第六章 素数检验

2024年12月16日 星期一 14:46

Fermant 素数检验

给出大奇整数 n，判断 n 是否为素数：

(1) 随机选取 $b_1 \in \mathbb{Z}$，$0 < b_1 < n$，计算 $d_1 = (b_1, n)$

(2) 若 d_1 $\begin{cases} > 1: n \text{不是素数} \\ = 1: (3) \end{cases}$

(3) 计算 $b_1^{n-1} \equiv 1 \pmod n$ 是否成立

$\begin{cases} \text{不成立}: n \text{不是素数} \\ \text{成立}: n \text{是合数的概率小于} \frac{1}{2} \end{cases}$

重复 (1) ~ (3) t 次

若成立，则 n 是合数的概率 $< \frac{1}{2^t}$，n 是素数的概率 $> 1 - \frac{1}{2^t}$

Miller-Rabin 素数检验

设 n 是奇素数，且有 $n-1 = 2^s t$，则有以下因数分解式

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

$\therefore$ 若 $b^{n-1} \equiv 1 \pmod n$

则 $b^t \equiv 1 \pmod n$

$b^t \equiv -1 \pmod n$

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

$\vdots$

$b^{2^{s-1}t} \equiv -1 \pmod n$

至少有一个成立

$\therefore$ 若 b 使 $\begin{cases} b^t \not\equiv 1 \pmod n \\ b^t \not\equiv -1 \pmod n \\ \vdots \\ b^{2^{s-1}t} \not\equiv -1 \pmod n \end{cases}$

则 n 是合数