Obs

- Se puede mejorar la potencia $\sqrt{2}$ en varias maneras.

(ejercicio) Por ejemplo, si $a \geq \sqrt{N}$, $a^2 \pmod N = \theta(\sqrt{N})$

- Ya hemos hablado de como verificar si un número es B-liso.

~~Tenemos que dividir por $\pi(B)$ primos~~

Tenemos que dividir $L(N)^{\sqrt{2}}$ números, por $\pi(B) \sim L(N)^{\sqrt{2}}$ primos.

O sea $\sim L(N)^{2\sqrt{2}}$ números.

Pregunta clave

¿Cómo se puede encontrar muchos enteros $a \geq \sqrt{N}$ t.q. cada $a^2 \pmod N$ es B-liso?

Sabemos que $B \approx L(N)^{1/\sqrt{2}}$. Cribas en general son maneras de encontrar números B-lisos. La criba cuadrática de Pomerance es la más rápida para factorizar $N = pq \approx 2^{350}$

Empezamos con la criba de Eratosthenes: encuentre muchos números B-lisos

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~	11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	~~19~~
21	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~	31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~	~~51~~	~~52~~	~~53~~	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	~~59~~	~~60~~

Subrayamos el primer número (2) y tachamos todos los números pares

Subrayamos el primer número que queda (3) y tachamos todos los números $0 \pmod 3$.

Subrayamos el primer número que queda (5) y tachamos todos los números $0 \pmod 5$

Se note que los números tachados varias veces son B-lisos (1)

aunque hay números B-lisos que no son todos. Las potencias de primos solo se van a tachar una vez.

Ahora en vez de tachar, supongamos que dividimos. En este caso los números que reducen a 1 son B-lisos, pero no son todos

P.ej $80 \rightsquigarrow 1$

$60 \rightsquigarrow 2$

Pro~~blem~~

Entonces cambiamos la criba un poco y cribamos por potencias de primos también. Cuando cribamos por 4 sacamos un factor de 2, por 8, otro más, etc... Y los que reducen a 1 son B-lisos.

¿Complejidad?

Para encontrar los números B-lisos $\leq X$ requiere entre

$X \ln \ln B$ divisiones.

Criba cuadrática

Pero no olvidemos que los que queremos no son todos los números B-lisos, sino una lista de la forma $a^2 \pmod N$ que son B-lisos.

Entonces definimos

$$F(T) = T^2 - N$$

y empezamos con $a = \lfloor \sqrt{N} \rfloor + 1$ (porque queremos $a^2 \pmod N$ pequeño).

Consideramos

$$L = F(a), F(a+1), \dots, F(b). \quad (\text{¡no se reducen módulo } N!)$$

y buscamos dos B-lisos cribando los primos $< B$ y fijamos cuales números son la lista $\rightsquigarrow$!

Def. Los primos $< B$ se llama una base de factores (BF).

Supongamos que $p \in BF$. Cuales de los ~~$F(a), F(a+1)$~~, $F(i) \in L$ son divisibles por p?

Sea, cuales t entre a y b cumplen

$$t^2 \equiv N \pmod p ?$$

Si no tiene solución las cortamos ? Si hay una solución, hay dos

$$t = \alpha_p \quad \text{y} \quad t = \beta_p.$$

Entonces $\Rightarrow$

$$F(\alpha_p), F(\alpha_p + p), F(\alpha_p + 2p), \dots$$

$$F(\beta_p), F(\beta_p + p), F(\beta_p + 2p), \dots$$

son $0 \bmod p$.

Ejemplo · $N = 221$

· $a = \lfloor \sqrt{221} + 1 \rfloor = 15$.

· $L = F(15), F(16), F(17), F(18), F(19), F(20)$

$= 4, 35, 68, 103, 140, 179, 220, 263, 308, 355, 404, 455, 508, 563, 620, 679$

1) Criba por 2

2, 35, 34, 103, 70, 179, 110, 263, 154, 355, 202, 455, 254, 563, 310, 679

2) Criba por 3: $\square$ son 1 o $0 \bmod 3$ $((3k)^2, (3k+1)^2, (3k+2)^2)$

$t^2 \equiv 221 \equiv 2 \pmod 3 \Rightarrow$ no hay

3) Criba por 4

= 1, 35, 17, 103, 35, 179, 55, 263, 77, 355, 101, 455, 127, 563, 155, 679

4) $p = 5$ $\quad t^2 \equiv 1 \pmod 5 \Rightarrow t \equiv 1 \pmod 5$ · $t \equiv 4 \pmod 5$

Criba $F(16), F(21), F(26)$ $\quad t \equiv 1 \pmod 5$

$F(19), F(23), F(28)$ $\quad t \equiv 1 \pmod 5$

1, 7, 17, 103, 7, 179, 11, 263, 77, 71, 101, 91, 127, 563, 31, 679

5) Criba por 7: $t^2 \equiv 221 \equiv 4 \pmod 7 \Rightarrow \alpha_7 = 2, \beta_7 \equiv 5 \pmod 7$

1, 1, 17, 103, 1, 179, 11, 263, 11, 71, 101, 13, 127, 563, 31, 97.

Observemos

$$F(15),\ F(16),\ F(19) \rightsquigarrow 1$$
$$4 \quad 35 \quad 140$$

$\Rightarrow$ $F(15) = 15^2 - 221$

$F(16) = 16^2 - 221$

$F(19) = 19^2 - 221$

Estos se factorizan en primos pequeños

En particular

$$15^2 \equiv 2^2 \pmod{221}$$
$$16^2 \equiv 5\cdot 7 \pmod{221}$$
$$19^2 \equiv 2^2 \cdot 5 \cdot 7 \pmod{221}$$

Paso 2

Se sigue que, en particular

$$(16\cdot 19)^2 \equiv (2\cdot 5\cdot 7)^2 \pmod{221}$$

Calculando

$$\gcd(221,\ 16\cdot 19 - 2\cdot 5\cdot 7) = 13$$

Paso 3

un factor no trivial de 221.

Obs: p primo impar $\Rightarrow$ $t^2 \equiv N \pmod p$ tiene 0 o 2 soluciones módulo p.

También ~~este~~ $t^2 \equiv N \pmod{p^e}$ tiene 0 o 2 soluciones

módulo 2 y potencias de 2 es diferente. Se tiene que hacer con un caso particular.

Obs: Hay ideas de como ~~interpretar~~ implementar la criba cuadrática para que sea más rápida. Sigue siendo $\Theta(L(N))$ pero se puede mejorar la constante.