Números lisos, cribas y creando relaciones

Hay tres pasos en muchos métodos de factorización

- Creando relaciones
- Eliminación ← cuadrático
- mcd ← rápido

El primer paso requiere la construcción de muchos números a_i tq $a_i^2 \bmod N$ es el producto de primos pequeños

Def: $n \in \mathbb{N}$ es B-liso si todo p que divide n es $\leq B$

$$\psi(X,B) = \#\{1 < n \leq X : n \text{ es } B\text{-liso}\}$$

¿Cómo comporta este conjunto para X y B grande?

Thm (Canfield, Pomerance, Erdös)

Fijemos $0 < \varepsilon < 1/2$ y supongamos $X, B \to \infty$ tq.

$$(\ln X)^{\varepsilon} < \ln B < (\ln X)^{1-\varepsilon}$$

Si escribimos $u = \dfrac{\ln X}{\ln B}$, tenemos que:

$$\psi(X,B) = X \cdot u^{-u(1+o(1))}$$

$o(1) \to 0$ cuando $X \to \infty$

¿Para B fijo cómo se elige B?

Cor: Si $L(X) = e^{\sqrt{(\log X)(\log\log X)}}$ para todo c fijo $0 < c < 1$,

$$\psi(X, L(X)^c) = X \cdot L(X)^{\left(\frac{1}{2c}\right)(1+o(1))}$$

Rem Si $B = L(x)^c$ y si tomamos $\varepsilon < \frac{1}{2}$,

$$\ln B = c \ln L(x) = c \sqrt{(\log x)(\log\log x)}$$

verifica $(\log x)^2 < \log B < (\log x)^{1-\varepsilon}$ Entonces aplicamos el teorema con

$$u = \frac{\log x}{\log B} = \frac{1}{c} \sqrt{\frac{\log x}{\log\log x}}$$

para deducir que

$$\psi(x, L(x)^c) = x\, u^{-u(1+o(1))}$$

Es muy cuesta verificar que u cumple

$$u^{-u} = L(x)^{-\frac{1}{2c}(1+o(1))}$$

(usar el hecho que $\frac{\log\log\log x}{\log\log x} \to 0$ cuando $x \to \infty$.)

□

La función $L(x) = e^{\sqrt{\ln x \ln\ln x}}$ aparece todo el tiempo cuando uno habla de números lisos. Entonces nos conviene entender cómo $L(x)$ crece como función de x.

Los números lisos aparecen todo el tiempo cuando uno habla de factorización

Def: $f(x), g(x), \quad f, g : \mathbb{R} \to \mathbb{R}^+$

- $f(x) = \Theta(g(x))$ si $\exists\, c, C$ t.q
  $f(x) \leq C g(x) \quad \forall x \geq c$

- $f(x) = \Omega(g(x))$ si $\exists\, c, C$ t.q
  $f(x) \geq C g(x) \quad \forall x \geq c$

- si $f(x) = \Theta(g(x))$ y $f(x) = \Omega(g(x))$, entonces
  $f(x) = \Theta(g(x))$.

Se dice que $f(x)$ crece exponencialmente si existen $\alpha, \beta > 0$ t.q
$$\Omega(x^\alpha) = f(x) = \Theta(x^\beta)$$

Se dice que $f(x)$ crece polinomialmente si $\exists\, \alpha, \beta > 0$ t.q
$$\Omega((\log x)^\alpha) = f(x) = \Theta((\log x)^\beta)$$

Se dice que $f(x)$ es subexponencial si $\forall \alpha > 0$ (se piensa como muy grande) y $\forall \beta > 0$ (se piensa como muy pequeño)
$$\Omega((\ln x)^\alpha) = f(x) = \Theta(x^\beta).$$

La función $L(x) = e^{\sqrt{k \cdot x \ln \ln x}}$ es subexponencial

En el paso de eliminación precisamos más relaciones que (cantidad de los c)

O sea $r >$ (cantidad de los c)

$> \pi(B)$ (cantidad de los primos).

O sea precisamos que haya por lo menos $\pi(B)$ números B-lisos

Prop $L(x) = e^{\sqrt{\ln x \ln\ln x}}$

$N \in \mathbb{Z}$, $N >> 0$

$B = L(N)^{\frac{1}{\sqrt{2}}}$

(a) Tendremos que testear $\approx L(N)^{\sqrt{2}}$ números módulo N para encontrar $\pi(B)$ números B-lisos

(b) Tendremos que testear $\approx L(N)^{\sqrt{2}}$ números de la forma $a^2 \pmod N$ para hayar suficientes números B-lisos para factorizar N

$\Rightarrow$ Los tres pasos toman tiempo subexponencial

Dem: (a) $\Leftrightarrow$ (b) si los L^2 mod N son sucesivamente aleatorios por que para factorizar N precisamos $\pi(B)$ números B-lisos.

Entonces probamos (a).

La probabilidad que N es B-liso es $\frac{\psi(N,B)}{N}$. Entonces para encontrar $\pi(B)$ números B lisos, tenemos que hacer

$$\frac{\pi(B)}{\psi(N,B)/N} \quad (*)$$

Queremos elegir B para minimizar esta función.

El corolario nos dice que

$$\frac{\psi(N, L(N)^c)}{N} \approx L(N)^{-\frac{1}{2c}}$$

Entonces fijamos $B = L(N)^c$ y buscamos el c que minimiza $(*)$

Sabemos que $\pi(B) \approx \frac{B}{\ln B}$, y entonces

$$\frac{\pi(L(N)^c)}{\psi(N, L(N)^c)/N} \approx \frac{L(N)^c}{c \log L(N)} \cdot \frac{1}{L(N)^{-1/2c}} = L(N)^{c+\frac{1}{2c}} \frac{1}{c \ln(L(N))}$$

El término $L(N)^{c+\frac{1}{2c}}$ domina esta expresión, y entonces buscamos el c que minimiza $c + \frac{1}{2c}$. O sea, $c = \frac{1}{\sqrt{2}}$ y el mínimo es $\sqrt{2}$.

□