Fermat, Mersenne, factorisation et nombres parfaits

Daniel PERRIN

Table des matières

Introduction

FIGURE 1 – Pierre de Fermat (1605-1665)

FIGURE 2 – Marin Mersenne (1588-1648)

Cette conférence s'inscrit dans le cycle *Un texte, un mathématicien* de la Bibliothèque Nationale de France. Les textes qui lui servent de point de départ sont deux lettres de Pierre de Fermat au révérend père Marin Mersenne, toutes deux datées de 1643 et toutes deux portant sur la factorisation de grands entiers. Il est important de rappeler plusieurs points qui concernent les mathématiques de cette époque. D'abord, le XVII-ième siècle marque un tournant crucial dans l'histoire des mathématiques avec l'invention du calcul différentiel et intégral, due essentiellement à Newton et Leibniz, mais où Fermat joue aussi un grand rôle, notamment en proposant une méthode pour

déterminer les tangentes à une courbe. En contrepartie, l'arithmétique est moins présente, sauf peut-être chez Fermat, justement. Ensuite, il faut se souvenir qu'à l'époque il n'y avait pas vraiment de mathématiciens professionnels (Fermat est magistrat au parlement de Toulouse, Mersenne est un religieux de l'ordre des minimes, d'autres comme Descartes et Pascal vivent de leurs rentes). Enfin, il ne faut pas oublier que la communication se faisait essentiellement de manière épistolaire [1] : il n'y avait pas de revues de mathématiques (elles apparaissent seulement au XIX-ième siècle), ni de rencontres dédiées à cette discipline. Mersenne fonde cependant en 1635 une *Academia parisiensis* (qui préfigure l'Académie des sciences créée en 1666 par Colbert) qui réunit Descartes, les Pascal père et fils, Gassendi, Frenicle, Roberval, Huygens, Fermat et bien d'autres [2], qui se rencontrent et/ou entretiennent une abondante correspondance. Souvent cette correspondance prend la forme de défis que les participants doivent relever comme on le verra dans ce qui suit. Elle est aussi émaillée de controverses parfois acerbes comme entre Descartes et Fermat sur les tangentes, entre Roberval et Fermat sur les leviers, etc. Ce point est encore renforcé par le fait que, la plupart du temps, les protagonistes affirment des résultats sans en donner de preuves.

1 La factorisation de 2027651281

1.1 La lettre de Fermat

Le premier texte est l'extrait suivant d'une lettre de Fermat à Mersenne, datant [3] de 1643 (voir [4], tome II, p. 256, lettre LVII).

Cela posé, qu'un nombre me soit donné, par exemple 2027651281*, on demande s'il est premier ou composé, et de quels nombres il est composé, au cas qu'il le soit. J'extrais la racine, pour connaître le moindre des dits nombres, et trouve* 45029 *avec* 40440 *de reste, lequel j'ôte du double plus* 1 *de la racine trouvée, savoir de* 90059 *: reste* 49619*, lequel n'est pas carré,*

1. Mersenne et Fermat, qui correspondent depuis 1636, ne se rencontrent qu'une seule fois, en 1646.

2. On a dénombré plus de 140 correspondants de Mersenne.

3. Il s'agit d'un fragment d'une lettre, qui n'est pas plus précisément daté. Dans l'édition des œuvres de Fermat, elle vient après celle d'avril 1643 qui concerne le nombre 100895598169, voir ci-dessous, mais j'ignore si les éditeurs avaient des raisons de la supposer postérieure. Les deux interprétations me semblent possibles, soit que Mersenne, connaissant la méthode de factorisation de Fermat pour 2027651281, ait voulu le mettre au défi sur un autre nombre, soit au contraire que Fermat, qui avait résolu le cas de 100895598169 par un artifice, se soit à cette occasion posé la question générale de la factorisation. Je penche plutôt pour cette dernière interprétation.

parce qu'aucun carré ne finit par 19*, et partant je lui ajoute* 90061*, savoir* 2 *plus* 90059 *qui est le double plus* 1 *de la racine* 45029*. Et parce que la somme* 139680 *n'est pas encore carrée, comme on le voit par les finales, je lui ajoute encore le même nombre augmenté de* 2*, savoir* 90063 *et je continue ainsi d'ajouter tant que la somme soit un carré, comme on peut voir ici. Ce qui n'arrive qu'à* 1040400 *; qui est carré de* 1020 *et partant le nombre donné est composé ; car il est aisé, par l'inspection des dites sommes, de voir qu'il n'y a aucune qui soit nombre carré que la dernière, car les carrés ne peuvent souffrir les finales qu'elles ont, si ce n'est* 499944 *qui néanmoins n'est pas carré. Pour savoir maintenant les nombres qui composent* 2027651281*, j'ôte le nombre que j'ai premièrement ajouté, savoir* 90061*, du dernier ajouté* 90081*. Il reste* 20*, à la moitié duquel plus* 2*, savoir à* 12*, j'ajoute la racine premièrement trouvée* 45029*. La somme est* 45041*, auquel nombre ajoutant et ôtant* 1020*, racine de la dernière somme* 1040400*, on aura* 46061 *et* 44021*, qui sont les deux nombres plus prochains qui composent* 2027651281*. Ce sont les seuls, pourceque l'un et l'autre sont premiers.*

1.2 Lecture commentée

Notons déjà qu'on dispose ici d'un des rares textes où Fermat explique comment il a trouvé ses résultats.

1.2.1 Explication de la procédure

Reprenons le texte de la lettre point par point, mais en décrivant la procédure avec des symboles [4]. On doit décomposer le nombre $N = 2027651281$ en produit de facteurs premiers. La première étape est d'en extraire une racine carrée approchée à une unité près : *J'extrais la racine, pour connaître le moindre des dits nombres.* Aujourd'hui les calculatrices donnent $\sqrt{N} \sim 45029,449$. Je suppose que Fermat utilisait l'algorithme classique (que l'on présente avec une potence comme la division [5]), voir §5 (Annexe 1) ci-dessous. Toujours est-il que Fermat donne la racine approchée $c := 45029$ qui vérifie $c^2 \leq N < (c+1)^2$. Bien sûr, si on a $N = c^2$ on a une décomposition de N. Ici, ce n'est pas le cas, comme le dit Fermat, il y a un reste $r := 40440$, ce qui signifie qu'on a $N = c^2 + r = 45029^2 + 40440$.

L'idée fondamentale est alors d'écrire N sous forme de différence de deux carrés [6] $N = R^2 - S^2 = (R-S)(R+S)$, ce qui donnera la factorisation

4. On voit ici quelle économie de pensée ils procurent !

5. Cet algorithme semble être connu depuis 499 après J.-C. par le mathématicien indien Aryabhata et il était encore enseigné en troisième quand j'étais collégien.

6. Ce point n'est pas dit dans le texte cité ci-dessus, mais il est évoqué avant, voir 1.3.1

cherchée. Pour cela, on cherche R sous la forme $R = c + k$ avec $k = 1, 2, ...$ Si $(c + k)^2 - N$ n'est pas un carré on l'élimine, si c'est un carré S^2 on a la factorisation. C'est ce qu'explique Fermat dans la lettre et il parcourt les entiers k de 1 à 12.

Voici comment Fermat fait ce calcul. On a $c^2 - N = -r$. On obtient le terme suivant $(c+1)^2 - N = (c^2 + 2c + 1) - N = (2c + 1) - r$ en retranchant $r = 40440$ de $2c + 1 = 90059$ et il reste 49619 comme le dit Fermat : *lequel j'ôte du double plus* 1 *de la racine trouvée, savoir de* 90059 *: reste* 49619.

Il ajoute que ce nombre n'est pas un carré *parce qu'aucun carré ne finit par* 19. L'argument utilisé ici est de déterminer les restes modulo 100 des carrés n^2, c'est-à-dire leurs deux derniers chiffres [7] en écriture décimale. La liste des possibles est la suivante : $0, 1, 4, 9, 16, 21, 24, 25, 29, 36, 41, 44, 49, 56, 61, 64, 69, 76, 81, 84, 89, 96$ (il suffit d'aller jusqu'à $n = 25$).

D'une manière générale, pour effectuer ce calcul, Fermat note que pour passer de $(c + k)^2$ à $(c + k + 1)^2$ on ajoute $2c + 1 + 2k$, c'est-à-dire $2c + 1$, $2c + 1 + 2$, etc. En effet, il dit : *et partant je lui ajoute* 90061*, savoir* 2 *plus* 90059 *qui est le double plus* 1 *de la racine* 45029

Et il poursuit en ajoutant à chaque pas 2 de plus qu'au pas précédent : *je lui ajoute encore le même nombre augmenté de* 2.

Il note ensuite que les nombres obtenus ne sont pas des carrés : *car les carrés ne peuvent souffrir les finales qu'elles ont, si ce n'est* 499944 *qui néanmoins n'est pas carré.* (Pour voir que ce dernier nombre n'est pas non plus un carré il suffit de noter qu'il est multiple de 3 mais pas de 9.)

Il poursuit ainsi jusqu'à trouver un carré. Il faut aller jusqu'à $k = 12$:

$$(c + 12)^2 - N = (45029 + 12)^2 - 2027651281 = 1040400 = (1020)^2 = S^2$$

ce qui donne la factorisation [8] :

$$N = (45029 + 12)^2 - 1020^2 = 45041^2 - 1020^2 = 44021 \times 46061.$$

Il ajoute enfin que les facteurs trouvés sont premiers [9] : *Ce sont les seuls, parce que l'un et l'autre sont premiers.*

---

ci-dessous.

7. On peut déjà noter qu'un carré ne se termine jamais par $2, 3, 7, 8$.

8. Le fait de ne pas écrire de symboles rend la fin du texte un peu laborieuse ! En particulier on ne comprend pas bien pourquoi, pour calculer k, il utilise $2c + 3 = 90061$ plutôt que $2c + 1 = 90059$.

9. Nous reviendrons plus loin sur les affirmations de Fermat concernant la primalité de grands nombres, mais pour des nombres de cette taille elles sont certainement fiables.

1.3 Discussion

1.3.1 L'universalité de la méthode

La méthode consistant à écrire $N = R^2 - S^2$ pour le factoriser est bien naturelle et elle a le mérite de fonctionner toujours (au moins en théorie). En effet, si $N = pq$ avec p, q premiers impairs et $p < q$ on peut l'écrire $N = \left(\frac{p+q}{2}\right)^2 - \left(\frac{q-p}{2}\right)^2 = R^2 - S^2$ et c'est la seule manière de l'écrire ainsi (hormis $N = \left(\frac{N+1}{2}\right)^2 - \left(\frac{N-1}{2}\right)^2$ qui donne la décomposition triviale $N = 1 \times N$).

Fermat sait cela et même précisément combien de décompositions en différence de carrés possède un entier. Il le dit au début de la même lettre :

Tout nombre impair non quarré est différent d'un quarré par un quarré, ou est la différence de deux quarrés, autant de fois qu'il est composé de deux nombres ...

et il ajoute plus loin, annonçant la méthode de décomposition :

Il est fort aisé de trouver les quarrés satisfaisant quand on a les parties, et d'avoir les parties lorsqu'on a les quarrés.

La méthode de Fermat consiste à chercher $R = \frac{p+q}{2}$ sous la forme $c + k := [\sqrt{pq}] + k$ en parcourant les entiers k. On voit qu'elle nécessite $k = \frac{p+q}{2} - \left[\sqrt{pq}\right]$ tentatives (on appellera cette quantité [10] la **patience** de l'utilisateur). La méthode n'est praticable (au moins à la main) que lorsque k est petit, c'est-à-dire lorsque les facteurs p, q sont proches [11], donc proches de la racine carrée de N. Ainsi, avec l'autre exemple qu'aborde Fermat et que nous étudierons plus loin, $F = 100895598169$, il faut aller jusque $k = 187723$, ce qui semble inabordable.

En revanche, le défi [12] proposé par Stanley Jevons en 1874 semble justiciable de cette méthode : *Le lecteur peut-il dire de quels deux nombres est composé le nombre* 8 616 460 799 *? Je pense qu'il est peu probable que personne d'autre que moi ne pourra jamais le savoir* [13]. En effet, la patience de l'utilisateur est ici seulement de 56 et on vérifie que la plupart des nombres obtenus ne sont pas des carrés grâce aux deux derniers chiffres, à l'exception

10. C'est essentiellement la différence entre la moyenne arithmétique et la moyenne géométrique de p et q, ou encore $\frac{1}{2}(\sqrt{q} - \sqrt{p})^2$.

11. Fermat en est conscient car la lettre de 1643 se termine ainsi : *Plusieurs abrégés se peuvent trouver, comme lorsqu'on ne fait qu'une addition au lieu de dix, aux endroits où les sommes ont leurs finales quarrées, quand les compositeurs sont beaucoup éloignés l'un de l'autre.*

12. Bien présomptueux.

13. Un article de Charles Busk dans *Nature* donnait le résultat en 1889.

des suivants : 2804801, 6518801, 8376101 (qui ne sont pas carrés car $\equiv 2 \pmod 3$), 8004625 (non carré car $\equiv -1 \pmod 7$) et 4661701 (non carré car multiple de 11 mais pas de 121).

1.3.2 L'intérêt de la méthode

Une question importante est de mesurer l'avantage de la méthode de Fermat par rapport à la méthode des divisions successives. La réponse à la question dépend un peu de ce dont on dispose. On sait qu'avec la méthode du crible, il suffit de tester si N admet un diviseur $\leq \sqrt{N} \sim 45029$. C'est d'ailleurs ce que dit Fermat : *Si l'on alloit par la voie ordinaire, pour trouver la composition d'un tel nombre, au lieu de onze additions, il eût fallu diviser par tous les nombres depuis* 7 *jusqu'à* 44021. En réalité, il n'y a pas tant de divisions à effectuer (on peut se limiter aux nombres impairs, éliminer les multiples de 5, ceux de 3, voire de 11, etc.) Mais, même si l'on dispose d'une table des nombres premiers $\leq \sqrt{N}$, on doit *a priori* essayer 4677 nombres premiers (4581 si l'on s'arrête à 44021). Si l'on part de la racine 45029 en descendant, il y a 1008 nombres jusqu'à 44021. Si l'on n'a pas de table des nombres premiers on peut toutefois éliminer les nombres pairs, ceux qui se terminent par 5 et les multiples de 3, voire de 11. Cela laisse tout de même 242 divisions à faire. Si l'on dispose d'une table des nombres premiers, il y a seulement 97 divisions. On voit que, même dans ce cas, il y a beaucoup plus d'opérations à effectuer que ce que fait Fermat (12 opérations seulement) et surtout, Fermat, lui, ne fait pas de division !

1.3.3 Un calcul grossier

Pour expliquer ce gain de productivité, il suffit d'un calcul grossier. On suppose qu'on a $N = pq$ avec $p < q$ premiers et p, q proches. On écrit $q = p+t$, avec t petit devant p, et on doit alors comparer deux nombres.

• Le nombre k d'essais requis par la méthode de Fermat. On a vu qu'on a $k = \dfrac{p+q}{2} - \sqrt{pq} = p + \dfrac{t}{2} - p\sqrt{1 + \dfrac{t}{p}}$ et un développement limité donne[14] aussitôt $k \sim \dfrac{t^2}{8p}$.

• Le nombre n de nombres premiers compris entre p et $c := \sqrt{pq}$, nombre de divisions à faire pour trouver le facteur p en parcourant les nombres premiers à partir de c en descendant. Le théorème des nombres premiers dit que n est de l'ordre de $\dfrac{c}{\ln c} - \dfrac{p}{\ln p}$. Mais on a $c = \sqrt{p(p+t)} \sim p + \frac{t}{2}$ et un

14. On voit que si t est plus petit que $2\sqrt{2p}$, la méthode marche au premier essai !

développement limité donne cette fois $n \sim \dfrac{t}{2\ln p}$.

On voit que, pour t petit et p grand, k est infiniment petit devant n, ce qui atteste la supériorité de la méthode de Fermat (sans compter que les opérations élémentaires de la méthode Fermat sont des additions, assorties d'un test permettant de savoir si un nombre est un carré, facile en général, alors que dans l'autre méthode, on doit faire des divisions).

1.1 *Remarque.* Une autre méthode naturelle pour factoriser N en écrivant $N = R^2 - S^2$ consiste à parcourir les entiers $S = 0, 1, 2, ...$ jusqu'à trouver S tel que $N + S^2$ soit un carré. Cette méthode est moins efficace dans le cas $N = pq$ avec $p < q$ et $q-p = t$ petit. En effet, elle requiert $S = (q-p)/2 = t/2$ opérations, alors que la méthode de Fermat n'en nécessite que $k \sim \dfrac{t^2}{8p}$.

2 La factorisation de 100895598169

2.1 La lettre du 7 avril 1643

Voici l'extrait de la lettre de Fermat à Mersenne, datée du 7 avril 1643, qui évoque ce nombre :

... Vous me demandiez ensuite si ce dernier nombre (100895598169) *est premier ou non, et une méthode pour découvrir dans l'espace d'un jour s'il est premier ou composé.*

...

À la seconde question je réponds que le dernier de ces nombres est composé et se fait du produit des deux : 898423 *et* 112303 *qui sont premiers. Je suis toujours, mon Révérend Père, votre très humble et très affectionné serviteur.*

J'ai utilisé ce fragment de lettre pendant des années, dans de nombreuses conférences, en ajoutant, avec un brin d'admiration, qu'on ignorait comment Fermat avait procédé et j'ai même imaginé une méthode qu'il aurait pu utiliser et que l'on trouvera plus bas [15].

La réalité est plus prosaïque [16] : sur cet exemple, Fermat bénéficiait d'un délit d'initié, comme je l'ai découvert en consultant le passionnant site *blogdemaths* :

`https://blogdemaths.wordpress.com/2014/05/18/savez-vous-factoriser-a-la-mode-de-fermat/`

15. Voir par exemple, sur ma page web, la conférence au lycée de Rambouillet et la rédaction sur le code RSA dans la rubrique *Mathématiques et autres disciplines.*

16. Et je m'en serais aperçu si j'avais regardé à la source, c'est-à-dire dans les œuvres complètes de Fermat car les éditeurs expliquent ce point.

https://blogdemaths.files.wordpress.com/2014/05/factorisation_de_100895598169_par_fermat.pdf

En effet, voici un autre extrait de la même lettre, qui précède celui cité plus haut :

Pour les parties aliquotes, j'ai découvert des choses excellentes et je puis vous envoyer quelques multiples autres que ceux que vous avez mis dans la préface du petit Livre Des pensées de Galilée *et pour ne vous laisser plus en doute que je possède la solution infaillible de ces questions, j'ai relu ces jours passés une question que vous me faisiez par ordre de M. Frenicle, dont je vous envoie présentement la solution.*

Vous me demandiez quelle proportion a le nombre, qui se produit des nombres suivants, avec ses parties aliquotes :

$$N = 214748364800000 \times 11 \times 19 \times 43 \times 61 \times 83 \times 169\times$$

$$223 \times 331 \times 379 \times 601 \times 757 \times 961 \times 1201 \times 7019\times$$

$$823543 \times 616318177 \times 6561 \times 100895598169$$

Vous me demandiez ensuite ...

La question de Mersenne porte donc, non seulement sur la factorisation du nombre $F := 100895598169$, mais sur les "parties aliquotes" d'un certain nombre N. Nous allons maintenant préciser de quoi il est question.

2.2 Diviseurs et nombres parfaits

Sur ces questions le lecteur pourra consulter [6] sur le plan mathématique et [3] pour l'historique [17].

2.2.1 Définitions

Tout d'abord, la terminologie. Si n est un entier positif, le mot "parties aliquotes" de n est l'ancien nom qui désigne les diviseurs de n, à l'exception de n lui-même, donc ceux qui vérifient $1 \leq d < n$, et on dit qu'un nombre n est **parfait** s'il est somme de ses parties aliquotes, donc de ses diviseurs $\neq n$. Par exemple, $6 = 1+2+3$ ou $28 = 1+2+4+7+14$ sont parfaits. La recherche des nombres parfaits remonte à l'antiquité. On sait notamment depuis Euclide que les nombres de la forme $2^{p-1}(2^p - 1)$ sont parfaits, à condition que $2^p - 1$

17. Dans ce que rapporte Dickson on ne peut qu'être frappé par le nombre de bêtises qui se sont dites dans l'histoire à propos des nombres parfaits. Aujourd'hui, avec l'ordinateur qui permet d'infirmer les conjectures hasardeuses, on court moins ce risque.

soit premier [18], et Euler a montré que les nombres parfaits pairs sont tous de cette forme. Les suivants sont $n = 496 = 16 \times 31$, $8128 = 2^6 \times 127$, etc. On en connaît aujourd'hui 39 seulement mais on ignore toujours s'il y en a une infinité et s'il existe des nombres parfaits impairs.

2.2.2 Diviseurs et fonction σ

En fait, il est plus astucieux de considérer tous les diviseurs de n, y compris n, et d'introduire la fonction $\sigma(n) = \sum_{\substack{d|n \\ 1\leq d\leq n}} d$. La raison est dans la proposition suivante :

2.1 Proposition. *La fonction σ est multiplicative au sens de l'arithmétique, c'est-à-dire vérifie $\sigma(mn) = \sigma(m)\sigma(n)$ si m et n sont premiers entre eux.*

Démonstration. C'est le fait que tout diviseur d de mn s'écrit de manière unique $d = pgcd(d, m) \times pgcd(d, n) := ef$, donc comme produit d'un diviseur de m et d'un diviseur de n, et on a alors :

$$\sigma(mn) = \sum_{\substack{d|mn \\ 1\leq d\leq mn}} d = (\sum_{\substack{e|m \\ 1\leq e\leq m}} e)(\sum_{\substack{f|n \\ 1\leq f\leq n}} f) = \sigma(m)\sigma(n).$$

Ce résultat permet de ramener le calcul de $\sigma(n)$ à celui de ses facteurs primaires $\sigma(p^\alpha)$, avec p premier, qui est facile :

$$\sigma(p^\alpha) = 1 + p + p^2 + \ldots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1}.$$

En particulier, on a $\sigma(p) = p + 1$ si p est premier et $\sigma(2^{r-1}) = 2^r - 1$. Un nombre n est parfait si l'on a $\sigma(n) = 2n$.

2.2 *Remarque.* Il me semble clair que Fermat connaissait ce résultat (peut-être sous une forme légèrement différente). Je suppose que c'est à cela qu'il fait allusion dans sa lettre à Frenicle du 18 octobre 1640 :

Reste à vous parler de la proposition fondamentale des parties aliquotes, laquelle m'étoit tellement connue que je vous l'avois envoyée par la première lettre que je vous écrivis, laquelle on m'a dit depuis s'être égarée. ...
Outre que cette proposition est si naturelle, qu'il est impossible de déterminer et de trouver la moindre chose sur ce sujet, qu'elle ne se présente d'abord ...

18. Les nombres $2^p - 1$ sont ce qu'on appelle maintenant les nombres de Mersenne, mais ils pourraient à bon droit s'appeler nombres d'Euclide.

2.2.3 Euclide

Les nombres parfaits font l'objet de la dernière proposition d'Euclide concernant l'arithmétique (Livre IX Prop. 36) :

Étant donnée une suite de nombres à partir de l'unité en proportion doublée et tels que leur somme soit un nombre premier, le produit de cette somme par le dernier terme de la suite est un nombre parfait.

La proportion doublée est la suite $1, 2, 4, \ldots, 2^{r-1}$, dont la somme est $p = 1+2+\cdots+2^{r-1} = 2^r - 1$, supposé premier, et le nombre $N = p \times 2^{r-1}$ est alors parfait. En effet, on a $\sigma(N) = \sigma(p)\sigma(2^{r-1}) = (p+1)(2^r-1) = 2^r p = 2N$.

2.2.4 Cataldi

Sur le sujet des nombres parfaits, ou, ce qui revient au même, des nombres de Mersenne, $M_n = 2^n - 1$, il faut noter les contributions de Cataldi (1548-1626) qui trouve que $2^{13} - 1 = 8191$, $2^{17} - 1 = 131071$ et $2^{19} - 1 = 524287$ sont premiers (le dernier est le record de l'époque). Mais il croit que c'est vrai aussi pour 23, 29, 31 et 37, à tort sauf pour 31. En effet, 47 divise M_{23}, 233 divise M_{29} et 223 divise M_{37}.

Au XVII-ième siècle, le sujet intéresse Descartes, Frenicle, Mersenne, Fermat, etc. que nous retrouverons à propos des nombres multi-parfaits

2.2.5 Euler

C'est à Euler que revient le mérite de prouver la réciproque du résultat d'Euclide :

2.3 Proposition. *Tout nombre parfait pair est de la forme* $2^{p-1}(2^p - 1)$ *où* $2^p - 1$ *est premier (donc aussi* p*).*

Démonstration. Soit donc n parfait et pair, $n = 2^\alpha m$ avec $\alpha \geq 1$ et m impair. Dire que n est parfait signifie qu'on a $\sigma(n) = 2n$. Par ailleurs, on a $\sigma(n) = \sigma(2^\alpha)\sigma(m) = (2^{\alpha+1} - 1)\sigma(m)$. On a donc $2^{\alpha+1}m = (2^{\alpha+1} - 1)\sigma(m)$. Comme $2^{\alpha+1}$ est premier avec $(2^{\alpha+1} - 1)$, il divise $\sigma(m)$ et on a donc $\sigma(m) = b \times 2^{\alpha+1}$ et aussi $m = b(2^{\alpha+1} - 1)$. Si b est > 1, on a $\sigma(m) \geq 1 + b + m \geq b \times 2^{\alpha+1} + 1$ et c'est absurde. On a donc $m = 2^{\alpha+1} - 1$ et $\sigma(m) = 2^{\alpha+1}$, ce qui impose que m est premier.

2.3 Les nombres multi-parfaits

À défaut de nombres parfaits, qui vérifient $\sigma(n) = 2n$, on peut s'intéresser aux nombres multi-parfaits, c'est-à-dire ceux qui vérifient $\sigma(n) = kn$ où k

est un entier, le plus petit possible. Le nombre k est la multiplicité de n et on dit que n est un P_k. Nous verrons que c'est le cas du nombre proposé par Mersenne à Fermat qui est un P_6.

2.3.1 Historique

Sur ce sujet, [3] est une mine de renseignements.

Le plus petit nombre multi-parfait (non parfait) est 120 qui vérifie $\sigma(120) = 360 = 3 \times 120$ (c'est donc un P_3). Il y a ensuite $672 = 2^5 \times 3 \times 7$ (un autre P_3). Ces nombres sont sans doute connus depuis l'antiquité. Au XVII-ième siècle, plusieurs nouveaux nombres multi-parfaits sont découverts. André Jumeau, prieur de Sainte-Croix, donne le troisième P_3 : $523776 = 2^9 \times 3 \times 11 \times 31$ (1638) et le communique à Descartes, qui donne le quatrième : $1476304896 = 2^{13} \times 3 \times 11 \times 43 \times 127$. Descartes donne aussi six P_4 et un P_5. Les voici [19] :

$$P_4^1 = 30240 = 2^5 \times 3^3 \times 5 \times 7$$

$$P_4^2 = 32760 = 2^3 \times 3^2 \times 5 \times 7 \times 13$$

$$P_4^3 = 23569920 = 2^9 \times 3^3 \times 5 \times 11 \times 31$$

$$P_4^4 = 142990848 = 2^9 \times 3^2 \times 7 \times 11 \times 13 \times 31$$

$$P_4^5 = 66433720320 = 2^{13} \times 3^3 \times 5 \times 11 \times 43 \times 127$$

$$P_4^6 = 403031236608 = 2^{13} \times 3^2 \times 7 \times 11 \times 13 \times 43 \times 127$$

$$P_5^1 = 14182439040 = 2^7 \times 3^4 \times 5 \times 7 \times 11^2 \times 17 \times 19 \sim 4 \times 10^{11}.$$

Ces nombres sont obtenus grâce à quelques règles très simples (par exemple, si n est un P_3 non multiple de 3, $3n$ est un P_4).

Frenicle, Mersenne et Fermat proposent aussi un certain nombre de tels nombres. Dans une lettre à Carcavi, toujours de 1643, Fermat annonce avec un peu de suffisance qu'il a une méthode générale pour les trouver tous [20] :

C'est parmi d'autres que j'ai trouvés, que j'ai choisi par avance ceux-ci pour vous en faire part, afin que vous en puissiez juger par cet échantillon. J'ai trouvé la méthode générale pour trouver tous les possibles, de quoi je suis assuré que M. de Roberval sera étonné et le bon Père Mersenne aussi ; car il n'y a certainement quoi que ce soit dans toutes les Mathématiques plus

19. Il est facile d'écrire un programme qui calcule tous les nombres multi-parfaits jusqu'à 10^7, il n'y en a que 10, quatre parfaits (6, 28, 496, 8128), trois de multiplicité 3 (120, 672 et 523776) et trois de multiplicité 4 (30240, 32760 et 2178540).

20. Je ne crois pas une seconde qu'il détienne vraiment une telle méthode, mais il est clair qu'il a compris beaucoup de choses sur le sujet.

difficile que ceci, et hors M. de Frenicle[21] *et peut-être M. Descartes, je doute que personne en connoisse le secret, qui pourtant ne le sera pas pour vous ...*

À l'appui de cette affirmation, il donne plusieurs multi-parfaits, dont m et n ci-dessous (tous deux P_6) :

$$m = 2^{27} \times 3^5 \times 5^3 \times 7 \times 11 \times 13^2 \times 19 \times 29 \times 31 \times 43 \times 61 \times 113 \times 127 \sim 10^{28}$$

$$n = 2^{23} \times 3^7 \times 5^3 \times 7^4 \times 11^3 \times 13^3 \times 17^2 \times 31 \times 41 \times 61 \times 241 \times 307 \times 467 \times 2801 \sim 10^{40}.$$

2.3.2 Le nombre de Frenicle et le défi de Mersenne

Bernard Frenicle de Bessy (1605 ?-1675) est le moins connu[22] des protagonistes de cette histoire, voir [5]. Il a travaillé en astronomie et en mécanique, mais surtout en théorie des nombres où il a notamment produit de nombreux exemples de carrés magiques.

FIGURE 3 – Frenicle (si ce n'est lui ...)

Le nombre N proposé par Frenicle et transmis par Mersenne à Fermat est le suivant :

$$N = 214748364800000 \times 11 \times 19 \times 43 \times 61 \times 83 \times 169 \times 223 \times 331 \times 379 \times 601 \times$$

21. On voit ici que Fermat tient Frenicle en grande estime.

22. D'ailleurs, on ne trouve pas de portrait de lui sur Internet, celui donné ici est celui de son frère Nicolas, poète.

$$757 \times 961 \times 1201 \times 7019 \times 823543 \times 616318177 \times 6561 \times 100895598169.$$

Voici sa décomposition en produits de facteurs premiers (ou presque ...) :

$$N = 2^{36} \times 3^8 \times 5^5 \times 7^7 \times 11 \times 13^2 \times 19 \times 31^2 \times 43 \times 61 \times 83 \times 223 \times 331 \times 379 \times 601 \times$$

$$757 \times 1201 \times 7019 \times 616318177 \times 100895598169$$

Tous les nombres apparaissant ici sont effectivement premiers, sauf le dernier nombre qui est le défi de Mersenne à Fermat : $100895598169 = 898243 \times 112303$. Hormis ce dernier point, la décomposition est relativement facile à trouver. Par exemple, le premier nombre est égal à $2^{36} \times 5^5$, 823543 n'est autre que 7^7, etc. Le seul point non évident est le nombre (premier) 616318177 que Fermat avait déjà rencontré, comme nous le voyons maintenant.

2.3.3 Factorisation de $2^{37} - 1$

En 1643, Fermat connaît bien la décomposition du nombre $2^{37} - 1 = 223 \times 616318177$ en produit de nombres premiers [23]. En effet, grâce à ce qu'on appelle maintenant le petit théorème de Fermat, il sait qu'un éventuel diviseur premier de $2^{37} - 1$ doit être de la forme $k \times 2 \times 37 + 1$. Ce point est évoqué dans une lettre à Mersenne de juin 1640 : *Lorsque l'exposant est nombre premier* (ici 37)*, je dis que son radical* (ici $2^n - 1$) *ne peut être mesuré par aucun nombre premier que par ceux qui sont plus grands de l'unité qu'un multiple du double de l'exposant* (ici $k \times 74 + 1$). Ici, il n'y a pas besoin d'aller très loin comme le dit Fermat : *... j'ai commencé mes divisions par* 149*, plus grand de l'unité que le double de* 74*, puis continuant par* 223*, plus grand de l'unité que le triple de* 74*, j'ai trouvé que ledit radical est multiple de* 223. Le théorème de Fermat est énoncé peu après, dans une lettre à Frenicle du 18 octobre 1640 :

Tout nombre premier mesure infailliblement une des puissances -1 *de quelque progression que ce soit, et l'exposant de la dite puissance est sous-multiple du nombre premier donné* -1 *et après qu'on a trouvé la première puissance qui satisfait à la question, toutes celles dont les exposants sont multiples de l'exposant de la première satisfont tout de même à la question.*

En langage moderne : si p est premier et a quelconque premier à p, il existe n tel que $a^n \equiv 1 \pmod{p}$, avec n qui divise $p - 1$ et si r est l'ordre de a (le plus petit n possible), n est multiple de r.

23. En fait, Fermat ne devait pas être si sûr que le second nombre est premier. En effet, il est de l'ordre de 6×10^8 et nous verrons plus loin qu'il s'est fourvoyé sur l'exemple de $2^{32} + 1$ qui vaut environ 4×10^9, donc de taille comparable. Ici, grâce au petit théorème de Fermat il y a seulement 72 divisions à faire.

2.4 *Remarques.* 1) Fermat, qui ne calcule pas aussi bien que Frenicle, dit à plusieurs reprises qu'il trouve pénible de faire les divisions et cherche donc des méthodes pour les éviter et c'est ainsi qu'il découvre son théorème. Il y a d'ailleurs, sur ce même point de réduire les divisions à effectuer, un autre théorème qui apparaît dans une lettre à Roberval d'août 1640 : *Si un nombre est composé de deux quarrés premiers entre eux, je dis qu'il ne peut être divisé par aucun nombre premier moindre de l'unité qu'un multiple du quaternaire.* En clair : une somme de deux carrés $a^2 + b^2$ avec $\text{pgcd}(a, b) = 1$ n'admet pas de diviseur premier $p \equiv -1 \pmod 4$. Et il applique cette remarque au nombre $10000000001 = (10^5)^2+1^2$: *... et ainsi, lorsque vous voudrez éprouver s'il est nombre premier, il ne faudra point le diviser ni par* 3*, ni par* 7*, ni par 11, etc.*

2) On notera que, sur tous ces points, Fermat affirme qu'il a des démonstrations mais ne les donne jamais (lettre de juin) : *Voilà trois fort belles propositions que j'ai trouvées et prouvées non sans peine : je les puis appeler les fondements de l'invention des nombres parfaits.*

2.3.4 Le délit d'initié

Expliquons maintenant pourquoi Fermat n'a eu aucune peine à factoriser le nombre 100895598169. La question de Mersenne porte sur le nombre N de Frenicle et elle comporte notamment la phrase suivante : *Vous me demandiez quelle proportion a le nombre, qui se produit des nombres suivants, avec ses parties aliquotes.* Cela sous-entend que N est multi-parfait, avec un coefficient k petit, et à partir de là, le raisonnement est facile.

Le nombre N s'écrit $N = 2^{36} \times M$ avec M impair, de sorte que l'on a $\sigma(N) = \sigma(2^{36}) \times \sigma(M) = (2^{37} - 1) \times \sigma(M) = 223 \times 616318177 \times \sigma(M)$. Si l'on pense que $\sigma(N) = kN$ avec k petit, c'est que le nombre premier 616318177, qui divise $\sigma(N)$, divise aussi N. Mais alors, $\sigma(616318177) = 616318178 = 2 \times 7^3 \times 898423$ divise $\sigma(N)$ en vertu de la multiplicativité de σ. Encore une fois, si $\sigma(N) = kN$ avec k petit, c'est que 898423 (qui est premier) divise N. Mais en examinant les divers facteurs de N, on voit qu'un seul peut être multiple de 898423, c'est 100895598169, ce qu'une simple division permet de vérifier et on trouve $100895598169 = 898423 \times 112303$. On retrouve d'ailleurs ce dernier nombre dans $\sigma(898423) = 898424 = 2^3 \times 112303$.

Pour conclure, Fermat n'a plus qu'à vérifier qu'on a bien $\sigma(N) = kN$ (ici avec $k = 6$), ce qui se fait sans difficulté en calculant le σ de chaque facteur primaire. Il répond donc à Mersenne :

À la première question, je vous réponds que le nombre qui se fait de tous les nombres précédents multipliés entre eux, est sous-quintuple de ses parties (autrement dit $\sigma(N) - N = 5N$ car dans les parties aliquotes on ne tient pas

compte de N).

2.3.5 Comment Frenicle a-t-il trouvé ce nombre ?

Si, le nombre N étant donné, il est facile de vérifier qu'il est multi-parfait, le trouver est une autre histoire. On ne dispose d'aucun élément permettant de préciser comment Frenicle a procédé, mais on peut tenter une explication.

L'idée de départ est de partir du résultat d'Euclide : si 2^n-1 est premier, alors le nombre $2^{n-1}(2^n-1)$ est parfait, en prenant $n=37$. Comme on l'a vu, Frenicle sait que $2^{37}-1$ n'est pas premier, mais il garde sans doute l'idée de partir du nombre 2^{36} pour fabriquer un nombre multi-parfait. Voici comment on peut imaginer son raisonnement. On cherche N sous la forme $N=2^{36}\times M$ avec M impair. On a vu ci-dessus que cela impose que les facteurs de $\sigma(2^{36}) = 2^{37}-1 = 223\times 616318177$ soient dans N et que cela implique qu'y soient aussi 898423 et 112303. Si l'on poursuit [24] avec les nombres obtenus on trouve $\sigma(112303) = 2^4\times 7019$, puis $\sigma(7019) = 2^2\times 3^3\times 5\times 13$ et $\sigma(223) = 2^5\times 7$. Au point où nous en sommes, hormis tout ce qui se simplifie, on en est donc à 2^{36} "en haut" et $2^{15}\times 3^3\times 5\times 7^4\times 13$ "en bas".

Un algorithme (naïf) pour continuer, consiste à ajouter, en haut, les facteurs du bas, en commençant par les plus grands. On continue donc avec $\sigma(13) = 2\times 7$. On a maintenant, dans $\sigma(N)$, 7^5 qui donne $\sigma(7^5) = 2^3\times 3\times 19\times 43$. Ensuite, 43 donne $2^2\times 11$, 19 donne $2^2\times 5$ et 11 donne $2^2\times 3$. Le terme 5^2 donne 31, puis 2^5. Il y a maintenant 3^5 dans $\sigma(N)$. Comme $\sigma(3^5) = 2^2\times 7\times 13$ redonne des termes déjà traités, il vaut mieux [25] prendre 3^6 qui donne 1093, puis 547, puis 137 et 23. On constate avec ravissement qu'avec le nombre obtenu, on a $\sigma(N) = 6N$:

$$n = 2^{36}\times 3^6\times 5^2\times 7^5\times 11\times 13\times 19\times 23\times 31\times 43\times 137$$
$$\times 223\times 547\times 1093\times 7019\times 112303\times 898423\times 616318177.$$

Mais on constate aussi que ce nombre, n'est pas celui de Frenicle [26] (il est de l'ordre de 3×10^{57} tandis que celui de Frenicle est de l'ordre de 5×10^{76}).

2.3.6 Une hypothèse pour Frenicle ?

J'ignore évidemment comment Frenicle a procédé et son N me semble nettement plus difficile à trouver que celui de Mason. Il est clair qu'il y a sans

24. Pour écrire ce genre de choses, il est commode de mettre N au-dessus d'un trait horizontal et $\sigma(N)$ en dessous.

25. Sinon, il faut reprendre les calculs précédents, et tous les architectes vous déconseilleront la reprise en sous-œuvre.

26. Bien que plus facile à trouver que celui de Frenicle (à mon avis), il n'a été découvert qu'en 1911 par Mason.

doute une part de tâtonnements. Ce qui est sûr, c'est que si l'on a les chiffres pour $3, 5, 7$ on a gagné. En effet, on a $\sigma(3^8) = 13\times757$, $\sigma(5^5) = 2\times3^2\times7\times31$ et $\sigma(7^7) = 2^5\times5^2\times1201$. On élimine les nouveaux arrivants en commençant par les plus grands : $\sigma(1201) = 2\times601$, $\sigma(757) = 2\times379$, $\sigma(601) = 2\times7\times43$, $\sigma(379) = 2^2\times5\times19$, $\sigma(13^2) = 3\times61$, $\sigma(61) = 2\times31$, $\sigma(31^2) = 3\times331$, $\sigma(331) = 2^2\times83$, $\sigma(83) = 2^2\times3\times7$, $\sigma(43) = 2^2\times11$, $\sigma(11) = 2^2\times3$.

Mais il n'est nullement évident de trouver ces valeurs et je ne peux que m'incliner respectueusement devant l'ingéniosité de Frenicle, ce que faisait aussi Fermat (lettre à Mersenne du premier avril 1640) :

Pour Monsieur de Frenicle, ses inventions en Arithmétique me ravissent et je vous déclare ingénûment que j'admire ce génie qui, sans l'aide de l'algèbre, pousse si avant dans la connoissance des nombres entiers, et ce que j'y trouve de plus excellent consiste en la vitesse de ses opérations, de quoi font foi les nombres aliquotaires qu'il manie avec tant d'aisance.

2.3.7 Compléments

Le lecteur intéressé pourra lui-même fabriquer des nombres multi-parfaits en appliquant les méthodes vues ci-dessus, mais il ne tardera pas à se rendre compte que les choses ne sont pas toujours aussi simples et que trouver les bonnes valeurs est parfois difficile [27]. Ainsi, les deux exemples de Fermat cités plus haut ne sont pas totalement évidents. On aura accès à une table (due à Schroeppel) des nombres multi-parfaits connus en 2014 en se rendant à l'adresse `http://wwwhomes.uni-bielefeld.de/achim/mpn.html`.

Tout cela part d'une conjecture :

2.5 Conjecture. *Pour tout entier $\alpha \geq 1$ il existe un entier n multi-parfait dont la valuation 2-adique est égale à α.*

Par exemple, il y a beaucoup d'autres exemples de multi-parfaits commençant par 2^{36} (30 exemples dans la table de Schroeppel). Mais tous sont relativement récents : Mason (1911), Carmichaël (1911), Poulet (1929), etc. En voici quelques uns vérifiant $\sigma(n) = 6n$, les quatre premiers dus à Mason, le cinquième à Carmichaël.

$$2^{36}\times3^7\times5^3\times7^5\times11\times13^2\times19\times31\times41\times43\times61\times223\times7019\times112303\times898423\times616318177$$

$$2^{36}\times3^{10}\times5^2\times7^5\times11\times13\times19\times23\times31\times43\times107\times223\times3851\times7019\times112303\times898423\times616318177$$

$$2^{36}\times3^6\times5^2\times7^5\times11\times13\times19\times23\times31\times43\times137\times223\times547\times1093\times7019\times112303\times898423\times616318177$$

$$2^{36}\times3^8\times5^3\times7^5\times11\times13^3\times17\times19^2\times43\times127\times223\times379\times757\times7019\times112303\times898423\times616318177$$

$$2^{36}\times3^5\times5^4\times7^7\times11^2\times13^2\times19\times31\times43\times61\times71\times223\times601\times1201\times7019\times112303\times898423\times616318177$$

27. Je conseille de commencer par calculer les valeurs de $\sigma(p^\alpha)$ pour p premier et α entier assez petits.

3 Factorisation aujourd'hui : le code RSA

Pour des détails sur le code RSA le lecteur pourra consulter [8] ou [9] :

3.1 Le code RSA

À l'époque de Fermat, s'intéresser à la factorisation des nombres entiers pouvait passer pour un passe-temps futile [28] et c'était encore le cas jusqu'aux années 1970. Depuis, avec l'invention en 1977 du code RSA (des noms de ses auteurs Rivest, Shamir et Adleman), les choses ont bien changé.

Le code RSA est un procédé de codage qui comporte une clé publique composée de deux nombres N et e et une clé privée d. Pour coder les messages il suffit de connaître N et e, pour les décoder il faut détenir d. Le nombre N est le produit de deux grands nombres premiers p et q. Pour calculer d à partir de N et e, il faut disposer des deux nombres p et q. Ce qui assure la sécurité de ce code c'est qu'on sait fabriquer de très grands nombres premiers p et q, disons de 200 chiffres, que les multiplier est un jeu d'enfant pour une machine, mais que, pour des nombres de cette taille (400 chiffres) **on ne sait pas** retrouver p et q à partir de leur produit pq.

Pour illustrer le décalage entre primalité et factorisation, un bon exemple, avec le logiciel *xcas*, est le nombre de 65 chiffres suivant :

$$c = 33263290819929542686848148817697305155927928386133083389000759099 7.$$

La machine répond instantanément qu'il n'est pas premier, mais met environ 23 secondes pour le factoriser.

3.2 Trouver de grands nombres premiers

On sait depuis Euclide qu'il y a une infinité de nombres premiers mais il n'est pas si facile d'en donner explicitement de très grands. Fermat avait cru trouver une formule donnant à coup sûr des nombres premiers. Voici un extrait d'une lettre à Frenicle, d'août 1640 :

Mais voici ce que j'admire le plus : c'est que je suis quasi persuadé que tous les nombres progressifs augmentés de l'unité, desquels les exposants sont des nombres de la progression double, sont nombres premiers, comme 3, 5, 17, 257, 65537, 4 294 967 297 et le suivant de 20 lettres 18 446 744 073

28. Comme le disait Descartes : *Pour ce que les questions d'arithmétique peuvent quelquefois mieux être trouvées par un homme laborieux qui examinera opiniâtrement la suite des nombres, que par l'adresse du plus grand esprit qui puisse être, et que d'ailleurs elles sont très inutiles, je fais profession de ne vouloir pas m'y amuser.*

709 551 617; 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'aurois peine à me dédire.

La traduction en symboles de cette phrase c'est que, pour tout entier n, le nombre [29] $F_n = 2^{2^n} + 1$ est premier. C'est effectivement le cas pour $n = 0, 1, 2, 3, 4$ qui correspondent respectivement aux nombres premiers $3, 5, 17$, 257, 65537, mais ce n'est pas vrai [30] pour F_5 qui est divisible par 641 comme l'a montré Euler [31] On notera qu'à l'heure actuelle on ne sait pas exactement lesquels parmi les F_n sont premiers ou non. La réponse est seulement connue pour un nombre fini de n et, sauf pour les cinq du début, tous les F_n en question sont composés.

À défaut des nombres de Fermat, on peut utiliser les nombres de Mersenne : $M_n = 2^n - 1$ que nous avons déjà rencontrés. C'est avec ces nombres qu'on obtient les records du plus grand nombre premier connu. Le dernier date du 26 décembre 2017, c'est $M_{77232917}$, qui est un nombre de plus de 23 millions de chiffres. Pour d'autres précisions sur ce sujet, voir §7 (Annexe 3).

3.3 Factoriser des grands nombres ?

On aura compris que les ordres de grandeur des nombres premiers que l'on sait exhiber, d'une part, et des nombres que l'on sait factoriser, d'autre part, ne sont pas du tout les mêmes. Ainsi, le record absolu de factorisation (qui date du 12 décembre 2009) est bien loin de celui de primalité, c'est un nombre n de 232 chiffres, produit de deux nombres p et q de 116 chiffres, et encore a-t-il fallu pour cela faire travailler plusieurs centaines d'ordinateurs en parallèle pendant 2 ans sur un algorithme très complexe, ce qui représente environ 1500 années de temps de calcul pour une machine seule.

Voici ces nombres :

$$123018668453011775513049495838496272077285356959533479219732245215172640050726365751874520219978646938995647494277406384592519255732630345373154826850791702612214291346167042921431160222124047927473779408066535141959745985690214341 3$$

$$= 3347807169895689878604416984821269081770479498371376856891243138898288379387800228761471165253174308773781446799948 9 \times 3674604366679959042824463379962795263227915816434308764267 60$$

29. Le lecteur se convaincra que seuls les $2^r + 1$ où r est une puissance de 2 ont une chance d'être premiers.

30. Même un grand mathématicien peut dire des bêtises.

31. C'est très étrange que Fermat ne soit pas aperçu que 641 divisait $2^{32} + 1$. Voir une discussion au §6 (Annexe 2).

32283815739666511279233373417143396810270092798736308917

On notera tout de même qu'il y a seulement 30 ans, on estimait qu'il faudrait 50 milliards d'années pour factoriser un nombre de 150 chiffres. Les progrès accomplis par les mathématiciens et les ordinateurs sont donc considérables. Bien entendu, cela ne remet pas en cause la fiabilité du code RSA : si on sait factoriser un nombre $n = pq$ de 250 chiffres il suffit de choisir des nombres p et q plus grands. On a vu qu'il y a de la marge puisqu'on sait expliciter des nombres premiers avec des millions [32] de chiffres. Les banques travaillent déjà avec des clés n de l'ordre de 300 chiffres et les militaires avec des clés de 600 chiffres.

3.4 Le crible quadratique : l'algorithme naïf

La plupart des méthodes modernes de factorisation reposent sur ce qu'on appelle le crible quadratique, qui est une généralisation de la méthode de Fermat, voir §7 (Annexe 3) pour d'autres précisions.

3.4.1 Le principe général

On cherche à factoriser un entier impair N, par exemple produit de deux grands nombres premiers p, q. On a vu que la méthode de Fermat consistait à écrire $N = R^2 - S^2$, ce qui donne la factorisation. Réduisant un peu nos ambitions, on peut se contenter de chercher R et S tels que N **divise** $R^2 - S^2$, donc tels que $R^2 \equiv S^2 \pmod{N}$. En effet, si l'on dispose d'une telle écriture, on a $LN = (R-S)(R+S)$ et on trouve un facteur de N en prenant le *pgcd* de N et de, disons, $R-S$. Si ce *pgcd* vaut 1 c'est que N divise $R+S$ (en vertu du théorème de Gauss), s'il vaut N c'est que N divise $R-S$, dans tous les autres cas, on obtient un diviseur non trivial de N. Autrement dit, si N ne divise ni $R-S$ ni $R+S$, ce procédé donne des facteurs non triviaux de N. De plus, le calcul du *pgcd* est très facile et très rapide en utilisant l'algorithme d'Euclide.

On notera que, si l'on dispose d'une écriture $LN = R^2 - S^2$, il y a de bonnes chances que N ne divise ni $R-S$ ni $R+S$. Ainsi, dans le cas $N = pq$, la probabilité est exactement $1/2$ comme on le voit en écrivant le lemme chinois $\mathbf{Z}/N\mathbf{Z} \simeq \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/q\mathbf{Z}$. Si on écrit $R = (a, b)$ et $S = (c, d)$, la condition $R^2 \equiv S^2$ donne $a^2 = c^2$ et $b^2 = d^2$. Si $c \equiv a$ et $d \equiv b$, N divise $R - S$, si $c \equiv -a$ et $d \equiv -b$, il divise $R + S$. En revanche si l'on a $c \equiv a$ et $d \equiv -b$ ou $c \equiv -a$ et $d \equiv b$, on a une solution acceptable.

32. Leur forme particulière disqualifie les nombres de Mersenne comme clés RSA, mais les logiciels comme Pari fournissent sans problème des nombres premiers de 5000 chiffres et *xcas* en donne de plus de 1500 chiffres en 40 secondes.

3.4.2 Un algorithme naïf

Cela permet de construire un algorithme naïf et brutal pour factoriser N. On parcourt les entiers L à partir de 1. Pour L fixé, on part de $R_0 := \lceil \sqrt{LN} \rceil$, partie entière supérieure de la racine (comme Fermat) et on parcourt les $R = R_0 + u$ en s'arrêtant si $R^2 - LN$ est un carré S^2.

Voici un programme écrit avec *xcas* qui met en œuvre cet algorithme. Ce programme est organisé pour augmenter progressivement la somme $n = L + u$:

```
naif(N):={local L,R0,R,S,u,n,L0;
L0:=1; u:=0; n:=L0+u;
R0:=ceil(sqrt(L*N)); R:=R0+u;
S:=sqrt(R^2-L*N);
tantque floor(S)!=S faire
pour L de L0 jusque n faire
u:=n-L; R0:=ceil(sqrt(L*N)); R:=R0+u; S:=sqrt(R^2-L*N);
fpour
n:=n+1; L0:=L;
ftantque
Disp L-1, gcd(N,R-S), gcd(N,R+S); }:;
```

Dans le cas du nombre N de Frenicle ($F = 100895598169$), ce programme donne instantanément la factorisation cherchée (le L est égal à 32).

Bien entendu, pour que cet algorithme soit raisonnable il faut que L et u soient assez petits, ou encore [33] que L et S soient petits. Nous analysons maintenant cette condition.

3.4.3 Analyse de l'algorithme naïf : les couples périlleux

Nous donnons ici un résultat un peu vague, qui sera précisé plus loin (voir Annexe 2, 8.5, 8.6, 8.7) :

3.1 Proposition. *Soient p, q deux (grands) nombres premiers et posons $N = pq$. Les conditions suivantes sont équivalentes :*

1) Il existe des entiers positifs L, R, S, avec L et S petits, vérifiant $LN = R^2 - S^2$.

2) Il existe des entiers positifs k, l, z avec k, l petits et z grand et des entiers relatifs a, b petits, tels que l'on ait $p = kz + a$ et $q = lz + b$.

3) Les nombres p, q vérifient une relation de Bézout $lp - kq = m$ avec k, l positifs et $m \in \mathbf{Z}$, $k, l, |m|$ petits.

33. En effet, dire que u est petit signifie que R proche de $\sqrt{LN}$, donc R^2 proche de LN, donc S^2 petit.

4) La fraction p/q est proche d'une fraction k/l avec k, l petits.
Un couple (p, q) qui vérifie ces propriétés sera dit **périlleux**.

Démonstration. L'équivalence de 3) est 4) est claire : si on a $lp - kq = m$ on en déduit $\frac{p}{q} - \frac{k}{l} = \frac{m}{lq}$ et inversement.

Si on a 2), donc l'écriture $p = kz + a$, $q = lz + b$, on a aussitôt 3) : $lp - kq = la - kb := m$, puis 1) avec $L = 4kl$, $R = kq + lp$, $S = lp - kq$.

Si l'on a 1), $LN = R^2 - S^2$, avec L, S petits (donc R grand), ou bien L est impair, ou bien il est multiple de 4. Supposons par exemple L impair, l'autre cas est analogue. On a $LN = Lpq = (R - S)(R + S)$. Si p, q divisent tous deux $R+S$, on a $R+S = uN$, donc $L = u(R-S)$. Mais c'est impossible car alors R serait petit. On élimine, de même, le cas où p et q divisent $R - S$. On peut donc supposer, par exemple, qu'on a $R - S = lp$ et $R + S = kq$, donc $kq - lp = 2S$, ce qui donne 3). Pour l'implication 3) $\Longrightarrow$ 2), si l'on a $lp - kq = m$ avec k, l, m petits, on montre que l'on a aussi une relation de Bézout $la - kb = m$ avec a, b petits et on obtient le résultat voulu par différence, voir Annexe 2, 8.2.

3.2 *Exemple.* Pour $p = 112303$ et $q = 898423$ (facteurs de $F = 100895598169$), on peut prendre $k = 1$, $l = 8$, $z = 112302$, $a = 1$ et $b = 7$. Plus généralement, si l'on se souvient que ces nombres ont été fabriqués à l'aide de la fonction σ (voir §2.2.2), on constate que si q est un grand nombre premier et p un grand facteur premier de $\sigma(q) = q + 1$, i.e. $q + 1 = kp$ avec k petit, le couple (p, q) est périlleux car on a $kp - q = 1$.

3.4.4 La problématique du chiffreur

Lorsque le chiffreur choisit les nombres p et q, il doit se prémunir [34] contre le fait que le couple soit périlleux car, s'il l'est, l'algorithme naïf permet de factoriser le produit pq, donc de casser le code. Pour tester si un couple est périlleux, il y a un algorithme très simple qui repose sur l'algorithme d'Euclide [35] et qui donne la taille de p, q (c'est-à-dire, avec les notations du point 3) de 3.1, le nombre $T := \mathrm{Max}\,(k, l, |m|)$). Voici le programme écrit pour *xcas* :

```
taille(p,q):={
local c,lp, lq, lr, Q, T, t;
si p<q alors c:=q; q:=p; p:=c; fsi
lp:=[1,0,p];
```

34. Il y a bien d'autres précautions à prendre lorsqu'on utilise le code RSA. Sur ce sujet, on se reportera au très intéressant article de Boneh, voir [1].

35. Pour une justification, voir 8.20.

```
T:=max(abs(lp[0]),abs(lp[1]),abs(lp[2]));
lq:=[0,1,q];
t:=max(abs(lq[0]),abs(lq[1]),abs(lq[2]));
tantque t<T faire
Q:=iquo(lp[2],q);
lr:=lp+(-Q)*lq; lp:=lq; lq:=lr; q:=lq[2];
T:=max(abs(lp[0]),abs(lp[1]),abs(lp[2]));
t:=max(abs(lq[0]),abs(lq[1]),abs(lq[2]));
ftantque
retourne T; }:;
```

Par exemple, dans le cas des facteurs p, q du nombre F de Frenicle, on trouve $T = 8$. En revanche, avec des nombres voisins $p = 112901$, $q = 899413$, on a $T = 948$ et le programme naïf, qui donnait la réponse instantanément dans le cas de F, met ici 7.6 secondes pour factoriser le produit.

3.4.5 La problématique du déchiffreur

Pour le déchiffreur, s'il suspecte que le couple p, q est périlleux, il s'agit de trouver une écriture de la forme $p = kz + a$, $q = lz + b$. Si tel est le cas, on a $N = pq = klz^2 + (kb + la)z + ab := Kz^2 + Az + B$, avec K, A, B petits, et on peut interpréter cette écriture comme une division euclidienne itérée de N par z : B est le reste dans la division euclidienne de N par z et, si Q en est le quotient, A est le reste dans la division euclidienne de Q par z et K le quotient. Cette opération est facile à programmer. On l'applique en faisant varier K de 1 jusqu'à la patience de l'utilisateur et en prenant $z = \lfloor \sqrt{N/K} \rfloor$. On repère pour quels K les nombres B et A sont tous deux petits. Il n'y a plus alors qu'à résoudre en k, l, a, b le système $kl = K$, $kb + la = A$, $ab = B$. Si l'on trouve des solutions entières on obtient la factorisation cherchée.

3.3 *Exemple.* Avec $F = 100895598169$, la tabulation de A, B selon K fait apparaître les valeurs $K = 8$, $A = 15$, $B = 7$, seul cas où $B < 1000$ pour $K \leq 20$. La résolution fournit aussitôt $k = 1$, $l = 8$, $a = 1$, $b = 7$.

3.4 *Remarque.* Si l'on imagine faire ce calcul à la main, il comporte 8 extractions de racines carrées ($\sqrt{KN}$ pour K variant de 1 à 8) et les 8 divisions de N par la valeur précédente. C'est lourd, mais pas infaisable. Pour calculer les racines carrées, une variante un peu plus simple consiste à faire, une fois pour toutes, la liste des $\sqrt{1/K}$ pour K petit (par exemple $\sqrt{1/2} = 0.707106$) et à multiplier $\sqrt{N}$ par ces quantités. À partir de $[\sqrt{N}] = 317640$, on obtient $[\sqrt{N/2}] = 224605$. En réalité, avec l'intuition de Fermat, il n'y a pas besoin d'aller plus loin ! En effet, la division de N par 224605 donne : $N = 224605 \times 449213 + 112304$ et on constate que le quotient est à peu près

le double du diviseur 224605 (ce qui est normal) mais surtout que le reste en est environ la moitié. Si l'on écrit tous ces nombres à partir de $n = 112303$, on constate avec ravissement qu'on a la factorisation $N = n(8n-1)$! C'est d'ailleurs encore plus évident si l'on fait la division par la partie entière supérieure $\lceil\sqrt{N/2}\rceil = 224606$ car le reste est alors 112303, exactement la moitié du diviseur et il est donc en facteur [36]. Nul doute que Fermat aurait pu trouver la factorisation par cette méthode !

3.5 *Remarque.* Le lien avec le crible quadratique c'est que si l'on a une écriture comme ci-dessus, l'équation en z, $Kz^2 + Az + B - N = 0$ admet une solution entière, ce qui impose en tous cas que son discriminant $\Delta = A^2 - 4K(B-N) = (kb-la)^2 - 4KN$ est un carré R^2, donc que $4KN$ est différence de deux carrés, $4KN = R^2 - S^2$ avec $S = kb - la$.

3.6 *Exemple.* On trouvera en 8.4.6 un exemple d'un nombre de 70 chiffres, produit des éléments d'un couple périlleux, que *xcas* met 94 secondes à factoriser avec son algorithme ordinaire et que la méthode ci-dessus permet de factoriser en moins de 3 secondes.

Conclusion : l'héritage de Fermat

Plus de trois cents ans après sa mort, il est indéniable que l'apport de Fermat, ne serait-ce qu'en théorie des nombres, est capital. Bien sûr, son nom est resté attaché à son "grand" théorème qui a coûté tant d'efforts aux mathématiciens avant d'être démontré par Andrew Wiles en 1993. Mais, si l'on regarde les questions liées à la primalité et à la factorisation, on voit que ses contributions sont encore à la base des techniques les plus pointues d'aujourd'hui, le petit théorème de Fermat pour la primalité et l'idée d'écrire $N = R^2 - S^2$ pour la factorisation. D'ailleurs, ses contemporains étaient conscients qu'ils avaient affaire à un vrai génie. Pour s'en convaincre, voici un extrait de la préface d'un livre (*Doctrinæ Analyticæ Inventum Novum*) du révérend père Jacques de Billy paru en 1670, quelques années après la mort de Fermat :

Il suffit qu'en tête de cet Ouvrage apparaisse le nom de Fermat pour que vous attendiez quelque chose de grand ; un tel homme n'a rien pu imaginer qui soit petit, rien même qui soit médiocre ; son esprit était illuminé de tant de clartés qu'il ne souffrait rien d'obscur ; vous eussiez dit un soleil qui en un instant dissipe les ténèbres, et dont les rayons innombrables portent une éclatante lumière au sein même des abîmes.

36. Ici, on a $p = z+1$ et $q = 8z+7$, $N = 8z^2 + 15z + 7$. La partie entière de $\sqrt{N/8}$ est z et la partie entière supérieure donne aussitôt le diviseur de N.

On ne saurait rêver plus belle épitaphe !

4 Annexe 0 : controverses et défis

4.1 Une controverse

Descartes à Mersenne, parlant de Fermat (janvier 1638) :

Je serois bien aise de ne rien dire de l'Ecrit que vous m'avez envoyé, pource que je ne saurois dire aucune chose qui soit à l'avantage de celui qui l'a composé. Mais à cause que je reconnois que c'est celui même qui avoit ci-devant tâché de réfuter ma Dioptrique et que vous me mandez qu'il a envoyé ceci après avoir lu ma Géométrie et s'étonnant que je n'avois point trouvé la même chose, c'est-à-dire, comme j'ai sujet de l'interpréter, à dessein d'entrer en concurrence et de montrer qu'il sait en cela plus que moi ; puis aussi à cause que j'apprends par vos lettres qu'il a la réputation d'être fort savant en géométrie, je crois être obligé de lui répondre.

L'amende honorable (Descartes à Fermat, juillet 1638) :

Je n'ai pas eu moins de joie de recevoir la Lettre par laquelle vous me faites la faveur de me promettre votre amitié, que si elle me venoit de la part d'une maîtresse dont j'aurois passionnément désiré les bonnes grâces : et vos autres écrits qui ont précédé me font souvenir de la Bradamante de nos poëtes laquelle ne vouloit recevoir personne qui ne se fût auparavant éprouvé contre elle au combat.

Ce n'est pas toutefois que je prétende me comparer à ce Roger qui étoit seul au monde capable de lui résister ; mais, tel que je suis, je vous assure que j'honore extrêmement votre mérite. Et voyant la dernière façon dont vous usez pour trouver les tangentes des lignes courbes, je n'ai autre chose à y répondre, sinon qu'elle est très bonne et que, si vous l'eussiez expliquée au commencement en cette façon, je n'y eusse point du tout contredit.

4.2 Un défi

Fermat à Digby, lettre du 6 juin 1657.

... j'ai demandé un nombre cube en nombres entiers, lequel ajouté à toutes ses parties aliquotes, fasse un nombre quarré. J'ai donné par exemple 343 *qui est cube et aussi nombre entier, lequel ajouté à toutes ses parties aliquotes, fait 400, qui est un nombre quarré ... Et si le Mylord Brouncker répond qu'en entiers il n'y a que le seul nombre* 343 *qui satisfasse à la question, je vous promets et à lui aussi de le désabuser en lui en exhibant un autre.*

En formules, il s'agit de trouver n tel que $\sigma(n^3)$ soit un carré a^2 (ici $n = 7$, $a = 20$). Wallis a donné plusieurs solutions à ce problème, la plus petite étant $n = 2.3.5.13.41.47 = 751530$ qui donne $a = 2^7.3^2.5^2.7.13.17.29$, voir [3].

5 Annexe 1 : sur l'extraction de racine carrée

5.1 L'algorithme de la potence

Décrivons cet algorithme dans le cas des entiers. Soit N l'entier dont on cherche la racine entière c à une unité près : $c^2 \leq N < (c+1)^2$. On écrit cet entier en base 100 : $N = \sum_{i=0}^{r} a_i\ 100^i$ avec $r \geq 0$ et les a_i entiers compris entre 0 et 99 (par rapport à l'écriture en base 10 on regroupe les chiffres deux par deux). Ainsi, $N = 20\,27\,65\,12\,81$ s'écrit $20 \times 100^4 + 27 \times 100^3 + 65 \times 100^2 + 12 \times 100 + 81$. On considère d'abord l'entier dominant dans N : $a_r 100^r$, ici 20×100^4 et on trouve un encadrement de $\sqrt{a_r}$ à une unité près : $b_r \leq \sqrt{a}_r < b_r + 1$, ou encore $b_r^2 \leq a_r < b_r^2 + 2b_r + 1$, avec $0 \leq b_r \leq 9$. Dans l'exemple, on a $b_r = 4$. Cela donne déjà l'encadrement $(10^r b_r)^2 \leq a_r 100^r < (10^r(b_r+1))^2$, ici $40000^2 \leq 20 \times 100^4 < 50000^2$.

Le pas suivant de l'algorithme consiste à "abaisser" la tranche de chiffres suivante, donc à regarder $a_r 100^r + a_{r-1}100^{r-1} = (100a_r + a_{r-1})\,100^{r-1}$. Plus généralement, si l'on a une racine carrée approchée B de A à une unité près, vérifiant donc $B^2 \leq A < (B+1)^2$, ou encore $A - B^2 \leq 2B$, on cherche une racine de $100A+a$, avec $0 \leq a < 100$, à une unité près, sous la forme $10B+b$, avec $0 \leq b < 10$. Le calcul repose sur la formule $(x+y)^2 = x^2 + 2xy + y^2$:

$$(10B+b)^2 = 100B^2 + 20Bb + b^2 \leq 100A + a < (10B + b + 1)^2.$$

On cherche alors le plus grand b tel que $20Bb + b^2 \leq 100(A - B^2) + a$. La condition $100(A - B^2) \leq 200B$ montre qu'un tel b est ≤ 9 (car $b = 10$ donne $20Bb + b^2 = 200B + 100 > 200B + a$).

Dans le cas qui nous intéresse, on a $A = 20$, $a = 27$, $B = 4$ et on cherche le plus grand b tel que $80b + b^2 \leq 427$. Il est clair que c'est $b = 5$.

On poursuit ainsi l'algorithme jusqu'à la tranche des unités. Ici, au pas suivant, on abaisse 65 et on a 265. On cherche $\bullet$ avec $90\bullet \times \bullet \leq 265$, d'où $\bullet = 0$. On abaisse 12 et on cherche $900\bullet \times \bullet \leq 26512$, d'où $\bullet = 2$ avec reste 8508. Enfin on abaisse le 81 et on cherche $\bullet$ tel que $9004\bullet \times \bullet \leq 850881$ on trouve $\bullet = 9$ et la racine 45029, ainsi que le reste 40440. L'algorithme est présenté en général sous la forme suivante (la potence) :

20	27	65	12	81	45029
-16					
4	27				$85 \times 5 = 425$
-4	25				
	2	65	12		$900 \times 0 = 0$
	-1	80	04		
		85	08	81	$9002 \times 2 = 18004$
		81	04	41	
		4	04	40	$90049 \times 9 = 810441$

5.2 La méthode de Héron

L'algorithme proposé par Héron d'Alexandrie (vers 10-vers 70 après J.-C. ?) consiste, pour calculer $\sqrt{N}$ à partir d'une valeur approchée x_0, à calculer $x_1 = \frac{1}{2}(x_0 + \frac{N}{x_0})$ et à recommencer éventuellement. Cet algorithme est prodigieusement rapide (c'est un cas particulier de la méthode de Newton). Par exemple, dans le cas du nombre $N = 2027651281$, on voit aisément que la racine carrée est de l'ordre de $x_0 = 45000$ (car $45^2 = (90^2)/4 = 2025$). Alors, le x_1 donné par Héron est un nombre dont la partie entière est exactement 45029, c'est-à-dire la partie entière de $\sqrt{N}$! Cela étant, aucun élément ne permet de penser que Fermat utilisait cette méthode.

6 Annexe 2 : Fermat, la primalité et le petit théorème

6.0.1 Fermat et la primalité

Dans une lettre à Mersenne du 26 décembre 1638, voilà ce que dit Fermat :

Sur lequel sujet [la recherche des nombres premiers] *je ne sais point de méthode que la vulgaire sinon qu'il suffit de faire la division jusques à la plus petite racine quarrée du nombre donné ...*

Un certain nombre de travaux de Fermat ont pour origine sa répugnance à faire de nombreuses divisions pour montrer qu'un nombre est premier (lettre à Mersenne, avril 1640) :

... il me semble que je vois devant moi Magnum maris æquor arandum [37] *à cause de ces fréquentes divisions qu'il faut faire pour trouver les nombres premiers.*

37. Une grande mer à labourer (Virgile, l'Énéide).

C'est sans doute pour s'éviter les divisions qu'il invente son petit théorème. En effet, si l'on cherche un diviseur premier p de $a^n - 1$, on a $a^n \equiv 1 \pmod{p}$, de sorte que n divise $p - 1$. C'est ainsi, en particulier, que Fermat trouve facilement le diviseur 223 de $2^{37} - 1$, voir la lettre à Mersenne de juin 1640 en 2.3.3 ci-dessus.

Un autre point : il affirme que les facteurs du défi de Mersenne, 898423 et 112303, sont premiers. Peut-être a-t-il vérifié cela (il faut respectivement 161 et 67 divisions). Peut-être simplement a-t-il fait confiance à Frenicle car, pour que le calcul de $\sigma(N)$ fonctionne et donne le résultat escompté, il faut que ces nombres soient premiers !

6.0.2 Compléments

La lettre à Frenicle du 18 octobre 1640 est, elle aussi, absolument passionnante. En effet, outre l'énoncé de son petit théorème ($a^{p-1} \equiv 1 \pmod{p}$ si p est premier), il se pose la question de l'ordre de a et en particulier quand cet ordre est-il impair. Il montre, en substance :

6.1 Proposition. *Soit p un nombre premier $\equiv -1 \pmod{4}$ et soit a premier à p. On suppose que a est un carré modulo p. Alors, a est d'ordre impair modulo p.*

Démonstration. D'abord, on a $p - 1 = 2q$ avec q impair. Ensuite, on a $a = b^2$ modulo p et $b^{p-1} = a^q \equiv 1$. L'ordre de a étant un diviseur de q est impair.

Je recopie la partie de la lettre qui explique cela. Il pose d'abord le problème :

En un mot, il faut déterminer quels nombres premiers sont ceux qui mesurent leur première puissance -1 en telle sorte que l'exposant de la dite puissance soit un nombre impair ...

Puis il donne le critère :

En la progression double, si d'un nombre quarré, généralement parlant, vous ôtez 2 *ou* 8 *ou* 32 *etc. les nombres premiers moindres de l'unité d'un multiple du quaternaire, qui mesureront le reste, feront l'effet requis.*

Comme de 25*, qui est un quarré, ôtez* 2 *: le reste* 23 *mesurera la* 11*-ième puissance moins* 1*.*

Otez 2 *de* 49*, le reste* 47 *mesurera la* 23*-ième puissance moins* 1*.*

Otez 2 *de* 225*, le reste* 223 *mesurera la* 37*-ième puissance moins* 1*.*

En la progression triple, si d'un nombre quarré up supra *vous ôtez* 3 *ou* 27 *ou* 243*, etc. les nombres les nombres premiers moindres de l'unité d'un multiple du quaternaire, qui mesureront le reste, feront l'effet requis.*

Comme :

Otez 3 *de* 25*, le reste* 22 *est divisé par* 11*, qui est premier et moindre de l'unité qu'un multiple du quaternaire ; aussi* 11 *mesure la* 5*-ième puissance* -1.

Il donne un autre exemple avec 3 (121) puis passe à 4 en ôtant 4 ou 64 ou 1024 et il dit : *à l'infini en toutes progressions, en procédant de la même façon.*

En fait, un argument très voisin aurait pu lui servir pour repérer le nombre 641 comme diviseur potentiel de $2^{32}+1$:

6.2 Proposition. *Si p premier divise $2^{32}+1$, $p-1$ est multiple de* 128*.*

Démonstration. Il suffit de montrer que 2 est un carré modulo p. En effet, si $2 \equiv a^2 \pmod{p}$ on a $a^{64} \equiv 2^{32} \equiv -1 \pmod{p}$, donc a est d'ordre 128 et 128 divise $p-1$.

Pour cela, il suffit de montrer[38] que si on a $p \equiv 1 \pmod 8$, 2 est un carré modulo p. Il y a deux voies. Soit on sait que $\mathbf{F}_p^*$ est cyclique d'ordre $p-1$, donc contient un élément ζ d'ordre 8, qui vérifie donc $\zeta^4+1=0$, donc $\zeta^2+\zeta^{-2}=0$, et on voit que $a=\zeta+\zeta^{-1}$ vérifie $a^2=2$.

Soit on sait ça, mais on fait semblant de ne pas le savoir et on regarde une racine huitième explicite, à savoir 2^8 et son inverse $2^{56}=-2^{24}$ et on montre que $a=2^8-2^{24}$ a pour carré 2. En effet, on a $(2^8-2^{24})^2=2^{16}+2^{48}-2.2^{32}$ et cela résulte de $2^{32}=-1$.

6.3 *Remarques.* 1) Au vu de ces résultats de Fermat on ne peut que s'étonner qu'il n'ait pas vu le diviseur 641 de $2^{32}+1$. Même sans le résultat de 6.2, il savait, avec le petit théorème de Fermat, qu'il fallait chercher un éventuel facteur premier parmi les nombres de la forme $64k+1$, ce qui ne demandait que 4 divisions, par $193, 449, 577$ et 641 (avec 6.2 il n'y a plus que 641). J'imagine que Fermat s'est trompé dans cette dernière. Il est aussi assez étrange que Frenicle n'ait pas relevé l'erreur, mais peut-être (il n'est pas très algébriste) n'avait-il pas bien compris le petit théorème de Fermat ?

2) La première évocation de ce résultat (?) date d'août 1640 (lettre à Frénicle) mais il y croit toujours en 1654 (lettre à Pascal du 29 août, p. 309-310 des œuvres) : *C'est une propriété de la vérité de laquelle je vous réponds. La démonstration en est très malaisée et je vous avoue que je n'ai pu encore la trouver pleinement : je ne vous la proposerois pas pour la chercher si j'en étois venu à bout.*

38. Résultat bien connu aujourd'hui.

7 Annexe 3 : les méthodes modernes de primalité et factorisation

Nous donnons juste un premier aperçu sur le sujet. Pour de plus amples renseignements sur les méthodes modernes concernant primalité et factorisation, le lecteur consultera l'excellent livre d'Henri Cohen [2].

7.1 Primalité

7.1.1 Fermat, Carmichaël, Miller-Rabin

La plupart [39] des tests de primalité modernes sont fondés sur le petit théorème de Fermat. En effet, si p est premier et a entier quelconque, on a $a^p \equiv a \pmod{p}$. Autrement dit, si cette relation n'est pas vérifiée pour un certain a, c'est que p n'est pas premier. Par exemple, on a $2^{2020} \equiv 661 \pmod{2021}$, ce qui montre que 2021 n'est pas premier (c'est 43×47). Attention cependant, ce test ne donne pas un critère sûr de primalité. En effet, il existe des nombres p, dits de Carmichaël, qui vérifient $a^p \equiv a \pmod{p}$ pour tout a et qui pourtant ne sont pas premiers. Les plus petits sont 561 et le nombre de Ramanujan 1729 et Alford, Granville et Pomerance ont montré en 1994 qu'il y a une infinité de nombres de Carmichaël.

Un autre test est le suivant :

7.1 Proposition. (Miller-Rabin) *Soit N un entier impair et a un entier. On écrit $N - 1 = 2^l q$ avec q impair. Si N est premier, ou bien $a^q \equiv 1 \pmod{N}$ ou bien il existe e avec $0 \leq e < l$ tel que $a^{2^e q} \equiv -1 \pmod{N}$. Si N n'est pas premier ce résultat est faux pour les $3/4$ des a avec $1 < a < N$.*

Démonstration. Supposons N premier. Soit a premier à N. Si l'on n'a pas $a^q \equiv 1 \pmod{N}$, il y a un plus grand e, $0 \leq e < l$ tel que $b := a^{2^e q} \not\equiv 1 \pmod{N}$. On a alors $b^2 \equiv 1$, donc $b \equiv -1$ (on est dans un corps, il n'y a que deux racines de 1 qui sont 1 et -1).

Ce test permet de traiter le cas du nombre de Ramanujan 1729 : on a $2^{27}, 2^{2\times 27} \not\equiv \pm 1 \pmod{1729}$ mais $2^{4\times 27} \equiv 1 \pmod{1729}$. Il donne un algorithme probabiliste : si test de Miller-Rabin est positif pour un a, la probabilité que p soit composé est $\leq 1/4$, s'il est vrai pour deux nombres a, b elle n'est plus que de $1/16$, etc. Avec l'hypothèse de Riemann généralisée on a même un algorithme déterministe (si p n'est pas premier, il y a un $a < 2\ln^2 N$ qui met en défaut Rabin-Miller).

39. Il y a aussi des méthodes utilisant les courbes elliptiques.

7.1.2 Le test de Lucas

Il s'agit d'un test très simple, spécifique aux nombres de Mersenne. Pour voir si $p := 2^n - 1$ est premier, on calcule par récurrence la suite (u_n) avec $u_0 = 4$ et $u_{n+1} = u_n^2 - 2$ modulo p et le nombre p est premier si et seulement si $u_{n-2} \equiv 0 \pmod{p}$. Ce test est prodigieusement efficace. Ainsi, *xcas* échoue à prouver que $2^{2443} - 1$ est premier directement, alors qu'un programme fondé sur le test de Lucas le donne instantanément. De même, il donne le cas $n = 23209$ en 19 secondes (c'est un nombre de 6987 chiffres, connu seulement depuis 1979) ; pour $n = 44497$ (13395 chiffres) il met 94 secondes, pour $n = 86243$ (25962 chiffres), 374 secondes !

Pour des détails sur le test de Lucas on pourra consulter :
`https://www.math.u-psud.fr/perrin/CAPES/arithmetique/Lucas.pdf`

7.2 Factorisation et crible quadratique : Kraitchik et Pomerance

Le point de départ est le même que ci-dessus : un entier N étant donné à factoriser, on cherche des entiers R, S tels que $R^2 \equiv S^2 \pmod{N}$. Une méthode pour cela remonte à Kraitchik (voir [7]) et a été développée par Pomerance (voir [10]). Elle consiste à chercher des entiers R_i (un peu plus grands que $\sqrt{N}$) tels que $R_i^2 - N$ n'ait que des petits facteurs premiers. Précisément, on se donne une borne B et on regarde les entiers B-friables (c'est-à-dire à facteurs premiers plus petits que B). Soit r le nombre de nombres premiers $\leq B$, et notons $p_1, \ldots, p_r$ ces nombres.

7.2 Proposition. *On suppose qu'il existe n nombres $R_i > \sqrt{N}$ distincts avec $n > r$ tels que $Q_i := R_i^2 - N$ soit B-friable. Alors, il existe des entiers $i_1, \ldots, i_k$ (avec $k \geq 1$) tels que le produit $Q_{i_1} \cdots Q_{i_k}$ soit un carré S^2 et N divise alors $R^2 - S^2$ avec $R = R_{i_1} \cdots R_{i_k}$.*

Démonstration. Comme on a $k \geq 1$, la dernière assertion est claire avec la formule $S^2 = (R_{i_1}^2 - N) \cdots (R_{i_k}^2 - N)$. Posons $Q_j = p_1^{\alpha_{1,j}} \cdots p_r^{\alpha_{r,j}}$. Pour trouver les i_k, on cherche des entiers λ_i égaux à 0 ou 1 tels que $Q_1^{\lambda_1} \cdots Q_n^{\lambda_n}$ soit un carré. Sur les exposants, cela signifie que, pour tout $i = 1, \ldots, r$, $\lambda_1 \alpha_{i,1} + \cdots + \lambda_n \alpha_{i,n} = 0$ est pair, donc nul modulo 2. On est donc ramené au lemme suivant :

7.3 Lemme. *Soient r, n deux entiers positifs, avec $n > r$ et soient α_{ij} des entiers modulo 2, avec $1 \leq i \leq r$ et $1 \leq j \leq n$. Il existe des entiers $\lambda_1, \ldots, \lambda_n$ égaux à 0 ou 1 et non tous nuls, tels que l'on ait, pour tout i, $\lambda_1 \alpha_{i,1} + \cdots + \lambda_n \alpha_{i,n} = 0$.*

Démonstration. C'est clair : on a un système de r équations homogènes à n inconnues dans $\mathbf{F}_2$, avec $n > r$, il y a donc une solution non triviale.

7.4 *Remarques.* 1) C'est plutôt mieux de prendre, au lieu de $R_i^2 - N$ la classe de R_i^2 modulo N. En fait, si l'on cherche les R_i en partant de $R_0 = [\sqrt{N}]$ et en prenant les $R_0 + k$, $k = 1, 2, ...$, c'est pareil pour k petit car $(R_0 + k)^2$ est juste un peu plus grand que N, donc sa classe est obtenue en retranchant N. Mais ça change pour k plus grand.

2) On peut aussi chercher des R_i tels que $-R_i^2$, pris modulo N, soit friable. L'intérêt est d'avoir ainsi plus de valeurs friables. En contrepartie, on doit prendre seulement un nombre pair de termes admettant le coefficient -1.

7.5 *Exemple.* Avec $N = 100895598169$, on prend $B = 30$, de sorte que l'on a $r = 10$. On a $R_0 := [\sqrt{N}] = 317640$ et les trois valeurs friables[40] $R_1 = 317641 = R_0 + 1$ avec $R_1^2 - N := (R_0 + 1)^2 - N = 2^3 \times 3^4 \times 11 \times 29$, $R_2 = 320106 = R_0 + 2466$, avec $R_2^2 - N := (R_0 + 2466)^2 - N = 7 \times 11^4 \times 23^2 \times 29$ et $R_3 = 320513 = R_0 + 2873$ avec $R_3^2 - N := (R_0 + 2873)^2 - N = 2^3 \times 3^2 \times 5^4 \times 7 \times 11 \times 23^2$. On voit que l'on a, en posant $R = R_1 R_2 R_3$:

$$R^2 = 2^6 \times 3^6 \times 5^4 \times 7^2 \times 11^6 \times 23^4 \times 29^2 = S^2$$

et $pgcd(N, R - S) = 898423$.

Mais, attention, d'autres solutions donnent des R tels que N divise $R \pm S$, par exemple, si $R := 317641 \times 317873 \times 318532$ on a $R^2 \equiv S^2 \pmod{N}$ avec $S = 2^3 \times 3^5 \times 5 \times 7 \times 11^2 \times 19 \times 29^2$, mais N divise $R - S$.

8 Annexe 4 : les couples périlleux

L'objectif de ce paragraphe est de préciser l'énoncé 3.1. On commence par établir un résultat sur les relations de Bézout.

8.1 Taille d'une relation de Bézout

8.1 Définition. *0) On appelle relation de Bézout entre deux entiers p, q une relation $ap + bq = c$ avec $a, b, c \in \mathbf{Z}$, a, b non nuls.*

1) La taille de la relation de Bézout $ap + bq = c$ est le nombre $T = \mathrm{Max}\,(|a|, |b|, |c|)$.

2) Soient $p, q \in \mathbf{N}^*$. La B-taille du couple (p, q) est le minimum des tailles des relations de Bézout $ap + bq = c$.

40. Comme N n'est un carré ni modulo 13, ni modulo 17, ces valeurs n'apparaissent jamais dans la liste.

Le résultat suivant est fondamental :

8.2 Proposition. *Soient k, l des entiers positifs, premiers entre eux, et soit m un entier relatif non nul. Posons $T = \mathrm{Max}\,(k, l, |m|)$. Il existe une relation de Bézout $ka + lb = m$ avec $a, b \in \mathbf{Z}$ et $|a|, |b| \leq T/2$, sauf dans le cas $k = l = 1$ où l'on a seulement $|a|, |b| \leq (T+1)/2$.*

Si l'on n'impose plus l'entier m, on en déduit le corollaire suivant (qui sera amélioré en 8.18) :

8.3 Corollaire. *Soient p, q des entiers positifs premiers entre eux, non tous deux égaux à 1. La B-taille du couple (p, q) est $\leq \mathrm{Max}\,(p, q)/2$.*

Démonstration. (de 8.2) On peut supposer $m > 0$ et $k \leq l$. Comme k et l sont premiers entre eux, ils sont distincts, sauf dans le cas $k = l = 1$. Dans ce cas, si $m = 2r$ on prend $a = b = r$ et si $m = 2r + 1$, $a = r$ et $b = r + 1$. Sinon, on a donc $k < l$.

Supposons d'abord $k \leq l - 2$. Comme k et l sont premiers entre eux, il existe a_0, b_0 tels que $ka_0 + lb_0 = m$. Soit a le résidu de a_0 modulo l qui est $\leq l/2$ en valeur absolue. On a donc $a_0 = a + nl$ et, en posant $b = b_0 + nk$, on a bien $ka + lb = m$. Il reste à voir qu'on a $|b| \leq T/2$. Si a et b sont ≥ 0, on a $lb \leq m$ donc $b \leq m/l \leq m/3 \leq T/2$. Si b est < 0 et $a \geq 0$ on a $l|b| \leq ka$ donc $|b| \leq \frac{k}{l}a \leq a \leq T/2$. Enfin, si l'on a $b \geq 0$ et $a < 0$ on a $lb = k|a| + m$ donc $b = \dfrac{k|a|}{l} + \dfrac{m}{l} \leq \dfrac{k}{2} + \dfrac{m}{l}$.

Il y a deux cas (le cas $m = l$ est trivial) :

• $m > l$. On a $b \leq \dfrac{k}{2} + \dfrac{m}{l} \leq \dfrac{l-2}{2} + \dfrac{m}{l} \leq \dfrac{m(l-2)}{2l} + \dfrac{m}{l} = \dfrac{m}{2}$.

• $m < l$. On a $b \leq \dfrac{k}{2} + \dfrac{m}{l} < \dfrac{k}{2} + 1 = \dfrac{k+2}{2} \leq \dfrac{l}{2}$.

Il reste donc seulement à traiter le cas $k = l - 1$. Pour $k = 1$ et $l = 2$, si $m = 2r$ on pose $a = 0$ et $b = r$, si $m = 2r + 1$, $a = 1$ et $b = r$.

On peut donc supposer $l \geq 3$. On cherche a, b tels que $a(l-1) + bl = m$ ou encore $(a + b)l = m + a$. Le cas $m = l$ est évident.

• On suppose $m < l$. Deux cas encore :

– si $m \leq l/2$ on prend $a = -m$, d'où $m + a = 0$, puis $b = m$ et c'est bon.

– si $m > l/2$ on prend $a = l - m < l/2$, d'où $a + m = l$, $a + b = 1$, $b = 1 - a$ et, comme a est positif, $|b| < a \leq l/2$.

• On suppose $m > l$. On écrit $m = lq - a$ avec $|a| \leq l/2$ ($-a$ est la classe de m modulo l comprise entre $-l/2$ et $l/2$). On pose alors $b = q - a = \dfrac{m+a}{l} - a$. On a $b = \dfrac{m}{l} + a\dfrac{1-l}{l}$. Si a est ≥ 0, on a $-a \leq b \leq \frac{m}{l}$ et le résultat. Si a est

< 0, on a $m = ql + |a|$ et $b = q + |a|$. Si $q \geq 2$ on a $l \leq m/2$ donc $|a| \leq m/4$ et l'inégalité $b = q + |a| = \dfrac{m - |a|}{l} \leq m/2$ équivaut à $|a| \leq \dfrac{m}{2}\dfrac{l-2}{l-1}$. Comme la deuxième fraction est $\leq 1/2$, on a le résultat. Si $q = 1$, le résultat est clair si $|a| \geq 2$. Si $|a| = 1$ on a $b = 2$ et $m = l + 1$. Comme on a supposé $l \geq 3$ on a le résultat [41].

8.4 *Remarque.* Le résultat de 8.2 est optimal. En effet, si $k = 2n+1, l = 2n+3$ sont deux entiers impairs consécutifs et si $m = 1$, on vérifie facilement que la plus petite relation de Bézout possible est avec $a = n + 1$ et $b = -n$.

8.2 Les couples périlleux

Les résultats suivants précisent 3.1. On parlera "d'écriture affine" pour une décomposition de la forme $p = kz + a$, $q = lz + b$.

8.2.1 Bézout et écriture affine

8.5 Proposition. *Soient p, q, T des entiers positifs.*

1) On suppose qu'il existe des entiers positifs k, l, z et des entiers relatifs a, b avec $k, l, |a|, |b| \leq T$ tels que l'on ait $p = kz + a$ et $q = lz + b$. Alors, p, q vérifient la relation de Bézout $kq - lp = m$ avec $k, l \leq T$ et $m = kb - la$ et on a $|m| \leq 2T^2$.

2) On suppose que p, q vérifient une relation de Bézout $kq - lp = m$ avec $0 \leq k, l, |m| \leq T$. Alors, il existe des entiers z, a, b avec $z > 0$ et $|a|, |b| \leq (T + 1)/2$ tels que $p = kz + a$ et $q = lz + b$. On a $m = kb - la$.

Démonstration. Le point 1) est immédiat. Pour 2), on peut supposer que k et l sont premiers entre eux. En effet, sinon, on a $k = dk'$, $l = dl'$ avec k' et l' premiers entre eux et, si $m = kq - lp$, d divise m, de sorte qu'on a $m = dm'$, et en divisant par d on est ramené au cas des coefficients premiers entre eux. La proposition 8.2 fournit alors a, b avec $|a|, |b| \leq (T + 1)/2$ tels que $kb - la = m$. Par différence, on a $k(q - b) = l(p - a)$ et, comme k et l sont premiers entre eux, on en déduit $p = a + kz$ et $q = b + lz$.

8.2.2 Bézout et fractions

La proposition suivante est immédiate :

41. Le lecteur qui trouverait cette démonstration saumâtre est prié d'en proposer une meilleure.

8.6 Proposition. *Soient p, q, T des entiers positifs.*

1) On suppose que p, q vérifient une relation de Bézout $kq - lp = m$ avec $0 < k, l, |m| \leq T$. Alors on a $|\frac{p}{q} - \frac{k}{l}| \leq \frac{T}{q}$.

2) On suppose qu'il existe des entiers positifs k, l avec $k, l \leq T$ tels que $|\frac{p}{q} - \frac{k}{l}| \leq \frac{T}{q}$. Alors on a une relation de Bézout $kq - lp = m$ avec $|m| \leq T^2$.

8.2.3 Crible et écriture affine

8.7 Proposition. *Soit $N = pq$ un entier produit de deux nombres premiers impairs distincts.*

1) On suppose que les nombres p, q admettent une écriture $p = kz + a$, $q = lz + b$ avec $k, l > 0$, $a, b \in \mathbf{Z}$ et $k, l, |a|, |b| \leq T$. Alors, il existe L, R, S tels que $LN = R^2 - S^2$ avec $L \leq 4T^2$ et $S \leq 2T^2$.

2) Soit T un nombre tel que $0 < T < N/3$. On suppose qu'il existe $L, R, S > 0$ tels que $LN = R^2 - S^2$ avec $L, S \leq T$. Alors, il existe k, l, a, b avec $k, l > 0$, $a, b \in \mathbf{Z}$ tels que $p = kz + a$ et $q = lz + b$ avec $k, l, |a|, |b| \leq T$.

Démonstration. 1) Supposons qu'on a $p = kz + a$ et $q = lz + b$, avec les conditions ci-dessus. Si kq et lp sont de même parité (c'est-à-dire si k, l le sont), on pose $R = \frac{kq + lp}{2}$ et $S = \frac{|kq - lp|}{2} = \frac{|kb - la|}{2}$ et on a $LN = R^2 - S^2$ avec $L = kl$. De plus on a $L \leq T^2$ et $S \leq T^2$, donc, *a fortiori*, les inégalités annoncées.

Si kq et lp ne sont pas de même parité, on pose $R = lp + kq$ et $S = |kq - lp| = |kb - la|$ et on a $R^2 - S^2 = 4klpq = LN$ avec $L = 4kl$. On en déduit les inégalités annoncées [42] sur L et S.

2) Supposons maintenant qu'on a $LN = R^2 - S^2$, ce qui impose que L est impair ou multiple de 4. Si p, q divisent tous deux $R + S$, on a $R + S = uN$, donc $L = u(R - S)$. On a donc $0 \leq R - S \leq L \leq T$, donc $R \leq 2T$. Mais on a alors $N \leq R + S \leq 3T$ et c'est absurde. On élimine, de même, le cas où p et q divisent $R - S$.

Supposons d'abord que L est impair. Comme p et q ne divisent pas tous deux $R - S$ ni $R + S$, on peut supposer, par exemple, qu'on a $R - S = lp$ et $R + S = kq$, donc $L = kl$ et $2S = kq - lp$. On en déduit $k, l \leq T$ et k, l impairs. Comme on a une relation de Bézout $kq - lp = 2S$, de taille $2T$, on peut alors écrire, en vertu de 8.5, $p = kz + a$, $q = lz + b$ avec $k, l, |a|, |b| \leq T$ comme annoncé.

42. Attention, pour S, a et b ne sont pas nécessairement de même signe, d'où la majoration par $2T^2$ seulement.

Si L est multiple de 4, $L = 4K$, on a $4KN = 4Kpq = (R-S)(R+S)$. Si R et S sont pairs, on peut les diviser par 2 et diviser L par 4 et on a une relation de même type, mais plus petite. On peut donc supposer que R et S sont tous deux impairs. De plus, comme ci-dessus, on peut supposer, par exemple, que p divise $R-S$ et que q divise $R+S$. Comme R et S sont impairs, on a $R-S = 2lp$ et $R+S = 2kq$, donc $L = 4kl$ avec $k, l \leq T/4$ et $S = kq - lp$. En vertu de 8.5, on peut alors écrire $p = kz + a$, $q = lz + b$ avec $k, l, |a|, |b| \leq T$ comme annoncé.

8.3 Division euclidienne itérée

8.3.1 Motivation

Si les entiers p, q ont une écriture affine $p = kz + a$, $q = lz + b$ avec $k, l, |a|, |b|$ petits, on a $N = pq = klz^2 + (kb + la)z + ab$, donc une écriture de la forme $N = Kz^2 + Az + B$ avec K, A, B petits. La définition suivante formalise cette notion.

8.3.2 Définition

8.8 Proposition-Définition. *Soient N, z des entiers positifs. Il existe des éléments $K, A, B \in \mathbf{N}$, uniques, vérifiant $N = Kz^2+Az+B$ et $0 \leq A, B < z$. On désigne cette opération sous le nom de* **division euclidienne itérée primitive** *de N par z.*

Démonstration. On effectue la division euclidienne de N par z : $N = zQ+B$ avec $0 \leq B < z$. On effectue ensuite la division de Q par z : $Q = Kz + A$ avec $0 \leq A < z$. On a donc $N = z(Kz + A) + B = Kz^2 + Az + B$ avec $0 \leq A, B < z$ comme annoncé. Pour l'unicité, on voit que B est le reste de la division euclidienne de N par z, puis que A est celui de la division de $Q := (N - B)/z$ par z et que K en est le quotient.

8.9 *Remarques.* 1) Comme on a $A, B < z$, donc $A, B \leq z-1$, on a $Az+B \leq z^2 - 1 < z^2$. On a donc $Kz^2 \leq N < (K+1)z^2$ soit $\sqrt{\dfrac{N}{K+1}} < z \leq \sqrt{\dfrac{N}{K}}$.

2) Attention, en général z n'est pas la partie entière de $\sqrt{N/K}$. Par exemple, avec $N = 92$ et $z = 7$ on a $K = 1$, $A = 6$, $B = 1$ et $[\sqrt{N/K}] = 9$.

3) On vérifie qu'il en est ainsi si l'on a $(2K + 1)^2 K \leq N$. Par exemple, avec le nombre de Frenicle $N = 100895598169$, la condition est $K \leq 2932$.

8.3.3 La variante avec des signes

Pour gagner un peu sur la taille, il est intéressant de tolérer des restes négatifs :

8.10 Proposition-Définition. *Soient N, z des entiers positifs. Il existe des éléments $K \in \mathbf{N}^*$, $A, B \in \mathbf{Z}$ vérifiant $N = Kz^2 + Az + B$ et $|A|, |B| \leq z/2$. De plus, ces éléments sont uniques si l'on impose la condition suivante : si $|A|$ (resp. $|B|$) est égal à $z/2$, alors A (resp. B) est positif. On désigne cette opération sous le nom de* **division euclidienne itérée** *de N par z.*

Démonstration. On considère la division euclidienne itérée primitive qui donne K_0, A_0, B_0 et on distingue plusieurs cas.

• Si on a $B_0 \leq z/2$ et $A_0 \leq z/2$, on pose $B = B_0$, $A = A_0$, $K = K_0$.

• Si on a $B_0 \leq z/2$ mais $A_0 > z/2$, on pose $B = B_0$, $A = A_0 - z$ et $K = K_0 + 1$.

• Si on a $B_0 > z/2$ et $A_0 \leq z/2 - 1$ on pose $B = B_0 - z$, $A = A_0 + 1$ et $K = K_0$.

• Enfin, si on a $B_0 > z/2$ et $A_0 > z/2 - 1$, on pose $B = B_0 - z$, $A = A_0 + 1 - z$ et $K = K_0 + 1$.

8.11 *Remarque.* Avec les notations de 8.10, on a $N \geq Kz^2$ si $A > 0$ ou si $A = 0$ et $B \geq 0$ et on a $N < Kz^2$ si $A < 0$ ou si $A = 0$ et $B < 0$.

8.3.4 Écriture affine et division euclidienne itérée

La proposition suivante fait le lien entre ces deux notions et permet de donner une définition précise des couples périlleux :

8.12 Proposition-Définition. *Soient p, q deux entiers possédant une écriture affine $p = kz + a$, $q = lz + b$ avec $k, l, z > 0$ et $a, b \in \mathbf{Z}$, de taille $T = \mathrm{Max}\,(k, l, |a|, |b|)$. On suppose qu'on a $4\,T^3 + T \leq \mathrm{Min}\,(p, q)$. Alors la division euclidienne itérée de $N = pq$ par z est donnée par $K = kl$, $A = kb + la$ et $B = ab$.*

Si, de plus, on a $|a| \leq k$ et $|b| \leq l$ avec l'une des inégalités stricte, on a $z = \left[\sqrt{N/K}\right]$ (si $A > 0$ ou si $A = 0$ et $B \geq 0$) ou $z = \left[\sqrt{N/K}\right] + 1$ (si $A < 0$ ou si $A = 0$ et $B < 0$), cf. 8.9.

On dit alors que le couple (p, q) est **périlleux** *(sous-entendu comme clé RSA).*

Démonstration. Supposons par exemple $p \leq q$. On a $p = kz + a$ et $q = lz + b$ d'où $N = pq = klz^2 + (kb + la)z + ab$ et il suffit de montrer qu'on a $|kb + la| \leq z/2$ et $|ab| \leq z/2$. Mais on a $k, l, |a|, |b| \leq T$, donc $|kb + la| \leq 2T^2$

et $|ab| \leq T^2$. Il suffit donc d'avoir $z \geq 4T^2$. Par ailleurs, on a $z = \dfrac{p-a}{k}$. Pour minorer z on majore k par T et on minore $p-a$ par $p-T$. On a donc $z \geq \frac{p}{T} - 1$. Comme on a supposé $p \geq 4T^3 + T$, on en déduit le résultat.

Montrons l'assertion complémentaire. Dans le premier cas, il s'agit de montrer qu'on a $Az + B < 2Kz + K$ ou encore $(al + bk)z + ab < 2klz + kl$. Avec la condition imposée, c'est clair. Dans le second cas on a à montrer $(2K + A)z \geq K - B$. Comme $|A| = |al + kb| < kl$ (car l'une des inégalités sur a ou b est stricte), on a $2K + A > 0$ et le résultat vient de $z \geq 4T^2$ et $K - B \leq 2T^2$.

8.13 *Remarque.* On constate expérimentalement qu'il y a peu de couples de petite taille. Ainsi, si l'on choisit aléatoirement des couples de nombres premiers $< 10^6$, la proportion de ceux qui sont périlleux est de l'ordre de 2.5%.

8.4 Un algorithme

Soit N un entier (grand), produit de deux nombres premiers p et q (avec par exemple $p < q$) comme dans le cas du code RSA. On cherche à factoriser N. On suppose que le couple p, q a été imprudemment choisi (c'est-à-dire que c'est un couple périlleux). On peut alors (voir 3.4.2) tenter d'appliquer l'algorithme brutal pour factoriser N, mais l'expérience montre qu'il n'est pas très efficace pour les grands nombres. On donne ici une alternative meilleure qui utilise la division euclidienne itérée.

L'objectif est de trouver l'écriture affine $p = kz + a$, $q = lz + b$ avec k, l, a, b petits et z grand. On a alors $N = pq = klz^2 + (kb + la)z + ab$ et on pose $K = kl$, $A = kb + la$ et $B = ab$. Si p, q est un couple périlleux, cette écriture est la division euclidienne itérée de N par z et si, de plus, a, b sont petits par rapport à k, l on a $z = \left[\sqrt{N/kl}\right]$.

8.4.1 Premier pas : évaluer la taille adéquate

Si T est la taille de p, q, l'algorithme ne va fonctionner que si l'on a $4T^3 + T \leq p \leq \sqrt{N}$. On va donc se limiter à chercher des solutions de taille $\leq T \sim \dfrac{\sqrt[6]{N}}{\sqrt[3]{4}} \sim 0,63\sqrt[6]{N}$.

Par exemple, pour le N de Frenicle, $N = 100895598169$, on prendra $T \leq 43$.

8.4.2 Second pas : trouver K, A, B

On fait varier K de 1 jusqu'à T^2 au plus[43]. On calcule $z = \left[\sqrt{\frac{N}{K}}\right]$. On effectue la division euclidienne itérée de N par z : $N = Kz^2 + Az + B$ et on conserve les valeurs K, A, B si l'on a $A, B \leq 2T^2$.

Dans le cas du nombre de Frenicle, on a $2T^2 = 1849$, $K = 8$ donne $A = 15$ et $B = 7$ (les autres $K \leq 20$ donnent des valeurs de B beaucoup plus grandes).

8.4.3 Troisième pas : trouver k, l, a, b

Maintenant qu'on a K, A, B, on cherche k, l, a, b tels que $K = kl$, $A = kb + la$ et $B = ab$.

On calcule $\Delta = A^2 - 4KB$. Si cette quantité n'est pas un carré parfait, on passe à la valeur suivante de K. Si elle l'est, $\Delta = m^2$, on cherche tous les couples k, l tels que $K = kl$ et on conserve ceux qui vérifient les deux propriétés suivantes :

- $2l$ divise $A - m$,
- $(A - m)/2l$ divise B.

S'il n'y a pas de telle solution on passe à la valeur suivante de K.

On peut alors résoudre en a, b, le système $kb + la = A$, $B = ab$. En tirant $b = B/a$ on se ramène à l'équation du second degré $la^2 - Aa + kB = 0$ dont le discriminant est $\Delta = A^2 - 4KB = m^2$. On a alors $a = \dfrac{A - m}{2l}$ et $b = B/a$ et les facteurs de N sont $p = kz + a$ et $q = lz + b$.

8.4.4 Discussion

8.14 *Remarques.* 1) On note ici que le fait que Δ soit un carré ne dépend que de K et pas de sa décomposition.

2) On ne trouve des solutions que si $\Delta = A^2 - 4KB$ est un carré. Mais l'écriture $Kz^2 + Az + B - N = 0$ montre que $\Delta' = A^2 - 4K(B - N)$ est, en tous cas, un carré. La condition implique donc que $4KN = \Delta' - \Delta$ est différence de deux carrés : on retrouve la condition de la méthode du crible ! L'avantage de cette méthode par rapport à la méthode brutale est double : d'abord, on a un moyen de sélectionner les K convenables grâce à la division euclidienne itérée, et ensuite, cette division donne les candidats qui vont permettre d'écrire $4KN$ comme différence de deux carrés. Du point de vue programmation, on peut d'ailleurs, une fois trouvés K, A, B, chercher directement le *pgcd* de N avec

43. On n'oubliera pas que moralement on a $K = kl$

$R-S$ et $R+S$ où l'on a posé $S^2=\Delta$ et $R^2=\Delta'$, voir le programme ci-dessous.

3) Attention, toutefois, l'existence d'une division euclidienne itérée avec de petits K, A, B n'est pas garante de l'existence d'une écriture affine de p et q. Prenons $p=8831$ et $q=9811$, $N=pq$. On a une division avec de petits K, A, B : $N=41\times 1453^2+56\times 1453+4$ qui ne donne pas de k, l, a, b (le discriminant Δ n'est pas un carré). En revanche, avec $N=90\times 981^2+29\times 981+2$, on trouve $k=9$, $l=10$, $a=2$ et $b=1$ et l'écriture $8831=9\times 981+2$ et $9811=10\times 981+1$.

8.4.5 Un programme

Ce programme appelle un programme `diveucliter` qui calcule les coefficients A, B de la division euclidienne itérée et que le lecteur écrira sans peine.

```
factorDP(N):={
local T,K,z,A,B,S,R,u;
T:=0.63*N^(1/6);
K:=1;
u:=0;
tantque K<T^2 et u==0 faire
z:=floor(sqrt(N/K));
A:=diveucliter(N,z)[1];
B:=diveucliter(N,z)[2];
si A <2*T^2 et B<T^2 et A^2-4*K*B >0 alors
S:=sqrt(A^2-4*K*B);
si floor(S)==S alors
R:=sqrt(A^2-4*K*B+4*K*N);
si gcd(N,R+S)!=1 et gcd(N,R-S)!=1 alors
Disp gcd(N,R+S), gcd(N,R-S);
u:=1;
fsi
fsi
fsi
K:=K+1;
ftantque
}:;
```

8.4.6 Un exemple

Si N est le nombre de 70 chiffres :

$$2467324798096533567875313467897546 17\times 2193177598308029838111389749242263 27$$

le programme standard de factorisation de *xcas* met 94 secondes pour le factoriser, tandis que le programme [44] ci-dessus met 2 secondes et 63 centièmes !

8.5 Compléments sur Bézout et l'algorithme d'Euclide

Dans ce paragraphe on montre que la B-taille d'un couple p, q avec $p < q$ est $\leq \sqrt{q}$ et qu'elle est donnée par l'algorithme d'Euclide. Ces résultats sont les mêmes que ceux qu'on obtient en utilisant les fractions continues, voir [6], mais on verra qu'on n'a pas besoin de cet outil : l'algorithme d'Euclide est une merveille !

8.5.1 L'algorithme

Soient $p, q \in \mathbf{N}^*$. On suppose $p < q$. L'algorithme d'Euclide associé à p, q est le suivant. On pose $r_0 = q$ et $r_1 = p$. On effectue la division euclidienne de q par p : $q = bp + r$ avec $0 \leq r < p$ et $b \geq 0$. On pose $r_2 = r$ et $a_1 = b$. On a donc $r_0 = a_1 r_1 + r_2$. Si r_2 est nul on s'arrête, sinon on effectue la division de r_1 par r_2 : $r_1 = a_2 r_2 + r_3$ avec $0 \leq r_3 < r_2 < q$. On continue jusqu'à ce qu'on ait $r_{N+1} = 0$. On a donc, pour un indice $k \geq 1$ quelconque $r_{k-1} = a_k r_k + r_{k+1}$ avec $0 \leq r_{k+1} < r_k$ et $r_{N-1} = a_N r_N$. On note que les coefficients a_k sont ≥ 0 et plus précisément > 0 pour $n \leq N$.

On sait que le dernier reste non nul r_N est alors le pgcd de p et q.

8.15 *Remarque.* Pour $n \geq 2$, on a $r_n < q/2$. En effet, on a $q = a_1 p + r_2$ avec $r_2 < p$, donc $a_1 > 0$, donc $q > r_2 + r_2 = 2r_2$.

8.5.2 Les relations de Bézout

L'algorithme fournit des relations de Bézout $p_n q - q_n p = (-1)^n r_n$ pour tout $n \geq 0$. Pour les obtenir, on pose $p_0 = 1$, $q_0 = 0$, $p_1 = 0$, $q_1 = 1$, puis on définit par récurrence $p_{n+1} = p_{n-1} + a_n p_n$ et $q_{n+1} = q_{n-1} + a_n q_n$.

Commençons par établir quelques identités :

44. Mais les nombres p et q choisis ici sont de B-taille vraiment petite (10). Sinon, c'est moins efficace ... D'ailleurs le programme naïf donne lui aussi le résultat plus rapidement que le programme de *xcas* (57.74 s)

8.16 Proposition. *1) On a* $p_n q - q_n p = (-1)^n r_n$.
2) On a $p_{n+1}q_n - p_n q_{n+1} = (-1)^{n+1}$.
3) On a $q_n r_{n+1} + q_{n+1} r_n = q$ *et* $p_n r_{n+1} + p_{n+1} r_n = p$.

Démonstration. Le point 1) vient de la définition des p_n, q_n. Les autres se montrent par récurrence. Par exemple, on écrit $q_n r_{n+1} + q_{n+1} r_n = q_n(r_{n-1} - a_n r_n) + (q_{n-1} + a_n q_n) r_n = q_n r_{n-1} + q_{n-1} r_n = q$.

8.17 Proposition. *Dans cette proposition, n est un entier qui vérifie $0 \leq n \leq N$.*
1) Les entiers p_n, q_n sont ≥ 0 pour $n \leq N$. Précisément, on a $q_n > 0$ pour $n \geq 1$ et $p_n > 0$ pour $n \geq 2$.
2) On a $q_n \leq q_{n+1}$ pour tout $n \geq 0$ et $q_n < q_{n+1}$ pour $n \geq 2$.
3) On a $p_n \leq p_{n+1}$ pour tout $n \geq 1$ et $p_n < p_{n+1}$ pour $n \geq 3$.
4) On a $p_n \leq q_n$ pour tout $n \geq 1$.
5) On a l'inégalité $q_{n+1} r_n \leq q$ pour tout $n \geq 0$.

Démonstration. Le point 1) est clair par récurrence car les a_k sont ≥ 0.
2) On a $q_0 = 0 < q_1 = 1$ et $q_{n+1} = q_{n-1} + a_n q_n \geq q_{n-1} + q_n$ car $a_n > 0$. On en déduit le résultat.
3) Cela résulte de la formule $p_{n+1} = p_{n-1} + a_n p_n$.
4) C'est évident par récurrence à partir de $p_1 = 0 < q_1 = 1$ et de $p_2 = 1 \leq q_2 = a_1$.
5) Cela résulte de $q_n r_{n+1} + q_{n+1} r_n = q$.

8.18 Théorème. *Soient p, q des entiers positifs avec $p < q$. La B-taille de (p, q) est $\leq \sqrt{q}$.*

Démonstration. On considère les termes p_n, q_n donnés par l'algorithme d'Euclide et on prend pour n le plus grand entier tel que $q_n \leq \sqrt{q}$. On a donc $\sqrt{q} < q_{n+1}$. On a la relation $p_n q - q_n p = (-1)^n r_n$. Je dis qu'elle est de taille $\leq \sqrt{q}$. C'est clair pour q_n, et pour p_n c'est 8.17.4. Pour r_n cela vient de l'inégalité $q_{n+1} r_n \leq q$ qui donne $r_n \leq \dfrac{q}{q_{n+1}} < \dfrac{q}{\sqrt{q}} = \sqrt{q}$.

8.19 *Remarque.* Le résultat est optimal. On montre en effet, par exemple, que la taille du couple $(11, 97)$ est égale à 9 et on a $\sqrt{97} \sim 9.84$.

On montre maintenant que la meilleure relation de Bézout entre p et q est nécessairement donnée par Euclide :

8.20 Théorème. *Soient p, q des entiers positifs. La B-taille de p, q est le minimum des tailles des relations de Bézout qui apparaissent dans l'algorithme d'Euclide.*

Démonstration. On peut supposer $p < q$ et on suppose aussi $q \geq 4$ (le lecteur vérifiera les cas $q = 2, 3$). On a alors $q/2 \geq \sqrt{q}$. Soit $bp - aq = c$ une relation de taille minimum. On a donc $|b|, |a|, |c| \leq \sqrt{q}$. On peut supposer $a, b > 0$ et a, b premiers entre eux (sinon on peut diviser la relation par un facteur commun). Montrons déjà qu'on a $a \leq b$. Sinon, on a $a > b$, donc $|c| = |bp - aq| = aq - bp > aq - bq \geq q$ et c'est absurde.

Comme la suite q_n est croissante on peut y intercaler b : $q_{n-1} < b \leq q_n$.

1) Si $b = q_n$ et $a \neq p_n$ (sinon, la relation est l'une de celles données par Euclide) on a $q_n p - p_n q = (-1)^{n+1} r_n$ et $bp - aq = c$. Par différence on a $(a - p_n)q = (-1)^{n+1} r_n - c$ et on en déduit $|c - (-1)^{n+1} r_n| \geq q$. Mais on a $r_n < q/2$ en vertu de 8.15, donc $c > q/2$ et c'est absurde car on aurait $q/2 < \sqrt{q}$.

2) Supposons maintenant que b n'est pas égal à l'un des q_n. On a donc $q_{n-1} < b < q_n$. On peut écrire : $a = \lambda p_n + \mu p_{n-1}$ et $b = \lambda q_n + \mu q_{n-1}$ avec λ, μ entiers car le déterminant de ce système est $p_n q_{n-1} - q_n p_{n-1} = (-1)^n$. Précisément, on a $\lambda = (-1)^n (q_{n-1} a - p_{n-1} b)$ et $\mu = (-1)^{n+1} (q_n a - p_n b)$. On a alors $c = (-1)^{n+1} \lambda r_n + (-1)^n \mu r_{n-1}$. On a $\lambda \neq 0$. Sinon, on a $q_{n-1} a = p_{n-1} b$ et, comme a, b sont premiers entre eux, b divise q_{n-1} ce qui contredit l'inégalité $q_{n-1} < b$.

Comme on a $0 < b = \lambda q_n + \mu q_{n-1} < q_n$ et $\lambda \neq 0$, on voit que λ et μ sont de signes opposés. Mais alors, les deux termes de $c = (-1)^{n+1} \lambda r_n + (-1)^n \mu r_{n-1}$ sont de même signe et on a donc $|c| > r_{n-1}$. Comme on a $0 \leq p_{n-1} \leq q_{n-1} < b$ et $r_{n-1} < |c|$, on en déduit que la taille de la relation $q_{n-1} p - p_{n-1} q = (-1)^n r_{n-1}$ est plus petite que celle de $bp - aq = c$.

Références

[1] Boneh Dan, *Twenty Years of Attacks on the RSA Cryptosystem*, Notices of the AMS, february 1999.

[2] Cohen Henri, *A Course in computational Algebraic Number Theory*, Springer, 1993.

[3] Dickson Leonard E., *History of the Theory of Numbers*, Carnegie Institution Washington, 1919.

[4] Fermat Pierre de, *Oeuvres*, Éditées par P. Tannery et Ch. Henry, Gauthier-Villars, Paris, 1894.

[5] Goldstein Catherine, *L'expérience des nombres de Bernard Frenicle de Bessy*, *Revue de synthèse*, 4° sér., n° 2-3-4, avr.-déc. 2001, p. 425-454.

[6] Hardy Godfrey H., Wright Edward M., *An introduction to the theory of numbers*, Oxford Clarendon Press, sixth edition, 2008.

[7] Kraitchik Maurice, *Théorie des nombres*, Gautier-Villars, Paris, 1922.

[8] Perrin Daniel, *Mathématiques d'école*, Cassini, 2005, 2011.

[9] Perrin Daniel, *Mathématiques et autres disciplines*
https ://www.math.u-psud.fr/ perrin/interdisciplines/Cours6cryptographie.pdf

[10] Pomerance Carl, *Analysis and comparison of some factoring algorithms*
in Computational methods in Number Theory (Lenstra and Tijdeman eds). Centre tracts 154/155 math. Centrum Amsterdam, pp. 89-139.