欧拉定理证明

- 对于正整数n，欧拉函数$\varphi(n)$表示：小于n的正整数中，与n互质的数的个数
  - ✓假设为$x_1, x_2, x_3, \cdots\cdots x_{\varphi(n)}$，它们跟$n$互质，(模$n$余数就是它们自己，因此均不同余)
- 若a,n互质 ⇨ 1) $ax_1, ax_2, ax_3, \cdots\cdots ax_{\varphi(n)}$模$n$均不同余;
  - ✓如果有ax_i和ax_j模n同余，则$n\,|(ax_i-ax_j)$ ⇨ $n\,|a(x_i-x_j)$ ⇨ $n\,|(x_i-x_j)$，推出一个矛盾；

    ⇨ 2)它们的模n余数与n互质
  - ✓a和x_i，跟n的最大公约数都是1。
- 因此$ax_1, ax_2, ax_3, \cdots\cdots ax_{\varphi(n)}$模n余数实际上就是$x_1, x_2, x_3, \cdots\cdots x_{\varphi(n)}$的一个乱序重排

  ⇨ $ax_1 \cdot ax_2 \cdot ax_3 \cdot \cdots\cdots \cdot ax_{\varphi(n)} \bmod n = x_1 \cdot x_2 \cdot x_3 \cdot \cdots\cdots \cdot x_{\varphi(n)} \bmod n$

  ⇨ $a^{\varphi(n)} \equiv 1 \pmod n$

RSA Decryption

- $\varphi(n) = (p-1)(q-1)$
- $\gcd(e, \varphi(n)) = 1$.
- d is an inverse of e modulo $\varphi(n)$, $de \equiv 1 \pmod{\varphi(n)}$

  ⇨ $de = k\varphi(n) + 1$，k为某个整数
- $C = M^e \bmod n$
- $C^d \bmod n = M^{de} \bmod n = M^{k\varphi(n)+1} \bmod n = ((M^{\varphi(n)})^k \bmod n) \cdot (M \bmod n)$
- 根据欧拉定理：$M^{\varphi(n)} \bmod n = 1$
  - ✓欧拉定理要求M和$n=pq$互质。因为实践中通常pq都是大质数、M是较小的数，这个要求是合理的。
- $C^d \bmod n = 1 \cdot M \bmod n = M$

- 思考题：如果M不和$n=pq$互质，$0<=M<n$，加解密等式成立吗？