刘梓池 5190211213

定理 2.4.1.

~~若总 $\varphi(m)$ 个数: $ar+$~~ 设 $r_1 \sim r_{\varphi(m)}$ 为 mod m 的最小正简化剩余系.

于是当 $(a,m)=1 \Rightarrow ar_1, ar_2 \cdots ar_{\varphi(m)}$ 也为 mod m 的最小正简化剩余系.

$\Rightarrow (a-r_1)(a-r_2)\cdots(a-r_{\varphi(m)}) \equiv r_1 r_2 \cdots r_{\varphi(m)} \pmod m$

$\Rightarrow a^{\varphi(m)} \cdot [r_1 \cdots r_{\varphi(m)}] \equiv r_1 r_2 \cdots r_{\varphi(m)} \pmod m$

由 $(r_i, m)=1 \Rightarrow (r_1 r_2 \cdots r_{\varphi(m)}, 1)=1 \pmod m$

$\Rightarrow a^{\varphi(m)} \equiv 1 \pmod m$ 证毕

1. i) $2^6 \equiv 1 \pmod 7$ $20 \equiv 2 \pmod 6$ $2021^{0322} \equiv 21^{0322} \equiv 4^{10322} \pmod 6$

$4^1 \equiv 5 \pmod 6$ $4^{10322} \equiv 5^{0322} \equiv 2^{322} \equiv 5^{22} \equiv 4^2 \equiv 0 \pmod 6$

$\therefore 2^{2021^{0322}} \equiv 1 \pmod 7$

ii) $(2,17)=1$ $2^{16} \equiv 1 \pmod{17}$ 实际上 $2^8 \equiv 1 \pmod{17}$

$8 \overline{)2021^{0322}}$ $\quad 252629$

16

42

40

21

16

50

48

23

16

72

72

2

$\therefore 2021^{0322} \equiv 2 \pmod 8$

$2^{2021^{0322}} \equiv 2^2 \equiv 4 \pmod{17}$

iii) $2^8 \equiv 1 \pmod{17}$ $2^6 \equiv 1 \pmod 7$ 和 $2^3 \equiv 1 \pmod 7$ $\therefore 2^{24} \equiv 1 \pmod{7 \cdot 17}$

$2021^{0322} \equiv 18 \pmod{24}$ $2^8 = 256 \equiv 18 \pmod{119}$ $7 \times 17 = 119$

$2^{2021^{0322}} \equiv 2^{18} \equiv 4 \cdot (2^8)^2 \equiv 4 \times 18 \times 18 \equiv 1296 \equiv 106 \pmod{7 \cdot 17}$

2. i) ~~$x \equiv 0$~~ 当 $x=0$ 时 $f(0) \equiv 1 \pmod 7$

$x \neq 0$ 时 $(x,7)=1$ $x^6 \equiv 1 \pmod 7 \Rightarrow$ ~~$x^{322} \equiv x^4 \pmod 7$~~ $322 \equiv 4 \pmod 6$

$2021 \equiv 5 \pmod 6$ $2021^3 \equiv 5 \pmod 6$ $2021^{0322} \equiv 0 \pmod 6$

$\therefore f(x) \equiv |1 + x^5 + x^5 + x^4 + 1| \equiv 2 + x^4 + 2 \cdot x^5 \pmod 7$

计算得 $f(1) \equiv 5 \pmod 7$ $f(2) \equiv 5^{(\mathrm{mod}\,7)}$ $f(3) \equiv 2^{(\mathrm{mod}\,7)}$ $f(4) \equiv 3^{(\mathrm{mod}\,7)}$ $f(5) \equiv 3^{(\mathrm{mod}\,7)}$ $f(6) \equiv 1 \pmod 7$

$f(0) \equiv 1 \pmod 7$

ii) $x=0$ 时 $f(0)\equiv 1 \pmod 7$ $x\neq 0$ 时.

$x^7\equiv x \pmod 7$ $2^4=16\equiv 4 \pmod 6$

$2^{11}\equiv (2^4)^2\cdot 2\equiv 4^2\cdot 2\equiv (2^4)^2\cdot 2\equiv 4^2\cdot 2\equiv 2^4\cdot 2\equiv 4\cdot 2\equiv 8\equiv 2 \pmod 6$

$\therefore f(x)\equiv x^2+x^4+x+x^4+1\equiv 1+x+x^2+2\cdot x^4 \pmod 7$

计算得 $f(1)\equiv 5 \pmod 7$ $f(2)\equiv 4 \pmod 7$ $f(3)\equiv 0 \pmod 7$

$f(4)\equiv 1 \pmod 7$ $f(5)\equiv 0 \pmod 7$ $f(6)\equiv 3 \pmod 7$

$f(0)\equiv 1 \pmod 7$

3、证明:

必要性:n为素数时:

当 $n=2$ $(n-1)!\equiv -1 \pmod 2$ 成立.

$n\neq 2$ 时 对每个整数 $1\leq a\leq p-1$ $\exists$ 唯一 $1\leq a'\leq p-1$ 使 $a\cdot a'\equiv 1 \pmod p$

而 $a=a' \Leftrightarrow a^2\equiv 1 \pmod p \Rightarrow a=1$ 或 $p-1$

$\therefore (p-1)!\equiv 1\cdot(\prod_{a}^{\frac{n-1}{2}} a\cdot a')\equiv -1 \pmod p$

充分性:若 $(n-1)!\equiv -1 \pmod n$

若n为合数,不妨设 $n=a\cdot b$, 且 $1\leq a,b\leq n-1$ 若 $a\neq b$.

若 $a\neq b$ $n\mid a\cdot b \Rightarrow n\mid (n-1)! \Rightarrow (n-1)!\equiv 0 \pmod n$

而若 n不可以有2个不等的为因子乘积 $\Rightarrow n=p^2$ p为素数.

而若 $p=2$ $3!\equiv 2 \pmod 4$ 若 $p\neq 2$ $0<p,2p<n$

$\therefore p^2\mid p\cdot 2p \Rightarrow n\mid (n-1)! \Rightarrow (n-1)!\equiv 0 \pmod n$

矛盾,则n为素数.

证毕.