$

   $= 7 \cdot 30 - 11 \cdot 19$

   $= 29 \cdot 30 - 11 \cdot 79$

   $= 29 \cdot 267 - 98 \cdot 79$

   $\therefore gcd(267, 79) = 29 \cdot 267 - 98 \cdot 79$. The Bézout coefficients of 267 and 79 are $29$ and $-98$.

   (c) $\because 267 \cdot 29 \equiv 1 \pmod{79}$

   $\therefore x \equiv 29 \cdot 267x \equiv 29 \cdot 3 \equiv 87 \equiv 8 \pmod{79}.$

   (d) Using Euclidean Algorithm to calculate $gcd(252, 356)$:

   $356 = 1 \cdot 252 + 104$

   $252 = 2 \cdot 104 + 44$

$104 = 2 \cdot 44 + 16$

$44 = 2 \cdot 16 + 12$

$16 = 1 \cdot 12 + 4$

$12 = 3 \cdot 4 + 0$

$\therefore gcd(252, 356) = 4,\ q_1 = 1,\ q_2 = 2,\ q_3 = 2,\ q_4 = 2,\ q_5 = 1,\ q_6 = 3.$

$\because s_0 = 1,\ s_1 = 0,\ t_0 = 0,\ t_1 = 1$

$\therefore s_2 = s_0 - s_1 q_1 = 1 - 0 \cdot 1 = 1,\ t_2 = t_0 - t_1 q_1 = 0 - 1 \cdot 1 = -1,$

$s_3 = s_1 - s_2 q_2 = 0 - 1 \cdot 2 = -2,\ t_3 = t_1 - t_2 q_2 = 1 - (-1) \cdot 2 = 3,$

$s_4 = s_2 - s_3 q_3 = 1 - (-2) \cdot 2 = 5,\ t_4 = t_2 - t_3 q_3 = (-1) - 3 \cdot 2 = (-7),$

$s_5 = s_3 - s_4 q_4 = (-2) - 5 \cdot 2 = -12,\ t_5 = t_3 - t_4 q_4 = 3 - (-7) \cdot 2 = 17,$

$s_6 = s_4 - s_5 q_5 = 5 - (-12) \cdot 1 = 17,\ t_6 = t_4 - t_5 q_5 = (-7) - 17 \cdot 1 = -24.$

$\therefore 4 = gcd(252, 356) = (-24) \cdot 252 + 17 \cdot 356.$

(e) According to Euclidean Algorithm, we have:

$a = q_1 \cdot b + r_1,$

$b = q_2 \cdot r_1 + r_2,$

$r_1 = q_3 \cdot r_2 + r_3,$

...

$r_i = q_{i+2} \cdot r_{i+1} + r_{i+2}$

In the process, $q_{i+2} \geq 1$, $r_{i+1} > r_{i+2}$.

If $r_{i+2} \geq \frac{r_i}{2}$, then $r_{i+1} < \frac{r_i}{2}$, i.e. $r_{i+1} < r_{i+2}$, which contradicts to $r_{i+1} > r_{i+2}$.

$\therefore r_{i+2} < \frac{r_i}{2}$.

$\therefore$ After every two steps, $r_i$ will be reduced to $\frac{r_i}{2}$ at most.

In worst-case, $a$ and $b$ are coprime with $b = a - 1$. Considering $b$ as $r_0$, we need $2 \cdot log_2 b$ steps to reduce $b$ to $1$.

$\therefore$ The time complexity is $O(log\ b)$.

6. Let $c_1 = \frac{c}{gcd(b,c)}$, $b_1 = \frac{b}{gcd(b,c)}$.

$\because c \mid ab$ i.e. $gcd(b, c) \cdot c_1 \mid a \cdot gcd(b, c) \cdot b_1$, $c_1$ and $b_1$ are coprime.

$\therefore c_1 \mid a$.

$\therefore c_1 \cdot gcd(b, c) \mid a \cdot gcd(b, c)$.

$\therefore c \mid a \cdot gcd(b, c)$.

7. (a) Assume that $b$ and $c$ are both inverse of $a$ modulo $m$, i.e. $ba \equiv 1 \pmod{m}$ and $ca \equiv 1 \pmod{m}$.

$\therefore ba \equiv ca \pmod{m}$.

$\therefore b \equiv c \pmod{m}$.

$\therefore$ Every other inverse of $a$ modulo m is congruent to $\overline{a}$ modulo $m$.

(b) Assume that if $gcd(a, m) > 1$ for positive integers $a$ and $m$, then $a$ still have inverse modulo $m$.

$\because \exists \overline{a}$ s.t. $\overline{a}a \equiv 1 \pmod{m}$

$\therefore \overline{a}a = k \cdot m + 1\ (k \in \mathbb{Z})$.

$\therefore 1 = \overline{a}a - k \cdot m$, which contradicts to $gcd(a, m) > 1$.

$\therefore$ If $gcd(a, m) > 1$ for positive integers $a$ and $m$, then $a$ does *not* have an inverse modulo $m$.

8. (a) $\because a \equiv b \pmod{m_1},\ a \equiv b \pmod{m_2},\ \ldots,\ a \equiv b \pmod{m_n}$

$\therefore (a - b) \equiv 0 \pmod{m_1},\ (a - b) \equiv 0 \pmod{m_2},\ \ldots,\ (a - b) \equiv 0 \pmod{m_n}$.

$\therefore a-b=k_1m_1=k_2m_2= \ \dots \ =k_nm_n.$

Consider $m_1$ and $m_2$:

$\because k_1m_1=k_2m_2$, $m_1$ and $m_2$ are coprime.

$\therefore \frac{k_1m_1}{m_2}=k_2,\ m_2 \mid k_1.$

Let $k_1=qm_2$, then $a-b=k_1m_1=qm_1m_2$, i.e. $a\equiv b \pmod{m_1m_2}$.

Extend to $m_n$:

Assume that when $n=k$, $a\equiv b \pmod{m_1m_2\dots m_k}$. Let $M=m_1m_2\dots m_k$.

When $n=k+1$, obviously $M$ and $m_{k+1}$ are coprime.

$\therefore a\equiv b \pmod{M\cdot m_{k+1}}$, i.e. $a\equiv b \pmod{m_1m_2\dots m_{k+1}}$.

$\therefore a\equiv b \pmod{m_1m_2\dots m_n}$ holds for any $n$.

$a\equiv b \pmod m$, where $m=m_1m_2\cdots m_n$.

9. (a) $\because 6=2\cdot 3,\ 10=2\cdot 5,\ 35=5\cdot 7$

$5 \bmod 2=1,\ 5 \bmod 3=2,\ 3 \bmod 2=1,\ 3 \bmod 5=3,\ 8 \bmod 5=3,\ 8 \bmod 7=1$

$\therefore x\equiv 1 \pmod 2,\ x\equiv 2 \pmod 3,\ x\equiv 3 \pmod 5,\ x\equiv 1 \pmod 7.$

(b) $\therefore M=m_1m_2m_3m_4=2\cdot 3\cdot 5\cdot 7=210.$

$\therefore M_1=\frac{M}{m_1}=\frac{210}{2}=105,\ M_1=\frac{M}{m_2}=\frac{210}{3}=70,\ M_1=\frac{M}{m_3}=\frac{210}{5}=42,\ M_4=\frac{M}{m_4}=\frac{210}{7}=30.$

$\therefore 105y_1\equiv 1 \pmod 2,\ 70y_2\equiv 1 \pmod 3,\ 42y_3\equiv 1 \pmod 5,\ 30y_4\equiv 1 \pmod 7.$

$\therefore y_1=1,\ y_2=1,\ y_3=3,\ y_4=4.$

$$\begin{aligned}\therefore x&=a_1M_1y_1+a_2M_2y_2+a_3M_3y_3+a_4M_4y_4\\&=1\cdot 105\cdot 1+2\cdot 70\cdot 1+3\cdot 42\cdot 3+1\cdot 30\cdot 4\\&=105+140+378+120\\&=743.\end{aligned}$$

Let $x_0$ represents the smallest nonnegative integer solution for the new system,

then $x_0=x \bmod M=743 \bmod 210=113.$

$\therefore$ All solutions for the new system can be represented by $x=k\cdot M+x_0=210k+113.$

10. (a) Assume that $m\cdot a\equiv n\cdot a \pmod p$, $m\neq n$, $m,\ n<p$.

$\therefore (m-n)\cdot a\equiv 0 \pmod p.$

$\therefore p\mid(m-n)$ or $p\mid a$, which contradicts to $p$ is prime and $p\nmid a$.

$\therefore$ *No* two of the integers $1\cdot a, 2\cdot a,\dots,(p-1)a$ are congruent modulo $p$.

(b) Let $\mathbb{Z}_p^+=\{1,2,\dots,p-1\}$, then $Z_i=i, i\in[1,p-1]$.

$\therefore gcd(Z_i,p)=1.$

$\because p\nmid a$

$\therefore gcd(a\cdot Z_i,p)=1.$

$\therefore (a\cdot Z_i) \bmod p\in[1,p-1].$

According to (a), for every $m\neq n$, $a\cdot Z_m\not\equiv a\cdot Z_n \pmod p$.

$\therefore \{x|x=Z_i \bmod p,\ i\in[1,p-1]\}=\{x|x=(a\cdot Z_i) \bmod p,\ i\in[1,p-1]\}=\mathbb{Z}_p^+.$

$\therefore Z_1Z_2\dots Z_{p-1}=(aZ_1 \bmod p)(aZ_2 \bmod p)\dots(aZ_{p-1} \bmod p).$

$\therefore (Z_1Z_2\dots Z_{p-1}) \bmod p=[(aZ_1 \bmod p)(aZ_2 \bmod p)\dots(aZ_{p-1} \bmod p)] \bmod p.$

$\therefore (Z_1Z_2\dots Z_{p-1}) \bmod p=(aZ_1\cdot aZ_2\cdot\dots\cdot aZ_{p-1}) \bmod p.$

$\therefore (p-1)!\equiv a^{p-1}(p-1)! \pmod p.$

(c) $\because p$ is prime, i.e. $p \nmid (p-1)!$

$\therefore$ We can simply divide $(p-1)!$ on both sides of $(p-1)! \equiv a^{p-1}(p-1)! \pmod{p}$.

$\therefore a^{p-1} \equiv 1 \pmod{p}$.

(d) If $a$ is divisible by $p$: $a^p \equiv 0 \pmod{p}$, $a^p \equiv 0 \pmod{p}$. $\therefore a^p \equiv a \pmod{p}$.

If $not$: Applying congruences of products to $a^{p-1} \equiv 1 \pmod{p}$, we can get $a^p \equiv a \pmod{p}$.

11. (a) $\because 2023 = 337 \cdot 6 + 1$.

$\therefore 5^{2023} = (5^6)^{337} \cdot 5 \equiv 5 \pmod{7}$.

$\therefore 5^{2023} \bmod 7 = 5 \bmod 7 = 5$.

(b) $n = 15 \to p = 3,\ q = 5$.

$\therefore \varphi(n) = (p-1)(q-1) = 2 \cdot 4 = 8$.

$\because 2023 = 252 \cdot 8 + 7$

$\therefore 8^{2023} = (8^8)^{252} \cdot 8^7 \equiv 8^7 \pmod{15}$.

$\because 8^7 \bmod 15 = [(8^2)^3 \cdot 8] \bmod 15 = [(64 \bmod 15)^3 \cdot (8 \bmod 15)] \bmod 15 = (4^3 \cdot 8) \bmod 15 = 2$

$\therefore 8^{2023} \bmod 15 = 8^7 \bmod 15 = 2$.

12. (a) $C = M^e \bmod n = 8^7 \bmod 65 = [(8^2 \bmod 65)^3(8 \bmod 65)] \bmod 65 = [(-1)^3 \cdot (-57)] \bmod 65 = 57$.

(b) $n = 65 \to p = 5, q = 13$

$\therefore \varphi(n) = (p-1)(q-1) = 4 \cdot 12 = 48$.

Using Euclidean Algorithm:

$48 = 6 \cdot 7 + 6$

$7 = 1 \cdot 6 + 1$

Using Bézout Theorem:

$1 = 7 - 1 \cdot 6$

$= 7 \cdot 7 - 1 \cdot 48$

$\because ed \equiv 1 (\bmod\ n)$

$\therefore d = 7$.

(c) $M = C^d \bmod n = 57^7 \bmod 65 = [(57^2 \bmod 65)^3(57 \bmod 65)] \bmod 65 = [(-1)^3 \cdot (-8)] \bmod 65 = 8$.