初等数论第一次作业 2022.2.22

习题 1.1.1

设 n 是奇数, 则 $8 \mid n^2-1$.

证明：由 n 是奇数，则令 $n=2k+1$，有 $n^2-1=(2k+1)^2-1=4k(k+1)$，由于 k 和 $k+1$ 一奇一偶，从而 $2 \mid k(k+1)$，则 $8 \mid n^2-1$

习题1.1.2

设 $n \geqslant 3$ 是奇数, 证明: $\left(1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n-1}\right)(n-1)!$ 被 n 整除.

证明：由 $n \in \text{odd}$ 则可以依次首尾相加得到

$$\begin{aligned}1+\frac{1}{2}+\cdots+\frac{1}{n-1}&=(1+\frac{1}{n-1})+(\frac{1}{2}+\frac{1}{n-2})+\cdots+(\frac{1}{\frac{n-1}{2}}+\frac{1}{\frac{n+1}{2}})\\&=n\cdot(\frac{1}{1\cdot(n-1)}+\frac{1}{2\cdot(n-2)}+\cdots+\frac{1}{\frac{n-1}{2}\cdot\frac{n+1}{2}})\end{aligned}$$

而 $(n-1)!$ 均有 $1,2,\cdots,n-1$ 的因子，从而 $n \mid (1+\frac{1}{2}+\cdots+\frac{1}{n-1})(n-1)!$

习题1.1.3

设 m 和 n 为正整数, $m \geqslant 3$. 证明: $2^m-1 \nmid 2^n+1$.

> 引理 1.1.1 $q \in Z, x-1 \mid x^q-1$，这是由于 $1+x+\cdots+x^{q-1}=\frac{x^q-1}{x-1} \in Z$

证明：显然当 $m>n$ 时结论不成立，假设结论不成立 $2^m-1 \mid 2^n+1$，由带余除法定理有 $n=mq+r, r<m$

$$\because 2^n+1=2^{mq+r}+1=2^r\cdot(2^{mq}-1)+2^r+1, 2^m-1\mid 2^{mq}-1$$
$$\therefore 2^m-1\mid 2^r+1 \text{ 而 } r<m, 2^m-1>2^r+1\Longleftrightarrow 2^m>2^r+2\Longleftrightarrow 2^m-2^r>2^{m-1}\geq 4>2$$

从而假设不成立，$2^m-1\nmid 2^n+1$

习题1.1.4

设 q 是大于 1 的整数. 证明:

(i) 每个正整数 n 可以惟一地表示成

$$n=a_0+a_1q+a_2q^2+\cdots+a_kq^k,$$

其中 a_i 是满足 $0\leqslant a_i\leqslant q-1$ 的整数 $(0\leqslant i\leqslant k)$, 并且 $a_k\neq 0$. 这叫作 n 的 q 进制表示.

(ii) $a_i=\left[\dfrac{n}{q^i}\right]-q\left[\dfrac{n}{q^{i+1}}\right](0\leqslant i\leqslant k)$.

证明：(i) 带余除法定理令 $n=b_0+m_1q, 0\leq b_0\leq q-1$，对 m_i 重复上述步骤有

$$m_1=b_1+m_2q, 0\leq b_1\leq q-1\cdots, m_k=b_k, 0\leq b_k\leq q-1$$

则回代得到 $n=b_0+q(b_1+q(b_2+\cdots+(b_k)))$，展开得到 $n=a_0+a_1q+\cdots+a_kq^k$

唯一性的证明：若有两种表示方法 $n=a_0+a_1q+\cdots+a_kq^k=c_0+c_1q+\cdots+c_kq^k$，有 $q\mid a_0-c_0$，则由于 $0\leq a_0,c_0\leq q-1$ 得 $a_0=c_0$，代入消去有 $a_1+a_2q+\cdots+a_kq^k=c_1+c_2q+\cdots+c_kq^k$，同理有 $a_i=c_i$，则表示方法唯一

(ii) 由 (i) 中表示有 $n=a_0+a_1q+\cdots+a_kq^k$，两边除以 q^i 有

$$\frac{n}{q^i}=\frac{a_0}{q^i}+\frac{a_1}{q^{i-1}}+\cdots a_i+a_{i+1}q+a_{i+2}q^2+\cdots+a_kq^{k-i}$$

由 $0\leq a_i\leq q-1$ 且有取整函数的定义可知 $[\dfrac{n}{q^i}]=a_i+a_{i+1}q+a_{i+2}q^2+\cdots+a_kq^{k-i}$

除以 q^{i+1} 重复上述步骤得 $[\dfrac{n}{q^{i+1}}]=a_{i+1}+a_{i+2}q+\cdots+a_kq^{k-i-1}$，比对上述两式得 $a_i=[\dfrac{n}{q^i}]-q[\dfrac{n}{q^{i+1}}]$

习题1.1.5

设 $\alpha_1,\cdots,\alpha_n$ 为实数 $(n\geqslant 2)$, 证明:

$$\begin{aligned}[\alpha_1]+[\alpha_2]+\cdots+[\alpha_n]&\leqslant[\alpha_1+\alpha_2+\cdots+\alpha_n]\\&\leqslant[\alpha_1]+[\alpha_2]+\cdots+[\alpha_n]+n-1\end{aligned}$$

证明：记 $\alpha_i=[\alpha_i]+\{\alpha_i\}, \forall\, x\in R, \{x\}\in[0,1)$，从而有 $[\sum\limits_{i=1}^n\alpha_i]=\sum\limits_{i=1}^n[\alpha_i]+[\sum\limits_{i=1}^n\{\alpha_i\}]\geq\sum\limits_{i=1}^n[\alpha_i]$

而 $[\sum_{i=1}^{n}\{\alpha_i\}]<[\sum_{i=1}^{n}1]=n$，由取整特性 $[\sum_{i=1}^{n}\{\alpha_i\}]\leq n-1$，则 $\sum_{i=1}^{n}[\alpha_i]\leq[\sum_{i=1}^{n}\alpha_i]\leq\sum_{i=1}^{n}[\alpha_i]+n-1$

习题1.1.11

设 n 为正整数, $n\geqslant 2$. 如果 n 没有小于或等于 $\sqrt{n}$ 的素数因子, 则 n 为素数.

证明：反证法，若 n 为合数，则 n 有素因子 q，则 $n=mq,m,q\in Z$，由于 n 没有 $\leq\sqrt{n}$ 的素数因子

$$\therefore m,q>\sqrt{n},mq>n$$

与假设矛盾，从而 n 为素数

习题1.1.12

对每个整数 $n\geqslant 3,n$ 和 $n!$ 之间必有素数. 由此证明素数有无限多个.

证明：反证法，假设 n 和 $n!$ 之间全为合数，则 $n!-1$ 为合数，其一定有素数因子，由假设知 $n+1$，$n+2,\cdots,n!$ 全为合数，不可能是 $n!-1$ 的素数因子，另一方面，$\forall\ n\geq a\geq 2,a\mid n!$，从而

$$P=\{p\mid p\in[2,n]\ \cap\ \text{p is prime}\},\forall\ x\in P,x\nmid n!-1$$

则 $n!-1$ 没有小于其自身的素数因子，从而 $n!-1$ 为素数，与假设矛盾，从而 n 和 $n!$ 之间一定有素数

从 3 开始，$(3,3!)$ 之间有素数，$(3!,(3!)!)$ 之间有素数，进而构造数列

$$a_1=3,a_{n+1}=a_n!$$

有 (a_n,a_{n+1}) 之间必有素数，且区间之间无交集，将自然数集分成无穷多个区间，从而有无穷多个素数

习题1.2.1

设 n 是正整数, 证明: $\dfrac{21n+4}{14n+3}$ 是既约分数.

证明：反证法，假设 $\dfrac{21n+4}{14n+3}$ 不是既约分数，则 $21n+4$ 和 $14n+3$ 有共同素因子 d，即

$$\begin{aligned}&\because(21n+4,14n+3)=d,21n+4=dm,14n+3=dn\\&\therefore 3\cdot dn-2\cdot dm=42n+9-(42n+8)=1=d(3n-2m)\end{aligned}$$

而 d 为大于 1 的素因子，$1\nmid d$，从而与假设矛盾，则 $\dfrac{21n+4}{14n+3}$ 是既约分数

习题1.2.2

设 m,n 为正整数, m 为奇数,证明:

$$(2^m-1,2^n+1)=1$$

证明：令 $(2^m-1,2^n+1)=d$，且有 $2^m-1=dx,2^n+1=dy,x,y\in Z$，$d$ 为奇数

$$\because 2^m=dx+1,2^n=dy-1\ \therefore 2^{mn}=(dx+1)^n=(dy-1)^m$$

将其二项式展开有 $\sum\limits_{i=0}^{n}C_n^i(dx)^i=\sum\limits_{i=0}^{m}C_m^i(dy)^i(-1)^{m-i}$，两边同时除以 d 得到

$$\sum_{i=1}^{n}C_n^id^{i-1}x^i+\frac{1}{d}=\sum_{i=1}^{m}C_m^id^{i-1}y^i(-1)^{m-i}+(-1)^m\cdot d^{-1}$$

由于 m 是奇数，若 $d\geq 3$，两边取整有 $\frac{1}{d}=1-\frac{1}{d}$，矛盾，从而 $d=1$

习题1.2.3

设 m,n,a 均为正整数, $a\geqslant 2$, 证明:

$$(a^m-1,a^n-1)=a^{(m,n)}-1.$$

证明：令 $(m,n)=d$，且有 $m=dx,n=dy,(x,y)=1$，由引理 1.1.1 知

$$\begin{aligned}a^d-1\mid a^{dx}-1,\ a^{dx}-1&=(a^d-1)\cdot(1+a^d+a^{2d}+\cdots+a^{(x-1)d})\\a^d-1\mid a^{dy}-1,\ a^{dy}-1&=(a^d-1)\cdot(1+a^d+a^{2d}+\cdots+a^{(y-1)d}),\end{aligned}$$

考虑辗转相除法，不妨设 $x>y$，

$$1+a^d+a^{2d}+\cdots+a^{(x-1)d}=a^{(x-y)d}(1+a^d+\cdots+a^{(y-1)d})+1+a^d+a^{2d}+\cdots+a^{(x-y-1)d}$$

继续判断 x 和 y 的大小关系，辗转相除，而 $(x,y)=1$，则

$$(1+a^d+a^{2d}+\cdots+a^{(x-1)d},1+a^d+a^{2d}+\cdots+a^{(y-1)d})=1$$

从而 $a^d-1=a^{(m,n)}-1$ 即为 a^m-1 和 a^n-1 的最大公因数

初等数论第二次作业 2022.3.2

习题1.2.4

设 $a,b,c\in Z,a\neq 0$。则 $a\mid bc$ 当且仅当 $\frac{a}{(a,b)}\mid c$

证明：取 $d=(a,b)$，令 $a=dx,b=dy$，且有 $(x,y)=1$

(1) 若 $a\mid bc$，$\exists t\in Z,\ bc=at\ \therefore yc=xt\ \ x\mid yc$，由于 $(x,y)=1$，得 $x\mid c$，即 $\frac{a}{(a,b)}\mid c$;

(2) 若 $\frac{a}{(a,b)}\mid c$，则 $\exists t\in Z,\ c=\frac{a}{(a,b)}\cdot t\ \therefore (a,b)\cdot c=at=dc=dxt$，即 $c=xt$，两边乘

以 $b=dy$ 得 $bc=xydt=ayt$，从而 $a\mid bc$。

综上，$a\mid bc\Longleftrightarrow \frac{a}{(a,b)}\mid c$

习题1.2.5

m 和 n 是互素的正整数，证明：

(1) 对每个整数 a，$(a,mn)=(a,m)(a,n)$;

(2) mn 的每个正因子 d 均可唯一地表示成 $d=d_1d_2$，其中 d_1 和 d_2 分别为 m 和 n 的正因子。

证明：(1) 对 $(a,mn)=(a,m)\cdot(\frac{a}{(a,m)},\frac{mn}{(a,m)})$，由于 $\frac{a}{(a,m)}$ 和 $\frac{m}{(a,m)}$ 互素，则

$$(a,mn)=(a,m)\cdot(\frac{a}{(a,m)},\frac{mn}{(a,m)})=(a,m)\cdot(\frac{a}{(a,m)},n)令\ a=k_1x,m=k_2x$$

$$\because (m,n)=1\ \therefore (k_2x,n)=(x,n)=1,(\frac{a}{(a,m)},n)=(k_1,n)=(k_1x,n)=(a,n)$$

则有 $(a,mn)=(a,m)(a,n)$

(2) 由算术基本定理，令 $m=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots p_r^{\alpha_r},n=q_1^{\beta_1}\cdot q_2^{\beta_2}\cdots q_k^{\beta_k},1\leq\alpha_i,\beta_i$，由 $(m,n)=1$

$\forall\ 1\leq i\leq r,1\leq j\leq k,p_i\neq q_j$，否则设相等素数为 p_{i_0} $(m,n)\geq p_{i_0}>1$ 矛盾，则有新序列集合

$\mathbb{S}=\{p_1,\cdots,p_r,q_1,\cdots,q_k\}$，有 $mn=p_1^{\alpha_1}\cdots p_r^{\alpha_r}\cdot q_1^{\beta_1}\cdots q_k^{\beta_k}$，若 d 为 mn 的因子，则

总有 $d=p_1^{\gamma_1}\cdots p_r^{\gamma_r}\cdot q_1^{\lambda_1}\cdots q_k^{\lambda_k},0\leq\gamma_i,\lambda_i$，则分离 $d_1=p_1^{\gamma_1}\cdots p_r^{\gamma_r},d_2=q_1^{\lambda_1}\cdots q_k^{\lambda_k}$

使得 $d=d_1d_2$，且由于 p_i 和 q_i 完全不同，该分解存在且唯一

习题1.2.6

设 n 为正整数，a,b 是不全为零的整数，证明：

(1) $(a^n,b^n)=(a,b)^n$；

(2) 若 a 和 b 是互素的正整数，$ab=c^n,c\in Z$，则 a 和 b 都是正整数的 n 次方幂。

证明：(1) 记 $(a,b)=d$，则有 $a=dx,b=dy,x,y\in Z$，从而 $a^n=d^nx^n,b^n=d^ny^n$

从而 $d^n\mid a^n,d^n\mid b^n,d^n\mid (a^n,b^n)$，则令 $(a^n,b^n)=td^n,t\in Z$，代入上式有

$\frac{a^n}{(a^n,b^n)}=tx^n,\ \frac{b^n}{(a^n,b^n)}=ty^n$，结合 $(x^n,y^n)=1$ 有 $1=(\frac{a^n}{(a^n,b^n)},\frac{b^n}{(a^n,b^n)})=t$，

$\therefore (a^n,b^n)=1\cdot d^n=(a,b)^n$

(2) 由算术基本定理，令 $a=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots p_r^{\alpha_r},b=q_1^{\beta_1}\cdot q_2^{\beta_2}\cdots q_k^{\beta_k},1\le\alpha_i,\beta_i$，由 $(a,b)=1$

$\forall\ 1\le i\le r,1\le j\le k,p_i\ne q_j$，否则设相等素数为 p_{i_0} $(m,n)\ge p_{i_0}>1$ 矛盾，则有新序列集合

$\mathbb{S}=\{p_1,\cdots,p_r,q_1,\cdots,q_k\}$，有 $ab=p_1^{\alpha_1}\cdots p_r^{\alpha_r}\cdot q_1^{\beta_1}\cdots q_k^{\beta_k}=c^n$，同理对 c 分解有

$c=m_1^{\gamma_1}\cdots m_l^{\gamma_l}$，代入有 $p_1^{\alpha_1}\cdots p_r^{\alpha_r}\cdot q_1^{\beta_1}\cdots q_k^{\beta_k}=m_1^{n\gamma_1}\cdots m_l^{n\gamma_l}$，由算术基本定理有

$\alpha_i=n\gamma_{a_i},\beta_i=n\gamma_{b_i}$，则 a 和 b 均能写成某个正整数的 n 次幂

习题1.29

求 $963x+657y=(963,657)$ 的全部整数解。

解：由欧几里得辗转相除法有

$$963=657+306\longrightarrow 657=306\times 2+45\longrightarrow 306=45\times 6+36$$
$$\longrightarrow 45=36\times 1+9\longrightarrow 36=9\times 4$$

从而 $(963,657)=9$，依次反向欧几里得算法有

$$9=45-36\times 1=45-(306-45\times 6)=45\times 7-306=(657-306\times 2)\times 7-306$$
$$=657\times 7-306\times 15=657\times 7-306\times 15=657\times 7-(963-657)\times 15$$
$$=963\times(-15)+657\times 22$$

则 $963x+657y=(963,657)=9$，可以化为 $107x+73y=1$，从而其解为

$$\begin{cases}x=-15+73t\\y=22-107t\end{cases}\quad t\in Z$$

习题1.2.10

求下列方程的全部整数解：

(1) $6x+20y-15z=23$；

(2) $25x+13y+7z=2$。

---

(1) 由 $(20,15)=5$，则 $6x+20y-15z=23 \Longleftrightarrow \begin{cases}20y-15z=5\omega\cdots①\\6x+5\omega=23\cdots②\end{cases}$

对②，由 $6=5\times1+1$，则 $1=6\times1+5\times(-1)$，则 ② 解为 $\begin{cases}x=23+5t\\\omega=-23-6t\end{cases}$

代入 ① 变形为 $4y-3z=\omega=-23-6t$，由 $4=3\times1+1$，则解 $\begin{cases}y=\omega+3u\\z=\omega+4u\end{cases}$

从而 $6x+20y-15z=23$ 的通解为 $\begin{cases}x=23+5t\\y=-23-6t+3u\\z=-23-6t+4u\end{cases}\quad t,u\in Z$

(2) 由 $(13,7)=1$，则 $25x+13y+7z=2 \Longleftrightarrow \begin{cases}13y+7z=\omega\cdots①\\25x+\omega=1\cdots②\end{cases}$

对②，由 $25=25\times1$，则 $1=25\times0+1\times1$，则 ② 解为 $\begin{cases}x=t\\\omega=1-25t\end{cases}$

代入 ① 变形为 $13y+7z=\omega=1-25t$，由 $1=7\times2-13$，则解 $\begin{cases}y=-\omega+7u\\z=2\omega-13u\end{cases}$

从而 $25x+13y+7z=2$ 的通解为 $\begin{cases}x=t\\y=-1+25t+7u\\z=2-50t-13u\end{cases}\quad t,u\in Z$

习题1.2.12

设 $f(x)=x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n$ 为首项系数为 1 的整系数多项式，

则 $f(x)$ 的每个有理根必为整数。

证明：若整系数多项式 $x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n=0$ 有理根为 $\frac{p}{q}(p,q\in Z,q\neq0)$

$$\because (p,q)=1,(\frac{p}{q})^n+a_1(\frac{p}{q})^{n-1}+\cdots+a_{n-1}\frac{p}{q}+a_n=0$$

$$\therefore p^n=-(a_1p^{n-1}q+\cdots+a_{n-1}pq^{n-1}+a_nq^n)\ \therefore q\mid p^n\Longrightarrow q=1$$

从而所有有理根必为整数

习题1.2.13

设 m 和 n 为正整数，则在 $n, 2n, \cdots, mn$ 这 m 个数当中恰有 (m,n) 个是 m 的倍数。

证明：令 $d=(m,n)$，且 $m=dx, n=dy, (x,y)=1$，从而 $kn, k=1,2,\cdots,m$ 满足

$m \mid kn, dx \mid kdy \Longrightarrow x \mid ky$，由于 $(x,y)=1$，则 $x \mid k$，即 k 是 x 的倍数，即 $k=xt, t \in Z$

而 $m=dx$，恰好为 $1\cdot x, 2\cdot x \cdots, d\cdot x$ ，恰共有 $d=(m,n)$ 个

习题1.2.16

设 m 和 n 是互素的非零整数。证明对整数 a，若 $m \mid a, n \mid a$，则 $mn \mid a$

证明：已知 $(m,n)=1$，由 $m,n \mid a$，设 $a=mx=ny, x,y \in Z$，有 $(mx,nx)=x(m,n)=x$

代入 $mx=ny$ 得 $x=(ny,nx)=n(y,x)$，则 $n \mid x, mn \mid mx=a$，即 $mn \mid a$

习题1.3.3

设 a,b,c 为正整数，证明

(1) $(a,[b,c])=[(a,b),(a,c)]$；

(2) $[a,(b,c)]=([a,b],[a,c])$。

证明：由算术基本定理，设 a,b,c 三者分解下所有质因数的交集为 $\{p_1 \cdots p_N\}$，且三者对应的

幂次为 $\{a_n\},\{b_n\},\{c_n\}, 0 \le a_i, b_i, c_i \in Z$，即 $a,b,c=\prod p_i^{a_i,b_i,c_i}$

(1) $(a,[b,c])=\prod p_i^{\min(a_i,\max(b_i,c_i))}$ 和 $[(a,b),(a,c)]=\prod p_i^{\max(\min(a_i,b_i),\min(a_i,c_i))}$

$(a,[b,c])=[(a,b),(a,c)] \Longleftrightarrow \min(a_i,\max(b_i,c_i))=\max(\min(a_i,b_i),\min(a_i,c_i))$

而对后者，调换 b 和 c 对等式左右两边都不变，不妨设 $b \le c$，从而分类以下三种情况：

$$i)a \le b \le c; \quad ii)b \le a \le c; \quad iii)b \le c \le a$$

$$i)\max\{a,\min\{b,c\}\}=\max\{a,b\}=b, \min\{\max\{a,b\},\max\{a,c\}\}=\min\{b,c\}=b;$$
$$ii)\max\{a,\min\{b,c\}\}=\max\{a,b\}=a, \min\{\max\{a,b\},\max\{a,c\}\}=\min\{a,c\}=a;$$
$$iii)\max\{a,\min\{b,c\}\}=\max\{a,b\}=a, \min\{\max\{a,b\},\max\{a,c\}\}=\min\{a,a\}=a;$$

从而后者成立，有 $(a,[b,c])=[(a,b),(a,c)]$ 成立

(2) 仿照 (1) 讨论 $\max(a_i,\min(b_i,c_i))=\min(\max(a_i,b_i),\max(a_i,c_i))$，也不妨设 $b \le c$

$$i)a \le b \le c; \quad ii)b \le a \le c; \quad iii)b \le c \le a$$
$$i)\min\{a,\max\{b,c\}\} = \min\{a,c\} = a, \max\{\min\{a,b\},\min\{a,c\}\} = \max\{a,a\} = a;$$
$$ii)\min\{a,\max\{b,c\}\} = \min\{a,c\} = a, \max\{\min\{a,b\},\min\{a,c\}\} = \max\{b,a\} = a;$$
$$iii)\min\{a,\max\{b,c\}\} = \min\{a,c\} = c, \max\{\min\{a,b\},\min\{a,c\}\} = \max\{b,c\} = c;$$

从而同理可得 $[a,(b,c)] = ([a,b],[a,c])$

习题1.3.4

不存在整数 $m \ge 2$ ，使得 $m^2 \mid n$ 的正整数 n 为无平方因子，证明：

(1) 正整数 n 是无平方因子当且仅当 $n = 1$ 或者是不素因子的乘积；

(2) 每个正整数 n 可以唯一地表示成 $n = m^2 \cdot n'$，其中 m^2 为平方数，而 n' 为无平方因子整数。

证明：(1) 若 $n = 1$ ，$\forall m \ge 2,\ m^2 \nmid n$，从而 1 为无平方因子，若 $n \ge 2$，由算术基本定理

令 $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$，若 $\exists\, \alpha_i \ge 2$，则取 $p_i^2 \mid p_i^{\alpha_i} \mid n$，则不是无平方因子，从而

$\forall\, \alpha_i \le 1$，而 $\alpha_i = 0$ 无意义（$p_i^0 = 1$），从而此时 n 为不同素因子乘积

又若 $n = 1$ 或者 n 为不同素因子乘积，显然满足无平方因子条件，从而两者等价

(2) 若 n 为无平方因子，则 $n = 1^2 \cdot n'$ 满足条件，若 n 不为无平方因子，由 (1) 得，$\exists\, \alpha_i \ge 2$

则挑选 $\mathbb{A} = \{i \mid \alpha_i \ge 2\}$，对 $\forall\, x \in \mathbb{A}$ 取 $\beta_i = 2\lfloor \dfrac{\alpha_i}{2} \rfloor, \gamma_i = \alpha_i - \beta_i = 0, 1$

则所有非 $\mathbb{A}$ 中的 α_j 以及 γ_i 对应素数幂次的乘积组成无平方因子 $n' = \displaystyle\prod_{\alpha_j \notin \mathbb{A}} p_j^{\alpha_j} \cdot \prod_{\alpha_i \in \mathbb{A}} p_i^{\gamma_i}$

其余组成完全平方数 $m^2 = \displaystyle\prod_{\alpha_i \in \mathbb{A}} p_i^{\beta_i} = \prod_{\alpha_i \in \mathbb{A}} p_i^{2\lfloor \frac{\alpha_i}{2} \rfloor}$，即 $m = \displaystyle\prod_{\alpha_i \in \mathbb{A}} p_i^{\lfloor \frac{\alpha_i}{2} \rfloor}$，使得 $n = m^2 \cdot n'$

下证其唯一性：若有两组 $(m_1, n_1'), (m_2, n_2')$ 使得 $n = m_1^2 n_1' = m_2^2 n_2'$，由 (1) 知

n_1 和 n_2 为 1 或者是不同素数的乘积，若两者不相同，则两边消去相同部分后总会剩余成单素数

即 $n'' = m_1^2 \prod p_i = m_2^2 \prod q_i$，考察 p_i 对应的幂次有左侧为奇次幂，右侧为偶次幂

这与 n'' 的算术基本定理矛盾，从而每个正整数能唯一地表示成完全平方数和无平方因子的乘积

初等数论第三次作业　　2022.3.8

习题1.2.1

设 m 为正整数, $(a,m)=1$. 我们用 a^{-1} 表示同余方程 $ax\equiv 1\pmod m$ 的任何一个整数解 (即 $a^{-1}\in\mathbf{Z}, aa^{-1}\equiv 1(\bmod m)$). 证明:

(1) 若 $(a,m)=(b,m)=1$, 则 $a\equiv b(\bmod m)\Longleftrightarrow a^{-1}\equiv b^{-1}(\bmod m)$;

(2) 若 $\{r_1,r_2,\cdots,r_{\varphi(m)}\}$ 是模 m 的缩系, 则 $\{r_1^{-1},r_2^{-1},\cdots,r_{\varphi(m)}^{-1}\}$ 也是模 m 的缩系。

证明：(1) 若 $a\equiv b(\bmod m)$，即 $a-b=k_1m,k_1\in Z$，令 a^{-1} 与 b^{-1} 中最小的正整数为 a_-,b_-，对上式乘以 a_-,b_- 得 $aa_-b_--a_-(bb_-)=k_1ma_-b_-$，两边对 m 求同余有 $a_-\equiv b_-(\bmod m)$，而 $\overline{a^{-1}}=a_-+km,k\in Z,\overline{b^{-1}}=b_-+km,k\in Z$ 则 $a\equiv b(\bmod m)\Longrightarrow a^{-1}\equiv b^{-1}(\bmod m)$，由对称性（$(a^{-1})^{-1}=a$），两者等价

(2) 由 $r_ir_i^{-1}\equiv 1(\bmod m)$，若 $(r_i^{-1},m)\geq 2$，则 $(r_ir_i^{-1},m)\geq 2$，与 $r_ir_i^{-1}\equiv 1(\bmod m)$ 矛盾，从而所有的 r_i^{-1} 与 m 互素；又若 $\exists\, i\neq j, r_i^{-1}=r_j^{-1}$，由 (1) 得 $r_i=r_j$，矛盾

而 m 的缩系有 $\varphi(m)$ 个，从而 $\{r_1^{-1},\cdots,r_{\varphi(m)}^{-1}\}$ 也为缩系

习题1.2.2

设正整数 n 的十进制表示为

$$n=a_0+a_1\cdot 10+a_2\cdot 10^2+\cdots+a_k\cdot 10^k,$$

证明: $\begin{cases} n\equiv a_0+a_1+\cdots+a_k(\bmod 9),\\ n\equiv a_0-a_1+a_2-\cdots+(-1)^k a_k(\bmod 11). \end{cases}$ 用这些结果来计算 12345×6789 被 9 和 被 11 除所得的余数。

证明：由 $u=\sum_{i=0}^{k}a_i10^i$，且 $10^i\equiv(9+1)^i\equiv 1+9^i\equiv 1(\bmod m)$

$10^i\equiv(11-1)^i\equiv(-1)^i+11^i\equiv(-1)^i(\bmod m)$，代入则得到

$$\begin{cases} n \equiv \sum\limits_{i=0}^{k} a_i (\mathrm{mod}\ 9), \\ n \equiv \sum\limits_{i=0}^{k} (-1)^i a_i (\mathrm{mod}\ 11). \end{cases}$$

代入计算 $12345 \times 6789 \equiv 15 \times 30 \equiv 0 (\mathrm{mod}\ 9)$，$12345 \times 6789 \equiv 3 \times 2 \equiv 6 (\mathrm{mod}\ 11)$

习题1.2.6

证明：当 $n \geqslant 3$ 时，$\varphi(n)$ 为偶数。

证明：① 若 n 有奇素数因子，则 $\varphi(n) = \prod\limits_i (p_i^{\alpha_i} - p_i^{\alpha_i - 1})$ 中对奇素数因子 $(p_i^{\alpha_i} - p_i^{\alpha_i - 1})$

总为偶数，从而此时 $\varphi(n) \equiv 0 (\mathrm{mod}\ 2)$

② 若 n 没有奇素数因子，由于 $n \geq 3$，则 $n = 2^k, k \geq 2$，此时 $\varphi(n) = 2^{k-1}$ 也为偶数

从而 $\forall\, n \geq 3$，$\varphi(n)$ 为偶数

习题1.2.7

设 m 和 n 是正整数，$m = nt (t \in \mathbf{Z})$. 证明: 模 n 的每个同余类都是模 m 的 t 个同余类之并。

证明：对 m 中特定 $\overline{a}$ ，取 $\overline{a}, \overline{a} + \overline{n}, \cdots, \overline{a} + (t-1)\overline{n}$ 共 t 个同余类，这些元素均模 n 余数为 a 模 n，而 $\overline{a}$ 取遍 $0, 1, \cdots, n-1$，得到模 n 的每个同余类。

习题1.2.10

设 $a, m \in \mathbf{Z}, m \geqslant 2, (a, m) = 1$. 计算 $\sum\limits_{x=0}^{m-1} \left[\dfrac{ax}{m} \right]$.

解：由于 $\{ax \big| x = 0, 1, \cdots, m-1\}$ 为 m 的完系，则拆开 $\left[\dfrac{ax}{m} \right] = \dfrac{ax}{m} - \{ \dfrac{ax}{m} \}$，则

$$\begin{aligned} \sum_{x=0}^{m-1} \left[\frac{ax}{m} \right] &= \frac{a}{m} \sum_{x=0}^{m-1} x - \frac{1}{m}(0 + 1 + \cdots + (m-1)) = \frac{a}{m} \cdot \frac{m(m-1)}{2} - \frac{m(m-1)}{2m} \\ &= \frac{a(m-1)}{2} - \frac{m-1}{2} = \frac{(a-1)(m-1)}{2} \end{aligned}$$

> 更一般地，对 $\forall\, a,m\in \mathbf{Z}$，都有 $\sum\limits_{x=0}^{m-1}\left[\dfrac{ax}{m}\right]=\dfrac{am-a-m+(a,m)}{2}$

习题2.2.1

设 α 是环 Z_m 中非零元素。若存在 Z_m 中非零元素 $\beta(\neq \overline{0})$, 使得 $\alpha\beta=\overline{0}$, 称 α 是零因子，证明：

(1) 非零元素 α 是零因子当且仅当 α 不可逆. 从而 Z_m 由彼此不同的三类元素构成：$\overline{0},\varphi(m)$ 个可逆元和 $m-\varphi(m)-1$ 个零因子;

(2) Z_m 中没有零因子当且仅当 m 是素数。

证明：(1) 若 $\alpha(\neq \overline{0})$ 是零因子，反证法，若 α 可逆，则 $\alpha\alpha^{-1}\equiv 1(\mathrm{mod}\, m)$，两边乘以 $\beta(\neq \overline{0})$ 得 $\alpha\beta\alpha^{-1}\equiv \beta(\mathrm{mod}\, m)$，左边为 0，右边不为 0，矛盾，从而 α 不可逆；又若 α 不可逆，则有 $\forall\, \beta\neq 0,\alpha\beta\neq 1$。则考虑 $\{0,\overline{\alpha},\overline{2\alpha},\cdots,\overline{(m-1)\alpha}\}$ ，该集合不为模 m 的同余类，否则一定能找到 $\overline{1}$ 与 α 不可逆的条件矛盾，则 $\exists\, i,j\in[1,m-1],\overline{i\alpha}=\overline{j\alpha}$，从而取 $\beta=i-j$，α 为零因子

(2) 若 m 为素数，$\varphi(m)=m-1$，则有 $m-\varphi(m)-1=0$ 个零因子

若 $m-\varphi(m)-1=0$ 成立，则 $\varphi(m)=m-1$，若 m 为合数，$m=ab$，则 a 和 b 为零因子，$\varphi(m)\leq m-1-2$ 矛盾

习题2.2.2

(1) 对于环 Z_m 中任何元素 α，m 个 α 相加为 $\overline{0}$.

(2) 设 p 为素数. 对于域 Z_p 中非零元素 α 和正整数 n，证明： n 个 α 相加为 $\overline{0}$ 当且仅当 $p\mid n$。

证明：(1) 由 $\alpha_i=\alpha_0+k_i\cdot m$，这些 m 个 α 之和为 $m\alpha_0+m\sum\limits_{i=1}^{m}k_i$，均模 m 余 0

而且对于 $\overline{0}$ 中的所有元素 Km，都能找到 k_i 使得 $\alpha_0+\sum\limits_{k=1}^{m}k_i=K$，则相加为 $\overline{0}$

(2) 若 $p\mid n$，有 n 个 α 相加后模 m 为 0，则 n 个 α 相加为 $\overline{0}$；又若 n 个 α 相加为 $\overline{0}$ 时

令 $\alpha_i=\alpha_0+k_i\cdot m$，相加后模 m 得 $n\alpha_0\equiv 0(\mathrm{mod}\, p)$，而 $\alpha_0=0,1,\cdots,p-1$

$(\alpha_0,p)=1$，则 $n\equiv 0(\mathrm{mod}\, p)$，即 $p\mid n$

习题2.2.3

证明当 p 为奇素数时，$2^{p-1}\cdot\left(\left(\frac{p-1}{2}\right)!\right)^2\equiv(-1)^{\frac{p+1}{2}}(\mathrm{mod}\ p)$。

证明：$2^{p-1}(\frac{p-1}{2}\cdot\frac{p-3}{2}\cdots\frac{4}{2}\cdot\frac{2}{2})^2=(p-1)^2(p-3)^2\cdots4^2\cdot2^2$，使用补偿法有

$$\begin{aligned}(p-1)^2(p-3)^2\cdots4^2\cdot2^2&\equiv2\cdot4\cdot6\cdots(p-1)\cdot(p-1)\cdot(p-3)\cdots4\cdot2\\&\equiv2\cdot4\cdot6\cdots(p-1)\cdot(p-(p-1))\cdot(p-(p-3))\cdots(p-4)\cdot(p-2)\cdot(-1)^{\frac{p-1}{2}}\\&\equiv2\cdot4\cdots(p-1)\cdot3\cdot5\cdots(p-2)\cdot(-1)^{\frac{p-1}{2}}\equiv(p-1)!(-1)^{\frac{p-1}{2}}\equiv(-1)^{\frac{p+1}{2}}(\mathrm{mod}\ p)\end{aligned}$$

其中使用威尔逊定理，对素数 p ，有 $(p-1)!\equiv-1(\mathrm{mod}\ p)$

习题2.2.4

对于整数 $m\geqslant2$, 证明: $(m-1)!\equiv-1(\mathrm{mod}\ m)$ 当且仅当 m 是素数。(判别 m 是否为素数)

证明：若 m 为素数，则由威尔逊定理得 $(m-1)!\equiv-1(\mathrm{mod}\ m)$；若 m 为合数，则 $m=ab$，

其中 $2\leq a\leq b$，则 $1\leq a,b\leq m-1$，从而 $(m-1)!$ 中一定能凑齐 m，此时模为 0

习题2.2.5

若 $Z_m^*=\left\{\alpha_1,\cdots,\alpha_{\phi(m)}\right\}$，则 $Z_m^*=\left\{\alpha_1^{-1},\cdots,\alpha_{\phi(m)}^{-1}\right\}$。如何将它转述成同余的语言?

证明：缩系等价性证明在习题 1.2.1 中。定义 $\alpha_ix_i\equiv1(\mathrm{mod}\ m)$ 中 x_i 的可取值为 α_i^{-1}

转述为 $(\alpha_i,m)=1$，所有 α_i 构成 Z_m^*，由 $\alpha_ix_i\equiv1(\mathrm{mod}\ m)$中，所有 x_i 也构成 Z_m^*

习题2.3.1

设 n 和 m 是互素的正整数，证明： $m^{\varphi(n)}+n^{\varphi(m)}\equiv1(\mathrm{mod}\ mn)$。

证明：由欧拉-费马定理，$m^{\varphi(n)}\equiv1(\mathrm{mod}\ n),n^{\varphi(m)}\equiv1(\mathrm{mod}\ m)$，且由$\varphi(x)\geq1$，得

$m^{\varphi(n)}\equiv0(\mathrm{mod}\ m),n^{\varphi(m)}\equiv0(\mathrm{mod}\ n)$，从而

$$m^{\varphi(n)}+n^{\varphi(m)}\equiv 1(\mathrm{mod}\ m), m^{\varphi(n)}+n^{\varphi(m)}\equiv 1(\mathrm{mod}\ n)$$

则 $m^{\varphi(n)}+n^{\varphi(m)}=1+mk_1=1+nk_2$，由于 $(m,n)=1$，则 $n\mid k_1$，原式成立

习题2.3.2

(1) 对每个与 10 互素的整数 a, 证明: $a^{20}\equiv 1(\mathrm{mod}\ 100)$;

(2) 求 3^{193} 的十进制表达式中的个位和十位数字。

解：(1) 由 $\varphi(4)=2,\varphi(25)=20$，结合 $(a,4)=(a,25)=1$ 有 $a^{20}\equiv 1(\mathrm{mod}\ 25)$，

$a^2\equiv 1(\mathrm{mod}\ 4)$，$a^{20}\equiv (a^2)^{10}\equiv 1(\mathrm{mod}\ 4)$，而 $(4,25)=1$，则 $a^{20}\equiv 1(\mathrm{mod}\ 100)$

(2) 由 $3^{193}\equiv 3^{160}\cdot 3^{33}\equiv 27^{11}\equiv 2^{11}\equiv 23(\mathrm{mod}\ 25)$，且 $3^{193}\equiv (-1)^{193}\equiv 3(\mathrm{mod}\ 4)$，

从而最后两位为 23

习题2.3.3

(1) 设 $a,b\in\mathbf{Z},n\geqslant 1,p$ 为素数。如果 $a\equiv b\left(\mathrm{mod}\ p^n\right)$，证明：对每个整数 $k\geqslant 0$，

$$a^{p^k}\equiv b^{p^k}\left(\mathrm{mod}\ p^{n+k}\right)$$

(2) 证明: 对每个奇数 a 和 $k\geqslant 1, a^{2^k}\equiv 1\left(\mathrm{mod}\ 2^{k+2}\right)$.

证明：(1) 令 $b=a+x\cdot p^n, x\in Z$，代入使用二项式展开有

$$b^{p^k}-a^{p^k}=(a+x\cdot p^n)^{p^k}-a^{p^k}=\sum_{i=1}^{k}C_{p^k}^{i}b^i(x\cdot p^n)^{p^k-i}$$

其中 $p^k\mid C_{p^k}^{i}$，且有 $p^n\mid (x\cdot p^n)^{p^k-i}$，从而 $a^{p^k}\equiv b^{p^k}\left(\mathrm{mod}\ p^{n+k}\right)$

(2) 由 a 为奇数，令 $a=2i+1$，则 $a^2=4i(i+1)+1$，且 i 和 $i+1$ 一奇一偶，从而

$a^2\equiv 1(\mathrm{mod}\ 2^3)$，代入 (1) 中结论有 $(a^2)^{2^k}\equiv 1(\mathrm{mod}\ 2^{3+k})$，令 $k'=k+1\geq 1$ 则有

$k'\geqslant 1, a^{2^{k'}}\equiv 1\left(\mathrm{mod}\ 2^{k'+2}\right)$，得证

初等数论第四次作业　　2022.3.15

习题2.1.3

解下列同余方程。

(1) $8x \equiv 5 (\mathrm{mod}\ 23)$;　　(2) $60x \equiv 7 (\mathrm{mod}\ 37)$.

解：(1) 由 $(8, 23) = 1$，则在 Z_{23} 中有唯一解，利用费马小定理

$$x \equiv 8^{\varphi(23)-1} \cdot 5 \equiv 8^{21} \cdot 5 \equiv 64^{10} \cdot 40 \equiv 5^{10} \cdot (-6) \equiv -(25)^5 \cdot 6 \equiv -2^5 \cdot 6 \equiv 15 \pmod{23}$$

(2) 由 $(60, 37) = 1$，则在 Z_{37} 中有唯一解，利用费马小定理

$$\begin{aligned} x &\equiv 60^{\varphi(37)-1} \cdot 7 \equiv (-14)^{35} \cdot 7 \equiv 196^{17} \cdot 13 \equiv 11^{17} \cdot 13 \\ &\equiv 10^8 \cdot (-5) \equiv -5 \cdot 11^4 \equiv -5 \cdot 10^2 \equiv (-5) \cdot (-11) \equiv 18 \pmod{37} \end{aligned}$$

习题2.1.4

对每个整数 n，证明：

$$\begin{aligned} &(1) n^2 \neq 2 (\mathrm{mod}\ 3); \quad (2) n^2 \equiv 0 \text{或} 1 (\mathrm{mod}\ 4); \\ &(3) n^3 \equiv 0, 1 \text{或} -1 (\mathrm{mod}\ 9); \quad (4) n^4 \equiv 0 \text{或} 1 (\mathrm{mod}\ 16). \end{aligned}$$

证明：(1) 由费马小定理，若 $(n, 3) = 1, n^{\varphi(3)} \equiv n^2 \equiv 1 \pmod{3}$，且若 $(n, 3) > 1$，则 $3 \mid n$，

此时有 $n^2 \equiv 0 \pmod{3}$，则 $n^2 \neq 2 \pmod{3}$

(2) 由费马小定理，若 $(n, 4) = 1, n^{\varphi(4)} \equiv n^2 \equiv 1 \pmod{4}$，且若 $(n, 4) > 0$，有 $2 \mid 4$

此时有 $n^2 \equiv 0 \pmod{4}$，则 $n^2 \equiv 0$或$1 \pmod{4}$

(3) 由费马小定理，若 $(n, 9) = 1, n^{\varphi(9)} \equiv n^6 \equiv 1 \pmod{9}$，即此时 $n^3 \equiv \pm 1 \pmod{9}$

若 $(n, 9) > 1$，则 $3 \mid 9$，此时 $n^3 \equiv 0 \pmod{9}$，则 $n^3 \equiv 0, \pm 1 \pmod{9}$

(4) 由费马小定理，若 $(n, 16) = 1, n^{\varphi(16)} \equiv n^8 \equiv 1 \pmod{16}$，此时分解因式有

$$(n^4 - 1)(n^4 + 1) \equiv 0 \pmod{16}$$

而 $n^4 \equiv 1 \pmod{8}$，故 $n^4 \equiv 1, 9 \pmod{16}$ 综上有 $n^4 \equiv 0, 1 \pmod{16}$

习题2.1.5

设 a 为奇数, $n \geqslant 1$. 证明: $a^{2^n} \equiv 1 \left(\mathrm{mod}\ 2^{n+2}\right)$

证明：（**使用归纳法，二项式展开较复杂**）对 $n=1$ 时成立（第一次作业第一题）

若 $n=k$ 时成立，即 $a^{2^k} \equiv 1 \pmod{2^{k+2}}$则存在 $t \in Z, a^{2^k}=1+2^{k+2} \cdot t$，则

$$a^{2^{k+1}} \equiv (a^{2^k})^2 \equiv (1+2^{k+2}t)^2 \equiv 1+2^{k+3}t+2^{2k+4}t^2 \equiv 1 \pmod{2^{k+3}}$$

由数学归纳法知，对 $\forall\, n \geq 1$ 均成立

习题2.4.1

解下列同余方程：(1) $32x \equiv 12(\mathrm{mod}\ 8)$;　(2) $28x \equiv 124(\mathrm{mod}\ 116)$;　(3) $5x \equiv 44(\mathrm{mod}\ 81)$

解：(1) 由判定 $(32,8)=8 \nmid 12$，则在 Z_8 下无解

(2) 由判定 $(28,116)=4 \mid 124$，则在 Z_{116} 下有 4 组解， $7x \equiv 31 \pmod{29}$，由费马小定理

$$x \equiv 7^{\varphi(29)-1} \cdot 31 \equiv 7^{27} \cdot 2 \equiv 49^{13} \cdot 14 \equiv -9^{13} \cdot 14 \equiv 6^6 \cdot 19 \equiv 7^3 \cdot 19 \equiv 21 \pmod{29}$$

则解为 $x \equiv 21, 50, 79, 108$

(3) 由判定 $(5,81)=1 \mid 44$，则在 Z_{81} 下有 1 组解，有 $5x \equiv 44 \equiv 125 \pmod{81}$

得 $x \equiv 25 \pmod{81}$

习题2.4.2

解下列同余方程组：

$$(1)\begin{cases} x \equiv 1(\mathrm{mod}\ 3), \\ x \equiv 1(\mathrm{mod}\ 5), \\ x \equiv 2(\mathrm{mod}\ 7); \end{cases} \quad (2)\begin{cases} x \equiv 2(\mathrm{mod}\ 4), \\ x \equiv 3(\mathrm{mod}\ 5) \\ x \equiv 7(\mathrm{mod}\ 9) \end{cases}$$

解：(1) 由中国剩余定理，有 $M_1=35, M_2=21, M_3=15$，而对应有

$$35M_1^{-1} \equiv 1 \pmod{3},\ 21M_2^{-1} \equiv 1 \pmod{5},\ 15M_3^{-1} \equiv 1 \pmod{7}$$

得 $M_1^{-1}=2, M_2^{-1}=1, M_3^{-1}=1$，则 $x \equiv 35 \cdot 2 \cdot 1+21 \cdot 1 \cdot 1+15 \cdot 1 \cdot 2 \equiv 16 \pmod{105}$

(2) 由中国剩余定理，有 $M_1=45, M_2=36, M_3=20$，而对应有

$$45M_1^{-1}\equiv 1 \pmod 4,\ 36M_2^{-1}\equiv 1 \pmod 5,\ 20M_3^{-1}\equiv 1 \pmod 9$$

得 $M_1^{-1}=1, M_2^{-1}=1, M_3^{-1}=5$，则 $x\equiv 45\cdot 1\cdot 2+36\cdot 1\cdot 3+20\cdot 5\cdot 7\equiv 178 \pmod{180}$

习题2.4.3

用中国剩余定理解同余方程 $37x\equiv 31(\mathrm{mod}\ 77)$.

解：由 $77=7\cdot 11$，对质因数 7 而言， $37x\equiv 31\equiv 185 \pmod 7$，则 $x\equiv 5 \pmod 7$

对质因数 11 而言，$37x\equiv 31\equiv 185 \pmod{11}$，则 $x\equiv 5 \pmod{11}$

则由中国剩余定理，显然 $x\equiv 5 \pmod{77}$，为原方程的解，且该解唯一

习题2.4.4

求 2^{400} 被 319 除的余数.

解：$319=11\cdot 29$，对质因数 11 ，$2^{400}\equiv 32^{80}\equiv(-1)^{80}\equiv 1 \pmod{11}$，对质因数 29

$$2^{400}\equiv 32^{80}\equiv 3^{80}\equiv 27^{26}\cdot 9\equiv 2^{26}\cdot 9\equiv 32^5\cdot 18\equiv 3^5\cdot 18\equiv 27^2\cdot 6\equiv 24 \pmod{29}$$

则转化成一次同余方程组 $\begin{cases}2^{400}\equiv 1 \pmod{11}\\ 2^{400}\equiv 24 \pmod{29}\end{cases}$，由中国剩余定理有

$M_1=29, M_2=11, M_1^{-1}\cdot 29\equiv 1 \pmod{11}, M_2^{-1}\cdot 11\equiv 1 \pmod{29}$

解得 $M_1^{-1}=8, M_2^{-1}=8$，则 $2^{400}\equiv 29\cdot 8+11\cdot 8\cdot 24\equiv 2344\equiv 111 \pmod{319}$

习题2.4.5

设 m_1, m_2 是正整数, $b_1, b_2\in\mathbf{Z}$. 证明: 同余方程组

$$\begin{cases}x\equiv b_1 (\mathrm{mod}\ m_1),\\ x\equiv b_2 (\mathrm{mod}\ m_2)\end{cases}$$

有整数解的充分必要条件是 $(m_1,m_2)\mid b_1-b_2$，且此条件成立时, 解为模 $[m_1,m_2]$ 的一个同余类.

证明：(1) **充要性**：若 $\begin{cases}x\equiv b_1 (\mathrm{mod}\ m_1),\\ x\equiv b_2 (\mathrm{mod}\ m_2)\end{cases}$ 有整数解，则 $x=m_1y_1+b_1=m_2y_2+b_2$，

两边除以 (m_1,m_2) 得到 $\dfrac{b_1-b_2}{(m_1,m_2)}=\dfrac{m_2y_2-m_1y_1}{(m_1,m_2)}\in Z$，此时有 $(m_1,m_2)\mid b_1-b_2$

若 $(m_1,m_2)\mid b_1-b_2$，有 $\frac{m_2y_2-m_1y_1}{(m_1,m_2)}=\frac{b_1-b_2}{(m_1,m_2)}\in Z$，而 $(\frac{m_1}{(m_1,m_2)},\frac{m_2}{(m_1,m_2)})=1$

由辗转相除法知，一定存在 y_{10},y_{20}，使得 $\frac{-m_1}{(m_1,m_2)}y_{10}+\frac{m_2}{(m_1,m_2)}y_{20}=1$

则扩大 $\frac{b_1-b_2}{(m_1,m_2)}$ 倍得到 y_1,y_2 的解，从而原同余方程组有解

(2) **同余类**：若上述条件成立时，对 $\frac{-m_1}{(m_1,m_2)}y_{10}+\frac{m_2}{(m_1,m_2)}y_{20}=1$ 有 y_{10} 对应解

所在同余类为模 $\frac{m_2}{(m_1,m_2)}$ ，而 $x=m_1y_1+b_1$ 则解为模 $\frac{m_1m_2}{(m_1,m_2)}=[m_1,m_2]$

习题2.4.6

设 m_1 和 m_2 是互素的正整数. 证明:

(1) 若 S_1 和 S_2 分别是模 m_1 和模 m_2 的完系. 则

$$S=\{m_1x_1+m_2x_2\mid x_1\in S_2,x_2\in S_1\}$$

是模 m_1m_2 的完系;

(2) 若 S_1 和 S_2 分别是模 m_1 和模 m_2 的缩系, 则

$$S=\{m_1x_1+m_2x_2\mid x_1\in S_2,x_2\in S_1\}$$

是模 m_1m_2 的缩系. (由此可知 $\varphi(m_1m_2)=\varphi(m_1)\varphi(m_2)$)

解：(1) 对 S 中的每个元素 $x_1=m_2y_1+t_1\in S_2,x_2=m_1y_2+t_2\in S_1$

$m_1x_1+m_2x_2=m_1m_2(y_1+y_2)+t_1m_1+t_2m_2$，其中，$y_1+y_2\in Z$ 能取遍所有整数

又由 $(m_1,m_2)=1$，由辗转相除法知 $\exists\, t_{10},t_{20}\in Z$，使得 $t_{10}m_1+t_{20}m_2=1$，

从而 $t_1m_1+t_2m_2$ 也能取遍 $0,1,\cdots,m_1m_2-1$，则 S 为模 m_1m_2 的完系

(2) 与 (1) 相比，对 $t_1m_1+t_2m_2$ 中 t_1,t_2 不是任意整数，需满足 $(t_1,m_2)=1,(t_2,m_1)=1$

此时 $t_1m_1+t_2m_2\nmid m_1m_2$，且由辗转相除法知，存在 t_{10},t_{20} 使得 $t_{10}m_1+t_{20}m_2=1$

且反证法若 $d=(t_{10},m_2)>1$，则上式对 d 同余有 $1\equiv 0\pmod d$，矛盾，t_{10},t_{20} 满足条件

对 $\forall\, 0\le x\le m_1m_2-1,(x,m_1m_2)=1$ $(x,m_1)=(x,m_2)=1$，取 xt_{10},xt_{20} 满足条件

从而 S 为 m_1m_2 的缩系

习题2.4.7

设 n 为正整数，证明：必有连续 n 个正整数，其中每个整数均被某个大于 1 的整数的平方所除尽。

证明：构造一次同余方程 $\begin{cases} x \equiv 0 \pmod{2^2} \\ x \equiv -1 \pmod{3^2} \\ x \equiv -2 \pmod{5^2} \\ \quad \vdots \\ x \equiv -(n-1) \pmod{p_n^2} \end{cases}$，其中 p_n 为第 n 个素数

对 $\forall\, p_i, p_j, (p_i^2, p_j^2) = 1$，由中国剩余定理，一定有最小正整数解 $x_{min}(n)$ 满足上述方程

该 x_{min} 能保证序列 $x_{min}, x_{min}+1, \cdots, x_{min}+(n-1)$ 中任何数能被某个大于 1 的整数平方整除

初等数论第五次作业　　2022.3.22

习题3.1.2

a 对模 m 和模 n 的阶分别为 s 和 t, 证明: a 对模 $[m,n]$ 的阶为 $[s,t]$.

证明：由 a 对模 m 和 模 n 的阶为 s,t，则 $a^s \equiv 1 \pmod{m}, a^t \equiv 1 \pmod{n}$

则令 a 对 $[m,n]$ 的阶为 r，即 $a^r \equiv 1 \pmod{[m,n]}$，有 $m,n \mid [m,n]$，则 $s,t \mid r$，则 $[s,t] \mid r$

又 $a^{[s,t]} \equiv (a^s)^{\frac{[s,t]}{s}} \equiv 1 \pmod{m}, a^{[s,t]} \equiv (a^t)^{\frac{[s,t]}{t}} \equiv 1 \pmod{n}$，则 $a^{[s,t]} \equiv 1 \mod [m,n]$

从而 $r \mid [s,t]$，则 $r = [s,t]$，即 a 对模 $[m,n]$ 的阶为 $[s,t]$

习题3.1.5

若 n 和 a 均是正整数, $a \geqslant 2$. 证明: $n \mid \varphi(a^n - 1)$.

证明：考虑 a 模 a^n-1 的阶 r，有 $a^n \equiv 1 \pmod{a^n-1}$，则 $r \mid n$，若 $r = \dfrac{n}{d}, d \geq 2$

但 $a^r = \sqrt[d]{a^n} \leq a^n - 1$，则此时 $a^r \not\equiv 1 \pmod{a^n-1}$，从而 $d=1$，即 a 模 a^n-1 阶为 n

由 a 模 a^n-1 阶一定为 $\varphi(a^n-1)$ 的因子，从而 $n \mid \varphi(a^n-1)$

习题3.1.6

如果 $n \geqslant 2$, 证明: $n \nmid 2^n - 1$.

证明：由于 $2^n - 1 \equiv 1 \pmod 2$，若 $2 \mid n$，则 $n \nmid 2^n - 1$，若 $2 \nmid n$，令 n 最小奇素数因子 p

则 $n = pt, t \in Z$，反证法若 $n \mid 2^n - 1$，令 $2^n = 1 + nx = 2^{pt} = 1 + ptx, x \in Z$

有 $2^{pt} \equiv 1 \pmod p$，而费马小定理给出 $2^{p-1} \equiv 1 \pmod p, 2^p \equiv 2 \pmod p$ 由 $pt \mid p - 1$ 矛盾

习题3.1.7

设 p 是奇素数, $n \geqslant 1$. 证明:

$$\sum_{k=1}^{p-1} k^n \equiv \begin{cases} -1 (\mathrm{mod}\ p), & \text{如果 } p-1 \mid n, \\ 0 (\mathrm{mod}\ p), & \text{如果 } p-1 \nmid n. \end{cases}$$

证明：由于 p 为奇素数，令其原根为 g，则 $Z_p = \{1, 2, \cdots, p-1\} = \{g, g^2, \cdots, g^{p-1}\}$

从而求和式 $\sum\limits_{k=1}^{p-1} k^n \equiv \sum\limits_{k=1}^{p-1} g^n \pmod p$，若 $p - 1 \mid n$，由费马小定理 $g^n \equiv g^{p-1} \equiv 1 \pmod p$

此时 $\sum\limits_{k=1}^{p-1} k^n \equiv \sum\limits_{k=1}^{p-1} 1 \equiv -1 \pmod p$，若 $p - 1 \nmid n$，则由等比数列求和

$$\sum_{k=1}^{p-1} g^n \equiv \frac{g^n(1 - g^{p-1})}{1 - g^n} \equiv \frac{g^n \cdot 0}{1 - g^n} (1 - g^n \neq 0) \equiv 0 \pmod p$$

从而 $\sum\limits_{k=1}^{p-1} k^n \equiv \begin{cases} -1 (\mathrm{mod}\ p), & \text{if } p-1 \mid n, \\ 0 (\mathrm{mod}\ p), & \text{if } p-1 \nmid n. \end{cases}$

习题3.1.8

(1) 设 $F_n = 2^{2^n} + 1$ (费马数), $n \geqslant 1$. 证明: F_n 的每个素因子都有形式 $2^{n+1}x + 1 (x \in \mathbf{Z})$.

(2) 对任意给定的整数 $l \geqslant 1$, 证明: 有无穷多个素数模 2^l 余 1 .

证明：(1) 对每个 F_n 的奇素数因子 p，有 $2^{p-1} \equiv 1 \pmod p$，而 $2^{2^n} \equiv -1 \pmod p$，两边平方

$2^{2^{n+1}} \equiv 1 \pmod p$，从而令 2 模 p 的次数为 r，则 $r \mid 2^{n+1}$，$r = 2^k$，显然 $k \neq n$，因为

$2^{2^n} \equiv -1 \pmod p$，若 $k < n$，则重复 $n - k$ 次平方操作得到 $2^{2^n} \equiv 1 \pmod p$ 与条件矛盾

从而 $r=2^{n+1}$，结合 $2^{p-1}\equiv 1\pmod{p}$ 可得 $2^{n+1}\mid p-1$

(2) 对任意两个不相同的费马数，F_m,F_n，不妨设 $m\geq n, m=n+k, k\geq 1\in Z$

则 $F_m=2^{2^{m+n}}+1=(2^{2^n})^{2^k}+1=(F_n-1)^{2^k}+1=p(F_n)+2$，其中 $p(F_n)$ 为多项式

从而 $(F_m,F_n)\mid 2$，又 $x\nmid F_n,F_m$，则 $(F_m,F_n)=1$，即所有费马数两两互素，而每个 F_n

都至少有一个素因子模 2^{n+1} 余 1，且不同费马数素因子不重合，则对给定的 l，取 $n\geq l-1$

则这些无穷个的费马数模 2^{n+1} 余 1，则也模 2^l 余 1

习题3.1.9

(1) 设 p 为奇素数, $a\geqslant 2$. 证明: 若 a^p-1 的素因子 q 不整除 $a-1$，则必有形式 $q=2px+1(x\in Z)$.

(2) 设 p 为给定的奇素数, 证明：形如 $2px+1(x\in\mathbb{Z})$ 的素数有无限多个.

证明：(1) 由于 q 为 a^p-1 素因子，则 $a^p\equiv 1\pmod{q}$，由 $q\nmid a-1$，得 $a\not\equiv 1\pmod{q}$

设 a 为模 q 的阶为 r，则有 $r\mid p$，又 $r\neq 1$，从而 $r=p$，有费马小定理 $a^{q-1}\equiv 1\pmod{q}$

从而 $r=p\mid q-1$；另一方面考虑奇偶性，若 $2\mid a$，$2\nmid a^p-1$，素因子 q 为奇数，若 $2\nmid a$，

a^p-1 有素因子 2，但此时要求 q 不整除 $a-1$，从而 $q\neq 2$，素因子 q 也为奇数，则 $q-1$ 中

有素因子 2，而 p 为奇素数，从而 $2p\mid q-1$

(2) 构造 $a_1=2^p-1, a_n=(\prod_{i=1}^{n-1}a_i)^p-1$，满足两两互素，$a^p-1$ 总能有不整除 $a-1$ 的素因子

否则所有素因子 $p_i=\dfrac{a-1}{k_i}, k_i\geq 2\in Z$，相乘有 $a^p-1=\dfrac{(a-1)^x}{\prod\limits_{i=1}^{x}k_i}$ 移项后有

$(a^p-1)\prod_{i=1}^{x}k_i=(a-1)^x$，两边对 a 取模得 $-\prod_{i=1}^{x}k_i\equiv(-1)^x\pmod{a}$ 矛盾

则两两互素的无穷整数数列 $\{a_n\}$ 中每个数都存在形如 $2px+1$ 的素因子，共无穷多个

柯召讲义5.1

证明: m 是一个素数的充分必要条件是存在某个整数 a, a 对模数 m 的次数为 $m-1$.

证明：1° 若 m 为一个素数，由素数必有原根可知，$\exists\, a\in Z$，使得 a 模 m 的阶数为 $m-1$

2° 若对某个 $a\in Z$，$a^r\equiv 1\pmod{m}$ 的最小正整数（阶数 r）为 $m-1$，有 $(a,m)=1$

由费马小定理 $a^{\varphi(m)} \equiv 1 \pmod{m}$，得 $m-1 \mid \varphi(m)$，若 m 不是素数，$m \geq 2$，令

$$m = p_1^{l_1} \cdots p_s^{l_s}, \varphi(m) = m\prod_{i=1}^{s}(1-\frac{1}{p_i}) \leq m\prod_{i=1}^{s}(1-\frac{1}{p_i^{l_i}}) < m(1-\prod_{i=1}^{s}\frac{1}{p_i^{l_i}}) = m-1$$

从而 m 为素数

柯召讲义5.2

设 g 是奇素数 p 的一个原根, 证明: 当 $p \equiv 1(\mathrm{mod}\ 4)$ 时, $-g$ 也是 p 的一个原根; 当 $p \equiv 3(\mathrm{mod}\ 4)$ 时, $-g$ 对 p 的次数为 $\dfrac{p-1}{2}$.

证明：若 g 是奇素数 p 的一个原根，则满足 $g^r \equiv 1 \pmod{p}$ 的最小 $r = p-1$，而 $2 \mid p-1$

则 $(-g)^{p-1} \equiv g^{p-1} \equiv 1 \pmod{p}$，且若存在 $1 \leq r' < p-1$，使得 $(-g)^{r'} \equiv 1 \pmod{p}$

r' 不能是偶数，否则与阶数矛盾，则 $2 \nmid p$，有 $g^{r'} \equiv -1 \pmod{p}$，则

$$g^{2r'} - 1 \equiv (g^{r'}+1)\cdot(g^{r'}-1) \equiv 0 \pmod{p}, g^{2r'} \equiv 1 \pmod{p}$$

则 $2r' \mid r$，由于 r' 为奇数，若 $p \equiv 1 \pmod{4}$，则 $4 \mid p-1$，此时 r' 不存在，从而 $-g$ 也为原根

若 $p \equiv 3 \pmod{4}$，有

$$g^{p-1} - 1 \equiv (g^{\frac{p-1}{2}}-1)\cdot(g^{\frac{p-1}{2}}+1) \equiv 0 \pmod{p}$$

且 $g^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$ 否则不满足阶数的性质，则 $(-g)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$，若 $1 \leq r'' < \dfrac{p-1}{2}$

使得 $(-g)^{r''} \equiv 1 \pmod{p}$，首先 r'' 不为偶数，若 r'' 为奇数，则 $g^{r''} \equiv -1 \pmod{p}$

从而平方 $g^{2r''} \equiv 1 \pmod{p}$，则有 $2 \leq 2r'' < p-1$ 使得 $g^{2r''} \equiv 1 \pmod{p}$ 与阶数矛盾

从而此时 $-g$ 对 p 的阶数为 $\dfrac{p-1}{2}$

初等数论第六次作业　　2022.4.1

习题3.1.1

设 $m \geqslant 2$, 整数 a 和 b 模 m 的阶分别为 s 和 t, 并且 $(s,t)=1$. 证明 ab 模 m 的阶为 st.

证明：设 ab 模 m 的阶为 r，$(ab)^r \equiv 1 \pmod{m}$，由 $(ab)^{st} \equiv (a^s)^r \cdot (b^r)^s \equiv 1 \pmod{m}$

得 $r \mid st$，则设 $st = pr, p \in Z \text{ and p is prime}$，由 $(s,t) = 1$，则 $p \mid s$ 或 $p \mid t$，不妨设 $p \mid s$

令 $s = px, xt = r$，有 $(ab)^r \equiv (ab)^{xt} \equiv a^{xt} \cdot 1 \equiv 1 \pmod{m}$

则 $s \mid xt$，由 $(s,t) = 1$，得 $s \mid x$，又 $x \mid s$，可得 $s = x, p = 1$，即 $r = st$

习题3.1.4

(1) 对于 $p = 5, 7, 11, 13, 23$, 求模 p 的最小正原根.

(2) 求模 7^2 的全部原根.

解：(1) 由在 Z_5 下 $\{2, 2^2, 2^3, 2^4\} = \{2, 4, 3, 1\}$ ，则 2 为 5 的最小正原根

在 Z_7 下 $\{2, 2^2, 2^3, 2^4, 2^5, 2^6\} = \{2, 4, 1, 2, 4, 1\}, \{3, 3^2, 3^3, 3^4, 3^5, 3^6\} = \{3, 2, 6, 4, 5, 1\}$

则 3 为 7 的最小正原根

在 Z_{11} 下 $\{2, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}\} = \{2, 4, 8, 5, 10, 9, 7, 3, 6, 1\}$ ，则 2 为 11 的

最小正原根

在 Z_{13} 下 $\{2, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}, 2^{11}, 2^{12}\} = \{2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1\}$

则 2 为 13 的最小正原根

在 Z_{23} 下 $\{2, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}, 2^{11}\} = \{2, 4, 8, 16, 9, 18, 13, 3, 6, 12, 1\}$

$\{3, 3^2, 3^3, 3^4\} = \{3, 6, 12, 1\}$ 对 5 而言

$$\{5, 5^2, 5^3, 5^4, 5^5, 5^6, 5^7, 5^8, 5^9, 5^{10}, 5^{11}, 5^{12}, 5^{13}, 5^{14}, 5^{15}, 5^{16}, 5^{17}, 5^{18}, 5^{19}, 5^{20}, 5^{21}, 5^{22}\} = \\ \{5, 2, 10, 4, 20, 8, 17, 16, 11, 9, 22, 18, 21, 13, 19, 3, 15, 6, 7, 12, 14, 1\}$$

则 5 为 23 的最小正原根

(2) 由定理， 7 有原根 3，则 3 和 10 必有一个为 49 的原根，有

$$3^2, 3^4, 3^6, 3^8, 3^{12}, 3^{16}, 3^{24} \equiv 9, 32, 43, 44, 36, 25, 22 \pmod{49}$$

从而 3 为 49 的原根，有 $\varphi(\varphi(49)) = \varphi(42) = 12$ 个原根，有 $3^r, (r, 42) = 1$ 均为原根，计算有

$\{3, 3^5, 3^{11}, 3^{13}, 3^{17}, 3^{19}, 3^{23}, 3^{25}, 3^{29}, 3^{31}, 3^{37}, 3^{41}\} = \{3, 47, 12, 10, 26, 38, 40, 17, 5, 45, 24, 33\}$

则 49 的所有原根为 $\boxed{3, 5, 10, 12, 17, 24, 26, 33, 38, 40, 45, 47}$，共 12 个

习题3.2.1

解同余方程:

(1) $x^8 \equiv 3 \pmod{13}$;

(2) $x^8 \equiv 3 \pmod{143}$;

(3) $7^x \equiv 4 \pmod{17}$.

解：(1) 由上题知 2 为 13 的一个原根，则原式等价于 $8\mathrm{ind}_2 x \equiv \mathrm{ind}_2 3 \pmod{12}$

由 $2^4 \equiv 3 \pmod{13}$ 得 $8\mathrm{ind}_2 x \equiv 4 \pmod{12}$ 且 $(8,12) = 4 \mid 4$，代换有

$2\mathrm{ind}_2 x \equiv 1 \equiv 4 \pmod{3}$，$\mathrm{ind}_2 x \equiv 2,5,8,11$，得解为 $x_1 \equiv 4,6,7,9 \pmod{13}$

(2) 结合 $x^8 \equiv 3 \pmod{11}$，由 2 为 11 的一个原根，等价于 $8\mathrm{ind}_2 x \equiv \mathrm{ind}_2 3 \equiv 8 \pmod{10}$

由 $(8,10) = 2 \mid 10$，则有两个解，$\mathrm{ind}_2 x \equiv 1,6 \pmod{10}$，则 $x_2 \equiv 2,9 \pmod{11}$

使用中国剩余定理，$11^{-1} \equiv 6 \pmod{13}, 13^{-1} \equiv 6 \pmod{11}$ 对应计算 $x_1 \cdot 6 \cdot 13 + x_2 \cdot 6 \cdot 11$

$$x \equiv 9,20,35,46,97,108,123,134 \pmod{143}$$

(3) 对 2 计算 $2^1, 2^2, 2^4, 2^8 \equiv 2,4,16,1 \pmod{17}$，则 2 不是 17 的原根，同理对 3 计算有

$3^1, 3^2, 3^4, 3^8 \equiv 3,9,13,16 \pmod{17}$，则 3 是 17 的原根，则对 $7^x \equiv 4 \pmod{17}$ 变换有

$x\mathrm{ind}_3 7 \equiv \mathrm{ind}_3 4 \pmod{16}$ 有 $\mathrm{ind}_3 7 = 11, \mathrm{ind}_3 4 = 12$，则 $11x \equiv 12 \pmod{16}$

$(11,16) = 1 \mid 12$ 只有一个整数解，得 $x \equiv 4 \pmod{17}$

习题3.2.2

(1) 写出模 37 的全部 8 次剩余和 15 次剩余.

(2) 写出模 11 的全部二次剩余.

解：(1) 取 37 的一个原根 2，由 $(8,36) = 4$，因此八次剩余 a 满足的条件为： $4 \mid \mathrm{ind}_2 a$ ，故

$\mathrm{ind}_2 a = 4,8,12,\cdots,36$ ，因此模 37 的全部 8 次剩余为: $a \equiv 2^4, 2^8, \cdots, 2^{36} (\mathrm{mod}\ 37)$;

$$a \equiv 16,34,26,9,33,10,12,7,1 \pmod{37}$$

而 $(15,36) = 3$ ，因此 15 剩余 a 满足的条件为： $3 \mathrm{ind}_2 a$ ，故 $\mathrm{ind}_2 a = 3,6,\cdots,36$ ，因此解为:

$$a \equiv 2^3, 2^6, \cdots, 2^{36} \equiv 8,27,31,26,23,36,29,10,6,11,14,1 (\mathrm{mod}\ 37)$$

(2) 模 11 的全部二次剩余为: $1^2, 2^2, \cdots, 5^2$ ，即 $1,3,4,5,9$

习题3.2.3

设 p 为素数, $p \equiv 2(\mathrm{mod}\ 3), a$ 和 b 是整数. 证明： $a^3 \equiv b^3(\mathrm{mod}\ p)$ 当且仅当 $a \equiv b(\mathrm{mod}\ p)$.

证明：若 $(a,p)=p$，则 $a \equiv b \equiv 0\ (\mathrm{mod}\ p)$，否则 $(a,p)=1$ 令 $p=3k+2, k \geq 1$，有

$a^3 \equiv b^3 \equiv c\ (\mathrm{mod}\ p)$，且 $(c,p)=1$，由欧拉定理 $a^{3k+1} \equiv b^{3k+1} \equiv c^k a \equiv c^k b \equiv 1\ (\mathrm{mod}\ p)$

从而 $a \equiv c^{-k} \equiv b\ (\mathrm{mod}\ p)$

> 设 $a^3 \equiv b^3 \equiv k(\mathrm{mod}\ p)$ ，因为 $(3, p-1)=1$ ，故 $x^3 \equiv k(\mathrm{mod}\ p)$ 在模 p 意义下仅有一个解， 故得证

习题3.2.4

设 p 为奇素数, 整数 a 模 p 的阶为 3，求 $\dfrac{a}{a+1}$ 模 p 的阶.

解：由题设定义 a 的数论倒数为 b，即 $ab \equiv 1\ (\mathrm{mod}\ p)$，有 $(\dfrac{a}{a+1})^{-1} = 1 + \dfrac{1}{a} = 1 + b$

由 x 与 x^{-1} 模 p 的阶是一样的，从而考虑 $1+b$ 模 p 的阶，由满足 $a^r \equiv 1\ (\mathrm{mod}\ p)$ 的最小正整数

为 3 ，也有 $b^3 \equiv 1\ (\mathrm{mod}\ p)$，$b^2+b+1 \equiv 0\ (\mathrm{mod}\ p)$，令 $1+b$ 模 p 的阶为 r'，

有 $(1+b)^{r'} \equiv 1\ (\mathrm{mod}\ p)$ ，有 $(1+b)^1 \not\equiv 1\ (\mathrm{mod}\ p), (1+b)^2 \equiv b \not\equiv 1\ (\mathrm{mod}\ p)$

但 $(1+b)^3 \equiv 3(b^2+b+1) - 2 + b^3 \equiv -1\ (\mathrm{mod}\ p)$，而 $(1+b)^4 \equiv -1 \not\equiv 1\ (\mathrm{mod}\ p)$

$(1+b)^5 \equiv -b \not\equiv 1\ (\mathrm{mod}\ p)$，且 $(1+b)^6 \equiv 1\ (\mathrm{mod}\ p)$，则 $\dfrac{a}{a+1}$ 模 p 的阶为 6

习题4.1.2

设 p 为奇素数, n 是最小正整数使得 $\left(\dfrac{n}{p}\right) = -1$. 证明: n 为素数

证明：由勒让德符号定义不存在整数 x 使得 $x^2 \equiv n\ (\mathrm{mod}\ p)$，取 p 的原根 g 有 $n = g^{2j+1}$

若 n 为合数，即 $n = n_1 n_2$，由 $\left(\dfrac{n}{p}\right) = \left(\dfrac{n_1}{p}\right)\left(\dfrac{n_2}{p}\right)$ 可知 n_1 和 n_2 一定一者为 1，另一者为 -1

而显然为 -1 的一者对应的 n_i 更小，与题设矛盾，从而 n 为素数

初等数论第七次作业　　2022.4.16

习题4.1.1

设 p 为奇素数, $a,b\in\mathbf{Z},(a,p)=1$. 证明:

$$\sum_{n=0}^{p-1}\left(\frac{an+b}{p}\right)=0$$

证明：由于 $(a,p)=1$，则 $a,a+b,\cdots,a(p-1)+b$ 构成模 p 的完系，可用反证法证明

其中模 p 的二次剩余和非二次剩余都为 $\dfrac{p-1}{2}$ 个，最后剩一个能被 p 整除的

则 $\displaystyle\sum_{n=0}^{p-1}\left(\frac{an+b}{p}\right)=\frac{p-1}{2}+(-1)\cdot\frac{p-1}{2}+0=0$

习题4.1.3

证明形如 $8m+3,8m+5,8m+7$ 的素数均有无穷多个

解：(1) 反证，假设 $8m+3$ 的素数有限个，设为 $p_1.p_2,\cdots,p_s$ 构造 $n=2(p_1p_2\cdots p_s)^2+1$ ，

由 $n\equiv 2\cdot(3^2)^s+1\equiv 3\pmod 8$，则由假设 n 为合数

设其素因子为 p，有 $2(p_1p_2\cdots p_s)^2\equiv -1\pmod p$，两边乘以 2，取勒让德符号

$$(\frac{-2}{p})=1=(\frac{2}{p})(\frac{-1}{p})=(-1)^{\frac{p^2-1}{8}+\frac{p-1}{2}}=(-1)^{\frac{(p-1)(p+5)}{8}}$$

从而 $2\mid\dfrac{(p-1)(p+5)}{8}$，从而 $p\equiv 1,3\pmod 8$。但 $n\equiv 3\pmod 8$，n 的所有素因子不可能

均模 8 余 3，从而一定存在一个模 8 余 3 的素因子，而该素因子不为 $p_1,\cdots,p_s$，这是因为

$n\equiv 1\pmod{p_i}$，从而矛盾，$8m+3$ 型素数有无穷多个

(2) 假设 $8m+5$ 的素数有限个，设为 $p_1,p_2,\cdots,p_s$，构造 $n=4(p_1\cdots p_s)^2+1$ 有

$n\equiv 5\pmod 8$，其为合数，设其素因子为 p

有 $(2p_1\cdots p_s)^2\equiv -1\pmod p$，取勒让德符号有 $(\dfrac{-1}{p})=1=(-1)^{\frac{p-1}{2}}$

则 $p \equiv 1,5 \pmod 8$ 而 $n \equiv 5 \pmod 5$，n 的所有素因子不可能全为 1，则其存在一个

不为 p_i 的素因子，与假设矛盾，从而 $8m+5$ 型素数有无穷多个

(3) 假设 $8m+7$ 的素数有限个，设为 $p_1, p_2, \cdots, p_s$，构造 $n = 8(p_1 \cdots p_s)^2 - 1$ 有

$n \equiv 7 \pmod 8$，其为合数，设其素因子为 p

有 $(4p_1 \cdots p_s)^2 \equiv 2 \pmod p$，使用勒让德符号有 $(\dfrac{2}{p}) = 1 = (-1)^{\frac{p^2-1}{8}}$

则 $p \equiv 1,7$，又由于 $n \equiv 7 \pmod 8$，n 所有素因子不可能全为 1，则其存在一个

不为 p_i 的素因子，与假设矛盾，从而 $8m+7$ 型素数有无穷多个

习题4.1.4

设 p 为奇素数. 证明: 有无穷多的素数是模 p 的二次非剩余.

证明：假设满足是模 p 二次非剩余的素数有限，为 $p_1, p_2, \cdots p_s$，有 $(\dfrac{p_i}{p}) = -1$，取模 p 的

一个二次非剩余 a，由中国剩余定理，满足 $x \equiv a \pmod p, x \equiv 1 \pmod{p_i}$ 同余方程的解

存在，设其中一个解为 x

则 $(\dfrac{x}{p}) = (\dfrac{a}{p}) = -1$，$x$ 必有素因子为二次非剩余，且使得该素因子与 p_i 均互素，这样与

有限个满足条件的素数矛盾，从而有无穷多个素数模 p 二次剩余

习题4.1.5

设 p 和 $q = 2p + 1$ 都是素数. 证明:

(1) 当 $p \equiv 1 (\mathrm{mod}\ 4)$ 时, 2 是模 q 的原根;

(2) 当 $p \equiv 3 (\mathrm{mod}\ 4)$ 时,-2 是模 q 的原根.

解：(1) 由于 $q - 1 = 2p$ 只有素因子 2 和 p，有 $2^2 \equiv 4 \neq 1 \pmod q$ 而对$2^p \equiv 2^{\frac{q-1}{2}}$，计算

$(\dfrac{2}{q}) = (-1)^{\frac{q^2-1}{8}} = (-1)^{\frac{p(p+1)}{2}} = -1$，则 2 为模 q 的二次非剩余，则取 q 的原根 g，有 $2 = g^{2j+1}$，代入计算
$2^p = g^{(2j+1)p} = (g^p)^{2j+1} = (g^{\frac{q-1}{2}})^{2j+1} = (-1)^{2j+1} = -1$，从而 $2, p$ 均不是模 p

下 2 的阶数，从而 2 为模 p 的原根

(2) 同上，只需考虑 $(-2)^p$，$p \neq 2$，计算 $(\dfrac{-2}{q}) = (\dfrac{-1}{q})(\dfrac{2}{q}) = (-1)^{\frac{q-1}{2}}(-1)^{\frac{q^2-1}{8}} = -1$，

则取 q 的原根 g，有 $-2=g^{2j+1}$，代入 $(-2)^p=(g^{\frac{q-1}{2}})^{2j}=(-1)^{2j+1}=-1$

从而 $2,p$ 均不是模 p 下 -2 的阶数，从而 -2 为模 p 的原根

习题4.1.6

设 p 为素数, $p\equiv 3(\mathrm{mod}\ 4)$. 记 $q=2p+1$. 则 q 为素数当且仅当 $q\mid 2^p-1$.

证明：由上题知，若 q 为素数，-2 为 q 的原根

$$2^p\equiv -(-2)^p\equiv -(-2)^{\frac{q-1}{2}}\equiv -(-1)\equiv 1\pmod{q}$$

则 $q\mid 2^p-1$ 。又若 $q\mid 2^p-1$ ，由欧拉定理 $2^{\varphi(q)}\equiv 1\pmod{q}$，即 $q\mid 2^{\varphi(q)}-1$

则 $p\mid \varphi(q)=\varphi(2p+1)$，若 q 不是素数，$\varphi(2p+1)<2p$，则 $p=\varphi(2p+1)$，而对于奇数

的欧拉函数为偶数，从而矛盾，则 q 为素数

习题4.1.7

设 p 为奇素数. 证明:

$$\prod_{\substack{r=1\\(\frac{r}{p})=1}}^{p-1} r\equiv -\left(\frac{-1}{p}\right)(\mathrm{mod}\ p)$$

解：满足 $(\frac{r}{p})=1$ 的所有 r 为 $g^0,g^2,\cdots,g^{p-3}$。其中 g 为 p 的一个原根，则

$$\prod r=g^{0+2+\cdots p-3}=g^{\frac{(p-3)(p-1)}{4}}=(g^{\frac{p-1}{2}})^{\frac{p-3}{2}}=(-1)^{\frac{p-3}{2}}$$

而 $-(\frac{-1}{p})=-(-1)^{\frac{p-1}{2}}=(-1)^{\frac{p-3}{2}}$，两者相等

习题4.1.8

设 p 为素数,

(1) 若 $p\equiv 1(\mathrm{mod}\ 4)$, 则

$$\sum_{\substack{r=1\\\left(\frac{r}{p}\right)=1}}^{p-1} r=\frac{p(p-1)}{4},\quad \sum_{a=1}^{p-1} a\left(\frac{a}{p}\right)=0$$

(2) 若 $p\equiv 3(\mathrm{mod}\ 4)$, 并且 $p\geqslant 7$, 则

$$\sum_{\substack{r=1\\ \left(\frac{r}{p}\right)=1}}^{p-1} r\equiv 0(\mathrm{mod}\ p), \sum_{r=1}^{p-1} a\left(\frac{a}{p}\right)\equiv 0(\mathrm{mod}\ p).$$

证明：(1) 由 $(\frac{p-x}{p})=(\frac{-x}{p})=(\frac{x}{p})(\frac{-1}{p})=(\frac{x}{p})(-1)^{\frac{p-1}{2}}=(\frac{x}{p})$

从而 $(i,p-i)$ 每对勒让德符号相同，从而所有满足 $(\frac{r}{p})=1$ 的 r 一定能配成和为 p 的 pairs

且共有 $\frac{p-1}{4}$ 对，求和为 $\frac{p(p-1)}{4}$，同理分离得到 $\sum\limits_{a=1}^{p-1}a(\frac{a}{p})=0+\sum\limits_{\substack{r=1\\ \left(\frac{r}{p}\right)=1}}^{p-1} r-\sum\limits_{\substack{r=1\\ \left(\frac{r}{p}\right)\neq 1}}^{p-1} r=0$

(2) 和上题类似，得到 $(\frac{p-x}{p})=-(\frac{x}{p})$，从而 $(i,p-i)$ 勒让德符号相反，有记

$$\sum_{\substack{r=1\\ \left(\frac{r}{p}\right)=1}}^{p-1} r\equiv A(\mathrm{mod}\ p),\ \sum_{\substack{r=1\\ \left(\frac{r}{p}\right)\neq 1}}^{p-1} r\equiv B(\mathrm{mod}\ p)$$

取模 p 的一个原根 g，则 g 是模 p 的一个二次非剩，$(\frac{g}{p})=-1$

$$\sum_{r=1,\left(\frac{r}{p}\right)=1}^{p-1} r\equiv 1+g^2+\cdots+g^{p-3}\equiv\frac{1-g^{\frac{p-1}{2}\cdot 2}}{1-g^2}\equiv 0\pmod p$$

$$\sum_{a=1}^{p-1}a\left(\frac{a}{p}\right)\equiv\sum_{i=0}^{p-2}g^i\left(\frac{g^i}{p}\right)\equiv\sum_{i=0}^{p-2}g^i(-1)^i\equiv\sum_{i=0}^{p-1}(-g)^i\equiv\frac{1-g^{p-1}}{1+g}\equiv 0\pmod p.$$

习题4.2.1

计算 $\left(\frac{17}{23}\right),\left(\frac{19}{37}\right),\left(\frac{92}{101}\right).$

由二次互反律计算有

$$\left(\frac{17}{23}\right)=\left(\frac{23}{17}\right)(-1)^{11\cdot 8}=\left(\frac{23}{17}\right)=\left(\frac{6}{17}\right)=\left(\frac{2}{17}\right)\left(\frac{3}{17}\right)$$

$$=(-1)^{\frac{17^2-1}{8}}\left(\frac{17}{3}\right)(-1)^8=\left(\frac{17}{3}\right)=\left(\frac{2}{3}\right)=-1$$

$$\left(\frac{19}{37}\right)=\left(\frac{37}{19}\right)(-1)^{9\cdot 18}=\left(\frac{37}{19}\right)=\left(\frac{-1}{19}\right)=(-1)^9=-1$$

$$\left(\frac{92}{101}\right)=\left(\frac{2}{101}\right)^2\left(\frac{23}{101}\right)=(-1)^{\frac{101^2-1}{8}}\left(\frac{23}{101}\right)=$$

$$\left(\frac{23}{101}\right)=\left(\frac{101}{23}\right)(-1)^{50\cdot 11}=\left(\frac{101}{23}\right)=\left(\frac{9}{23}\right)=\left(\frac{3}{23}\right)^2=1$$

习题4.2.4

若 $p=10m-1$ 为素数, 证明: $p\mid 5^{5m-1}-1$.

证明：计算 $(\frac{5}{p})=(\frac{p}{5})(-1)^{2\cdot\frac{p-1}{2}}=(\frac{p}{5})=(\frac{-1}{5})=(-1)^2=1$，则 5 是 p 的二次剩余

令 g 为 p 的二次剩余，$5\equiv g^{2j}$，有 $5^{5m-1}\equiv(g^{2j})^{\frac{p-1}{2}}\equiv(g^{p-1})^j\equiv 1\pmod p$

习题4.2.5

设 $n\geqslant 2, p=2^n+1$ 为素数. 证明:

(1) 对每个 $a\in\mathbf{Z}, a$ 为模 p 的原根当且仅当 $\left(\frac{a}{p}\right)=-1$;

(2) 证明 3 和 7 均为模 p 的原根.

证明：(1) 若 a 为模 p 的原根，有 $(\frac{a}{p})=-1$；若 $(\frac{a}{p})=-1$，若 a 不是模 p 的原根，则对

$p-1=2^n$ 的因子为对应的阶，总有 $a^2\equiv 1\pmod p$，这与 $(\frac{a}{p})=-1$ 矛盾，从而 a 是模 p 的原根

(2) 由于 $p=2^n+1$ 为素数，故 $n=2^k$ ，其中 $k\geq 1$.

由 $(\frac{3}{p})=(\frac{p}{3})(-1)^{1\cdot\frac{p-1}{2}}=(\frac{p}{3})$ ，而 $2^{2^n}+1\equiv(-1)^{2^n}+1\equiv 2\pmod 3$

有 $(\frac{2}{3})=-1$，则 $(\frac{3}{p})=-1$，从而 3 为模 p 的原根；同理 $(\frac{7}{p})=(\frac{p}{7})$

若 $2^k\equiv 1(\mathrm{mod}\ 3)$ ，则 $\left(\frac{2^{2^k}+1}{7}\right)=\left(\frac{\left(2^3\right)^t\cdot 2+1}{7}\right)=\left(\frac{3}{7}\right)=-\left(\frac{7}{3}\right)=-1.$

若 $2^k \equiv -1 (\mathrm{mod}\ 3)$ ，则 $\left(\frac{2^{2^k}+1}{7}\right) = \left(\frac{\left(2^3\right)^t \cdot 2^2+1}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{7}{5}\right) = \left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = -1.$

因此 $\left(\frac{7}{p}\right) = -1$ ，故 7 是模 p 的原根.

初等数论第八次作业　　2022.4.23

习题4.2.2

确定以 a 为二次剩余的素数, 其中 $a = -3, 5$ 和 15 .

$a = -3$ 时，2 满足题意，此外， $\frac{1}{2}\varphi(3) = 1$. 且 7 满足题意，则解为奇素数 $p = 3k+1$ 和 2

$a = 5 \equiv 1 \pmod 4$，2 满足题意. 此外， $\frac{1}{2}\varphi(5) = 2$ ，且 $11, 19$ 均满足题意. 故 2 和奇素数 $5k \pm 1$ 满足题意.

$a = 15$ 时， 2 满足题意. $\frac{1}{2}\varphi(60) = 8$ ，且经过验证， $7, 11, 17, 43, 53, 59, 109, 181$ 都满足.

解为 2 和素数 $60k+1, 60k+7, 60k+11, 60k+17, 60k+43, 60k+49, 60k+53, 60k+59$

习题4.2.3

设 $p = 4k+1$ 是素数, a 是 k 的因子, 证明: $\left(\frac{a}{p}\right) = 1.$

证明：由二次互反律 $(\frac{a}{p}) = (\frac{p}{a})(-1)^{\frac{p-1}{2}\frac{a-1}{2}} = (\frac{p}{a}) = (\frac{4k+1}{a}) = (\frac{4ax+1}{a}) = (\frac{1}{a}) = 1$

习题4.2.6

(1) 设 $n = 2^m a + 1$, 其中 $m \geqslant 2, 1 \leqslant a < 2^m$. 如果 p 为奇素数, 并且 $\left(\frac{n}{p}\right) = -1$, 证明: n 是素数当且仅当 $p^{\frac{n-1}{2}} \equiv -1 (\mathrm{mod}\ n)$.

(2) 设 $n = 2^m + 1, m \geqslant 2$. 证明: n 为素数当且仅当 $3^{\frac{n-1}{2}} \equiv -1 \pmod n$.

证明：(1) 若 n 为素数，由于 $n=2^m a+1$ 故 $\left(\dfrac{n}{p}\right)=\left(\dfrac{p}{n}\right)=-1$ ，故 $p^{\frac{n-1}{2}}\equiv -1(\mathrm{mod}\ n)$.

另一方面，若 $p^{\frac{n-1}{2}}\equiv -1(\mathrm{mod}\ n)$ ，任取 n 的一个素因子 q，$q\geq 3$. 令 d 为 p 模 q 的阶，由于 $p^{\frac{n-1}{2}}\equiv -1(\mathrm{mod}\ q)$ ，故 $p^{2^{m-1}a}\equiv -1(\mathrm{mod}\ q)$ ，因此 $2^m\mid d$ ，又 $d\mid q-1$ ，则 $2^m\mid q-1$

$q\geq 2^m+1$. 由于 $n=2^m a+1$，$a<2^m$ ，所以 $q^2>n$，这样的 q 只能为 n 本身，则 n 为素数

(2) 在 (1) 中取 $a=1,p=3$ 当 n 为素数时，满足 m 为奇数，否则 3 为 n 的素因子，此时 $\left(\dfrac{2^m+1}{3}\right)=\left(\dfrac{2}{3}\right)=-1$ ，故满足 (1) 的条件，则 $3^{\frac{n-1}{2}}\equiv -1$

若 $3^{\frac{n-1}{2}}\equiv -1$，由 (1) 中的推导中没有使用到 $\left(\dfrac{n}{p}\right)=-1$ 条件知 n 为素数

习题4.3.2

设 $f(x,y)$ 是关于 x,y 的整系数多项式. $(x,y)=(a,b)$ 和 (c,d) 均是同余方程

$f(x,y)\equiv 0(\mathrm{mod}\ m)$ 的整数解, 即 $f(a,b)\equiv 0\ (\mathrm{mod}\ m), f(c,d)\equiv 0(\mathrm{mod}\ m)$.

称这两组解为模 m 的同一个解, 是指 $a\equiv c(\mathrm{mod}\ m)$, 并且 $b\equiv d(\mathrm{mod}\ m)$.

(1) 设 p 为奇素数, a 为整数. 证明:同余方程

$$x^2-y^2\equiv a\pmod p$$

的模 p 解数为 $p-1$ （若 $p\nmid a$） 或 $2p-1$ （若 $p\mid a$）.

(2) 证明:

$$\sum_{y=0}^{p-1}\left(\frac{y^2+a}{p}\right)=\begin{cases}-1, & \text{若 } p\nmid a,\\ p-1, & \text{若 } p\mid a.\end{cases}$$

证明：(1) 当 $p\nmid a$ 时， $(x+y)(x-y)\equiv a(\mathrm{mod}\ p)$. 设 $x+y\equiv b(\mathrm{mod}\ p)$ ，其中 $(b,p)=1$.

则 $x-y\equiv ab^{-1}(\mathrm{mod}\ p)$. 从而 $(x,y)=\left(\dfrac{b+ab^{-1}}{2},\dfrac{b-ab^{-1}}{2}\right)$. 因此解数为 b 的个数 $p-1$.

当 $p\mid a$ 时， $p\mid (x+y)(x-y)$ ，所以 $x\equiv y(\mathrm{mod}\ p)$ 或 $x\equiv -y(\mathrm{mod}\ p)$.

共有 $(0,0),(b,-b),(-b,b)$ 即 $2\cdot(p-1)+1=2p-1$ 组解.

(2) 设 $x^2\equiv y^2+a(\mathrm{mod}\ p)$. $\left(\dfrac{y^2+a}{p}\right)=1$ 时，有两组解， $\left(\dfrac{y^2+a}{p}\right)=-1$ 时，无解

计算其总解数为 $\sum\limits_{y=0}^{p-1}\left(1+\left(\dfrac{y^2+a}{p}\right)\right)=p+\sum\limits_{y=0}^{p-1}\left(\dfrac{y^2+a}{p}\right)=\begin{cases}p-1, & p\nmid a\\ 2p-1, & p\mid a\end{cases}$

因此 $\sum\limits_{y=0}^{p-1}\left(\dfrac{y^2+a}{p}\right)=\begin{cases}-1, & p\nmid a\\ p-1, & p\mid a\end{cases}$

习题4.3.3

设 p 为奇素数, $a,b,c\in\mathbf{Z},p\nmid a,D=b^2-4ac$. 证明:

$$\sum_{x=0}^{p-1}\left(\frac{ax^2+bx+c}{p}\right)=\begin{cases}-\left(\dfrac{a}{p}\right), & \text{若 } p\nmid D,\\ (p-1)\left(\dfrac{a}{p}\right), & \text{若 } p\mid D.\end{cases}$$

证明: 令 $y=x+\dfrac{b}{2a}=x+b\cdot 2^{-1}\cdot a^{-1},a'=c-b^2\cdot 4^{-1}\cdot a^{-1}$ 代入上题结论得到

$$\sum_{y=\frac{b}{2a}}^{\frac{b}{2a}+p-1}(\frac{ay^2+a'}{p})=\sum_{y=0}^{p-1}(\frac{ay^2+a'}{p})=(\frac{a}{p})\sum_{y=0}^{p-1}(\frac{y^2+a'a^{-1}}{p})=\begin{cases}-\left(\dfrac{a}{p}\right), & \text{若 } p\nmid D,\\ (p-1)\left(\dfrac{a}{p}\right), & \text{若 } p\mid D.\end{cases}$$

习题4.2.4

设 $a,b,c\in\mathbf{Z},p\nmid ab$, 则同余方程

$$ax^2+by^2\equiv c\pmod p$$

模 p 的解数为

$$N=\begin{cases}p+(p-1)\left(\dfrac{-ab}{p}\right), & \text{若 } p\mid c,\\ p-\left(\dfrac{-ab}{p}\right), & \text{若 } p\nmid c.\end{cases}$$

证明: $ax^2+by^2\equiv c(\bmod p)$ 等价于 $x^2\equiv -a^{-1}by^2+a^{-1}c(\bmod p)$. $(a,p)=(b,p)=1$ 解数

$$\begin{aligned}&\sum_{y=0}^{p-1}\left(1+\left(\frac{-a^{-1}by^2+a^{-1}c}{p}\right)\right)=p+\sum_{y=0}^{p-1}\left(\frac{-a^{-1}b}{p}\right)\left(\frac{y^2-cb^{-1}}{p}\right)\\ &=p+\left(\frac{-ab}{p}\right)\sum_{y=0}^{p-1}\left(\frac{y^2-cb^{-1}}{p}\right)=\begin{cases}p+(p-1)\left(\dfrac{-ab}{p}\right), & p\mid c\\ p-\left(\dfrac{-ab}{p}\right), & p\nmid c\end{cases}\end{aligned}$$

其中用到上题结论 $\sum\limits_{x=0}^{p-1}\left(\dfrac{ax^2+bx+c}{p}\right)=\begin{cases}-\left(\dfrac{a}{p}\right), & \text{若 } p\nmid D,\\ (p-1)\left(\dfrac{a}{p}\right), & \text{若 } p\mid D.\end{cases}$

初等数论第九次作业　　2022.4.30

习题4.3.1

解下列同余方程:

(1) $2x^2+3x+1\equiv 0 \pmod{28}$;

(2) $x^2\equiv -1 \pmod{169}$;

(3) $x^2\equiv 2 \pmod{98}$;

(4) $3x^2+x+6\equiv 0 \pmod{45}$.

解：(1) $28\mid(2x+1)(x+1)$. 且有 $(2x+1,x+1)=(1,x+1)=1$ 两者互素，且 $28=4\times 7$ 则

$2x+1\equiv 0(\mathrm{mod}\ 4), x+1\equiv 0(\mathrm{mod}\ 7)$ 或者 $2x+1\equiv 0(\mathrm{mod}\ 7), x+1\equiv 0(\mathrm{mod}\ 4)$

又或者 $x+1\equiv 0 \pmod{28}$ 解得 $x\equiv 3,27(\mathrm{mod}\ 28)$.

(2) $x^2\equiv -1(\mathrm{mod}\ 13)$ 解得 $x=13k+5,13k+8$. 代入 $(13k+5)^2\equiv -1(\mathrm{mod}\ 169)$ 可以化简得

$10k+2\equiv 0(\mathrm{mod}\ 13)$. 解得 $k\equiv 5(\mathrm{mod}\ 13)$. $(13k+8)^2\equiv -1(\mathrm{mod}\ 169)$ 化简得: $3k\equiv -5(\mathrm{mod}\ 13)$

解得 $k\equiv 7(\mathrm{mod}\ 13)$. 从而 $x\equiv 70,99(\mathrm{mod}\ 169)$.

(3) $x^2\equiv 2(\mathrm{mod}\ 98)$ x 为偶数. 设 $x=2k$ ，则 $2k^2\equiv 1(\mathrm{mod}\ 49)$. 即 $k^2\equiv 25(\mathrm{mod}\ 49)$. 考虑

$k^2\equiv 25(\mathrm{mod}\ 7)$ ，解得 $k=7m+2,7m+5$. 分别代入 $k^2\equiv 25(\mathrm{mod}\ 49)$ 解得

$k\equiv 44,5(\mathrm{mod}\ 49)$. 因此 $x\equiv 10,88(\mathrm{mod}\ 98)$.

(4) $3x^2+x+6\equiv 0(\mathrm{mod}\ 45)$. 两边模 3 有 $x\equiv 0(\mathrm{mod}\ 3)$. 令 $x=3y$. 代入 $9y^2+y+2\equiv 0(\mathrm{mod}\ 15)$.

模 3 知， $y\equiv 1(\mathrm{mod}\ 3)$. 设 $y=3z+1$ ，代入可知 $2z^2-z-1\equiv 0(\mathrm{mod}\ 5)$. $(2z+1)(z-1)\equiv 0(\mathrm{mod}\ 5)$.

解得 $z\equiv 1,2(\mathrm{mod}\ 5)$. 从而 $x\equiv 12,21(\mathrm{mod}\ 45)$.

习题5.1.1

求下列方程的全部整数解：

(1) $2x^2-5y^2=7$;　　(2) $x^2-2xy^2+5z^3+3=0$;

(3) $y^2=41x^3+3$;　　(4) $x^2-xy+y^2-x-y=0$;

(5) $y^2=x^3-6$　　(6) $y^2=x^3-x$.

解：(1) $x^2\equiv 0,1,2,4(\mathrm{mod}\ 7)$. 对原方程两边模 7 知: $x^2+y^2\equiv 0(\mathrm{mod}\ 7)$. 因此 $x\equiv y\equiv 0(\mathrm{mod}\ 7)$.

两边模 49 有 $0\equiv 7\ (\mathrm{mod}\ 49)$ 矛盾，从而无解

(2) 方程两边模 5 知 $x^2-2xy^2+3\equiv 0(\mathrm{mod}\ 5)$，故 $\left(x-y^2\right)^2\equiv y^4-3(\mathrm{mod}\ 5)$. 注意到

$x^2\equiv 0,1,-1(\mathrm{mod}\ 5), x^4\equiv 0,1(\mathrm{mod}\ 5)$，则 $y^4\equiv 2,3,4\ (\mathrm{mod}\ 5)$ 矛盾，从而无解

(3) 两边模 41 可知: $y^2\equiv 3(\mathrm{mod}\ 41)$. 而 $\left(\dfrac{3}{41}\right)=\left(\dfrac{41}{3}\right)=\left(\dfrac{-1}{3}\right)=-1$，故没有整数解.

(4) $x^2-xy+y^2-x-y=0$ 主元后 $x^2-(y+1)x+y^2-y=0$ 其判别式

$\Delta=\sqrt{(y+1)^2-4(y^2-y)}=\sqrt{-3y^2+6y+1}$ 为整数，则 $-3y^2+6y+1=t^2$

$3y^2-6y+(t^2-1)=0$ 其判别式 $\Delta=\sqrt{6^2-4\cdot 3\cdot(t^2-1)}=2\sqrt{3(4-t^2)}$ 也为完全平方数

从而 $3(4-t^2)$ 为完全平方数，可以得到 $t^2=1,4$ 解得 $y=0,1,2$ 回代解得

$(x,y)=(0,0),(0,1),(1,0),(1,2),(2,1),(2,2)$

(5) 方程两边模 8. 注意到 $y^2\equiv 0,1,4(\mathrm{mod}\ 8)$，$x^3\equiv 0,\pm 1,\pm 3(\mathrm{mod}\ 8)$，对比有 $x\equiv 7(\mathrm{mod}\ 8)$.

$y^2-2=x^3-8=(x-2)\left(x^2+2x+4\right)=(x-2)\left((x+1)^2+3\right)$. 其中 $(x+1)^2+3\equiv 3(\mathrm{mod}\ 8)$.

任取它的一个素因子 p，p 为奇数. $y^2\equiv 2(\mathrm{mod}\ p)$. 因此 $1=\left(\dfrac{2}{p}\right)$，则 $p\equiv\pm 1(\mathrm{mod}\ 8)$.

这与 $(x+1)^2+3\equiv 3(\mathrm{mod}\ 8)$ 矛盾，所以原方程没有整数解.

(6) $y^2=x(x-1)(x+1)$，当 $x=0,\pm 1$ 时，$y=0$. $|x|\geq 2$ 时，若 x 是偶数，$x,x+1,x-1$ 两两互素.

因此存在整数 a,b 使得 $x=a^2, x+1=b^2$，即 $b^2-a^2=1$，其中 $b>a>1$. 显然这是无解的.

若 x 是奇数，则 $\left(\dfrac{y}{2}\right)^2=x\cdot\dfrac{x+1}{2}\cdot\dfrac{x-1}{2}$. 其中 $x,\dfrac{x-1}{2},\dfrac{x+1}{2}$ 两两互素，同理，存在整数 a,b 使得

$a^2=\dfrac{x+1}{2}, b^2=\dfrac{x-1}{2}, a^2-b^2=1$ 故原方程的解为 $(0,0),(1,0),(-1,0)$.

初等数论第十次作业 2022.5.8

习题5.2.1

求所有正整数 m 和 n,使 2^m+3^n 是完全平方.

解：由题设 $2^m+3^n=x^2$ 有 $2,3\nmid x$ 方程两边模 3 有 $(-1)^m\equiv x^2\equiv 1\pmod 3$ 则 $m\equiv 0\pmod 2$

$m\geq 2, 2^m\geq 4, 2^m\equiv 0\pmod 4$，方程两边模 4 有 $0+(-1)^n\equiv x^2\pmod 4$ 而 $x^2\equiv 0,1\pmod 4$

则 $n\equiv 0\pmod 2$。令 $m=2k, n=2t$，原方程化为费马方程 $(2^k)^2+(3^t)^2=x^2$ 本原解满足

$$2^k=2mn, 3^t=m^2-n^2$$

且 m,n 一奇一偶，而 $2^{k-1}=mn$ 则 $n=1, m=2^{k-1}$ 代入有

$$3^t=2^{2(k-1)}-1\Longrightarrow 3^t=(2^{k-1}+1)(2^{k-1}-1)$$

而 $(2^{k-1}-1, 2^{k-1}+1)=1$，则 $2^{k-1}-1=1, k=2, t=1$ 则仅有唯一解 $m=4, n=2, 2^4+3^2=5^2$

习题5.2.2

求不定方程 $3^x+4^y=5^z$ 的所有正整数解.

解：方程模 3 有 $1\equiv 2^z\equiv(-1)^z\pmod 3$ 得到 $z\equiv 0\pmod 2$。方程模 4 有 $(-1)^x\equiv 1\pmod 5$

则 $x\equiv 0\pmod 2$，令 $x=2r, z=2k$，原方程化为费马方程 $(3^r)^2+(2^y)^2=(5^k)^2$ 本原解满足

$$2^y=2mn, 3^r=m^2-n^2=(m-n)(m+n)$$

由 $2^{y-1}=mn$ 知 $m=2^s, n=2^t$。有 $(m+n)-(m-n)=2n=2^{t+1}, 3\nmid 2^{t+1}$ 则 $m-n=1$

有 $2^s=2^t+1$，只有 $t=0, s=1$ 唯一解，回代得到唯一解 $(x,y,z)=(2,2,2)$

习题5.2.4

证明: $x^4+4y^4=z^2$ 没有正整数解.

证明：假设有解 (x,y,z) 若 $(x,y)>1$ 记素数 p 为 (x,y) 的一个约数，有 $p^4\mid x^4+4y^4=z^2$ 得到 $p^2\mid z$ 从而 $(\frac{x}{p},\frac{y}{p},\frac{z}{p^2})$ 为原方程的整数解，则有限步操作后总能使得 $(x,y)=1=(x^2,y^2)$ 若 $2\mid x$ 令 $x=2t$ 有 $2\nmid y$ 则 $16t^4+4y^4=z^2\Longrightarrow y^4+4t^4=(\frac{z}{2})^2$ 与原方程相同，且 $2\nmid y$，总可以化为 $2\nmid x$，有 $(x^2,2y^2)=1$ 则 $x^2,2y^2,z$ 为费马方程的本原解。令 z 为解中最小的，由 $2\mid 2y^2$ 可知，m,n 一奇一偶，$(m,n)=1,m>n$

$$x^2=m^2-n^2,2y^2=2mn,z^2=m^2+n^2$$

有 $m^2=x^2+n^2$ 因为 $(m,n)=1$，则 $(x,n)=1$，(x,n,m) 也为费马方程的本原解，由 x 为奇数

$$x=c^2-d^2,n=2cd,m=c^2+d^2,y^2=mn=2cd(c^2+d^2)$$

由 $2\mid mn=y^2,2\mid y$，则 $\frac{cd(c^2+d^2)}{2}=(\frac{y}{2})^2$ 为完全平方数，设 c,d 中偶数、奇数为 s,t $\frac{st(s^2+t^2)}{2}=(\frac{y}{2})^2$ 也成立，令 $s=2k$ 有 $kt(4k^2+t^2)=(\frac{y}{2})^2$ 又 $(c,d)=1=(k,t)$ 三者为完全平方数 则 $k=a^2,t=b^2,4k^2+t^2=c^2$ 消元有 $b^4+4a^4=c^2$ 而 $c^2=m-d^2<m=\sqrt{z^2-n^2}<z<z^2$ 与假设最小矛盾，从而原方程无解

习题5.2.6

证明: 1 不是同余数, 即不存在面积为 1、 三边长为有理数的直角三角形.

证明：原问题等价于满足 $a^2+b^2=c^2,ab=2d^2$ 的正整数解不存在，假设存在有若 $(a,b)=2$，则 $2\mid c,4\mid ab=2d^2,2\mid d$，从而 $(\frac{a}{2},\frac{b}{2},\frac{c}{2},\frac{d}{2})$ 也为解，若 $(a,b)=p\geq 3$ 则 $p^2\mid c^2,d^2$ 同理 $(\frac{a}{p},\frac{b}{p},\frac{c}{p},\frac{d}{p})$ 也为解，在有限步之后，总能使得 $(a,b)=1$，满足费马方程，a,b 一奇一偶，不妨设 $a=2k$ 有 $bk=d^2,(b,k)=1$ 则 $b=x^2,k=y^2$ 代入 $a^2+b^2=c^2$ 有 $4y^4+x^4=c^2$，由上题知该方程无解

习题5.3.1

证明: 形如 $4^a(8k+7)$ 的正整数不能表为三个整数的平方和.

证明：由 $x^2\equiv 0,1,4\pmod 8$ 计算 $a^2+b^2+c^2\equiv 0,1,2,3,4,5,6\not\equiv 7\pmod 8$ 从而 $8k+7$ 的正整数不能表示为三个整数平方和。对 $4(8k+7)=a^2+b^2+c^2$ 有 $x^2\equiv 0,1\pmod 4$，而三者之和模 0，则 $a^2\equiv b^2\equiv c^2\pmod 4$，有 $a,b,c\equiv 0\pmod 2$，则可以转化为 $a'^2+b'^2+c'^2=8k+7$ 的情况

从而 $4^a(8k+7)$ 均与 $8k+7$ 等价，从而不能表示为三个整数的平方和

习题5.3.2

(1) 确定哪些整数可表为两个整数的平方差.

(2) 证明: 对任意整数 n, 不定方程

$$x^2+y^2-z^2=n$$

均有无穷多组正整数解.

解：(1) $z=x^2-y^2=(x+y)(x-y)$，而 $(x+y)-(x-y)=2y$ 从而 $z\equiv 0,1,3\pmod 4$

而只要 $z\not\equiv 2\pmod 4$，分三种情况 $z=4k=2\cdot 2k, z=4k+1=1\cdot(4k+1), z=4k+3=1\cdot(4k+3)$

三种情况都对应有 x,y 解，从而当且仅当 $z\not\equiv 2\pmod 4$ 时该整数可以表示为两个整数的平方差

(2) 由 $y^2-z^2=n-x^2$ 且上问给出只要 $n-x^2\not\equiv 2\pmod 4$，就一定有解，而 $x^2\equiv 0,1\pmod 4$

对 $n\equiv 0,1,2,3\pmod 4$，所有情况都有 $x^2\equiv 0,0,1,0\pmod 4$ 使得 $n-x^2\not\equiv 2\pmod 4$ 成立

而满足上述条件的 x 有无穷多个，从而对应解 (x,y,z) 也有无穷多个

习题5.3.3

证明: 对任意给定的 $n\geqslant 1$, 均存在连续 n 个正整数, 其中每个都不是两个整数的平方和.

证明：取 $4k+3$ 型素数 n 个，存在正整数 N 使得

$$N\equiv -i+p_i\pmod{p_i^2}\quad(1\leqslant i\leqslant n)$$

从而 $N+i(1\leq i\leq n)$ 分解后 p_i 的幂次为 1，从而不能写成两个整数平方和，则 $N+1,\cdots,N+n$ 为所求

初等数论第十一次作业　　2022.5.11

设 F 是一个域, $f(x),g(x)\in F[x]$ 。

(1) 证明存在多项式 $q(x),r(x)\in F[x]$ 使得 $f(x)=g(x)q(x)+r(x)$ 且 $r(x)$ 的次数严格小于 $g(x)$;

(2) 设 $h(x)=(f(x),g(x))$ 是首项系数为 1 的最大公因式, 则存在 $p(x),q(x)\in F(x)$ 使得

$$f(x)p(x)+g(x)q(x)=h(x)$$

(3) 设 $f(x)\in F_p[x]$ 且 $g(x)$ 是模 $f(x)$ 的一个缩同余类。则存在 $h(x)$ 使得 $g(x)h(x)\equiv 1\ (\mathrm{mod}\ f(x))$ 。

证明：(1) 设 $f(x),g(x)$ 最高幂次为 x^{n_1},x^{n_2}，且系数分别为 a,b，不妨设 $n_1\geq n_2$，由非零元素存在乘法逆元

构造 $h(x)=ab^{-1}x^{n_1-n_2}$，有 $ax^{n_1}-bx^{n_2}\cdot ab^{-1}x^{n_1-n_2}=0$，则 $f(x)-h(x)g(x)$ 首项系数被消去。如此

新的最高幂次不超过 n_1-1，执行上述操作 n_1-n_2+1 之后，总能得到 $h_{tot}(x)=\sum\limits_{i=1}^{n_1-n_2+1}h_i(x)$

使得 $f(x)-g(x)h(x)$ 的最高次数严格小于 $g(x)$

(2) 由 (1) 中可知，实际上给出了域上的多项式有带余除法，使用辗转相除法

$$f(x)=g(x)q_1(x)+f_1(x),g(x)=f_1(x)q_2(x)+g_1(x),\cdots$$

最终得到 $f_N(x),g_{N-1}(x)=ah(x)$，从而 $h(x)=a^{-1}f_N(x)$，一直回代，每次保证为线性组合

从而有限次数之后总能找到 $f(x)q(x)+g(x)p(x)=h(x)$

(3) 由 (2) 可以得到，当 $(f(x),g(x))=1$ 时，存在 $p(x),h(x)$ 使得 $f(x)p(x)+g(x)h(x)=1$，从而

$$g(x)q(x)\equiv 1\pmod{f(x)}$$

2

证明 $\left(x^a-1,x^b-1\right)=\left(x^{(a,b)}-1\right)$ 。特别的, $\left(x^{a^m-1}-1,x^{a^n-1}-1\right)=x^{a^{(m,n)}}-1$ 。

证明：不妨设 $a\geq b$，$(x^a-1,x^b-1)=(x^b-1,x^a-x^b)=(x^b-1,x^b(x^{a-b}-1))$

而 $(x^b-1,x^b)=(1,x^b)=1$，则 $(x^a-1,x^b-1)=(x^{a-b}-1,x^b-1)$ 相当于指数项可以相互加减

则类比辗转相除法，经过有限步辗转相除后 $(x^a-1,x^b-1)=(x^{(a,b)}-1,x^{\lambda(a,b)}-1)=x^{(a,b)}-1$

3

设 $f(x)\in F_p[x]$ 。

(1) 证明 $f(x)^p=f\left(x^p\right)$;

(2) 证明 $f(x)$ 的导函数为 0 当且仅当存在 $g(x) \in F_p[x]$ 使得 $f(x) = g\left(x^p\right)$ 。

---

(1) 由费马小定理 $f(x)^p = (\sum_{i=0}^{n-1} a_i x^i)^p = \sum_{i=0}^{n-1} a_i^p x^{ip} + pg(x) = \sum_{i=0}^{n-1} a_i^{p-1} a_i (x^p)^i = \sum_{i=0}^{n-1} a_i (x^p)^i = f(x^p)$

(2) 由 $f(x) = \sum_{i=0}^{n-1} a_i x^i, f'(x) = \sum_{i=1}^{n-1} i a_i x^{i-1} = 0$ 从而存在数论倒数的 $p \nmid j$，$j a_j x^{j-1} = 0 \Longrightarrow a_j = 0$

从而剩下 $p \mid i$，使得 a_i 不一定为 0，则 $f(x) = \sum_{p|i} a_i x^i = g(x^p)$

4

证明 $F := \{a + bi \mid a, b \in \mathbb{Z}_5\}$ 不是一个域。

证明：假设 F 为一个域，由域有乘法逆元，考虑 $1 + 2i$ 的逆，在 F 中设为 $a + bi$，显然 F 的乘法单位元为 1，

故 $(1 + 2i)(a + bi) \equiv 1 \pmod 5$，整理为 $a \equiv 2b + 1 \pmod 5, 2a \equiv -b \pmod 5$，得 $0 \equiv 1 \pmod 5$ ，矛盾

初等数论第十二次作业 2022.5.21

柯召7.22

求出 F_2 上的全部四次不可约多项式.

解：计算 $\Phi_2(4) = \frac{1}{4}(\mu(1)2^4 + \mu(2)2^2 + \mu(4)2^1) = 3$. 从而共有 3 个四次不可约多项式， F_2 上，有

一次不可约多项式为 $x, x + 1$. 有 $x^2 \equiv x \pmod 2$ 从而当且仅当 $f(x)$ 的非零系数有偶数个时都不是不可约多项式（验证）

F_2 上的多项式 $f(x)$ 被 x 整除当且仅当 $f(0) = 0$ 从而排除掉上述情况有 F_2 上的不含有一次因子的四次多项式

$$x^4 + x^3 + x^2 + x + 1, x^4 + x^3 + 1, x^4 + x^2 + 1, x^4 + x + 1$$

而 $x^4 + x^2 + 1 = \left(x^2 + x + 1\right)^2$ 可约，则该多项式排除，则 F_2 上的全部四次不可约多项式为

$$x^4+x^3+x^2+x+1, x^4+x^3+1, x^4+x+1$$

柯召7.23

证明：若 $p\neq q$ 是两个奇素数, 则 F_p 上首项系数为 1 的 q 次不可约多项式的个数为 $\dfrac{p^q-p}{q}$.

证明：由 $\Phi_p(q)=\dfrac{1}{q}\sum\limits_{l|q}\mu(l)p^{\frac{q}{l}}=\dfrac{1}{q}(1\cdot p^q+(-1)\cdot p)=\dfrac{p^q-p}{q}$

柯召7.27

证明: 若 $(r,p^n-1)=1$, 则 F_{p^n} 中任一个元 α 是 F_{p^n} 中的 r 次幂元，若 $r\mid p^n-1$，则 α 是 F_{p^n} 中的 r 次幂元的充分必要条件是 $\alpha^{\frac{p^n-1}{r}}=1$

证明：若 $(r,p^n-1)=1$ ，则 r 存在数论倒数 r^{-1}。取 $F_p[x]$ 中的一个 n 次不可约多项式，取模 f 的原根 g.

则对任意的 $\alpha\in F_{p^n}$ ，都存在整数 s ，使得 $\alpha\equiv g^s(\mathrm{mod}\ f)$. 令 $t=sr^{-1}$ ，则 $\left(g^t\right)^r\equiv g^s\equiv\alpha(\mathrm{mod}\ f)$

从而 α 是 r 次幂元

若 $r\mid p^n-1$，$\Longrightarrow$: $\alpha=\beta^r,\alpha^{\frac{p^n-1}{r}}=\beta^{p^n-1}\equiv 1\pmod f$ $\Longleftarrow$: 设 $\alpha=g^s$ 代入有

$$\alpha^{\frac{p^n-1}{r}}=1=g^{\frac{s(p^n-1)}{r}}\equiv 1\pmod f$$

由原根的性质可得 $r\mid s$ 从而 α 为 r 次幂元

柯召7.28

证明：设 $\alpha_1,\cdots,\alpha_{p^n-1}$ 是 F_{p^n} 中的全体非零元, 则

$$\alpha_1\cdots\alpha_{p^n-1}=-1.$$

证明：类比威尔逊定理的证明，取 $F_p[x]$ 中的一个 n 次不可约多项式，然后取其原根 g 则

$$\alpha_1\cdots\alpha_{p^n-1}\equiv g^{1+2+\cdots+(p^n-1)}\equiv\left(g^{\frac{p^n-1}{2}}\right)^{p^n}\equiv(-1)^{p^n}\equiv-1(\mathrm{mod}\ f)$$

其中 $g^{\frac{p^n-1}{2}}\equiv-1\pmod{p^n-1}$ 为原根的性质

> **特殊情况**，考虑 $p=2$ 有 $(-1)^{p^n}\equiv 1\equiv-1\pmod f$ 从而对所有素数成立

柯召7.32

证明：若 F_p 上 n 次不可约多项式的周期为 l, 则 p 模 l 的次数为 n.

证明：由原根的性质可知，$l \mid p^n-1$，令 $p^x \equiv 1 \pmod{l}$ 显然次数 r 满足 $r \mid n$，

于是 $f \mid x^{p^r}-x$ ，但 f 是 n 次的，故 $n \leq r$. 于是 $r=n$ ，即 p 模 l 的次数为 n.

初等数论第十三次作业　　2022.5.28

柯召7.34

分别求出 F_2 上多项式 $f(x)=(x+1)\left(x^3+x+1\right)\left(x^3+x^2+1\right)$ 和 $g(x)=(x^2+x+1)\cdot$

$\left(x^4+x+1\right)^3$ 的周期.

解：由定理可知周期等于 $[l_1,\cdots,l_n]e, e=\{2^r:r\in Z, r\geq 0, 2^r\geq 1(f(x)),3(g(x))\}=1,4$，求 l_i

由 $x+1 \mid x-1$ 最小正整数为 1，则对 $f(x)$ 中 $(x+1)$ 的周期为 1，对 (x^3+x+1) 和 (x^3+x^2+1)

均为不可约多项式，且 $2^3-1=7$ 为素数，从而两者周期均为 7，故 $f(x)$ 周期为 $[1,7,7]\cdot 1=7$

$x^2-1=3$ 为素数，且 x^2+x+1 为不可约多项式，则其周期为 3

对 (x^4+x+1) 有 $2^4-1=15$ 为合数，而分别计算 $x^5, x^3 \stackrel{?}{\equiv} 1 \pmod{x^4+x^2+1}$

$$x^5=x\cdot x^4\equiv x(-x-1)\equiv -x^2-x\equiv -x(x+1)\not\equiv 1 \pmod{x^4+x+1}$$
$$x^3\not\equiv 1 \pmod{x^4+x+1}$$

故 15 为 x^4+x+1 的周期，$g(x)$ 周期为 $[3,15]\cdot 4=60$，故 $f(x)$ 和 $g(x)$ 的周期为 7 和 60

柯召7.36

求 F_2 上多项式 $x^{2\cdot 3^k}+x^{3^k}+1$ 的周期, 并证明它是不可约的。

解：由立方差公式 $x^{3\cdot 3^k}-1=(x^{2\cdot 3^k}+x^{3^k}+1)(x^{3^k}-1)$ 则 $x^{2\cdot 3^k}+x^{3^k}+1 \mid x^{3^{k+1}}-1$ 令其周期为 r

有 $r \mid 3^{k+1}$，而考虑 $x^{2\cdot 3^k}+x^{3^k}+1 \mid x^r-1$ 的最高次项，$r \geq 2\cdot 3^k$，故 $r=3^{k+1}$

假设该多项式不可约，则其能被分解为若干个不可约多项式之积，由不可约多项式周期相关定理有

$$3^{k+1}=[l_1,l_2,\cdots,l_n]e$$

由 $e=2^r$ 则 $e=1,\exists\ s\in[1,n],s.t.\ l_s=3^{k+1}$ 令该不可约多项式为 $p(x)$ 令其最高幂次项为 n，有

$$3^{k+1}\mid 2^n-1$$

两边模 3 有 $(-1)^n\equiv 1\pmod 3$，则 $n\equiv 0\pmod 2$，取 $n=2t$ 代入有 $3^{k+1}\mid 4^t-1$

将其展开 $4^t-1=(1+3)^t-1$ 其中 3 的最小幂次为 $k+1$ 则 $3^{k+1}\mid 3t,3^k\mid t$ 则 $n=2t\geq 2\cdot 3^k$

恰为 $f(x)$ 的最高幂次，从而该多项式即为其本身，故其不可约

柯召8.16

设 p 是一个奇素数, $d=(m,p-1)$, 证明: $N\left(x^m=a\right)=N\left(x^d=a\right)$.

证明：当 $x^d\equiv a\pmod p$ 无解时，$x^m\equiv a\pmod p$ 也无解（否则 $(x^{\frac{m}{d}})^d$ 为前者的解）

又当 $x^d\equiv a\pmod p$ 有解时，其解有 d 个，设为 $x_1,\cdots,x_d$ ，又注意到 $(\dfrac{m}{d},p-1)=1$ 则有

$p-1$ 的完系均为 $\dfrac{m}{d}$ 次剩余，则 $x^m\equiv a\pmod p$ 等价于 $x^{\frac{m}{d}}\equiv x_i\pmod p$ ，每个方程都只有一解

（取 p 的原根 g，有 $\dfrac{m}{d}\mathrm{ind}_g x\equiv \mathrm{ind}_g x_i\pmod{p-1}$ 则只有一解）故两者解为 d 个

柯召8.21

证明：若 $k\mid p-1,\chi$ 是 F_p 上一个 k 阶特征, 则

$$\sum_{j=0}^{k-1}\chi^j(-1)=\begin{cases}k, & \text{当}\left(\dfrac{-1}{p}\right)_k=1\text{时},\\ 0, & \text{当}\left(\dfrac{-1}{p}\right)_k\neq 1\text{时}.\end{cases}$$

证明：由定理可知，$\sum\limits_{j=0}^{k-1}\chi^j(-1)=N(x^k=-1)$，则当 $(\dfrac{-1}{p})_k=1$ 时，显然该方程有 k 个解，当 $(\dfrac{-1}{p})_k=1$ 时，

该方程无解，故 $\sum\limits_{j=0}^{k-1}\chi^j(-1)=\begin{cases}k, & \text{当}\left(\dfrac{-1}{p}\right)_k=1\text{时},\\ 0, & \text{当}\left(\dfrac{-1}{p}\right)_k\neq 1\text{时}.\end{cases}$

初等数论第十四次作业　　2022.6.2

阶以及雅可比和

设 $\chi \neq \chi_0$ 是 F_p 上的一个特征。设 $\rho(a) = \left(\dfrac{a}{p}\right)$ 是唯一的 2 阶特征。设 $p \neq 2$ 。

(1) 证明

$$\sum_{t \in F_p} \chi\left(1-t^2\right) = J(\chi, \rho)$$

(2) 设 $0 \neq k \in F_p$ 。证明

$$\sum_{t \in F_p} \chi(t(k-t)) = \frac{\chi\left(k^2\right)}{\chi\left(2^2\right)} J(\chi, \rho)$$

(提示：利用 (1))

(3) 证明 $J(\chi, \chi) = \chi(2)^{-2} J(\chi, \rho)$; (提示：利用 (2))

(4) 设 $\chi^2 \neq \chi_0$ 。证明 $g_1(\chi)^2 = \chi(2)^{-2} J(\chi, \rho) g_1\left(\chi^2\right)$;

(5) 设 $p \equiv 1 (\mathrm{mod}\ 3)$ 且 χ 是一个 3 阶特征。证明 $g_1(\chi)^3 = p \cdot \chi(2) J(\chi, \rho)$;

(6) 设 $p \equiv 1 (\mathrm{mod}\ 4)$ 且 χ 是一个 4 阶特征。证明 $\chi^2 = \rho$ 且 $J(\chi, \chi) = \chi(-1) J(\chi, \rho)$ 。

(提示: 证明 $\chi(-1) = (\dfrac{2}{p})$)

解：(1) 由雅可比定义，代入 $\left(\dfrac{a}{p}\right) = N(x^2 = a) - 1$ 有

$$J(\chi, \rho) = \sum_{t \in F_p} \chi(1-t)\rho(t) = \sum_{t \in F_p} \chi(1-t)(N(x^2 = t) - 1)$$

$$= \sum_{t \in F_p} \chi(1-t) N(x^2 = t) - \sum_{t \in F_p} \chi(1-t) = \sum_{t \in F_p} \chi(1-t) N(x^2 = t)$$

而 $N(x^2 = t)$ 对求和有贡献的有两类，当 $N(x^2 = t) = 1$ 时 $t = 0$，当 $N(x^2 = t) = 2$ 时，t 为二次剩余

$$J(\chi, \rho) = \chi(1-0) \cdot 1 + 2 \cdot \sum_{(\frac{t}{p}) = 1} \chi(1-t)$$

而对每一个二次剩余 $t = b^2$，且 $\chi(1-b^2)$ 中 $\pm b$ 对应同一个 t，且保证所有的 b 不同，构成 F_p 中所有非零元素

$$J(\chi, \rho) = 1 + 2 \cdot \sum_{b \in F_p, b \neq 0} \chi(1-b^2) = \sum_{t \in F_p} \chi\left(1-t^2\right)$$

(2) 由 $(2, p) = 1$ 以及 $(k, p) = 1$，则 $\{2t \mid t \in F_p\}$ 和 $\{kt \mid t \in F_p\}$ 构成 F_p 中的完系，则

$$\chi(k)^2\sum_{t\in F_p}\chi(1+t)\chi(1-t)=\sum_{t\in F_p}\chi(k+kt)\chi(k-kt)=\chi(k)^2\sum_{t\in F_p}\chi(1-t^2)=\sum_{t\in F_p}\chi(k+t)\chi(k-t)$$
$$=\sum_{t\in F_p}\chi(t)\chi(2k-t)=\sum_{t\in F_p}\chi(2t)\chi(2k-2t)=\chi(2)^2\sum_{t\in F_p}\chi(t)\chi(k-t)$$

代入 (1) 中结论 $\sum_{t\in F_p}\chi\left(1-t^2\right)=J(\chi,\rho)$ 则得到 $\sum_{t\in F_p}\chi(t(k-t))=\dfrac{\chi\left(k^2\right)}{\chi\left(2^2\right)}J(\chi,\rho)$

(3) 取 $k=1$ 有 $\sum_{t\in F_p}\chi(t(1-t))=\dfrac{\chi\left(1^2\right)}{\chi\left(2^2\right)}J(\chi,\rho)=\sum_{t\in F_p}\chi(t)\chi(1-t)=J(\chi,\chi)$

而 $\chi(1)=1$，代入得 $J(\chi,\chi)=\chi(2)^{-2}J(\chi,\rho)$

(4) 由雅可比和与高斯和之间的关系有 $J(\chi,\chi)=\dfrac{g_1(\chi)\cdot g_1(\chi)}{g_1(\chi^2)}=\chi(2)^{-2}J(\chi,\rho)$

移项整理得到 $g_1(\chi)^2=\chi(2)^{-2}J(\chi,\rho)g_1\left(\chi^2\right)$

(5) 在 (4) 等式左右乘以 $g_1(\chi)$ 可以得到 $g_1(\chi)^3=\chi(2)^{-2}J(\chi,\rho)g_1\left(\chi^2\right)g_1(\chi)$，而由于 χ 为 3 阶特征

则 $\chi(2)^3=1$ 则 $g_1(\chi)^3=\chi(2)J(\chi,\rho)g_1\left(\chi^2\right)g_1(\chi)$ 由于

$$\overline{g(\chi)}=\sum_t\overline{\chi(t)}\zeta^{-t}=\chi(-1)\sum_t\overline{\chi(-t)}\zeta(-t)=\chi(-1)g(\chi)$$

有 $\chi(-1)^3=1$ 且 $\chi(-1)^2=\chi(1)=1$，故 $\chi(-1)=1$，代入有

$$g\left(\chi^2\right)g(\chi)=g(\bar{\chi})g(\chi)=\overline{g(\chi)}g(\chi)=|g(\chi)|^2=p$$

则 $g_1(\chi)^3=p\cdot\chi(2)J(\chi,\rho)$

(6) 由于 χ 的阶为 4，则 χ^2 的阶为 2，而 ρ 为唯一的二阶特征，故 $\chi^2=\rho$，由高斯和与雅可比和之间关系

$$g(\chi)^4=\chi(-1)pJ(\chi,\chi)J\left(\chi,\chi^2\right)=\chi(-1)pJ(\chi,\chi)J(\chi,\rho)$$

又对 (4) 中的等式两边平方得到

$$g(\chi)^4=\chi(2)^{-4}J(\chi,\rho)^2\left[g\left(\chi^2\right)\right]^2$$

而由 4 阶特征可以得到 $\chi\left(2^4\right)=\chi^4(2)=\chi_0(2)=1$, and $g\left(\chi^2\right)=g(\rho)=g$, so $\left[g\left(\chi^2\right)\right]^2=g^2$ ，而有

$$g_ag_{-a}=(\frac{a}{p})(\frac{-a}{p})g^2=(\frac{-1}{p})g^2\Longrightarrow\sum_a g_ag_{-a}=\left(\frac{-1}{p}\right)(p-1)g^2$$

而使用另一种方法计算左边有

$$g_ag_{-a}=\sum_x\sum_y\left(\frac{x}{p}\right)\left(\frac{y}{p}\right)\zeta^{a(x-y)}=\sum_x\sum_y\left(\frac{x}{p}\right)\left(\frac{y}{p}\right)\delta(x,y)p=(p-1)p$$

两式对比有 $g^2=(\dfrac{-1}{p})p$ 由于 $p\equiv1\pmod 4$ 则 $(\dfrac{-1}{p})=1$ 则 $g^2=p$，则有

$$\chi(-1)pJ(\chi,\chi)J(\chi,\rho)=J(\chi,\rho)^2p$$

由于 $g(\chi)^4\neq0$ 以及 $|g(\chi)|^2=p$，有 $J(\chi,\rho)\neq0$, 则两边约去 $pJ(\chi,\rho)$ 有

$$\chi(-1)J(\chi,\chi)=J(\chi,\rho)$$

$[\chi(-1)]^2=\chi\left((-1)^2\right)=\chi(1)=1$, 故 $\chi(-1)=\pm1$, 从而 $\chi(-1)^{-1}=\chi(-1)$, 移项得到

$$J(\chi,\chi)=\chi(-1)J(\chi,\rho)$$

初等数论第十五次作业 2022.6.12

雅可比和以及加密解密

1. 设 p 是一个奇素数, 计算
   (1) $N\left(x^3-y^3=1\right),p=37$;
   (2) $N\left(9x^2+8y^2=a\right),p=17,a\in F_{17}^*$ 。
2. 使用加密密钥 $E(x)\equiv x+3(\mathrm{mod}\ 26)$ 将信息 “mathematics” 加密.
3. 已知加密密钥 $E(x)\equiv x+5(\mathrm{mod}\ 26)$ 。将信息 "lttijajsnsl" 解密.
4. 假设加密密钥 $E(x)\equiv 3x+1(\mathrm{mod}\ 26)$, 求去密密钥 $D(y)$, 并将信息 “EBOBO BEBOK" 解密。

1、解：(1) 计算 $M(x^3+(-y)^3=1)=\sum\limits_{i=0}^{2}\sum\limits_{j=0}^{2}\chi^i(a)\chi^j(1-a)=p+J(\chi,\chi)+J(\chi^2,\chi^2)-2\chi(-1)$

$=p-2+J(\chi,\chi)+J(\chi^2,\chi^2)=p-2+J(\chi,\chi)+\overline{J(\chi,\chi)}$ 令 $J(\chi,\chi)=a+b\omega,\omega=-\dfrac{1}{2}+\dfrac{\sqrt{3}}{2}i$

得到 $p-2+2a-b$，由分解定理 $4p=(2a-b)^2+27(\dfrac{b}{3})^2=148=11^2+27\cdot1\Longrightarrow a=7,b=3$ 要求 $2a-b\equiv1\pmod 3$

则 $2a-b=-11$ $N(x^3-y^3=1)=37-2+(-11)=24$

(2) 由 $p=17$ 得 $N(9x^2+8y^2=a)=N(9(x^2-y^2)=a)$ 而 $\{3x\}$ 与 $\{x\}$ 均取遍所有 F_p^*，故化解为 $N(x^2-y^2=a)$

由 $(\dfrac{-1}{p})=(-1)^{\frac{p-1}{2}}=1$ 知 -1 为二次剩余，从而 $-y^2=(a_0)^2(y)^2=(a_0y)^2$ 又可化解为 $N(x^2+y^2=a)$

$$\begin{aligned}N(x^2+y^2=a)&=\sum_{i=0}^{1}\sum_{j=0}^{1}\chi^i(t)\chi^j(a-t)=p+J(\chi,\chi_0)+J(\chi_0,\chi)+J(\chi,\chi)\\&=p-\chi(-1)=p+\sum_{c\in F_p}\chi(\frac{c}{a-c})\end{aligned}$$

而 $\dfrac{c}{a-c}=t\Longrightarrow c=\dfrac{at}{t+1}$ 只有 $t=-1$ 元素没有遍历，从而 $\sum\limits_{c\in F_p}\chi(\dfrac{c}{a-c})=0-\chi(-1)=-1$

故原方程有 $17+(-1)=16$ 个解

2、使用 python 编程计算，代码如下，加密结果为 **pdwkhpdwlfv**

```
charList = "abcdefghijklmnopqrstuvwxyz"
word = "mathematics"
for i in word:
    print(charList[(ord(i) - ord("a") + 3) % 26], end = "")
```

3、只需改动一行代码，解密结果为 **goodevening**

```
  print(charList[(ord(i) - ord("a") - 5) % 26], end = "")
```

4、反解同余方程得 $x \equiv 9 \cdot (y-1) \equiv 9y + 17 \pmod{26}$，代码如下，解密结果为 **BANAN ABAND**

```
  print(charList[(9 * (ord(i) - ord("A")) + 17) % 26], end = ""
```