Assignment 3 12212726

Q1. $a c \mid b c \Rightarrow \exists$ integer k s.t. $bc = kac$

1°. $b = 0$. Since $a \neq 0$, we know $a \mid b$ obviously.

2°. $b \neq 0$. $bc = kac \Rightarrow b = ka \Rightarrow a \mid b$

Q2. (a) $-2023 = -62 \times 33 + 23$ $\therefore -2023 \text{ div } 33 = -62$

(b) $(20234 - 2023) \bmod 25 = 18211 \bmod 25 = 11$

(c) $94232 \cdot 2982 \bmod 7$

$= 94232 \,;_7\, 2982$

$= 5 \cdot 0$

$= 0$

Q3. (a) $(11011)_2 = 1\times 2^4 + 1\times 2^3 + 0\times 2^2 + 1\times 2^1 + 1\times 2^0 = 27$

(b) $(101100)_2 = (54)_8$ since $(101)_2 = 5_8$ and $(100)_2 = (4)_8$

(c) $(AE01F)_{16} = (10101110000000011111)_2$ since

$A = (1010)_2$, $E = (1110)_2$, $F = (1111)_2$

(d) $(720235)_8 = (111\ 010\ 000\ 010\ 011\ 101)_2$

$= (3A09D)_{16}$

Q4. (a) $8085 = 5 \times 1617 = 5 \times 3 \times 539 = 5 \times 3 \times 7 \times 77$

$8085 = 3^1 \cdot 5^1 \cdot 7^2 \cdot 11^1$

(b) $12! = 2 \cdot 3 \cdot 2^2 \cdot 5 \cdot 2 \cdot 3 \cdot 7 \cdot 2^3 \cdot 3^2 \cdot 2 \cdot 5 \cdot 11 \cdot 2^2 \cdot 3$

$= 2^{10} \cdot 3^5 \cdot 5^2 \cdot 7^1 \cdot 11^1$

Q5. (a) $267 = 79 \times 3 + 30$

$79 = 30 \times 2 + 19$

$30 = 19 \times 1 + 11$

$19 = 11 \times 1 + 8$

$11 = 8 \times 1 + 3$

$8 = 3 \times 2 + 2$

$3 = 2 \times 1 + 1$

$1 = 1 \times 1 + 0$ $\therefore \gcd(267, 79) = 1$

(b) $\gcd(267, 79) = 1 = 3 - 2\times 1$

$= 3\times 3 - 8$

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

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

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

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

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

29 and -98 are desired.

(c) $267x \equiv 3 \pmod{79}$

According to (b): $\overline{267} = 29$

$x \equiv \overline{267}\, 267 x \equiv 29 \cdot 3 \pmod{79}$

$\Rightarrow \quad x \equiv 87 \pmod{79}$

(d)

Q6. Prime factor b into $b = b_1 b_2 \cdots b_m$, then $c \mid a b_1 b_2 \cdots b_m$

$\gcd(b, c) = g_1 . g_2 \cdots g_p$

Prime factor $\frac{b}{\gcd(b,c)}$ into $\frac{b}{\gcd(b,c)} = \frac{b_1 b_2 \cdots b_m}{g_1 g_2 \cdots g_p} = h_1 h_2 \cdots h_q$

$b = (g_1 g_2 \cdots g_p) \cdot (h_1 h_2 \cdots h_q)$

$$\left.\begin{array}{l} \text{I. } g_i \text{ and } h_i \text{ are primes} \\ \text{II. } g_i \mid c \wedge h_i \nmid c \end{array}\right\} \Rightarrow \gcd(h_i, c) = 1$$

By corollary, we know that for each h_i, $i \in \{1, 2, 3 \cdots q\}$

$$\left.\begin{array}{l} \text{I. } \gcd(h_i, c) = 1 \\ \text{II. } c = \mid a (g_1 g_2 \cdots g_p) \cdot (h_1 h_2 \cdots h_q) \end{array}\right\} \Rightarrow c \mid a (g_1 g_2 \cdots g_p)$$

Which is as the same as $c \mid a \gcd(b, c)$

Q7. (a) Assume two arbitary inverses of $a \bmod m$ are $\overline{a_1}$ and $\overline{a_2}$. We have $\gcd(a,m)=1$

$\overline{a_1}a \equiv 1 \pmod m \wedge \overline{a_2}a \equiv 1 \pmod m$

$\because \gcd(a,m)=1$

$\therefore \overline{a_1} \equiv \frac{1}{a} \pmod m$

$\because 1 \equiv a\overline{a_2} \pmod m$

$\therefore \overline{a_1} \equiv \frac{1}{a} \cdot a\overline{a_2} \pmod m$

Also $\overline{a_1} \equiv \overline{a_2} \pmod m$

Assign $\overline{a}$ to $\overline{a_1}$, then we know every $\overline{a_i}$ is congruent to $\overline{a} \bmod m$

(b) Suppose $\overline{a}$ is the inverse of $a \bmod m$

Then $\overline{a}a \equiv 1 \pmod m$, which means there $\exists k \in \mathbb{Z}$

$\overline{a}a + km = 1 \Rightarrow a = -\frac{k}{\overline{a}}m + \frac{1}{\overline{a}}$. $|\frac{1}{\overline{a}}| < 1$

According to Euclidean Algorithm, since $|\frac{1}{\overline{a}}| < 1$

we know $\gcd(a,m)=1$.

This contradict to $\gcd(a,m)>1$

Q8. (a) For each m_i s.t. $a \equiv b \pmod{m_i}$:

We know $m_i | a-b$. $i \in \{1,2,3 \dots n\}$

$$\begin{cases} m_i | a-b \\ m_j | a-b \end{cases} \Rightarrow \begin{cases} a-b = k_i m_i \\ a-b = k_j m_j \end{cases} \qquad a-b = ?\, m_i m_j$$

$\gcd(m_i, m_j) = 1 \Rightarrow p_i m_i + p_j m_j = 1$. $p_i, p_j \in \mathbb{Z}$

$\Rightarrow p_i m_i k_j + p_j m_j k_j = k_j$

$\Rightarrow p_i m_i k_j + p_j m_i k_i = k_j$

$\Rightarrow m_i(p_i k_j + p_j k_i) = k_j$

$a-b = k_j m_j = m_i(p_i k_j + p_j k_i) m_j = (p_i k_j + p_j k_i) m_i m_j$

$\therefore m_i m_j | (a-b)$, $i \neq j$

Obviously, $\gcd(m_t, \prod_{i \neq t} m_i) = 1$

$\therefore m | (a-b)$

(b) Suppose x and y are solutions:

$$\left.\begin{array}{l} x \equiv a_i \pmod{m_i} \\ y \equiv a_i \pmod{m_i} \end{array}\right\} \Rightarrow \quad x \equiv y \pmod{m_i}$$

From (a), we know $x \equiv y \pmod{m}$, $m = \prod_{i=1}^{n} m_i$

It shows x and y are the same.

Thus, the solution is unique.

Q9. (a) $x \equiv 5 \pmod 6 \Rightarrow \begin{cases} x \equiv a_1 \pmod 2 \\ x \equiv a_2 \pmod 3 \\ 6k_1 + 5 = 3a_1 + 4a_2 \end{cases} \Rightarrow \begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \end{cases}$

$x \equiv 3 \pmod{10} \Rightarrow \begin{cases} x \equiv a_3 \pmod 2 \\ x \equiv a_4 \pmod 5 \\ 10k_2 + 3 = 5a_3 + 6a_4 \end{cases} \Rightarrow \begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 3 \pmod 5 \end{cases}$

$x \equiv 8 \pmod{35} \Rightarrow \begin{cases} x \equiv a_3 \pmod 5 \\ x = a_4 \pmod 7 \\ 35k_3 + 8 = 21a_3 + 15a_4 \end{cases} \Rightarrow \begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 8 \pmod 7 \\ x \equiv 1 \pmod 7 \end{cases}$

$$\therefore \quad \begin{array}{l} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 1 \pmod 7 \end{array}$$

(b) $m = 2 \cdot 3 \cdot 5 \cdot 7 = 210$

$1 \cdot 105 \equiv 1 \pmod 2$

$1 \cdot 70 \equiv 1 \pmod 3$

$3 \cdot 42 \equiv 1 \pmod 5$

$4 \cdot 30 \equiv 1 \pmod 7$

$\therefore x = 1 \cdot 1 \cdot 105 + 2 \cdot 1 \cdot 70 + 3 \cdot 3 \cdot 42 + 1 \cdot 4 \cdot 30 \equiv 743 \equiv 113 \equiv \pmod{210}$

$\therefore x \equiv 113 \pmod{210}$

Q10.

(a) Let $a = kp + b$, where $b \in (0, p)$, then for arbitary two of those integers ia and ja, where $i, j \in \{1, 2, \cdots p-1\}$

$(ia - ja) \equiv (i-j)a \equiv (i-j)(kp+b) \equiv (i-j)b \pmod p$

$|i-j| \in \{1, 2, \cdots p-2\}$

$b \in \{1, 2 \cdots p-1\}$

Prime factor $(i-j)b$, we can find that every factors are smaller than p. Also means $(i-j)b$ doesn't have p as factor since p is prime.

$\therefore (i-j) \bmod p \neq 0 \quad \therefore (ia - ja) \bmod p \neq 0$

$\therefore$ No two of these integers are congruent modulo p.

(b) List the equation and simplify every equations so that $i_n \in [1, p-1]$

$1a \equiv i_1 \pmod p$

$2a = i_2 \pmod p$

$(\cdots)$

$na = i_n \pmod p$

$(\cdots)$

$(p-1)a = i_{p-1} \pmod p$

From (a), we know that $i_s \neq i_t$ for $s \neq t$

i_s range from 1 to p-1 without repeation.

$\therefore \prod_{j=1}^{p-1} i_j = (p-1)!$

And $\prod_{j=1}^{p-1} = ja = (p-1)!\, a^{p-1}$

Thus, $(p-1)! \equiv (p-1)!\, a^{p-1} \pmod p$

(c) Prime factor $(p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-1)$

$= p_1 p_2 \cdots p_n,\ p_i < p$ since p is prime

$p = 1 \cdot p \quad \wedge \quad p \nmid (p-1)!$

$\therefore \gcd(p, (p-1)!) = 1$ ①

From (b), we know $(p-1)! \equiv a^{p-1}(p-1)! \pmod p$ ②

From ① and ②, we know $1 \equiv a^{p-1} \pmod p$

(d) I. $p \mid a$

Obviously: $p \mid a^{p-1}$

$\therefore a \bmod p = a^{p-1} \bmod p = 0$

$\therefore a^p \equiv a \pmod p$

II. $p \nmid a$

From (c), we know $a^{p-1} \equiv 1 \pmod p$

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

Q11. (a) $5^{2023} \equiv (5^6)^{337} \cdot 5^1 \pmod 7) \equiv 1^{337} \cdot 5^1 \pmod 7)$

$\equiv 5 \pmod 7$ since $7 \nmid 5$

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

(b) $\phi(15) = (3-1)(5-1) = 8$

$\therefore a^{\phi(15)} \equiv a^8 \equiv 1 \pmod{15}$

$8^{2023} \equiv (8^8)^{252} \cdot 8^2 \equiv 1^{252} \cdot 8^2 \equiv 64 \equiv \pmod{15}$

$\therefore 8^{2023} \bmod 15 = 4$

Q12. (a) $\phi(n) = \phi(65) = 4 \times 12 = 48$

$\gcd(e, \phi(n)) = \gcd(7, 48) = 1$

$ed \equiv 1 \equiv 7d \pmod{48} \Rightarrow d = 7$

$C = M^e \bmod n = 8^7 \bmod 65 = 57$

(b) $d = 7$

(c) $M = C^d \bmod n = 57^7 \bmod 65 = 8$