重点版

No.
Date. / /

C1

· $a|b,\ a|c \Leftrightarrow a|bx+cy$

· 判素数 $p \le \sqrt{n}$ 的所有 $p$ 均 $\nmid n$

· $a,b$ 互素 $\Leftrightarrow \exists x,y \in \mathbb{Z}$, 使得 $xa+yb=1$

· $[a,b]\cdot(a,b)=a\cdot b$

· 算术基本定理 $n>1,\ n\in\mathbb{N}$, 必有 $n=p_1p_2\cdots p_s$, 不计次序唯一, 求 [ ], ( )

· Euclid: $(a,b)=(a,b-qa)$

· 辗转相除法求 [ ], ( )

递推: $\begin{cases} s_{-1}=1,\ t_{-1}=0 \\ s_0=0,\ t_0=1 \end{cases} \Rightarrow \begin{cases} s_i=s_{i-2}-q_is_{i-1} \\ t_i=t_{i-2}-q_it_{i-1} \end{cases}$, $q_i=\left[\frac{r_{i-2}}{r_{i-1}}\right]$

· 习题 ☆

例. 证形如 $4k-1$ 的素数有无穷多个.

先证 ① 形 $4k-1$ 必有 $4k-1$ 因子, $(4k+1)(4k+1)$ 还是 $4k+1$, 必有 $4k-1$;

② 假设有限, $n=4p_1\cdots p_n-1$ 为合, $p_j:4k-1$

$p_j\in\{p_1,\cdots p_n\}$, $p_j|n$, $p_j|p_1\cdots p_n \Rightarrow p_j\nmid 1$ 矛盾!

C2

· 积性 $\forall m,n\in\mathbb{N}$, $(m,n)=1$ 时 $f(mn)=f(m)f(n)$

完全积性 $\forall m,n\in\mathbb{N}$, $f(mn)=f(m)f(n)$

· 求 $\varphi(n)$: 积性

① 素 $\varphi(p)=p-1$

② $\varphi(n)=n\prod_{p|n}(1-\frac{1}{p})$ $\quad n=p_1^{a_1}\cdots p_s^{a_s}$

(会求)

No.
Date. / /

C3

· 等价关系 自反、对称、传递

· $a \equiv b \bmod m_i$，当且仅当 $a \equiv b \bmod [m_1, m_2, \cdots, m_n]$

会用，会证。 $\Rightarrow m_i \mid a-b$

$\Leftarrow m_i \mid [m_1 m_2 \cdots m_n]$

· $(m_1, m_2) = 1$，$x, y$ 分别遍历，$m_2 x + m_1 y$ 遍历 $m_1 m_2$

证明：① $m_1 m_2$ 个

② 两两不同余 反证，$m_2 x + m_1 y \equiv (m_2 x' + m_1 y') \bmod m_1$

$m_2 x \equiv m_2 x' \bmod m_1 \Rightarrow x \equiv x'$

· 3定理

Euler $(a, m) = 1$，$a^{\varphi(m)} \equiv 1 \bmod m$

Fermat $p$ 素，$a^p \equiv a \bmod p$

Wilson $p$ 素，$(p-1)! \equiv -1 \bmod p$

例题. 分解为同余项 $1 \cdot (p-1)$，$\cdots (p-2)(p-(p-2))$

C4

· 解同余方程，化简系数，在 $m$ 个完全剩余系中考虑

· 一次方程 $ax \equiv b \bmod m$ 有解 $\Leftrightarrow (a, m) \mid b$，解为 $(a, m)$ 个 △

$\frac{a}{d} x \equiv \frac{b}{d} \bmod \frac{m}{d}$ $x_0 + \frac{m}{d} t$，$t = 0, 1, 2, \cdots d-1$

☆ · 中国剩余定理

$$x \equiv \left(\frac{M}{m_1} e_1 a_1 + \cdots + \frac{M}{m_k} e_k a_k\right) \bmod M$$

① 求 $M$、$M_i$ ② $e_i = M_i^{-1} \bmod a_i$ ③ 解出 $x$ $\Sigma M_i e_i a_i$

$m = m_1 \cdots m_k$，$m_i$ 两两互素 分开求解.

$$\begin{cases} f(x) \equiv a \bmod m_1 \\ f(x) \equiv a \bmod m_k \\ \cdots \end{cases}$$

No. 重点版 x-2
Date. / /

C5

·二次剩余 $\Leftrightarrow a^{\frac{p-1}{2}} \equiv 1 \bmod p$ 非则为 -1 p为素数!!!

-1是 $\Leftrightarrow p \equiv 1 \bmod 4$

负负得正

·会求 Legendre

$(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \bmod p$，完全积性

$(\frac{1}{p})=1$，$(\frac{-1}{p})=(-1)^{\frac{p-1}{2}}$，$(\frac{a^2}{p})=1$

$p>2$：$(\frac{2}{p})=(-1)^{\frac{p^2-1}{8}}$

[$(a,2p)=1$ 时，$(\frac{a}{p})=(-1)^T$，T …]

二次互反 $p,q>2$！$p\neq q$，

$$(\frac{q}{p})=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}(\frac{p}{q})$$

例. 求 $(\frac{137}{227})=(\frac{-90}{227})=(-\frac{1}{227})(\frac{2\cdot3^2\cdot5}{227})=(-1)\cdot(\frac{2}{227})\cdot(\frac{3^2}{227})\cdot(\frac{5}{227})$

$(\frac{2}{227})=(-1)^{\frac{227^2-1}{8}}=-1$，$(\frac{3^2}{227})=1$，$(\frac{5}{227})=(\frac{227}{5})=(\frac{2}{5})=-1$

非素数要分解为素数!!!

分解后均为1才有解 △

$p=p_1\cdots p_s$ $(\frac{-1}{p})=(-1)^{\frac{p-1}{2}}$，$(\frac{2}{p})=(-1)^{\frac{p^2-1}{8}}$

互反：p、q为奇数，$p>1$，$q>1$，$(p,q)=1$

$$(\frac{q}{p})(\frac{p}{q})=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

C6

·原根定义：$m\in N$，$(a,m)=1$，使$a^d\equiv1 \bmod m$ 成立的最小正整d 阶 $\delta_m(a)$，$\delta_m(a)=\varphi(m)$ 时为原根

· $\delta_m(a^k)=\frac{\delta_m(a)}{(k,\delta_m(a))}$ ☆

· $\delta_m(a)=s$，$\delta_m(b)=t$，$\delta_m(ab)=st \Leftrightarrow (s,t)=1$ △

· p 有模p的原根，$\varphi(p-1)$ 个

No.
Date. / /

5 同

·同态定义 $\begin{cases} h: S \to S' \\ h(a*b) = h(a) *' h(b) \\ h(\circ a) = \Delta' h(a) \\ h(k) = k' \end{cases}$

群：封、结、幺、逆

交换群：Abel

·子群 $a*b^{-1} \in H$

$h(e_A) = e_H$

$h(a^{-1}) = [h(a)]^{-1}$

· $\ker(h)$ 是 $\langle G, * \rangle$ 子群，h单同 $\Leftrightarrow \ker(h) = \{e\}$.

证明：$h(a*b^{-1}) = h(a) \cdot h(b^{-1}) = e_H \cdot e_H^{-1} = e_H \in \ker(h)$

$\Rightarrow h(a) = e_H = h(e)$，$a = e$，$\ker(h) = \{e\}$

$\Leftarrow \ker(h) = \{e\}$，$h(a) = h(b)$ 有

$h(a*b^{-1}) = h(a) \cdot h(b)^{-1} = e_H$，$a*b^{-1} \in \ker(h)$，$a*b^{-1} = e$

$a = b$. 单.

· 子群 $H \subseteq G$

(1) $aH = \{c \mid c \in G$ 且 $c^{-1} * a \in H\}$

(2) $aH = bH \Leftrightarrow b^{-1} * a \in H$

(3) $aH \cap bH = \phi \Leftrightarrow b^{-1} a \in H$

(4) $aH = H = Ha$

正规子群 $aH = Ha$

判断：$aHa^{-1} = H$

$aHa^{-1} \subseteq H$