张旭辉. 2022200x036. 计科3班.

第4题

解: 观察2幂模13的一个周期:

$2^1 \equiv 2 \pmod{13}$　　$2^{10} \equiv 10 \pmod{13}$

$2^2 \equiv 4 \pmod{13}$　　$2^{11} \equiv 7 \pmod{13}$

$2^3 \equiv 8 \pmod{13}$　　$2^{12} \equiv 1 \pmod{13}$

$2^4 \equiv 3 \pmod{13}$

$2^5 \equiv 6 \pmod{13}$

$2^6 \equiv 12 \pmod{13}$

$2^7 \equiv 11 \pmod{13}$

$2^8 \equiv 9 \pmod{13}$

$2^9 \equiv 5 \pmod{13}$

~~故~~ 由 故 $2^{70} \bmod 13 = 2^{10} \bmod 13$

$= 10$,

同理可得 $3^{70} \bmod 13 = 3^{10} \bmod 13 = 3$

$\because 2^{70} \equiv 10, 3^{70} \equiv 3 \bmod 13$

$\therefore 2^{70} + 3^{70} \equiv (13) \bmod 13$

故 13 整除 $2^{70}+3^{70}$.

5. 解:

① 假设 P 是一个素数, 计算 $(P-1)! \bmod P$

由费马小定理, 对 $\forall a$, 都有 $a^{P-1} \equiv 1 \pmod{P}$

a 不是 P 的倍数

现考虑 $(P-1)! = 1\cdot2\cdot3\cdots(P-1)$, 每个数都是 P 的倍数. 因此在模 P 下为 0, $(P-1)! \bmod P = 0$

当 P 是素数时, $(P-1)! \bmod P = 0$.

定理: 对任意素数 P, $(P-1)! \bmod P$ 等于 0

证明:

由费马小定理, 对 $\forall a \in \mathbb{Z}$, 有 $a^{P-1} \equiv 1 \pmod{P}$,

其中 a 不是 P 的倍数.

考虑 $(P-1)! = 1\cdot2\cdot3\cdots(P-1)$, 对每个数 $k\ (1 \le k \le P-1)$,

存在另一个数 $(P-k)$, 使得 $k\cdot(P-k) \equiv -k^2 \equiv 1 \pmod{P}$.

因为 P 是素数, 不存在 $k \in \mathbb{Z}$ 使得 $k \equiv -k \pmod{P}$, 故两数不等.

由此, $(P-1)!$ 中每个数 k 都有一个相对应的数 $(P-k)$, 它们乘积模 P 等于 1. 由于 $(P-1)!$ 中包含 P 的倍数, 所以它们对 P 取模后均为 0, 所以 $(P-1)! \bmod P$ 结果为 0.

故定理得证.