Number Theory

ppwwyyxxc@gmail.com

July 8, 2013

目录

1 Order

Definition: $\delta_m(a) = \min\{x | a^x \equiv 1 \pmod m\}$

推广: $a^d \equiv b^d \pmod p$,取倒数 $bb' \equiv 1 \pmod p$,则 $d = \delta_p(ab')$.性质类似

若 $a^n \equiv 1 \pmod m$,则 $\delta_m(a) \mid n$. 否则设 $n = \delta_m(a)q + r, a^r \equiv a^n \equiv 1$ 且 $r < \delta_m(a)$.矛盾

特别地,若 $a^p \equiv 1 \pmod m$, 则 $\delta_m(a) = 1$ 或 p

Mersenne's Prime 的因子特征:$q \mid 2^p - 1 \Rightarrow p = \delta_q(2) \mid (q-1) \Rightarrow q \equiv 1 \pmod{2p}$

$(a,p) = 1$,则在 $p^0, p^1, \dots p^{a-1} \pmod{a}$ 中抽屉得 $\exists d \le a-1 : a | p^d - 1 \Rightarrow \delta_p(a) \le a-1$

证明 $n \nmid 2^n - 1$:
设 n 最小素因子 p,则 $\delta_p(2) \mid (p-1, n) = (p-1, \dfrac{n}{p^\alpha}) = 1$.
或者利用递降:$n \to \delta_n(2); (a,b) \to (b, (a,b))$

$n \mid 2^n + 1 \Rightarrow \delta_p(2) \mid (2n, p-1) = (2, p-1) \Rightarrow p = 3$.
事实上有 $3^k \mid 2^{3^k} + 1$,以及 $n \mid 2^n + 1 \Rightarrow m \mid 2^m + 1, m = 2^n + 1$

反证 $n \nmid m^{n-1} + 1$:
设 $n - 1 = 2^k t \Rightarrow m^{2^k t} \equiv -1 \pmod{p} \Rightarrow \delta_p(m) \nmid 2^k t, \delta_p(m) \mid 2^{k+1} t \Rightarrow 2^{k+1} \mid \delta_p(m)$
又 $\delta_p(m) \mid p - 1, \therefore p \equiv 1 \pmod{2^{k+1}}$. 考虑到 p 为 n 任意素因子 $\Rightarrow n \equiv 1 \pmod{2^{k+1}}$,与 $n - 1 = 2^k t$ 矛盾

关于 $r_k = \delta_{p^k}(a)$ 的求解(p 为奇数).设 $p^{k_0} \parallel a^{r_1} - 1$
i)当 $1 \le k \le k_0$ 时,$a^{r_k} \equiv 1 \pmod{p^k \to p} \Rightarrow r_1 \mid r_k$
$a^r \equiv 1 \pmod{p^{k_0} \to p^k} \Rightarrow r_k \mid r_1. \therefore r_k = r_1$
ii)当 $k \ge k_0$ 时,对 k 归纳证明 $r_k = r_1 p^{k-k_0}$
引理:$p^{k_0+i} \parallel a^{r_1 p^i} - 1 \Leftrightarrow a^{r_1 p^i} = 1 + p^{k_0+i} u, (u,p) = 1$.
证明:归纳. $a^{r_1 p^{i+1}} = (a^{r_1 p^i})^p = (1 + p^{k_0+i} u)^p = 1 + p^{k_0+i+1}(1 + C_p^2 u^2 p^{k_0+i-1})$
引理中取 $i = k - k_0$, 则 $a^{r_1 p^{k-k_0}} \equiv 1 \pmod{p^k} \Rightarrow r_k \mid r_1 p^{k-k_0}$
$a^{r_k} \equiv 1 \pmod{p^k \to p^{k-1}} \Rightarrow r_{k-1} \mid r_k \therefore r_1 p^{k-k_0-1} \mid r_k \mid r_1 p^{k-k_0}$
再取 $i = k - k_0 - 1$,由 $p^{k-1} \parallel a^{r_1 p^{k-k_0-1}} - 1$ 知 $a^{r_1 p^{k-k_0-1}} \not\equiv 1 \pmod{p^k}$.

$$\therefore r_k = \begin{cases} r_1, & 1 \le k \le k_0 \\ r_1 p^{k-k_0}, & k \ge k_0 \end{cases}$$

$r_k = \delta_{2^k}(a)$ 的求解:

i)$a = 4k+1, 2^{k_0} \parallel a - 1, r_k = \begin{cases} 1, & 1 \le k \le k_0 \\ 2^{k-k_0}, & k \ge k_0 \end{cases}$

ii)$a=4k+3, 2^{k_0} \parallel a+1, r_k = \begin{cases} 1, & k=1 \\ 2, & 2 \le k \le k_0+1 \\ 2^{k-k_0}, & k \ge k_0+1 \end{cases}$

引理的推广:$a^{mrp^i} = 1+p^{k_0+i}u, (u,p)=1.$

设 $n=mrp^i$ 可得一命题:$r=\delta_p(a), r \mid n, p^\alpha \parallel n \Rightarrow p^\alpha \parallel \dfrac{a^n-1}{a^r-1}$

反证:对给定 n,a,不存在无穷个 $k, s.t. n^k \mid a^k-1$

i)n 含奇因子 $p, a^k \equiv 1 \pmod{p^k} \Rightarrow r_k = r_1 p^{k-k_0} \mid k \Rightarrow k > r_1 p^{k-k_0} \ge 3^{k-k_0}$ 不可能无穷个

ii)若 k 为奇,则 $2^k \mid a^k-1 \Rightarrow 2^k \mid a-1$, 只有有限个 k.

若 k 为偶,$a^{2l} \equiv 1 \pmod{2^l}$. 当 $l > k_0$ 时,$2^{l-k_0} \mid l$ 不可能无穷个.

$r_k = \delta_m(a^k) = \dfrac{r_1}{(r_1,k)}$.

证:设 $r' = \dfrac{r_1}{(r_1,k)}$.显然 $(r', \dfrac{k}{(r_1,k)}) = 1$

由定义,$a^{kr_k} \equiv 1 \pmod{m}, a^{kr'} \equiv 1 \pmod{m}. \Rightarrow r_1 \mid kr_k, r_k \mid r'$

$\therefore r' = \dfrac{r_1}{(r_1,k)} \mid \dfrac{k}{(r_1,k)} r_k \Rightarrow r' \mid r_k. \therefore r' = r_k$

推论:有 $\varphi(r_1)$ 个 $k, s.t. (r_1,k)=1$. 又 $a^0, a^1, \cdots, a^{r_1-1}$ 对模 m 不同余

所以其中至少有 $\varphi(r_1)$ 个 $k, s.t. \delta_m(a^k) = r_1$.

即在模 m 的一个缩系中至少有 $\varphi(r_1)$ 个 $k, s.t. r_k = r_1$

若 $(m_1,m_2)=1$, 则 $\delta_{m_1m_2}(a) = [\delta_{m_1}(a), \delta_{m_2}(a)] = [r_1, r_2]$

证:i)显然对 $\forall n \mid m, \delta_n(a) \mid \delta_m(a). \therefore [r_1,r_2] \mid \delta_{m_1m_2}(a)$

ii)$a^{[r_1,r_2]} \equiv 1 \pmod{m_1, m_2 \to m_1m_2} \Rightarrow \delta_{m_1m_2} \mid [r_1,r_2]$

推论:$(m_1,m_2)=1$,则对 $\forall a_1,a_2, \exists a, s.t. \delta_{m_1m_2}(a) = [\delta_{m_1}(a_1), \delta_{m_2}(a_2)]$

证:取 $a \equiv a_i \pmod{m_i}, i=1,2$.则 $\delta_{m_i}(a) = \delta_{m_i}(a_i)$.由原命题即证.

$\min\{n | 2^n \equiv -1 \pmod{p}\} < \delta_p(2)$, 否则 ,$2^{n-\delta_p(2)} \equiv 2^n \equiv -1$,与最小性矛盾.

$p=3k+2$ 时,x 取 $\mod p$ 完系,则 x^3 亦遍历.否则 $x^3 \equiv y^3 \Rightarrow \delta_p(xy^{-1}) \mid (3,p-1)=1$.矛盾

无穷数列 $\dfrac{1}{9}(10^{k\delta_{9a}(10)}-1)(k \ge 1)$ 中,每项均由 1 组成且均为 a 的倍数

奇素 $p, p^n|a^p-1 \Rightarrow p^{n-1}|a-1$

$\exists n, s.t. p \parallel 2^n-1 \Rightarrow p \parallel 2^{p-1}-1$

证:假设 $p^2 \mid 2^{p-1}-1 \Rightarrow \delta_{p^2}(2) \mid p-1$.

又 $2^{pn}-1=(2^n-1)(2^{n(p-1)}+2^{n(p-2)}+\cdots+2^n+1) \equiv (2^n-1)p \equiv 0 \pmod{p^2}$

$\therefore \delta_{p^2}(2) \mid (pn, p-1)=(n, p-1) \mid n \Rightarrow 2^n \equiv 1 \pmod{p^2}$.矛盾

奇素数 $p, pn+1$ 中含无穷多素数:

证:取 x^p-1 的因子 $q, s.t. q \nmid x-1$ (why can?).则 $\delta_q(x)=p$.

设 $(q-1,p)=d$,则 $\exists u, v, s.t. u(q-1)+vp=d \Rightarrow x^d \equiv (x^{q-1})^n(x^p)^v \equiv 1 \pmod{q} \Rightarrow d=p$

$\therefore p \mid q-1 \Leftrightarrow q=pn+1$.又 $\dfrac{x^p-1}{x-1}$ 含无穷个素因子 q,可知 $pn+1$ 中有无穷多素数

2 Wilson

Wilson 定理:素数 $p \Leftrightarrow (p-1)! \equiv -1 \pmod{p}$

可推出:$(p-k)!(k-1)! \equiv (-1)^k \pmod{p}$

Lagrange 定理:$f(x)=\sum\limits_{i=1}^{n} a_i x^i, p \nmid a_i$,则 n 次同余方程 $f(x) \equiv 0 \pmod{p}$ 的解数 $\leq n$

对 n 归纳反证.假设 $n+1$ 个解 $c_1 \cdots c_{n+1}$,则 $f(x)-f(c_1)=(x-c_1)h(x)$

于是 $c_2, \cdots c_{n+1}$ 均为 $n-1$ 次同余方程 $h(x) \equiv 0 \pmod{p}$ 的解.矛盾

推论:若 $f(x) \equiv 0$ 的解数 $> n$,则各项系数均被 p 整除.

$f(x)=(x-1)(x-2)\cdots(x-p+1)=\sum\limits_{i=0}^{p-1} s_i x^i \equiv x^{p-1}-1 \pmod{p}$(Fermat)

$\Rightarrow f(x)-x^{p-1}+1=\sum\limits_{i=1}^{p-2} s_i x^i+(p-1)!+1 \equiv 0 \pmod{p}$

由 Lagrange 得 $p \mid s_i, 1 \leq i \leq p-2$

$f(x)=f(p-x) \Rightarrow f(-x)=f(p+x)$

$\Rightarrow x^{p-1}+\sum\limits_{i=1}^{p-2}(-1)^i s_i x^i=(p+x)^{p-1}+\sum\limits_{i=1}^{p-2} s_i(p+x)^i$

两边模 p^2 得,$x^{p-1}+\sum\limits_{i=1}^{p-2}(-1)^i s_i x^i \equiv x^{p-1}+(p-1)px^{p-2}+\sum\limits_{i=1}^{p-2} s_i x^i$

$\Rightarrow \sum_{i=1}^{p-2}[(-1)^i-1]s_ix^i \equiv p(p-1)x^{p-2} \pmod{p^2}$
$\Rightarrow \sum_{i=1}^{p-3}[(-1)^i-1]s_ix^i \equiv 0 \pmod{p^2}(\because s_{p-2}=-\dfrac{p(p-1)}{2})$
$\Rightarrow p^2 \mid s_1, s_3, \cdots s_{p-4}$
推论:$p^2 \mid s_1=(p-1)!(1+\dfrac{1}{2}+\cdots+\dfrac{1}{p-1}), p \mid s_{p-3}=\sum\limits_{1\leq i\leq j\leq p-1} ij$

Wilson 定理推广:
T1.奇素数 p,设 $c=\varphi(p^l), r_1,\cdots,r_c$ 是 modp^l 的缩系,则 $\prod\limits_{i=1}^{c} r_i \equiv -1 \pmod{p^l}$
证:对每个 r_i 有唯一 r_j 使 $r_ir_j \equiv 1 \pmod{p^l}$.
此时 $r_i=r_j \Leftrightarrow r_i \equiv 1,-1 \pmod{p^l}$ 配对即得证.

T2:$\because \varphi(p^l)=\varphi(2p^l)$, 取 $r_i'=\begin{cases} r_i, & 2 \nmid r_i \\ r_i+p^l, & 2 \mid r_i \end{cases}$,则 r_i' 为 mod$2p^l$ 的缩系
且 $\prod\limits_{i=1}^{c} r_i' \equiv -1 \pmod{p^l}, 2 \mid \prod\limits_{i=1}^{c} r_i'+1 \Rightarrow \prod\limits_{i=1}^{c} r_i' \equiv -1 \pmod{2p^l}$

T3:设 $c=\varphi(2^l), l \geq 3, r_1\cdots r_c$ 是 mod2^l 的缩系.则 $\prod\limits_{i=1}^{c} r_i \equiv 1 \pmod{2^l}$
证:同 T1,使 $r_i=r_j$ 的充要条件是 $\dfrac{r_i-1}{2}\dfrac{r_i+1}{2} \equiv 0 \pmod{2^{l-2}} \Leftrightarrow r_i \equiv 1, 2^{l-1}\pm 1, 2^l-1$

3 Special Numbers

2^k-1 为素数 $\Rightarrow k$ 为素数
Mersenne's Prime$\Leftrightarrow$Perfect Number:($\sigma(n)=2n \Leftrightarrow n=\dfrac{1}{2}M_{(p)}(M_{(p)}+1)$)
i)若 $n=2^{p-1}M_{(p)}$, 则 $\sigma(n)=(1+2+\cdots+2^{p-1})(1+M_{(p)})=2n$
ii)若 n 为偶完全数,易知 $n\neq 2^k$,
于是设 $n=2^{m-1}u \Rightarrow 2^mu=\sigma(n)=\sigma(2^{m-1})\sigma(u)=(2^m-1)\sigma(u)$
从而 $\sigma(u)=u+\dfrac{u}{2^m-1} \Rightarrow u=2^m-1$, 且 2^m-1 为素数

n^k+1 为素数 $\Rightarrow k$ 为 2 的幂
Fermat's Number
$n \geq 5$ 时 $2^n \equiv 2^{n-4} \pmod 10 \Rightarrow F_n(n\geq 2) \equiv 7 \pmod 10$
$F_n=2^{2^n}+1, F_0F_1\cdots F_{n-1}+2=F_n \Rightarrow (F_n,F_m)=1 \Rightarrow$ 素数无穷多

在任意形如 a^x-1 中设 $x=2^kq$,则可分解 $a^x-1=(a^q)^{2^k}-1=\cdots$

设 F_n 的任一素因子 $p,2^{2^n}\equiv -1 \pmod p \therefore \delta_p(2)\mid 2^{n+1}\Rightarrow \delta_p(2)=2^k$

又 $2^{2^k}\equiv 1 \pmod p, 2^{2^n}\equiv -1 \pmod p \Rightarrow k>n\Rightarrow k=n+1$

有结论:$\delta_p(2)=2^{n+1},2^{n+1}\mid p-1$

一般地,$a^{2^k}\equiv -1 \pmod m \Rightarrow \delta_m(a)=2^{k+1}$

伪素数递归构造

$n\mid 2^n-2\Rightarrow 2^{2^n-1}-2=2^{nk+1}-2=2(2^{nk}-1)\equiv 0 \pmod{2^n-1}$

孪生素数 $p,q=p+2.p+q\mid p^p+q^q$

证:$RHS=p^p+(p+2)^p+(p+2)^{p+2}-(p+2)^p=A(p+q)+q^p(p+1)(p+3)$

Sylvester's Sequence $a_1=2,a_n=a_{n-1}^2-a_{n-1}+1\Rightarrow \sum\limits_{i=1}^{n}\frac{1}{a_i}+\frac{1}{\prod\limits_{i=1}^{n}a_i}=1$

$a_{n+1}=\prod\limits_{i=1}^{n}a_i+1\Rightarrow (a_n,a_m)=1,a_n\geq 2^{n-1}$

最佳单位分数逼近:对 $\forall\{x_n\},\sum\limits_{i=1}^{n}\frac{1}{x_i}<1\Rightarrow \sum\limits_{i=1}^{n}\frac{1}{x_i}\leq\sum\limits_{i=1}^{n}\frac{1}{a_i}$

证:设有 $\sum\limits_{i=1}^{j}\frac{1}{x_i}\leq\sum\limits_{i=1}^{j}\frac{1}{a_i},j=1,2,\cdots n,\sum\limits_{i=1}^{n+1}\frac{1}{x_i}>\sum\limits_{i=1}^{n+1}a_i$

作 Abel 变换:

$$n+1=\sum_{i=1}^{n+1}\frac{x_i}{x_i}=x_{n+1}\sum_{i=1}^{n+1}\frac{1}{x_i}+\sum_{j=1}^{n}(\sum_{i=1}^{j}\frac{1}{x_i})(x_j-x_{j+1})$$

$$>x_{n+1}\sum_{i=1}^{n+1}\frac{1}{a_i}+\sum_{j=1}^{n}(\sum_{i=1}^{j}\frac{1}{a_i})(x_j-x_{j+1})=\sum_{i=1}^{n+1}\frac{x_i}{a_i}$$

$$\geq (n+1)\sqrt[n+1]{\frac{\prod x_i}{\prod a_i}}\Rightarrow\prod_{i=1}^{n+1}x_i<\prod_{i=1}^{n+1}a_i\Rightarrow\sum_{i=1}^{n+1}\frac{1}{x_i}<\sum_{i=1}^{n+1}\frac{1}{a_i}$$

Sophie Germain 素数 $p(2p+1$ 也为素数).

若 $p\equiv 3 \pmod 4$,则 $2p+1\mid 2^p-1=M_{(p)}$

证:设 $k=2p+1=8t-1,2^{\frac{k-1}{2}}\equiv 1 \pmod k\Leftrightarrow (\frac{2}{k})=1=(-1)^{\frac{k^2-1}{8}}$

4 Arithmetic Function

$d(n)$ 约数个数,$\sigma(n)$ 约数和,$\varphi(n)$ 缩系大小,均有积性

$n=\prod p_i^{\alpha_i}$ 则 $d(n)=\prod(\alpha_i+1),\sigma(n)=\prod\frac{p_i^{\alpha_i}-1}{p_i-1},\varphi(n)=n\prod(1-\frac{1}{p_i})$

$d(n)$ 为奇 $\Leftrightarrow n=k^2$;$\sigma(n)$ 为奇 $\Leftrightarrow n=k^2,2k^2$

$\varphi(n)=\varphi(2n)\Leftrightarrow n$ 为奇.

$\varphi(n)\mid n\Leftrightarrow n=1,2^\alpha 3^\beta(\alpha\geq 1,\beta\geq 0)$

n 的最小正缩系元素和为 $\frac{1}{2}n\varphi(n)$.配对

估界:

n 在 $[1,\sqrt{n}]$ 中约数至多 $\sqrt{n}$ 个,$\therefore d(n)\leq 2\sqrt{n}$

$\sigma(n)=\frac{1}{2}\sum_{d|n}d+\frac{n}{d}\geq\frac{1}{2}d(n)2\sqrt{n}=\sqrt{n}d(n)$

$\sigma(n)^2\underset{cauchy}{\leq}d(n)\sum_{d|n}d^2=d(n)\sum_{d|n}(\frac{n}{d})^2\leq n^2d(n)\sum\frac{1}{k^2}<2n^2d(n)$

$\varphi(p^a)=p^a-p^{a-1}>p^{\frac{a}{2}},\varphi(2^a)>\frac{2^{\frac{a}{2}}}{2}\Rightarrow\varphi(n)>\frac{\sqrt{n}}{2}$.$n$ 为奇时有 $\varphi(n)>\sqrt{n}$

$\varphi(n)\leq n-1,d(n)+\varphi(n)\leq n+1$ 当 n 为合数时,$\varphi(n)\leq n-\sqrt{n}$.

$$\sum_{d|n}\varphi(d)=\sum_{e_1=0}^{\alpha_1}\varphi(p_1^{e_1})\sum_{e_2=0}^{\alpha_2}\varphi(p_2^{e_2})\cdots=\prod_{i=1}^{r}\sum_{j=0}^{\alpha_i}\varphi(p_i^j)=\prod_{i=1}^{r}p_i^{\alpha_i}=n$$

$$\frac{\varphi(mn)}{mn}=\prod_{p|mn}(1-\frac{1}{p})=\frac{\prod_{p|m}(1-\frac{1}{p})\prod_{p|n}(1-\frac{1}{p})}{\prod_{p|(m,n)}(1-\frac{1}{p})}=\frac{\frac{\varphi(m)}{m}\frac{\varphi(n)}{n}}{\frac{\varphi((m,n))}{(m,n)}}$$

$\Rightarrow\varphi(mn)\varphi((m,n))=(m,n)\varphi(m)\varphi(n)$

$d(n)=\prod(\alpha+1)\geq 2^r,\varphi(n)\geq n\prod(1-\frac{1}{2})=\frac{n}{2^r}\Rightarrow d(n)\varphi(n)\geq n$

对 $\pi(n)=$ 小于 n 的素数个数估界:

设 $n=k^2l,k$ 有 $\sqrt{n}$ 种取法,l 为不同素数积,有 $2^{\pi(n)}$ 种取法.

$n\leq\sqrt{n}2^{\pi(n)}\Rightarrow\pi(n)\geq\frac{1}{2}\log_2 n$

Fermat-Euler Theorem: $(a,m)=1\Rightarrow a^{\varphi(m)}\equiv 1\pmod m$

证:取 m 一组缩系 $x_1\cdots x_{\varphi(m)}$, 则 ax_i 也构成一组缩系.$\prod ax_i\equiv\prod x_i$

推广:$a^m\equiv a^{m-\varphi(m)}\pmod m$

证:设 $m=m_1m_2:m_1$ 的素因子均被 a 整除,而 $(m_2,a)=1$, 则 $(m_1,m_2)=1$.

首先有 $a^{\varphi(m_2)} \equiv 1 \pmod{m_2} \Rightarrow a^{\varphi(m) \equiv 1 \pmod{m_2}} \Rightarrow a^m \equiv a^{m-\varphi(m) \pmod{m_2}}$.

于是只需 $a^m \equiv a^{m-\varphi(m)} \pmod{m_1} \Leftrightarrow m_1 \mid a^{m-\varphi(m)}$

$\Leftrightarrow V_p(m_1) \leq (m-\varphi(m))V_p(a)$

又 $V_p(m_1) = V_p(m) \leq 2^{V_p(m)-1} \leq p^{V_p(m)-1} \leq p^{V_p(m)-1}\varphi(\frac{m}{p^{V_p(m)}})$

$= p^{V_p(m)}\varphi(\frac{m}{p^{V_p(m)}}) - \varphi(p^{V_p(m)})\varphi(\frac{m}{p^{V_p(m)}}) = p^{V_p(m)}\varphi(\frac{m}{p^{V_p(m)}}) - \varphi(m)$

$\leq m - \varphi(m) \leq (m-\varphi(m))V_p(a)$ $\square$.

一些等式:

$(m,n) = 1 \Rightarrow m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \pmod{mn}$

$a\varphi(a^k b^{k+1}) = b\varphi(b^k a^{k+1})$

$n = 4k+3 \Rightarrow \forall d \mid n, d + \frac{n}{d} \equiv 0 \pmod 4 \Rightarrow 4 \mid \sigma(n)$

$(m,n) = 1, \{a_i\}_1^{\varphi(m)}, \{b_i\}_1^{\varphi(n)}$ 为缩系,则

$S = \{mb_i + na_j | 1 \leq j \leq \varphi(m), 1 \leq i \leq \varphi(n)\}$ 为 mod mn 缩系.

1.$(S_k, mn) = 1$;

2.$S_i \equiv S_j \pmod n \Rightarrow b_i \equiv b_j \pmod n \Rightarrow i = j$;

3.$|S| = \varphi(m)\varphi(n) = \varphi(mn)$;

5 Gauss Function

$[x] + [y] \leq [x+y]$;

$x + y \in Z \Rightarrow \{x\} + \{y\} = 0, 1$

$[x] + [y] + [x+y] \leq [2x] + [2y]$

$[\frac{m}{n}] \geq \frac{m-n+1}{n}$,带余除

$[\frac{x}{m}] = [\frac{[x]}{m}]$

$[a] + [a + \frac{1}{n}] + \cdots + [a + \frac{n-1}{n}] = [na], n \in N, a \in R$

$[x + \frac{1}{2}] = [2x] - [x] \Rightarrow \sum_{k=0}^{\infty} [\frac{n+2^k}{2^{k+1}}] = n$, 或用二进制证明.

$[\sqrt{n} + \sqrt{n+1}] = [\sqrt{4n+1}] = [\sqrt{4n+2}] = [\sqrt{4n+3}] = [\sqrt{n} + \sqrt{n+2}]$

$\sum_{i=1}^{\infty} [\frac{k}{p^i}] \leq \sum_{i=1}^{\infty} \frac{k}{p^i} \leq k \Rightarrow p^k \nmid k!$.

特别地,$p \geq 3 \Rightarrow V_p(k!) \leq \frac{k}{2}$, 可用于组合数/阶乘证明中.

$[\frac{x^2}{y}] + [\frac{y^2}{x}] = [\frac{x^2+y^2}{xy}] + xy \Rightarrow -1 < \frac{x^2}{y} + \frac{y^2}{x} - \frac{x^2+y^2}{xy} - xy < 2$

$$\Rightarrow \begin{cases} y^3-(1+x^2)y^2-2xy+x^3-x^2<0 \\ y^3-(1+x^2)y^2+xy+x^3-x^2>0 \end{cases} \quad \text{设 } y \geq x$$

① $\Leftrightarrow y(y(y-(1+x^2))-2x)+x^3-x^2<0.$

若 $y \geq x^2+2 \Rightarrow LHS \geq y(x-1)^2+x^3-x^2>0.$矛盾

② : 若 $y \leq x^2 \Rightarrow (LHS)' = 3y^2-(2+2x^2)y+x$ 令其等于 0

$\Rightarrow \max\{LHS\} = \max\{f(x), f(x^2)\} \leq 0.$矛盾

$\therefore y = x^2+1$

n 阶方格表,对列号为行号的倍数的格子数算两次:

$\sum_{i=1}^{n}[\frac{n}{i}]$ 为第 i 行所有(i 的倍数)列,$\sum_{i=1}^{n}d(i)$ 为第 i 列所有(i 的约数)行.两者相等.

另证由 $[\frac{n}{i}]-[\frac{n-1}{i}] = \begin{cases} 0, i \nmid n \\ 1, i \mid n \end{cases} \Rightarrow f(n) = f(n-1)+d(n) = \cdots$

类似结论:$\sum_{i=1}^{n} i[\frac{n}{i}] = \sum_{i=1}^{n}\sigma(i)$

$[ax] = x, x \in N$ 有 n 个解

$\Rightarrow x = [ax] = [a]x + [\{a\}x]$ 有 n 个解 $\Leftrightarrow [a] = 1$ 且 $\{a\}x < 1$ 有 n 个解

$\therefore \{a\} \in [\frac{1}{n}, \frac{1}{n-1}) \Rightarrow a \in [1+\frac{1}{n}, 1+\frac{1}{n-1})$

6 Diophantine Equation

Pythagoras: $a^2+b^2=c^2, (a,b,c)=1, 2 \mid b$ 的所有 N^+ 上的解为:

$a = u^2-v^2, b = 2uv, c = u^2+v^2, (u,v)=1, u \geq v, 2 \nmid u+v$

$a^2-mab+b^2=k, k \leq m$ 且非平方数,方程无解. 证:假设有最小解 $(a_0, b_0), a_0 \geq b_0$, 且 a_0+b_0,令 $a' = mb_0-a_0$,则 $a' \leq 0$ 或 $a' \geq a_0$

若 $a'=0$ 则 k 平方数;若 $a'<0 \Rightarrow a_o \geq mb_0+1 \Rightarrow a^2-ma_0b_0+b_0^2 > m \geq k$

若 $a' \geq a_0 \Rightarrow b_0^2-k = a_0a' \geq a_0^2 \geq b_0^2 \geq b_0^2-k$.每种情况均矛盾.

Pell: 标准 Pell 方程 $x^2-dy^2=1, d \in \mathbb{N}^+, d$ 非平方数必有无穷多解,(x_0, y_0) 称为基本解, 所有解为 $x_n+\sqrt{d}y_n = (x_0+\sqrt{d}y_0)^n$

$x^2-dy^2=C$ 若有解则必有无穷多解.设最小解 (x_1, y_1),则 $x_n+\sqrt{d}y_n = (x_1+\sqrt{d}y_1)(x_0+\sqrt{d}y_0)^{n-1}$ 为部分解

对上式中改变符号:$\begin{cases} x_n+\sqrt{d}y_n=(x_0+\sqrt{d}y_0)^n \\ x_n-\sqrt{d}y_n=(x_0-\sqrt{d}y_0)^n \end{cases}$ $\Rightarrow$ 两式加减即可求出通项

特征根为 $\lambda_{1,2}=x_0\pm\sqrt{d}y_0 \Rightarrow$ 特征方程 $\lambda^2-2x_0\lambda+1=0 \Rightarrow$

递推关系 $\begin{cases} x_{n+1}=2x_0x_n-x_{n-1} \\ y_{n+1}=2x_0y_n-y_{n-1} \end{cases}$

$x^2-dy^2=-1$, 设 $\sqrt{d}$ 的连分数周期为 l,则 l 为偶 $\Leftrightarrow$Pell 方程无解

特别地,素数 $p=4k+1$ 时,$x^2-py^2=-1$ 有解

$x^2-dy^2=-1$ 若有解则必有无穷多解.设最小解 (x_1,y_1),则所有解为 $x_n+\sqrt{d}y_n=(x_1+\sqrt{d}y_1)^{2n-1}$

Lemma:

$x^2-dy^2=4$ 的整数解 $x=u,y=v$ 是正整数解 $\Leftrightarrow \dfrac{u+\sqrt{d}v}{2}>1$

证:$\dfrac{u+\sqrt{d}v}{2}>1 \Rightarrow \dfrac{u-\sqrt{d}v}{2}\in(0,1)$, 两式相加得 $u>1$ 即 $u\geq 2$

又 $1>\dfrac{u-\sqrt{d}v}{2}\geq 1-\dfrac{\sqrt{d}v}{2}\Rightarrow v>0.$ $\square$

$x^2-dy^2=4$ 若有最小解 (x_1,y_1),则所有解 $\dfrac{x_n+\sqrt{d}y_n}{2}=(\dfrac{x_1+\sqrt{d}y_1}{2})^n$

证:设数列 x,y, $\dfrac{x_n+\sqrt{d}y_n}{2}=(\dfrac{x_1+\sqrt{d}y_1}{2})^n$, 假设有解 (a,b) 不在其中

不妨设 $(\dfrac{x_1+\sqrt{d}y_1}{2})^{n+1}>\dfrac{a+\sqrt{d}b}{2}>(\dfrac{x_1+\sqrt{d}y_1}{2})^n$,则

$\dfrac{x_1+\sqrt{d}y_1}{2}=\dfrac{x_n^2-dy_n^2}{4}\dfrac{x_1+\sqrt{d}y_1}{2}=(\dfrac{x_1+\sqrt{d}y_1}{2})^{n+1}\dfrac{x_n-\sqrt{d}y_n}{2}>\dfrac{a+\sqrt{d}b}{2}\dfrac{x_n-\sqrt{d}y_n}{2}$

$\overset{\text{def}}{=}\dfrac{s+\sqrt{d}t}{2}>(\dfrac{x_1+\sqrt{d}y_1}{2})^n\dfrac{x_n-\sqrt{d}y_n}{2}=1$

解方程 $x^2-5y^2=-4$,有恒等式 $(\dfrac{3x-5y}{2})^2-5(\dfrac{3y-x}{2})^2=x^2-5y^2$

$\therefore (x,y)\to(\dfrac{3x-5y}{2},\dfrac{3y-x}{2})$,

可证当 $y>1$ 时总有 $0<\dfrac{3x-5y}{2}<x, 0<\dfrac{3y-x}{2}<y$,完成递降

递推可求得其所有解为 $\dfrac{x_n+\sqrt{5}y_n}{2}=(\dfrac{x_1+\sqrt{5}y_1}{2})^{2n+1}$

事实上也有恒等式 $(ax-Dby)^2-D(ay-bx)^2=(a^2-Db^2)(x^2-Dy^2)=x^2-Dy^2$,但用它递降不总能做到边界

(Catalan)$a^x-b^y=1$ 只有 $3^2-2^3=1$ 一组解.

Techniques:

$x^4+y^4=z^2, x^4+y^2=z^4, x^{4m}+y^{4m}=z^{4m}$ 无非零解

解构造:$x^n+y^n=z^{n+1}$:$x=1+k^n, y=kx, z=x$

$x^n+y^n=z^{n-1}$:$x=(1+k^n)^{n-2}, y=kx, z=(1+k^n)x$

$x!y!=z!$:$z=x!, y=z-1$

$x^n+1=y^{n+1}, (x,n+1)=1$ 无解:

证:$x^n=(y-1)(y^n+\cdots+1)$.假设 $d=(y-1,y^n+\cdots+1)>1$

则 $\exists p\mid d, s.t. y\equiv 1 \pmod p, x\equiv 0 \pmod p$

$\Rightarrow \therefore y^n+\cdots+1\equiv n+1 \pmod p \Rightarrow p\mid n+1$ 矛盾

$\therefore d=1\Rightarrow y-1=a^n, y^n+\cdots+1=b^n\in(y^n,(y+1)^n)$ 矛盾

$3x^2-4xy+3y^2=35\Rightarrow(3x-2y)^2+5y^2=105\Rightarrow y^2\le 21$ 为避免负项配方估界

(CMO)解 $a^m+1\mid a^n+203, n<m$ 时估界,$n=m$ 时易.

$n>m$ 时,$\Rightarrow a^m+1\mid a^{n-m}-203$.若 $a^s<=203$ 估界.

$a^s>203$ 时 $\Rightarrow a^m+1\mid a^{s-m}+203=2^{n-2m}+203$ 类似前结构派生解

7 多项式

$f(x)$ 次数 $\le n$,且 $f(k)(k=0\cdots n)$ 均为整数,

则 $f(x)$ 为整值多项式,且整值多项式必可表为 $\sum_{i=0}^{n}a_iC_x^i$

证:设 $f(x)=\sum_{i=0}^{n}a_iC_x^i, a_i\in\mathbb{C}$,取 $x=0,1,\cdots$

$\mathbb{Z}\ni f(0)=a_0$.又 $\mathbb{Z}\ni f(1)=a_0+a_1\Rightarrow a_1\in\mathbb{Z}\cdots a_i\in\mathbb{Z}$

推论:$f(x)$ 次数 $\le n$,且对连续 $n+1$ 个整自变量取整值,则其为整值多项式(平移即可)

整系数多项式 $P(x): u-v\mid P(u)-P(v)\Rightarrow P(1)\equiv P(k+1)\equiv\cdots\equiv P(nk+1) \pmod k$

设有 $a_1,\cdots a_m$ 满足对 $\forall n,\exists i, a_i\mid F(n)$, 则 $\exists i,\forall n, a_i\mid F(n)$

反证:设 $\exists x_1, a_1\nmid F(x_1),\cdots\exists x_m, a_m\nmid F(x_m)\Leftrightarrow\exists d_i=p_i^{r_i}, d_i\mid a_i$ 且 $d_i\nmid F(x_i)$

$d_1,\cdots d_m$ 中同底数只保留低次幂,得 $d_1\cdots d_s$. 则 $\exists N,\forall i, N\equiv x_i \pmod{d_i}$

$\therefore \forall i, F(N) \equiv F(x_i) \not\equiv 0 \pmod{d_i} \Rightarrow \forall i, F(N) \not\equiv 0 \pmod{a_i}$

设素数 $p_1, \cdots p_k, \forall i, \exists x_i, p_i \mid P(x_i) \Rightarrow \exists x, \prod_{i=1}^{k} p_i \mid P(x)$
证:孙子.$x \equiv x_i \pmod{)} p_i \Rightarrow P(x) \equiv P(x_i) \equiv 0$

整系数多项式 $P(x) = a_n x^n + \cdots a_1 x \pm 1$ 值域的素因子无穷:假设有限-$p_1 \cdots p_k$
则 $P(i \prod p_t)$ 不含素因子 $\Rightarrow P(i \prod p_t) = \pm 1$ 但 n 次多项式至多给出 $2n$ 个 ± 1

(Gauss)本原多项式的乘积仍是本原多项式.
证:设 $f(x)g(x)$ 各项系数 c_k 有公因子 p,设 $i = \min\{t : p \nmid a_t\}, j = \min\{t : p \nmid b_t\}$
则由 c_{i+j} 的展开可得矛盾
进一步,记各项系数的 gcd(多项式的容度)为 $c(f)$,有 $c(fg) = c(f)c(g)$

(Eisenstein)$f(x) = \sum_{i=0}^{n} a_n x^n, \exists p \in P, p \nmid a_n, p^2 \nmid a_0, p \mid a_0 \cdots a_{n-1} \Rightarrow f$ 不可约
证:设 $f(x) = \sum_{i=0}^{s} b_i x^i \sum_{i=0}^{t} c_i x^i$, 不妨设 $p \mid b_0$, 显然有 $p \nmid c_0, p \nmid b_n$
设 $i = \min\{t : p \nmid b_t\}$,考虑 a_i 的展开可得矛盾
证 p 阶分圆多项式不可约:取 $x = y + 1$

8 表 n 为 ax+by

$(a, b) = 1 \Rightarrow \exists x, y \in \mathbb{N}^+, ax - by = 1$

$\forall n > ab - a - b$ 可表为 $ax + by, x, y \in \mathbb{N}$.
证:设 $n = a(x_0 + bt) + b(y_0 - at)$, 可取 t 使得 $0 \le y = y_0 - at \le a - 1$
则 $ax = n - (y_0 - at)b > ab - a - b - (a-1)b = -a \Rightarrow x > -1 \Rightarrow x \in \mathbb{N}$

$n = ab - a - b$ 不可表.反设结论不成立,则 $ab = (x+1)a + (y+1)b \Rightarrow b \mid x + 1 \Rightarrow x + 1 \ge b$ 矛盾

写 n 为 $ax + by, 0 \le x \le b - 1$,若 $n = ax + by$ 中 $y \ge 0$
则 $n' = (b - 1 - x)a + (-1 - y)b$ 中仍有 $0 \le b - 1 - x \le b - 1$,但 $-1 - y < 0$.
于是 n 可表 $\Rightarrow ab - a - b - n$ 不可表.$\therefore [0, ab - a - b]$ 中有 $\frac{(a-1)(b-1)}{2}$ 个不可表.

在矩形 $\begin{matrix} 0 \le x \le b \\ 0 \le y \le a \end{matrix}$ 中有 $(a+1)(b+1)$ 个整点.

其中使 $0 \le ax + by < ab$ 的整点有 $\dfrac{(a+1)(b+1)}{2} - 1$ 个

$n = ax+by, x, y \in \mathbb{N}^+$ 有至少两种表法 $\Leftrightarrow n$ 可表为 $ab+a+b+ax+by, x, y \in \mathbb{N}$

i) $ab + a + b + ax + by = a(1 + b + x) + b(1 + y) = b(1 + a + y) + a(1 + x)$

ii) $ax_1 + by_1 = ax_2 + by_2 \Rightarrow a \mid y_2 - y_1 \Rightarrow y_2 \ge a + 1$

$\therefore ax_2 + by_2 = ab + a + b + (y_2 - a - 1)b + (x_2 - 1)a$

9 Quadratic Residue

Def: $\exists x, x^2 \equiv d \pmod p, d < p, p$ 为奇素数.

T1: $\pmod p$ 的一个缩系中有 $\dfrac{p-1}{2}$ 个 $\pmod p$ 的二次剩余与二次非剩余, 且方程 $x^2 \equiv d \pmod p$ 若有解必有两解.

证:取绝对最小缩系 $S = \{-\dfrac{p-1}{2}, \cdots -1, 1, \cdots \dfrac{p-1}{2}\}$.

$(\dfrac{d}{p}) = 1 \Leftrightarrow d \equiv 1^2, \cdots, (\dfrac{p-1}{2})^2 \pmod p$. 于是有 $\dfrac{p-1}{2}$ 个二次剩余

T2(Euler):$(\dfrac{d}{p}) \equiv d^{\frac{p-1}{2}} \pmod p$. (由 Fermat 定理显然 $d^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$)

证:i)若 $(\dfrac{d}{p}) = 1$, 则 $\exists x_0^2 \equiv d \Rightarrow d^{\frac{p-1}{2}} \equiv x_0^{p-1} \equiv 1$

ii)对 $p \nmid d$,满足 $ax \equiv d \pmod p$ 的缩系中的 a, x 一一对应.

假设 $(\dfrac{d}{p}) = -1$, 则总有 $a \ne x$,则 $d^{\frac{p-1}{2}} \equiv \displaystyle\prod_{i=1}^{\frac{p-1}{2}} (a_i x_i) \equiv (p-1)! \equiv -1 \pmod p$

T3(Gauss 引理):设对 $1 \le j < \dfrac{p}{2}, t_j \equiv jd \pmod p$ 且 $0 < t_j < p$. 设在 $t_1 \ldots, t_{\frac{p-1}{2}}$ 中有 n 个 $> \dfrac{p}{2}$,则 $(\dfrac{d}{p}) = (-1)^n$

证:设 $> \dfrac{p}{2}$ 的为 $r_1, \ldots, r_n, < \dfrac{p}{2}$ 的为 $s_1, \ldots, s_k. k + n = \dfrac{p-1}{2}$.

由于 $\forall 1 \le j < i < \dfrac{p}{2}, t_j \pm t_i \equiv (j \pm i)d \not\equiv 0 \Rightarrow t_j \not\equiv \pm t_i \Rightarrow s_j \not\equiv -r_i \pmod p$

又 $1 \le p - r_i < \dfrac{p}{2}$, 于是 $s_1, \ldots, s_k, p - r_1, \ldots, p - r_n$ 为 $1, 2, \ldots, \dfrac{p-1}{2}$ 的排列.

$\Rightarrow (\dfrac{p-1}{2})! d^{\frac{p-1}{2}} \equiv \displaystyle\prod_{i=1}^{\frac{p-1}{2}} t_i \equiv \prod_{i=1}^{k} s_i \prod_{i=1}^{n} r_i \equiv (-1)^n \prod_{i=1}^{k} s_i \prod_{i=1}^{n} (p - r_i) \equiv (-1)^n (\frac{p-1}{2})!$

$\Rightarrow (\dfrac{d}{p}) = d^{\frac{p-1}{2}} \equiv (-1)^n$

特别地,$d = 2$ 时,对 $1 \le j < \dfrac{p}{4}, 1 \le t_j = 2j < \dfrac{p}{2}$;对 $\dfrac{p}{4} < j < \dfrac{p}{2}, \dfrac{p}{2} < t_j = 2j < p$,

$\therefore n = \frac{p-1}{2} - [\frac{p}{4}] \Rightarrow (\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$
T4: x 取遍缩系,则 x^2 取遍缩系中的一半值. **证**: 由 T1 即得.

$4k+1$ 型素数有无穷多: 假设有穷,考虑 $4(p_1p_2\cdots p_k)^2+1$,若为素数则矛盾,若为合数则必有 $4k+1$ 型因子.

x^4+1 的因子必位 $8k+1$ 型: 显然为 $4k+1$ 型,又 $1 = (\frac{(x^2+1)^2}{p}) = (\frac{(x^2+1)^2-(x^4+1)}{p}) = (\frac{2x^2}{p}) = (\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$
推论:$8k+1$ 型素数无穷多,否则考虑 $(2p_1\cdots p_k)^4+1$

10 Sum of Square

T1:奇素数 $p, x^2+y^2=p$ 有解 $\Leftrightarrow p=4k+1$.
i) 设有解 x_0, y_0, 显然 x_0, y_0, p 两两互素.设 $y_0y_0^{-1} \equiv 1 \pmod p$.
原方程 $\Rightarrow (x_0y_0^{-1})^2+1 \equiv p(y_0^{-1})^2 \equiv 0 \pmod p \Rightarrow (\frac{-1}{p}) = 1 \Rightarrow p = 4k+1$
ii) 若 $(\frac{-1}{p}) = 1$, 则 $\exists x \in [-\frac{p-1}{2}, \frac{p-1}{2}]$,使 $x^2+1 = mp$.也即 $\exists 1 \le m < p$, s.t. $x^2+y^2 = mp$.
设满足以上条件的最小的 m 为 m_0,则必须 $(x,y)=1$, 否则 $\frac{m}{(x,y)}$ 更小.假设 $m_0>1$,取绝对(值)最小剩余 $\begin{cases} u \equiv x \\ v \equiv y \end{cases} \pmod{m_0}, |u|,|v| \le \frac{m_0}{2}$
$\Rightarrow 0 < u^2+v^2 \le \frac{m_0^2}{2}, u^2+v^2 \equiv x^2+y^2 \pmod{m_0}$
设 $u^2+v^2 = m_1p$, 则 $(u^2+v^2)(x^2+y^2) = m_1m_0^2p = (ux+vy)^2+(uy-vx)^2$.
由 $ux+vy \equiv x^2+y^2 \equiv 0, uy-vx \equiv 0$,可知 $(\frac{ux+vy}{m_0})^2 + (\frac{uy-vx}{m_0})^2 = m_1p$, 其中 $m_1 = \frac{u^2+v^2}{p} \le \frac{m_0^2}{2p} < m_0$, 与最小性矛盾.于是 $m_0 = 1$. □

T2:$x^2+y^2 = n = d^2m$ 有解(m 无平方因子)$\Leftrightarrow$ m 不含 $4k+3$ 因子.
$\Leftarrow)$: d^2 显然可表,m 的所有因子可表,于是 n 可表.
$\Rightarrow)$: 设 $p = 4k+3 \mid n$.假设 $p \nmid x \Rightarrow p \nmid y$,则 $(xy^{-1})^2 \equiv -1 \pmod p$ 与 $p = 4k+3$ 矛盾.
$\therefore p \mid \Rightarrow p \mid y \Rightarrow p^2 \mid n \Rightarrow p \nmid m$. □

T3:$x^2+y^2 = n$ 有互素解 $\Leftrightarrow$ n 只含 $4k+1$ 型奇素因子且 $V_2(n) \le 1$
$\Rightarrow)$: 若 $4 \mid n$,则 $4 \mid x^2+y^2 \Rightarrow x, y$ 为偶数,矛盾;

若 $p=4k+3\mid n$, 由 T2 知 $p\mid x, p\mid y$, 矛盾.

$\Leftarrow)$: **引理 1:**方程 $x^2+y^2=p^\alpha, p=4k+1$ 有互素解:

对 α 归纳,设已有 $x_k^2+y_k^2=p^k,(x_k,y_k)=1$,又因为存在 $x_1^2+y_1^2=p,(x_1,y_1)=1$,可得 $(x_1x_k+y_1y_k)^2+(x_1y_k-y_1x_k)^2=(x_1x_k-y_1y_k)^2+(x_1y_k+y_1x_k)^2=p^{k+1}$

考虑上式中两对数的最大公约数 d_1,d_2, 若 $d_1,d_2>1$,则由 $d|p^{k+1}\Rightarrow p|d_1,d_2\Rightarrow p|2x_1x_k\Rightarrow p|x_1$或$p|x_k$, 矛盾

所以 d_1,d_2 有一个为 1. $\square$

引理 2:$(n_1,n_2)=1,\begin{cases}x_1^2+y_1^2=n_1,(x_1,y_1)=1\\x_2^2+y_2^2=n_2,(x_2,y_2)=1\end{cases}$ 则 $d=(x_1x_2+y_1y_2,x_1y_2-x_2y_1)=1$

假设 $d>1$, 取素因子 q,进行假设分析可知 $q\nmid x,y$.

于是由 $\begin{cases}x_1x_2\equiv -y_1y_2\\x_1y_2\equiv x_2y_1\end{cases}\pmod q$ 两式相乘后可得 $\begin{cases}x_1^2+y_1^2\equiv 0\\x_2^2+y_2^2\equiv 0\end{cases}\pmod q$,与 $(n_1,n_2)=1$ 矛盾. $\square$

由上述两引理立刻可得定理. $\square$

Lagrange 四平方定理:

引理:$x^2+y^2\equiv -1\pmod p, 0\le x,y\le\dfrac{p-1}{2}$ 有解,且 $1\le\dfrac{x^2+y^2+1}{p}<p$.

证:$\dfrac{p+1}{2}$个数$a^2(a=0,1\cdots,\dfrac{p-1}{2})$ 对 p 不同余;$\dfrac{p+1}{2}$个数 $-b^2-1(b=0,1,\cdots,\dfrac{p-1}{2})$ 对 p 不同余.

共 $p+1$ 个数.$\therefore \exists a_0,b_0,a_0^2\equiv -b_0^2-1$.且显然有 $a_0^2+b_0^2+1\le 2(\dfrac{p-1}{2})^2+1<p^2$. $\square$

事实上,将 -1 换成 a,可证 x^2+y^2 跑遍 $\pmod p$ 的完系.

下证定理:取 $m_0=\min\{m,mp=x_1^2+x_2^2+x_3^2+x_4^2\},m<p$.引理保证了这样的 m 的存在性. 由最小性可得 $(x_1,x_2,x_3,x_4)=1$.

假设 m_0 为偶,则