Miller-Rabin

若 $x^2 \bmod p = 1$，我们有 $(x^2-1) \bmod p = 0$，即 (x^2-1) 是可以被 p 整除的。

~~因为 p 是一个素数，~~

我们有 $(x^2-1) = np$，n 是正整数 $\{0, 1, 2, 3, \cdots\}$

$(x-1)(x+1) = np$，因 p 是个素数，p 只能是 1 或 p 且不能有其它两正整数乘积组合。

但 n 可以有。我可以把 n 拆为 $\frac{n}{t}$ 和 t。$\frac{n}{t}$ 和 t 可以相互交换，我们只有七做后序计算。n 和 t 是正整数。

$(x-1)(x+1) = \frac{n}{t}tp$

① $\begin{cases} x+1 = tp \\ x-1 = \frac{n}{t} \end{cases}$

② $\begin{cases} x+1 = \frac{n}{t} \\ x-1 = tp \end{cases}$

因为我们只看 p，可以得出

① $x = tp-1$

② $x = tp+1$

当 $t=0$ 时，$x = \pm 1$。因为 x 我们都只会用大于 0 的数。所以 $x=1$，$x \bmod p = 1$

当 $t \neq 0$ 时 $x \bmod p = (tp \pm 1) \bmod p = \begin{cases} 1 \\ p-1 \end{cases}$

所以我们得出，<u>若 $x^2 \bmod p = 1$ 且 p 是素数，那么 $x \bmod p$ 只可得是 1 或 $p-1$。</u>

返回 Fermat. $x^{p-1} \bmod p = 1$ 若 p 是素数。

$(p-1)$ 一定是一个偶数（合数）。那么 $(p-1)$ 可以拆为一个奇数和 s 个 2 的乘积。

$p-1 = d \cdot 2^s$　　d 是个正整奇数，s 是正整数。

若 $x^{d \cdot 2^s} \bmod p = 1$，$x^{d 2^{s-1}} \bmod p$ 可以是 1 或 $n-1$，当 p 是素数。

若 $x^{d \cdot 2^{s-1}} \bmod p$ 还为 1，$x^{d 2^{s-1}} \bmod p$ 也可以是 1 或 $n-1$。

⋮ 以此类推。

最 $x^d \bmod p$ 可以是 1 或 $p-1$

这是 Miller-Rabin 本质推断：但是我们来分析一下可能出现的情况，最后再推出规则。

① $x^{d\cdot 2^s} \bmod p = 1$

$x^{d\cdot 2^{s-1}} \bmod p = 1$

⋮

$x^{d} \bmod p = 1$

很可能是素数，一直是得1.

② $x^{d\cdot 2^s} \bmod p =$?

$x^{d\cdot 2^{s-1}} \bmod p =$?

⋮

$x^{d} \bmod p = p-1$

最后是(p-1)，也很可能是素数.

③ $x^{d\cdot 2^s} \bmod p = 1$

$x^{d\cdot 2^{s-1}} \bmod p = 1$

⋮

$x^{d\cdot 2^r} \bmod p = p-1$

⋮

$x^{d} \bmod p$

在中间某个位置，得出(p-1)，很可能是素数，不继续算是因为 =(p-1) 无法确当后面值了.

④ $x^{d\cdot 2^s} \bmod p = X?$

$x^{d\cdot 2^{s-1}} \bmod p = X?$

⋮

$x^{d} \bmod p = X?$

一定不是素数. 因为 ~~这~~ 一开始就不对

⑤ $x^{d\cdot 2^s} \bmod p = 1$

$x^{d\cdot 2^{s-1}} \bmod p = 1$

⋮

$x^{d\cdot 2^r} \bmod p = X?$

在中间发现了不是1和p-1的不是1

一定不是素数.

※ 这里 $X?$ 是既不等于1也不等于p-1.

对于上述5种情况，是从 $d\cdot 2^s \Rightarrow d\cdot 2^0$ 的过程。如果我们倒过来看，即 $d\cdot 2^0 \Rightarrow d\cdot 2^s$，情况更少，也更优化

为什么更优化：(不是最重要).

p是素数，$x^{p-1} \bmod p = 1$ ， $x^d \bmod p = 1$，一般会同时满足。

为什么情况更少. (省略情况①，结合②③). (情况①不用考虑是因为 $x^d \bmod p = 1$，那过程一定都是1).

$x^d \bmod p \Rightarrow x^{d\cdot 2^s} \bmod p$

① 只要 过程中算出(p-1) $\Rightarrow$ 可能是素数.

② 只要碰 $x^d \bmod p = 1$，过程中算出1 $\Rightarrow$ 不是素数. ← 情况⑤

③ 推回到 $\underset{\text{碰}}{s-1}$ 的过程结果，没算出1或(p-1) $\Rightarrow$ 也不素数 (情况④)

(碰s，因为 $x^{d\cdot 2^s} \bmod p$，只有1和不是1两种情况。没等p-1这种其讨论)

---

miller-robin：若p是个素数，那么 $a^d \bmod p = 1$ 或者 ~~$a^{d\cdot 2^i} \bmod p$~~ 存在一个i，使得 $a^{d\cdot 2^i} \bmod p = n-1$. $(0 \le i < s)$

(有一个就行)

$(p-1) = d\cdot 2^s$

code 逻辑：循环多次 $\Rightarrow$

- $a^d \bmod p = 1$ 或 $p-1$ ⇓ true!
- $a^d \bmod p \neq 1$ 且 $\neq p-1$ $\Rightarrow$
  - $a^{d\cdot 2^i} \bmod p = 1 \Rightarrow$ false
  - $a^{d\cdot 2^i} \bmod p = p-1 \Rightarrow$ ture.
  - 出了i循环还(i>s-1) $\Rightarrow$ false.