# 代数结构HW4答案

张朔宁

April 2, 2025

38. (1). 算出关于原根2的最小指数表(mod 29);
    (2). 利用此表解 $9x \equiv 2 \pmod{29}$;
    (3). 利用此表解 $x^9 \equiv 2 \pmod{29}$.

**解**. (1).

| $a$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\mathrm{ind}_2(a)$ | 0 | 1 | 5 | 2 | 22 | 6 | 12 | 3 | 10 | 23 | 25 | 7 | 18 | 13 | 27 | 4 | 21 | 11 | 9 |

| $a$ | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 |
|---|---|---|---|---|---|---|---|---|---|
| $\mathrm{ind}_2(a)$ | 24 | 17 | 26 | 20 | 8 | 16 | 19 | 15 | 14 |

(2). $\mathrm{ind}_2(9) = 10, \mathrm{ind}_2(2) = 1$, 因此$\mathrm{ind}_2 x = 1 - 10 \equiv 19 \pmod{28}$, 故$x \equiv 26 \pmod{29}$

(3). $9\mathrm{ind}_2(x) = 1 \pmod{28}$, 由于$(9, 28) = 1$, 因此解唯一。解得$\mathrm{ind}_2(x) = 25$, 因此$x \equiv 11 \pmod{29}$

**注**. $\mathrm{ind}_2(x)$是以28为周期循环，而非29

41. 证明：若$p, q$为奇素数, $q \mid (a^p + 1)$, 则有$q \mid (a+1)$或$q \mid (2kp+1)$, 其中$k$为某个整数.

*Proof.* $a^p \equiv -1 \pmod{q}$, 因此$a^{2p} \equiv 1 \pmod{q}$. 故$a$模$q$的阶为整除$2p$.
$p$为奇素数，因此$a$的阶只可能为$1, 2, p, 2p$. $a^p \equiv -1 \pmod{q}$，故$a$的阶不可能为$1, p$
若$a$的阶为2，则$a^2 \equiv 1 \pmod{q}$, 又$q \nmid (a-1)$, 故$q \mid (a+1)$
若$a$的阶为$2p$, 则由$a^{q-1} \equiv 1 \pmod{q}$, 因此$2p \mid q-1$, 故原命题成立 □

**注**. 这道题有很多不同的证法。原因之一在于$q \mid 2kp+1$这个结论实际上很弱。其等价于$mq - 2kp = 1$有解$(m, k)$，这当且仅当$\gcd(2p, q) = 1$,也即$p \neq q$. 因此只要讨论两种不同情况即可。事实上，原题的结论可以加强到$q = 2kp + 1$

42. 证明：若$a$模$p$的阶为3, 则$a+1$模$p$的阶为6.

*Proof.* $a$模$p$的阶为$3 \Rightarrow a^3 \equiv 1 \pmod{p} \Rightarrow p \mid (a-1)(a^2+a+1)$
由于$a$模$p$的阶不为1，因此$p \nmid a - 1 \Rightarrow (a^2+a+1) \equiv 0 \pmod{p}$
故

$$\begin{aligned}
(a+1)^6 &\equiv a^6 + 6a^5 + 15a^4 + 20a^3 + 15a^2 + 6a + 1 \pmod{p} \\
&\equiv 1 + 6a^2 + 15a + 20 + 15a^2 + 6a + 1 \pmod{p} \\
&\equiv 21(a^2+a+1) \pmod{p} \\
&\equiv 0 \pmod{p}
\end{aligned}$$

下面验证$1, 2, 3$不是$a+1$的阶
$a \nmid p \Rightarrow 1$不是$a+1$的阶
$(a+1)^2 \equiv a^2 + 2a + 1 \equiv a \pmod{p} \Rightarrow 2$不是$a+1$的阶
$(a+1)^3 \equiv a^3 + 3a^2 + 3a + 1 \equiv 3(a^2+a+1) - 1 \equiv -1 \pmod{p} \Rightarrow 3$不是$a+1$的阶
因此$a+1$的阶为6

□

3. 下列函数中哪些是单射、满射或双射？说明理由。其中，$\mathbb{Z}$与$\mathbb{Z}^+$分别为整数集合与正整数集合。

(1) $f:\mathbb{Z}\to\mathbb{Z}^+$，$f(n)=|n|+1$。

(3) $f:\mathbb{Z}\to\mathbb{Z}$，$f(n)=n+1$；$g:\mathbb{Z}\to\mathbb{Z}$，$g(n)=n-1$。

**解.** (1). 满射但不是单射。理由: $\forall n\in\mathbb{Z}^+, f(n-1)=n \Rightarrow$ 满射; $f(1)=f(-1)\Rightarrow$ 不是单射;

(3). 既是单射也是满射。理由: $\forall n\in\mathbb{Z}, f(n-1)=n, g(n+1)=n \Rightarrow$ 满射; $\forall n\neq m, f(n)\neq f(m), g(n)\neq g(m)\Rightarrow$ 单射

6. 设$A=\{a_1,a_2,...,a_n\}$、$B=\{b_1,b_2,...,b_m\}$，$S(B)$表示集合$B$中元素构成的所有有序$n$元组所构成的集合，即

$$S(B)=\{(b_{i_1},b_{i_2},...,b_{i_n})|b_{i_j}\in B,1\le j\le n\}.$$

用$F$表示从$A$到$B$的所有映射构成的集合，对于$F$中的每个映射$f$，令

$$g(f)=(f(a_1),f(a_2),...,f(a_n)),$$

证明：$g$是从$F$到$S(B)$的双射，并由此证明从$A$到$B$的映射有$m^n$个。

*Proof.* 单射：$\forall f_1\neq f_2,\exists a_i, f_1(a_i)\neq f_2(a_i)\Rightarrow g(f_1)\neq g(f_2)$
满射: $\forall s\in S(B)$，构造函数$h$, $h(a_j)=s_j, 1\le j\le n, s_j$为$s$的第$j$个元素。则显然有$h\in F, g(h)=s$
故为双射，因此$|F|=|S(B)|=m^n$, 即$A$到$B$的映射有$m^n$个

□

8. 设$f$是集合$S$到$T$的映射，$A$是$S$的子集，$A$在$S$中的补集为$\widetilde{A}=S-A$。当$f$为单射或满射时，分别讨论$f(\widetilde{A})$与$\widetilde{f(A)}$的关系。

**解.** $f$为单射$\Rightarrow f(A)\cap f(\widetilde{A})=\emptyset\Rightarrow f(\widetilde{A})\subseteq\widetilde{f(A)}$
$f$为满射$\Rightarrow f(A)\cup f(\widetilde{A})=T\Rightarrow f(\widetilde{A})\supseteq\widetilde{f(A)}$

12. 设$\sigma=\begin{pmatrix}1&2&3&4&5&6\\3&1&4&5&6&2\end{pmatrix}$，$\tau=\begin{pmatrix}1&2&3&4&5&6\\2&4&1&3&6&5\end{pmatrix}$。计算$\tau\sigma$，$\tau^2\sigma$，$\sigma^2\tau$，$\sigma^{-1}\tau\sigma$。

**解.** $\tau\sigma=\begin{pmatrix}1&2&3&4&5&6\\1&2&3&6&5&4\end{pmatrix}$

$\tau^2\sigma=\begin{pmatrix}1&2&3&4&5&6\\2&4&1&3&6&5\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6\\1&2&3&6&5&4\end{pmatrix}=\begin{pmatrix}1&2&3&4&5&6\\2&4&1&5&6&3\end{pmatrix}$

$\sigma^2\tau=\begin{pmatrix}1&2&3&4&5&6\\4&3&5&6&2&1\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6\\2&4&1&3&6&5\end{pmatrix}=\begin{pmatrix}1&2&3&4&5&6\\3&6&4&5&1&2\end{pmatrix}$

由$\sigma^{-1}=\begin{pmatrix}1&2&3&4&5&6\\2&6&1&3&4&5\end{pmatrix}$, 因此

$\sigma^{-1}\tau\sigma=\begin{pmatrix}1&2&3&4&5&6\\2&6&1&3&4&5\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6\\2&4&1&3&6&5\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6\\3&1&4&5&6&2\end{pmatrix}=\begin{pmatrix}1&2&3&4&5&6\\2&6&1&5&4&3\end{pmatrix}$