初等数论
第六章 素性检验

卢 伟

Email: luwei3@mail.sysu.edu.cn

中山大学 数据科学与计算机学院

1. 拟素数

1.1. 引子

根据欧拉定理我们知道, 当b与$n(n>1)$互素时, 有$b^{\varphi(n)} \equiv 1 \bmod n$成立,
更进一步, 如果n是素数, 则$\varphi(n) = n-1$, 则有$b^{n-1} \equiv 1 \bmod n$成立,
即"如果n是素数, 则对所有与n互素的b, $b^{n-1} \equiv 1 \bmod n$成立"

- 逆否命题成立: 将其反过来说就是, 如果存在与n互素的b使得$b^{n-1} \equiv 1 \bmod n$不成立(即$b^{n-1} \not\equiv 1 \bmod n$成立), 则$n$是合数;
  (即$\not\equiv 1 \Longrightarrow n$是合数)
- 未必: "如果n是合数, 则对所有与n互素的b, $b^{n-1} \not\equiv 1 \bmod n$"
  (即n是合数$\not\Longrightarrow \not\equiv 1$)
  反例: 63是合数, 8与63互素,但有$8^{62} = (2^6)^{31} \equiv 1 \bmod 63$.

反例: 63是合数, 8与63互素,但有$8^{62} = (2^6)^{31} \equiv 1 \bmod 63$.

我们对类似于63与8这样关系的数给一个专门的定义:

1.2. 拟素数

设n是一个合数, 如果对于与n互素的整数b, 有

$$b^{n-1} \equiv 1 \bmod n$$

成立, 则称n为(对于基b的)的拟素数

所以63是对于基8来说的拟素数.

1.3 存在无穷多个对于基2的拟素数

我们要证明如果n是对于基2的拟素数, 则$m \triangleq 2^n - 1$也是对于基2的拟素数.

这样, 找到一个对于基2的拟素数n_0(比如$341(= 11 \times 31, 2^{340} \equiv 1 \bmod 341)$后, 只需要逐次计算$n_1 = 2^{n_0} - 1, n_2 = 2^{n_1} - 1, \ldots$就得到无穷多的对于基2的拟素数.

事实上, n是对于基2的拟素数$\Longrightarrow$ n是奇合数且$2^{n-1} \equiv 1 \bmod n$

而n是奇合数$\Longrightarrow$有分解式$n = dq(1 < d, q < n)$

$$\Longrightarrow 2^n - 1 = (2^d)^q - 1 = (2^d - 1)((2^d)^{q-1} + (2^d)^{q-2} + \ldots + 2^d + 1)$$

$$\Longrightarrow (2^d - 1)|(2^n - 1)$$

$$\Longrightarrow 2^n - 1\text{是合数}$$

还需要说明$2^{m-1} \equiv 1 \bmod m$

$$2^{n-1} \equiv 1 \bmod n \Longrightarrow (2^{n-1} - 1) = kn$$

$$\Longrightarrow m - 1 = 2^n - 2 = 2(2^{n-1} - 1) = (2k)n$$

$$\Longrightarrow (2^n - 1)|(2^{m-1} - 1)(i.e., m|(2^{m-1} - 1))$$

$$\Longrightarrow 2^{m-1} \equiv 1 \bmod m$$

1.4 如果n是一个奇合数, 则n是对于基b的拟素数 $\iff$ $\mathrm{ord}_n(b)|(n-1)$

"$\Longrightarrow$":

$$n\text{是对于基}b\text{的拟素数} \Longrightarrow b^{n-1} \equiv 1 \bmod n \Longrightarrow \mathrm{ord}_n(b)|(n-1)$$

"$\Longleftarrow$":

$$\mathrm{ord}_n(b)|(n-1) \Longrightarrow (n-1) = k \cdot \mathrm{ord}_n(b) \Longrightarrow b^{n-1} = (b^{\mathrm{ord}_n(b)})^k \equiv 1 \bmod n \quad \diamond$$

1.5 如果n是一个奇合数, 如果n是对于基b_1的拟素数,且n是对于基b_2的拟素数, 则n是对于基b_1b_2的拟素数

事实上, n是对于基b_1的拟素数

$$\Longrightarrow b_1^{n-1} \equiv 1 \bmod n;$$

n是对于基b_2的拟素数

$$\Longrightarrow b_2^{n-1} \equiv 1 \bmod n;$$

从而

$$\Longrightarrow (b_1b_2)^{n-1} \equiv 1 \bmod n;$$

即n是对于基b_1b_2的拟素数 $\diamond$

1.6 设n是一个奇合数, 如果n是对于基b的拟素数, 则n是对于基b^{-1}的拟素数

事实上, n是对于基b的拟素数

$$\Longrightarrow b^{n-1} \equiv 1 \bmod n;$$

又因为

$$\begin{aligned} & b^{n-1} \cdot (b^{-1})^{n-1} \equiv 1 \bmod n \\ \Longrightarrow & (b^{-1})^{n-1} \equiv (b^{n-1})^{-1} \bmod n \\ \Longrightarrow & (b^{-1})^{n-1} \equiv 1 \bmod n \end{aligned}$$

即n是对于基b^{-1}的拟素数 $\diamond$

注意到:

$$b^{n-1} \equiv 1 \bmod n \Longrightarrow (b^{-1})^{n-1} \equiv 1 \bmod n$$

1.7 如果n是一个奇合数, 如果存在整数$b((b,n)=1)$使得$b^{n-1}\not\equiv 1 \bmod n$, 则在模$n$的简化剩余系(比如$\{b_1,b_2,\ldots,b_s,b_{s+1},\ldots,b_{\varphi(n)}\}$) 中至少有一半的数使得$b_i^{n-1}\not\equiv 1 \bmod n$

假设$\{b_1,b_2,\ldots,b_s\}$使得$b_i^{n-1}\equiv 1 \bmod n$; $\{b_{s+1},\ldots,b_{\varphi(n)}\}$使得$b_i^{n-1}\not\equiv 1 \bmod n$

则首先对b_1来说,有$(bb_1)^{n-1}\not\equiv 1 \bmod n$

因为否则的话,

$$\left.\begin{array}{c}(bb_1)^{n-1}\equiv 1 \bmod n \\ b_1^{n-1}\equiv 1 \bmod n \Longrightarrow (b_1^{-1})^{n-1}\equiv 1 \bmod n\end{array}\right\} \Longrightarrow (bb_1\cdot b_1^{-1})^{n-1}\equiv 1 \bmod n$$

$$\Longrightarrow b^{n-1}\equiv 1 \bmod n$$

矛盾.

类似地,

$$(bb_2)^{n-1} \not\equiv 1 \bmod n$$
$$(bb_3)^{n-1} \not\equiv 1 \bmod n$$
$$\cdots\cdots$$
$$(bb_s)^{n-1} \not\equiv 1 \bmod n$$

注意到$bb_i(i = 1, 2, \ldots, \varphi(n))$也是简化剩余系, 这样我们找到$s$个不同简化剩余使得

$$x^{n-1} \not\equiv 1 \bmod n$$

所以有

$$s \leq \varphi(n) - s \Longrightarrow s \leq \frac{\varphi(n)}{2} \Longrightarrow \varphi(n) - s \geq \frac{\varphi(n)}{2} \qquad \diamond$$

从而我们证明了对于奇合数n, 如果有b使得$b^{n-1} \not\equiv 1 \bmod n$, 则在其任意的简化剩余系中至少有一半的数满足

$$x^{n-1} \not\equiv 1 \bmod n$$

这其实就是说, 对于奇合数n, 如果我们任取一个与n互素的数b_i, 那么非常大的可能$(> \frac{1}{2})$会有关系$b_i^{n-1} \not\equiv 1 \bmod n$出现.

换句话说, 对于任意整数n, 如果我们任取一个与n互素的数b_i, 出现了关系$b_i^{n-1} \equiv 1 \bmod n$, 那么我们很有理由怀疑这个数是素数(即这个数有非常大的可能是素数).

如果对n是否是素数还有担心的话, 我们就继续去一个与n互素的数b_j来计算b_j^{n-1}, 看它是否与1模n同余: 如果确实与1同余, 则就确认了我们的"n应该是一个素数"的信念; 如果不同余, 那么当然n肯定是一个合数.

如果对n是否是素数仍然持有担心的话, 我们就继续去一个与n互素的数b_k来计算b_k^{n-1}, 看它是否与1模n同余: 如果确实与1同余, 则就更加确认了我们的"n应该是一个素数"的信念; 如果不同余, 那么当然n肯定是一个合数.

.....

如果经过一定次数(比如64次)的这样的检验都能确认我们的信念的话, 那么我们基本上就可以说n就是素数了.

这个检验n是否是素数的过程我们称之为Fermat素性检验.(概率性检查)

对于任意的整数n, 当然也不排除这样一种可能性, 那就是:

所有与n互素的数b, 都有$b^{n-1} \equiv 1 \bmod n$,

但n自身还是一个合数,
这种数称之为Carmichael数.(卡米切尔)

比如$n = 561$就是一个Carmichael数(因子分解$(3 \times 11 \times 17)$.

这也说明: 对所有与n互素的b都有$b^{n-1} \equiv 1 \bmod n \not\Longrightarrow n$是素数

2. Eular拟素数

根据勒让得符号的定义和欧拉判别准则, 我们知道, 如果$n = p$是一个素数, 则对任意的整数b来说都有下式成立:

$$b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \bmod n$$

- (逆否命题成立) 换句话说, 给定一个整数n, 如果存在与n互素的整数b使得

  $$b^{\frac{n-1}{2}} \not\equiv \left(\frac{b}{n}\right) \bmod n$$

  则这个整数n肯定不是一个素数.(即$\not\equiv \Longrightarrow$是合数)
- (不成立) 但不排除一种情况, 那就是, 当n不是一个素数时, 有与n互素的b使得同余式成立$b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \bmod n$, 我们把这种$n$称为是对基$b$的Eular拟素数.

完整定义是: 设n是一个正奇合数, 如果有与n互素的整数b满足条件$b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \bmod n$, 则称$n$是对于基$b$的Eular拟素数.

比如: $n = 1105$是一个合数, 对于$b = 2$来说, 分别计算$2^{552} \equiv 1 \bmod 1105$和$(\frac{2}{1105})$, 可以发现$2^{\frac{1105-1}{2}} \equiv (\frac{2}{1105}) \bmod 1105$, 所以1105是对于基2的欧拉拟素数.

2.1 n是对于基b的欧拉拟素数$\Longrightarrow n$是对于基b的拟素数

事实上, n是对于基b的欧拉拟素数$\Longrightarrow b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \bmod n$ 逆否命题

$$\Longrightarrow b^{n-1} \equiv \left(\frac{b}{n}\right)^2 \bmod n$$

$$\Longrightarrow b^{n-1} \equiv 1 \bmod n$$

则n是对于基b的拟素数.

2.2 n是对于基b的拟素数$\not\Longrightarrow n$是对于基b的欧拉拟素数

反例: $n = 341, b = 2$.

2.3 素性检查

我们同样可以判断一个给定的整数n是否是素数, 判断过程完全类似上节, 即:

取一个与n互素的数b_j来计算$b_j^{\frac{n-1}{2}}$和$(\frac{b}{n})$(雅可比符号), 看它们是否模n同余:
如果确实同余, 则可以继续下一次确认;
如果不同余,那么当然n肯定是一个合数.

这个过程可以持续一定的次数(比如64次).

这个素性检测的方法称为Solovay-Stassen素性检测.

3. 强拟素数

3.1 引子 设n是正奇整数, 并且$n-1=2^s t$, 则下面等式显然成立:

$$b^{n-1}-1=(b^{2^{s-1}t}+1)(b^{2^{s-2}t}+1)\dots(b^{2^2 t}+1)(b^{2t}+1)(b^t+1)(b^t-1)$$

这样, 如果n是一个素数(b与n互素), 则应该有$b^{n-1}-1\equiv 0 \bmod n$, 从而应该有

$$(b^{2^{s-1}t}+1)(b^{2^{s-2}t}+1)\dots(b^{2^2 t}+1)(b^{2t}+1)(b^t+1)(b^t-1)\equiv 0 \bmod n$$

这也就是

$$b^t-1\equiv 0 \bmod n (i.e., b^t\equiv 1 \bmod n)$$
$$b^t+1\equiv 0 \bmod n (i.e., b^t\equiv -1 \bmod n)$$
$$b^{2t}+1\equiv 0 \bmod n (i.e., b^{2t}\equiv -1 \bmod n)$$
$$\dots\dots$$
$$b^{2^{s-1}t}+1\equiv 0 \bmod n (i.e., b^{2^{s-1}t}\equiv -1 \bmod n)$$

中至少有一个成立.

$$b^t - 1 \equiv 0 \bmod n (i.e., b^t \equiv 1 \bmod n)$$
$$b^t + 1 \equiv 0 \bmod n (i.e., b^t \equiv -1 \bmod n)$$
$$b^{2t} + 1 \equiv 0 \bmod n (i.e., b^{2t} \equiv -1 \bmod n)$$
$$\cdots\cdots$$
$$b^{2^{s-1}t} + 1 \equiv 0 \bmod n (i.e., b^{2^{s-1}t} \equiv -1 \bmod n)$$

中至少有一个成立., 那么我们有如下的结论：

- 逆否命题成立: 给定n和与它互素的b, 如果这些式子均不成立, 则n肯定不是素数;
- 如果n是合数的话, 也有可能这些式子至少有一个成立, 我们把这种n称为是关于b的强拟素数, 更详细的定义是:

3.2 设n是一个奇合数, $n-1=2^s t(t$为奇数), 如果对于与n互素的整数b来说, 有$b^t \equiv 1 \bmod n$成立, 或者是存在一个r, $0 \leq r < s$, $s.t.$,

$$b^{2^r t} \equiv -1 \bmod n$$

则称n是对于基b的强拟素数.

反过来这些同余式

$$b^t - 1 \equiv 0 \bmod n(i.e., b^t \equiv 1 \bmod n)$$
$$b^t + 1 \equiv 0 \bmod n(i.e., b^t \equiv -1 \bmod n)$$
$$b^{2t} + 1 \equiv 0 \bmod n(i.e., b^{2t} \equiv -1 \bmod n)$$
$$\cdots\cdots$$
$$b^{2^{s-1}t} + 1 \equiv 0 \bmod n(i.e., b^{2^{s-1}t} \equiv -1 \bmod n)$$

都不成立, 这就意味着n肯定不是素数(因为对于素数的n, 这个式子应该成立). 这样我们也就得到了类似前面判断素数的方法.

3.3 素性检验

给定一个奇整数n,

1. 将$n-1$写成$n-1=2^s t$(t为奇整数);
2. 随机取整数b,
   1. 计算$r_0=(b^t \bmod n)$, 如果r_0的值等于± 1, 则我们知道n可能为素数, 这样可以继续选取b来确认;
   2. 否则的话, 计算$r_1=(r_0^2 \bmod n)$(即$b_0^{2t} \bmod n$), 如果r_1的值等于-1(即$n-1$), 则我们知道n可能为素数, 这样可以继续选取b来确认;
   3. 否则的话, 计算$r_2=(r_1^2 \bmod n)$(即$b_0^{2^2 t} \bmod n$), 如果r_2的值等于-1(即$n-1$), 则我们知道n可能为素数, 这样可以继续选取b来确认;
   4. 否则的话, 计算$r_3=(r_2^2 \bmod n)$(即$b_0^{2^3 t} \bmod n$), 如果r_3的值等于-1(即$n-1$), 则我们知道n可能为素数, 这样可以继续选取b来确认;
   5. 这个计算过程一直进行下去, 一直到计算$r_{s-1}=(r_{s-2}^2 \bmod n)$(即$b_0^{2^{s-1} t} \bmod n$), 如果$r_{s-1}$的值等于$-1$(即$n-1$), 则我们知道$n$可能为素数, 这样可以继续选取$b$来确认;
   6. 否则的话, 我们知道此时n肯定不是素数.

选取b的次数也可以为较多次(如64次)以确信n是素数.

这个检测方法称为Miller-Rabin素性检测.

3.4 存在无穷多个对于基2的强拟素数.

为了证明结论, 我们将说明"n是对于基2的拟素数$\Longrightarrow m \triangleq 2^n-1$是对于基2的强拟素数"(显然$m$是奇数).
这样因为我们知道存在无穷多个对于基2的拟素数, 所以也就存在无穷多个对于基2的强拟素数.
事实上, 在前面证明"n是对于基2的拟素数$\Longrightarrow m \triangleq 2^n-1$是对于基2的强拟素数"中,我们已经知道$m=2^n-1$必定是奇合数.
另外, n是对于基2的拟素数$\Longrightarrow 2^{n-1}\equiv 1 \bmod n \Longrightarrow 2^{n-1}-1=nk$, 这里$k$必定是奇数(如果$k$是偶数,则$2^{n-1}-1$是偶数, 不可能), 从而$nk$是奇数.
根据强拟素数的定义, 我们需要有$m-1$的分解形式,事实上,
$m-1=2^n-1-1=2^n-2=2(2^{n-1}-1)=2^1(nk)$(即强拟素数定义中的$t=nk$)
为了说明m是强拟素数需要说明
$2^t\equiv 1 \bmod m$ or $2^t\equiv -1 \bmod m$ or $2^{2t}\equiv -1 \bmod m$ ... or $2^{2^{s-1}t}\equiv -1 \bmod m$
其实我们有

$$2^t=2^{nk}=(2^n)^k=(2^k-1+1)^k=(m+1)^k$$

从而$2^t\equiv 1 \bmod m$. $\diamond$

3.5 n是对于基b的强拟素数$\Longrightarrow$ n是对于基b的欧拉拟素数.

不证.

从而我们有: "n是对于基b的强拟素数$\Longrightarrow$ n是对于基b的欧拉拟素数$\Longrightarrow$ n是对于基b的拟素数."

4. 多项式时间检测算法AKS

2002年由印度计算机科学家证明的素性判别是存在多项式时间内有效快速算法问题的理论成果.

unlike prime factorization, primality testing was long believed to be a P-problem. This had not been demonstrated, however, until Agrawal et al. unexpectedly discovered a polynomial time algorithm for primality testing that has asymptotic complexity of $O(\log^{\frac{15}{2}} n)$.

(M. Agrawal, N. Kayal, N. Saxean. "Primes in P.", Preprint, Aug. 6, 2002.

`http://fatphil.org/maths/aks/`)


cnsphoto