Problem 5

(i) $m \in \mathbb{Z}$, $m > 0$
The order of $a \in \mathbb{Z}$ modulo m is the smallest positive integer n, such that $a^n \equiv 1 \pmod{m}$ (provided $(a, m) = 1$).
Clearly, $n \leq \phi(m)$. By Euclid's property $\phi(m) = nq + r$, $0 \leq r < n$. Then

$$a^{\phi(m)} = a^{nq+r} = (a^n)^q a^r \equiv 1^q a^r = a^r$$

$\equiv 1 \pmod{m}$, so that either $r = 0$ or $a^r \equiv 1 \pmod{m}$ & $r < n$ – contradiction in the last case $\Rightarrow r = 0 \Rightarrow$ $\boxed{4}$
$\Rightarrow n \mid \phi(m)$.

BW

(ii) Let $m \in \mathbb{Z}$, $m > 0$. let $a \in \mathbb{Z}$, $(a, m) = 1$.
Let $|a|_n$ – be the order of a mod m.
If $n = \phi(m)$ then we say that a is a primitive root mod m.

BW

Let g be a primitive root mod m. Assume

$$g^r \equiv g^s \pmod{m}$$

Without loss of generality we may assume $r \geq s$. Since g is a prim. root $\Rightarrow$ in particular, $(g, m) = 1$. Therefore,

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

$\Rightarrow \phi(m) \mid (r - s) \Rightarrow r \equiv s \pmod{\phi(m)}$.
Conversely, if $r \equiv s \pmod{\phi(m)} \Rightarrow$

(12)

$r = s + t\phi(m) \Rightarrow$

$$g^r = g^{s+t\phi(m)} = g^s\left(g^{\phi(m)}\right)^t \equiv g^s \pmod m.$$

$\boxed{5}$

(iii) Let $i,j \in \{0,1,\dots,\phi(m)-1\}$ and $i \neq j$.

BW

Suppose $g^i \equiv g^j \pmod m$. Then, by (ii),

$i \equiv j \pmod{\phi(m)} \Rightarrow i = j$ - contradiction.

Then $\{1, g, g^2, \dots, g^{\phi(m)-1}\}$ are pair-wise distinct mod m and $\#\{1, g, g^2, \dots, g^{\phi(m)-1}\} =$

$= \phi(m)$, so that

$$\{1, g, g^2, \dots, g^{\phi(m)-1}\} \underset{m}{\overset{\text{mod}}{=\!=}} \{a \in \mathbb{Z} \mid 1 \leq a \leq m, (a,m)$$

$\boxed{6}$

(iv) Let's find all primitive roots mod 7.

BW

Residues mod 7 are $\cancel{0}, \cancel{1}, \cancel{2}, 3, 4, 5, 6$

$\phi(7) = 6$

NW

$2^2 = 4 \not\equiv 1 \pmod 7$
$2^3 = 8 \equiv 1 \pmod 7 \Rightarrow$ not a prim. root

$3^2 \equiv 2 \not\equiv 1 \pmod 7$
$3^3 \equiv 6 \not\equiv 1 \pmod 7$
$3^4 = 4 \not\equiv 1 \pmod 7$
$3^5 \equiv 12 \equiv 5 \not\equiv 1 \pmod 7$
$3^6 \equiv 15 \equiv 1 \pmod 7 \Rightarrow 3$ is a prim. root

$4^2 \equiv 2 \pmod 7$
$4^3 \equiv 1 \pmod 7 \Rightarrow 4$ not a root

$5^2 = 25 \equiv 4 \pmod 7$
$5^3 \equiv 20 \equiv 6 \pmod 7$
$5^4 \equiv 30 \equiv 2 \pmod 7$
$5^5 \equiv 10 \equiv 3 \pmod 7$
$5^6 \equiv 15 \equiv 1 \pmod 7$ 5 is a root

$6^2 = 36 \equiv 1 \pmod 7$ not a root (13)

Thus, 3 and 5 are the only $\overset{\text{prim.}}{\text{roots}}$ mod 7.

$\boxed{2}$

(v) $5x^3 \equiv 5 \pmod 7$

HW

Since $3 \cdot 5 + (-2) \cdot 7 = 15 - 14 = 1$

$\Rightarrow$ 3 is the inverse to 5 mod 7.

$$3 \cdot 5 \cdot x^3 \equiv 3 \cdot 5 \pmod 7$$

$$x^3 \equiv 1 \pmod 7$$

Since 3 is a primitive root mod 7 say a, such that $(a,7)=1$, is of the form 3^i for some $i \in \{0,1,2,\dots,5\}$ because $6 = \phi(7)$. So:

$$(3^i)^3 \equiv 3^0 \pmod 7$$

$$\Updownarrow$$

$$3i \equiv 0 \pmod 6$$

$$i \equiv 0 \pmod 2$$

$\Rightarrow$ i is even among $\{0,1,2,\dots,5\}$

$\Rightarrow$ $i \in \{0,2,4\}$

$\Rightarrow x = 1, 9, 81 \pmod 7$

$x = 1, 2, 4 \pmod 7$

$\boxed{3}$

Problem 6

(i) $m \in \mathbb{Z}$, $m > 2$

BW

$m = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$

Since $m > 2 \Rightarrow$ either $s = 1$ and $\alpha_1 \geq 2$ or $s \geq 2$. In the firs case $\phi(m) = \phi(2^\alpha) = 2^{\alpha-1}$ even, in the second case $\phi(m)$ has a factor of type $p-1$ for a prime p, and $p-1$ is even.

$\boxed{3}$

(ii) $x^2 \equiv 1 \pmod m$

BW

± 1 obvious solutions, which are distinct if $m > 2$.

Let a be a solution to $x^2 \equiv 1 \pmod m$

If $(a, m) = d \neq 1 \Rightarrow$ some prime p, dividing d, divides 1 – contradiction $\Rightarrow (a, m) = 1$. Then $a = g^k$ for some $k \in \{0, 1, 2, \ldots, \phi(m) - 1\}$ where g is a primitive root!

Hence, $g^{2k} \equiv g^0 \pmod m$

$$\Updownarrow$$

$$2k \equiv 0 \pmod{\phi(m)}$$

Since $\phi(m)$ is even, $\frac{\phi(m)}{2} \in \mathbb{Z}$

and

$$k \equiv 0 \pmod{\frac{\phi(m)}{2}}$$

$$\Rightarrow k = s \cdot \frac{\phi(m)}{2}, \quad s \in \mathbb{Z}$$

If $s = 2t$, $t \in \mathbb{Z}$, then

$$k = 2t \cdot \frac{\phi(m)}{2} = t\phi(m)$$

Then $a = g^k = \left(g^{\phi(m)}\right)^t \equiv 1 \pmod m$

If $s = 2t+1$, $t \in \mathbb{Z}$, then

$$k = (2t+1)\frac{\phi(m)}{2} = t\phi(m) + \frac{\phi(m)}{2}$$

and $a = g^k = g^{t\phi(m) + \frac{\phi(m)}{2}} =$

$$= g^{\frac{\phi(m)}{2}} \pmod m$$

$$\Rightarrow g^{\frac{\phi(m)}{2}} \equiv -1 \pmod m \qquad \boxed{5}$$

BW

(iii) Let $m \in \mathbb{Z}$, $m > 0$, $m = ab$, where $a > 2$ & $b > 2$ & $(a, b) = 1$
Let $c \in \mathbb{Z}$, $c > 0$ and $(c, m) = 1$
Since $(a, b) = 1 \Rightarrow \phi(m) = \phi(ab) = \phi(a)\phi(b)$. Since $a > 2$ & $b > 2 \Rightarrow$
$\Rightarrow \phi(a)$ and $\phi(b)$ are both even.
$\Rightarrow \phi(m)$ is even.

Start to compute:

$$c^{\frac{\phi(m)}{2}} = c^{\frac{\phi(a)\phi(b)}{2}} =$$

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

Similarly,

$$c^{\frac{\phi(m)}{2}} \equiv 1 \pmod b$$

As $(a, b) = 1$, we get:

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

Therefore, if $m = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ and $s > 1, \alpha_1$

then $m = ab$ when $a > 2, b > 2 \Rightarrow$

$$\Rightarrow c^{\frac{\phi(m)}{2}} \equiv 1 \pmod m \Rightarrow |c|_m \leq \frac{\phi(m)}{2} < \phi(m$$

$\Rightarrow$ no prim. roots mod m.

If $m = p^\alpha$ or $m = 2p^\alpha$ then one can expect primitive roots. $\boxed{6}$

BW

HW

(iv) $2x^4 \equiv 22 \pmod{20}$

$x^4 \equiv 11 \pmod{10}$

$x^4 \equiv 1 \pmod{10}$

$\phi(10) = \phi(2 \cdot 5) = (2-1)(5-1) = 4$

Not hard to see that $7 \not\equiv 1 \pmod{10}$

$7^2 = 49 \not\equiv 1 \pmod{10}$

$7^3 \not\equiv 1 \pmod{10}$

but $7^4 = 2401 \equiv 1 \pmod{10} \Rightarrow 7$ is a prim. root mod 10 $\Rightarrow x = 7^i$

$$(7^i)^4 \equiv 7^0 \pmod{10}, \quad i \in \{0,1,2,3\}$$

$$4i \equiv 0 \pmod 4$$

$$i \equiv 0 \pmod 1$$

$\Rightarrow i$ is any amongst $\{0,1,2,3\}$

$$\Rightarrow x \equiv 1, 7, 49, 343 \pmod{10}$$

$$x \equiv 1, 3, 7, 9 \pmod{10}$$

$\boxed{3}$

(v) $3x^5 \equiv 101 \pmod 7$

JW

$$101 \equiv 150 = 3 \cdot 50 \pmod 7$$

$$3x^5 \equiv 3 \cdot 50 \pmod 7 \quad (\text{as } (3,7) = 1)$$

$$x^5 \equiv 50 \equiv 1 \pmod 7$$

$g = 3$ is a prim. root mod 7

$$x = 3^i, \quad i \in \{0, 1, 2, \dots, 5\}$$

$$(3^i)^5 \equiv 3^0 \pmod{\cancel{7}\ 6}$$

$$5i \equiv 0 \pmod 6$$

$$(-4)\,6 + 5 \cdot 5 = -24 + 25 = 1$$

$$5 \cdot 5i \equiv 5 \cdot 0 \pmod 6$$

$$i \equiv 0 \pmod 6$$

$\Rightarrow i = 0$ only

$\boxed{3}$

$x \equiv 1 \pmod 7$ – the only solution to $3x^5 = 101$ in $\mathbb{F}_7$.

Problem 7

(18)

BW

HW

(i) Let p be a prime. For $\forall n \in \mathbb{Z}$, $(n,p)=1$, if $n \equiv a^2 \pmod p$ for some $a \in \mathbb{Z}$, then $\left(\frac{n}{p}\right) = +1$, otherwise $\left(\frac{n}{p}\right) = -1$. In other words, if $[\bar{n}] \in \mathbb{Z}/p$ is a square in the field $\mathbb{F}_p = \mathbb{Z}/p$ then $\left(\frac{n}{p}\right) = +1$, if not then $\left(\frac{n}{p}\right) = -1$.

$\boxed{3}$

(ii) Euler's Criterion:

$$\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} \pmod p$$

for $\forall (n,p)=1$. In particular,

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1, & \text{if } \frac{p-1}{2} \text{ is even} \\ -1, & \text{if } \frac{p-1}{2} \text{ is odd} \end{cases} =$$

$$= \begin{cases} +1, & \text{if } p-1 \text{ is a multiple of } 4 \\ -1, & \text{otherwise} \end{cases}$$

$$= \begin{cases} +1, & \text{if } p \equiv 1 \pmod 4 \\ -1, & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

$\boxed{4}$

(iii) $\left(\frac{2}{p}\right) = 1 \iff p \equiv \pm 1 \pmod 8$

BW

Hw

$\left(\frac{2}{p}\right) = -1 \iff p \equiv \pm 3 \pmod 8$

$\boxed{4}$

(iv) By Euler's criterion:

BW

$$\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} \pmod p$$

$$\left(\frac{m}{p}\right) \equiv m^{\frac{p-1}{2}} \pmod p$$

$$\left(\frac{mn}{p}\right) \equiv (mn)^{\frac{p-1}{2}} \pmod p$$

$$\shortparallel$$

$$m^{\frac{p-1}{2}} n^{\frac{p-1}{2}}$$

$$|||$$

$$\left(\frac{n}{p}\right)\left(\frac{m}{p}\right) \pmod p$$

$\left(\frac{n+sp}{p}\right) = \left(\frac{n}{p}\right)$ because $n+sp \equiv n \pmod p$

so test if n is a square then so is $n+sp$, and vice versa.

$\boxed{5}$

(v) Gauss' Reciprocity:

BW

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

for $\forall$ p, q - primes, $p \neq q$.

BW HW

$$\left(\frac{78}{89}\right) = \left(\frac{2}{89}\right)\left(\frac{3}{89}\right)\left(\frac{13}{89}\right) = \left(\frac{3}{89}\right)\left(\frac{13}{89}\right) =$$

$$= \left(\frac{89}{3}\right)\left(\frac{13}{89}\right) = \left(\frac{2}{3}\right)\left(\frac{13}{89}\right) = -\left(\frac{13}{89}\right) =$$

$$= -\left(\frac{89}{13}\right) = -\left(\frac{11}{13}\right) = -\left(\frac{13}{11}\right) = -\left(\frac{2}{11}\right) = -(-1) = +1$$

$$\left(\frac{385}{389}\right) = \left(\frac{5\cdot 7\cdot 11}{389}\right) = \left(\frac{5}{389}\right)\left(\frac{7}{389}\right)\left(\frac{11}{389}\right) =$$

$$= \left(\frac{389}{5}\right)\left(\frac{7}{389}\right)\left(\frac{11}{389}\right) = \left(\frac{4}{5}\right)\left(\frac{7}{389}\right)\left(\frac{11}{389}\right) =$$

$$= \left(\frac{7}{389}\right)\left(\frac{11}{389}\right) = \left(\frac{389}{7}\right)\left(\frac{11}{389}\right) = \left(\frac{4}{7}\right)\left(\frac{11}{389}\right) =$$

$$= \left(\frac{11}{389}\right) = \left(\frac{389}{11}\right) = \left(\frac{4}{11}\right) = +1$$

$$\cancel{\left(\frac{7429}{7433}\right) =}$$

$$\left(\frac{66}{139}\right) = \left(\frac{2\cdot 3\cdot 11}{139}\right) =$$

$$= \left(\frac{2}{139}\right)\left(\frac{3}{139}\right)\left(\frac{11}{139}\right) = (-1)\left(\frac{3}{139}\right)\left(\frac{11}{139}\right) =$$

$$\cancel{= (-1)\left(\frac{139}{}\right)} = (-1)\left(-\left(\frac{139}{3}\right)\right)\left(\frac{11}{139}\right) =$$