ARITHMÉTIQUE AU COLLÉGE ET AU LYCÉE : AUTOUR DE LA CRYPTOGRAPHIE ET DES NOMBRES PREMIERS

Daniel PERRIN
Professeur Honoraire
Université Paris-Sud, Orsay
daniel.perrin@universite-paris-saclay.fr

Ce texte est la rédaction d'une conférence faite le 15 juin 2023 lors du colloque : *Raisonner en arithmétique. Est-ce incongru ?* organisé par les commissions Inter-IREM collège et lycée. Je remercie les organisateurs de m'avoir invité à faire cette conférence et particulièrement Laurianne et Patricia pour leur gentillesse, leur dévouement et leur efficacité.

I - CRYPTOGRAPHIE ET NOMBRES PREMIERS

Cette partie est reprise d'une conférence que j'ai faite plus de quatre-vingt fois devant des publics divers : collégiens, lycéens, grand public, notamment lors de la fête de la science, etc. On en trouve des rédactions variées sur ma page web et quelques vidéos sur You Tube.

1. Les nombres premiers : inutiles?

La question de l'utilité des mathématiques est l'une de celles que les collégiens et les lycéens posent le plus souvent et il n'est pas toujours facile d'y répondre, notamment dans le cas de l'arithmétique, dont on a longtemps pensé qu'elle ne servait à rien, témoin ce qu'en dit Descartes dans une lettre à Mersenne datant de 1638 :

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.

C'est même l'opinion d'un grand spécialiste du sujet, le mathématicien anglais[1] G.H. Hardy, pourtant spécialiste de théorie des nombres (dans une conférence faite en 1915) :

La théorie des nombres a toujours été perçue comme l'une des branches les moins utiles des Mathématiques Pures. On ne pourra guère contester cette accusation, encore moins lorsqu'elle vise les parties de la théorie plus particulièrement liées aux nombres premiers. Une science est qualifiée d'utile si son développement contribue à accentuer les inégalités dans la répartition des richesses ou, lorsqu'il promeut plus directement la destruction de la vie humaine. La théorie des nombres premiers ne vérifie pas de tels critères. Ceux qui l'explorent ne tenteront pas, si toutefois ils sont doués de sagesse, de justifier l'intérêt qu'ils portent à un sujet si futile et isolé.

D'ailleurs, moi-même, à la question : *à quoi servent les nombres premiers ?* j'aurais sans doute répondu en 1970 : à rien, on les étudie *pour l'honneur de l'esprit humain* (comme disait Jacobi vers 1850) et j'aurais peut-

[1] On appréciera l'humour britannique.

être ajouté, comme aurait pu dire notre collègue Roger Godement (mort en juillet 2016) : *au moins, quand on fait de l'arithmétique*[2]*, on ne travaille pas pour la bombe atomique !* Eh bien, nous aurions dit une bêtise, comme l'invention du code RSA le montrera peu après ...

2. La cryptographie

La cryptographie (du grec crypto, caché et graphie, écrire), est la science des codes secrets. Le premier dont l'histoire atteste qu'il utilisait de tels codes est Jules César, qui employait un système d'alphabets décalés. Ainsi, on pourrait imaginer qu'il envoya au Sénat, au soir de la bataille de Zela, le communiqué sibyllin suivant : *TCLG TGBG TGAG* ...

Ce type de codage, ou chaque caractère du message originel correspond à un et un seul caractère du message codé, est appelé codage par substitution. En voici un exemple très simple. Supposons que l'on soit en difficulté et qu'on veuille envoyer un message pour demander du secours, sans que l'ennemi puisse comprendre. On part du message : A L' AIDE, que l'on transcrit[3] en chiffres en remplaçant chaque lettre par son rang dans l'alphabet : 1 12 1 9 4 5, puis, par un procédé ultra-secret et très difficile à décrypter (sic), on code ce message en : 25 14 25 17 22 21 et on peut ensuite le retranscrire en lettres : Y N Y Q V U.

Bien entendu, contrairement à ce que j'ai affirmé ci-dessus, le codage est très facile à déchiffrer, mais, et c'est un point essentiel, même sur un message aussi court, on voit apparaître ce qui va être le défaut rédhibitoire de ce type de codage : la lettre A, deux fois présente dans le message initial, est codée par Y qui apparaît aussi deux fois dans le message final : les fréquences sont conservées. Cela permet de déchiffrer aisément ce type de codage[4], comme on le sait depuis le tragique épisode de Marie Stuart que je relate maintenant.

Marie Stuart est une princesse écossaise, brièvement reine de France (1559-1560, c'était l'épouse de François II) puis reine d'Ecosse. A cette époque, l'Écosse et l'Angleterre étaient ennemies et Marie est capturée par la reine d'Angleterre Élisabeth première en 1568. En 1586 elle participe de sa prison à un complot contre Élisabeth et communique avec ses partisans au moyen de messages codés. Mais son code est décrypté par le linguiste flamand Thomas Phelippes, par la méthode d'analyse de fréquences. Cela permet à Élisabeth de traduire Marie en justice en l'accusant de complot. Elle est condamnée à mort et décapitée en 1587. On pourra consulter, sur ce sujet, http://codes.secrets.free.fr/stuart/stuart5.htm

Pour comprendre la méthode, un exemple littéraire va nous éclairer, il s'agit de la nouvelle *Le scarabée d'or* d'Edgar Poe. Dans ce texte, le personnage principal, William Legrand, décrypte un message du capitaine Kidd (un pirate du XVIII-ième siècle) indiquant l'emplacement d'un trésor. Voici le message :

53‡‡+305))6* ;4826)4‡4‡) ;806* ;48+8 960))85 ;1‡(; :+*8+83(88)5*+ ;46(;88*96 * ? ;8)*‡(;48
5) ;5*+2 :*‡(;4956*2(5*-4)8 98* ;4069285) ;)6+8)4‡‡ ;1(‡9 ;48081 ;8 :8‡ 1 ;48+85 ;4)485+5288
06*81(‡9 ;48 ;(88 ;4 (‡ ?34 ;48)4‡ ;161 ; :188 ;‡ ? ;

[2] Godement disait plutôt cela à propos des groupes d'homotopie des sphères, mais l'idée est la même.

[3] Ce n'est pas du tout ainsi qu'on procède en réalité pour numériser les messages. On peut utiliser par exemple le code ASCII.

[4] Bien qu'on sache depuis 1580 que ce genre de code est vulnérable, il a cependant été utilisé depuis, par les généraux sudistes lors de la guerre de sécession (1861-1865), par les troupes russes au début de la guerre de 1914-1918 et par le mafioso sicilien Bernardo Provenzano en 2006, ce qui a permis son arrestation.

Legrand note d'abord que, comme Kidd est anglais, le message est sans doute écrit dans cette langue. Ensuite, il utilise le fait qu'en anglais, les lettres n'apparaissent pas toutes avec la même fréquence, la plus courante étant E. Comme c'est le signe 8 qui est le plus fréquent dans le message, il en infère qu'on a 8=E et continue ainsi avec les autres lettres. Il constate aussi la présence de plusieurs groupements ; 48 dans le message. Un mot de trois lettres se terminant par E et fréquent en anglais, il n'est pas besoin d'être grand clerc pour penser qu'il s'agit de THE, ce qui donne ;=T et 4=H, etc. Bien entendu, à la fin, il trouve le trésor.

Le lecteur qui voudrait s'exercer déchiffrera le texte suivant[5] :

SALCFCFVHLCNEANVHHPLGNZIPUUANAKNRNHHLBNCFVHNYOANEGLYHKNZKVSOANHU NARNGNHZLHHNVAHGNZFGNHHNZANOHUALYZLPHKNHNHMPFYHYFYOMKVHTVLSPNY HNONYPA UNKPZPOLOPFYH en sachant que les lettres les plus fréquentes en français sont, dans l'ordre : E S A R I N T U O L

Attention, ces fréquences sont statistiques et dans un vrai texte il peut, par exemple, y avoir plus de T que de N.
J'ai moi-même été mis en difficulté par les élèves d'une classe de sixième du collège Alain Fournier à Orsay, qui avaient travaillé sur ce thème et m'avaient envoyé un message codé dont voici la traduction :

Jadis vivait un garçon, dans un camping-car, dans un bois. Il n'avait pas un sou. Mais il avait un voisin. Franck avait un chaton blanc, qui adorait dormir. Pour nourrir son chaton, il ramassa un abricot. Alors Franck a vu son voisin sortir son chiot, jusqu'à un marchand d'animaux pour avoir un chat. Puis alla au parc où il trouva un ami fictif, Yoan. Yoan lui raconta alors sa fiction. Un jour Yoan, alors rugbyman cassa sa FIAT, alors qu'il finissait son rugby match. Il prit donc un taxi. Joris, un ami, qui finissait lui son triathlon, l'aida. Un soir, Romain, un larron, cambriola Yoan, donc il alla au QG du FBI dans un hall pour dormir. Il faisait doux.

J'ai mis un certain temps à comprendre qu'il s'agissait d'un texte « à la Perec », c'est-à-dire sans la lettre E! Inutile de dire qu'ESARINTUOL n'est plus la bonne clé. Pour la trouver on peut faire une statistique sur le livre *La disparition* de Georges Perec, livre de 319 pages, dans lequel ne figure jamais la lettre E.

3. Le code RSA

3.1. Définition

Comme on l'a vu avec l'exemple de Marie Stuart[6], l'histoire de la cryptographie est une longue bataille entre codeurs et déchiffreurs. La problématique qui sous-tend la création du code RSA est la suivante.

Imaginons un espion E, loin de son pays et de son chef C. Il doit transmettre des messages secrets à C. Pour cela, il a besoin d'une clé[7] pour coder ses messages. Cette clé doit lui être transmise par son chef. Le problème, de nos jours, avec tous les satellites espions, c'est qu'on n'est pas sûr du tout que les ennemis n'écoutent pas les messages transmis. Or, avec la plupart des systèmes de codage, si l'on connaît la clé de codage, on sait aussi décoder les messages. Par exemple, imaginons que la clé soit l'opération qui, à une lettre, représentée par un nombre x modulo 26, associe $11x - 7$ (toujours modulo 26), ce qui associe par

[5] D'autres sont donnés en annexe.

[6] Voir aussi le décryptage du code de la machine Enigma des Allemands par Alan Turing pendant la seconde guerre mondiale.

[7] Par exemple, le message SALCFCF…proposé ci-dessus a été codé avec la clé : $x \to 7x+5$ modulo 26.

exemple à la lettre E la lettre V . On calcule alors facilement l'opération inverse[8], ce qui permet de décoder les messages.

Tout l'intérêt du code RSA, inventé en 1978 par Rivest, Shamir et Adleman, c'est, au contraire, qu'il est à sens unique : même si l'on connaît la clé de codage on n'en déduit pas une clé de décodage ! Voici le principe de cette méthode.

Le chef C calcule deux grands nombres premiers p et q (de nos jours, des nombres de l'ordre de 200 chiffres sont nécessaires), il calcule ensuite le produit pq (cela ne représente qu'une fraction de seconde pour une machine). Il choisit aussi un nombre e premier avec $p-1$ et $q-1$ (il y en a beaucoup, par exemple un nombre premier qui ne divise ni $p-1$ ni $q-1$). Il transmet à E la clé de codage, qui est constituée du nombre pq et du nombre e (mais il garde jalousement secrets les deux nombres p et q). La clé est **publique** : peu importe si l'ennemi l'intercepte. Pour coder le message, E n'a besoin que pq et de e, en revanche, pour le décoder, le chef C a besoin des deux nombres p et q. Le principe qui fonde le code RSA c'est qu'il est beaucoup plus facile de fabriquer de grands nombres premiers p et q (et de calculer pq) que de faire l'opération inverse qui consiste à décomposer le nombre pq en le produit de ses facteurs premiers.

Voici précisément la méthode de codage. Le message est un nombre $a < pq$ et premier[9] avec p et q. Pour le coder, E calcule a^e modulo pq (le reste b de a^e dans la division par pq). Là encore, une machine fait cela instantanément, voir ci-dessous. C'est ce nombre b qu'il envoie à son chef.

Comment faire pour retrouver a à partir de b ? Nous l'expliquons en détail au paragraphe suivant. L'idée est la suivante : comme e est premier avec $p-1$ et $q-1$, le théorème de Bézout montre qu'il existe un nombre d tel que $de \equiv 1 \pmod{(p-1)(q-1)}$. On montre que grâce à ce d on peut calculer a en faisant l'opération à l'envers : $a = b^d \pmod{pq}$. Il suffit donc de calculer d. Quand on connaît $(p-1)(q-1)$, trouver d est facile (c'est l'algorithme d'Euclide). Mais voilà : on a $(p-1)(q-1) = pq - p - q + 1$ et pour connaître ce nombre il nous faut $p+q$, donc p et q, mais, pour des nombres de cette taille (400 chiffres) on ne sait pas retrouver p et q à partir de leur produit pq et c'est ce qui assure la sécurité du code RSA. Pour illustrer notre propos, voici un exemple d'un nombre pq de 65 chiffres :

33263290819929542686848148817697305155927928386133083389000759099 7

Le logiciel SAGE répond instantanément qu'il n'est pas premier. En revanche, pour le factoriser, il met environ 20 secondes.

3.2. Quelques résultats arithmétiques

Rappelons d'abord le petit théorème de Fermat (voir par exemple [1] ou **3.14** ci-dessous) :

1.1 Théorème. *Soient p un nombre premier et $a \in \mathbb{Z}$. Alors p divise $a^p - a$ donc on a $a^p \equiv a$ modulo p. Si de plus a est premier avec p, on a $a^{p-1} \equiv 1 \pmod{p}$.*

[8] C'est $x \to 7x+3$, exercice.

[9] Pour être sûr de réaliser cela on prendra des messages plus petits que p et q. Par exemple si pq a 400 chiffres, on prendra des messages de moins de 200 chiffres. Ce seront des messages élémentaires, il en faudra sans doute plusieurs pour faire un message réel.

On a un corollaire de ce théorème :

1.2 Corollaire. *Soient p et q deux nombres premiers distincts et soit a premier avec pq. Alors on a* $a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$.

Démonstration. Il suffit de montrer que la congruence est vraie modulo p et modulo q. Pour cela on note que, comme $a^p - 1$ est congru à 1 modulo p, on a aussi $a^{(p-1)(q-1)} = (a^p - 1)^{q-1} \equiv 1^{q-1} = 1 \pmod{p}$. On procède de même pour q.

Le résultat suivant concerne encore les congruences (et c'est aussi la recette pour résoudre des équations du genre $ax \equiv b \pmod{s}$) :

1.3 Proposition. *Soit s un entier > 0 et soit e un entier > 0 premier avec s. Alors il existe un entier d > 0 tel que* $de \equiv 1 \pmod{s}$.

Démonstration. On applique le théorème de Bézout à s et e : il existe des entiers λ et μ avec $\lambda s + \mu e = 1$. Si μ est > 0 il suffit de poser $d = \lambda$. Sinon, on remplace μ par $\mu + sk$ et λ par $\lambda - ek$ avec k assez grand.

Enfin, le dernier résultat est la base de la méthode RSA :

1**.4 Proposition**. *Soient p et q deux nombres premiers distincts et soit a > 0 premier avec pq. Soit e un entier > 0 premier avec* $(p-1)(q-1)$ *et soit d > 0 tel que de soit congru à 1 modulo* $(p-1)(q-1)$ *(un tel entier existe par* ***1.3****).*
Alors, on a $a^{de} \equiv a \pmod{pq}$.

Démonstration. On a $de = 1 + m(p-1)(q-1)$, avec $m > 0$, donc, en vertu de **1.2** :

$$a^{de} = a \times a^{(p-1)(q-1)m} \equiv a \times 1^m = a \pmod{pq}:$$

3.2. Méthodes de calcul

Pour mettre en œuvre le code RSA on a besoin de calculer des puissances modulo pq. Bien entendu, si les nombres sont grands, pour calculer $a^e \pmod{pq}$ on ne peut pas commencer par calculer la puissance, puis la réduire modulo (pq). En effet, le nombre a^e dépasse très vite la capacité des ordinateurs. Une première méthode consiste à réduire modulo (pq) à chaque pas : on calcule a^2, on réduit : $a^2 \equiv b^2 \pmod{pq}$, puis on calcule ab^2, on réduit, etc. Il est très facile d'écrire un programme utilisant cette procédure. En voici un écrit avec le logiciel SAGE[10] :

```
def pw(a,e,p) :
z=1
for k in [1..e] : z= a*z%p
return z
```

[10] Qui utilise le langage Python.

Cette méthode est déjà bien meilleure, mais pas encore optimale. Une méthode plus astucieuse consiste à utiliser les puissances de 2. Elle combine deux types d'opérations simples : l'élévation au carré et la multiplication par a. Le lecteur pourra l'expérimenter en calculant (de tête) 23^{19} modulo 101.

Voici le programme correspondant sur SAGE[11] :

```
def pwr(a,e,p) :
z=1
while e!=0 :
if e%2==0 :
   e=e/2 ; a = a² %p
else :
  e=(e-1)/2 ; z=z*a%p ; a = a² %p
return z
```

Ce programme mérite un mot d'explication. On cherche $b := a^e \pmod p$. On entre a, e, p et on pose $z = 1$. On a donc $a^e z = a^e = b$. Dans le programme, les quantités a, e, z évoluent de telle sorte que $a^e z$ reste constant. En effet, si e est pair, z ne change pas, a devient a^2 et e devient e/2, donc $a^e z$ est invariant. Si e est impair, $e = 2k + 1$, a devient a^2, e devient k et z devient az, donc $a^e z$ devient $(a^2)^k \times az = a^{2k+1}\, z = a^e z$.
À la dernière _étape on a $e = 0$, donc $a^e z = z$ et cette quantité est bien le b cherché.

Avec le programme `pw`, le calcul `pw(642168086464,653246743,875312570876475323578)` prend près de 8 minutes tandis que la variante `pwr` ne prend que 196 milli-secondes.

Pour le décodage, il y a besoin d'expliciter les coefficients de Bézout de deux entiers $a; b$. C'est l'algorithme d'Euclide que SAGE exécute avec la commande `xgcd(a,b)`. Le lecteur qui voudrait en savoir plus sur le type de programme utilisé pourra consulter [2].

4. Fabriquer de grands nombres premiers c'est facile

4.1. Fermat

On a vu que le code RSA requiert de disposer de grands nombres premiers. Bien sûr, 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. Pierre de Fermat (1601-1665) avait cru trouver une formule donnant à coup sûr des nombres premiers. Voilà ce qu'il dit :

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 18 446 744 073 709 551 617 ; etc. Je n'en ai pas la démonstration exacte, mais j'ai exclu si grande quantité de diviseurs par dém établissent ma pensée, que j'aurois peine à me dédire. onstrations infaillibles, et j'ai de si grandes lumières, qui

[11] En fait, si l'on utilise SAGE, il y a une commande power_mod(a, e, p) qui fait exactement ce travail, un tout petit peu plus vite encore.

Traduit en formules, cela signifie que, pour tout entier n, le nombre[12] $Fn = 2^{2^n} + 1$ 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. On peut d'ailleurs faire le calcul à la main jusqu'à 257, voir **§2.3** quelques techniques pour cela. Pour voir que 65537 est premier, on peut utiliser la fonction is_prime de SAGE. En revanche, on constate, toujours avec SAGE, que $2^{32}+1$, $2^{64}+1$ et $2^{128}+1$ ne le sont pas. (Jusqu'à $2^{8192}+1$ SAGE donne une réponse négative en moins d'une seconde, pour $2^{16384}+1$ il met moins de trois secondes et pour $2^{32768}+1$, 15 secondes.) L'ordinateur factorise instantanément[13] :

$$2^{32}+ + 1 = 641 \times 6700417, \qquad 2^{64}+ + 1 = 274177 \times 67280421310721$$

$$2^{128}+ + 1 = 59649589127497217 \times 5704689200685129054721$$

et il met moins de 5 secondes pour $2^{256}+1$. En revanche, il cale sur le suivant[14], à savoir $2^{512}+1$ (qui a quand même 150 chiffres, c'était il n'y a pas si longtemps le record du monde de factorisation). En tous cas, on constate sur cet exemple que la primalité est plus facile que la factorisation !

On notera qu'à l'heure actuelle on ne sait pas exactement lesquels parmi les Fn sont premiers ou non. La réponse est seulement connue[15] pour un nombre fini de n et, sauf pour les 5 du début, tous les Fn en question sont composés. Cet exemple montre déjà deux choses, d'abord qu'un grand mathématicien peut dire des bêtises, et ensuite qu'il y a des questions, somme toute assez simples, pour lesquelles on n'a pas de réponse.

4.2. Mersenne

Faute de Fermat, on utilise les nombres de Mersenne (1588-1648) : $M_n = 2^n - 1$. Bien sûr, tous ne sont pas premiers, par exemple $2^4 - 1 = 15$ ne l'est pas. On montre (exercice) qu'il faut que l'exposant soit premier, mais cela ne suffit pas (par exemple on a $2^{11} - 1 = 2047 = 23 \times 89$). Cependant, c'est avec ces nombres qu'on obtient les records du plus grand nombre premier connu. Le plus ancien est celui de Cataldi en 1588 avec $M_{19} = 524287$. Il y eut ensuite Lucas (1876) avec M_{127} qui a 39 chiffres. Lucas a inventé un critère de primalité très efficace pour les nombres de Mersenne. Avec ce test, sur mon ordinateur, je montre instantanément que M_{11213} est premier (3376 chiffres, record 1963), ainsi que M_{216091} (en 18 minutes, c'est un nombre de 65050 chiffres, record 1985). Pour une description du test de Lucas, voir :

https://www.imo.universite-paris-saclay.fr/~daniel.perrin/CAPES/arithmetique/Lucas.pdf

Les records actuels sont détenus par d'énormes ordinateurs. Le dernier en date (7 décembre 2018) est $M_{82589933}$ qui a 24 millions de chiffres. Il faudrait pour l'écrire un livre de près de 10000 pages, mais le lecteur montrera, à titre d'exercice que ce nombre commence par 148894 et finit par 902591.

---

[12] Seuls les $2^r + 1$ où r est une puissance de 2 ont une chance d'être premiers à cause de la formule $a^m + 1 = (a+1)(a^{m-1} - a^{m-2} + a^{am-3} - \ldots - a+1)$ lorsque m est impair qui montre que $a+1$ divise $a^m + 1$ (ce qu'on retrouve encore plus simplement grâce aux congruences).

[13] Pour comprendre pourquoi 641 divise F_5 (ce qu'Euler avait montré) et d'où il sort, voir Annexe 6.

[14] J'ai laissé tourner la machine quinze heures sans succès.

[15] Précisément, le plus grand connu est $F_{2747497}$ qui est composé, le plus petit dont on ignore s'il est premier ou non est F_{33}.

5. Factoriser des grands nombres ?

Ce qu'il faut comprendre, c'est 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, comme on l'a déjà senti à propos des nombres de Fermat. Pendant longtemps, factoriser un nombre de l'ordre d'un milliard était considéré comme à peu près impossible. Ainsi Mersenne, en 1643, avait donné à Fermat, comme un défi, de factoriser le nombre 100895598169. Fermat avait répondu très rapidement :

À cette question je réponds que ce nombre 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.*

En fait, dans cet exemple, il y avait une sorte de tricherie. En revanche, Fermat savait factoriser 2027651281 et, dans ce cas il a explicité sa méthode. Sur tout cela, voir https://www.imo.universite-paris-saclay.fr/~daniel.perrin/Conferences/BNFredaction.pdf

Le même défi avait été présenté, de manière un peu présomptueuse, comme impossible par Stanley Jevons en 1874 avec le nombre 8616460799. Aujourd'hui, une calculatrice un peu perfectionnée factorise tous ces nombres sans difficulté.

Cependant, le record absolu de factorisation (daté du 2 décembre 2019) est bien loin de celui de primalité, c'est un nombre n de 240 chiffres, produit de deux nombres p et q de 120 chiffres, et encore a-t-il fallu pour trouver p et q 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. Voilà ces nombres :

$$124620366781718784065835044608106590434820374651678805754818788883289666801188210855036039570272508747509864768438458621054865537970253930571891217684318286362846948405301614416430468066875699415246993185704183030512549594371372159029236099 =$$
$$509435952285839914555051023580843714132648382024111473186660296521821206469746700620316443478873837606252372049619334517\times$$
$$244624208838318150567813139024002896653802092578931401452041221336558477095178155258218897735030590669041302045908071447$$

On notera tout de même que, dans les années 1980, 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 l'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[16] de chiffres. Les banques travaillent déjà avec des clés de l'ordre de 300 chiffres et les militaires avec des clés de 600 chiffres.

Et si un mathématicien améliorait fondamentalement les algorithmes de factorisation et leur permettait de rattraper les tests de primalité ? Alors, pour un temps au moins, il ne serait pas loin d'être le maître du monde[17] !

[16] En fait, les nombres de Mersenne sont proscrits comme clés RSA car ils sont trop particuliers, mais les logiciels comme Pari fournissent sans problème des nombres premiers de 5000 chiffres et SAGE en donne de plus de 1500 chiffres en quelques secondes.

[17] N'ayez pas trop d'espoir tout de même. On pense qu'il y a vraiment une raison profonde qui fait que la factorisation est beaucoup plus difficile que la primalité.

Si vous pensez détenir une méthode, voici deux nombres à factoriser. Pour une poignée de dollars (75 000 $), factoriser le code RSA suivant :

41202343698665954385553136533257594817981169
98443279828454556264338764455652484261980988 7
04231618418792614202471888694925609317763750 33
42113098239748515094490910691026986103186214 88
08669705649029036536588674370413731720813104
10519086425479328260139125762403394637326939 1

Et pour quelques dollars de plus (200 000 $), factoriser :

25195908475657893494027183240048398571429282126204032027777137 83
60436620207075955562640185258807844069182906412495150821892985 591
49176184502808489120072844992687392807287776735971418347270261 896
37501497182469116507761337985909570009733045974880842840179742 9100
64245869181719511874612151517265463228221686998754918242243363 7259
08514186546204357679842338718477444792073993423658482382428119 81638
15010674810451660377306056201619676256133844143603833904414952 634432
19011465754445417842402092461651572335077870774981712577246796292638635637328
99121548314381678998850404453640235273819513786365643912120103971228221207203 57

Ne passez pas trop de temps là-dessus : la société RSA qui mettait sur le marché quelques-uns de ses codes pour vérifier qu'ils étaient solides, en donnant des primes à qui les factoriserait, ne le fait plus depuis déjà quelque temps !

6. Annexe : Euler et les nombres de Fermat

On a vu, grâce à l'ordinateur, que 641 divise $F_5 = 2^{32} + 1$. La question est de savoir comment on peut trouver ce facteur et comment montrer directement qu'il divise F_5.

Le fait que 641 divise F_5 est facile. On pose $p = 641$ (on vérifie que c'est bien un nombre premier). On note les deux formules : $641 = 625 + 16 = 5^4 + 2^4$ et $641 = 640 + 1 = 5 \times 2^7 + 1$. On calcule 2^{32} modulo p. On a $5 \times 2^7 \equiv -1 \pmod{p}$. En élevant cette relation à la puissance 4 on a $5^4 \times 2^{28} \equiv 1 \pmod{p}$. Mais, on a $5^4 \equiv -2^4 \pmod{p}$ et donc $2^{32} \equiv -1 \pmod{p}$. Cela signifie exactement que p divise $2^{32} + 1$.
Une autre question est de trouver le facteur 641. En fait, c'est assez naturel et Fermat était familier de ce type d'arguments[18].
On suppose que F_5 admet un facteur premier p et on travaille dans le groupe multiplicatif $G = (\mathbb{Z}/p\mathbb{Z})^*$. Dans ce groupe on a $2^{32} = -1$, donc $2^{64} = 1$. On voit que 2 est un élément d'ordre 64 de G. Comme l'ordre d'un élément divise l'ordre du groupe, c'est que 64 divise $p - 1$. Cela signifie que p est congru à 1 modulo 64.
On peut même montrer que si p divise $2^{32} + 1$, p est congru à 1 modulo 128. Pour cela, il suffit de montrer que si l'on a $p \equiv 1 \pmod{8}$, 2 est un carré modulo p. En effet, si 2 est le carré de a, on a $2^{32} = a^{64} = -1$ et a est

[18] Il a trouvé ainsi le diviseur 223 de $2^{37}-1$, voir sa lettre à Mersenne de juin 1640. Cela rend son erreur assez mystérieuse. C'est probablement une simple erreur de calcul.

d'ordre[19] 128. Or on sait que F_p^* est cyclique d'ordre $p-1$, donc contient un élément ζ d'ordre 8, qui vérifie donc $\zeta^4 + 1 = 0$, ou encore $\zeta^2 + \zeta^{-2} = 0$, et on voit que $a = \zeta + \zeta^{-1}$ vérifie $a^2 = 2$.

Avec ce raisonnement, il n'y a plus que 641 comme candidat plausible.

II - L'ARITHMÉTIQUE AU COLLÉGE ET AU LYCÉE AUTOUR DE PRIMALITÉ ET FACTORISATION

1. Motivations

1.1. Côté mathématique

On a vu l'importance pour la cryptographie de savoir reconnaître qu'un nombre est premier et de savoir factoriser les nombres qui ne le sont pas. Les suggestions d'exercices ci-dessous se rapportent donc souvent à ces problèmes. Elles ont pour cadre le village[20] de Saint-Tricotin-sur-Pelote (Marne-et-Garonne) ...

Les connaissances mises en jeu ne sont peut-être pas explicitement au niveau du collège, mais peuvent toujours s'y rattacher. Attention, je ne prétends pas que tous ces thèmes peuvent être utilisés dans leur intégralité, ce sont seulement des pistes.

1.2. Des objectifs « philosophiques »

Un objectif essentiel de l'apprentissage des mathématiques est - à mon avis - d'apprendre aux élèves à chercher en les faisant réfléchir sur des problèmes ouverts : comment aborder un problème inconnu notamment par des méthodes expérimentales.

Un deuxième objectif est de leur montrer certains aspects méconnus des mathématiques : les applications, l'existence de questions non résolues, les incertitudes de la recherche, etc.

Un dernier objectif est de montrer qu'on peut s'amuser en faisant des mathématiques ...

1.3. Des objectifs techniques

À ces objectifs s'ajoutent des points plus techniques qu'il est nécessaire de renforcer. On peut citer : le calcul mental, les manipulations algébriques, l'utilisation des outils informatiques et de la programmation.

Du point de vue arithmétique, les exercices utilisent principalement la décomposition en produit de facteurs premiers, mais ils effleurent aussi de nombreux résultats (la division euclidienne, les congruences, Gauss, Bézout, Fermat, etc.).

1.4. Quels intérêts didactiques ?

Les exercices sont le plus souvent à géométrie variable, avec des possibilités d'adaptation, de simplification, d'extension ... Ils permettent d'illustrer l'idée que, même si l'on ne sait pas résoudre entièrement un problème, on peut toutefois s'en approcher.

[19] Avec cette ruse, il y a seulement à éliminer 257 et c'est à peu près évident car c'est lui-même un nombre de Fermat.

[20] Faut-il préciser qu'il est imaginaire ? Cela évite de se poser des questions de vraisemblance.

2. Primalité : dizaines riches ou pauvres

2.2. Dizaines riches

Fortuné Richard, le plus gros propriétaire de Saint-Tricotin-sur-Pelote (Marne-et-Garonne), ne jure que par la richesse. Il sait qu'à partir de 10, les nombres premiers se terminent par 1, 3, 7, 9 et il aime particulièrement les dizaines riches où les quatre possibles sont premiers comme 11, 13, 17, 19.
Il aimerait bien en avoir d'autres, mais il n'est pas très fort en calcul. Pouvez-vous l'aider à en trouver ? Y en a-t-il beaucoup ? une infinité ?

L'examen des premières dizaines montre qu'il n'y a aucune autre dizaine riche jusqu'à 100, mais que 101, 103, 107 et 109 sont premiers. Pour aller plus loin, il vaut mieux écrire quelques lignes de programme et c'est une bonne occasion d'en montrer l'intérêt :

```
def jujumeau(k) :
n=11
while n<k :
        if is prime(n) and is prime(n+2) and is prime(n+6) and is prime(n+8) :
          print (n)
n=n+30
```

(L'instruction $n = n + 30$ est un moyen d'accélérer le programme en notant que, dans deux dizaines sur trois, il y a un multiple de 3 qui se termine par 1, 3, 7 ou 9.)

On trouve alors les dizaines suivantes : 190, 820, 1480, etc. Il y en a 165 jusqu'à 106 et on a le sentiment qu'il doit y en avoir une infinité. Cela étant, et c'est l'intérêt de l'exercice, ce n'est qu'une conjecture, on ignore aujourd'hui encore s'il y a une infinité de dizaines riches[21] : il reste des choses à faire en mathématiques.

2.2. Dizaines pauvres

Pierre Labbé, lui, est plutôt du côté des opprimés. Il s'intéresse aux dizaines pauvres qui ne contiennent pas de nombre premier. En connaissez-vous ?
Sa tâche humanitaire ne s'arrête pas là : il prétend qu'il y a des centaines pauvres et même qu'on peut trouver un million de nombres de suite sans aucun nombre premier. Là, il exagère, non ?

La première dizaine pauvre est celle des 200 : 201 et 207 sont multiples de 3, 203 de 7 et 209 de 11. On peut aussi écrire un programme pour en trouver d'autres, mais ici, le résultat évoqué : *pour tout entier n il existe toujours n nombres consécutifs sans aucun nombre premier* est facile. Bien entendu il faut une idée, celle d'utiliser la factorielle[22] $n!$ et de considérer[23] $n! + 2$, $n! + 3$, ..., $n! + n$.

---

[21] Cette conjecture contient celle de l'infinitude des paires de nombres premiers jumeaux, c'est-à-dire distants de 2, comme 11 et 13, 17 et 19, 29 et 31, toujours ouverte elle aussi. Si la conjecture est vraie on peut montrer que le nombre de dizaines riches $\leq N$ est équivalent à $67:13N=(\ln(10N))^4$:

[22] Qu'on ne vienne pas me dire que cette notion n'est pas enseignée au collège. C'est vrai, mais mon expérience c'est que les collégiens comprennent immédiatement la notion et son utilité pour ce problème.

[23] Exercice : montrer que, si $n > 2$, on obtient n nombres composés consécutifs en ajoutant à ceux-là $n! + 1$ ou $n! + n + 1$. Voir la solution en annexe.

L'intérêt que je vois à ces deux exercices est de montrer l'imprévisibilité de la recherche : avec les dizaines pauvres et riches on a deux énoncés qui semblent voisins et pourtant l'un est inabordable et l'autre élémentaire.

2.3. Fabriquer des nombres premiers

Hortense Aignante, qui enseigne les mathématiques au collège Sainte-Aiguille de Saint- Tricotin a un truc pour fabriquer des nombres premiers : elle les prend sous la forme $a^2 + 1$.
Bien entendu, cela ne marche pas toujours, il faut faire attention au dernier chiffre de a, pourquoi ?
Avec cette précaution, $a^2+ 1$ n'est pas multiple de 2 ni de 5. Il n'est pas non plus multiple de 3. Pourquoi ? Et pour 7, 11, 13 ? Pouvez-vous trouver beaucoup de nombres premiers de la forme $a^2 + 1$? Une infinité ?
Sa cousine Clémence, qui joue la fille d'Euler, préfère utiliser les nombres de la forme $n^2 + n + 41$ ...

L'idée, comme pour les nombres de Fermat ou de Mersenne, est celle d'une sorte d'équité de la répartition: au voisinage d'un nombre très composé comme a^2, les autres ont plus tendance être premiers[24].

La question est donc : quels sont les a tels que $a^2 + 1$ soit premier ? Hormis le cas de $a = 1$, qui donne 2, il faut évidemment que a soit pair. Ensuite, l'exercice est une occasion d'un premier contact avec les congruences, d'abord dans leur forme élémentaire : quel peut être le dernier chiffre de a ? Hormis $a = 2$, qui donne 5, on constate expérimentalement qu'il faut que a se termine par 0, 4, 6 (sinon $a^2 + 1$ est multiple de 5). On peut le montrer[25] en écrivant, par exemple : $(10k + 2)^2 + 1 = 100k^2 + 40k + 4 + 1$. On trouve des exemples avec les trois finales : $101 = 10^2 +1$, $17 = 4^2 + 1$ et $37 = 6^2 + 1$.

On constate ensuite qu'un nombre de la forme $a^2 + 1$ n'est jamais multiple de 3. Pour le prouver, on écrit $a = 3k + r$ avec $r = 0, 1, 2$ et on calcule le carré[26] $9k^2 + 6rk + r^2$ avec $r^2 = 0, 1, 4$, de sorte que $r^2 + 1$ n'est pas multiple de 3. Si l'on veut aller plus loin, on peut voir que $a^2 + 1$ n'est jamais non plus multiple de 7, ni de 11. Pour ceux-là on peut se contenter de l'expérience, mais si l'on veut, par exemple pour 7, on y arrive en énumérant les carrés modulo 7. (Quand on est savant on sait que -1 est un carré modulo un nombre premier impair p si et seulement si on a $p \equiv 1 \pmod 4$, voir ci-dessous **§III.6**.)
Avec 13, comme on a $-1 \equiv 5^2$, pour avoir des mauvais a (c'est-à-dire des a tels que a^2+1 soit multiple de 13) il suffit de prendre $a \equiv \pm 5 \pmod{13}$.
La question naturelle, qui émerge si l'on écrit un programme donnant les $a^2 + 1$ est celle de leur infinitude. C'est encore une question ouverte ! Si l'on note $P_1(N)$ le nombre d'entiers $1 \leq n \leq N$ tels que $n^2 + 1$ soit premier on ne sait donc pas si $P_1(N)$ tend vers l'infini, mais si c'est le cas, Shanks a montré qu'on a $P_1(N) \sim 0.6864 \int_2^N \frac{dt}{\ln t} \sim 0.6864 \frac{N}{\ln N}$. Si la conjecture est vraie, un petit calcul montre que la probabilité de trouver un nombre premier de la forme $a^2 + 1$ avec $a \leq 10^n$ en se limitant aux nombres se terminant par 0, 4, 6 est presque exactement $1/n$.
Pour l'exemple des nombres $n^2 + n + 41$ (qui donnent des nombres premiers pour tout n entre 0 et 39), voir https://www.imo.universite-paris-saclay.fr/~daniel.perrin/journeedu2311/redaction2311e.pdf

[24] Idée aussi naïve que celle des joueurs de Loto qui pensent qu'un nombre qui vient de sortir à moins de chances de revenir.

[25] Je sais, on ne voit plus la formule donnant $(a + b)^2$ au collège, mais c'est un scandale absolu et, par ailleurs, on la retrouve aisément en développant $(a + b)(a + b)$ et elle saute aux yeux si l'on décompose un carré de côté $a + b$ en deux carrés et deux rectangles.

[26] Cet exercice est une véritable publicité pour deux choses : pour le dialogue expérience, conjecture, preuve et aussi pour les identités remarquables.

3. Factorisation

Pierre Landin, mathématicien en retraite à Saint-Tricotin, plus connu sous son pseudonyme de Dernier Lapin, a quelques trucs pour factoriser[27] un entier n. Il utilise la technique élémentaire qui consiste à diviser n par les nombres premiers p jusque $\sqrt{n}$. *Mais il a quelques ruses supplémentaires ...*

3.1. Les critères de divisibilité

Ils sont évidents pour 2 et 5 et faciles pour 3 et 11 mais c'est l'occasion d'un travail algébrique pour montrer ces critères, disons avec des nombres de trois chiffres. On écrit $n = 100c + 10d + u$. Pour 3, on écrit $n = 99c + 9d + c + d + u$ et n est multiple de 3 si et seulement si $c + d + u$ l'est. Pour 11 on écrit $n = 99c + 11d + c - d + u$ et n est multiple de 11 si et seulement si $c - d + u$ l'est.

3.2. Ajuster en retranchant ou en ajoutant

Pour voir si le nombre de Fermat 257 est multiple de 7, on retranche 7, il reste $250 = 25 \times 10 = 5 \times 5 \times 2 \times 5$ qui n'est pas multiple de 7, donc 257 non plus. C'est le lemme suivant :

2.1 Lemme. *Si p divise a et b il divise a + b et a − b.*

Démonstration. On écrit $a = pa'$, $b = pb'$ et on a $a - b = p(a' - b')$ et $a + b = p(a' + b')$.
Pour appliquer cette méthode, on se souvient que les nombres premiers se terminent par deux types de finales 3, 7 d'une part et 1, 9 de l'autre. L'application est facile si n et p sont du même type par rapport à 3, 7 ou 1, 9 comme 257 avec 7 ou 13. Précisément, si le nombre n se termine par 3 ou 7 il est facile de tester $p = 7, 13, 17, 23$, etc. S'il se termine par 1 ou 9 c'est facile pour 19, 29, 31, etc. C'est plus difficile si n et p sont de types différents. Dans ce cas il faut connaître des multiples de l'autre type. Voici les plus commodes : $3 \times 7 = 21$, $7 \times 7 = 49$, $3 \times 13 = 39$, $7 \times 13 = 91$, $3 \times 17 = 51$, $3 \times 19 = 57$, $3 \times 23 = 69$, $3 \times 29 = 87$, etc.

Cette méthode pose une question : pourquoi est-on sûr qu'il y a toujours un multiple de p qui se termine par un « bon » chiffre ? C'est le lemme suivant :

2.2 Lemme. *Soit p premier (distinct de 2 et 5) et soit a un chiffre en base 10, premier à 10 (donc 1, 3, 7, 9). Il y a toujours un multiple de p qui se termine par a.*

*Démonstration***.** Savamment, c'est le fait que p engendre $(\mathbb{Z}/10\mathbb{Z})^*$, qui n'est autre que le théorème de Bézout. Mais il n'y a pas besoin de ça, il suffit de regarder les terminaisons : si p se termine par 1, on obtient a en multipliant p par a, s'il se termine par 3 on multiplie par 7, 1, 9, 3 pour attraper 1, 3, 7, 9, etc. Autrement dit on constate, en faisant tous les produits $a \times b$ avec $a, b \in \{1, 3, 7, 9\}$:

2.3 Lemme. *Dans la table des 1, 3, 7 ou 9 on trouve un et un seul nombre se terminant par chacun des chiffres 1, 3, 7 ou 9.*

3.3. Une autre ruse pour éliminer des indésirables

C'est encore le lemme précédent (ou presque) qui sert pour voir qu'un nombre n (disons de trois chiffres) n'est pas multiple d'un p (disons 41) grâce aux terminaisons et aux ordres de grandeur. Si par exemple n est < 410, il y a un seul multiple de 41 pour chaque terminaison possible et on conclut avec l'ordre de

[27] Je me livre à ce genre de calcul en permanence, avec le total de mon ticket de cantine, avec les numéros des voitures dans la rue, etc.

grandeur. Par exemple, à cause de la terminaison, si 237 était multiple de 41 ce ne pourrait être que 7 × 41, mais comme on a 7 × 4 = 28, il est clair que 7 × 41 est trop grand. On peut faire le même raisonnement avec 373 et 47 (ce serait 9 × 47 donc de l'ordre de 430). Voici le lemme :

***2.4 Lemme**. Soit p un nombre premier distinct de 2 et 5 et soient a, b des chiffres en base 10. Si ap et bp ont même chiffre des unités on a a = b.*

Comme on le voit, toutes ces ruses requièrent une bonne connaissance des tables de multiplication et sont une motivation pour les réviser.

3.3. Divisible c'est bien beau, mais encore faut-il diviser

Ceci s'applique notamment pour 9 et 11. Dans le cas où l'on a repéré, grâce au critère de divisibilité, que n est multiple de 9 ou de 11, il s'agit de calculer le quotient. Pour cela, on repère l'ordre de grandeur et le dernier chiffre. Par exemple, si l'on cherche $n = 3483/9$, il se termine par 7, il est dans les 300 et plus grand que 348. De plus on doit retrouver $n \times 10$ en ajoutant n à 3483. On voit que n est de l'ordre de 370 ou 380 et c'est précisément[28] 387.

3.4. Différence de deux carrés

C'est la méthode qu'utilisait Fermat (et qui reste à la base des méthodes actuelles de factorisation). Si n est de la forme $a^2 - b^2$ il se factorise en $(a - b)(a + b)$. Par exemple on a $221 = 225 - 4$ et si l'on sait que $225 = 15^2$, on voit que c'est $(15 - 2)(15 + 2)$, donc 13×17.

De même on a $323 = 324 - 1 = 17 \times 19$, $5893 = 5929 - 36 = 77^2 - 6^2 = 71 \times 83$.

3.5. Les copains d'abord

Enfin, il y a plein de nombres que je connais comme premiers ou non, tous ceux < 100 (il suffit de savoir que $91 = 7 \times 13$), en fait jusqu'à 130 et quelques-uns qui sont mes copains pour diverses raisons : 163, 257, 641, 1729, etc.

3.6. Un exemple pas tout à fait évident : 3763

Il n'est pas multiple de 3 ni de 11. Pour 7 on voit le 63, pour 13, on utilise, en retranchant, $375 = 25 \times 15$ ou $375 = 390 - 15$, pour 17, $378 = 340 + 38$, pour 19, $3763 = 3800 - 37$, pour 23, $374 = 11 \times 34$, pour 29, $3763 + 87 = 3850$ et $385 = 5 \times 77$ ou 11×35, pour 31, $3763 = 3100 + 620 + 43$, 37 est clair, pour 41, $3763 - 123 = 3640$ et 364 serait 4×41, qui est trop petit, pour 43, 372 serait 4×43, non, pour 47, 381 serait 3×47 non, pour 53, 371 serait 7×53. Ah, c'est ça ! et on a donc $3763 = 53 \times 71$.

4. D'autres problèmes de Saint-Tricotin : la crue de la Pelote

À la suite des inondations provoquées par la crue de la Pelote, tout le canton de Saint-Tricotin a été sinistré. Le préfet de Marne-et-Garonne, Henri Bambel, est chargé de répartir les secours. Malheureusement, le bordereau qui portait la somme à diviser en parts égales entre les 396 victimes a été endommagé par les eaux et certains chiffres de la somme sont invisibles. On lit seulement 38 ••2 *Le préfet est bien embêté car il se souvient seulement que la somme attribuée à chacun était un nombre entier d'euros. Combien doit-il donner à chaque sinistré ?*

[28] On notera que 387 est encore multiple de 9 : 9 x 43.

Voici quelques éléments de solution. L'énoncé indique que le nombre $N = 38\bullet\bullet2$ est multiple de 396. Mais, ce dernier nombre se décompose en produit de facteurs premiers (ou plutôt primaires) : $396 = 4 \times 9 \times 11$. Il en résulte que N doit être à la fois multiple de 4, de 9 et de 11. (En fait, c'est équivalent, mais il n'y a pas besoin de savoir ça.) Examinons donc ce que donne chaque facteur.

Pour la divisibilité par 9 on a le critère déjà vu : la somme des chiffres doit être divisible par 9. Ici, il y a un point essentiel qui est de donner[29] un nom aux deux chiffres manquants : $N = 38xy2$ avec x, y entre 0 et 9. Dire que le nombre est divisible par 9 c'est dire que $3 + 8 + x + y + 2 = 13 + x + y$ l'est. On se récite la table des 9 en n'oubliant pas que x et y sont ≤ 9. Il reste deux possibilités : $x + y + 13 = 18$ ($x + y = 5$) ou $x + y + 13 = 27$ (donc $x + y = 14$) (le suivant $x + y + 13 = 36$ donne $x + y = 23$ et c'est trop). On garde ça en réserve.

On fait la même chose avec 11, mais avec la somme alternée des chiffres : $3 - 8 + x - y + 2 = x - y - 3$ doit être multiple de 11. Attention, là, $x - y - 3$ peut être négatif, et c'est une grosse difficulté. On regarde donc les multiples de 11 et il y a une autre difficulté qui est de ne pas oublier 0. Si $x - y - 3 = 11$, on a $x - y = 14$ et c'est impossible avec $x \leq 9$. Bien sûr c'est encore pire avec 22, etc. Si $x - y - 3 = 0$ on a $x - y = 3$. Si $x - y - 3 = -11$, on a $x - y = -8$ ou encore $y - x = 8$, et c'est tout juste possible, avec $x = 0$, $y = 8$ ou $x = 1$, $y = 9$. On garde ça en réserve.

Pour la divisibilité par 4 il faut regarder la table des 4 et on voit que les multiples de 4 sont pairs (ça c'est clair !), ce qui est le cas ici, car le chiffre des unités est 2, mais attention, parmi les nombres se terminant par 2, seuls ceux dont le chiffre des dizaines est impair[30] sont multiples de 4 (12, 32, 52, 72 et 92 mais pas 22, 42, etc.) Les centaines et les chiffres d'ordre plus grand ne changent rien car 100 est multiple de 4. On retient donc une seule chose : le nombre y est impair.

On revient à ce qu'on a trouvé avec 11. On a soit $x - y = 3$, soit $y - x = 8$ et on a vu que cette dernière solution donne, avec y impair, $y = 9$ et $x = 1$. Mais la somme $x + y$ est alors égale à 10, donc ni à 5 ni à 14. Bref, il reste $x + y = 3$. Du côté de la somme on a soit $x + y = 5$, soit $x + y = 14$. Si l'on est malin, on note que $x - y$ et $x + y$ sont de même parité car on a $x + y = x - y + 2y$. Il reste donc $x + y = 5$. Là, avec $x - y = 3$, on voit aussitôt la solution qui est $x = 4$, $y = 1$. (Si l'on ne voit rien on peut calculer $(x + y) + (x - y) = 8 = 2x...$) et on trouve $N = 38412$ et $N/396 = 97$.

En fait, si l'on est astucieux, on peut trouver ce résultat très vite[31]. On voit que le quotient q de N (de l'ordre de 38000) par 396 doit être un peu en dessous de 100. On voit aussi que le chiffre des unités de q doit être 2 ou 7 (car il faut trouver 2 en multipliant par 6). On essaie 92, c'est trop petit, mais 97 convient !

Il est clair que cet exercice est difficile et qu'il demande de l'initiative. Le contenu mathématique proprement dit comporte la factorisation (de 396), l'introduction d'inconnues, les critères de divisibilité et l'exploitation des résultats. On peut adapter la difficulté, par exemple on a une variante facile avec 36 sinistrés et $N = 7x6$ à distribuer et une variante difficile avec 2772 sinistrés et $N = 71xyz4$ (seule solution 712404, parts de 257, avec là encore une variante plus rapide par division et essais.). Pour éviter l'usage de cette méthode par division et essais, il suffit d'effacer le premier chiffre de N. Par exemple on peut prendre,

[29] Pour un mathématicien c'est un réflexe évident, mais c'est un point dont les élèves ne sont pas toujours persuadés. Cet exemple est très convaincant de ce côté.

[30] Ici, on peut se convaincre du résultat en énumérant tous les possibles ou écrire une preuve algébrique.

[31] C'est un défaut de cette version de l'exercice !

toujours avec 396 sinistrés, N = •02•2 (solution 50292 = 396 × 127). Attention aussi à la position des inconnues, de manière à avoir la somme avec le critère par 9 et la différence avec celui par 11. Sans cela, il y a souvent plusieurs solutions (5 solutions pour 3*x*4*y*2 avec 396).

5. Les dimensions des champs

A la suite des inondations provoquées par la crue de la Pelote, les champs rectangulaires d'Elisabeth Rave ont été inondés, leurs bornes ont disparu et le cadastre a été endommagé. Elisabeth, qui a pris un coup de vieux, a oublié les dimensions de ses champs. Elle se souvient juste qu'elles étaient toutes entières et plus grandes que 20. Pour les deux premiers, elle se souvient que leurs aires étaient de 851 et 858 et que leurs périmètres n'étaient pas plus que 120. Pour le dernier que le périmètre était 360 et le pgcd des dimensions 18. Aidez-là à retrouver les dimensions de ses champs.
L'unité de longueur est le décamètre (1 dam = 10m) l'unité d'aire est l'are ou dam².

Si l'aire d'un champ rectangulaire est de 851, on décompose ce nombre en produit de facteurs premiers : 851 = 23 × 37. Les dimensions peuvent donc être seulement 23 et 37 (*a priori* il y a aussi 1 et 851, mais, outre le fait que c'est très improbable pour un champ, c'est contraire à l'hypothèse sur le périmètre). Dans ce cas facile la réponse est donc 23 et 37.

Pour le second on a 858 = 2 × 3 × 11 × 13 il y a beaucoup plus de solutions. Il faut énumérer les diviseurs de ce nombre. Je propose pour cela une méthode qui consiste à ordonner ces diviseurs selon le nombre de leurs facteurs premiers : 0 facteur : 1, puis 1 facteur, 2, 3, 11, 13 puis 2 facteurs : 6, 22, 26, 33, 39, 143, puis 3 facteurs (les « compléments » des 1 facteur) : 66, 78, 286 et 429 et enfin 858. Chacun de ces diviseurs vient avec son complément. La condition sur les périmètres permet d'écarter aussitôt nombre de solutions et il ne reste que 22, 39 ou 26, 33. Dans le premier cas le périmètre est 122, dans le second 118. La solution est donc 26, 33.

Il reste le champ de périmètre 360. Appelons a, b ses dimensions. On a donc $a + b = 180$ et $pgcd(a, b) = 18$. Ce qu'il faut connaître, là, c'est ce que j'appelle la comptine du *pgcd* : on a $a = 18a'$, $b = 18b'$ avec a' et b' premiers entre eux. On a donc $a' + b' = 10$ et, si l'on n'oublie pas la condition premiers entre eux, il reste seulement les solutions $a' = 1$, $b' = 9$, $a' = 3$, $b' = 7$ (ou les mêmes à l'envers). Cela donne $a = 18$, $b = 162$, que l'on rejette car l'une des dimensions est < 20, ou $a = 54$, $b = 126$ qui est la bonne solution.

Le thème général de ce type d'exercices est de déterminer deux entiers a, b à partir de certaines quantités qui leur sont liées. Sur ce dernier point, il y a une foule de possibilités et on peut laisser libre cours à son imagination. Il y a bien sûr la somme $a + b$ et le produit ab mais aussi $a^2 + b^2$, $a^2 - b^2$, le *pgcd*, le *ppcm*, etc. Ces variantes peuvent être plus ou moins difficiles selon les choix, voir de nombreux exemples dans [1]. Parfois une seule donnée suffit. L'intérêt majeur de l'exercice proposé est le travail sur la factorisation et l'énumération de diviseurs. Du point de vue technique, il y a aussi l'utilisation de la disjonction de cas et de la comptine du pgcd. Certains choix peuvent même mener à des problèmes ouverts, par exemple $a^3 - b^2$ (ou $a^3 + b^2$) qui correspond à l'équation de Bachet.

6. Le druide de Septimanie

Dans la Gaule antique, le village de Saint-Tricotin-sur-Pelote (Marne-et-Garonne) se trouvait au cœur d'une région appelée Septimanie, nommée ainsi parce que ses habitants avaient la manie de compter en base 7. On sait que les Gaulois ne craignaient qu'une chose, c'est que le ciel ne leur tombe sur la tête, ce qui est une façon de craindre la fin du monde. D'ailleurs, feu le druide Pacorabanix, fort versé en numérologie, avait prévu ce cataclysme pour l'an

$\overline{5555}$. *Les esprits forts savent que cette prévision est sujette à caution, puisqu'il n'y a aucune raison que ce nombre, remarquable en base 7, le soit encore dans une autre base et ils le vérifieront en calculant ce nombre en base 10.*

C'est juste une récréation : le nombre 5555 en base 7 n'est autre que 2000 en base 10 !

7. Les champs carrés

Elisabeth Rave, la fermière de Saint-Tricotin, aime les champs carrés et elle connaît bien les entiers qui sont des carrés parfaits (1, 4, 9, 16, ..., 2809, ...). À défaut elle essaie d'écrire les entiers $n \geq 0$ comme différence de carrés parfaits (donc sous la forme $n = x^2 - y^2$ avec x, y entiers ≥ 0). Elle y arrive souvent, mais pas toujours.
Peut-on le faire avec les entiers suivants (et, lorsque c'est possible, de combien de manières) : 5, 11, 14, 17, 18, 20, 44, 45, 56, 66, 162, 257, 391, 426, 432, 452 ?
Pouvez-vous préciser tous les entiers qui peuvent s'écrire sous cette forme ?

On commence par explorer l'exercice avec les premières valeurs données[32]. On a facilement $5 = 9 - 4 = 3^2 - 2^2$, $11 = 36 - 25 = 6^2 - 5^2$. Avec un peu de patience on trouve $17 = 81 - 64 = 8^2 - 7^2$, mais, même avec un peu d'obstination, 14 n'a pas l'air de marcher. Si l'on regarde bien, on voit que dans tous les cas positifs ci-dessus on a pris la différence de deux carrés consécutifs. Si l'on écrit cela algébriquement[33] $(n + 1)^2 - n^2 = 2n + 1$ (en développant $(n + 1)^2$ ou en utilisant la différence de deux carrés), on voit qu'on va attraper ainsi tous les impairs. Par exemple, $391 = 2 \times 195 + 1 = 196^2 - 195^2$.

Il reste les pairs. On commence par le commencement, c'est-à-dire le nombre 2. En consultant la liste des carrés et la taille des différences, on constate que 2 ne peut pas s'écrire comme différence de deux carrés. On le prouve facilement avec l'écriture algébrique, si l'on connaît les identités remarquables. En effet, si l'on a $2 = x^2 - y^2 = (x - y)(x + y)$, la seule façon de faire cela en entiers c'est de prendre $x - y = 1$ et $x + y = 2$, mais ça n'existe pas ! Il y a de multiples manières de le voir, la plus simple étant de noter que x et y sont compris entre 0 et 2 et d'essayer tous les cas. Mais on peut aussi résoudre le système et constater qu'il apparaît des demi-entiers, ou encore noter $x + y = (x - y) + 2y$ de sorte que $x - y$ et $x + y$ doivent être de même parité.

On peut alors revenir au cas de 14. Si $14 = (x - y)(x + y)$, avec x, y entiers, les seules solutions sont $x - y = 1$ et $x + y = 14$ ou $x - y = 2$ et $x + y = 7$ et, là encore, la parité contredit. Avec cette réflexion on obtient le résultat général. En effet, supposons qu'on ait $n = x^2 - y^2$ avec n pair. On a donc $n = (x - y)(x + y)$ donc l'un des nombres $(x - y)$ ou $(x + y)$ est pair. Mais alors ils le sont tous les deux et n est multiple de 4. On ne peut donc pas écrire sous cette forme les nombres pairs qui ne sont pas multiples de 4.

Il faut encore vérifier que les multiples de 4 marchent. L'expérience avec $4 = 2^2 - 0^2$, $8 = 3^2 - 1^2$, $12 = 4^2 - 2^2$ montre qu'il faut prendre des entiers écartés de 2 : $4p = (p + 1)^2 - (p-1)^2$, toujours les identités remarquables.

Il reste la question plus délicate du nombre de façons d'écrire n sous la forme $x^2 - y^2$ quand c'est possible. Supposons d'abord n impair. On décompose n en produit de facteurs premiers $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ et on cherche à l'écrire $(x - y)(x + y)$. Pour cela, on prend pour $a = x - y$ et $b = x + y$ deux diviseurs de n, « complémentaires » (c'est-à-dire tels que leur produit soit égal à n) avec $a \leq b$. Il reste à montrer le lemme suivant :

[32] Il peut être utile d'établir la liste des carrés des nombres de 1 à 20.

[33] On voit ici, de manière éclatante, tout l'intérêt de l'écriture algébrique.

2.5 Lemme. *Si a, b sont des entiers impairs, avec* $a \leq b$, *le système* $a = x - y$, $b = x + y$ *a une solution unique dans les entiers* ≥ 0.

Démonstration. La solution est $x = \frac{b+a}{2}$ et $y = \frac{b-a}{2}$.
Le nombre *S* de solutions, dans le cas impair, est donc le nombre de diviseurs *a* de *n* tels que $a \leq b = n/a$. Comme le nombre total de diviseurs de *n* est (α_1+1) _ _ _ (α_r+1), *S* est la moitié de ce nombre (s'il est pair, ce qui est le cas sauf si n est un carré, cas que le lecteur examinera ...). Par exemple, pour $n = 391 = 17 \times 23$, on a $\alpha_1 = \alpha_2 = 1$, donc il y a deux solutions, $a = 1$, $b = 391$ qui donne $x = 196$ et $y = 195$, mais aussi $a = 17$, $b = 23$ qui donne $x = 20$ et $y = 3$. Pour $6615 = 3^3 \times 5 \times 7^2$ il y a 12 solutions.

Il reste le cas où *n* est multiple de 4 : on écrit $n = 4k = (x - y)(x + y)$ avec $x - y$ et $x + y$ de même parité donc pairs, $x - y = 2p$, $x + y = 2q$, donc $k = pq$ et on est ramené à chercher les décompositions de *k*. Par exemple, pour $464 = 4 \times 116$, les décompositions de 116 sont 1, 116 ; 2, 58 et 4, 29 qui donnent pour *x*, *y* : 117, 115 ; 60, 56 et 33, 25.

Il est facile d'écrire un programme qui donne toutes les décompositions : le seul point délicat est de borner *x*. Comme on a $x + y \leq n$ et $x > y$ on en déduit $y < n/2$, comme $x - y$ divise *n*, on a $x < 3n/2$. Voici un exemple écrit avec SAGE :

```
def rave(n):
    for y in [0..(n-1)/2] :
        for k in [0..sqrt(y^2+n)-y] :
            if k^2+2*k*y==n :
                print (y+k,y)
```

Cet exercice montre l'intérêt d'une approche expérimentale des mathématiques. En effet, pour le résoudre, on peut commencer par regarder quelques cas particuliers, avec des *n* petits, par tous les moyens, y compris très artisanaux. L'intérêt est de voir se dégager les phénomènes : le cas des impairs, la difficulté pour les nombres pairs non multiples de 4. Cette approche peut mener à des conjectures qui donneront le résultat final. Ensuite, pour écrire une preuve on aura besoin de l'écriture algébrique, particulièrement efficace dans ce cas, qui mettra aussi en évidence l'intérêt de factoriser en arithmétique. On verra aussi apparaître d'autres notions : les congruences modulo 4, les équations linéaires. Enfin, pour la question du nombre de solutions, c'est encore la décomposition en produit de facteurs premiers qui sera essentielle, avec l'énumération des diviseurs.

8. Non à l'euro ! ¶

Le maire de Saint-Tricotin-sur-Pelote (Marne-et-Garonne), Jacques Huse, très hostile à l'Europe, a décidé de quitter la zone euro et de faire utiliser aux habitants de Saint-Tricotin leur propre monnaie : la maille. Pour éviter de frapper trop de sortes de pièces, deux types de pièces seulement seront disponibles, l'une de 9 mailles, l'autre de 11 mailles.

1) Au début de l'opération, les commerçants n'ont pas de pièces pour rendre la monnaie et les acheteurs doivent faire l'appoint. Faire la liste des sommes ≤ 30 mailles que l'on peut payer. Peut-on payer les sommes suivantes (en mailles) : 41, 53, 71, 79 *?*

2) Montrer qu'on peut payer toutes les sommes de c mailles avec $80 \leq c \leq 88$, *puis toutes les sommes* $c \geq 80$, *par exemple 118 ou 417 (on suppose que l'acheteur a à sa disposition autant de pièces qu'il veut) (¶). Indiquer toutes les manières de le faire (¶¶).*

3) On suppose qu'au bout d'un certain temps les commerçants ont un stock de pièces suffisant pour rendre la monnaie. Montrer qu'on peut maintenant payer n'importe quelle somme entière (on pourra commencer par la somme de une maille). Comment payer les sommes suivantes : 13 mailles, 41 mailles, 79 mailles en manipulant le moins possible de pièces (¶¶) ?

Je détaille ci-dessous la solution et les divers arguments. Bien entendu, tout n'est pas faisable en classe, mais c'est un thème très riche.

8.1. Sans rendre la monnaie, 1)

Si l'on ne rend pas la monnaie, les seules sommes que l'on peut payer sont de la forme $9a + 11b$ avec a, b entiers ≥ 0. Pour avoir toutes les sommes possibles ≤ 30 et ne pas en oublier, une technique sûre consiste à ordonner les tentatives selon les valeurs de $s = a + b$. Ainsi, $a + b = 0$ donne $a = b = 0$, $a + b = 1$ donne (1, 0) ou (0, 1), etc. On obtient comme sommes possibles : 0 ($s = 0$) ; 9, 11 ($s = 1$) ; $18 = 2 \times 9$, $20 = 9 + 11$, $22 = 2 \times 11$ ($s = 2$) ; $27 = 3 \times 9$, $29 = 2 \times 9 + 11$ ($s = 3$) et c'est tout pour les sommes ≤ 30 car $9 + 2 \times 11 = 31$ et $4 \times 9 = 36$.

Pour décider lesquelles sont possibles parmi les quatre propositions 41, 53, 71, 79, on peut faire la liste des multiples de 9 et de 11 et essayer d'en ajuster deux qui font le total. On trouve ainsi, avec un peu de patience, $53 = 44 + 9$ et $71 = 44 + 27$.

En revanche, on ne peut pas payer 41 ni 79. Détaillons le raisonnement pour 41. On regarde les multiples de 11 plus petits que 41 et on ne gagne que si la différence avec 41 est multiple de 9. Or on a $41 = 33 + 8 = 22 + 19 = 11 + 30 = 0 + 41$ et aucun ne convient. On peut même aller un peu plus vite, par exemple pour 79 on part de 77, avec $79 = 77 + 2$ et chaque fois qu'on diminue de 11 le 77 on ajoute 11 à 2. On trouve successivement : 2, 13, 24, 35, 46, 57, 68, 79. Comme aucun n'est multiple[34] de 9 le paiement est impossible. On peut d'ailleurs utiliser cette méthode aussi pour traiter les cas positifs. Avec 53 on gagne tout de suite, $53 = 44 + 9$, avec 71 on a $71 = 66 + 5 = 55 + 16 = 44 + 27$, stop.

8.2. Sans rendre la monnaie, 2)

Pour les sommes entre 80 et 88 c'est un peu plus rusé. Il y a évidemment deux nombres faciles : $88 = 8 \times 11$ et $81 = 9 \times 9$. Si, dans le $88 = 8 \times 11$, on change un 11 pour un 9, on diminue la somme de 2, donc on obtient 86, 84, 82, 80 (et même 78, 76, 74, 72 mais on n'en a pas besoin ici). Si, dans $81 = 9 \times 9$, on change un 9 pour un 11 on augmente de 2, et on obtient donc 83, 85, 87 (et les suivants jusqu'à 99). On voit qu'on a bien obtenu toutes les sommes comprises entre 80 et 88.

En fait, cette procédure donne un moyen d'avoir toutes les sommes possibles. On part d'un seul 9, on peut le changer en 11, on a donc 9, 11. Avec deux 9 on trouve 18, 20, 22, on continue ainsi à partir du multiple $k \times 9$ en allant de deux en deux jusqu'au multiple $k \times 11$, par exemple 36, 38, 40, 42, 44, etc. (Ici on voit que 41 manque). Du côté de 79 la série est $72 = 8 \times 9$, 74, 76, 78, 80, …, $88 = 8 \times 11$.

Il reste à montrer qu'au-delà de 80, on peut payer toutes les sommes. L'idée est très simple : si l'on peut payer une somme s, on peut payer aussi[35] $s + 9$, $s + 18$, $s + 27$, etc. Mais, comme on a toutes les sommes entre 80 et 88, on a, pour le dire savamment, toutes les congruences modulo 9, donc on va pouvoir tout

[34] Mais on voit bien que si l'on en prenait un 11 de plus, on aurait un multiple de 9, à savoir 90.

[35] On peut aussi ajouter 11, 22, etc.

obtenir. De manière élémentaire, si l'on ajoute 9 à 80, on voit qu'on obtient 89 (donc on fait la jonction avec 88) et avec 81,…, 88 on obtient les 8 suivants jusqu'à 97. En recommençant avec 89, 90, …, 97 on obtient 98 et les 8 suivants, etc.

Quand on part d'une somme fixée, par exemple 118, on peut procéder par essais et erreurs, mais si l'on veut éviter cela, le raisonnement est le suivant. On divise 118 par 9 : $118 = 9 \times 13 + 1$, le reste est 1. Pour trouver le point de départ convenable entre 80 et 88 on prend le nombre dont le reste est 1, c'est 82 et on a $118 - 82 = 36 = 4 \times 9$. Comme on a $82 = 5 \times 11 + 3 \times 9$ on trouve $118 = 5 \times 11 + 7 \times 9 = 55 + 63$.

Dans le cas de 417, on a $417 = 9 \times 46 + 3$ et $84 = 9 \times 9 + 3$. Comme on a $84 = 6 \times 11 + 2 \times 9$, on ajoute $417 - 84 = 333 = 37 \times 9$. On obtient la solution $417 = 6 \times 11 + 39 \times 9$.

Bien sûr, quand on sait que la congruence modulo 9 d'un nombre est aussi celle de la somme de ses chiffres, par exemple qu'on a $417 \equiv 4 + 1 + 7 \equiv 3 \pmod 9$, on trouve le résultat bien plus vite.

On obtient ainsi une solution. Pour les avoir toutes il suffit de remplacer 11×9 par 9×11 jusqu'à plus soif et on trouve $417 = 15 \times 11 + 28 \times 9$ puis $417 = 24 \times 11 + 17 \times 9$ et enfin $417 = 33 \times 11 + 6 \times 9$. Ce qui est derrière est le résultat suivant :

2.6 Lemme. *Si l'on a $9a + 11b = 9c + 11d$, avec, par exemple, $a < c$, on a $c - a = 11k$ et $b - d = 9k$ avec $k > 0$.*

Démonstration. On a $9(c - a) = 11(b - d)$ et, comme 11 est premier avec 9, il divise $c - a$ par Gauss, donc on a $c - a = 11k$ et on en déduit $b - d = 9k$.

On peut aussi trouver ces solutions en écrivant quelques lignes de programme.

Pour déterminer le nombre de solutions dans le cas général le mieux est d'écrire une relation de Bézout avec 1, par exemple $1 = 5 \times 9 - 4 \times 11$. Cela donne $n = 5n \times 9 - 4n \times 11$ et le raisonnement ci-dessus montre que toutes les solutions de l'équation $n = 9a + 11b$ sont de la forme $n = (5n - 11k) \times 9 + (9k - 4n) \times 11$, avec $k \in \mathbb{Z}$. Pour avoir des coefficients $a, b \geq 0$, il suffit que $5n - 11k$ et $9k - 4n$ soient ≥ 0. Cela signifie $\frac{4n}{9} \leq k \leq \frac{5n}{11}$. Si l'écart est ≥ 1 on est sûr de trouver un entier. Comme l'encadrement s'écrit $\frac{44n}{99} \leq k \leq \frac{45n}{99}$, c'est évidemment vrai pour $n \geq 99$.

Traitons l'exemple de 417. On écrit $417 = (5 \times 417 - 11k) \times 9 - (9k - 4 \times 417) \times 11$ et il faut que les deux coefficients soient ≥ 0 ce qui donne $185.33 \leq k \leq 189.54$, donc $k = 186, 187, 188$ ou 189 et retrouve les quatre solutions ci-dessus.

Pour une discussion approfondie sur ce thème, voir :

https://www.imo.universite-paris-saclay.fr/~daniel.perrin/CAPES/arithmetique/diophantepositif.pdf

8.3. En rendant la monnaie

Pour traiter le cas général il suffit d'écrire une relation de Bézout avec 1 et les deux plus simples sont $1 = 55 - 54 = 5 \times 11 - 6 \times 9$ ou $1 = 45 - 44 = 5 \times 9 - 4 \times 11$. À partir de ces relations, on trouve tous les entiers n en multipliant ces relations par n.

Cela étant, la solution ainsi obtenue n'est pas toujours optimale (au sens où $|a| + |b|$ est minimal : manipuler le moins de pièces possible). Ainsi on trouve avec cette procédure $13 = 13 \times 5 \times 11 - 13 \times 6 \times 9$ alors qu'on peut faire $13 = 22 - 9$. Pour trouver la plus petite solution on peut partir d'une de celles dont

on dispose $n = 11a - 9b$ et prendre $11(a - 9k) - 9(b - 11k)$ en prenant pour k un entier tel que $|a - 9k|$ et $|b - 11k|$ soient les plus petits possibles.

Attention, si $n > 99$ il n'y a pas de raison que les quotients euclidiens de a par 9 et de b par 11 soient les mêmes. Par exemple, avec $417 = 2085 \times 11 - 2502 \times 9$ on a $2085 = 231 \times 9 + 6$ et $2502 = 227 \times 11 + 5$. En prenant au milieu 229 on trouve $417 = 24 \times 11 + 17 \times 9$, avec un coût $c = 24 + 17 = 41$, mais on peut faire mieux avec $33 \times 11 + 6 \times 9$, $c = 39$. Quelques lignes de programme montrent que c'est le meilleur résultat possible.

Voici les réponses optimales pour les sommes proposées : $13 = 22 - 9$, coût en nombre de pièces 3, $41 = 63 - 22$, coût 9, $79 = 88 - 9$, coût 9.

Le lecteur curieux et patient pourra établir le résultat général :

2.7 Proposition. *Soit n un entier positif. On écrit $5n = 11q + r$ avec $0 \leq r < 11$. La solution optimale de l'équation $9x+11y = n$ dans $\mathbb{Z}$ (c'est-à-dire celle pour laquelle $|x|+|y|$ est minimum) est donnée par $x = 5n + 11k$ et $y = -4n - 9k$ avec k défini comme suit :*

A) *Si $q \geq 4r$, on a $k = -q$ et le minimum vaut $n - 2q$.*

B1) *Si $q < 4r$ et $9r \leq q + 50$, on a $k = -q$ et le minimum vaut $9n - 20q$.*

B2) *Si $q < 4r$ et $9r > q + 50$, on a $k = -q - 1$ et le minimum vaut $-9n + 20q + 20$.*

2.8 *Remarque*. Le cas B1 se produit pour les n suivants : 1, 3, 5, 7, 10, 12, 14, 16, 21, 23, 25, 30, 32, 34, 41, 43, 50, 5, 61, 70. Le cas B2 pour les n suivants : 2, 4, 6, 8, 13, 15, 17, 19, 24, 26, 28, 35, 37, 39, 46, 48, 57, 59, 68, 79. Pour tous les autres n on est dans le cas A.

C'est une situation très riche et il me semble qu'il faut admettre, dans un premier temps, des solutions artisanales par approximations successives. Qui n'a jamais tâtonné pour trouver un résultat mathématique ne s'est sans doute jamais frotté à un résultat un peu difficile. Bien entendu, ensuite, il est important de donner aussi des méthodes fiables et certaines.

C'est enfin un thème où l'utilisation de l'ordinateur apporte beaucoup. Du point de vue mathématique, le ressort de l'exercice est le fait que 9 et 11 étant premiers entre eux ils vérifient une relation de Bézout. Le théorème de Gauss n'est pas très loin non plus.

III - ANNEXE 1 : QUELQUES COMPLÉMENTS

Je donne ici quelques démonstrations de résultats utilisés dans ce qui précède, avec des versions relativement élémentaires[36], renvoyant le lecteur qui voudrait en savoir plus à [1].

1. Deux axiomes

Les deux axiomes ci-dessous seront essentiels pour les démonstrations. On peut les considérer comme intuitivement évidents.

Il y a d'abord l'axiome de « bon ordre » sur les entiers :

[36] Mais rédigées pour des professeurs, pas pour des élèves.

3.1 Axiome. *Toute partie non vide de* $\mathbb{N}$ *admet un plus petit élément.*

Cet axiome, évoqué par René Cori dans sa conférence, est essentiellement équivalent au principe de récurrence, voir [1] chapitre 1. Il s'utilise en raisonnant par « absurde et minimalité » : pour montrer qu'une propriété (P) portant sur les entiers est vraie, on suppose qu'elle ne l'est pas, elle admet donc un contre-exemple et on choisit un tel contre-exemple minimal.

Il y a ensuite le caractère archimédien de $\mathbb{N}$:

3.2 Axiome. *Étant donnés deux entiers a et N de* $\mathbb{N}$*, avec* $a > 0$*, il existe un entier n tel que* $na \geq N$.

Cet axiome est la traduction d'un nombre incalculable de proverbes du genre : *les petits ruisseaux font les grandes rivières.*

2. La division euclidienne

3.3 Théorème. *Soient* $a, b \in \mathbb{N}$ *avec* $b > 0$*. Il existe des entiers q et r uniques tels que* $a = bq + r$ *et* $0 \leq r < b$.

Démonstration. Le cas $a = 0$ étant évident on peut supposer $a > 0$. En vertu de **3.2** il existe un entier $n > 0$ tel que $bn \geq a$. On considère alors le plus petit de ces entiers (il existe d'après **3.1**). On le note $q + 1$ et le couple q, $r = a - bq$ convient.

Pour l'unicité on suppose qu'on a $a = bq + r = bq' + r'$ avec, par exemple, $q < q'$. On écrit $b(q'-q) = r - r'$ et on a une contradiction avec les hypothèses sur r, r'.

3. Existence et unicité de la décomposition en produit de facteurs premiers

On suppose qu'on a défini les nombres premiers.

3.4 Théorème. *Soit a un entier positif. Alors a s'écrit, de manière unique, sous la forme* $a = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ *avec* $r \geq 0$*, les* p_i *premiers vérifiant* $p_1 < p_2 < \dots < p_r$ *et les* $\alpha_i > 0$.

3.5 *Remarques.* 1) Le cas $r = 0$ (produit vide) correspond à $a = 1$.
2) L'existence d'une décomposition en produit d'irréductibles est banale (elle est vraie dans tout anneau noetherien). En revanche l'unicité caractérise ce qu'on appelle les anneaux factoriels.

Démonstration. On utilise systématiquement le raisonnement par absurde et minimalité.
1) Existence. Sinon il y aurait un plus petit entier a ne s'écrivant pas sous la forme annoncée. En particulier, a n'est pas premier, donc s'écrit $a = bc$ avec $b, c < a$. Mais alors b et c ne sont plus des contre-exemples, donc sont produits de nombres premiers et a aussi, ce qui est absurde.
2) L'unicité est plus difficile. On commence par montrer le lemme d'Euclide[37]:

3.6 Lemme. *Soient a, b des entiers positifs. Si un nombre premier p divise le produit ab il divise a ou b.*

Démonstration. Le résultat est évident si a ou b est égal à 1. On peut donc supposer $a, b \geq 2$.
On raisonne par absurde et minimalité : on suppose que la propriété n'est pas vraie et on prend le plus petit ab qui soit un contre-exemple et, pour cet ab, le plus petit p qui mette en défaut le lemme. On a donc

[37] Pour une preuve via Bézout et Gauss, voir [1], pour une preuve plus proche de celle d'Euclide, voir le paragraphe suivant.

$ab = pc$. L'hypothèse de minimalité implique $a, b < p$ (sinon en les divisant par p on a un exemple plus petit) et on en déduit $c < a < p$, $c < b < p$ et $c > 1$ car p est premier. Mais, c admet un diviseur premier q (c'est l'existence de la décomposition), on a $c = qc'$ et, comme q est plus petit que p et divise ab, ce n'est plus un contre-exemple, donc il divise a par exemple. On a donc $a = qa'$ et $a'b = c'p$. Comme $a'b$ est plus petit que ab, ce n'est plus un contre-exemple, donc p divise a' ou b, donc a ou b.

3.7 Corollaire. *Si un nombre premier p divise un produit de nombres premiers $q_1 \dots q_r$ il est égal à l'un d'eux.*

Démonstration. Sinon, on prend un contre-exemple avec le nombre r de facteurs minimum et on applique le lemme d'Euclide pour avoir une contradiction.

Revenons à l'unicité. On prend encore un plus petit contre-exemple, $a = p_1^{\alpha_1} \dots p_r^{\alpha_r} = q_1^{\beta_1} \dots q_s^{\beta_s}$. Le corollaire du lemme d'Euclide montre que p_1 est égal à l'un des q_i. En divisant les deux membres par ce nombre on a un contre-exemple plus petit et c'est absurde.

4. Retour sur le lemme d'Euclide

Lors du colloque est apparu plusieurs fois un théorème qui semble avoir été communément admis dans l'enseignement au XIXème siècle et au début du XXème et qui porte sur l'écriture d'un rationnel sous forme de fraction irréductible. Ce résultat est notamment à la racine de preuves de l'irrationalité de $\sqrt{2}$ et d'autres qui ont été abordées dans les ateliers animés par Nathalie Chevalarias, par Fréderic Laurent et dans la conférence de Véronique Battie. J'essaie de faire le point sur ce thème, en revenant pour l'essentiel à Euclide, mais dit en langage moderne.

4.1. L'énoncé

Le résultat évoqué ci-dessus est le suivant :

***3.8* Théorème**. *Soient a, b, c, d des entiers positifs. Si l'on a $\frac{a}{b} = \frac{c}{d}$ et si a et b sont premiers entre eux, alors il existe e tel que $c = ae$ et $d = be$. En particulier, l'écriture d'un rationnel sous forme de fraction irréductible est unique.*

Ce théorème est essentiellement la réunion des propositions 20 et 21 du Livre VII d'Euclide.

4.2. Conséquences

Le théorème **3.8** a deux corollaires essentiels : le lemme d'Euclide (voir **3.6** ci-dessus) et l'irrationalité de $\sqrt{n}$ où n est un entier qui n'est pas un carré parfait.

Traitons **3.6**. On suppose que p divise ab. S'il divise a on a fini. Sinon, on écrit $ab = pc$ et on a $\frac{a}{b} = \frac{c}{d}$.
Comme p ne divise pas a, il est premier avec a, donc, par **3.8**, il divise b.
Montrons maintenant l'irrationalité de $\sqrt{n}$. Si $\sqrt{n}$ est rationnel, on a $\sqrt{n} = \frac{a}{b}$ avec a, b positifs et premiers entre eux, donc $n = \frac{a^2}{b^2}$ et a^2 et b^2 sont encore premiers entre eux (c'est le lemme d'Euclide !). On a donc $\frac{n}{1} = \frac{a^2}{b^2}$ et par **3.8**, on a $1 = b^2e$ et $n = a^2e$. Mais la première égalité impose $b = e = 1$ et on a donc $n = a^2$, contrairement à l'hypothèse.

4.3. La preuve de 3.8

La preuve d'Euclide n'est pas très facile à suivre à cause notamment de l'emploi de la notion : être des parties de *dont la définition n'est pas très claire et qui est donc délicate à utiliser. J'en donne une variante dont le ressort est la division euclidienne, qui est aussi à la base de tout le Livre VII.*

Une remarque d'abord. Si l'on a $\frac{a}{b} = \frac{c}{d}$ avec des entiers positifs et si $a \leq c$, alors on a $b \leq d$. En effet, sinon on a $b > d$ et $ad = bc$. Mais $a \leq c$ et $d < b$ implique $ad < bc$ et c'est une contradiction.

Le théorème repose alors sur le lemme suivant (proposition 20 d'Euclide) :

3.9 Lemme. *Soit r un rationnel. On suppose qu'on a deux écritures sous forme de fractions : $r = \frac{a}{b} = \frac{c}{d}$ où a, b, c, d sont des entiers positifs et où a est le plus petit entier vérifiant cette propriété. Alors il existe e tel que $c = ae$ et $d = be$.*

Démonstration. On divise c par a et d par b (voir **3.3**) : $c = ae + r$ avec $0 \leq r < a$ et $d = bf + s$ avec $0 \leq s < b$. On en déduit $ad = bc = abf + as = abe + br$ (*). Si r est nul on a $c = ae$ mais aussi $abf + as = abe$. En simplifiant par a on voit que b divise s, ce qui impose $s = 0$, puis $f = e$ et on a le résultat.
Si r est > 0 on a $as < ab$ et $br < ab$, de sorte que les deux expressions de (*) sont des divisions euclidiennes de $ad = bc$ par ab. En vertu de **3.3** on a unicité du reste, donc $as = br$, soit encore $\frac{a}{b} = \frac{r}{s}$ et comme on a $r < a$, cela contredit l'hypothèse de minimalité.
On peut alors finir de prouver **3.8**. Il suffit de montrer que la fraction irréductible a/b avec a, b premiers entre eux est celle qui a le plus petit a possible. Sinon on écrit $\frac{a}{b} = \frac{u}{v}$ avec u le plus petit possible (qu'une telle écriture existe vient de l'axiome du bon ordre **3.1**) et on suppose $u < a$. Mais, par le lemme **3.9**, on a alors $a = ue$ et $b = ve$ avec $e > 1$ et cela contredit le fait que a et b sont premiers entre eux.

5. Le principe des congruences

Le résultat le plus utile concerne la multiplication :

3.10 Lemme. *Si l'on a $x \equiv a \pmod n$ et $y \equiv b \pmod n$, alors on a $xy \equiv ab \pmod n$.*

Démonstration. Il s'agit de montrer que n divise $xy - ab$. C'est une vieille ruse, on écrit $xy - ab = x(y - b) + b(x - a)$.

6. Les carrés modulo *p*

Il s'agit de montrer, de manière élémentaire, que -1 est un carré modulo p (premier impair) si et seulement si p est congru à 1 modulo 4. On a vu que ce résultat intervient dans la recherche des nombres premiers de la forme $a^2 + 1$. Même si l'on peut ne pas parler de congruences au collège et au lycée, je le fais par commodité. Avec des élèves on parlera des restes dans la division euclidienne.

Dans tout ce qui suit p désigne un nombre premier impair.

3.11 Lemme. *Soit a un reste non nul modulo p. Les restes des ab, pour b = 1, …, p − 1 sont tous distincts.*

Démonstration. En effet, si $ab \equiv ab' \pmod p$, p divise $a(b - b')$ donc $b - b'$ par Euclide, donc $b = b'$.

3.12 Corollaire. *Soit a un reste non nul modulo p. Il existe un unique reste b tel que $ab \equiv 1 \pmod p$. On parle de l'inverse de a modulo p.*

Démonstration. Comme les restes des ab, pour $b = 1 \ldots p-1$, parcourent les restes non nuls et sont tous distincts, ils les atteignent tous[38].

3.13 Corollaire. *Le reste $p-1$ (ou -1) modulo p est un carré si et seulement si $p \equiv 1 \pmod 4$.*

Démonstration. Posons $p-1 = 2k$. On regarde les $p-1$ restes de la division par p. On note d'abord que les restes de a^2 et de $(p-a)^2$ sont égaux (car $(p-a)^2 = p^2 - 2ap + a^2 \equiv a^2 \pmod p$). On a donc k restes des carrés parmi lesquels évidemment 1. On note ensuite que si $ab \equiv 1$ on a aussi $a^2b^2 \equiv 1$ par un calcul similaire. Si c est le carré de a et si d est l'inverse de c, soit b l'inverse de a. Comme on a $a^2 \equiv c$ et $a^2b^2 \equiv 1$ et comme d est unique, on a $d \equiv b^2$, autrement dit, d est aussi un carré. De plus, si $c \not\equiv 1$, c et d sont distincts. En effet, sinon on aurait $c^2 \equiv 1$, ce qui signifie que p divise $c^2 - 1 = (c-1)(c+1)$ et on conclut par le lemme d'Euclide. (Bien entendu, si p n'est pas premier c'est faux, par exemple, modulo 8 on a $(\pm 1)^2 \equiv (\pm 3)^2 \equiv 1$). Les carrés distincts de ± 1 se regroupent donc deux par deux (un carré et son inverse) et il y en donc un nombre pair $2m$. Pour faire k il ne reste que 1 et éventuellement -1 qui est un carré si et seulement si k est pair, donc $p \equiv 1 \pmod 4$.

7. Le petit théorème de Fermat

Il y a beaucoup de preuves de ce théorème (en utilisant la théorie des groupes, les coefficients binomiaux, etc.) En voici une très simple.

3.14 Théorème. *Soit p un nombre premier. On a les congruences $a^p \equiv a \pmod p$ pour tout a et $a^{p-1} \equiv 1 \pmod p$ si a n'est pas multiple de p.*

Démonstration. Il suffit de montrer le second point. Soit a un entier compris entre 1 et $p-1$. On considère le produit $N := \prod_{b=1}^{p-1} b$. On a $a^{p-1}N = \prod_{b=1}^{p-1} ab$. Mais on a vu que les congruences des ab sont toutes distinctes (cf. **3.11**), donc qu'elles parcourent les entiers de 1 à $p-1$, de sorte qu'on a $a^{p-1} N \equiv N \pmod p$. Comme p ne divise pas N (par le lemme d'Euclide), il divise $a^{p-1} - 1$ (par le même argument).

8. Solution d'un exercice

3.15 Proposition. *Soit n un entier > 2. Alors l'un des nombres $n! + 1$ et $n! + n + 1$ est composé.*

Démonstration. Si $n+1$ n'est pas premier il admet un diviseur premier $p \leq n$ et p divise $n!$ et $n+1$ donc $n! + n + 1$ qui est donc composé. Si $p := n+1$ est premier on sait qu'on a $(p-1)! \equiv -1 \pmod p$ (c'est le théorème de Wilson, que l'on prouve en regroupant les classes $\bar{a}$ et $\bar{a}^{-1}$ de $\mathbb{Z}/p\mathbb{Z}$). Autrement dit, $p = n+1$ divise $n!+1$ et, comme n est plus grand que 2, c'est un diviseur strict et on a gagné.

[38] Quand on est savant on dit qu'injectif implique surjectif, mais on n'a pas attendu d'avoir ces mots pour comprendre ça.

9. Quelques messages à décrypter

9.1. Deux messages par substitution

EYVOZMTVKGPPGLAGQGXOTAPQMBMPMBGZYGBPMPJSVGKMAL
TYEVGEYBCAFYGTGEZGOAPGEPOBPMPFGEMYTVGETOYGEFAQ
YBGAEGEXOTPYGEVGELMFGPEQOFRGTQGEBAOBKOYGBPGPOB
YQOYGBPFGEBMYTGEXTMRMBVGATEVGKGXOSEMTYCYBOF

NGWBLOINOAPMPOWBUWQMBBQDMQPOIIGWVVLOIWBA
OVMQPOAOPMQPHMTGBHWZOTLGWQIIOSOZPHOPGQPIH
OAJOSQZOOIHOBWOIHONLMAOIHOVLOAJOIHOALGAJOBI

9.2. Deux messages codés par Vigenère

Le code de Vigenère (1523-1596) permet de contrer l'analyse de fréquence. Le principe est le suivant : on choisit un mot clé, par exemple le mot CODE, qui correspond aux nombres 3, 15, 4, 5. On décale la première lettre du message de 3 crans, la deuxième de 15, la troisième de 4, la quatrième de 5, puis on recommence, la cinquième de 3, etc. Si on dépasse Z on continue avec A. Avantage : la même lettre n'est pas forcément codée par le même caractère, donc l'analyse de fréquence ne marche plus.

Un exemple, le message à coder :

RENDEZ-VOUS EN PRISON VOUS NE PASSEZ PAS PAR LA CASE DE DEPART VOUS NE TOUCHEZ PAS VINGT MILLE EUROS

Le message codé :

UTRIHOZTXHISSGMXRCZT XHRJSPW XHOTFVEEWOPG FVTHJGTTFUI ZTXHRJWDYH KTDUDHZNQVXRLAPJHJVTV

Pour décrypter Vigenère on repère des groupements fréquents :

UTRIHOZTXHISSGMXRCZTXHRJSPW XHOTFVEEWOPG FVTHJGTTFUI ZTXHRJWDYH KTDUDHZNQVXRLAPJHJVTV

et on en déduit la longueur du mot clé (ou au moins un multiple de cette longueur).

Voir http://www.dcode.fr/chiffre-vigenere

Un exemple facile codé par Vigenère :

npw fpgqoiwcw npw rwyu aitqstxepew, npw opmnwiwcw, ep wqyx npw tzfqew.
kww elpefpgyx vzyvpw npw ezqdtrctwqyw, kww pp wg qevtkwprv ueolmu.
dm xzyu lvttzgk e fpgtjtvpv ep qgdwcri, xzyu aswcvgk zqfw opwwcit lyz csdzxu.
dmpzr, xzyu oixpd gygqci vcexlmnwit fr rpy. ezytlkg.

Un exemple plus difficile :

zvtolgvfscgkdaavfkebidgnbscsmgslppyfksgcstsravruuldvfscsewtpsjabgsehosfmmqsstwu
vaveeoizkolhcwsnzlkdgtwacgzvkaacelelhvjelhfmtcollrcqygscbfftnczftaclluksuwnbsjarcfgd
uqelalqsegnrseiumwzdncgkhaqjisiqsdtlypcwqsskguqgvlrmagwnrarasnzllorqvdarsdgiebv
iuczrhuggjsnasuwbgsebuesiwtbwjlilulwrjsmjagrrneazvxaslhmicgkhrmdiwmcbkueoiffnm
adwlcpffscbjgujoisiqcewsrbrlupscdekseleeocwelhfmsjsjzokavkerozfsgelwlyrznepgzleb
segsmdzfimbjfetwvftnojveashmejsjmnqgfftnzlkrywjgnlosdeqelwlcgrmtpsjeaggjwujsdwn
rrvueoivfosgtgnbizkolgegsnsekecggsrbwmwrqsjnogsjwtlstgnqwuwrmbjhaqzvkmcavkcfc
jwsaoiuelsjlpygrkscnusvmwideqdiatzceeaggcwppweuinocwsrrvdandcaqssiticbcwsnzlkg
poeveqodwsqcelcydrtlcguwsnzlkgpoevstwtwsyijkizwvfqssuwsnzlkgpoeveqjvjtsgvlccioiu
gbveapqywnrelwfmfkdelhveelhgwutselatoeueppvsuaclhdyjrftyuvkijgjmitseltmiagupgcwd
pczlcfsdanoivfedcelccioiugqfmrcbkwtoizkelscgiebvft

9.3. *Un exemple de codage RSA*

Ma signature encodée en ASCII et cryptée c avec pq et e :

$$pq = 3182025935200771015207983046670052747435834209343862515620620481366 83$$
$$e = 94321654323578865325687908765434567779 99$$
$$c = 16710022994275830171960951435588588665707246512802868028703054827 8619$$

Pour des précisions sur le code ASCII on peut consulter :
https://fr.wikipedia.org/wiki/American_Standard_Code_for_Information_Interchange

IV - RÉFÉRENCES

[1] Perrin D. *Mathématiques d'école*, Cassini, 2011.

[2] Perrin D. *Arithmétique et cryptographie*

https://www.imo.universite-paris-saclay.fr/~daniel.perrin/interdisciplines/Cours6cryptographie.pdf

email : *daniel.perrin@universite-paris-saclay.fr*