Herman te Riele Days

SMOOTH NUMBERS

2 Dec 2011

Marije Elkenbracht-Huizing 14 May 1997

Factoring integers with the Number Field Sieve

Henk Boender 10 June 1997

Factoring large integers with the Quadratic Sieve

Stefi Cavallar 5 June 2002

On the Number Field Sieve Integer Factorisation Algorithm

Willemien Ekkelkamp 20 January 2010

On the amount of sieving in factorization methods

Sieving of <u>(semi)smooth numbers</u>

Psixyology – Pieter Moree

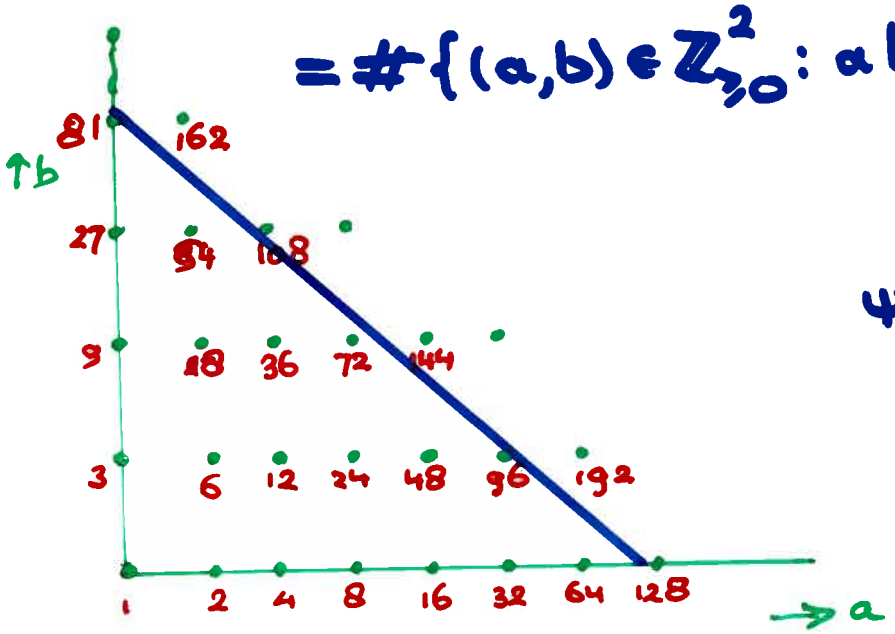
$$P(n) := \max_{p \mid n} p$$ Greatest prime factor of n

$$\psi(x,y) := \#\{1 \le n \le x : P(n) \le y\}$$

$y=2$: $\psi(x,y) = \lfloor {}^{2}\log x \rfloor + 1$

$y=3$: $\psi(x,y) = \#\{1 \le n \le x : n = 2^a \cdot 3^b\}$

$= \#\{(a,b) \in \mathbb{Z}^2_{\ge 0} : a \log 2 + b \log 3 \le \log x\}$



$\psi(100,3)$

$$\psi(x,3) \sim \frac{1}{2} \cdot \frac{\log x}{\log 2} \cdot \frac{\log x}{\log 3}.$$

$y=5$ number of lattice points in tetrahedron

$$\psi(x,5) \sim \frac{1}{3!} \cdot \frac{\log x}{\log 2} \cdot \frac{\log x}{\log 3} \cdot \frac{\log x}{\log 5}.$$

General y $\pi(y)$-dimensional simplex

$$\psi(x,y) \sim \frac{1}{(\pi(y))!} \prod_{p \le y} \frac{\log x}{\log p}.$$

Ennola (1969) Uniformly for $2 \le y \le \sqrt{\log x}$ we have

$$\psi(x,y) = \frac{1}{(\pi(y))!} \prod_{p \le y} \frac{\log x}{\log p} \left\{ 1 + O\left(\frac{y^2}{(\log x)(\log p)} \right) \right\}$$

Beukers (1975) For y fixed

$$\psi(x,y) = \frac{1}{(\pi(y))!} \prod_{p \le y} \frac{\log x}{\log p} \left\{ 1 + \frac{\frac{1}{2}\pi(y) \sum_{p \le y} \log p}{\log x} (1+o(1)) \right\}$$

applying a result of Hardy and Littlewood (1922)

What happens if y is large?

Heuristics

$$\psi(x,y) \sim x \prod_{y < p \le x} \left(1 - \frac{1}{p}\right)$$

is wrong!

$\psi(x,y)$ is much smaller than RHS.

Dickman (1930) Put $u = \dfrac{\log x}{\log y}$.

Then
$$\lim_{y\to\infty} \frac{\psi(x,y)}{x} = \rho(u)$$

~~[illegible]~~ where $\rho(u)$ is the unique continuous solution of
$$u\rho'(u) = -\rho(u-1) \qquad (u>1)$$
with $\rho(u) = 1 \qquad (0 \le u \le 1)$.

E.g. $\psi(x, \sqrt{x}) \sim (1-\log 2)x$.

Dickman function $\rho(u)$ is positive, decreasing for $u>1$, and satisfies
$$\log \rho(u) \sim -u \log u \quad (u\to\infty).$$

Thus
$$\psi(y^u, y) \approx \frac{1}{u!} y^u.$$

De Bruijn (1951)
$$\psi(x,y) = x\rho(u)\left\{1 + O\left(\frac{\log(u+1)}{\log y}\right)\right\}$$
uniformly in the range $y \ge 2$, $1 \le u \le (\log y)^{\frac{3}{5}-\varepsilon}$.

Hildebrand (1986)
$$\ldots \quad 1 \le u \le \exp\{(\log y)^{\frac{3}{5}+\varepsilon}\}.$$

Ramaswami (1949):

$$\psi(x,y) = x\rho(u) + (1-\gamma)\rho(u-1)\frac{x}{\log x} + \frac{c(u)x}{(\log x)^{3/2}}$$

Tenenbaum (2000): for any H

$$\psi(x,y) = \sum_{0\le h\le H} \frac{x\,\phi_h(u)}{(\log x)^h} + O_H\left(\frac{\phi_{H+1}(u)}{(\log x)^{H+1}}\right).$$

Ekkelkamp (2010):

$$\psi(x,y) = x\rho(u) + (1-\gamma)\rho(u-1)\frac{x}{\log x} + O\left(\frac{u^3 x}{(\log x)^2}\right).$$

For y small respect to x good estimates,
for y large totally different good estimates.
What happens in between, $y \sim \log x$ say?

De Bruijn (1966)

$$\log\psi(x,y) = Z\left\{1 + O\left(\frac{1}{\log y} + \frac{1}{\log\log x}\right)\right\}$$

where

$$Z = Z(x,y) = \frac{\log x}{\log y}\log\left(1+\frac{y}{\log x}\right) + \frac{y}{\log y}\log\left(1+\frac{\log x}{y}\right)$$

dominating $\quad$ y larger $\log x$ $\quad$ y smaller $\log x$

$$\operatorname{Log}\psi(x,\log x) \sim 2\,\frac{\log x}{\log\log x}\log 2 \qquad \text{(Erdős)}$$

1986 (Hildebrand & Tenenbaum)

Uniformly in the range $x \geq y \geq 2$, we have

$$\psi(x,y) = \frac{x^{\alpha}\,\zeta(\alpha,y)}{\alpha\sqrt{2\pi\,\phi_2(\alpha,y)}}\left\{1 + O\left(\frac{1}{u} + \frac{\log y}{y}\right)\right\}$$

where $\zeta(s,y) = \prod_{p \leq y} (1-p^{-s})^{-1}$,

$$\phi(s,y) = \log \zeta(s,y),$$

$$\phi_k(s,y) = \frac{d^k}{ds^k}\,\phi(s,y),$$

and $\alpha = \alpha(x,y)$ is the unique solution to the equation

$$-\phi_1(\alpha,y) = \sum_{p \leq y} \frac{\log p}{p^{\alpha}-1} = \log x.$$

If $u \to \infty$ and $y \to \infty$, then $\psi(x,y)$ behaves so regular that you can give an asymptotic formula.

For fixed u $\quad \psi(x,y) \sim x\,\rho(u) \quad \left(u = \frac{\log x}{\log y}\right)$

for $u \to \infty$ no longer proportional to x.

Work of Herman's students

There are not enough smooth numbers for factorization purposes.

Idea: divide out all prime factors $\leq x^{\alpha}$ and allow a remaining 'large' prime $\leq x^{\beta}$ $(\alpha < \beta)$

Bach & Peralta (1996):

$$\psi_1(x, x^{\alpha}, x^{\beta}) = x \int_{\alpha}^{\beta} \rho\left(\frac{1-\lambda}{\alpha}\right) \frac{d\lambda}{\lambda} + O\left(\frac{\log(1/\alpha)}{\alpha(1-\beta)} \frac{x}{\log x}\right)$$

Later: Allow at most 2 primes $\leq x^{\beta}$ (and $> x^{\alpha}$)

Lambert (1996):

$$\psi_2(x, x^{\alpha}, x^{\beta}) = \frac{x}{2} \int_{\alpha}^{\beta}\int_{\alpha}^{\beta} \rho\left(\frac{1-\lambda_1-\lambda_2}{\alpha}\right) \frac{d\lambda_1}{\alpha} \frac{d\lambda_2}{\alpha} + O\left(\cdots \frac{x}{\log x}\right)$$

Later: Allow ≤ 3 primes $\leq x^{\beta}$, others $\leq x^{\alpha}$.

Zhang (2002):

Estimates using recursively defined functions

$$\psi_k(x, x^\alpha, x^\beta) := \#\{n \le x : p_{k+1} \le x^\alpha < p_k \le x^\beta\}$$

where $n = p_1 \cdots p_r$ with $p_1 \ge p_2 \ge \cdots \ge p_r$.

Cavallar (2002):

If $\log x > \frac{1}{\alpha} \max\left(\log 2, \frac{1-k\alpha}{\alpha}, \frac{1}{\log \frac{1}{k\alpha}}\right)$,

then

$$\psi_k(x, x^\alpha, x^\beta) = \frac{x}{k!} \int_\alpha^\beta \cdots \int_\alpha^\beta \rho\left(\frac{1-(\lambda_1+\cdots+\lambda_k)}{\alpha}\right) \frac{d\lambda_1}{\lambda_1} \cdots \frac{d\lambda_k}{\lambda_k}$$

$$+ O\left(\frac{\log^k\left(\frac{1}{k\alpha}\right)}{\alpha(1-k\beta)} \frac{x}{\log x}\right).$$

Ekkelkamp (2010):

$$\cdots \left(1 + O\left(\frac{\log\left(\frac{1}{\alpha}\right)}{\alpha \log x}\right)\right)$$

Here the error term has a small factor $\rho(\cdots)$.

Moreover, Ekkelkamp considered the situation

$\beta_1 > \beta_2 > \cdots > \beta_k > \alpha$, $\quad p_j \le x^{\beta_j}$ for $j = 1, \ldots, k$,

$p_j \le x^\alpha$ for $j > k$.

Moreover, Ekkelkamp computed an error term after two main terms. (For factorized integers second term was 10% of the first term.)

If $0 < \alpha < \beta_k \leq \cdots \leq \beta_1$,

$\alpha + \beta_1 + \cdots + \beta_k \leq$ and $x^\alpha \geq 2$,

then

$$\psi_k(x, x^{\beta_1}, x^{\beta_2}, \ldots, x^{\beta_k}, \alpha) =$$

$$x \int_\alpha^{\beta_k} \int_{\lambda_k}^{\beta_{k-1}} \cdots \int_{\lambda_2}^{\beta_1} \rho\left(\frac{1-(\lambda_1+\cdots+\lambda_k)}{\alpha}\right) \frac{d\lambda_1}{\lambda_1} \cdots \frac{d\lambda_k}{\lambda_k} +$$

$$(1-\gamma)\frac{x}{\log x} \int_\alpha^{\beta_k} \int_{\lambda_k}^{\beta_{k-1}} \cdots \int_{\lambda_2}^{\beta_1} \rho\left(\frac{1-(\lambda_1+\cdots+\lambda_k)-\alpha}{\alpha}\right) \times$$

$$\times \frac{1}{1-(\lambda_1+\cdots+\lambda_k)} \frac{d\lambda_1}{\lambda_1} \cdots \frac{d\lambda_k}{\lambda_k}$$

$$+ O\left(\frac{\log\frac{\beta_1}{\alpha} \cdots \log\frac{\beta_k}{\alpha}}{\alpha^3(1-(\beta_1+\cdots+\beta_k))^2} \cdot \frac{x}{(\log x)^2}\right).$$