初等数论 期中复习

1. 试叙述良序公理，并用它证明$\sqrt{2}$($\sqrt{3}$, $\sqrt{5}$)是无理数。

证：良序公理：每个非空的正整数集合都有最小元。

考虑反证，假设$\sqrt{2}$为有理数，$\sqrt{2}=\frac{a}{b}$，$a,b\in\mathbb{Z}^+$，则$a=\sqrt{2}b$

设集合$S=\{\sqrt{2}k \mid k与\sqrt{2}k都是正整数\}$，则$a\in S$，S非空。

由良序公理，S有最小元，设为m，$m=\sqrt{2}t$，$t\in\mathbb{Z}^+$

考虑$\sqrt{2}m-m$。

$0<\sqrt{2}m-m=(\sqrt{2}-1)m<m$，且$\sqrt{2}m-m=\sqrt{2}\cdot\sqrt{2}t-m=2t-m$，$2t,m\in\mathbb{Z}^+$，则$\sqrt{2}m-m\in\mathbb{Z}^+$

$\sqrt{2}m-m=\sqrt{2}(m-t)$，$m-t\in\mathbb{Z}^+$，故$\sqrt{2}m-m\in S$。

由$\sqrt{2}m-m<m$知~~与假设矛盾~~与良序公理矛盾，故假设不成立。

所以$\sqrt{2}$是无理数，证毕。

（注，若证$\sqrt{5}$，只需取$\sqrt{5}m-2m$，证其$\in S$即可）

2. 用良序公理证明每个非空负整数集都有最大元。

证：设A为某非空负整数集，取$B=\{-a \mid a\in A\}$，则B为一非空正整数集

由良序公理，B中有最小元，即$\exists m\in B$，$\forall b\in B$，$m\le b$。

也即$\exists m\in B$，$\forall a\in A$，$m\le -a$

设$m'=-m$，则$m'\in A$，且有$\forall a\in A$，$-m'\le -a$，$m'\ge a$。

即A有最大元m'，原命题得证。

3. 用良序公理证明：设$a\in\mathbb{Z}$，$b\in\mathbb{Z}^+$，存在唯一的$q,r\in\mathbb{Z}$，使得$a=bq+r$。$(0\le r\le b-1)$

证：构造集合$T=\{a-bk \mid k\in\mathbb{Z}且a-bk\ge 0\}$，由良序公理，T中有最小元$r=a-bq\ge 0$

~~当$a-bk=0$时，$a=bk+0$~~ （此处最好先证良序公理的推广：非空非负整数集有最小元，课本上证明不少说）

假设$r\ge b$，则有$0\le r-b=a-bq-b=a-(q+1)b<r$，故$r-b\in T$但$r-b<r$与r是最小元矛盾。

因此$r\le b-1$。

下证q、r唯一。

假设有两个等式均成立，$a=bq_1+r_1$，$a=bq_2+r_2$，且满足$0\le r_1,r_2\le b-1$

有$a-a=b(q_1-q_2)+(r_1-r_2)=0$，即$r_2-r_1=b(q_1-q_2)$

那么必有$b\mid(r_2-r_1)$，然而由$0\le r_1,r_2\le b-1$知$-b<r_2-r_1<b$，矛盾。

故假设不成立，q,r唯一。

综上，原命题成立

4. 证明：大于1的整数都有素因子.

证：考虑反证. 假设存在整数大于1且没有素因子，这些数组成集合S.

S非空，由良序公理，S中有最小元，设为m。m是m的因子，故m不是素数.

那么必有 $m=ab$. $a,b\in Z^+$ 且 $1<a,b<m$

既然 $a<m$，那么 $a\notin S$. a有素因子，设为p，$p\mid a$，而 $m=ab$，故 $p\mid m$

即p是m的因子. 这与m没有素因子矛盾. 故假设不成立，不存在这样的数.

原命题得证.

证明：

5. 存在无穷多个素数

证：考虑反证、假设素数为有限多个，分别为 p_1、p_2、… p_n. $n\in Z^+$

构造 $Q_n=p_1p_2\cdots p_n+1$

Q_n 至少有1个素因子，设为q. 由假设，$q=p_i$. $1\le i\le n$

那么 $q\mid Q$ 且 $q\mid p_1p_2\cdots p_n$，那么 $q\mid(Q-p_1p_2\cdots p_n)$ 即 $q\mid 1$. 这是不可能的.

故假设不成立，原命题得证.

6. 证明：若 $(a,b)=d$，$a,b\in Z$，则 $(a/d,b/d)=1$

证：假设 $(a/d,b/d)=e\ne1$，$\frac{a}{d}=me$，$\frac{b}{d}=ne$，则有 $a=med$，$b=ned$.

即 $ed\mid a$ 且 $ed\mid b$，由于 $e\ne1$，故 $e>1$，$ed>d$. 与 $(a,b)=d$ 矛盾.

故假设不成立，原命题得证.

7. 证明：两个不全为0的整数a和b的最大公因子是a，b线性组合中最小的正整数.

证：设集合 $S=\{ma+nb\mid m,n\in Z \text{ 且 } ma+nb>0\}$ 由良序公理，S有最小元d. （$a,-a,b,-b$ 至少有1个 $\in S$，故S非空）

设 $d=ma+nb$，$m,n\in Z$，不妨设 $a\ne0$

下证 $d\mid a$，

设 $a=dq+r$，$0\le r<d$. $r=a-dq=a-(ma+nb)q=a-mqa-nqb=(1-qm)a-qnb$

若 $r>0$，即r也是a、b线性组合且 $r<d$. 与d是最小元矛盾，所以 $r=0$.

即 $a=dq$，$d\mid a$. 同理 $d\mid b$. d是a、b的公因子.

$\because\ \forall e\in Z$，若e整除a，b. 即e是a，b的公因子，那么 $e\mid ma+nb=d$，$e\le d$

所以d是最大公因子. 原命题得证.

8. 证明：$a,b\in\mathbb{Z}$且不全为0，那么 $d=(a,b)$ $\Leftrightarrow$

① $d|a$ 且 $d|b$ （如果做这个题就把他做了吧）

② 若 $c\in\mathbb{Z}$ 且 $c|a, c|b$，则 $c|d$

证："$\Rightarrow$"：已知 $d=(a,b)$

$d|a$ 且 $d|b$ 成立.

由题7知，$\exists\, m,n\in\mathbb{Z}$ 使 $d=ma+nb$. 则若 $\exists\, c\in\mathbb{Z}$ 且 $c|a$. $c|b$. $c\,|\,ma+nb=d$.

"$\Leftarrow$"：已知①②

对于所有 a,b 的公因子 c，$c|d$. 必有 $c\le d$. 而 d 也是 a,b 的公因子

即 d 是最大的公因子. $d=(a,b)$

综上，充要，原命题得证.

9. 证明：设 $a_1,a_2,\cdots a_n\in\mathbb{Z}^+$，$p$ 是素数，若 $p\,|\,a_1a_2\cdots a_n$，且 $\exists\, a_i$，$i\in[1,n]$. 使得 $p|a_i$

证：略.（此题为 P_{113} Lemma 3.5. 若要严密证明需先证 Lemma 3.4. 若要证 Lemma 3.4 需先证 P_{96} Corollary 3.8.2 …… 大家看看书吧. 建议放弃这道题）

10. 证明：每个大于1的正整数都可以唯一地表示成非负素数的乘积.

（需要用到第9题结论，并不知道需不需要做完9才能做10）

证：假设存在大于1的正整数无法表示成非负素数的乘积，它们组成集合 S，S 非空.

由良序公理，S 中有最小元 n.

若 n 为素数，$n=n$ 也可认为是素数乘积. 矛盾，故 n 是合数.

设 $n=ab$，$a,b\in\mathbb{Z}^+$ 且 $1<a,b<n$. 那么 $a,b\notin S$. a,b 可写成非负素数的乘积.

而 $n=ab$ 也必然可写成非负素数的乘积. 与 $n\in S$ 矛盾. 故假设不成立，每个大于1的正整数都可以表示为非负素数的乘积.

下证这种表示唯一.

假设表示不唯一，$n=p_1p_2\cdots p_s=q_1q_2\cdots q_t$，$p_i$、$q_j$ 是素数，$i\in[1,s]$，$j\in[1,t]$

且 $p_1<p_2\cdots<p_s$，$q_1<q_2\cdots<q_t$

※ 约掉 p_i 和 q_j 中相同的素数，得

$$p_{i_1}p_{i_2}\cdots p_{i_u}=q_{j_1}q_{j_2}\cdots q_{j_v} \qquad u,v\in\mathbb{Z}^+ \text{ 且 } u,v\ge 1.$$

那么有 p_{i_1} 可整除左边但不能整除右边，矛盾. 故假设不成立，表示是唯一的.

综上，原命题得证.

11. 证明：$a,b\in Z$，$m\in Z^+$，$a\equiv b \pmod m$，当且仅当存在一整数k使得 $a=b+km$

证："⇒"：已知 $a\equiv b \pmod m$

由定义，$m\mid(a-b)$，即 $\exists k\in Z$，$a-b=km$，$a=b+km$.

"⇐"：已知 $a=b+km$

则 $a-b=km$，$m\mid(a-b)$ 由定义知，$a\equiv b \pmod m$.

12. 证明：若 $r_1,r_2,\cdots r_m$ 是一个模m的完全剩余系，且正整数a使得 $(a,m)=1$. 则对任何整数b，$ar_1+b, ar_2+b,\cdots ar_m+b$ 都是模m的完全剩余系.

证：即证 $ar_1+b,\cdots ar_m+b$ 任意两数模m不同余.

假设 $\exists i\neq j$，$(ar_i+b)\equiv(ar_j+b) \pmod m$

则 $m\mid[(ar_i+b)-(ar_j+b)]$，$m\mid a(r_i-r_j)$

由于 $(a,m)=1$，所以 $m\mid(r_i-r_j)$，换言之，$r_i\equiv r_j \pmod m$

这与 $r_1,\cdots r_m$ 是模m的完全剩余系矛盾. 故假设不成立，原命题得证.

13. 设 $m_1,m_2,\cdots m_k$ 两两互素，$M=m_1m_2\cdots m_k$，$M_j=M/m_j$，$j=1,2,\cdots k$. 证明当 $a_1,a_2\cdots a_k$ 分别取遍 $m_1,m_2\cdots m_k$ 的完全剩余系时，$M_1a_1+M_2a_2\cdots+M_ka_k$ 取遍M的完全剩余系.

证：a_i 有 m_i 种取法，则 $\sum_{i=1}^{k}M_ia_i$ 有 $\prod_{i=1}^{k}m_i$ 种取法，即M种.

只须证明这M种取法中任意两种互不模M同余.

假设有 $\sum_{i=1}^{k}M_ia_i'\equiv\sum_{i=1}^{k}M_ia_i'' \pmod M$，$\forall i=1,2,\cdots k$，$a_i'\not\equiv a_i'' \pmod m$

那么，$M\mid\sum_{i=1}^{k}M_i(a_i'-a_i'')$，那么 $m_1\mid\sum_{i=1}^{k}M_i(a_i'-a_i'')$

$\forall i=2,3,\cdots k$，$m_1\mid M_i$，而由于 $m_1,m_2,\cdots m_k$ 两两互素，$m_1\nmid M_1$

所以 $m_1\mid M_1(a_1'-a_1'')$，$m_1\mid(a_1'-a_1'')$

那么 $a_1'\equiv a_1'' \pmod m$，与假设矛盾. 所以假设不成立. 原命题得证.

补充：试叙述中国剩余定理，并用它解同余方程组 $\begin{cases}x\equiv1 \pmod 3\\x\equiv2 \pmod 5\\x\equiv3 \pmod 7\end{cases}$

解：中国剩余定理：

设 $m_1,m_2,\cdots m_r$ 两两互素的正整数，则

$x\equiv a_1 \pmod{m_1}$

$x\equiv a_2 \pmod{m_2}$

……

$x\equiv a_r \pmod{m_r}$

有模 $m_1m_2m_3\cdots m_r$ 的唯一解.

解方程组：

$M=3\times5\times7=105$

$M_1=105/3=35$

$M_2=105/5=21$

$M_3=105/7=15$

$M_1y_1\equiv1 \pmod 3$

$\Rightarrow y_1\equiv2 \pmod 3$

$M_2y_2\equiv1 \pmod 5$

$\Rightarrow y_2\equiv1 \pmod 5$

$M_3y_3\equiv1 \pmod 7$

$\Rightarrow y_3\equiv1 \pmod 7$

故所求 $x\equiv1\times35\times2+2\times21\times1+3\times15\times1\equiv157$

$\equiv52 \pmod{105}$

14、证明：设 $a,b\in\mathbb{Z}$，$d=(a,b)$，方程 $ax+by=c$ 有整数解的充要条件为 $d|c$。
若 $x=x_0$，$y=y_0$ 是一组特解，则通解是 $x=x_0+(b/d)n$，$y=y_0-(a/d)n$，$n\in\mathbb{Z}$。

证：首先假设 $d\nmid c$。 [P137，定理3.23]

设 $x,y\in\mathbb{Z}$ s.t. $ax+by=c$。由 $d=(a,b)$ 知 $d|a$ 且 $d|b$。由定理1.9得 $d|c$，与假设矛盾。因此 $d\nmid c$ 时 $ax+by=c$ 不存在整数解。

下面设 $d|c$。

由 $d=(a,b)$，由定理3.8知 $\exists s,t\in\mathbb{Z}$ s.t. $d=as+bt$。①

又 $d|c$，故 $\exists e\in\mathbb{Z}$ s.t. $c=de$。在①式两端同时乘以 e，有

$c=de=a(se)+b(te)$。这说明此时存在一组特解：$x_0=se$，$y_0=te$。

下面证明通解是 $x=x_0+(b/d)n$，$y=y_0-(a/d)n$。

先把 x,y 代入原方程，有：$ax+by=ax_0+a(b/d)n+by_0-b(a/d)n$

$=ax_0+by_0=c$。因此 x,y 是原方程的一组解。

再证原方程的任一组解 x,y 均可写成如上形式：

设 $x,y\in\mathbb{Z}$ s.t. $ax+by=c$。又 $ax_0+by_0=c$，故

$(ax+by)-(ax_0+by_0)=0$。即 $a(x-x_0)=b(y_0-y)$；

两边同时除以 d，有 $(a/d)(x-x_0)=(b/d)(y_0-y)$。

因为 $(a,b)=d$，故由定理3.6，$(a/d,b/d)=1$。

又由引理3.4，$(a/d)|(y_0-y)$。即 $\exists n\in\mathbb{Z}$，$y_0-y=na/d$。

故 $y=y_0-(a/d)n$。代入原方程有 $x=x_0+(b/d)n$。 □

15、证明：设 $a,b,c\in\mathbb{Z}$，$m\in\mathbb{Z}^+$，$a\equiv b\pmod m$，则

1) $a+c\equiv b+c\pmod m$， 2) $a-c\equiv b-c\pmod m$，

3) $ac\equiv bc\pmod m$。

[P148，定理4.4]

证：因为 $a\equiv b\pmod m$，由定义知 $m\mid(a-b)$

(1) 由于 $(a+c)-(b+c)=a-b$，故 $m\mid((a+c)-(b+c))$，即 $a+c\equiv b+c\pmod m$。

(2) 同理 $(a-c)-(b-c)=a-b$，故 $m\mid((a-c)-(b-c))$，即 $a-c\equiv b-c\pmod m$。

(3) $ac-bc=c(a-b)$。因为 $m\mid(a-b)$，$(a-b)\mid c(a-b)$，故 $m\mid c(a-b)$，

即 $ac\equiv bc\pmod m$。 □

16. 证明：设 $a,b,c\in\mathbb{Z}$，$m\in\mathbb{Z}^+$，$d=(c,m)$，$ac\equiv bc\pmod m$，则 $a\equiv b\pmod{m/d}$。

[P149，定理4.5]

证：因为 $ac\equiv bc\pmod m$，故 $m\mid(ac-bc)=c(a-b)$。

即 $\exists k\in\mathbb{Z}$，s.t. $c(a-b)=km$。两边同时除以 d，得到

$(c/d)(a-b)=(m/d)k$。因为 $d=(c,m)$，故 $(c/d,m/d)=1$。

由引理3.4，$(m/d)\mid(a-b)$。即 $a\equiv b\pmod{m/d}$。 □

17. 证明：设 $a,b,c\in\mathbb{Z}$，$m\in\mathbb{Z}^+$，$a\equiv b\pmod m$，$c\equiv d\pmod m$，则

1) $a+c\equiv b+d\pmod m$，　2) $a-c\equiv b-d\pmod m$，

3) $ac\equiv bd\pmod m$。

[P149，定理4.6]

证：因为 $a\equiv b\pmod m$，$c\equiv d\pmod m$，故 $m\mid(a-b)$，$m\mid(c-d)$，

即 $\exists k,l\in\mathbb{Z}$ s.t. $km=a-b$，$lm=c-d$。

(1) $(a+c)-(b+d)=(a-b)+(c-d)=(k+l)m$，故 $m\mid((a+c)-(b+d))$，

即 $a+c\equiv b+d\pmod m$。

(2) $(a-c)-(b-d)=(a-b)-(c-d)=(k-l)m$，故 $m\mid((a-c)-(b-d))$，

即 $a-c\equiv b-d\pmod m$。

(3) $ac-bd=(a-b)c+bc+b(c-d)-bc=(a-b)c+b(c-d)=(kc+lb)m$，

故 $m\mid(ac-bd)$，即 $ac\equiv bd\pmod m$。 □

18、设 $a,b,m\in\mathbb{Z}$，$m\in\mathbb{Z}^+$，$(a,m)=d$，若 $d\nmid b$，则 $ax\equiv b\pmod m$ 无解，若 $d\mid b$，则 $ax\equiv b\pmod m$ 恰有 d 个模 m 互不同余的解。［P158，定理4.11］

证：线性同余方程 $ax\equiv b\pmod m$ 等价于二元线性丢番图方程 $ax-my=b$。x 是原方程的解当且仅当存在 $y\in\mathbb{Z}$ s.t. $ax-my=b$。

由第14题结论知，$d\nmid b$ 时，$ax-my=b$ 无整数解，

$d\mid b$ 时，$ax-my=b$ 有无数组解，通解为 $x=x_0+(m/d)t$，$y=y_0+(a/d)t$。

即，原方程有无穷多解 x，满足 $x=x_0+(m/d)t$ 的形式。

下证模 m 互不同余的解 x 有 d 个。

考虑 $x_1=x_0+(m/d)t_1$，$x_2=x_0+(m/d)t_2$ s.t. $x_1\equiv x_2\pmod m$。

即 $x_0+(m/d)t_1\equiv x_0+(m/d)t_2\pmod m$。

两边同时减去 x_0，（定理4.4），有：$(m/d)t_1\equiv(m/d)t_2\pmod m$。

又 $(m,m/d)=m/d$，故再由定理4.5，$t_1\equiv t_2\pmod d$。

这说明原方程的所有解由 $x=x_0+(m/d)t$ 给出，其中 t 取遍 d 的一个完全剩余集，如 $t=0,1,2,\dots,d-1$。□

（因此原方程恰有 d 个模 m 互不同余的解。）

19、设 $H_n=\sum_{j=1}^{n}\frac{1}{j}$，用数学归纳法证明：$1+\frac{n}{2}\le H_{2^n}\le 1+n$。［P27，习题1.3：15，16］

证：当 $n=0$ 时，$1+\frac{0}{2}\le H_{2^0}=H_1=1\le 1+0$，原命题成立。

假设 $n=k$ 时原命题成立，$n=k+1$ 时，

$$H_{2^{k+1}}=\sum_{j=1}^{2^k}\frac{1}{j}+\sum_{j=2^k+1}^{2^{k+1}}\frac{1}{j}\ge H_{2^n}+\sum_{j=2^k+1}^{2^{k+1}}\frac{1}{2^{k+1}}\ge 1+\frac{k}{2}+\frac{2^k}{2^{k+1}}=1+\frac{k+1}{2}.$$

$$H_{2^{k+1}}=\sum_{j=1}^{2^k}\frac{1}{j}+\sum_{j=2^k+1}^{2^{k+1}}\frac{1}{j}\le H_{2^n}+\sum_{j=2^k+1}^{2^{k+1}}\frac{1}{2^k}\le 1+k+\frac{2^k}{2^k}=1+(k+1).$$

即，$n=k+1$ 时，原命题成立。

故由数学归纳法，原命题成立。□

20、证明：若 $a_n=\frac{1}{\sqrt5}(\alpha^n-\beta^n)$，$\alpha=\frac{1+\sqrt5}{2}$，$\beta=\frac{1-\sqrt5}{2}$，则 $a_n=a_{n-1}+a_{n-2}$，$a_1=a_2=1$。

[P35，习题1.4：40]

证：$a_1=\frac{1}{\sqrt5}\left(\frac{1+\sqrt5}{2}-\frac{1-\sqrt5}{2}\right)=\frac{2\sqrt5}{2\sqrt5}=1$.

$a_2=\frac{1}{\sqrt5}\left(\left(\frac{1+\sqrt5}{2}\right)^2-\left(\frac{1-\sqrt5}{2}\right)^2\right)=\frac{1}{\sqrt5}\left(\frac{3+\sqrt5}{2}-\frac{3-\sqrt5}{2}\right)=1$.

$$a_n=\frac{1}{\sqrt5}(\alpha^n-\beta^n)=\frac{1}{\sqrt5}\left(\alpha^{n-2}\cdot\frac{3+\sqrt5}{2}-\beta^{n-2}\cdot\frac{3-\sqrt5}{2}\right)$$
$$=\frac{1}{\sqrt5}\left(\alpha^{n-2}(1+\alpha)-\beta^{n-2}(1+\beta)\right)=\frac{1}{\sqrt5}\left(\alpha^{n-1}-\beta^{n-1}+\alpha^{n-2}-\beta^{n-2}\right)$$
$$=\frac{1}{\sqrt5}\left(\alpha^{n-1}-\beta^{n-1}\right)+\frac{1}{\sqrt5}\left(\alpha^{n-2}-\beta^{n-2}\right)=a_{n-1}+a_{n-2}.\ \Box$$

21. 若 $a\equiv b \bmod m$，$c\equiv d \bmod n$，$a,b,c,d\in\mathbb{Z}$，$m,n\in\mathbb{Z}^+$，下列结论是否成立？若成立，请给出证明；若不成立，请举出反例。

1) $a\pm c\equiv b\pm d\ (\mathrm{mod}\ (m,n))$，$ac\equiv bd\ (\mathrm{mod}\ (m,n))$，

2) $a\pm c\equiv b\pm d\ (\mathrm{mod}\ [m,n])$，$ac\equiv bd\ (\mathrm{mod}\ [m,n])$。

解：(1) 成立，证明如下：记 $e=(m,n)$，则 $e\mid m$，$e\mid n$。

因为 $a\equiv b \bmod m$，$c\equiv d \bmod n$，故 $\exists k,l\in\mathbb{Z}$，$a-b=km$，$c-d=ln$。

于是 $(a\pm c)-(b\pm d)=(a-b)\pm(c-d)=km\pm ln$。

由定理1.9，$e\mid(km\pm ln)$，即 $e\mid((a\pm c)-(b\pm d))$，故 $a\pm c\equiv b\pm d\ (\mathrm{mod}\ (m,n))$。

$ac-bd=(a-b)c+bc+(c-d)b-bc=kcm+lbn$。

同理，$e\mid(ckm+bln)$ 即 $e\mid(ac-bd)$，故 $ac\equiv bd\ (\mathrm{mod}\ (m,n))$。

(2) 不成立，反例如下：$a=5$，$b=9$，$c=8$，$d=32$，$m=4$，$n=6$，$[m,n]=12$。

即 $5\equiv 9\ (\mathrm{mod}\ 4)$，$8\equiv 32\ (\mathrm{mod}\ 6)$，而 $(5+8)\bmod 12=1$，$(9+32)\bmod 12=5$；

$(5-8)\bmod 12=3$，$(9-32)\bmod 12=11$；$(5\times 8)\bmod 12=4$，$(9\times 32)\bmod 12=0$。

故 $a\pm c\not\equiv b\pm d\ (\mathrm{mod}\ [m,n])$，$ac\not\equiv bd\ (\mathrm{mod}\ [m,n])$。$\Box$