信安数基第2次作业-汤尔宁-2022302181149

(2) 证明：$\because m-1\equiv-1 \pmod m$

$\therefore (m-1)^2\equiv(-1)^2\equiv 1 \pmod m$

则 $0^2, 1^2, \cdots (m-1)^2$ 一定不是模m的完全剩余系

(6)

$\because 2^3=8\equiv 1 \pmod 7$

$20030509=6676836\times 3+1$

$\therefore 2^{20030509}=(2^3)^{6676836}\cdot 2\equiv 2 \pmod 7$

故 $2^{20030509}$ 天是星期日

(8) $\because a^2\equiv b^2 \pmod n$

$\therefore n \mid a^2-b^2$

即 $n\mid(a-b)(a+b)$ 又 $n\nmid a-b, n\nmid a+b$

又 $n=pq$，则 $pq\mid(a-b)(a+b)$，又 p, q 均为素数

则 $p\mid(a-b)$，或 $p\mid(a+b)$ 故有 $(n,a-b)=(pq,a-b)>1$

同理有 $q\mid(a-b)$ 或 $q\mid(a+b)$ 以及 $(n,a+b)=(pq,a+b)>1$

(24) $3^{1000000} \pmod 7$

由欧拉定理：$3^{\varphi(7)}\equiv 3^6\equiv 1 \pmod 7$

故 $3^{1000000}=(3^6)^{166666}\cdot 3^4\equiv 81\equiv 4 \pmod 7$

(25) $137^{113} \pmod{227}$

$113=(1110001)_2$. $a=1$, $b=137$, $m=227$

$n_0=1$ $a_0=a\times b\equiv 137$, $b_1=b^2\equiv 155$, mod 227

$n_1=0$ $a_1=137$, $b_2=b_1^2\equiv 190$, mod 227

$n_2=0$ $a_2=137$, $b_3=b_2^2\equiv 7$ mod 227

$n_3=0$, $a_3=137$, $b_4=b_3^2\equiv 49$, mod 227

$n_4=1$, $a_4=130$, $b_5=131$, mod 227

$n_5=1$, $a_5=5$, $b_6=136$, mod 227

$n_6=1$, $a_6=226$.

故原式 $=226$ mod 227