第七章 欧拉φ函数与因数和

张志强
智能信息处理研究中心
http://rciip.hrbeu.edu.cn

梅森素数

- 我们称形如2^p-1的素数为梅森素数。前几个梅森素数是
- $2^2-1=3$，$2^3-1=7$，$2^5-1=31$，$2^7-1=127$，$2^{13}-1=8191$….
- 是否所有形如2^p-1数都是素数？
  - No
  - $2^{11}-1=2047=23*89$
  - $2^{29}-1=536870911=233*1103*2089$

梅森(Marin Mersenne,1588-1648)

- 神父梅森在1644年断言，当p=2,3,5,7,13,17,19,31,67,127,257时，

  2^p-1是素数
- 上述断言并不正确
  - p=67，p=257时，$2^{67}-1$和$2^{257}-1$均是合数
  - 并且丢掉了p=61,89,107
- 1876年卢卡斯才证明$2^{127}-1$是素数
- 20世纪50年代才被突破
  - 可以使用Woltman的部分专用软件
  - www.mersenne.org/prime.htm

梅森素数

- 你想在15分钟内出名吗？
  - 寻找已知最大的梅森素数是一个不错的途径！
- 更有意义问题
  - 存在无穷多个梅森素数吗？

完全数

- 古希腊人注意到数6具有惊人的性质，如果取6的真因数（即除6本身之外的因数），将它们加起来就回到数6

$$6=1+2+3$$

- 是否还存在这类的数？

n	n的真因数之和	
6	1+2+3=6	和正好相等（完全数）
10	1+2+5=8	和太小
12	1+2+3+4+6=16	和太大
15	1+3+5=9	和太小
20	1+2+4+5+10=22	和太大
28	1+2+4+7+14=28	和正好相等（完全数）
45	1+3+5+9+15=33	和太小

σ 函数

- σ(n)=n的所有因数之和（包括1与n）
  - σ(6)=1+2+3+6=12
  - σ(8) =1+2+4+8=15
  - σ(18)=1+2+3+6+9+18=39
- 如果p是素数
  - σ(p)=1+p
- 如果是素数的幂p^k
  - $\sigma(p^k) =1+p+p^2+p^3+\ldots+p^k= \frac{p^{k+1}-1}{p-1}$

σ 函数短表

σ(1)=1		σ(3)=4			σ(6)=12		σ(8)=15
σ(9)=13		σ(11)=12	σ(12)=28	σ(13)=14	σ(14)=24	σ(15)=24	σ(16)=31
σ(17)=18	σ(18)=39	σ(19)=20	σ(20)=42	σ(21)=32	σ(22)=36	σ(23)=24	σ(24)=60
σ(25)=31	σ(26)=42	σ(27)=40		σ(29)=30	σ(30)=72	σ(31)=32	σ(32)=63
σ(33)=48	σ(34)=54	σ(35)=48	σ(36)=91	σ(37)=38	σ(38)=60	σ(39)=56	σ(40)=90
σ(41)=42	σ(42)=96	σ(43)=44	σ(44)=84	σ(45)=78	σ(46)=72	σ(47)=48	σ(48)=124
σ(49)=57	σ(50)= 93	σ(51)=72	σ(52)=98	σ(53)=54	σ(54)=120	σ(55)=72	σ(56)=120
σ(57)=80	σ(58)=90	σ(59)=60	σ(60)=168	σ(61)=62	σ(62)=96	σ(63)=104	σ(64)=127

σ 函数公式

- 定理(σ 函数公式)：
  - 如果p是素数，k≥1，则

    $\sigma(p^k)=1+p+p^2+p^3+\ldots+p^k=\frac{p^{k+1}-1}{p-1}$

  - 如果gcd(m,n)=1，则

    $\sigma(mn)=\sigma(m)\,\sigma(n)$

- 试求 σ(16072)=?

  $\sigma(16072)=\sigma(2^3*7^2*41)$

  $=\sigma(2^3)*\sigma(7^2)*\sigma(41)$

  $=(1+2+2^2+2^3)(1+7+7^2)*(1+41)$

  $=15*57*42=35910$

σ函数公式

- 证明：

  —你们自己来证明，作业

欧拉完全数定理

- 定理(欧拉完全数定理)：如果n是偶完全数，则n是$n=2^{p-1}(2^p-1)$形式，其中2^p-1是梅森素数。(证明略)

- 问题：是否存在奇完全数？
  - 截止目前为止，没人找到奇完全数
  - 最好的结果，不存在小于10^{300}的奇完全数
  - 还没有证明奇完全数不存在

欧拉 ϕ 函数

- 先做个实验：将欧拉 ϕ 函数应用到每个因数，然后再把这些欧拉函数值相加
  - 例1，n=15，其因数为1,3,5,15，$\phi(1)=1$，$\phi(3)=2$，$\phi(5)=4$，$\phi(15)=8$，则有 $\phi(1)+\phi(3)+\phi(5)+\phi(15)=15$
  - 例2，n=315，其因数为1,3,5,7,9,15,21,35,45,63,105,315，则有 $\phi(1)+\phi(3)+\phi(7)+\phi(9)\ \phi(15)+\phi(21)+\phi(35)+\phi(45)+\phi(63)+\phi(105)+\phi(315)=315$

欧拉 ϕ 函数

- 猜想 设 $d_1,d_2,\ldots,d_r$ 是整除n的数，其中包括1和n，则 $\phi(d_1)+\phi(d_2)+\ldots+\phi(d_r)=n$
  - 当n=p时，p的因数有1和p，则 $\phi(1)+\phi(p)=1+p-1=p$，成立
  - 当 $n=p^k$ 时，p^k 的因数有 $1,p,\ldots,p^{k-1},p^k$，则 $\phi(1)+\phi(p)+\ldots+\phi(p^{k-1})+\phi(p^k)=1+(p-1)+(p^2-p)+\ldots+(p^k-p^{k-1})=p^k$
  - 当n不是素数幂次时，最简单情况当n=pq是两个素数的乘积

欧拉ϕ函数

– n的因数为1,p,q,pq，则有ϕ(1)+ϕ(p)+ϕ(q)+ϕ(pq)，之前我们证明过当m,n互素时有ϕ(mn)=ϕ(m)ϕ(n)，因此ϕ(1)+ϕ(p)+ϕ(q)+ϕ(pq)=pq

- 定义函数F(n)：
  – $F(n)=\phi(d_1)+\phi(d_2)+\ldots+\phi(d_r)$
  – 其中$d_1,d_2,\ldots,d_r$是n的因数
- 我们的目标是证明F(n)=n

欧拉ϕ函数

- 断言1：如果gcd(m,n)=1，则F(mn)=F(m)F(n)
- 证明：设$d_1,d_2,\ldots,d_r$是n的因数，$e_1,e_2,\ldots,e_s$是m的因数，由于m与n互素，则mn的因数可全部枚举出如下所示：

$d_1e_1,d_1e_2,\ldots,d_1e_s,d_2e_1,d_2e_2,\ldots,d_2e_s,\ldots,d_re_1,d_re_2,\ldots,d_re_s$，进而由于每个$d_i$与$e_j$均互素，所以由$\phi(d_ie_j)=\phi(d_i)\,\phi(e_j)$，可得

$$\begin{aligned}F(mn)&=\phi(d_1e_1)+\phi(d_1e_s)+\phi(d_2e_1)+\ldots+\phi(d_2e_s)+\ldots+\\&\quad\phi(d_re_1)+\ldots+\phi(d_re_s)\\&=\phi(d_1)\,\phi(e_1)+\ldots+\phi(d_r)\,\phi(e_s)\\&=(\phi(d_1)+\ldots+\phi(d_r))(\phi(e_1)+\ldots+\phi(e_s))\\&=F(m)F(n)\end{aligned}$$

欧拉ϕ函数

- 定理(欧拉ϕ函数求和公式)：设$d_1,d_2,\ldots,d_r$是n的因数，则$\phi(d_1)+\phi(d_2)+\ldots+\phi(d_r)=n$
- 证明：设$F(n)=\phi(d_1)+\phi(d_2)+\ldots+\phi(d_r)$，我们需要验证F(n)总是等于n。我们已经证明了对素数的幂次有$F(p^k)=p^k$，首先将n分解为素数幂的乘积，$n=p_1^{k1}p_2^{k2}\ldots p_r^{kr}$，彼此是不同的素数幂是互素的，所以用F的乘法公式得$F(n)=F(p_1^{k1}p_2^{k2}\ldots p_r^{kr})=F(p_1^{k1})F(p_2^{k2})\ldots F(p_r^{kr})=p_1^{k1}p_2^{k2}\ldots p_r^{kr}$