(iii) $36x \equiv 38 \pmod{22}$

BW HW

Divide by 2:

$18x \equiv 19 \pmod{11} \equiv 8 \pmod{11}$

$\gcd(18, 11) = 1$

$$\left(\begin{array}{cc|c} 1 & 0 & 11 \\ 0 & 1 & 18 \end{array}\right) \sim \left(\begin{array}{cc|c} 5 & -3 & 1 \\ * & * & * \end{array}\right)$$

$5 \cdot 11 + (-3) \cdot 18 = 1$

$-3 \cdot 18x \equiv -3 \cdot 8 \equiv 8^2 = 64 \pmod{11}$

$x \equiv 64 \equiv 9 \pmod{11}$

$x = 9 + 11t, \quad t \in \mathbb{Z}$

The second congruence:

$143x \equiv 187 \pmod{35}$

$\gcd(143, 35) = 1$

$$\left(\begin{array}{cc|c} 1 & 0 & 143 \\ 0 & 1 & 35 \end{array}\right) \sim \left(\begin{array}{cc|c} 12 & -49 & 1 \\ * & * & * \end{array}\right)$$

$12 \cdot 143 + (-49) \cdot 35 = 1$

$12 \cdot 143 \equiv 1 \pmod{35}$

$12 = 143^{-1} \pmod{35}$

$x \equiv 12 \cdot 187 \pmod{35} \equiv$

$\equiv 12 \cdot 12 \equiv 144 \equiv 4 \pmod{35}$

$x = 4 + 35t, \quad t \in \mathbb{Z}$

(v)

HW

$$3x \equiv 4 \pmod{11}$$
$$6x \equiv 3 \pmod{13}$$
$$9x \equiv 2 \pmod{17}$$

$\gcd(3, 11) = 1$

$4 \cdot 3 \equiv 1 \pmod{11}$

$4 \cdot 3x \equiv 4 \cdot 4 = 16 \equiv 5 \pmod{11}$

$x \equiv 5 \pmod{11}$

$\gcd(6, 13) = 1$

$(-2) \cdot 6 = -12 \equiv 1 \pmod{13}$

$-2 \cdot 6x \equiv -6 \equiv 7 \pmod{13}$

$x \equiv 7 \pmod{13}$

$\gcd(9, 17) = 1$

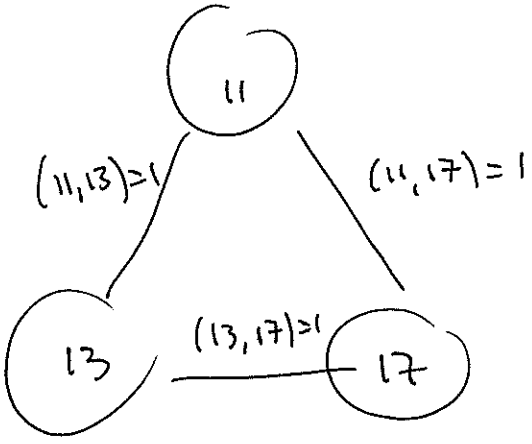
$2 \cdot 9 \equiv 1 \pmod{17}$

$2 \cdot 9x \equiv 4 \pmod{17}$

$x \equiv 4 \pmod{17}$

Thus:

$$\begin{cases} x \equiv 5 \pmod{11} \\ x \equiv 7 \pmod{13} \\ x \equiv 4 \pmod{17} \end{cases}$$



$m_1 = 11 \quad k_1 = 13 \cdot 17 = 221 \quad n_1 = 1 \quad a_1 = 5$

$m_2 = 13 \quad k_2 = 11 \cdot 17 = 187 \quad n_2 = -5 \quad a_2 = 7$

$m_3 = 17 \quad k_3 = 11 \cdot 13 = 143 \quad n_3 = 5 \quad a_3 = 4$

$221 \cdot 1 + 11(-20) = 221 - 220 = 1$

$(-5)187 + 13 \cdot 72 = -935 + 936 = 1$

$5 \cdot 143 + (-42) \cdot 17 = 715 - 714 = 1$

The solution

$$b = 5 \cdot 1 \cdot 221 + 7 \cdot (-5) \cdot 187 + 4 \cdot 5 \cdot 143 =$$

$$= 1105 - 6545 + 2860 =$$

$$= 3965 - 6545 = -2580 \pmod{11 \cdot 13 \cdot 17} =$$

$$= -2580 \pmod{2431} \equiv -149 \pmod{2431} \equiv$$

$$\equiv 2282 \pmod{2431}$$

$$b = 2282 + 2431t, \quad t \in \mathbb{Z}$$

Problem 4:

HW (i) $875 = 5 \cdot 155 = 5^2 \cdot 31$

$$\phi(875) = (5^2 - 5) \cdot 30 = 20 \cdot 30 = 600$$

~~$\phi(1331) = 1330$~~ $\quad 1331 = 11^3$

$$\phi(1331) = 11^3 - 11^2 = 1331 - 121 =$$

$$= 1210$$

$$109512 = 3 \cdot 36504 = 3^2 \cdot 12168 =$$

$$= 3^2 \cdot 3 \cdot 4056 = 3^3 \cdot 3 \cdot 1352 = 3^4 \cdot 2 \cdot 676$$

$= 3^4 \cdot 2^2 \cdot 338 = 3^4 \cdot 2^3 \cdot 169 = 3^4 \cdot 2^3 \cdot 13^2$ (13)

$\phi(109512) = \phi(2^3)\phi(3^4)\phi(13^2) =$

$= (2^3 - 2^2)(3^4 - 3^3)(13^2 - 13) =$

$= 2^2(2-1)3^3(3-1)13(13-1) =$

$= 4 \cdot 1 \cdot 27 \cdot 2 \cdot 13 \cdot 12 =$

$= 4 \cdot 27 \cdot 26 \cdot 12 = 33696$

(ii) $a, m \in \mathbb{Z}$, $m > 0$, $\gcd(a, m) = 1$

Euler: $a^{\phi(m)} \equiv 1 \pmod{m}$.

BW

□ $k = \phi(m)$

$T = \{x \in \mathbb{Z} \mid 1 \leq x \leq m \ \& \ \gcd(m, x) = 1\}$

Then $T = \{r_1, r_2, \ldots, r_k\}$

Let $S = \{ar_1, ar_2, \ldots, ar_k\}$.

If $i \neq j$ then $ar_i \not\equiv ar_j \pmod{m}$

(otherwise $r_i = r_j$ since $\gcd(a, m) = 1$).

Then $S \equiv T \pmod{m}$ $\Rightarrow$

$(ar_1)(ar_2)\cdot\ldots\cdot(ar_k) \equiv r_1 r_2 \cdot\ldots\cdot r_k \pmod{m}$

$a^{\phi(m)} r_1 r_2 \cdot\ldots\cdot r_k \equiv r_1 r_2 \cdot\ldots\cdot r_k \pmod{m}$

$$a^{\varphi(m)} \equiv 1 \pmod m$$

because $\gcd(r_1 r_2 \cdots r_k, m) = 1$.

q.e.d.

(iii) $4^6 \equiv 1 \pmod 7$ (Euler)

HW $4^{42} = (4^7)^6 \equiv 4^6 \equiv 1 \pmod 7$ (Euler)

$294 = 49 \cdot 6$

$4^{294} = (4^6)^{49} \equiv 1^{49} = 1 \pmod 7$

$4 + 4^6 + 4^{42} + 4^{294} \equiv 4 + 1 + 1 + 1 = 7 \equiv$

$\equiv 0 \pmod 7$.

(iv) for any $d \mid m$ let

HW $C_d = \{ x \in \mathbb{Z} \mid 1 \le x \le m \ \& \ \gcd(x, m) = d \}$

(for example $\#C_1 = \varphi(m)$).

Then $C_d \cap C_{d'} = \emptyset$ for any two divisors d and d', and $\bigcup_{d \mid m} C_d = \{1, 2, \ldots, m\}$.

Hence

$m = \sum_{d \mid m} \#C_d$. But

$x \in C_d \iff 1 \le x \le m$ & $\gcd(x, m) = d$

$\iff 1 \le \frac{x}{d} \le \frac{m}{d}$ and $\gcd\left(\frac{x}{d}, \frac{m}{d}\right) = 1$

$\Rightarrow \quad \# C_d = \phi\left(\frac{m}{d}\right)$, so that

$$m = \sum_{d|m} \# C_d = \sum_{d|m} \phi\left(\frac{m}{d}\right) =$$

$$= \sum_{d|m} \phi(d) .$$

Problem 5 :

(i) Let $|a|_m$ be the order of ~~One~~ ~~in~~ an integer a modulo m, where $m \in \mathbb{Z}$ and $m > 0$. Then $|a|_m \le \phi(m)$ by Euler's theorem.

BW

Let $\phi(m) = q \cdot |a|_m + r$, for some $0 \le r < |a_m|$.

Then, if $r \neq 0$, we get

$$a^{\phi(m)} = \left(a^{|a|_m}\right)^q \cdot a^r \equiv 1 \cdot a^r = a^r \pmod m$$

$$\| \quad \Rightarrow a^r \equiv 1 \pmod m$$

$1 \pmod m$

Since $r < |a|_m$ - contradiction

(ii) Let $m \in \mathbb{Z}$, $m > 0$.

HW Let g be a primitive root modulo m. We have to show that $g^s \equiv g^t \pmod m \Leftrightarrow s \equiv t \pmod{\phi(m)}$

Well, if $g^s \equiv g^t$ then, without loss of generality, $s \geq t$. Since g is a primitive root, then $\gcd(g, m) = 1 \Rightarrow \exists\, g^{-1} \pmod m$.

Let $g^{-t} = (g^{-1})^t \bmod (m)$.

Then:

$$g^{s-t} \equiv 1 \pmod m$$

$\Rightarrow |g|_m$ divides $s - t$.

But $|g|_m = \phi(m)$ as g is a prim. root. $\Rightarrow$

$$s \equiv t \pmod{\phi(m)},$$

Conversely, if $s \equiv t \pmod{\phi(m)}$ then $s = t + l \cdot \phi(m) \Rightarrow$

$$\Rightarrow g^s = \left(g^{\phi(m)}\right)^l \cdot g^t \equiv 1 \cdot g^t = g^{t \pmod m}$$

(iii) Suppose $\exists\ i, j \in \{0,1,2,\dots,\phi(m)-1\}$ such that $i \neq j$ and

$$g^i \equiv g^j \pmod m.$$

Then $i \equiv j \pmod{\phi(m)}$. Since $i, j \leq \phi(m)-1 \Rightarrow i = j$ — contradiction.

$\Rightarrow \{g^0, g^1, \dots, g^{\phi(m)-1}\} \equiv \{r_1, r_2, \dots, r_{\phi(m)}\} \pmod m$.

(iv) Let $k = |2|_{11}$. Then $k \mid \phi(11)$.

Since $\phi(11) = 11-1 = 10$ we have that k is either 2, or 5, or 10. But $2^2 = 4 \not\equiv 1 \pmod{11}$ and $2^5 = 32 \not\equiv 1 \pmod{11}$

Therefore $|2|_{11} = 10 = \phi(11) \Rightarrow$

$\Rightarrow 2$ is a prim. root.

Hence, if x is a solution, then

$x = 2^z$ where $z \in \{0,1,2,\dots,9\}$

HW

$$8x^3 \equiv 7 \pmod{11}$$

$$8(2^z)^3 \equiv 7 \pmod{11}$$

$$2^3 \cdot (2^z)^3 \equiv 7 \equiv -4 = -2^2 \pmod{11}$$

$$2^{3+3z} \equiv (-1)\cdot 2^2 \pmod{11}$$

$$2^{3(1+z)} \equiv 2^5 \cdot 2^2 \pmod{11} \quad \text{as } 2^5 \equiv -1 \pmod{11}$$

$$2^{3(1+z)} \equiv 2^{7} \pmod{11}$$

$$3(1+z) \equiv 7 \pmod{10}$$

$$3+3z \equiv 7 \pmod{10}$$

$$3z \equiv 4 \pmod{10}$$

$\gcd(3,10) = 1$

$1 \cdot 10 + (-3) \cdot 3 = 10 - 9 = 1$

$$-3 \cdot 3z \equiv -3 \cdot 4 \pmod{10}$$

$$z \equiv -12 \pmod{10}$$

$$z \equiv 8 \pmod{10}$$

$\Rightarrow z = 8 + 10t, \; t \in \mathbb{Z}.$

Since z must be taken from the set $\{0, 1, 9, \ldots, 9\}$ we have only one possibility

$$z = 8$$

$$\Rightarrow x \equiv 2^{8} \pmod{11}.$$

$$x \equiv 3 \pmod{11}$$

Indeed

$$8 \cdot 3^{3} = 8 \cdot 27 \equiv 8 \cdot 5 = 40 \equiv 7 \pmod{11}$$

Problem 6:

(i) $m = rs$, $r, s > 2$, $m > 0$

BW $\gcd(r, s) = 1$

$a \in \mathbb{Z}$, $\gcd(a, m) = 1$

$$a^{\frac{1}{2}\phi(m)} = a^{\frac{1}{2}\phi(r)\phi(s)} =$$

$$= \left(a^{\phi(r)}\right)^{\frac{1}{2}\phi(s)} \equiv 1 \pmod{r}$$

Similarly:

$$a^{\frac{1}{2}\phi(m)} \equiv 1 \pmod{s},$$

Since $\gcd(r, s) = 1 \Rightarrow$

$$a^{\frac{1}{2}\phi(m)} \equiv 1 \pmod{m}.$$

(ii) Notice that since $r, s > 2$ the numbers $\phi(r)$ and $\phi(s)$ are even, so that $\frac{1}{2}\phi(r)$ and $\frac{1}{2}\phi(s)$ make sense.

(ii) Let $m > 2$ and let g be a primitive root modulo m. Suppose

BW $\exists\, x \in \mathbb{Z}$, such that

$$x^2 \equiv 1 \pmod{m},$$