Factorisation d'entiers

Francesco Pappalardi

Théorie des nombres et algorithmique

15-26 novembre, Bamako (Mali)

Quelle est la taille des "grands nombres"

- NOMBRE DE COMBINAISONS À LA LOTERIE: 622.614.630
- NOMBRE DE CELLULES DANS UN CORPS HUMAIN: 10^{15}
- NOMBRE D'ATOMES DANS L'UNIVERS: 10^{80}
- NOMBRE DE PARTICULES SUBATOMIQUES: 10^{120}
- NOMBRE D'ATOMES DANS LE CERVEAU HUMAIN: 10^{27}
- NOMBRE D'ATOMES DANS UN CHAT: 10^{26}

$$
\begin{aligned}
RSA_{2048} = {} & 25195908475657893494027183240048398571429282126204 \\
& 032027777137836043662020707595556264018525880784406918290641249 \\
& 515082189298559149176184502808489120072844992687392807287776735 \\
& 971418347270261896375014971824691165077613379859095700097330459 \\
& 748808428401797429100642458691817195118746121515172654632282216 \\
& 869987549182422433637259085141865462043576798423387184774447920 \\
& 739934236584823824281198163815010674810451660377306056201619676 \\
& 256133844143603833904414952634432190114657544454178424020924616 \\
& 515723350778707749817125772467962926386356373289912154831438167 \\
& 899885040445364023527381951378636564391212010397122822120720357
\end{aligned}
$$

RSA_{2048} est un nombre avec 617 chiffres (décimaux)

`http://www.rsa.com/rsalabs/challenges/factoring/challengenumbers.txt`

$$RSA_{2048}{=}p\cdot q,\qquad p,q\approx 10^{308}$$

$\boxed{\textbf{PROBLEME: it Calculer } p \textbf{ et } q}$

PRIX: 200.000 US\$ ($\sim$ 94.580.000 XOF)!!

Théorème. Si $a\in\mathbb{N}$, il ya $p_1<p_2<\cdots<p_k$ *premier* unique telle que $a=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$

Malheureusement: RSAlabs estime que l'affacturage en un an nous avons besoin:

nombre	ordinateurs	mémoire
RSA_{1620}	1.6×10^{15}	120 Tb
RSA_{1024}	$342,000,000$	170 Gb
RSA_{760}	215,000	4Gb.

`http://www.rsa.com/rsalabs/challenges/factoring/challengenumbers.txt`

Nombre	Prix ($US)
RSA_{576}	\$10,000
RSA_{640}	\$20,000
RSA_{704}	\$30,000
RSA_{768}	\$50,000
RSA_{896}	\$75,000
RSA_{1024}	\$100,000
RSA_{1536}	\$150,000
RSA_{2048}	\$200,000

`http://www.rsa.com/rsalabs/challenges/factoring/challengenumbers.txt`

Nombre	Prix ($US)	Etat
RSA_{576}	\$10,000	Factorizé Décembre 2003
RSA_{640}	\$20,000	Factorizé Novembre 2005
RSA_{704}	\$30,000	pas factorizé
RSA_{768}	\$50,000	pas factorizé
RSA_{896}	\$75,000	pas factorizé
RSA_{1024}	\$100,000	pas factorizé
RSA_{1536}	\$150,000	pas factorizé
RSA_{2048}	\$200,000	pas factorizé

Célèbre citation!!!

Un phénomène dont la probabilité est 10^{-50} *ne se produira jamais, et moins sera jamais observé.*

- Émil Borel (La probabilités et sa vie)

L'École d'Athènes (Raffaello Sanzio)

Euclide d'Alexandrie

Naissance: 325 avant JC (Approx.)

Décès: 265 avant JC (Approx.)

Il ya une infinité de nombres premier!!

Etat de "l'art de la factorisation"

220AC (Ératosthène de Cyrène)

Etat de "l'art de la factorisation"

1730 Euler $2^{2^5} + 1 = 641 \cdot 6700417$

Comment avez Euler factorisé $2^{2^5}+1$?

PROPOSITION *Supposons quw $p \mid b^n+1$. Il s'ensuit que*

1. $p \mid b^d+1$ *pour certains diviseur propre d de n tel que n/d est impair, ou bien*
2. $p \equiv 1 \bmod 2n$.

Application. Soit $b=2$ et $n=2^5=64$. Alors $2^{2^5}+1$ est soit an nombre premier ou bien est divisible par un nombre premier $p \equiv 1 \bmod 128$.

Notez que
$1+1\times 128 = 3\times 43$, $1+2\times 128=257$ est premier,
$1+3\times 128 = 5\times 7\times 11$, $1+4\times 128 = 3^3\times 19$ et $1+5\cdot 128 = 641$ est premier.

Enfin

$$\frac{2^{2^5}+1}{641} = \frac{6700417}{641} = 6700417$$

.

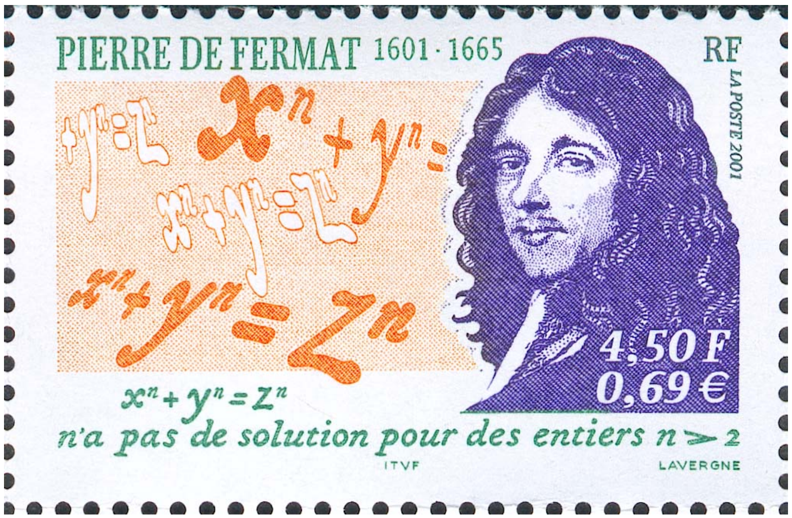
Etat de "l'art de la factorisation"

1730 Euler $2^{2^5} + 1 = 641 \cdot 6700417$

Etat de "l'art de la factorisation"

1750–1800 Fermat, Gauss (Cribles - Tableaux)

Etat de "l'art de la factorisation"



1750–1800 Fermat, Gauss (Cribles - Tableaux)

Premier algorithme de factorisation par crible $N = x^2 - y^2 = (x - y)(x + y)$

Etat de "l'art de la factorisation"

- 220AC (Ératosthène de Cyrène)
- 1730 Euler $2^{2^5}+1 = 641 \cdot 6700417$
- 1750–1800 Fermat, Gauss (Cribles - Tableaux)
- 1880 Landry & Le Lasseur:

$$2^{2^6}+1 = 274177 \times 67280421310721$$

- 1919 Pierre et Eugène Carissan (Machine pour Factoriser)

Ancien Machine pour factoriser dei Carissan

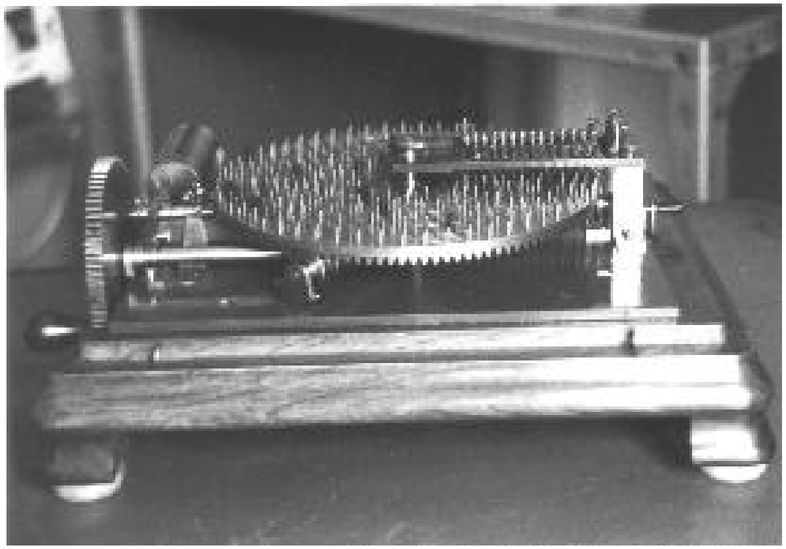


Figure 1: Conservatoire Nationale des Arts et Métiers in Paris

`http://www.cs.uwaterloo.ca/~shallit/Papers/carissan.html`

Figure 2: Lieutenant Eugène Carissan

$225058681 = 229 \times 982789$	2 minutes
$3450315521 = 1409 \times 2418769$	3 minutes
$3570537526921 = 841249 \times 4244329$	18 minutes

Etat de "l'art de la factorisation"

- 220AC (Ératosthène de Cyrène)
- 1730 Euler $2^{2^5}+1=641\cdot 6700417$
- 1750–1800 Fermat, Gauss (Cribles - Tebleaux)
- 1880 Landry & Le Lasseur:

$$2^{2^6}+1=274177\times 67280421310721$$

- 1919 Pierre et Eugène Carissan (Machine pour Factoriser)
- 1970 Morrison & Brillhart

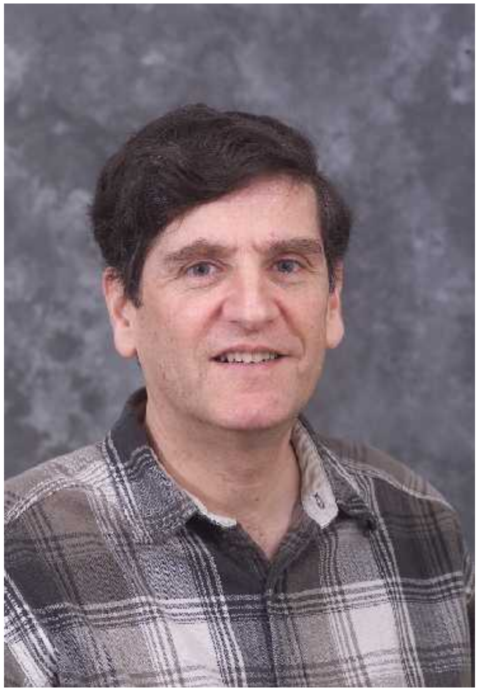
$$2^{2^7}+1=59649589127497217\times 5704689200685129054721$$

Etat de "l'art de la factorisation"

1970 - John Brillhart & Michael A. Morrison

$$2^{2^7}+1 = 59649589127497217 \times 5704689200685129054721$$

Etat de "l'art de la factorisation"



1982 - Carl Pomerance - Le Crible Quadratique

Etat de "l'art de la factorisation"

- 220AC (Ératosthène de Cyrène)
- 1730 Euler $2^{2^5} + 1 = 641 \cdot 6700417$
- 1750–1800 Fermat, Gauss (Cribles - Tebleaux)
- 1880 Landry & Le Lasseur:
$$2^{2^6} + 1 = 274177 \times 67280421310721$$
- 1919 Pierre et Eugène Carissan (Machine pour Factoriser)
- 1970 Morrison & Brillhart
$$2^{2^7} + 1 = 59649589127497217 \times 5704689200685129054721$$
- 1982 Crible Quadratique **QS** (Pomerance) $\rightsquigarrow$ Crible del sur corps numèrique **NFS**
- 1987 Factorisation avec Courbes Elliptiques **ECF** (Lenstra)

Etat de "l'art de la factorisation"

1987 - Hendrik Lenstra - Factorisation avec courbes elliptiques

Factorisation Contemporanea

❶ 1994, Crible Quadratique (QS): (8 mois, 600 volontaires, 20 Nations)
D.Atkins, M. Graff, A. Lenstra, P. Leyland

$$RSA_{129} = 114381625757888867669235779976146612010218296721242362562561842935706\\ 935245733897830597123563958705058989075147599290026879543541 =\\ = 3490529510847650949147849619903898133417764638493387843990820577 \times\\ 32769132993266709549961988190834461413177642967992942539798288533$$

❷ (2 Février 1999), Crible sur corps numèrique (NFS): (160 Sun, 4 mois)

$$RSA_{155} = 109417386415705274218097073220403576120037329454492059909138421314763499842\\ 8893478471799725789126733249762575289978183379707653724402714674353159335433 3897 =\\ = 102639592829741105772054196573991675900716567808038066803341933521790711307779 \times\\ 106603488380168454820927220360012878679207958575989291522270608237193062808643$$

❸ (3 Décembre, 2003) (NFS): J. Franke et al. (174 chiffres décimal)

$$RSA_{576} = 1881988129206079638386972394616504398071635633794173827007633564229888597152346\\ 65485319060606504743045317388011303396716199692321205734031879550656996221305168759307650257059 =\\ = 398075086424064937397125500550386491199064362342526708406385189575946388957261768583317 \times\\ 472772146107435302536223071973048224632914695302097116459852171130520711256363590397527$$

❹ Factorisation avec courbes elliptiques: mis en place par H. Lenstra.
convenient pour trouver des petits factors (50 chiffres)

Tous: "complexité sous–exponentielle"

La factorisation de RSA_{200}

RSA_{200} = 27997833911221327870829467638722601621070446786955428537560009929326128400107609345671052955360856061822351910951365788637105954482006576775098580557613579098734950144178863178946295187237869221823983

Date: Mon, 9 May 2005 18:05:10 +0200 (CEST) From: "Thorsten Kleinjung" Subject: rsa200

We have factored RSA200 by GNFS. The factors are

3532461934402770121272604978198464368671197400197625023649303468776121253679423200058547956528088349

and

7925869954478333033347085841480059687737975857364219960734330341455767872818152135381409304740185467

We did lattice sieving for most special q between 3e8 and 11e8 using mainly factor base bounds of 3e8 on the algebraic side and 18e7 on the rational side. The bounds for large primes were 2^{35}. This produced 26e8 relations. Together with 5e7 relations from line sieving the total yield was 27e8 relations. After removing duplicates 226e7 relations remained. A filter job produced a matrix with 64e6 rows and columns, having 11e9 non-zero entries. This was solved by Block-Wiedemann.

Sieving has been done on a variety of machines. We estimate that lattice sieving would have taken 55 years on a single 2.2 GHz Opteron CPU. Note that this number could have been improved if instead of the PIII- binary which we used for sieving, we had used a version of the lattice-siever optimized for Opteron CPU's which we developed in the meantime. The matrix step was performed on a cluster of 80 2.2 GHz Opterons connected via a Gigabit network and took about 3 months.

We started sieving shortly before Christmas 2003 and continued until October 2004. The matrix step began in December 2004. Line sieving was done by P. Montgomery and H. te Riele at the CWI, by F. Bahr and his family.

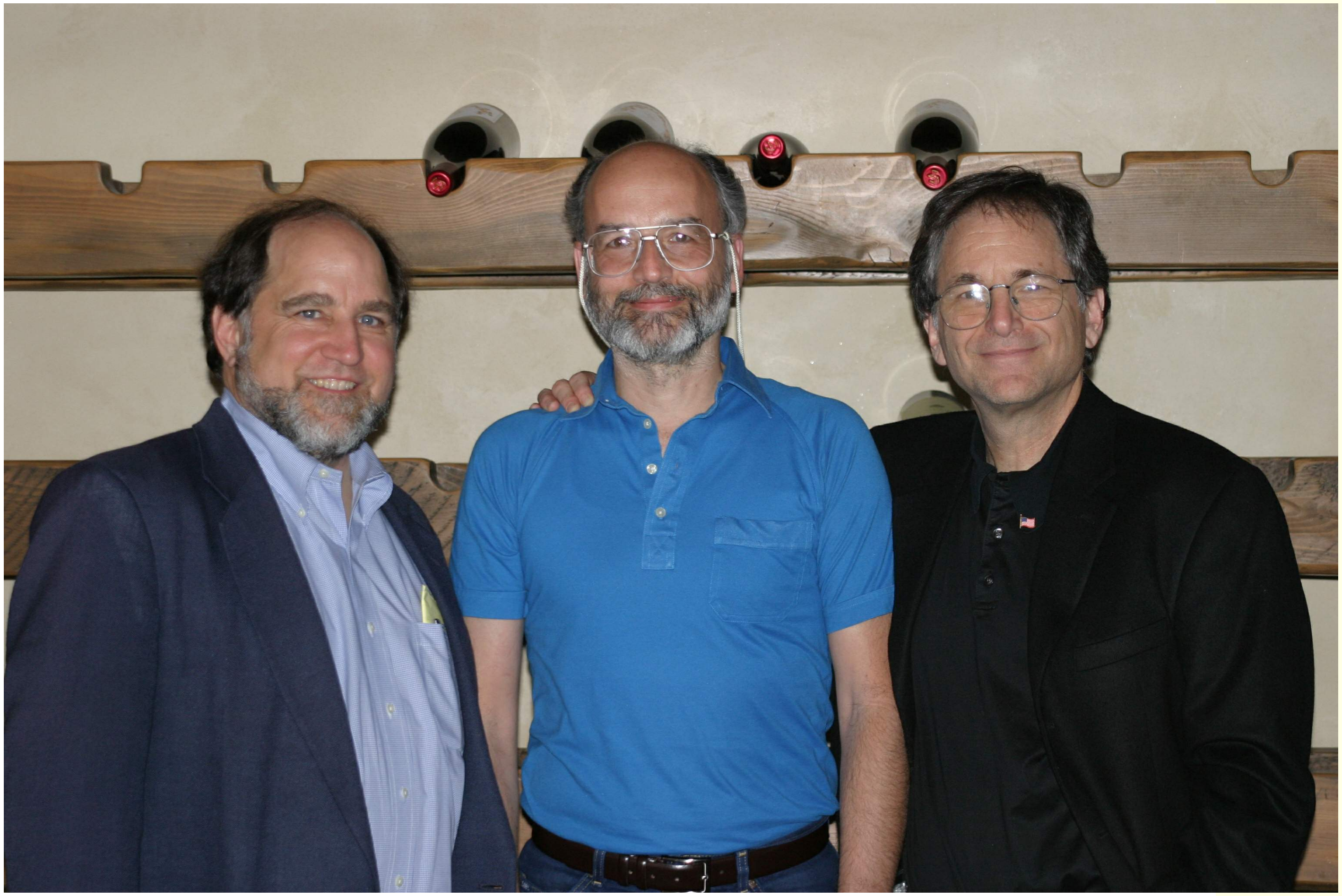
More details will be given later.

F. Bahr, M. Boehm, J. Franke, T. Kleinjung

RSA

Adi Shamir, Ron L. Rivest, Leonard Adleman (1978)

RSA



Ron L. Rivest, Adi Shamir, Leonard Adleman (2003)

Problème: Étant donné $n \in \mathbb{N}$, trouver un diviseur propre de

- Un problème très ancien et tres difficile;
- Trial division requires $O(\sqrt{n})$ division which is an exponential time (i.e. impractical)
- Plusieurs algorithmes différents
- nous passons en revue la méthode élégante de Pollard (métode ρ).

Suppose n is not a power and consider the function:

$$f : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}, \quad x \mapsto f(x) = x^2 + 1.$$

The k-th iterate of f is $f^k(x) = f^{k-1}(f(x))$ with $f^1(x) = f(x)$.

If $x_0 \in \mathbb{Z}/n\mathbb{Z}$ is chosen "sufficiently randomly", the sequence $\{f^k(x_0)\}$ behaves as a random sequence of elements of $\mathbb{Z}/n\mathbb{Z}$ and we exploit this fact.

Pollard ρ factoring method

```
Input:   n ∈ ℕ odd and not a perfect power (to be factored)
Output:  a non trivial factor of n
1.  Choose at random x ∈ ℤ/nℤ = {0, 1, ..., n − 1}
2.  For i = 1, 2 ....
            g := gcd(f^i(x) − f^{2i}(x), n)
            If g = 1, goto next i
            If 1 < g < n then output g and halt
            If g = n then go to Step 1 and choose another x.
```

What is going on here?

Is is obviously a probabilistic algorithm but it is not even clear that it will ever terminate.

But in fact it terminates with complexity $O(\sqrt[4]{n})$ which is attained in the worst case (i.e. when n is an RSA module (for RSA see course in Cryptography by K. Chakraborty).

The birthday paradox

Elementary Probability Question: *what is the chance that in a sequence of k elements (where repetitions are allowed) from a set of n elements, there is a repetition?*

Answer: The chance is $1 - \frac{n!}{n^k(n-k)!} \approx 1 - e^{-k(k-1)/2n}$

In a party of 23 friends there 50.04% chances that 2 have the same birthday!!

Relevance to the ρ-Factoring method:

If d is a divisor of n, then in $O(\sqrt{d}) = O(\sqrt[4]{n})$ steps there is a high chance that in the sequence $\{f^k(x_0) \bmod d\}$ there is a repetition modulo d.

REMARK (WHY ρ). If $y_1, \ldots, y_m, y_{m+1}, \ldots, y_{m+k} = y_m, y_{m+k+1} = y_{m+1}, \ldots$. and i is the smallest multiple of k with $i \geq m$, then $y_i = y_{2i}$ (the Floyd's cycle trick).

Références pour ce cours

[1] J. Buhler & S. Wagon *Basic algorithms in number theory* Algorithmic Number Theory, MSRI Publications Volume **44**, 2008 http://www.msri.org/communications/books/Book44/files/02buhler.pdf

[2] C. Pomerance *Smooth numbers and the quadratic sieve* Algorithmic Number Theory, MSRI Publications Volume **44**, 2008 http://www.msri.org/communications/books/Book44/files/03carl.pdf

[3] R. Crandall and C. Pomerance, *Prime numbers*, 2nd ed., Springer-Verlag, New York, 2005.

[4] E. Bach and J. Shallit, *Algorithmic number theory, I: Efficient algorithms*, MIT Press, Cambridge, MA, 1996.

[5] J. von zur Gathen and J. Gerhard, *Modern computer algebra*, 2nd ed., Cambridge University Press, Cambridge, 2003.

[6] V. Shoup, *A computational introduction to number theory and algebra,* Cambridge University Press, Cambridge, 2005.

[7] These notes http://www.mat.uniroma3.it/users/pappa/bamako2010_A.pdf