
teoria dos numeros
gema
grupo de estudos
matemáticos abundantes
miller rabin
dikson

O que é Miller Rabin?

Um algoritmo (muito) rápido que identifica se um número (muito) grande é primo.

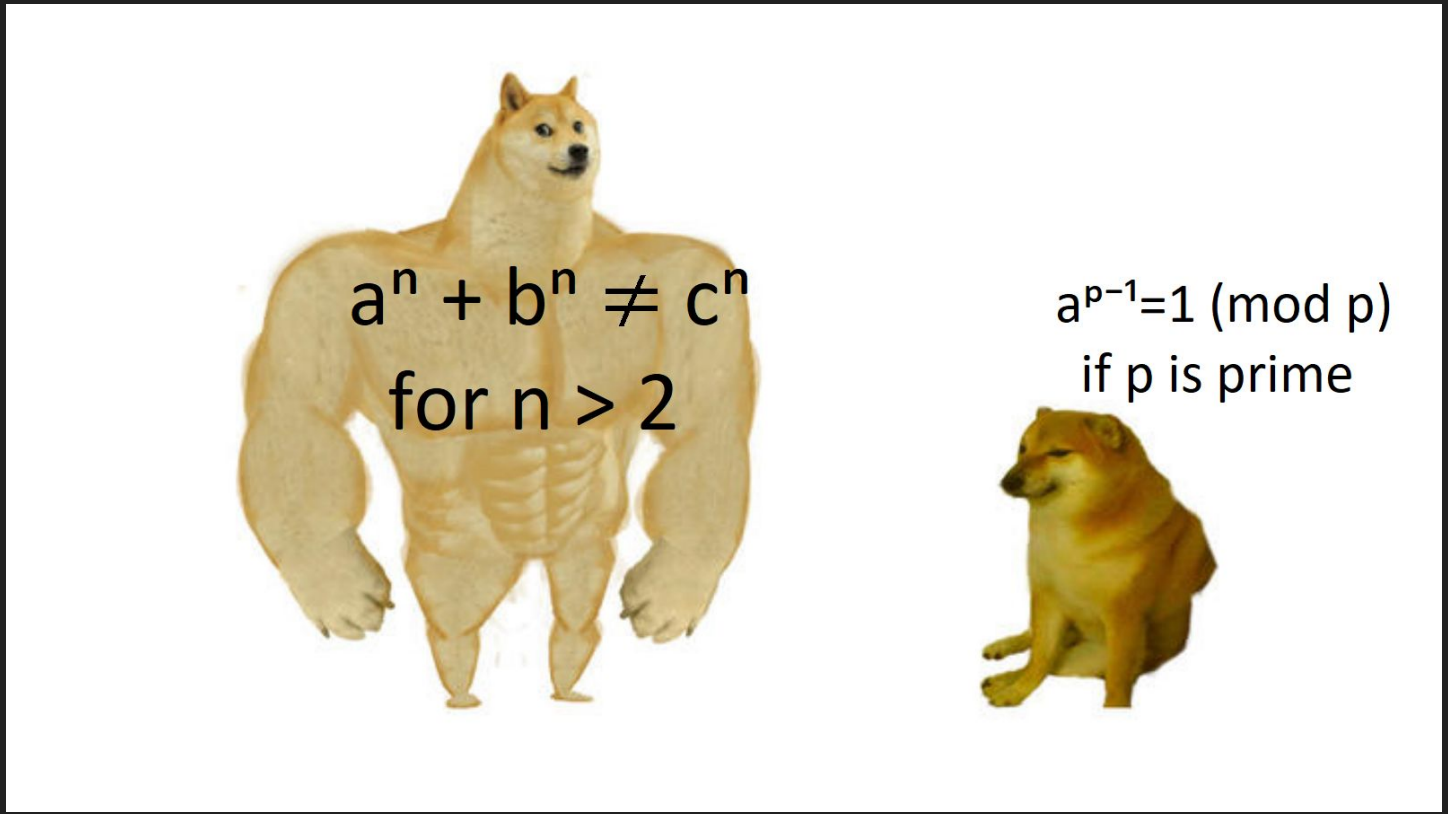
Melhor algoritmo até agora: $O(\sqrt{n})$

Notação

$$x \equiv y \ (mod \ z) \iff x\%z == y\%z$$

$$(x \ e \ y \ possuem \ o \ mesmo \ resto \ módulo \ z)$$

(Pequeno) Teorema de Fermat



(Pequeno) Teorema de Fermat

Teorema: se p é primo e a não é um múltiplo de p, então $a^{p-1} \equiv 1 \ (mod \ p)$

Exemplos:

$2^{3-1} \equiv 4 \equiv 1 \ (mod \ 3)$

$4^{5-1} \equiv 256 \equiv 1 \ (mod \ 5)$

Prova: ##########################

p primo e a coprimo ⇒ $a^{p-1} \equiv 1 \ (mod \ p)$

A volta é verdadeira?

Se $a^{p-1} \equiv 1 \ (mod \ p)$ e a não é múltiplo de p, então p é primo?

RESPOSTA: **NÃO** o(T⌒To)

Contra-exemplo: $a = 2,\ p = 2047$

$$2^{2046} = (2^{11})^{186} = (2048)^{186}$$

$$2048 \equiv 1\ (mod\ 2047)$$

$$\Rightarrow 2^{2047-1} \equiv 2048^{186} \equiv 1^{186} \equiv 1\ (mod\ 2047)$$

2047 = 23 * 89

2047 é ***pseudoprimo*** na ***base*** 2

Crewmate

There is 1 pseudoprimo among us

Escolha de outra base?

$$2^{2046} \equiv 1 \ (mod\ 2047)$$

$$3^{2046} \equiv 1013 \ (mod\ 2047)$$

$$20^{2046} \equiv 622 \ (mod\ 2047)$$

É só testar várias bases, certo?

RESPOSTA: **NÃO**

Números de Carmichael

Ex: $561 = 3 \cdot 7 \cdot 11$

Passam no teste de Fermat

para todas as bases coprimas

Miller Rabin - Primeiros passos

$$Lema: se\ p\ é\ primo\ e\ q^2 \equiv 1\ (mod\ p),\ então\ q \equiv \pm 1\ (mod\ p)$$

$$Prova:$$

$$q^2 \equiv 1\ (mod\ p) \iff$$

$$(q-1)(q+1) \equiv 0\ (mod\ p) \iff$$

$$q-1 \equiv 0\ (mod\ p)\ ou\ q+1 \equiv 0\ (mod\ p) \iff$$

$$q \equiv 1\ (mod\ p)\ ou\ q \equiv -1\ (mod\ p)$$

$$Assim,\ q^2 \equiv 1 (mod\ p) \iff q \equiv \pm 1 (mod\ p)$$

Descrição do algoritmo

queremos saber se um número n é primo.

$$n\ par \Rightarrow \ldots$$

$$n\ \text{ímpar} \Rightarrow\ n-1 = q \cdot 2^k,\ q\ \text{ímpar}$$

$$n - 1 = q \cdot 2^k$$

$$a^{q \cdot 2^k} \equiv 1 \,(mod\, n)$$

$$a^{q \cdot 2^{k-1}} \equiv \pm 1 \,(mod\, n)$$

$$a^{q \cdot 2^{k-2}} \equiv ??? \,(mod\, n)$$

$$\dots$$

$$a^{q \cdot 2^1} \equiv ??? \,(mod\, n)$$

$$a^{q \cdot 2^0} \equiv ??? \,(mod\, n)$$

(pelo teorema de fermat)

n *primo e* $gcd(a, n) = 1$

$$\Rightarrow a^{n-1} \equiv 1 \,(mod\, n)$$

(pelo lema anterior)

se n *é primo :*

$$a^{q \cdot 2^t} \equiv 1 \,(mod\, n) \iff a^{q \cdot 2^{t-1}} \equiv \pm 1 \,(mod\, n)$$

Teste de Miller Rabin:

checa se vem um -1 antes do primeiro 1 (ou já começa com um 1)

p primo ⇒ p passa no teste de miller rabin

p passa no teste de miller rabin ⇒ p primo?

RESPOSTA: NÃOO ಥ_ಥ

p é ***fortemente pseudoprimo*** na ***base*** a

sim, eu passo no teste de primalidade de miller rabin, como adivinhou?

No que ajuda?

Miller Rabin >>> Fermat

⇒ Não existem “fortemente pseudoprimos de Carmichael”

Teorema: “se um número d é fortemente pseudoprimo para pelo menos $\frac{d}{4}$ bases, então d é definitivamente primo”

⇒ Testar pra $\frac{d}{4}$ bases é muito pior que $O(\sqrt{d})$

⇒ Solução?

Algoritmo Randomizado

⇒ Um número d só pode ser fortemente pseudoprimo com $\frac{d}{4}$ bases

⇒ Qual a chance de darmos azar e pegarmos uma dessas bases? $\frac{1}{4}$

⇒ E se tentarmos com k bases, de forma aleatória? $(\frac{1}{4})^k = \frac{1}{4^k}$

⇒ Com k = 40, a chance do computador ser atingido por um raio cósmico e errar o resultado[1] é maior do que a chance do miller rabin em si falhar

[1] http://stackoverflow.com/questions/6325576/how-many-iterations-of-rabin-miller-should-i-use-for-cryptographic-safe-primes

Complexidade

Em Python, consegue dizer se um número de 1024 bits é primo (usado em RSA)

Complexidade em C++:

$$O(k \cdot log(n)) \; se \; n < 2 \cdot 10^9$$
$$O(k \cdot log^2(n)) \; se \; n > 2 \cdot 10^9$$

Em breve, nos cinemas...

⇒ Se um número é composto, como eu fatoro ele?

⇒ RESPOSTA: **Pollard - Rho**, Curvas Elípticas, GNFS…

Trivia

⇒ Se alguém descobrir um jeito rápido de fatorar um número composto, a criptografia RSA seria completamente quebrada

⇒ `factor` no ubuntu (<2^127)

```
dikson@Notebookson:~$ factor 42
42: 2 3 7
dikson@Notebookson:~$ factor 123456789012345678907
123456789012345678907: 191 34759 18595777298003
dikson@Notebookson:~$
```

⇒ Inverso de um primo:

$$a^{p-1} \equiv a \cdot a^{p-2} \equiv 1 \Rightarrow a^{p-2} \text{ é o inverso de } a \bmod p$$

Dúvidas?