第六章 素数计数

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

素数

- 素数是数论的基本构件
  - 前面的算术基本定理告诉我们，每个数都可唯一表示成一个素数幂次的乘积形式
  - 化学中的基本元素
  - 核物理中的三种基本粒子，质子、中子和电子
  - 软件行业中的构件
  - ……

素数

- 定理1(无穷多素数定理)：存在无穷多的素数
- 证明(欧几里得)：
  - 基本思想，假设有限，然后利用有限的素数构造出一个新的素数
  - 假设现有素数表为$p_1,p_2,\ldots,p_r$，我们得到如下的数 $A=p_1*p_2*p_3*\ldots*p_r+1$
  - 如果A本身是素数，则证明完成，因为A太大不在最初的表中。

素数

  - 如果A不是素数，则其肯定会被某个素数整除，设q是某个整除A的素数，且设其为最小的那个，可知q不在最初的表中（为什么？），所以它是期望的新素数。重复这个过程可创建素数表，这表明必有无穷过个素数。
- 尝试自己创建素数表
  - 最初素数表为{2}
  - 第一次得{2,3}
  - 第二次得{2,3,7}
  - 第三次得{2,3,7,43}
  - ……

素数

- 2是仅有的偶素数！
- 有时需要对素数进行分类，如(除2之外)
  - 哪些素数模4余1？
  - 哪些素数模4余3？

p≡1(mod 4)	5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109, 113, 137, 149, 157, 173, 181, 193, 197,…
p≡3(mod 4)	3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83, 103, 107, 127, 131, 139, 151, 163, 167, 179,…

素数

- 定理2：存在无穷多个模4余3的素数
- 证明：
  - 采用与定理1同样的思想
  - 第1步，假设已经得到有限个的模4余3的素数表，$\{3, p_1, p_2, \ldots, p_r\}$
  - 第2步，构造数$A=4*p_1*p_2*p_3*\ldots*p_r+3$
  - 第3步，将A分解为素数乘积$A=q_1*q_2*q_3*\ldots*q_s$
  - 第4步，证明$q_1, q_2, q_3, \ldots, q_s$中必有一个$q_i$是模4余3的
  - 第5步，证明这个q_i不在最初的表中

素数

- 课堂讨论：前面我们知道模4余3的素数有无穷多个，那么模4余1的素数是否也无穷多个？是否可以利用上面的方法来证明？
- 答：是无穷多个，但是不能用上面的方法来证明。
  - 构造数$A=4*p_1*p_2*p_3*\ldots*p_r+1$
  - 但是我们不能得到如果$A\equiv 1 \pmod 4$，那么其有素因数能够模4余1.
    - 例如，$A=4*5+1=21=3*7$

素数

- 定理(算术级数的素数狄利克雷定理)：设a与m是整数，gcd(a,m)=1，则存在无穷多个素数模m余a，即存在无穷多个素数p满足

$$p\equiv a \pmod m$$

- 证明：略

素数计数

- 素数是无穷多个的，合数也是无穷多个，那么哪个更多一些？
- 问题：素数的分布满足什么样的规律？
- 引入素数计数函数 $\pi(x)=\#\{\text{素数}p \mid p\leqslant x\}$

X	10	25	50	100	200	500	1000	5000
π (x)	4	9	15	25	46	95	168	669
π (x)/x	0.400	0.360	0.300	0.250	0.230	0.190	0.168	0.134

素数计数

- 定理(素数定理)：当x很大时，小于x的素数个数近似等于x/ln(x)，换句话说，

$$\lim_{x\to\infty}\frac{\pi(x)}{x/\ln(x)}=1$$

其他素数猜想

- 哥德巴赫猜想：每个偶数n≥4可表示成两个素数之和
  - 10^{18}以下的偶数都经过了验证，但仍然尚未得到证明
  - 1966年，陈景润证明了每个充分大的偶数可表示成p+a的形式，其中p是素数，a是素数或两个素数的乘积

其他素数猜想

- 孪生素数猜想：存在无穷多个素数p，使得p+2也是素数
  - 素数分布很不规则，两个素数之间可能间隔非常大，如370261与370383之间隔了111个合数
  - 但是，确实能够找到很多的孪生素数

(3,5),(5,7),(11,13),(17,19),(29,31),(41,43),(59,61),(71,73),101,103),(107,109),(137,139),(149,151),…,(269,171),…

  - 陈景润1966年证明存在无穷多素数p使得p+2是素数或两个素数的乘积

其他素数猜想

- N^2+1猜想：存在无穷多个形如N^2+1的素数
  - 目前最好的结果，Hendrik Iwaniec于1978年证明，存在无穷多个N使得N^2+1是素数或两个素数的乘积

其他素数猜想

- 黎曼假设
  - 20世纪早期，德国数学家希尔伯特曾说，如果他在死后醒来，他将问的第一个问题便是：黎曼猜想得到证明了吗？然而，时间的脚步走到100年后的今天，黎曼猜想仍然没有将被解决的迹象。
  - 黎曼观察到素数的频率紧密相关于一个精心构造的所谓黎曼蔡塔函数z(s)的性态。著名的黎曼假设断言，方程z(s)=0的所有有意义的解都在一条直线上。这点已经对于开始的1,500,000,000个解验证过。在证明素数定理的过程中，黎曼提出了一个论断：Zeta函数的零点都在直线Res(s) = 1/2上。

生成所有素数的公式

- 1976年，人们找到了一个详细的精确的公式
  - $(K+2)\{1-[WZ+H+J-Q]^2-[(GK+2G+K+I)(H+J)+H-Z]^2-[2N+P+Q+Z-E]^2-[16(K+1)^3(K+2)(N+1)^2+1-F^2]^2-[E^3(E+2)(A+1)^2+1-O^2]^2-[(A^2-1)Y^2+1-X^2]^2-[16R^2Y^4(A^2-1)+1-U^2]^2-[((A+U^2(U^2-A))^2-1)*(N+4DY)^2+1-(X+CU)^2]^2-[N+L+V-Y]^2-[(A2-1)L^2+1-M^2]^2-[AI+K+1-L-I]^2-[P+L(A-N-1)+B(2AN+2A-N^2-2N-2)-M^2]2-[Q+Y(A-P-1)+S(2AP+2A-P^2-2P-2)-X^2]^2-[Z+PL(A-P)+T(2AP-P^2-1)-PM]^2\}$
  - 随机取A到Z的取值，如果输出结果大于零，则这个结果一定是素数，如果结果为负数就忽略它。

作业

- 利用欧几里得的思想证明命题："可以找到任意长度的区间，在其中不存在素数"
- 另一个有趣问题"究竟需要走多远，才能碰到下一个素数？"
  - 约瑟夫伯特兰在1845年猜测："任意取一个数N，那么在你数到它的两倍时，你一定可以发现一个素数"
  - 伯特兰—切比雪夫定理：对于所有大于1的整数n，存在一个素数p，符合$n < p < 2n$。