1.4.4 费马小定理

Pierre de Fermat
(1601-1665)

- **费马小定理**(菲尔马小定理): 如果p为素数, a是一个不能被p整除的整数, 则$a^{p-1} \equiv 1\ (mod\ p)$. 再者, 对每个整数$a$, $a^p \equiv a\ (mod\ p)$.
- 该定理的证明自行验证.
  - 该定理在计算整数高次幂的模p余数时非常有用.
  - 可以用来验证是否为素数(必要不充分条件). 只能说明不满足上式, 那么一定不是素数.
- 例: 计算$7^{222}\ \boldsymbol{mod}\ 11$.
- 解:根据费马小定理, $7^{10} \equiv 1\ (mod\ 11)$, 所以对每个正整数$k$有$(7^{10})^k \equiv 1\ (mod\ 11)$. 因此, $7^{222} = 7^{22\times 10+2} = (7^{10})^{22} \times 7^2 \equiv (1)^{22} \times 49 \equiv 5\ (mod\ 11)$. 因此$7^{222}\ \mathbf{mod}\ 11 = 5$.
- 备注: 还可以用之前学的模指数运算来求解.

1.4.4 费马小定理

- 例: 计算29^{25} $\boldsymbol{mod}$ 11.
- 解:
  - $29 \equiv 7\ (mod\ 11)$
  - 那么, $29^{25} \equiv 7^{25} (mod\ 11)$
  - 根据费马小定理, $7^{10} \equiv 1\ (mod\ 11)$, 所以对每个正整数$k$有$(7^{10})^k \equiv 1\ (mod\ 11)$.
  - 因此, $7^{25} = 7^{2\times 10+5} = (7^{10})^2 \times 7^5 \equiv (1)^2 \times 7 \times (-4)^4 \equiv 7 \times 256 \equiv 7 \times 3 \equiv 10\ (mod\ 11)$. 因此$29^{25}$ $\boldsymbol{mod}$ 11 = 10.

1.4.5 伪素数

- 【定义】:令b是一个正整数，如果n是一个正合数，且$b^{n-1}\equiv 1 \pmod n$，则n称为以b为基数的**伪素数**.
- 给定一个正整数n，使得$2^{n-1}\equiv 1 \pmod n$. 如果存在这样的n，则n要么是素数(参见费马小定理)，要么是一个以2为基数的伪素数.
- 例:$2^{5-1}=16\equiv 1 \pmod 5$, 5为素数.
- 例:$2^{341-1}\equiv 1 \pmod{341}$, 且$341=11*31$, 341是以2为基数的伪素数.

1.4.5 卡米切尔数

Robert Carmichael
(1879-1967)

- 【定义】：一个正合数n，如果对于所有满足$\gcd(b,n) = 1$的正整数b都有同余式$b^{n-1} \equiv 1 \pmod{n}$成立，则称为**卡米切尔数**(carmichael number, 或称卡迈克尔数，卡米歇尔数).

- 判断一个数是否为卡米切尔数常会用到的性质:
- 假设$m_1, m_2, \ldots, m_n$是大于等于2的整数且两两互素. $m = m_1 m_2 \ldots m_n$ 如果$a \equiv b \pmod{m_i}$，其中$i=1,2,\ldots,n$, 则$a \equiv b \pmod{m}$
- 备注:证明略

1.4.5 卡米切尔数

- 例: 561是否是卡米切尔数?
- 解:
  - 首先注意561是合数, 因为$561 = 3 \cdot 11 \cdot 17$.
  - 其次, 如果$\gcd(b, 561) = 1$, 则$\gcd(b, 3) = \gcd(b, 11) = \gcd(b, 17) = 1$.
  - 利用费马小定理可得$b^2 \equiv 1 \pmod{3}$, $b^{10} \equiv 1 \pmod{11}$, $b^{16} \equiv 1 \pmod{17}$.
  - 从而, $b^{560} = (b^2)^{280} \equiv 1 \pmod{3}$, $b^{560} = (b^{10})^{56} \equiv 1 \pmod{11}$, $b^{560} = (b^{16})^{35} \equiv 1 \pmod{17}$.
  - 对于满足$\gcd(b, 561) = 1$的正整数b, 都有$b^{560} \equiv 1 \pmod{561}$. 所以, 561是卡米切尔数.

1.4.6 原根

- 【定义】：模素数p的一个**原根**是Z_p中的整数r，使得Z_p中的每个非零元素都是r的一个幂次.

- 例: 判断2是否是模7的原根, 3是否是模7的原根?
- 解:
  - 在Z_7中计算2的幂次时, 可得2^1 **mod** 7= 2, 2^2 **mod** 7= 4, 2^3 **mod** 7= 1, 2^4 **mod** 7= 2, 2^5 **mod** 7= 4, 2^6 **mod** 7= 1. 可以看到Z_7中的非零元素(1,2,...,6)不全在2的幂次结果中, 所以2不是模7的原根.
  - 在Z_7中计算3的幂次时, 可得3^1**mod** 7= 3, 3^2 **mod** 7= 2, 3^3 **mod** 7= 6, 3^4 **mod** 7= 4, 3^5 **mod** 7= 5, 3^6 **mod** 7= 1. 因为Z_7中的的非零元素都是3的幂次, 所以3是原根.

1.4.6 离散对数

- 【定义】：假设p是一个素数，r是一个模p的原根，而a是1和p-1之间的一个整数．如果$r^e \ \mathbf{mod}\ p = a$，且$1 \le e \le p-1$，我们说$e$是以$r$为底$a$模$p$的**离散对数**，并记作$log_r a = e$ (这里隐含理解为有素数p).
- 离散对数也称指标．一般来说寻找离散对数是一个非常困难的问题，这个问题的困难性也就成为了许多密码系统安全性的基础.

- 例: 分别找出以3为底3模7的离散对数, 以3为底5模7的离散对数
- 解:上面计算模7的3幂次时得到$3^1 = 3$, $3^5 = 5$都在Z_7中, 故以3为底3和5模7的离散对数分别是1和5. 我们写成$log_3 3 = 1$, $log_3 5 = 5$.

第1.4节 求解同余方程小结

- 线性同余方程$ax \equiv b(mod\ m)$, 通过a模m的逆$\bar{a}$来求解
- 同余方程组求解，中国剩余定理$\boldsymbol{x} = \boldsymbol{a_1 M_1 y_1} + \boldsymbol{a_2 M_2} y_2 + \cdots + \boldsymbol{a_n}\ \boldsymbol{M}_n y_n$, 或者反向替换
- $a^{p-1} \equiv 1\ (mod\ p)$, 费马小定理
- 以b为基数的伪素数，$b^{n-1} \equiv 1(mod\ n)$成立的合数n
- 卡米切尔数，合数n使得对所有满足$gcd(b,n) = 1$的正整数b，n是以b为基数的伪素数
- 素数p的原根,Z_p中的整数r使得每个不能被p整除的整数模p同余r的一个幂次
- 以r为底a模p的离散对数，满足$0 \le e \le p-1, \mathrm{r^e} \equiv \mathrm{a\ (mod\ p)}$的整数$e$