同余性质

Lemma: $N_1, \cdots, N_k \in \mathbb{Z}$, $N_1 \neq 0$ 且 $\cdots$ 且 $N_k \neq 0$, $a, b \in \mathbb{Z}$, 则有:

$$\begin{cases} a \equiv b \pmod{N_1} \\ \vdots \\ a \equiv b \pmod{N_k} \end{cases} \iff a \equiv b \pmod{\operatorname{lcm}(N_1, \cdots, N_k)}$$

Proof: $\because N_1, \cdots, N_k \in \mathbb{Z}$, $N_1 \neq 0, \cdots, N_k \neq 0$

$\therefore \operatorname{lcm}(N_1, \cdots, N_k) \in \mathbb{Z}_{\geqslant 1}$

$\because a, b \in \mathbb{Z}$ $\therefore a-b \in \mathbb{Z}$

$\therefore N_1, \cdots, N_k \in \mathbb{Z}$, $N_1, \cdots, N_k$ 全不为 0, $a-b \in \mathbb{Z}$

$$\therefore \begin{cases} a \equiv b \pmod{N_1} \\ \cdots\cdots \\ a \equiv b \pmod{N_k} \end{cases} \iff N_1 \mid a-b \text{ 且 } N_2 \mid a-b \text{ 且} \cdots \text{且 } N_k \mid a-b$$

$\iff$ 对 $\forall j = 1, \cdots, k$, $N_j \mid a-b$

$\iff \operatorname{lcm}(N_1, \cdots, N_k) \mid a-b$

$\iff a \equiv b \pmod{\operatorname{lcm}(N_1, \cdots, N_k)}$ $\square$

定理 (Fermat's little theorem) p 为任意的素数, a 为任意的整数, 则有:

$$a^p \equiv a \pmod{p}$$

Proof: $\because p$ 是任意的素数 $\therefore p \in \mathbb{Z}$ 且 $p \geqslant 2$ $\therefore p-1 \in \mathbb{Z}$ 且 $p-1 \geqslant 1$

~~1~~ 当 $p \mid a$ 时. $\exists \beta \in \mathbb{Z}$, s.t. $a = p\beta$ $\therefore a^p = (p\beta)^p = p^p \beta^p$

$\therefore a^p - a = p^p \beta^p - p\beta = p(p^{p-1}\beta^p - \beta)$

$\because a^p - a \in \mathbb{Z}$, $p \in \mathbb{Z}$ 且 $p \geqslant 2$, $p^{p-1}\beta^p - \beta \in \mathbb{Z}$ $\therefore p \mid a^p - a$ $\therefore a^p \equiv a \pmod{p}$

当 $p\nmid a$ 时，$\because$ p是素数，$a\in\mathbb{Z}$，$p\nmid a$ $\quad\therefore \gcd(p,a)=1$

$\because p-1\in\mathbb{Z}$ 且 $p-1\geqslant 1$ $\quad\therefore$ 设 $x_1,\cdots,x_{p-1}$ 是 $1,\cdots,p-1$ 的一个任意的排列.

$\therefore x_1\cdots x_{p-1}=1\times\cdots\times(p-1)=(p-1)!$

$\because a\in\mathbb{Z}$ $\quad\therefore ax_1,\cdots,ax_{p-1}\in\mathbb{Z}$

假设 $\exists\lambda,\mu\in\{1,\cdots,p-1\}$，$\lambda\neq\mu$，s.t. $ax_\lambda\equiv ax_\mu \pmod p$.

则有：$p\mid ax_\lambda-ax_\mu$ $\quad\therefore p\mid a(x_\lambda-x_\mu)$

$\because p,a,x_\lambda-x_\mu\in\mathbb{Z}$，$p\neq 0$，$\gcd(p,a)=1$，$p\mid a(x_\lambda-x_\mu)$

$\therefore p\mid x_\lambda-x_\mu$

$\because x_\lambda,x_\mu\in\{1,\cdots,p-1\}$ 且 $x_\lambda\neq x_\mu$ $\quad\therefore x_\lambda-x_\mu\in\{-(p-2),\cdots,-1,1,\cdots,p-2\}$

$\therefore |p|\leqslant|x_\lambda-x_\mu|\leqslant p-2$ $\quad\therefore p\leqslant p-2<p$ 矛盾.

$\therefore$ $ax_1,\cdots,ax_{p-1}$ 关于 mod p 两两不同余.

假设 $\exists\delta\in\{1,\cdots,p-1\}$，s.t. $ax_\delta\equiv 0 \pmod p$. 则有：$p\mid ax_\delta$.

$\because p,a,x_\delta\in\mathbb{Z}$，$p\neq 0$，$\gcd(p,a)=1$，$p\mid ax_\delta$ $\quad\therefore p\mid x_\delta$.

$\therefore |p|\leqslant|x_\delta|=x_\delta\leqslant p-1$ $\quad\therefore p\leqslant p-1<p$ 矛盾.

$\therefore ax_1,\cdots,ax_{p-1}$ 都不与 0 关于 mod p 同余.

$\therefore ax_1,\cdots,ax_{p-1}$ 除以 p 所得的余数是 $1,\cdots,p-1$ 的一个排列.

$\therefore (ax_1)\cdots(ax_{p-1})\equiv(p-1)! \pmod p$

$\therefore a^{p-1}\cdot(p-1)!\equiv(p-1)! \pmod p$

$\because \gcd(p,1)=1,\cdots,\gcd(p,p-1)=1$ $\quad\therefore \gcd(p,(p-1)!)=1$

$\because \dfrac{a^{p-1}(p-1)!}{(p-1)!} = a^{p-1} \in \mathbb{Z}$ $\quad \therefore (p-1)! \mid a^{p-1}(p-1)!$

$\because p \in \mathbb{Z},\ p \neq 0,\quad a^{p-1}(p-1)! \in \mathbb{Z},\ (p-1)! \in \mathbb{Z},\quad a^{p-1}(p-1)! \equiv (p-1)! \pmod p$

$(p-1)! \in \mathbb{Z},\ (p-1)! \neq 0,\ (p-1)! \mid a^{p-1}(p-1)!,\ (p-1)! \mid (p-1)!,\ \gcd((p-1)!, p) = 1$

$\therefore \dfrac{a^{p-1}(p-1)!}{(p-1)!} \equiv \dfrac{(p-1)!}{(p-1)!} \pmod p$ $\quad \therefore a^{p-1} \equiv 1 \pmod p$

$\therefore a^p \equiv a \pmod p$ $\quad \square$

~~Lemma~~ 定理 (Fermat's little theorem) p为任意的素数，a为任意的整数，$p \nmid a$，则有：$a^{p-1} \equiv 1 \pmod p$

Proof: $\because p$是任意的素数 $\therefore p \in \mathbb{Z}$ 且 $p \geq 2$ $\quad \therefore p-1 \in \mathbb{Z}$ 且 $p-1 \geq 1$

$\because p \nmid a$ $\quad \therefore$由上一定理的证明过程得：$a^{p-1} \equiv 1 \pmod p$ $\quad \square$