(16) 计算: ① 2^{32} (mod 47). ② 2^{47} (mod 47). ③ 2^{200} (mod 47).

① $32 = 2^5$

$n_0 = 0,\ a_0 = 1,\ b_0 = 4$

$n_1 = 0,\ a_1 = 1,\ b_1 = 16$

$n_2 = 0,\ a_2 = 1,\ b_2 = 21$

$n_3 = 0,\ a_3 = 1,\ b_3 = 18$

$n_4 = 0,\ a_4 = 1,\ b_4 = 42$

$n_5 = 1,\ a_5 = 42$

② $47 = 2^5 + 2^3 + 2^2 + 2^1 + 2^0$

$n_0 = 1,\ a_0 = 2,\ b_0 = 4$

$n_1 = 1,\ a_1 = 8,\ b_1 = 16$

$n_2 = 1,\ a_2 = 34,\ b_2 = 21$

$n_3 = 1,\ a_3 = 9,\ b_3 = 18$

$n_4 = 0,\ a_4 = 9,\ b_4 = 42$

$n_5 = 1,\ a_5 = 2$

③ $200 = 2^7 + 2^6 + 2^3$

$n_0 = 0,\ a_0 = 1,\ b_0 = 4$

$n_1 = 0,\ a_1 = 1,\ b_1 = 16$

$n_2 = 0,\ a_2 = 1,\ b_2 = 21$

$n_3 = 1,\ a_3 = 21,\ b_3 = 18$

$n_4 = 0,\ a_4 = 21,\ b_4 = 42$

$n_5 = 0,\ a_5 = 21,\ b_5 = 25$

$n_6 = 1,\ a_6 = 8,\ b_6 = 14$

$n_7 = 1,\ a_7 = 18$

(22) 运用 Wilson 定理, 求 $8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13 \pmod 7$.

$8 . 9 . 10 . 11 . 12 . 13 \pmod 7$

$\equiv 6! \bmod 7$

$\equiv -1$

(23) 计算 $2^{20\,040\,118} \pmod 7$.

$2^{20040118} \pmod 7$

$\equiv (2^{6\times 3340019} \cdot 2^4) \pmod 7$

$\equiv (2^{6\times 3340019} \pmod 7) \cdot (16 \bmod 7)) \bmod 7$

$\equiv ((2^6 \pmod 7))^{3340019} \cdot 2) \bmod 7 \quad (\because (2,7)=1)$

$\equiv (1^{3340019} \cdot 2) \bmod 7$

$\equiv 2$

(25) 证明: 如果 p 是奇素数, 那么

$$1^2 \cdot 3^2 \cdot \cdots \cdot (p-4)^2 \cdot (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod p.$$

左式 $\equiv (1 \cdot 3 \cdot \cdots \cdot (p-4) \cdot (p-2))^2 \pmod p$

$\equiv ((-1)\cdot(-3)\cdot \cdots \cdot (4-p)\cdot(2-p))^2 \pmod p$

$\equiv (((p-1)(p-3) \cdots 4 \cdot 2) \pmod p)^2 \pmod p$

$\equiv ((2^{\frac{p-1}{2}})(\frac{p-1}{2})!) \pmod p)^2 \pmod p$

$\equiv ((2^{p-1} \pmod p)) \cdot ((\frac{p-1}{2})! \pmod p))^2) \pmod p$

$\equiv ((\frac{p-1}{2})! \pmod p))^2 \pmod p \quad (\because (2,p)=1)$

$\equiv ((\frac{p-1}{2})! \pmod p \cdot (\frac{p-1}{2})! \pmod p) \pmod p$

$\equiv ((-1)^{\frac{p-1}{2}} \pmod p \cdot ((-1)\cdot(-2)\cdot \cdots \cdot (\frac{1-p}{2})) \pmod p) \cdot (\frac{p-1}{2})! \pmod p)) \pmod p$

$\equiv ((-1)^{\frac{p-1}{2}} \pmod p) \cdot ((p-1)(p-2)\cdot \cdots \cdot (\frac{p+1}{2})) \pmod p) (\frac{p-1}{2})! \pmod p)) \pmod p$

$\equiv ((-1)^{\frac{p-1}{2}} \pmod p) \cdot (p-1)! \pmod p) \pmod p$

$\equiv ((-1)^{\frac{p-1}{2}} \pmod p) \cdot (-1)) \pmod p$

$\equiv (-1)^{\frac{p+1}{2}} \pmod p$

(26) 证明: 如果 p 是素数, 并且 $p \equiv 3 \pmod 4$, 那么

$$\left(\frac{p-1}{2}\right)! \equiv \pm 1 \pmod p.$$

$$\left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)! \pmod p$$

$$\equiv \left((-1)^{\frac{p-1}{2}}\left((-1)\cdot(-2)\cdot\cdots\cdot\left(\frac{1-p}{2}\right)\right)\right) \pmod p$$

$$\equiv \left((-1)^{\frac{4k+3-1}{2}}\left((p-1)(p-2)\cdot\cdots\cdot\left(\frac{p+1}{2}\right)\right)\right) \pmod p \quad (\because p \equiv 3 \bmod 4)$$

$$\equiv \left(\frac{(p-1)!}{\left(\frac{p-1}{2}\right)!}\right) \pmod p$$

$$\therefore \left(\left(\frac{p-1}{2}\right)! \pmod p\right)^2 \equiv (p-1)! \pmod p \equiv 1 \bmod p$$

$$\therefore \left(\frac{p-1}{2}\right)! \equiv \pm 1 \pmod p$$

(28) 证明: 如果 p 是素数, 并且 $0 < k < p$, 那么 $(p-k)!\,(k-1)! \equiv (-1)^k \pmod p$.

$$(p-k)!(k-1)! \equiv \left((p-k)!\,(k-1)!\right) \pmod p$$

$$\equiv \left((-1)^{p-k}\left((-1)\cdot(-2)\cdot\cdots\cdot(k-p)\right)(k-1)!\right) \pmod p$$

$$\equiv \left((-1)^{p-k}\left((p-1)(p-2)\cdot\cdots\cdot k\right)(k-1)!\right) \pmod p$$

$$\equiv \left((-1)^{p-k}(p-1)!\right) \pmod p$$

$$\equiv \left(-(-1)^k(-1)\right) \pmod p \quad (\because p\text{是素数}\therefore\text{奇数})$$

$$\equiv (-1)^k \pmod p$$

(30) 证明: 如果 p 是素数, 那么 $\binom{2p}{p} \equiv 2 \pmod p$.

$$\binom{2p}{p} \equiv \frac{(2p)!}{p!\,p!} \pmod p$$

$$\equiv \frac{(2p)\cdot(2p-1)\cdot\cdots\cdot(p+1)}{p!} \pmod p$$

$$\equiv \left(2\cdot\frac{(2p-1)\cdot\cdots\cdot(p+1)}{(p-1)!}\right) \pmod p$$

$$\equiv \left(2\cdot\frac{(p-1)\cdot\cdots\cdot 1}{(p-1)!}\right) \pmod p$$

$$\equiv \left(2\cdot\frac{(p-1)!}{(p-1)!}\right) \pmod p$$

$$\equiv 2 \pmod p$$