中国科学技术大学
University of Science and Technology of China

数学实验

实验五：素数

翟晓雅

Email: xiaoyazhai@ustc.edu.cn
Homepage: https://xiaoyazhai.github.io/

实验目的

- 素数表的构造
- 素数的判别
- 最大的素数
- 构造生成素数的公式
- 素数的分布

5.1 素数的判别与求解

- 素数：如果一个大于1的自然数只能被1及它本身整除
- 合数：如果一个大于1的自然数可以被除1及其它本身整除

在古希腊时期，欧几里得就证明了每一个合数都可以分解若干个素数的乘积，并且在不计较素数的排列时这个分解是唯一的。

算数基本定理

5.1 素数的判别与求解

- 素数到底有多少个?
- 会不会在某一充分大的自然数以后就没有素数了?

欧几里得证明

假设素数只有有限个，按从小到大的顺序排列为$p_1, p_2, \cdots, p_n$，令$N = (p_1 p_2 \cdots p_n)+1$则N不被$p_i\ (i = 1, 2, \cdots, n)$中任何一个整除。因而，N要么是素数，要么有比$p_n$大的素因子，这与$p_n$为最大素数相矛盾。

5.1 素数的判别与求解

- 如何求出小于某一给定整数的所有素数?

Eratosthenes证明

将自然数列从2开始按顺序排列至某一整数N，从上述数列中划去所有2的倍数（不包括2）。在剩下的数中，除2外最小的是3，从数列中划去所有3的倍数（不包括3）.然后在剩下的数中，再划去5的倍数……一直进行……

Eratosthenes筛法（用乘法寻找素数）

得到了不超过N的所有素数

5.1 素数的判别与求解

- 如何求出小于某一给定整数的所有素数?

试除方法

假设已经找到了前n个素数$p_1 = 2, p_2 = 3, \cdots, p_n$，为了寻找下一个素数我们从$p_n +$ 2开始一次检验每一个整数N，看N是否能被某个$p_i(i = 1, 2, \cdots, n)$整除。如果N能被前面的某个素数整除，则N为合数，否则N即为下一个素数p_{n+1}。（统计不超过$\sqrt{N}$的素数）

↑

试除方法

5.1 素数的判别与求解

- Eratosthenes筛法和试除法可以求出所有的素数，但是构造大的素数是不合实际的。
- 10^{50}以内的素数表，计算机也要一百亿年。
- 二十年前，11⋯1（23个1）以及$2^{127}-1$的素性判别问题难倒了很多数学家。

2003年11月17日为止，找到的最大素数是$2^{20996011}-1$其十进制形式有6320430位。

5.1 素数的判别与求解

- 对n=2,3,⋯,100。观察2^{n-1}被n整除所得的余数。观察结果得出什么结论？再取其他的整数m(如3，4，5)，观察m^{n-1}被n整除的情况。特别观察当n为素数时的结果。所得出的结论的逆命题是否成立？用你的结论能否给出判别一个数是否时素数的判别方法。

```
b = zeros(2,99);
for n = 2:1:100
    a = mod(2^(n-1),n);
    b(:,n-1) = [n,a];
end
```

2，4，8，16，32⋯

2	3	4	5	6	7	8	9	10	11
0	1	0	1	2	1	0	4	2	1

5.1 素数的判别与求解

当n为素数且m不被n整除时，m^{n-1}被n整除的余数都是1.

$m^{n-1} \equiv 1 \bmod n$ ($a \equiv b \bmod n$ 表示 a与b被n整除的余数相同)

法国数学家Fermat发现，费尔马小定理

逆定理并不成立

5.1 素数的判别与求解

- 费尔马小定理的逆定理并不成立:

$m^{n-1} \equiv 1 \bmod n$ 并不能推出n为素数

- 称满足费尔马小定理结论的合数为伪素数。
- 伪素数比素数稀少的多。

5.1 素数的判别与求解

- 对互质的整数n=2及m=1,2,⋯,1000,求得使n^d除m的余数为1的最小整数d。当m为素数时，观察d与m之间的关系，能得出什么结论？类似地，对n=3,4,5做进一步的观察，你能否确信你的结论？所得结论的逆命题是否成立？

给出一个简明的素数判别定理并不容易

5.1 素数的判别与求解

n-1 检验法

假设n-1=FR, 其中F>R且gcd(F,R)=1. 如果对F的每一个素因子q都存在一个整数a>1满足

$$a^{n-1} \equiv 1(mod\ n), \qquad gcd\left(a^{n-1/q} - 1, n\right) = 2$$

则n是素数

GCD 函数用于计算两个或多个整数的最大公约数。

5.1 素数的判别与求解

基于广义黎曼猜想的判别法

1976年，数学家缪内发现了素性判别与黎曼猜想之间的一个深刻联系即

在广义黎曼假设下，存在常数C，对任何整数n，若n为合数，则存在$a < C(\log n)^2$,使得

$$a^{\frac{n-1}{2}} \neq \binom{a}{n} (mod\, n)$$

5.1 素数的判别与求解

基于广义黎曼猜想的判别法（维路）

1978年，数学家维路指出上述常数C可取70，由此设计如下素数判别法：

$$a^{\frac{n-1}{2}} \neq \left(\frac{a}{n}\right) (mod\ n)$$

对任意n，依次对$a = 1, 2, \dots, 70(\log n)^2$检验上式是否成立，若对每一个a都不成立，则n为素数，否则n为合数。

5.1 素数的判别与求解

概率判别法

Lehmann等给出了以概率为标准的素数判别方法，给定整数p，判别它是否为素数：

(1) 选择一个小于p的随机数a;

(2) 如果a与p不互素，则p为合数;

(3) 计算$J \equiv a^{p-1}\ mod\ p$;

(4) 如果$J \neq 1$或者-1，那么p为合数;

(5) 如果J = 1或者-1，那么p不是素数的可能性最多是50%;

重复k次实验，那么p不是素数的可能性不超过$1/2^k$。

5.1 素数的判别与求解

概率判别法

利用Lehmann给出的素数判别法可以产生大的随机素数:

(1) 产生随机数p;

(2) 确定p不被较小的素数整除;

(3) 产生随机数a，利用上述算法检测p的素性，直到经过多次测试为止。

作业5.1

通过编程求500以内的所有素数

- 利用Eratosthenes筛法计算；
- 利用试除方法计算；
- 利用维路判别法计算；
- 利用概率判别法计算；

（统计上述四种方法的计算时间，判断哪一个更有效？）

作业5.2 素数的分布

- 将素数在数轴上标出来，观察素数的分布，试图通过以下实验进行进一步的观察：

用$\pi(n)$表示不超过n的素数的个数，$\pi(m,n)$表示区间[m,n]内素数的个数，试计算$\pi(100), \pi(1000), \pi(10000)$, 以及$\pi(100，200)$, $\pi(1000，1100), \pi(10000，10100)$. 从计算结果上看，随着整数范围的扩大，素数是越来越稀还是越来越密?

5.2 生成素数公式

若干问题:

（1）能否找到一个正好生成全部素数的公式?

（2）否是存在单变量整系数的多项式，只生成素数并可以得到全部的素数? ✗

（3）是否存在一个生成素数的多变量函数公式? √

（4）能否找到一个虽不能给出全部但是能给出无穷多个素数（且只给出素数）的公式?

费尔马，欧拉，高斯……

5.2 生成素数公式

1640年**费尔马**在给Mersenne的信中指出，对所有的整数n，$F_n = 2^{2^n} + 1$永远是素数

验证：

$F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$ 都是素数；

1732年，**欧拉**指出$F_5 = 4294967297$不是素数，并找出其因式分解。此后人们陆续发现F_6, F_7, F_8都是合数。

德国数学家**Gauss**在他19岁时发现：F_n与正多边形作图有紧密联系：一个正n边形可用直尺与圆规作图的充要条件是$n = 2^k$或者$n = 2^k p_1 p_2 \ldots p_r$，其中$p_1 p_2 \ldots p_r$为不同的费尔马数。

5.2 生成素数公式

是否存在一个生成素数的多变量函数公式?

作为Hilbert第十个问题的一个推论，马蒂亚舍维奇证明了:
存在一个多元多项式$P(x_1, x_2, \dots, x_n)$，其正值构成的集合恰好是素数的全体。

后来经过众多数学家的努力，在1977年构造了一个具有26个变量的25次的素数生成多项式。

5.3 更多问题

Goldbach猜想（1742年）

每个不少于6的偶数都可以表示为两个奇素数的和;
每个不少于9的奇数都可以表示为三个奇素数的和;

两百多年来，无数科学家花费了无数心血都未能解决这一问题。

5.3 更多问题

Goldbach猜想（1742年）

我国数学家陈景润的工作是迄今为止最好的结果:

他证明了:
任何一个充分大的偶数可以表示为一个素数与另两个素数的乘积和。

感兴趣的可以对10000以内的偶数进行验证。

5.3 更多问题

大整数的素因子分解

将一个大整数分解为素因子的乘积是一件非常困难的事情。目前最有效的素因子分解算法的运算量大约为$O(\exp(cL^{\frac{1}{3}}\log(L)^{\frac{2}{3}}))$其中L为要分解的整数N的位数。

计算过于庞大，至今无人能分解费尔马数F_9.

5.4 更多问题

完全数: 它的所有因子（除去它本身）之和等于该数，则该数称为完全数。

完全数都有一些奇妙的特性:

- 每个完全数(除6外)可以表为几个连续的奇数立方之和，如$28 = 1^3 + 3^3$。
- 所有的完全数的倒数都是调和数。
- 所有的完全数都是三角形数。一定数目的点或圆在等距离的排列下可以形成一个等边三角形，这样的数被称为三角形数。6=1+2+3；28=1+2+3+4+5+6+7；496=1+2+3+...+30+31；8128=1+2+3⋯+126+127。

5.4 更多问题

孪生素数：差为2的两个相邻的素数

一个问题：孪生素数是否有无穷多个?

5.4 更多问题

Bertrand猜测

当n>3时，n与2n-2之间至少存在一个素数

清一色数的素性

由n个1组成的数11 ... 1叫做清一色数。

当n为何值时，清一色数时素数？如果清一色数是合数，如何将其做素因子分解？

课堂总结

- 素数
  - 素数的判别与求解
    - n-1检验法
    - 基于广义黎曼猜想的判别法
    - 概率判别法
  - 生成素数的公式
  - 素数的分布
  - 进一步的问题
    - Goldbach猜想
    - 大整数的素因子分解
    - 完全数
    - 孪生素数
    - Bertrand猜测
    - 清一色的素性

作业5.1

通过编程求500以内的所有素数

- 利用Eratosthenes筛法计算；
- 利用试除方法计算；
- 利用维路判别法计算；
- 利用概率判别法计算；

（统计上述四种方法的计算时间，判断哪一个更有效？）

作业5.2 素数的分布

- 将素数在数轴上标出来，观察素数的分布，试图通过以下实验进行进一步的观察：

用$\pi(n)$表示不超过n的素数的个数，$\pi(m,n)$表示区间[m,n]内素数的个数，试计算$\pi(100), \pi(1000), \pi(10000)$, 以及$\pi(100，200)$, $\pi(1000，1100), \pi(10000，10100)$. 从计算结果上看，随着整数范围的扩大，素数是越来越稀还是越来越密?

Q&A?

下节课内容

实验六：概率

翟晓雅
Email: xiaoyazhai@ustc.edu.cn
Homepage: https://xiaoyazhai.github.io/
Lab: http://gcl.ustc.edu.cn/