Ex sheet 1

Ex 1: 1) • $\underbrace{1+1+\dots+1}_{m \text{ times}} \equiv 0 \pmod{15} \iff m \equiv 0 \pmod{15} \iff 15 \mid m.$

So $\mathrm{ord}_+(1) = 15$

• $\underbrace{2+\dots+2}_{m \text{ times}} \equiv 0 \pmod{15} \iff 15 \mid 2m \iff 15 \mid m$ (coprime)

So $\mathrm{ord}_+(2) = 15$

• $\underbrace{3+\dots+3}_{m \text{ times}} \equiv 0 \pmod{15} \iff 15 \mid 3m \iff 5 \mid m$ (simplify by 3)

So $\mathrm{ord}_+(3) = 5$

• Similarly, $\mathrm{ord}_+(4) = 15$, $\mathrm{ord}_+(5) = 3$.

2) Multiplicative order of 1, 2, 4: (because 3 and 5 are not invertible mod 15, because they are not coprime to 15).

• $1^1 = 1$ so $\mathrm{ord}_\times(1) = 1$

• $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16 \equiv 1 \bmod 15$ so $\mathrm{ord}_\times(2) = 4$.

• $4^2 \equiv 1$ so $\mathrm{ord}_\times(4) = 2$

Ex 2: We look for $n \in \mathbb{Z}$ such that $\begin{cases} n \equiv 2 \pmod 5 \\ n \equiv 3 \pmod 7 \end{cases}$.

We look for it in the form $n = a + 5b$.
We want $n \equiv 2 \pmod 5$ so we choose $a = 2$.
Then we want $2 + 5b \equiv 3 \bmod 7$ so $5b \equiv 1 \pmod 7$.
We multiply by the inverse of 5 (mod 7), which is the residue class of 3 since $3 \times 5 = 15 \equiv 1 \pmod 7$. So $b \equiv 3 \pmod 7$

Thus, if we choose $b=3$ we obtain $n = 2+5\times 3 = 17$ which satisfies the system.

Ex3: 1. $p=5$: $2^2 = 4 \equiv -1 \pmod 5$ and $2^4 \equiv 1 \pmod 5$

So $\boxed{2}$ has order 4: it is a generator of $\mathbb{F}_5^\times$

$p=7$: $2^2 = 4$, $2^3 = 8 \equiv 1 \pmod 7$: 2 has order 3: not a generator

$3^2 = 9 \equiv 2$, $3^3 = 6 \equiv -1$, $3^6 = (3^3)^2 \equiv 1$

So $\boxed{3}$ has order 6: it is a generator.

$p=11$: $2^2 = 4$ $2^3 = 8 = -3$ $2^4 = -6$ $2^5 = \underbrace{-1}$ need to square it to obtain 1

So $\boxed{2}$ has order 10, it is a generator

2.

k	$2^k \bmod 11$
0	1
1	2
2	4
3	8
4	5
5	10
6	9
7	7
8	3
9	6

So $\log_g(1) = 0$
$\log_g(2) = 1$
$\log_g(3) = 8$
$\log_g(4) = 2$
$\log_g(5) = 4$ etc...

Ex4: $\forall m \in \mathbb{Z}$, $(x^k)^m = 1 \iff n = \text{ord}(x) \mid km$

$\iff \frac{n}{(n,k)} \mid \frac{k}{(n,k)} m \iff \frac{n}{(n,k)} \mid m$

($\frac{n}{(n,k)}$ and $\frac{k}{(n,k)}$ coprime)

So $\text{ord}(x^k) = \frac{n}{(n,k)} = \frac{\text{ord}(x)}{\gcd(\text{ord}(x), k)}$

Ex 5: For all $k \in \{1, \dots, p^\alpha\}$, k is not coprime with $p^\alpha \iff p \mid k$.

So $p^\alpha - \varphi(p^\alpha) = \#\{\text{multiples of } p \text{ in } \{1, \dots, p^\alpha\}\}$

But $1 \leq mp \leq p^\alpha \iff \frac{1}{p} \leq m \leq p^{\alpha-1}$

$\iff 1 \leq m \leq p^{\alpha-1}$

So $\#\{\text{multiples of } p \text{ in } \{1, \dots, p^\alpha\}\} = p^{\alpha-1}$

So $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$.

Ex 6: 1. $\ker(f) = \{x \in \mathbb{F}_p^\times,\ x^2 = 1\} = \{\pm 1\}$

because $+1$ and -1 are distinct roots (p odd) and since $\mathbb{F}_p$ is a field, the polynomial $X^2 - 1$ cannot have more than two roots (its degree)

Since f is surjective by definition,

$$|\mathrm{Im} f| = |(\mathbb{F}_p^\times)^2| = \frac{|\mathbb{F}_p^\times|}{|\ker f|} = \frac{p-1}{2}$$

(1st isomorphism thm)

2. $\forall x \in \mathbb{F}_p^\times,\ \left(x^{\frac{p-1}{2}}\right)^2 = x^{p-1} = 1$ (Lagrange's theorem)

So $\mathrm{Im} g \subseteq \{\text{roots of } X^2 - 1 \text{ in } \mathbb{F}_p\} = \{\pm 1\}$.

Moreover, $-1 \in \mathrm{Im} g$ because otherwise the polynomial $X^{\frac{p-1}{2}} - 1$ would have $p-1$ roots (more than its degree), which is a contradiction.

So $\mathrm{Im}(g) = \{\pm 1\}$

3. $\frac{|\mathbb{F}_p^\times|}{|\ker g|} = |\mathrm{Im} g| = 2$ so $|\ker g| = \frac{p-1}{2}$

4. If $y = x^2 \in \mathrm{Im} f$ then $g(y) = y^{\frac{p-1}{2}} = (x^2)^{\frac{p-1}{2}} = x^{p-1} = 1$

So $y \in \ker g$. This shows that $\mathrm{Im} f \subseteq \ker g$.

But by q° 1 and 3, $|\mathrm{Im} f| = |\ker g|$, hence $\mathrm{Im} f = \ker g$.

So $\forall x \in \mathbb{F}_p^\times$, $x^{\frac{p-1}{2}} = \begin{cases} 1 \text{ if } x \in (\mathbb{F}_p^\times)^2 \\ -1 \text{ otherwise.} \end{cases}$

Ex 7: 1. - If χ is the trivial character, $\sum_{g \in G} \chi(g) = |G|$

- otherwise, let $g_0 \in G$ be such that $\chi(g_0) \neq 1$.

Then $\chi(g_0) \underbrace{\sum_{g \in G} \chi(g)}_{S} = \sum_{g \in G} \chi(g_0 g) = \underbrace{\sum_{h \in G} \chi(h)}_{S}$

So $\underbrace{(\chi(g_0) - 1)}_{\neq 0} S = 0 \Rightarrow S = 0$.

Cl: $\frac{1}{|G|} \sum_{g \in G} \chi(g) = \langle \mathbb{1}, \chi \rangle = 1$

2. Note that ψ_a is well-defined because if $a' \equiv a \pmod n$, then $\psi_a = \psi_{a'}$.

Now, we have that $a \mapsto \psi_a$ is a group homomorphism because $\forall x$,

$\psi_{a+b}(x) = e^{\frac{2i\pi(a+b)x}{n}} = \psi_a(x)\psi_b(x)$ so $\psi_{a+b} = \psi_a \psi_b$

- It is injective because if $\psi_a = 1$ (the trivial character) then

$$\psi_a(1) = 1 = e^{\frac{2i\pi a}{n}} \quad \text{so } n \mid a \cdot \text{ i.e. } a \equiv 0 \pmod n$$

- It is surjective because if $\psi \in \widehat{(\mathbb{Z}/n\mathbb{Z})}$ then, denoting $w =: \psi(1)$,

$$\psi(\underbrace{1+\cdots+1}_{x \text{ times}}) = \psi(1)\cdots\psi(1) = w^x \qquad (*)$$

In particular, $\psi(n) = w^n = 1$ because $n \equiv 0 \pmod n$

So $\exists! a \in \mathbb{Z}/n\mathbb{Z}$ such that $w = e^{\frac{2i\pi a}{n}}$ and $(*)$ shows that then $\psi = \psi_a$.

3.

$$\frac{1}{n}\sum_{a=0}^{n-1} e^{\frac{2i\pi ak}{n}} = \frac{1}{n}\sum_{a=0}^{n-1} \psi_k(a)$$

$$= \begin{cases} 1 \text{ iff } \psi_k \text{ is the trivial character of } \mathbb{Z}/n\mathbb{Z} \\ 0 \text{ otherwise} \end{cases}$$

↑ q°1

$$= \begin{cases} 1 \text{ iff } n \mid k \\ 0 \text{ otherwise} \end{cases}$$

↑ q°2