次数取模

Ⅰ. 模数为素数

一. 结论：$a^x \equiv a^{x\%(p-1)}(\%p)$

由费马小定理得：$a^{p-1} \equiv 1(\%p)$

二. 证明：$\therefore a^x \equiv \frac{a^x}{a^{p-1}} \equiv a^{x-(p-1)}(\%p)$

$\therefore a^x \equiv a^{x\%(p-1)}(\%p)$

Ⅱ. 模数为任意正整数

一. 结论：x> ϕ(m) 时 $a^x = a^{x\%\phi(m)+\phi(m)} \ (Mod\ m)$

将m因式分解：$m = p_1^{\alpha_1} \dots p_n^{\alpha_n}$

由CRT得：只要满足每一组$p_i^{\alpha_i}$即可

将a中所有p_i提出得：$a = p_i^k \cdot Q \ \ (\gcd(Q, p_i) = 1)$

$$\begin{cases} a^x = p_i^{k\cdot x} \cdot Q^x \\ a^{x\%\phi(m)+\phi(m)} = p^{k(x\%\phi(m)+\phi(m))} \cdot Q^{x\%\phi(m)+\phi(m)} \end{cases}$$

二. 证明：$\because k \geq 1, x \geq \phi(m) \geq \alpha_i$

$\therefore k \cdot x \geq \alpha_i, k(x\%\phi(m)+\phi(m)) \geq \alpha_i$

$\therefore p_i^{k\cdot x} \equiv p^{k(x\%\phi(m)+\phi(m))} \equiv 0 \ \ (Mod\ p_i^{\alpha_i})$

$\therefore a^x \equiv a^{x\%\phi(m)+\phi(m)} \ \ (Mod\ p_i^{\alpha_i})$