22.03.2022

Complexity of the quadratic sieve.

Canfield, Erdős and Pomerance theorem. (Erdős with \H{o} not \"o in TeX) because he was Hungarian.

Let $\Psi(x,y)$ be the number of y-smooth integers in the interval $[1, x]$. Set $u = \ln x / \ln y$. Let $\varepsilon \in]0,1[$ be fixed. There exists a function μ in $o(1)$ class such that

$$\Psi(x,y) = x\, u^{-u(1+\mu(u))}$$

whenever $(\ln x)^{\varepsilon} < u < (\ln x)^{1-\varepsilon}$.

Corollary $L_N(\alpha, c) = \exp\left((c+o(1))\left((\ln N)^{\alpha}(\ln\ln N)^{1-\alpha}\right)\right)$, $\alpha \in]0,1[$
$\alpha = 0$: polynomial time, $\alpha = 1$: exponential time. $c>0$.

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

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

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

$\to$ a loop of length $L_N(\alpha, c)$ (iterations) where each iteration costs $L_N(\alpha, c')$ will take a total time of $L_N(\alpha, c+c')$.

$\alpha = \frac{1}{2}$ for the quadratic sieve $\to e^{(c+o(1))\sqrt{\ln N \ln\ln N}}$ What is c?

Quadratic sieve:

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

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

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

B is the smoothness bound.

The linear algebra costs B^2 with Block-Wiedeman algorithm.

What is the size of the integers to be factored?

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

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

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

$$= (\sqrt{N}+\varepsilon)(2\varepsilon - 2a) + a^2 - \varepsilon^2 \approx -2a\lceil\sqrt{N}\rceil \to \leq 2A\lceil\sqrt{N}\rceil$$

$N = \exp\left((1+o(1))\ln N(\ln\ln N)^0\right) = L_N(1,1)$

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

$2A\sqrt{N} = 2\, L_N(\alpha_A, c_A)\, L_N(1, \frac{1}{2})$

because $A << \sqrt{N}$, $\alpha_A < 1$ and the dominating term is $L_N(1, \frac{1}{2})$.

$B = L_N(\alpha_B, c_B)$.

Canfield-Erdős-Pomerance with $B = L_N(\alpha_B, c_B)$ on integers of size $L_N(1, \frac{1}{2})$:

$$\mathbb{P} = L_N\left(1-\alpha_B, (1-\alpha_B)\frac{1/2}{c_B}\right)^{-1+o(1)}$$

$$= L_N\left(1-\alpha_B, \frac{-(1-\alpha_B)}{2c_B}\right)^{1+o(1)}$$

How many relation do we get? the probability times A. (or $2A$ if we consider $+/-a$).

$$\mathbb{P}\cdot A = L_N\left(1-\alpha_B, \frac{-(1-\alpha_B)}{2c_B}\right) L_N\left(\alpha_A, c_A\right)$$

We need a square matrix, and there are B columns and $\mathbb{P}\cdot A$ rows:

$\mathbb{P}\cdot A = B$. that is, $\max(1-\alpha_B, \alpha_A) = \alpha_B$

- if $\max(1-\alpha_B, \alpha_A) = \alpha_A$ then $\alpha_A = \alpha_B$ and $1-\alpha_B \leqslant \alpha_B \iff 1 \leqslant 2\alpha_B$ $\iff \frac{1}{2} \leqslant \alpha_B$.
  but we want to minimize the time: $\alpha_B = \alpha_A = 1/2$.
- if $\max(1-\alpha_B, \alpha_A) = 1-\alpha_B$ then $\alpha_B = 1-\alpha_B \iff \alpha_B = 1/2$.

Cost of sieving: $L_N(\alpha_A, c_A)$, cost of linear algebra: $L_N(\alpha_B, 2c_B) = B^2$.

because there are $B/\log B$ primes up to B and the $\log B$ term disapears
(th. of Hadamard (Fr) and De la vallée Poussin (Belgium), on ideas of Riemann (German).

balance both costs:

$$L_N(\alpha_A, c_A) = L_N(\alpha_B, 2c_B) \to \alpha_A = \alpha_B,\ c_A = 2c_B$$

$$\mathbb{P}\cdot A = L_N\left(\frac{1}{2}, \frac{-1}{4c_B} + c_A\right) = B = L_N\left(\frac{1}{2}, c_B\right) \qquad \frac{-1}{4c_B} + c_A = c_B$$

$$\iff c_A = c_B + \frac{1}{4c_B} \qquad \text{minimize } c_B + \frac{1}{4c_B}.$$

22.03.2022.

Let $f : x \longmapsto x + \frac{1}{ax}$ and $x > 0$. We search the minimum.

$$f'(x) = 1 - \frac{1/2\ a}{(ax)^2} = 1 - \frac{1}{2ax^2} \quad f'(x) = 0 \iff 1 = \frac{1}{2ax^2} \iff 2ax^2 = 1 \iff x^2 = 1/2a$$
$$x = 1/\sqrt{2a}.$$

$\rightarrow c_B = 1/\sqrt{4} = 1/2$.

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 time of sieving is $A = L_N\left(\frac{1}{2}, 1\right) = \exp\left(\sqrt{(1+o(1))\ln N \ln\ln N}\right)$

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