Date

第三次习题课.

一、$\begin{cases} x\equiv 6 \pmod{10} \\ x\equiv 10 \pmod{12} \\ x\equiv 1 \pmod{15} \end{cases}$ $\Rightarrow$ $x\equiv 0 \pmod 2$, $x\equiv 1 \pmod 5$, $x\equiv 1 \pmod 3$, $x\equiv 2 \pmod 4$, $x\equiv 1 \pmod 3$, $x\equiv 1 \pmod 5$

整理得 $\begin{cases} x\equiv 2 \pmod 4 \\ x\equiv 1 \pmod 3 \\ x\equiv 1 \pmod 5 \end{cases}$ $\Rightarrow$ $\begin{cases} x\equiv 46 \pmod{60} \end{cases}$

注意另一点：$2a\equiv 4 \pmod 8 \Leftrightarrow a\equiv 2 \pmod 4$.

二、求解方程 $x^3-2x+6\equiv 0 \pmod{25}$

首先看 $x^3-2x+6\equiv 0 \pmod 5$

$\Rightarrow x=5t+1$ 或 $x=5t+2$.

① $x=5t+2$,

$x^3-2x+6=(125t^3+150t^2+60t+8)-2(5t+2)+6$

$=125t^3+150t^2+50t+10$

$\Rightarrow 25\nmid x^3-2x+6$.

② $x=5t+1$.

$x^3-2x+6=(125t^3+75t^2+15t+1)-2(5t+1)+6$

$=125t^3+75t^2+5t+5$.

若 $25\mid x^3-2x+6 \Rightarrow 5\mid t+1$, $\Rightarrow t=5k-1$.

$\Rightarrow x=25k-4$.

三，证明：$v_2(a^n-b^n)=v_2(a^2-b^2)+v_2(n)-1$.

设 $n=2^m t$，t 为奇数.

$$a^n-b^n=a^{2^m t}-b^{2^m t}$$
$$=(a^t-b^t)(a^t+b^t)\underbrace{(a^{2t}+b^{2t})\cdots(a^{2^{m-1}t}+b^{2^{m-1}t})}_{m-1}$$

由 $a^2+b^2\equiv 2 \pmod 4$.

下面考虑 $v_2(a^{2t}-b^{2t})$.

$$a^{2t}-b^{2t}=(a^2)^t-(b^2)^t$$
$$=(a^2-b^2)((a^2)^{t-1}+(a^2)^{t-2}(b^2)+\cdots+(b^2)^{t-1})$$

$\Rightarrow v_2(a^{2t}-b^{2t})=v_2(a^2-b^2)$.

综上，$v_2(a^n-b^n)=v_2(a^2-b^2)+v_2(n)-1$.

四，

Recall：群 G，$H\le G$，左陪集

$aH=bH \Leftrightarrow a\in bH$（或 $b\in aH$）

$\Leftrightarrow b^{-1}a\in H$（或 $a^{-1}b\in H$）.

(1) $17-8=9\in H \Rightarrow 8+H=17+H$.

(2) $8-(-1)=9\in H \Rightarrow -1+H=8+H$.

(3) $20-4=16\notin H \Rightarrow 4+H\neq 20+H$

Date

五. Recall: $\phi \neq H \subseteq G$, $H \leq G \Leftrightarrow \begin{cases} \forall a,b \in H, \text{有} ab \in H \\ \forall a \in H, a^{-1} \in H. \end{cases}$

"$\Rightarrow$" $H \leq G$, $\Rightarrow \forall a,b \in H$, 有 $ab \in H$

"$\Leftarrow$" ① 由于 H 的运算继承自 G, 满足结合律.

② H 是有限集, 设 $H = \{a_1, a_2, \cdots, a_n\}$, $\forall a \in H$, 有 $aH = \{aa_1, aa_2, \cdots, aa_n\}$, 由运算封闭, $aH \subseteq H$,

若 $\exists i \neq j \in \{1,2,\cdots,n\}$, $aa_i = aa_j \Rightarrow a_i = a_j$ 与 H 是集合矛盾

$\Rightarrow aH = H$.

则对 $\forall a,b \in H$. $\exists a_i \in H$ 有 $aa_i = b$, 即 $\forall a,b \in H$ 方程 $ax = b$ 在 H 中有解.

同理, $\forall a,b \in H$ 方程 $ya = b$ 在 H 中有解.

(由有限集自然知道包含单位元).

另证: $a, a^2, \cdots, a^n, \cdots$ 不可能是两两不同的,

$\exists i,j$. s.t $a^i = a^j = a^i \cdot a^{j-i}$

$\Rightarrow e = a^{j-i} = a \times a^{j-i-1}$.

六、 $x \to \frac{b}{a}x$.

定义：$\phi: (R,+) \to (R,+)$

$x \longrightarrow \frac{b}{a}x$ (因为$a \neq 0$，则分母有意义)

则 $\varphi(a) = b$，下证：ϕ 是同构映射.

① ϕ 是单射. $\forall x, y \in G$，若 $\phi(x) = \phi(y)$，则 $\frac{bx}{a} = \frac{by}{a}$

由 $\frac{b}{a} \neq 0 \Rightarrow x = y$

② ϕ 是满射，$\exists \frac{ay}{b} \in G$，有 $\phi(\frac{ay}{b}) = \frac{b}{a}(\frac{ay}{b}) = y$.

③ 满足同构的定义，

$$\phi(x+y) = \frac{b(x+y)}{a} = \frac{bx+by}{a} = \phi(x) + \phi(y)$$

综合①②③知，ϕ 是一个同构映射.

Date

七.

① 证明 H 是 G 的子群. $\forall a, b \in H$, 则由 H 定义, 设 $\operatorname{ord} a = m$, $\operatorname{ord} b = n$, $\Rightarrow a^m = e$, $b^n = e$ 进而 $(ab^{-1})^{mn}$ $\underline{\underline{G\text{交换}}}$ $a^{mn} \cdot (b^{-1})^{mn} = (a^m)^n \cdot (b^n)^{-m}$
$= e^n \cdot (e)^{-m} = e$.
$\Rightarrow ab^{-1}$ 的阶是有限的, $\Rightarrow H \leq G$.

② 证明 H 是 G 的正规子群.
$\forall a \in G$, $\forall h \in H$, 设 $\operatorname{ord} h = k$, $\therefore h^k = e$
$\therefore (aha^{-1})^k = (aha^{-1}) \cdots (aha^{-1})$
$= ah^k a^{-1} = aea^{-1} = aa^{-1} = e$.
$\Rightarrow aha^{-1}$ 的阶是有限的
$\Rightarrow aha^{-1} \in H$. $\Rightarrow H \lhd G$.

③ 证明: G/H 中除单位元 H 外, 其余元素的阶无限.
$\forall H \neq aH \in G/H$. $\Rightarrow a \in H$. 进而对 $\forall k \in \mathbb{Z}$.
$a^k \notin H$ ……(※)
假设 $\operatorname{ord} aH = l$, 则
$H = (aH)^l = (aH) \cdots (aH) \underline{\underline{H \lhd G}} a^l H$.
$\Rightarrow a^l \in H$ 与 (※) 矛盾.
$\therefore G/H$ 中除 H 外所有元素阶都是无穷的.

八，

Z_m 是 m 阶循环群，生成元是 $\bar{1}$，单位元是 $\bar{0}$

Z_k 是 k 阶循环群，生成元是 $[1]$，单位元是 $[0]$

$\exists$ 满同态映射 $\phi: Z_m \to Z_k$

$$n\bar{1} \to n[1]$$

$$\begin{aligned}
\text{其中 } \ker\phi &= \{\bar{x} \in Z_m \mid \phi(\bar{x}) = [0]\} \\
&= \{\bar{x} \in Z_m \mid x[1] = [0]\} \\
&= \{\bar{x} \in Z_m \mid k \mid x\}. \\
&= \langle \bar{k} \rangle.
\end{aligned}$$

$\therefore$ 根据同态基本定理 $Z_m/\ker\phi \cong Z_m/\langle \bar{k} \rangle \cong Z_k$