C.I.R.M. Théorie des Nombres et applications 14/18 janvier 2002

Some applications of computers to Number Theory

Marc Deléglise

17 janvier 2002, 60 ans de J.L Nicolas

deleglise@euler.univ-lyon1.fr

M. Deléglise, J. Rivat et X. Roblot remercient Jean-Louis Nicolas pour sa gentillesse, son optimisme, et ses encouragements.
Dès son arrivée à Lyon, il a réussi à mettre en place d'excellentes conditions de travail, et développé l'utilisation des ordinateurs en Théorie des Nombres. Les travaux présentés ci dessous, lui doivent beaucoup.

Recouvrement optimal du cercle par les multiples d'un intervalle

Problem : Let h be a positive integer, find an interval I on the torus $\mathbb{R}/\mathbb{Z}$, as short as possible, such that $I, 2I, \ldots, hI$ cover the whole of the torus. Let $L(h)$ and $\alpha(h)$ the length and the origin of I.

Origin : An additive number theory problem about asymptotic bases. (Erdős-Graham 1980).

G. Grekos proved that $L(h)$ is bounded by

$$L(h) \leq \frac{3}{h^2}(1 + o(1))$$

and conjectured with J.M. Deshouillers that

this bound is the best possible.

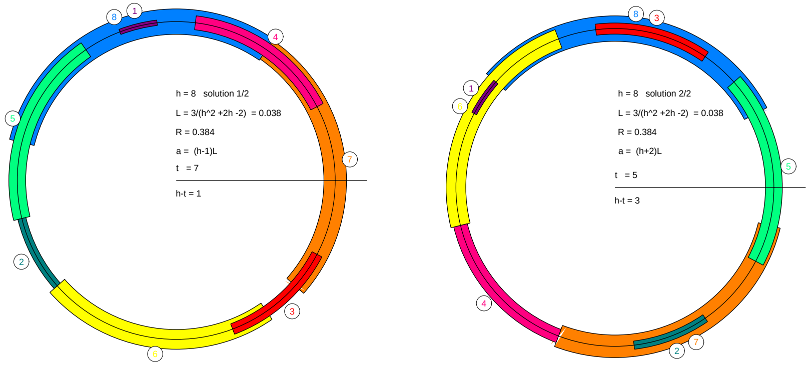

Figure: Recouvrement optimal du cercle : les deux solutions pour $h = 8$

It is easy to prove that the $L(h)$ and $\alpha(h)$ are rational numbers with relatively small numerators, and not too large denominators. Starting from this, we computed $L(h)$, for $1 \leq h \leq 35$, and found that

$$L(h) = \begin{cases} \dfrac{3}{h^2 + 2h} & \text{when} \quad h \equiv 0, 1 \pmod 3 \\ \dfrac{3}{h^2 + 2h - 2} & \text{when} \quad h \equiv 2 \pmod 3 \end{cases} \quad \text{Deléglise (1991).}$$

That simple formula depending only on the class of h modulo 3 suggests the existence of an arithmetic proof. Indeed, we proved it, using the three-distance theorem.

Computing large values of $M(x), \Psi(x), \pi(x)$ in $O\left(x^{2/3\pm\epsilon}\right)$

Exercice : How to compute efficiently a sum like

$$\sum_{n\leq x} f\left(\left[\frac{x}{n}\right]\right)$$

Solution : There are at most $2\sqrt{x}-1$ different values for $\left[\frac{x}{n}\right]$.

Cost of this computation : (when the computation of one value of f is $O(1)$)

$$O(\sqrt{x}) \quad \text{instead of} \quad O(x).$$

Computation of $M(x)$

Let

$$M(x) = \sum_{n \le x} \mu(n)$$

denote the summatory function of Möbius function.

$\lim_{x \to \infty} M(x)/x = 0$ is equivalent to the Prime Number Theorem.

Mertens conjectured that $M(x) \le \sqrt{x}$. That was disproved by Odlyzko and Te Riele (1985).

Computation of one single value of $M(x)$

F. Dress	$O\left(x^{3/4}\right)$	(1993)
Deléglise-Rivat	$O\left(x^{2/3}\right)$	(1996)

$$M(x) = M(u) - \sum_{m\le u} \mu(m) \sum_{\frac{u}{m}\le n\le \frac{x}{m}} M\left(\frac{x}{mn}\right)$$

The inner sum is a sum of the type

$$\sum_{n\le y} f\left(\left[\frac{y}{n}\right]\right) \quad \text{with } f = M, \quad y = \frac{x}{m}.$$

Choose $u = x^{1/3}$. After sieving the whole interval $[1, x^{2/3}]$, $O(x^{2/3}\log\log x)$ operations, each value $M\left(\frac{x}{mn}\right)$ is obtained with cost $O(1)$. So the inner sum is computed in time

$$\sum_{1\le m\le x^{1/3}} \sqrt{\frac{x}{m}} = O(x^{2/3})$$

and the total cost is

$$O(x^{2/3}\log\log x), \quad \text{Deléglise-Rivat (1996).}$$

With the same ideas, using the following formula of Vaughan :

$$\psi(x) = \sum_{n \le u} \Lambda(n) + \sum_{\substack{m \le u \\ mn \le x}} \mu(m) \ln n + \sum_{\substack{l \le u \\ m \le u}} \mu(l)\Lambda(m) \left[\frac{x}{lm}\right] + \sum_{\substack{u < m \le x \\ u < n \le x \\ mn \le x}} \Lambda(m) \sum_{\substack{d | n \\ d \le u}} \mu(d)$$

we can compute $\psi(x)$ in time $O(x^{2/3+\epsilon})$ (Deléglise-Rivat 1998).

Computation of $\pi(x)$

Let $x \in \mathbb{R}$ and $b \in \mathbb{N}$. Define

$$F(x,b) = \mathrm{card}\{n \le x, \quad p \mid n \implies p > p_b\}$$

$F(x,b)$ is the number of integers that remain after sieving the interval $[1, x]$ by the b first prime numbers $p_1, p_2, \dots, p_b$. Denote also

$$P_2(x,b) = \text{card}\{n \ ; \ n \le x; \ n = p_i p_j, \quad p_i, p_j > p_b\}.$$

Choose $a = \pi(x^{1/3})$, and sieve $[1, x]$ by $p_1, \dots, p_a$. Partitioning the integers that remain according to the number of their prime factors, we get

$$F(x,a) = \underbrace{1}_{0 \text{ prime}} + \underbrace{\pi(x) - a}_{1 \text{ prime}} + \underbrace{P_2(x,a)}_{2 \text{ primes}},$$

and Meissel's formula :

$$\pi(x) = F(x,a) + a - 1 - P_2(x,a).$$

The easy part. We have to count the couples of primes (p, q) such that

$$x^{1/3} < p \leq q \quad \text{and} \quad pq \leq x.$$

The primes p satisfy $y < p \leq x^{1/2}$, and for each value of p, q satisfies $p \leq q \leq x/p$. Henceforth

$$P_2(x, a) = \sum_{x^{1/3} < p \leq \sqrt{x}} \left[\pi\left(\frac{x}{p}\right) - (\pi(p) - 1) \right]$$

Computation: Sieve the interval $[1, x^{2/3}]$.
Cost of this computation :

$$O\left(x^{2/3} \log\log x\right)$$

Recurrence formula for $F(x, b)$.

Partitioning the integers less than x counted by $F(x, b)$ in two classes

1. the ones that are multiple of p_{b+1},
2. the ones that are not multiple of p_{b+1}.

We get the formula

$$\begin{aligned} F(x, 0) &= [x] \\ F(x, b+1) &= F(x, b) - F\left(\frac{x}{p_{b+1}}, b\right) \end{aligned}$$

Computation of $F(x, a)$

To compute $F(x, a)$, there are two opposite extreme ways:

1. To sieve the whole interval $[1, x]$ by all the primes $2, 3, \ldots, p_a$
2. To use only the recurrence equation.

Both of these methods cost more than $x^{1-\epsilon}$.

The new idea, introduced by Lagarias, Miller, Odlyzko, is to mix both methods to get an $O\left(x^{2/3}/\log x\right)$ algorithm (1985).

Improvement in $O\left(x^{2/3}/\log^2 x\right)$

A careful analysis of LMO's algorithm shows that the essential part of the computation's time is the computation of the sum

$$\sum_{x^{1/4}\le p<x^{1/3}} \quad \sum_{p<q\le \min(x/p^2, x^{1/3})} \pi\left(\frac{x}{pq}\right)$$

The inner sum is of the type $\sum f(x/n)$. For each fixed value of p, the different values $\pi(x/pq)$ are much fewer that the number of values of q. Speeding up the computation of this sum with the same trick than before, the total cost becomes

$$O\left(x^{2/3}/\log^2 x\right) \quad \text{Deléglise, Rivat(1996),}$$

gaining a factor $\log x$, and the value

$$\pi(10^{18}) = 24\ 739\ 954\ 287\ 740\ 860.$$

Counting primes in arithmetic progressions

P. Dusard noticed that Meissel's formula can be adapted to the computation of

$$\pi(x, k, l)$$

the number of primes congruent to l mod k up to x.
With X.-F. Roblot, we wrote a program and computed values of $\pi(x, 4, 1)$ and $\pi(x, 4, 3)$ for x up to 10^{20}.

The difference

$$\delta(x) = \pi(x, 4, 3) - \pi(x, 4, 1)$$

has an infinity of changes of sign (Littlewood (1914)). Nevetherless it is more often positive than negative. Until recently, there were only 7 regions known (up to 10^{12}) where $\delta(x) < 0$. We found 2 new regions, one around $9 \cdot 10^{12}$, and the other one around 10^{18}.

x	$\pi(x,4,1)$	$\pi(x,4,3)$	$\delta(x)$
10^9	25 423 491	25 424 042	551
10^{10}	227 523 275	227 529 235	5 960
10^{11}	2 059 020 280	2 059 034 532	14 252
10^{12}	18 803 924 340	18 803 987 677	63 337
10^{13}	173 032 709 183	173 032 827 655	118 472
10^{14}	1 602 470 783 672	1 602 470 967 129	183 457
10^{15}	14 922 284 735 484	14 922 285 687 184	951 700
10^{16}	139 619 168 787 795	139 619 172 246 129	3 458 334
10^{17}	1 311 778 575 685 086	1 311 778 581 969 146	6 284 060
10^{18}	12 369 977 142 579 584	12 369 977 145 161 275	2 581 691
10^{19}	117 028 833 597 800 689	117 028 833 678 543 917	80 743 228
10^{20}	1 110 409 801 150 582 707	1 110 409 801 410 336 132	259 753 425

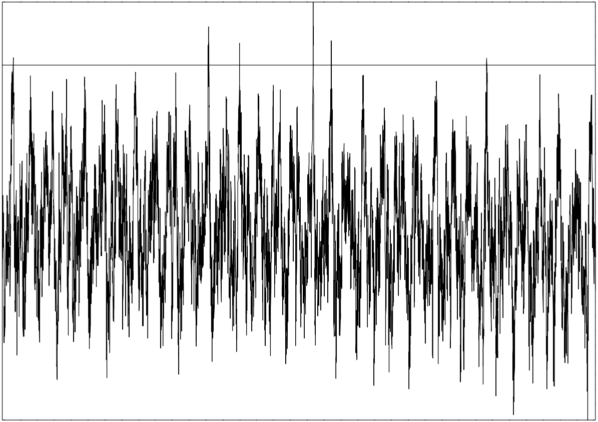

Figure: Graph of $\delta(\log 10)(x))/(\ sqrt x \ln x)$ for $1 \leq \log_{10}(x) \leq 18.2$.

Density of abundant integers

$\sigma(n)$ denotes the sum of all divisors of $n \in \mathbb{N}$.
n is abundant if

$$\sigma(n) \geq 2n,$$

(more generally n is α−abundant if $\sigma(n)/n \geq \alpha$). The proportion of abundant numbers between 1 and x has a limit when $x \to \infty$ (Davenport 1933)

$$A(2) = \lim_{x \to \infty} \frac{1}{x} \mathrm{card}\,\{n \leq x;\ n \text{ abundant}\}$$

But it is strange that this constant is difficult to compute.

$0.241 < A(2) < 0.314$	Behrend (1933)
$0.244 < A(2) < 0.291$	Wall (1972)
$0.2474 < A(2) < 0.2480$	Deléglise (1996)

A good method is still to be found.