Date

一、集合 A,B,C，证明：

1、对 $\forall\ x\in A-(B\cup C)$，有 $x\in A$，且 $x\notin B$，$x\notin C$，

$\Rightarrow x\in A-B$，$x\in A-C$

$\Rightarrow x\in (A-B)\cap(A-C)$

$\Rightarrow A-(B\cup C)\subset(A-B)\cap(A-C)$.

对 $\forall x\in(A-B)\cap(A-C)$，有 $x\in A-B$，$x\in A-C$

$\Rightarrow x\in A$，且 $x\notin B$，$x\notin C$，

$\Rightarrow x\in A-(B\cup C)$.

2、对 $\forall x\in A-(B\cap C)$ 有，$x\in A$，$x\notin B\cap C$.

$\Rightarrow x\in A-B$ 或 $x\in A-C$

$\Rightarrow x\in(A-B)\cup(A-C)$

同理，对 $\forall\ x\in(A-B)\cup(A-C)$，

有 $x\in A-B$ 或 $x\in A-C$.

$\Rightarrow x\in A$，$x\notin B\cap C$

$\Rightarrow x\in A-(B\cap C)$

$\Rightarrow A-(B\cap C)=(A-B)\cup(A-C)$.

二、$A\Delta K=B\Delta K$.

$\Rightarrow (A-K)\cup(K-A)=(B-K)\cup(K-B)$.

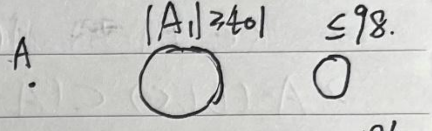
$$\left.\begin{aligned}&\Rightarrow A-K=B-K\\&\Rightarrow K-A=K-B.\ \Rightarrow K-K\cap A=K-K\cap B.\end{aligned}\right\}\Rightarrow A=B.$$

~~对 $\forall x\in A$，若 $x\in A-K$，$\Rightarrow x\in B-K$.~~

三，对任意代表A，将A认识的集合记为A_1，剩余的人记为A_2. 则 $|A_1| \geq 401$

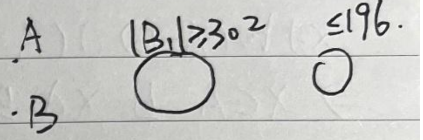
在集合A_1中任取B，将B认识的人与A_1的交记为B_1，

则 $|B_1| \geq 401-99=302$.



......

则 $|C_1| \geq \cancel{40}\,401-198=203$.



......

则 $|D_1| \geq 401-300=101$

......

则 $|E_1| \geq 401-400=1$.

四，$3141=1\cdot 1592+1549$.

$1592=1549+43$

$1549=36\times 43+1$.

$\Rightarrow (3141,1592)=1$.

$\Rightarrow \cancel{1=1549=36\times 43+1}$

$1=1549-36\times 43$

$=3141-1592-36(1592-1549)$.

$=3141-37\times 1592+36\times(3141-1592)$.

$=3141\times 37-73\times 1592$.

Date

五、$\begin{cases} 2x \equiv 1 \pmod 5 \\ 3x \equiv 2 \pmod 7 \\ 4x \equiv 1 \pmod{11}. \end{cases} \Rightarrow \begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 3 \pmod 7 \\ x \equiv 3 \pmod{11}. \end{cases}$

$\Rightarrow x \equiv 3 \bmod 385 \Rightarrow x = 3 + 385t.$

六、设 $m = p^{a} \cdot p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_n^{\alpha_n} \quad (p_i \neq p)$

$n = p^{b} \cdot q_1^{\beta_1} \cdot q_2^{\beta_2} \cdots q_m^{\beta_m} \quad (q_i \neq p).$

$\varphi(m) \cdot \varphi(n) = m \cdot (1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_n})(1 - \frac{1}{p})$

$n \cdot (1 - \frac{1}{q_1}) \cdots (1 - \frac{1}{q_n})(1 - \frac{1}{p})$

$= \varphi(mn) \cdot (1 - \frac{1}{p}).$

七、(1) $\varphi(n) = n \cdot (1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_n}).$

$\leq \frac{n}{3}$

(2) $2 \mid n$. $3 \mid n$. $\overset{(1)}{\Rightarrow} \varphi(n) \leq \frac{n}{3}$.

八、$a^3 \equiv -1 \pmod p$. $\Rightarrow a^6 \equiv 1 \pmod p$.

$a \not\equiv -1 \pmod p$.

设 r 为 a 模 p 的阶. $\Rightarrow r \mid 6$. $\Rightarrow r = 1, 2, 3, 6$.

$\Rightarrow r=1, r=2, r=3$ 不成立 $\Rightarrow r = 6$.

十、$C_m^n = \dfrac{m(m-1)\cdots(m-n+1)}{n \cdot (n-1) \cdots 1}$ $\qquad n^{-1} \equiv n^{p-2} \pmod p$

$\Rightarrow C_m^n = m \cdot (m-1) \cdots (m-n+1) \cdot n^{p-2} \cdots 1^{p-2} \pmod p.$

九, $\Rightarrow p \mid a^2+a+1$.　　$p \nmid (a-1)$. …※

由 $a^3 \equiv 1 \pmod p$. …※

$\Rightarrow (a+1)^6 \equiv 21a^2+21a+22$.

$\equiv 1 \pmod p$. 类似8题有, $r=1,2,3,6$

验证 $r=1,2,3$ 不成立.

① 若 $r=1$, 则 $a+1 \equiv 1 \pmod p$

$\Rightarrow a \equiv 0 \pmod p$ 与※矛盾.

② 若 $r=2$, 则 $(a+1)^2 \equiv 1 \pmod p$.

由 $p \mid a^2+a+1 \Rightarrow a \equiv 1 \pmod p$ 与※矛盾.

③ 若 $r=3$, 则 $(a+1)^3 \equiv 1 \pmod p$.

$$(a+1)^3 \equiv (a+1)(a^2+2a+1)$$
$$\equiv (a+1)a$$
$$\equiv a^2+a$$
$$\equiv -1 \pmod p$$ 矛盾

$\therefore \Rightarrow r=6$.