Complexity of the quadratic sieve.

Canfield, Erdős and Pomerance theorem. (Erdős with $\emptyset \subseteq U \subseteq \mathbb{R}$ in Tex) because he was Hungarian.

Let $\Psi(x,y)$ be the number of $y$-smooth integers in the interval $[1, x]$.

Let $\mu = \ln x / \ln y$. Let $\epsilon \in [0, 1]$ be fixed. There exists a function $\mu$ in $o(1)$ class such that

$$\Psi(x, y) = x \cdot \mu - \mu(1 + \mu(x))$$

wherever $(\ln x)^{\epsilon} < \mu < (\ln x)^{1-\epsilon}$.

**Corollary**

$$L_N(d, c) = \exp \left( \left( c + o(\epsilon) \right) \left( (\ln N)^\alpha (\ln \ln N)^{1-\alpha} \right) \right), \epsilon \in [0, 1], \alpha \in [0, 1]$$

The probability that a number of size $L_N(a, b)$ is $B$-smooth, $B = L_N(c, d)$

$$P = L_N(a-c, (a-c) \frac{b}{d})^{1+o(1)}$$

Useful formula: $L_N(a, c) \cdot L_N(a, c') = L_N(a, c+c')$

A loop of length $L_N(a, c)$ (iterations) where each iteration costs $L_N(a, c+c')$

will take a total time of $L_N(a, c+c')$.

$\alpha = \frac{1}{2}$ for the quadratic sieve. $\Rightarrow e^{(c+o(\epsilon)) \sqrt{\ln N} \ln \ln N}$

What is $c$?

---

**Quadratic sieve:**

A bound on $a$ in $(m+a)^2 - N$

The relation collection takes a time $A$. cost of sieving and finding the factors.

We need $B+1$ relations to get a non-trivial vector in the left kernel.

Big the smoothness bound.

The linear algebra costs $B^2$ with Black-Weisman algorithm.

What is the size of the integers to be factored?

$$(m+a)^2 - N = (\sqrt{N} + a)^2 - N = (\sqrt{N} + a)^2 - a^2 - 2a \sqrt{N} - N$$

$$= N + 2a + 2a \sqrt{N} + a^2 - 2a \sqrt{N} - 2aN - N$$

$$= 2a \sqrt{N} - 2a \sqrt{N} + a^2$$

$$= (\sqrt{N} + c)^2 - a^2 - 2a \sqrt{N} \Rightarrow \leq 2a \sqrt{N}$$

$$N = \exp \left( (1+o(1)) \ln N \ln \ln N \right) = L_N(1, 1)$$
So \( \sqrt{N} = N^{1/2} = \exp(\ln(N^{1/2})) = \exp\left(\frac{1}{2} \ln N\right) = L_N\left(1, \frac{1}{2}\right) \).

2 \( A \sqrt{N} = 2 \ L_N\left(\alpha_A, c_A\right) \ L_N\left(1, \frac{1}{2}\right) \) because \( A \ll \sqrt{N} \), \( \alpha_A < \frac{1}{2} \) and the dominating term is \( L_N\left(1, \frac{1}{2}\right) \).

\[ B = L_N\left(\alpha_B, c_B\right) \]

Canfield-Enflo's -Pomeren -with \( B = L_N\left(\alpha_B, c_B\right) \) on integers of size \( L_N\left(1, \frac{1}{2}\right) \).

\[ P = L_N\left(1-\alpha_B, \frac{1}{2} - \alpha_B\right) \]

\[ = L_N\left(1-\alpha_B, \frac{1}{2C_B}\right) \]

\[ = \frac{1+o(1)}{2C_B} \]

How many relations do we get? The probability times \( A \), for \( 2A \) if uneven \( \frac{1}{2} \).

\[ P - A = L_N\left(1-\alpha_B, \frac{1}{2C_B}\right) \]

\[ \times 2 \]

We need a square matrix, and there are \( B \) columns and \( P \cdot A \) rows:

\[ P \cdot A = B \quad \text{that is,} \quad \max(1-\alpha_B, \alpha_A) = \alpha_B \]

\[ \cdot \text{if} \quad \max(1-\alpha_B, \alpha_A) = \alpha_A \quad \text{then} \quad \alpha_A = \alpha_B \quad \text{and} \quad 1-\alpha_B < \alpha_A \Rightarrow 1 \leq 2\alpha_B \quad \Rightarrow \frac{1}{2} \leq \alpha_B \]

\[ \cdot \text{if} \quad \max(1-\alpha_B, \alpha_A) = 1-\alpha_B \quad \text{then} \quad \alpha_B = 1-\alpha_B \quad \Rightarrow \alpha_B = \frac{1}{2} \]

Cost of mixing: \( L_N\left(\alpha_A, c_A\right) \), cost of linear algebra: \( L_N\left(\alpha_B, 2C_B\right) = B^2 \) because there are \( B \log B \) plane up to \( B \) and the \( \log B \) term disappears (th. of Hadamard (Fr) and De la vallee Poussin (Belgium), on idea of Riemann (Germany)).

Balance both costs:

\[ L_N\left(\alpha_A, c_A\right) = L_N\left(\alpha_B, 2C_B\right) \Rightarrow \alpha_A = \alpha_B, \quad c_A = 2C_B \]

\[ P \cdot A = L_N\left(\frac{1}{2}, -\frac{A}{4C_B} + C_A\right) = B = L_N\left(\frac{1}{2}, C_B\right) \]

\[ \Rightarrow C_A = C_B + \frac{A}{4C_B} \quad \text{minimizing} \quad C_B + \frac{A}{4C_B} \]
22.03.2022.

Let \( f: x \mapsto x + \frac{1}{ax} \) and \( x > 0 \). We search the minimum.

\[
f'(x) = 1 - \frac{1/2}{(ax)^2} = 1 - \frac{1}{2ax^2}
\]

Thus \( f'(x) = 0 \) \( \iff \) \( 1 = \frac{1}{2ax^2} \) \( \iff \) \( 2ax^2 = 1 \) \( \iff \) \( x^2 = 1/2a \)

\[ x = \frac{1}{\sqrt{2a}}. \]

So \( c_B = \frac{1}{\sqrt{2a}} = \frac{1}{2}. \]

Finally, \( c_A = c_B + \frac{1}{4c_B} = \frac{1}{2} + \frac{1}{2} = 1. \)

\( A = L_N\left(\frac{1}{2}, 1\right) \) and \( B = L_N\left(\frac{1}{2}, \frac{1}{2}\right) \)

The line of mixing is \( A = L_N\left(\frac{1}{2}, 1\right) = \exp \left( \frac{-1}{4(1-e)} \ln N \cdot \ln \ln N \right) \)

and the time of linear algebra is \( B^2 = L_N\left(\frac{1}{2}, 1\right) = \) the same expression.