ACTUALITÉ MATHÉMATIQUE : LA FACTORISATION COMPLÈTE DU NEUVIÈME NOMBRE DE FERMAT

Jean-Pierre FRIEDELMEYER

La récente médiatisation qu'a connue la démonstration par A. Wiles du dernier théorème de Fermat (1) est plutôt rare pour un résultat mathématique. Cette démonstration, si elle s'avère définitivement correcte, ne clôt pourtant pas les travaux suscités par ce grand mathématicien, dont certains continuent à stimuler diverses activités de recherche certes moins éclatantes mais parfois plus utiles. Parmi celles-ci, certaines ont des retombées directement utilisables dans des domaines non mathématiques, par exemple pour les problèmes de cryptographie, c'est-à-dire de messages codés. Les milieux financiers, politiques ou militaires ont besoin de codes secrets qui résistent à la puissance de calcul des ordinateurs actuels. Or une nouvelle méthode dite à "clef publique" a été inventée en 1975 par un groupe de trois personnes : Rivest, Shamir et Adleman qui satisfait parfaitement à cette exigence (2). Cette performance tient au fait que l'on connaît ajourd'hui de très grands nombres premiers, mais qu'il est pratiquement impossible (c'est-à-dire dans un délai raisonnable) de trouver les facteurs premiers p et q d'un nombre $N = p \times q$ lorsque N est très grand (plus d'une centaine de chiffres décimaux). Une excellente illustration de cette difficulté nous est fournie par la toute récente décomposition en facteurs premiers du nombre dit de Fermat $F_9 = 2^{2^9} + 1$, qui a 155 chiffres décimaux.

1. Les nombres de Fermat

Les nombres de Fermat sont les nombres de la forme $F_n = 2^{2^n} + 1$ où n est un entier naturel. Fermat les croyait tous premiers :

"*Je suis quasi persuadé que tous les nombres progressifs augmentés de l'unité, desquels les exposants sont des nombres de la progression double, sont des nombres premiers comme 3, 5, 17, 257, 65537, 4294967297 et le suivant de 20 lettres 18446744073709551617; etc...*

Je n'en ai pas la démonstration exacte, mais j'ai exclu si grande quantité de diviseurs par démonstrations infaillibles, et j'ai de si grandes lumières qui établissent ma pensée, que j'aurais peine à me dédire" (3).

---

(1) Voir l'article de N. Schappacher dans '*L'Ouvert*' n° 73 : "Les 350 ans du grand théorème de Fermat".

(2) Voir l'article de M. Mignotte dans '*L'Ouvert*' n° 18 : "Transmission des messages secrets grâce à l'arithmétique".

(3) Lettre de Fermat à Frénicle (août 1640) dans P. Fermat, Oeuvres X LIII, p. 205-206.

effectivement F_n est premier pour $n \leq 4$ mais en 1732 Euler a démontré que F_5 est composé :

$$F_5 = 4.294967297 = 641 \times 6700417.$$

En 1801 Gauss a mis en évidence l'intérêt des nombres de Fermat en géométrie : un polygone régulier de N côtés peut être construit à la règle et au compas si et seulement si N est une puissance de 2 ou le produit d'une puissance de 2 et de nombres de Fermat premiers distincts. Il en est ainsi pour $N = 17 = F_2$ ou $N = 340 = 2^2 \times 5 \times 17 = 2^2 \times F_1 \times F_2$, mais pas pour $N = 7$ ou $N = 13$.

Comme le montre l'écriture décimale de F_5 ou F_6 ci-dessus, les nombres de Fermat deviennent vite très grands. Comment savoir s'ils sont premiers ou non ?

2. Les connaissances actuelles sur les facteurs premiers composant F_n.

Il faut attendre 1877 pour obtenir deux résultats importants concernant les diviseurs éventuels de F_n. Le premier est publié par E. Lucas qui démontre que pour $n > 1$, tout diviseur de F_n est de la forme $2^{n+2} \times k + 1$ ($k \in \mathbb{N}$). Ainsi pour $n = 5$, $641 = 2^7 \times 5 + 1$ divise F_5, de même que l'autre facteur $6700417 = 2^7 \times 52347 + 1$. Ce sont probablement des diviseurs de ce type qu'Euler a essayé, puisque dans une publication datée en 1747 nous trouvons énoncé le résultat suivant :
"*Tout diviseur de F_n est de la forme* $2^{n+1} \times k + 1$"

Le second résultat est un test remarquable, le test de Pépin, qui permet de savoir si F_n est premier ou composé :
"*F_n est premier si et seulement si il divise* $3^{\frac{F_n-1}{2}} + 1$"

Ce test demande néanmoins du temps pour être appliqué, car déjà F_n est grand, combien plus grand encore est $3^{\frac{F_n-1}{2}}+1$! Par exemple F_{1945} est un nombre si grand qu'il faut plus de 580 chiffres pour écrire le nombre de ses chiffres. Et pourtant le test de Pépin lui fut appliqué avec succès, et en 1957, R.-M. Robinson découvrit que $5 \times 2^{1947} + 1$ divise F_{1945}. Aujourd'hui, le plus grand nombre de Fermat connu comme composé est F_{23471}. En 1984, Keller en avait trouvé un diviseur premier, le nombre $5 \times 2^{23473} + 1$. L'on conjecture qu'il n'existe pas de nombre de Fermat premier au-delà de l'indice $n = 4$.

Mais savoir que F_n est composé ne signifie pas pour autant qu'on connaisse des diviseurs, encore moins **tous ses diviseurs premiers**. Ainsi nous ne connaissons l'ensemble des diviseurs de F_7 que depuis 1970 (Morrison et Brillhart). Pour F_9, Western avait déterminé en 1903 le diviseur $37 \times 2^{16} + 1 = 2424833$, mais on ne savait rien du quotient. Il faudra attendre 1967 pour que Brillhart démontre que ce quotient était lui-même composé, ce que l'on peut considérer comme un exploit, compte tenu du fait que $F_9/2424833$ s'écrit avec 148 chiffres.

Voici l'état actuel des connaissances sur cette question :
• la décomposition complète de F_n en facteurs premiers est connue pour $n \leq 9$ et $n = 11$;
• un ou plusieurs facteurs de F_n sont connus pour les entiers n inférieurs ou égaux

à 32 sauf 14, 20, 22, 24, 28, 31 ainsi que pour 76 valeurs plus grandes de n, la plus grande, comme nous l'avons signalé plus haut étant $n = 23471$;
• pour $n = 10, 12, 13, 15, 16, 17, 18$ on sait que le cofacteur est composé ;
• aucun facteur de F_{14} et F_{20} n'est connu, mais on sait que ces nombres sont composés ;
• pour $n = 22, 24, 28, 31$ et les valeurs supérieures à 32 exceptées les 76 évoquées plus haut, on ne sait pas si F_n est premier ou composé.

Le plus petit nombre de Fermat non encore complètement décomposé est F_{10}. Deux de ses facteurs premiers sont connus : $11131 \times 2^{12} + 1 = 45592577$ et $395937 \times 2^{14} + 1 = 6487031809$.

La décomposition de F_9 est récente. Elle a été réalisée en 1990 par une équipe américaine du Mathematical Science Research Institute de Berkeley. F_9 a 155 chiffres :

$F_9 =$ 134 078 079 299 425 970 995 740 249 982 058 461 274
793 658 205 923 933 777 235 614 437 217 640 300 735
469 768 018 742 981 669 034 276 900 318 581 864 860
508 537 538 828 119 465 699 464 336 490 060 840 97.

Il est le produit de trois nombres premiers, ayant respectivement 7, 49 et 99 chiffres :

P_7 =242 483 3 déjà connu
P_{49}=745 560 282 564 788 420 833 739 573 620 045 491 878 336 634 265 7
P_{99}=741 640 062 627 530 801 524 787 141 901 937 474 059 940 781 097 519
023 905 821 316 144 415 759 504 705 008 092 818 711 693 940 737.

Il ne nous est pas possible, dans le cadre de cet article, de rendre compte en détail des techniques utilisées pour cette décomposition (4). Celle-ci a mis à contribution environ 700 centres de calcul dispersés à travers le monde entier et dans l'une des dernières étapes un super calculateur. La factorisation complète a duré quatre mois. Nous voudrions seulement montrer ici combien la mise en œuvre de cette décomposition a eu recours à toutes les ressources de l'algèbre moderne : algèbre linéaire, corps finis, anneaux d'entiers algébriques. En voici quelques aperçus.

3. Le sous groupe des racines carrées de l'unité, dans $\mathbb{Z}/n\mathbb{Z}$

Dans la suite, n est un entier impair supérieur à 1. Ce sera en fait l'entier que nous souhaitons décomposer en facteurs premiers. Selon les notations habituelles $\mathbb{Z}$ désigne l'anneau des entiers relatifs, $\mathbb{Z}/n\mathbb{Z}$ l'anneau des entiers modulo n, et $(\mathbb{Z}/n\mathbb{Z})^*$ le groupe des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$. Alors l'ensemble

$$E = \{x \in \mathbb{Z}/n\mathbb{Z}; x^2 = 1\}$$

(4) Celles-ci sont développées dans un article paru dans la revue "Mathematics of computation" vol. 61, n° 203, July 1993, pp. 319-349 : "The factorization of the ninth Fermat number" A.K. Lenstra, H.-W. Lenstra, J.-R. M.-S. Manasse and J.-M. Pollard.

est un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^*$ et peut être considéré comme un espace vectoriel sur le corps fini à deux éléments $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$, l'addition vectorielle étant définie par la multiplication. Par exemple, pour $n = 3 \times 5 \times 7 = 105$, l'ensemble E est constitué des éléments : $E = \{1, 29, 34, 41, 64, 71, 76, 104\}$ dont une base est définie par $e_1 = 29; e_2 = 34; e_3 = 64$ engendrant $41 = e_1 + e_2 \equiv 29 \times 34; 104 = e_1 + e_2 + e_3 \equiv 29 \times 34 \times 64$ (modulo 105) etc...

Cette base de E contient trois éléments parce que 105 comprend trois facteurs premiers distincts : 3, 5 et 7. Ce fait est général et se trouve à l'origine de nombre d'algorithmes de décomposition des entiers en facteurs premiers : la dimension de l'espace vectoriel E sur $\mathbb{F}_2$ est égale au nombre de facteurs premiers distincts de n.

Si n n'est pas une puissance de nombre premier, on montre qu'il existe alors un élément x de $\mathbb{Z}/n\mathbb{Z}; x \neq \pm 1$, tel que $x^2 = 1$. De plus, la connaissance explicite d'un tel élément x, disons $x \equiv y \pmod{n}$ conduit à une factorisation non triviale de n. En effet : $y^2 \equiv 1; y \not\equiv \pm 1 \pmod{n}$ entraîne que n divise le produit $(y-1)(y+1)$ sans diviser aucun des facteurs $(y-1)$ ou $(y+1)$, de sorte que les pgcd de $(y-1, n)$ et $(y+1, n)$ sont des diviseurs non triviaux de n. En fait, il y a des facteurs complémentaires, de sorte qu'un seul des deux pgcd suffit, qu'on peut déterminer par l'algorithme d'Euclide. Nous pouvons donc conclure que pour factoriser n, il suffit de trouver un x de $\mathbb{Z}/n\mathbb{Z}$ vérifiant $x^2 = 1$ sans que $x = 1$ ou $x = -1$.

Cette méthode, cependant, est en défaut si n est une puissance de nombre premier. Il faudrait donc s'assurer d'abord que l'entier n que l'on veut décomposer ne rentre pas dans cette catégorie. On peut d'abord soumettre n à un test de primalité. Si n est premier, la factorisation est terminée. S'il ne l'est pas, la vérification qu'il n'est pas une puissance de nombre premier reste à faire. Des test existent là aussi, mais cette vérification est souvent omise, car il est hautement improbable que n soit une puissance de nombre premier lorsqu'il n'est pas premier. Les auteurs de la décomposition de F_9 avouent avoir tout simplement oublié de penser à cette vérification :
"*Si (le nombre $F_9/2424833$) avait été une puissance de nombre premier, notre méthode aurait échoué complètement, et nous aurions été extrêmement embarassés envers les nombreuses personnes qui nous ont aidé dans ce projet. On peut penser que le risque que nous avons pris inconsciemment était extrêmement faible, mais jusqu'à ce que le nombre ait été factorisé, ce n'était là rien de plus qu'une conviction.*"

Voici, en trois étapes, le schéma général utilisé par l'équipe américaine pour la décomposition de $n = F_9/2424833$ qui, rappelons le, est un nombre d'environ 150 chiffres.

4. Schéma général de recherche d'un système de générateurs du $\mathbb{F}_2$ espace vectoriel E.

La recherche d'un élément x de $\mathbb{Z}/n\mathbb{Z}$ vérifiant $x^2 = 1$ et $x \neq \pm 1$ qui permette d'aboutir à un facteur non trivial de n, peut se faire par la détermination d'un système de générateurs de l'espace vectoriel E sur $\mathbb{F}_2$. Comment obtenir un tel

système?

Première étape : sélection d'une base de facteurs

Il s'agit de choisir un ensemble d'éléments a_p de $\mathbb{Z}/n\mathbb{Z}$ où p parcourt un ensemble fini P d'indices. Le choix de cet ensemble est fait de façon à rendre efficace la prochaine étape décrite ci-dessous. L'ensemble des $(a_p)_{p\in P}$ est appelé **base de facteurs**. Nous supposons que tous les (a_p) appartiennent à $(\mathbb{Z}/n\mathbb{Z})^*$ ce qui en pratique est vraisemblable, puisque n étant difficile à factoriser, on ne peut guère espérer que l'un de ses facteurs soit l'un des a_p. Soit alors $\mathbb{Z}^p$ le groupe abélien additif formé des vecteurs $(v_p)_{p\in P}$ avec $v_p \in \mathbb{Z}$, et f l'homomorphisme de groupe : $\mathbb{Z}^p \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*$ qui à $(v_p)_{p\in P}$ associe $\Pi_{p\in P} a_p^{v_p}$. Cette application est surjective si et seulement si les $(a_p)_{p\in P}$ engendrent $(\mathbb{Z}/n\mathbb{Z})^*$. Pour le choix des a_p fait en pratique (5), c'est généralement le cas, mais, avouent encore les auteurs : "*nous sommes en général incapables de le prouver*", et d'ajouter : "*D'ailleurs peu de chose a été prouvé rigoureusement au sujet des algorithmes pratiques de factorisation !*".

Seconde étape : rassembler des relations entre les a_p

Chaque élément $v = (v_p)_{p\in P}$ du noyau de f donne une relation entre les a_p, en ce sens que $\Pi_{p\in P} a_p^{v_p} = 1$. La seconde étape va consister à collecter de telles relations, jusqu'à ce que leur nombre soit grossièrement supérieur au cardinal de P.

Troisième étape : recherche de dépendances

Soit V l'ensemble des v déterminés dans la seconde étape, et $\overline{v} \in (\mathbb{Z}/2\mathbb{Z})^p = \mathbb{F}_2^p$ le vecteur obtenu à partir de v en réduisant ses composantes modulo 2. Comme le cardinal de V est supérieur à celui de P, les vecteurs $\overline{v}$ sont linéairement dépendants sur $\mathbb{F}_2$. La troisième étape va consister à chercher des dépendances explicites en résolvant un système linéaire. La matrice de ce système tend à être énorme mais avec beaucoup de 0 et des 1 éparpillés par ci par là, et il existe des méthodes spéciales pour résoudre ce type de système. Néanmoins ici, les auteurs ont utilisé la méthode classique de Gauss. Les matrices les plus importantes présentaient approximativement 80000 colonnes et un peu moins de lignes!

Chaque dépendance trouvée peut s'écrire $\sum_{v\in W} \overline{v} = 0$ pour un certain ensemble W inclus dans V, et chaque W donne naissance à un vecteur $w = \frac{1}{2}(\sum_{v\in W} v) \in \mathbb{Z}^p$ pour lequel $2.w$ appartient à $\ker f$. Chaque w de ce type, à son tour, donne naissance à un élément $x = f(w)$ qui appartient à $(\mathbb{Z}/n\mathbb{Z})^*$ et qui vérifie $x^2 = f(2.w) = 1$ et donc donne naissance à une décomposition de n en facteurs non triviaux.

5. Mise en place d'une base de facteurs

Pour la décomposition de $n = F_9/2424833$ la sélection d'une base de facteurs a été construite sur l'utilisation de l'anneau des entiers algébriques $\mathbb{Z}[\sqrt[5]{2}]$. Rappelons-en les principales caractéristiques.

L'ensemble $\mathbb{Z}[\sqrt[5]{2}]$ est formé des réels $\alpha = \sum_{i=0}^{i=4} \alpha_i \sqrt[5]{2}^i$ où les α_i sont des entiers

(5) Voir § 5 du présent article.

relatifs. Multiplier un élément $x = \sum_{i=0}^{i=4} x_i \sqrt[5]{2}^i$ par α revient à multiplier le vecteur colonne $(x_i)_{0 \leq i \leq 4}$ par la matrice

$$\begin{pmatrix} \alpha_0 & 2\alpha_4 & 2\alpha_3 & 2\alpha_2 & 2\alpha_1 \\ \alpha_1 & \alpha_0 & 2\alpha_4 & 2\alpha_3 & 2\alpha_2 \\ \alpha_2 & \alpha_1 & \alpha_0 & 2\alpha_4 & 2\alpha_3 \\ \alpha_3 & \alpha_2 & \alpha_1 & \alpha_0 & 2\alpha_4 \\ \alpha_4 & \alpha_3 & \alpha_2 & \alpha_1 & \alpha_0 \end{pmatrix}$$

La norme $N(\alpha)$ est définie comme étant le déterminant de cette matrice, qui est un entier. Elle vérifie :

$$N(\alpha\beta) = N(\alpha).N(\beta) \text{ pour } \alpha \text{ et } \beta \text{ appartenant à } \mathbb{Z}[\sqrt[5]{2}].$$

En particulier la norme $N(a - b\sqrt[5]{2}^i) = a^5 - 2^i b^5$ pour $(a, b) \in \mathbb{Z}^2; 0 \leq i \leq 4$, joue un rôle important dans la décomposition de n.

Homomorphisme d'anneaux

Si $\mathcal{A}$ est un anneau commutatif unitaire, et $\Psi : \mathbb{Z}[\sqrt[5]{2}] \longrightarrow \mathcal{A}$ un homomorphisme d'anneau, alors l'élément $c = \Psi(\sqrt[5]{2})$ de $\mathcal{A}$ vérifie $c^5 = 2$ où 2 est l'élément $1 + 1$ de l'anneau unitaire $\mathcal{A}$. Reciproquement, si c appartenant à $\mathcal{A}$ vérifie $c^5 = 2$, il existe un unique homomorphisme d'anneau $\Psi : \mathbb{Z}[\sqrt[5]{2}] \longrightarrow \mathcal{A}$, tel que $\Psi(\sqrt[5]{2}) = c$, à savoir l'application définie par :

$$\Psi\Big(\sum_{i=0}^{i=4} \alpha_i \sqrt[5]{2}^i\Big) = \sum_{i=0}^{i=4} \alpha_i c^i \quad (\alpha_i \in \mathbb{Z})$$

où les α_i à droite sont interprétés comme éléments de $\mathcal{A}$, de la même manière que nous avons définis $2 = 1 + 1$. Ainsi, se donner un homomorphisme d'anneau de $\mathbb{Z}[\sqrt[5]{2}]$ dans $\mathcal{A}$ est équivalent à se donner un élément c de $\mathcal{A}$ vérifiant $c^5 = 2$. L'exemple suivant va jouer le rôle essentiel dans la décomposition de $n = F_9/2424833$.

Prenons $\mathcal{A} = \mathbb{Z}/n\mathbb{Z}$ et $c \equiv 2^{205} \pmod{n}$.
En nous rappelant que $F_9 = 2^{512} + 1$, alors $2^{512} \equiv -1 \pmod{n}$ et donc $c^5 \equiv 2^{1025} \equiv 2 \times (2^{512})^2 \equiv 2 \pmod{n}$.

Il existe donc un homomorphisme $\Psi : \mathbb{Z}[\sqrt[5]{2}] \longrightarrow \mathbb{Z}/n\mathbb{Z}$ avec $\Psi(\sqrt[5]{2}) \equiv 2^{205} \pmod{n}$.

Cet homomorphisme a l'avantage suivant que l'image de $\alpha = -\sqrt[5]{2}^3$ étant $\Psi(\alpha) \equiv (-2^{615}) \equiv 2^{103} \pmod{n}$, 2^{103} est relativement petit par rapport à n (une trentaine de chiffres seulement, contre 150 pour n).

Anneau principal

L'anneau $\mathbb{Z}[\sqrt[5]{2}]$ se trouve avoir cette propriété remarquable d'être un anneau principal, ce qui signifie que tout idéal $\mathbf{b}$ de cet anneau est principal, c'est-à-dire engendré par un unique élément β, ou encore qu'il est de la forme $\beta\mathbb{Z}[\sqrt[5]{2}]$ avec β appartenant à $\mathbb{Z}[\sqrt[5]{2}]$. (β est appelé générateur de l'idéal $\mathbf{b}$).

Un ensemble de $\mathbb{Z}[\sqrt[5]{2}]$ en est un idéal si et seulement si il est le noyau d'un homomorphisme d'anneau défini sur $\mathbb{Z}[\sqrt[5]{2}]$. On appelle **idéal premier** de $\mathbb{Z}[\sqrt[5]{2}]$ tout idéal qui est le noyau d'un homomorphisme d'anneau de $\mathbb{Z}[\sqrt[5]{2}]$ sur un corps fini $\mathbb{F}_p$. En particulier, si p est un entier premier, l'idéal est appelé idéal premier du premier ordre (first-degree prime). Ces idéaux là jouent le même rôle dans $\mathbb{Z}[\sqrt[5]{2}]$ que les nombres premiers dans $\mathbb{Z}$. Précisément, tout élément non nul x de $\mathbb{Z}[\sqrt[5]{2}]$ peut se décomposer de façon unique sous la forme :

$$x = \varepsilon \Pi_p \pi_p^{m(p)}$$

où ε appartient au groupe $(\mathbb{Z}[\sqrt[5]{2}])^*$ des éléments inversibles de $\mathbb{Z}[\sqrt[5]{2}]$ (ses unités). p désigne un idéal premier et π_p un générateur de cet idéal; $m(p)$ désigne un entier naturel.

Par exemple $5 = \varepsilon_3(1 + \sqrt[5]{2}^2)^5$ avec $\varepsilon_3 = \varepsilon_1^2 \varepsilon_2^{-2}$ où $\varepsilon_1 = -1 + \sqrt[5]{2}^2$ et $\varepsilon_2 = -1 + \sqrt[5]{2}^2 - \sqrt[5]{2}^3 + \sqrt[5]{2}^4$.

La base de facteurs $(a_p)_{p \in P}$ utilisée pour la décomposition de n sera finalement construite à partir de l'ensemble P des éléments suivants :
1) Les 99700 nombres premiers p inférieurs à $B_1 = 1295377$.
2) Les trois entiers algébriques $\varepsilon_0, \varepsilon_1, \varepsilon_2$ où $\varepsilon_0 = -1$ et ε_1 et ε_2 sont les nombres définis ci-dessus. Ces trois entiers sont des générateurs du sous anneau $(\mathbb{Z}[\sqrt[5]{2}])^*$ des éléments inversibles de $\mathbb{Z}[\sqrt[5]{2}]$, c'est-à-dire que chaque élément ε de ce sous anneau peut s'écrire sous la forme $\varepsilon = \varepsilon_0^{v(0)} \varepsilon_1^{v(1)} \varepsilon_2^{v(2)}$ avec $v(0), v(1), v(2)$ éléments de $\mathbb{Z}$.
3) Les générateurs π_p des 99500 entiers algébriques du premier ordre de $\mathbb{Z}[\sqrt[5]{2}]$ dont la norme est inférieure à $B_2 = 1294973$.

Les contraintes B_1 et B_2 sont des contraintes empiriques imposées par la réalisation effective des divers calculs.

La base de facteurs $(a_p)_{p \in P}$ est alors définie pour chaque indice $p \in P$ par $a_p = \Psi(p)$ où Ψ est l'homomorphisme défini ci-dessus. Elle était donc composée de $3+99700+99500 = 199203$ éléments, pour lesquels ont été déterminés un ensemble V de 226688 relations. La recherche de celles-ci avait été répartie entre environ 700 "workstations" reliées à un centre général de calcul DEC SRC à Palo Alto. Voici comment les auteurs décrivent les dernières minutes de cette prodigieuse réalisation.

"*Le 15 juin 1990, tôt dans la matinée, les relations de dépendance furent envoyées électroniquement à DEC SRC où elles furent converties en dépendances sur la 200000 matrice originale (6).*

Du moins, nous espérions que les choses se passeraient bien ainsi. A 9 h 15 PDT (7) nous démarrions notre programme final, la tentative de factoriser n

(6) La matrice 226688 × 199203 regroupant les relations, réduites modulo 2.
(7) heure locale soit heure GMT - 7h.

en parcourant les relations de dépendance séquentiellement jusqu'à ce que la factorisation soit trouvée. Ce fut le moment le plus excitant de toute la factorisation de F_9 : à 9 h 45 PDT le programme concluait que la première relation trouvée entre les colonnes de la 200000 matrice était une relation exacte. Ce moment de grande émotion ne put être gâté par le message décevant émis à 10 h 15 PDT, que la première relation de dépendance n'a donné naissance qu'à la factorisation triviale de n. Une heure plus tard, à 11 h 15 PDT (18 h 15 GMT) la seconde dépendance s'avéra plus chanceuse en détectant un facteur de 49 chiffres. Ce facteur ainsi que le cofacteur de 99 chiffres furent tous deux annoncés comme premiers, parce qu'aucun témoignage de leur éventuel caractère composé ne put être découvert parmi cinq entiers choisis de façon aléatoire (8).

Cinq minutes après, le processus d'élimination gaussien, ne fonctionnant pourtant plus que dans un seul poste de calcul était terminé, cinq jours avant le délai fixé. Le même jour encore, ce 15 juin, Andrew Odlyzk utilisait un test de primalité pour prouver que chacun des deux facteurs était vraiment premier".

(8) pour lesquels $a^n \equiv a \pmod{n}$.