素数初步

MDZfirst of TJU-Tornado

2007-12-23

把素数和合成数区分开来和把合成数分解出素因子是算术中最重要和有益的问题之一 …… 科学本身的自尊要求人们采用一切可能的手段来探索去解决这个如此精美和著名的问题。

——高斯

主要内容

- 素数的定义和性质
- 素性检测
- 欧拉函数
- 梅森素数

素数的定义

所谓素数（也称质数），就是一个正整数，除了本身和 1 以外并没有任何其他因子。例如 2、3、5、7 是素数，而 4、6、8、9 则不是，后者称为合成数（也称合数）。

从这个观点可将整数分为两种，一种叫素数，一种叫合成数。

素性检测

目前有许多种素性检测方法，可以按照不同的观点分类。

- 对任意正整数的素性检测
- 对某些特殊形式数的素性检测

- 确定型的检测
- 概率型（或蒙特·卡罗）检测

素性检测法一

给了自然数 N，依次对 n = 2, 3, …… 直到 N – 1 去试 n 是否整除 N。如果这些 n 均不整除 N，则 N 为素数。如果某个 N_0 整除 N，则 $N = N_0N_1$，从而 $N_1 < N$。再对 N_0 和 N_1 重复上述程序，最终给出N的素因子完全分解。

一点点改进

有 N 盏灯放在一排，从 1 到 N 依次编号，有 N 个人也从 1 到 N 依次编号，第一个人将灯全部打开，第二个人将凡是2的倍数的灯全部关闭，……， N个人都把自己编号的倍数的灯作相反处理。问第N个人走过后，哪些灯是开着的？

……

因此，只需除至不超过sqrt(N)的最大整数。

素数的性质

素数有无限多个。

任何一个正整数都能分解成几个素数的乘积。（又被称为“唯一分解定理”）

欧几里得关于质数无限性的经典性证明

假设质数只有有限个：P_1、P_2、…、P_n，令 $P = P_1P_2\cdots P_n+1$，显然$P>1$且$P>P_i$ （$i = 1、2、3、\cdots、n$），从而P必为合数，因而必能被某个质数$P_k(1\leqslant k\leqslant n)$整除，但显然$P \% P_k == 1$，发生矛盾，故假设不成立，因此质数有无限多个。

关于唯一分解定理的几点说明

- 整数的一般表示
- 因数倍数的特征
- 互质的特征

- lcm(a, b) = a * b / gcd(a, b)
- 天津市赛F题 (2845. Factorial)

进一步改进

可以只用不超过sqrt(N)的素数试除。

如何知道哪些数是质数？

素性检测法二

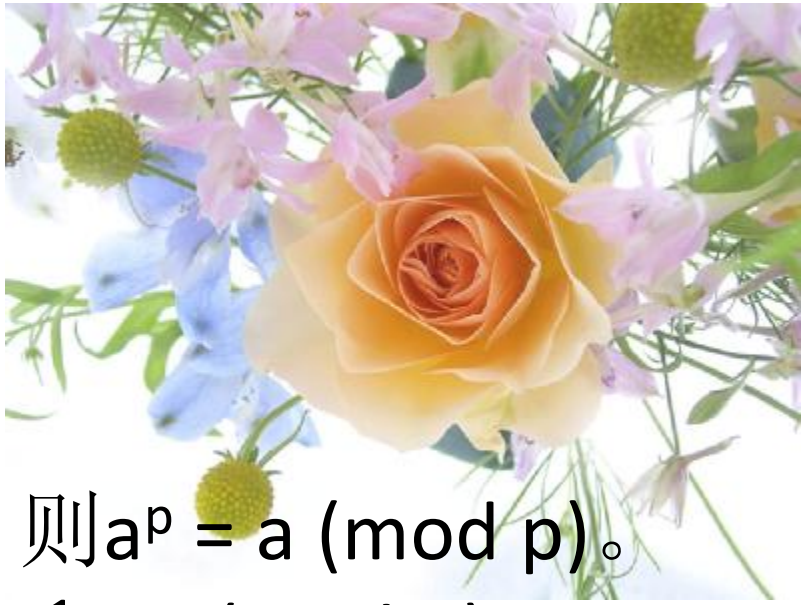
埃拉托色尼(Eratosthenes)筛法

开一个数组is_prime[]，用is_prime[i]来标记 i 是否是质数，开始时全部置 1。

然后从 2 开始向后检查，遇到一个标记为 1 的数，说明它不能被小于它的任何素数整除，因此它是素数。同时将它的倍数（本身除外）都清零，表示它们是合数。

TOJ 上题目 Goldbach’s Conjecture

费马小定理



若p为素数并且a为整数，则$a^p = a \pmod p$。
特别若a不被p整除，则$a^{p-1} = 1 \pmod p$。

证明 当a = 1时显然成立。假设定理对a成立，由归纳法知$(a+1)^p = a^p + 1 = a + 1 \pmod p$。所以定理对每个自然数a均正确。

素性检测法三

Miller-Rabin 伪素数测试法

随机选取与p互质的数a，验证 $a^{p-1} = 1 \pmod{p}$是否成立。

当N是素数时，上述方法判定N是素数的概率大于 $1 - 1/4^k$. (k为重复实验的次数)

还有很多素数检测方法：APR检测、椭圆曲线检测、AKS检测、数域筛法。

欧拉函数

对每个$n \geq 1$，以$\phi(n)$表示从1到n之中与n互素的整数个数。如果$n = p$为素数，则

$$\phi(p) = p - 1$$

进一步

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

又若m和n是互素的正整数，则

$$\phi(mn) = \phi(m)\phi(n)$$

对任意正整数

$$\varphi(n) = n \times \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$$

欧拉定理

若$\gcd(a, n) = 1$，则$a^{\phi(n)} = 1 \pmod{n}$。

欧拉定理是费马小定理的推广。

梅森质数

法国有个教士马丁·梅森在1600年提出了一个猜想：当P是质数时，任何形如 $2^P - 1$ 的数都是质数。

1903 年10 月，哥伦比亚大学教授科尔发现：

$2^{67} - 1 = 193707721 * 761838257287$

证明梅森的猜想是错误的。

梅森质数

尽管如此，但他给数学家们指明了寻找最大质数的一个方向。人们为了纪念梅森的探索精神，把形状如$2^P - 1$的数叫“梅森数”，形如$2^P - 1$的质数叫做梅森质数。

至今人们已发现44个梅森质数，最后一个梅森质数是2006年9月4日发现的，P= 32582657，共有9808358位。

还有很多特殊形式的素数被研究：正规素数、Sophie Germain素数、Wieferich素数、Wilson素数、全1素数。

哎吗呀！
累死我了！
总算讲完了……

GAME OVER