Miller-Rabin

一. 二次探测定理：

a) 有一个很显然的性质：p 是奇素数时，

$$x^2 \equiv 1\ (Mod\ p) \rightarrow x \equiv \pm 1\ (Mod\ p)$$

b) 不难得出：此方法对于强伪素数也有效

c) 所以我们可以通过增加二次探测的次数来增加算法的可靠性

二. 关于进行二次探测时的基底的选择

a) 选取 2~23 之间的质数可以保证 $3 \cdot 10^{18}$ 以内的正确性

b) 选取 2~37 之间的质数可以保证 2^{64} 以内的正确性