W5 10-2 Fermat and Euler

1、Fermat's theorem

费马小定理：若p为素数，则任给$x\in Z_p^*$，有

$$x^{p-1} = 1\ (mod\ p)$$

对于$x\in Z_p^*$，$x\cdot x^{p-2}=1$，即$x^{-1}=x^{(p-2)}$，这也是一个找到x的逆元的方法，但是效率比欧几里得更慢，大约是对数立方阶$O(\log^3 p)$

2、Application: generating random primes

假设我们需要生成一个大素数p（如p有1024 bits），一个简单的步骤可以生成大素数

1. 选择一个随机整数$p\in[2^{1024}, 2^{1025}-1]$
2. 计算$2^{(p-1)}==1$，如果等于则输出p，不等于则返回步骤1

算法得到不是素数的概率很低，对于1024 bits的p而言，不是素数的概率约为2^{-60}，因此并不是一个好的算法，因为可能生成伪素数

3、The structure of Z_p^*

欧拉定理：Z_p^* 为循环群，$\exists g\in(Z_p)$，有$\{1, g, g^2, g^3, ..., g^{(p-2)}\} = Z_p$，且g为$Z_p^*$生成元

注意到幂数只到p-2次幂，根据费马小定理，g的p-1次幂实际上是等于1，p次幂等于g，因此得到一个循环

需要注意是，定理中为存在$g\in Z_p^*$，而非任意g，即不是所有元素都是生成元

对于由生成元g生成的集合，称为g的生成群，记为

定义：记$ord_p(g)$为g的阶为的大小，即$ord_p(g)=||$，同时也是使得$g^a=1$成立的最小的a

拉格朗日定理：对于$\forall g\in Z_p^*$,$ord_p(g)$可以整除p-1

4、Euler's generalization of Fermat

定义：对于整数N而言，定义欧拉φ函数，即$\varphi(N)=|Z_N^*|$

欧拉ϕ函数也就是1~N-1中与N互素的数的个数，对于N是素数而言，$\varphi(N)=N-1$，对于RSA中需要用到的大整数$N=p\cdot q$而言，$\varphi(N)=(p-1)(q-1)$

欧拉定理：$\forall x\in Z_N^*$，$x^{\varphi(N)}=1$

欧拉定理是费马小定理的一个推广，同时也是RSA密码系统的基础