欧拉定理（又称费马-欧拉定理）：已知a和n为正整数，并且a和p互素，则a^phi(n) ≡ 1(mod p)。

证明：

　　设集合Z = {X1, X2, X3, .... , Xphi(n)}，其中Xi (i = 1, 2, .. phi(n))表示第i个不大于n与n互质的数。

　　考虑集合S = {a\*X1(mod n), a\*X2(mod n), ... ,a\*Xphi(n) (mod n) }，则集合Z = S;

　　1) 因为a和n互质，Xi和n也互质，所以a\*Xi 也与n互质。所以对任意一个Xi，a\*Xi (mod n)一定是Z里面的元素;

　　2)对于任意Xi, Xj, 如果Xi != Xj，则a\*Xi(mod n) != a\*Xj(mod n);

　　所以S = Z；

　　那么 (a\*X1\*a\*X2\*...\*a\*Xphi(n))(mod n) ---------------------------------------------------- (1)

　　= (a\*X1(mod n)\* a\*X2(mod n)\* ... \*a\*Xphi(n) (mod n)) (mod n)

　　= (X1\* X2\* X3\* .... \* Xphi(n)) (mod n) ------------------------------------------------------ (2)

　　式(1)整理得 [a^phi(x) \* (X1\* X2\* X3\* .... \* Xphi(n))] (mod n)

　　与(2)式一同消去 (X1\* X2\* X3\* .... \* Xphi(n))，即得 a^phi(n) ≡ 1 (mod n)；