Homework 2

1. For each equation in $\mathbb{Z}_n$ find all solutions for $x \in \mathbb{Z}_n$.
   (a) $3x \equiv 10 \pmod{16}$
   (b) $7x \equiv 9 \pmod{18}$
   (c) $4x \equiv 5 \pmod{12}$
   (d) $2x \equiv 6 \pmod{12}$

(a) $\gcd(3,16)=1$ so there is an inverse of $3 \pmod{16}$.
In fact the inverse is $-5 \pmod{16}$.

Thus $3x \equiv 10 \pmod{16} \Rightarrow x \equiv (-5)3x \equiv (-5)10 \equiv -50 \equiv 14 \pmod{16}$

(b) $\gcd(7,18)=1$ so there is an inverse of $7 \pmod{18}$.
This inverse is $-5 \pmod{18}$, since

$$7\cdot(-5) \equiv -35 \equiv -36+1 \equiv 1 \pmod{18}.$$

Then

$$x \equiv (-5)7x \equiv (-5)9 \equiv -45 \equiv 9 \pmod{18}.$$

(c) $4x \equiv 5 \pmod{12} \iff \underbrace{4x-5}_{\text{odd}} = \underbrace{12k}_{\text{even}}$ for some k, impossible. No solutions

(d) By listing all possible $x \in \mathbb{Z}_{12}$ we get

$2\cdot 0 \equiv 0 \pmod{12}$
$2\cdot 1 \equiv 2 \pmod{12}$
$2\cdot 2 \equiv 4 \pmod{12}$
$\rightarrow 2\cdot 3 \equiv 6 \pmod{12}$
$2\cdot 4 \equiv 8 \pmod{12}$
$2\cdot 5 \equiv 10 \pmod{12}$
$2\cdot 6 \equiv 0 \pmod{12}$
$2\cdot 7 \equiv 2 \pmod{12}$
$2\cdot 8 \equiv 4 \pmod{12}$
$\rightarrow 2\cdot 9 \equiv 6 \pmod{12}$
$2\cdot 10 \equiv 8 \pmod{12}$
$2\cdot 11 \equiv 10 \pmod{12}$

Thus $x \equiv 3, 9 \pmod{12}$

2. Find the orders of the following elements.

   (a) 9 (mod 51) in the group $(\mathbb{Z}_{51}, +)$
   (b) 3 (mod 16) in the group $(\mathbb{Z}_{16}^{\times}, \times)$
   (c) $\sqrt{7}$ in the group $(\mathbb{R}, +)$
   (d) $\sqrt{7}$ in the group $(\mathbb{R}^{\times}, \times)$

(a) $\text{Ord} = 51/\gcd(51,9) = 51/3 = 17.$

(b) $3^1 \equiv 3 \pmod{16}$ $\quad 3^3 \equiv 27 \equiv 11 \pmod{16}$

$3^2 \equiv 9 \pmod{16}$ $\quad 3^4 \equiv 3 \cdot 11 \equiv 33 \equiv 1 \pmod{16}.$

Thus order is 4.

(c) $K\sqrt{7} = \underbrace{\sqrt{7} + \cdots + \sqrt{7}}_{K \text{ times}} \neq 0$ (the identity)

for any positive integer K. Thus order $= \infty$.

(d) $\sqrt{7}^K = \underbrace{\sqrt{7} \cdots \sqrt{7}}_{K \text{ times}} \neq 1$ (the identity)

for any positive integer K. Thus order $= \infty$.

3. Find the orders of the following elements in the general linear group $\mathrm{GL}_2(\mathbb{R})$.

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \qquad C = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

A: $A^k = \begin{pmatrix} 2^k & 0 \\ 0 & 3^k \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ for any positive integer k.

So order is ∞

B: $B^2 = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$

$B^3 = B^2 B = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$B^4 = B^3 B = -B \neq e$

$B^5 = B^3 B^2 = -B^2 \neq e$

$B^6 = B^3 \cdot B^3 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = e.$

Thus $\mathrm{ord}(B) = 6$.

C: $C = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ $\qquad C^2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$

$C^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ for any positive integer k.

Thus $\mathrm{ord}(C) = \infty$.

4. Let G be a finite group and $a \in G$ any element.

   (a) Show that if $a^k = e$ then $\mathrm{ord}(a)$ divides k.
   (Hint: Write $k = \mathrm{ord}(a)q + r$ where $0 \leqslant r < \mathrm{ord}(a)$ is the remainder.)

   (b) Suppose G is abelian, and $b \in G$. Write $m = \mathrm{ord}(a)$, $n = \mathrm{ord}(b)$. Show that $\mathrm{ord}(ab)$ divides the least common multiple of m, n.

   (c) Consider the group $G = \{e, r, b, g, o, y\}$ from Lecture 1. Compute the orders of each element in G. Show part (b) is not true for non-abelian groups, in general.

(a) $K = \mathrm{ord}(a)q + r \qquad 0 \leq r < \mathrm{ord}(a)$

$$e = a^K = a^{\mathrm{ord}(a)\cdot q + r} = \left(a^{\mathrm{ord}(a)}\right)^q a^r = e^q a^r = a^r$$

$r = 0$ since $r < \mathrm{ord}(a)$. Thus $K = \mathrm{ord}(a)\cdot q$.

(b) Let $L = \mathrm{lcm}(m,n)$.

By (a), suffices to show $(ab)^L = e$. So:

$$(ab)^L \underset{\uparrow}{=} a^L b^L \underset{\uparrow}{=} a^{m\cdot x} b^{n\cdot y} = (a^m)^x (b^n)^y$$

a,b commute m,n divide L

$$= e^x e^y = e.$$

(c) $\mathrm{ord}(e) = 1$, $\mathrm{ord}(r) = \mathrm{ord}(b) = \mathrm{ord}(g) = 2$.
$\mathrm{ord}(y) = \mathrm{ord}(o) = 3$.

Part (b) fails:

$\mathrm{ord}(r) = \mathrm{ord}(b) = 2$. So $\mathrm{lcm}(\mathrm{ord}(r), \mathrm{ord}(b)) = 2$.

But $\mathrm{ord}(rb) = \mathrm{ord}(o) = 3$ doesn't divide 2.

5. Prove or disprove the following statements.

   (a) $(\mathbb{Q}^\times, \times)$ is a cyclic group.

   (b) $(\mathbb{Z}_4^\times, \times)$ is a cyclic group.

   (c) If a group has no proper non-trivial subgroups then it is cyclic.
   (Proper: not the whole group; non-trivial: not the trivial subgroup $\{e\}$.)

(a) $(\mathbb{Q}^\times, \times)$ is not cyclic. Suppose for contradiction that $\frac{a}{b} \in \mathbb{Q}^\times$ generates the group, $\gcd(a,b) = 1$.

Choose a prime p such that it doesn't divide a, b. Since $\frac{a}{b}$ generates, $p = \frac{a^k}{b^k}$ for some $k \in \mathbb{Z}$. Then $pb^k = a^k$ implies p divides a, a contradiction.

(b) $\mathbb{Z}_4^\times$ is cyclic. $\mathbb{Z}_4^\times = \{1 \pmod 4, 3 \pmod 4\}$ and $3^2 \equiv 9 \equiv 1 \pmod 4$, so $3 \pmod 4$ generates.

(c) If $G = \{e\}$ we are done. So assume $G \neq \{e\}$. Let $a \in G$, $a \neq e$. Consider the subgroup $\langle a \rangle \subseteq G$. This is not trivial, i.e. $\langle a \rangle \neq \{e\}$ because $a \neq e$. So by assumption we must have $\langle a \rangle = G$. Thus G is cyclic, generated by a.

6. For any abelian group, show that the subset of elements of finite order is a subgroup.

Let $H = \{a \in G : \operatorname{ord}(a) < \infty\}$

$= \{a \in G : \exists k \in \mathbb{Z},\ k > 0 \text{ with } a^k = e\}$

1. $e \in H$ since $e^1 = e$, i.e. $\operatorname{ord}(e) = 1$.

2. Suppose $a, b \in H$. Let $N = \operatorname{ord}(a)\operatorname{ord}(b)$. Then

$$(ab)^N \underset{\substack{\uparrow \\ G \text{ abelian}}}{=} a^N b^N = \left(a^{\operatorname{ord}(a)}\right)^{\operatorname{ord}(b)} \cdot \left(b^{\operatorname{ord}(b)}\right)^{\operatorname{ord}(a)}$$
$$= e^{\operatorname{ord}(b)} e^{\operatorname{ord}(a)} = e.$$

Thus $ab \in H$.

3. Suppose $a \in H$ so that $a^{\operatorname{ord}(a)} = e$.

Here $\operatorname{ord}(a)$ is a positive integer. Then

$$(a^{-1})^{\operatorname{ord}(a)} = a^{-\operatorname{ord}(a)} = \left(a^{\operatorname{ord}(a)}\right)^{-1} = e^{-1} = e$$

Thus $a^{-1} \in H$.

Therefore H is a subgroup.