第五章欧拉φ函数与中国剩余定理

张志强

智能信息处理研究中心

http://rciip.hrbeu.edu.cn

欧拉公式

- 费马小定理：设p是素数，a是任意整数且$a \not\equiv 0 \pmod p$，则 $a^{p-1} \equiv 1 \pmod p$
  - 如果p是合数，上述结论是不正确的，例如 $5^5 \equiv 5 \pmod 6$， $2^8 \equiv 4 \pmod 9$
  - 但是也有这样的结果$7^4 \equiv 1 \pmod{10}$
  - 问题：是否存在有依赖于模m的指数，使得$a^{???} \equiv 1 \pmod m$？
  - 观察：如果gcd(a,m)>1，则上述问题是无解的，为什么？

观察一个实际例子

m	{a:1≤a≤m,gcd(a,m)=1}
1	{1}
2	{1}
3	{1，2}
4	{1，3}
5	{1，2，3，4}
6	{1，5}
7	{1，2，3，4，5，6}
8	{1，3，5，7}
9	{1，2，4，5，7，8}
10	{1，3，7，9}

欧拉公式

- 在0与m之间且与m互素的整数个数是个重要的量，我们赋予这个量一个名称

$$\Phi(m)=\#\{a:1\leqslant a\leqslant m,\gcd(a,m)=1\}$$

- 函数Φ称为欧拉函数，前面的表可以得到1≤a≤10时的Φ(m)值

m	1	2	3	4	5	6	7	8	9	10
Φ(m)	1	1	2	2	4	2	6	4	6	4

欧拉公式

- 观察1：如果p是素数，则有公式$\Phi(p)=p-1$
- 观察2：假设a=7，m=10，观察7的幂次模10余1。考察所有小于10的与10互素的数，它们是1，3，7，9，有

  $7*1 \equiv 7 \pmod{10}$，$7*3 \equiv 1 \pmod{10}$，
  $7*7 \equiv 9 \pmod{10}$，$7*9 \equiv 3 \pmod{10}$
- 仿照费马小定理的证明，我们将上面各式乘起来得

$$(7*1)(7*3)(7*7)(7*9) \equiv 1*3*7*9 \pmod{10}$$
$$7^4(1*3*7*9) \equiv 1*3*7*9 \pmod{10}$$
$$7^4 \equiv 1 \pmod{10}$$

欧拉公式

- 定理5.1(欧拉公式) 如果gcd(a,m)=1，则$a^{\Phi(m)} \equiv 1 \pmod{m}$
  - 证明：令$1 \leqslant b_1 < b_2 < \ldots < b_{\Phi(m)} < m$是0与m之间与m互素的$\Phi(m)$个整数
  - 第一步：证明如果gcd(a,m)=1，则数列$b_1a, b_2a, \ldots, b_{\Phi(m)}a \pmod{m}$与数列$b_1, b_2, \ldots, b_{\Phi(m)} \pmod{m}$相同，尽管可能次序不一样
  - 第二步：两个数列中数的乘积模m结果相等

欧拉Φ函数

- 我们看到欧拉公式非常简洁优美有力

$$a^{\Phi(m)} \equiv 1 (\mathrm{mod}\ m)$$

- 如果在实际当中能够有效应用上述欧拉公式，就需要计算Φ(m)的值
  - 列出所有1到m-1的所有整数来检查每个数是否与m互素
    - 当m很大时，这个过程是非常耗时的
  - 当m=p是素数时，显然有Φ(m)=p-1
  - 当m=p^k是素数幂次时， Φ(p^k)=？

Φ(p^k)的计算

- 方法一(枚举法)：计数1到p^k之间的与p^k互素的整数个数
  - 没有实际意义
- 方法二(删除法)：
  - 在1到p^k之间将那些与p^k不互素的整数丢弃
  - 那么数a什么时候与p^k不互素呢？其中$1 \leqslant a \leqslant p^k$

$\Phi(p^k)$的计算

a与p^k不互素，即$\gcd(a, p^k)>1$

p^k的因数仅为p的幂次，即$p^0, p^1, p^2, \ldots, p^k$

因此如果a被p整除时，a一定与p^k不互素，则有

$$\Phi(p^k) = p^k - \#\{a: 1 \leqslant a \leqslant p^k, p \mid a\}$$

- 1～p^k之间有多少个被p整除的数？

$$P, 2p, 3p, \ldots, (p^{k-1}-2)p, (p^{k-1}-1)p, p^k$$

- 因此最后得

$$\Phi(p^k) = p^k - p^{k-1}$$

$\Phi(p^k)$的计算

- 当m是素数的幂次时，我们已知如何计算$\Phi(m)$，那么当m是两个素数的幂次乘积时$m=p^j*q^k$，应该如何计算$\Phi(m)$？

p^j	q^k	$p^j q^k$	$\Phi(p^j)$	$\Phi(q^k)$	$\Phi(p^j q^k)$
2	3	6	1	2	2
4	5	20	2	4	8
3	7	21	2	6	12
8	9	72	4	6	24
9	25	225	6	20	120

$\Phi(p^k)$的计算

- 前表揭示了：$\Phi(p^j q^k)=\Phi(p^j)*\Phi(q^k)$
- 进一步尝试：$\Phi(14)=6$, $\Phi(15)=8$, $\Phi(14*15)=48$
- 猜想：如果gcd(m,n)=1，则有 $\Phi(m*n)=\Phi(m)*\Phi(n)$
  - 对于任意的m，可以对其进行素数积分解，然后再用上述乘法公式来计算$\Phi(m)$

一则练习

$$\Phi(1512)$$
$$=\Phi(2^3*3^3*7)$$
$$=\Phi(2^3)*\Phi(3^3)*\Phi(7)$$
$$=(2^3-2^2)*(3^3-3^2)*(7-1)$$
$$=4*18*6$$
$$=432$$

Φ函数公式

- 定理：
  - (a)如果p是素数且k≥1，则Φ(p^k)= p^k - p^{k-1}
  - (b)如果gcd(m,n)=1，则有Φ(m*n)=Φ(m)*Φ(n)

Φ函数公式

- 证明：(a)的证明略；(b)证明的基本思想，首先通过构造一个包含Φ(mn)个元素的集合和一个包含Φ(m) Φ(n)个元素的集合；其次，证明这两个集合的元素个数相同。
- 第一步：构造两个集合
  - 第一个集合
    {a:1≤a ≤mn, gcd(a,mn)=1}
  - 第二个集合
    {(b,c): 1≤b≤m, gcd(b,m)=1, 1≤c≤n, gcd(c,n)=1}

Φ函数公式

- 第二步：构建两个集合元素之间的一一映射关系

$$\left\{a: \begin{array}{c} 1 \le a \le mn \\ \gcd(a, mn) = 1 \end{array}\right\} \to \left\{(b,c): \begin{array}{c} 1 \le b \le m, \gcd(b,m) = 1 \\ 1 \le c \le m, \gcd(c,n) = 1 \end{array}\right\}$$

$$a \mod mn \quad |\to \quad (a \mod m, a \mod n)$$

  - 例子：当m=4，n=5时
  - 第一个集合为：{1,3,7,9,11,13,17,19}
  - 第二个集合为：
    {(1,1),(1,2),(1,3),(1,4),(3,1),(3,2),(3,3),(3,4)}

Φ函数公式

- 例子的映射结果

$$1 |\to (1,1)$$
$$3 |\to (3,3)$$
$$7 |\to (3,2)$$
$$9 |\to (1,4)$$
$$11 |\to (3,1)$$
$$13 |\to (1,3)$$
$$17 |\to (1,2)$$
$$19 |\to (3,4)$$

Φ函数公式

- 证明一一映射的方法
  - (1)第一个集合的不同元素对应第二个集合的不同序对；
  - (2)第二个集合中的每个序对都对应于第一个集合中的某个数
- (1)的证明：
  - 取第一个集合中的两个数a1和a2，假设它们在第二个集合中有相同的象，则意味着下列两式 a1≡a2(mod m)与a1≡a2(mod n)成立，因此a1-a2被m与n整除，然而m与n互素，因此a1-a2一定被mn整除，换句话说，a1 ≡a2(mod mn)，这表明a1与a2是第一个集合的相同元素，(1)得证#

Φ函数公式

- (2)的证明：
  - 即需要证明对于b与c的任何已知值，至少可以得一个整数a满足a≡b(mod m)与a≡c(mod n)
- 如果这个同余式组有解，那么上述的证明就完成了。

中国剩余定理

- 定理(中国剩余定理)：设m与n是整数，gcd(m,n)=1，b与c是任意整数，则同余式组x ≡b(mod m)与x ≡c(mod n)，恰有一个解0≤x≤mn
- 证明：由x ≡b(mod m)可知，其解由形如x=my+b的所有数组成，将其代入到第二个同余式中得my ≡c-b(mod n)，已知gcd(m,n)=1，由前面的定理可知恰有一个解y1，0≤y1<n，则x1=my1+b给出了原来同余式的解，这是唯一解0≤x1<mn，因为在0与n之间有唯一解y1，且用m乘y1得x1，定理得证#

中国剩余定理

- 韩信是汉高祖刘邦手下的大将，他英勇善战，智谋超群，为汉朝的建立了卓绝的功劳。据说韩信的数学水平也非常高超，他在点兵的时候，为了保住军事机密，不让敌人知道自己部队的实力，先令士兵从1至3报数，然后记下最后一个士兵所报之数；再令士兵从1至5报数，也记下最后一个士兵所报之数；最后令士兵从1至7报数，又记下最后一个士兵所报之数；这样，他很快就算出了自己部队士兵的总人数，而敌人则始终无法弄清他的部队究竟有多少名士兵。

中国剩余定理

- 历史插曲
  - 中国剩余定理的第一个记载出现在3世纪末和4世纪初的中国数学著作中

“今有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何？”

——《孙子算经》(第3卷问题26)

作业

- 请用删除法证明下述命题成立
  - 当p和q是素数时，有$\Phi(p^j q^k)=\Phi(p^j)*\Phi(q^k)$