

108062135 呂佳恩

$$1. \quad \phi(1720) = \phi(5) \times \phi(8) \times \phi(43) \\ = 4 \times 4 \times 42 = 672.$$

$$2. (1) \quad n^j \equiv n^k \equiv 1 \pmod{m}$$

$$n^{sj} \equiv n^{tk} \equiv 1 \pmod{m} \quad \forall s, t$$

$$\left. \begin{aligned} n^{sj+tk} &\equiv 1 \pmod{m} \quad \forall s, t \\ n^{\gcd(j,k)} &\equiv 1 \pmod{m} \end{aligned} \right\} \gcd(j,k) = sj+tk$$

(2) Fermat little theorem

$$2^{p-1} \equiv 1 \pmod{p}$$

$$n \mid 2^n - 1 \Rightarrow p \mid 2^n - 1 \quad 2^n \equiv 1 \pmod{p}$$

$$2^{\gcd(p-1, n)} \equiv 1 \pmod{p}$$

(3) p is the smallest prime factor of n
 $\gcd(p-1, n) = 1$

$$2^{\gcd(p-1, n)} = 2 \quad (\nless) \quad 2^{\gcd(p-1, n)} \equiv 1 \pmod{p}$$

Therefore, $2^n \equiv 1 \pmod{n}$ is false

$$2^n \not\equiv 1 \pmod{n} \text{ for all } n \geq 1$$

3. (a) $2^{m+1} - 1$ is prime, the divisors are 2^i and $2^i(2^{m+1} - 1)$

$$\sum_{i=0}^m 2^i + \sum_{i=0}^m 2^i(2^{m+1} - 1) - n = (2^{m+1} - 1) + \frac{2^{m+1} - 1}{2} - 2^m(2^{m+1} - 1) \\ = \underline{2^m(2^{m+1} - 1)} = n.$$

(b) if n is a perfect number, $\sigma(n) = 2n$

Since Q is an odd integer,

$$\gcd(2^m, Q) = 1 \Rightarrow \sigma(2^m \cdot Q) = \sigma(2^m) \sigma(Q)$$

$$\sigma(2^m) = 1 + 2 + 2^2 + \dots + 2^m = \frac{2^{m+1} - 1}{1}$$

$$\sigma(n) = (2^{m+1} - 1) \sigma(Q) = 2n$$

(c) $2^{m+1} Q = (2^{m+1} - 1) \sigma(Q)$

$$(2^{m+1} - 1) \mid (2^{m+1} - 1) Q$$

$$(2^{m+1} - 1) \mid Q \text{ since } \gcd(2^{m+1} - 1, 2^{m+1}) = 1$$

(d) $2^{m+1} Q = (2^{m+1} - 1) \sigma(Q)$

$$(2^{m+1}) \cancel{(2^{m+1} - 1)} Q = \cancel{(2^{m+1} - 1)} \sigma(Q)$$

$$\sigma(Q) = 2^{m+1} Q \quad Q = (2^{m+1} - 1) Q$$

$$Q + Q = 2^{m+1} Q$$

$$Q + Q = Q + (2^{m+1} - 1) Q = 2^{m+1} Q \Rightarrow$$

$$\sigma(Q) = Q + Q$$

$$4. n = 2419 = 41 \times 59$$

$$\phi(2419) = 40 \times 58 = 2320$$

$$e = 211$$

$$211 \cdot 11 = 2321 \equiv 1 \pmod{2320}$$

$$d = 11$$

$$1040^{11} \equiv 70 \pmod{2419}$$

$$1182^{11} \equiv 101 \pmod{2419}$$

$$1075^{11} \equiv 114 \pmod{2419}$$

$$741^{11} \equiv 109 \pmod{2419}$$

$$2366^{11} \equiv 99 \pmod{2419}$$

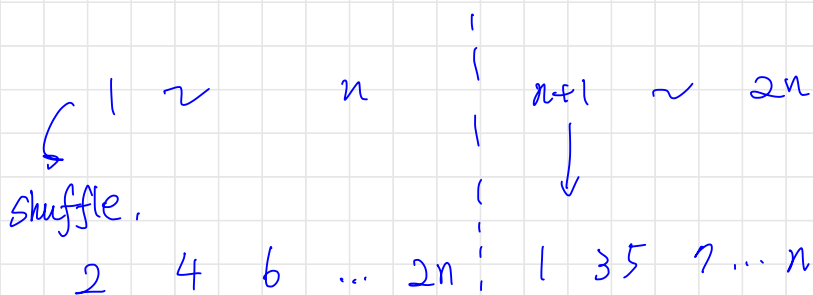
$$1495^{11} \equiv 116 \pmod{2419}$$

$$70, 101, 114, 109, 99, 116,$$

F e r m a t \(\in\) ASCII

5.1a

Consider a deck with $2n$ cards



Cards at position i will be moved to $2i \pmod{2n+1}$

We just have to find $2^r \equiv 1 \pmod{2n+1}$

then the card will return to original position

We already know $\gcd(2, 2n+1) = 1$

Euler's theorem $2^{\phi(2n+1)} \equiv 1 \pmod{2n+1}$

\Rightarrow After $\phi(2n+1)$ shuffles, the cards return to original position.

(b) We want to find smallest r in the previous question

since $x \leq r = \phi(2n+1)$

where $x \mid r$, we have

$$x \mid \phi(2n+1)$$