密码理论与技术

–计算机密码学理论与应用

第一部分：数学基础（2）

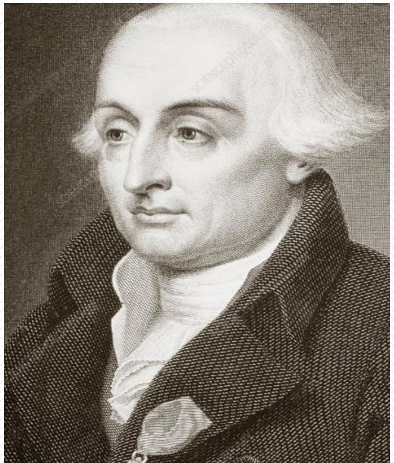
$$ed = 1 \bmod \varphi(N)$$

$$Y = M^e \bmod N$$

$$M = Yd \bmod N$$

Fermat公式、Euler公式及Lagrange公式

- 基本主题（*Stallings*教程8.1~8.3节）：
- (1) 特例：*Fermat*公式 $a^{p-1}=1 \bmod p$，p是素数。
- (2) Euler函数$\varphi(N)$及其重要的性质
- (3) Euler公式 $a^{\varphi(N)}=1 \bmod N$
- (4) 推广：有限群、交换群、子群、Lagrange定理



一个特例：Fermat公式

- (1)若p是素数且不整除a，则 $a^{p-1}=1 \bmod p$。
- (2)例：$2^4=1 \bmod 5$，$4^6=1 \bmod 7$，$6^3=1 \bmod 5$.
- (3)证明概要：
- 只要对$1\le a\le p-1$的a证明以上命题即可（为什么？）。
- 消去律：若$aA=bA \bmod N$ 且A和N互素，则$a=b \bmod N$（为什么？）
- 考虑集合$Z_p^*=\{1,2,\ldots,p-1\}$，在此不关心具体元素，简单将其记做a_1、…、a_{p-1}，a也是其中之一。固定a而考虑映射$a_i^*=aa_i \bmod p$，$i=1,\ldots,p-1$，由于p是一个素数，故这是一个一一对应(请验证！)，即当元素a_i跑遍集合Z_p^*时a_i^*也恰好跑遍集合Z_p^*，因此
- $$a_1^*\ldots a_{p-1}^*= a_1\ldots a_{p-1} \bmod p$$
- 但左面也等于$a^{p-1}a_1\ldots a_{p-1} \bmod p$，从而$a^{p-1}a_1\ldots a_{p-1}=a_1\ldots a_{p-1} \bmod p$，也就是(为什么？) $p \mid (a^{p-1}-1)\, a_1\ldots a_{p-1}$，这意味着$a^{p-1}=1 \bmod p$。

【练习】准确回答上述括号中的问题，以此得到完整的论证。

Euler函数与Euler公式(1)

- **Euler函数**$\varphi(N)$的定义：
- (1) $\phi(N)$的值等于在1和N-1之间与N互素的所有整数的个数。
- (2)记Z_N^* = {a: (a,N)=1, a=1,2,…,N-1}，于是
- $\varphi(N)$ = 集合Z_N^*的大小
- (3)例： $\varphi(12) = Z_{12}^*$的大小 $= |\{1,5,7,11\}| = 4$；
- $\varphi(25)$
- $= Z_{25}^*$的大小
- $= |\{1,2,3,4,6,7,8,9,11,12,13,14,16,17,18,19,21,22,23,24\}|$
- $= 20$

Euler函数与Euler公式(2)

- (4) $\phi(N)$的重要性质之一：
- 对任何素数p，$\varphi(p^m) = p^m - p^{m-1}$
- 特别地，$\varphi(p) = p - 1$。
- 【习题】根据$\phi(.)$的定义证明上述等式。
- (5) $\phi(N)$的重要性质之二：
- 对任何互素的N_1和N_2，$\varphi(N_1N_2) = \varphi(N_1)\varphi(N_2)$
- 续前面的例：$\varphi(12) = \varphi(3)\varphi(4) = 2\times2 = 4$
- $\phi(25) = 5^2 - 5 = 20$
- 更复杂的例：$\phi(300) = \phi(25)\phi(12) = 20\times4 = 80$
- 注：若N_1和N_2非互素，则上式不成立，例如 $4=\phi(12)\neq\phi(2)\phi(6)=2$。

Euler函数与Euler公式(3)

- (6)性质二的证明（注意应用上节课所学知识！）

- 对互素的整数N_1和N_2，令$N=N_1N_2$，考虑集合Z_N^*和$Z_{N_1}^* \times Z_{N_2}^* = \{(a_1,a_2): a_1$属于$N_1$, a_2属于$N_2\}$之间的映射：
- A：$Z_N^* \to Z_{N_1}^* \times Z_{N_2}^*$：$a \to (a_1, a_2)$，其中$a_1 = a \bmod N_1$，$a_2 = a \bmod N_2$；
- (i) A的像属于集合$Z_{N_1}^* \times Z_{N_2}^*$（为什么？）
- (ii) A是单射，即不同的a必有不同的像(a_1, a_2)（为什么？）
- (iii) A是满射，即$Z_{N_1}^* \times Z_{N_2}^*$中的每一个$(a_1, a_2)$，都存在相应的a属于N，使$A(a) = (a_1, a_2)$（为什么？）

【提示】借助中国剩余定理论证上属性质(ii)和(iii)。

根据以上性质，集合Z_N^*和$Z_{N_1}^* \times Z_{N_2}^*$一一对应，故两者元素数目相同：

$$\varphi(N) = \varphi(N_1)\varphi(N_2)$$

证毕。

注：注意条件“N_1和N_2互素”在以上论证中所起的作用：在哪个环节上，该条件是必须的？

Euler函数与Euler公式(4)

- (7)前述性质的推论：
- 对任何整数N，若已知N的素因子分解N=$p_1^{e_1}\ldots p_m^{e_m}$, $p_1,\ldots,p_m$是不同的素数，则
- $$\varphi(\mathrm{N}) = \varphi(p_1^{e_1})\ldots\varphi(p_m^{e_m})$$
- $$= (p_1^{e_1}-p_1^{e_1-1})\ldots(p_m^{e_m}-p_m^{e_m-1})$$

- (8)上述公式具有很强的理论价值，但并非计算φ(N)的实用型算法，原因是其前提“求整数的素因子分解问题”在计算上难解。
- 事实上，**不存在计算φ(N)的多项式复杂度算法！**

（这正是RSA公钥加密方案安全性的根本依据，参见本课程下一单元）

算法猫：“好失望...就说我无论怎样聪明，也无法找到计算φ(N)的实用算法？！”
RSA狗：“准确地说是N很大时的实用算法......不过幸亏如此，伙计！”

Euler函数与Euler公式(5)

- Euler公式
- 若整数a、N互素，则恒有$a^{\varphi(N)}$=1 mod N。
- 【习题】仿Fermat公式的证明，论证Euler公式。
- 提示：验证在集合Z_N^*上成立消去律。

【习题】Stallings教程第八章习题8.2、8.3、8.4、8.10~8.12。

- 注：某些习题与讲义上布置的练习类同，例如8.10~8.12，完成两者之一即可。
- 【习题】
- 1. 计算 φ(256)、φ(49)、φ(118)　　2. 用Fermat或Euler公式计算3^{201}mod11=？ 2^{1025}mod 15=？
- 提示：201 mod φ(11)=？ 1025 mod φ(15)=？

- 下节课内容
- Euler公式的推广：有限群、交换群、子群、Lagrange定理