LES CONTACTS PREMIERS

HENRI COHEN

1. Autour des Nombres Premiers

1.1. **L'algorithme d'Euclide.** Avant d'aborder les nombres premiers proprements dits, il nous faut parler de nombres **premiers entre eux**, ce qui est différent (et valable uniquement pour plusieurs nombres).

On dit que deux entiers a et b sont premiers entre eux s'ils n'ont pas de diviseurs en commun, autre bien sûr que 1, qui divise tout le monde.

Par exemple 16 et 21 sont premiers entre eux (mais ne sont pas premiers, voir plus bas), par contre 15 et 21 ne le sont pas puisqu'ils sont tous deux divisibles par 3.

Le théorème fondamental est le suivant:

Sia et b sont premiers entre eux il existe des entiers u et v (éventuellement négatifs) tels que

$$au + bv = 1 \ .$$

Noter que ce résultat n'est pas complètement évident: essayez de le montrer sans tricher.

De plus, Euclide donne une méthode pour calculer u et v, **l'algorithme d'Euclide**, très certainement le plus ancien algorithme de tous les temps.

En France, le théorème ci-dessus s'appelle le théorème de Bezout, mais partout ailleurs on l'appelle théorème d'Euclide étendu. (Le "vrai" théorème de Bezout est un théorème beaucoup plus difficile sur les intersections de courbes algébriques.)

Pour notre exemple $a = 16$, $b = 21$, on peut prendre $u = 4$ et $v = -3$: $4\times16+(-3)\times21 = 1$, mais il y a une infinité d'autres possibilités: trouvez en d'autres, et même pouvez-vous donner une formule les donnant toutes ?

1.2. **Definitions et Théorème Fondamental. Première définition:** un nombre premier est un entier strictement plus grand que 1 et divisible seulement par 1 et par lui-même (1 n'est PAS premier, c'est ce qu'on appelle une *unité*).

Exemples: 3, 11, 89 sont premiers, mais $15 = 3 \times 5$ ou $91 = 7 \times 13$ ne le sont pas.

Les plus petits sont:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41,...

Le Théorème Fondamental: Tout entier est produit de nombres premiers de manière **unique** (en les mettant par ordre croissant).

Exemple: $12 = 2 \times 2 \times 3$, ce qu'on préfère écrire $12 = 2^2 \times 3$, ou $37901 = 151 \times 251$.

Les nombres premiers forment donc les **briques de base** des entiers pour la multiplication.

Deuxième définition: un nombre premier est un entier strictement plus grand que 1 ayant la propriété suivante: s'il divise un produit, il divise l'un des facteurs. Exemples:

7 divise 13×28, et effectivement 7 divise 28.

Par contre 15 divise $30 = 5 \times 6$, et pourtant 15 ne divise ni 5 ni 6, donc 15 n'est pas premier (ce qu'on savait déjà!).

Exercice: Montrez que cette deuxième définition est bien celle d'un nombre premier (ce n'est pas tout à fait évident: utilisez par exemple le théorème d'Euclide étendu ci-dessus).

La deuxième définition est souvent plus utile que la première.

Il y a tout de même un rapport entre nombres premiers et nombres premiers entre eux: si p est un nombre premier et a un autre entier, alors par définition d'un premier, si a et p ont un diviseur en commun cela ne peut être que 1 ou p. Donc, soit a est divisible par p, soit a et p n'ont pas d'autres diviseur commun que 1, donc sont **premiers entre eux**. Nous utiliserons cette propriété ci-dessous.

1.3. **Irrégularités et Régularités.** Théorème datant de l'antiquité: il y a une **infinité** de nombres premiers (pas difficile). Nombreuses questions: comment sont-ils distribués, combien y en a-t-il (à peu près), etc...

Les nombres premiers sont répartis de manière assez **irrégulière**: par exemple entre 100 et 110 il y en a 4 (le maximum possible vu qu'on doit enlever les pairs et les multiples de 5): 101, 103, 107, 109. Par contre, entre 115 et 125 il n'y en a aucun.

Pourtant en **moyenne** ils manifestent une certaine régularité: par exemple, regardons le tableau suivant: parmi les entiers jusqu'à 10^k, il y en a $1/f(k)$ qui sont premiers (par exemple il y a 25 premiers jusqu'à $100 = 10^2$, donc $f(2) = 4$):

$$\begin{aligned}
k = 2 : &\quad f(k) = 4.00 \\
k = 3 : &\quad f(k) = 5.95 \\
k = 4 : &\quad f(k) = 8.14 \\
k = 5 : &\quad f(k) = 10.42 \\
k = 6 : &\quad f(k) = 12.73 \\
k = 7 : &\quad f(k) = 15.05 \\
k = 8 : &\quad f(k) = 17.36 \\
k = 9 : &\quad f(k) = 19.67 \ .
\end{aligned}$$

Il y a donc proportionnellement de moins en moins de nombres premiers parmi les entiers, ce qui n'est pas du tout étonnant vu qu'on leur demande de ne **pas** être divisibles par de plus en plus de nombres.

On constate que la progression de $f(k)$ est très régulière: à partir de $k = 4$ $f(k)$ augmente d'environ 2.3 quand k augmente de 1.

Pour ceux qui connaissent la fonction logarithme, ceci s'exprime mathématiquement en disant que le nombre de premiers jusqu'à N (ici $N = 10^k$) est **de l'ordre de** $N/\log(N)$ ($\log$ est le logarithm néperien), et 2.3 est approximativement $\log(10)$.

Celà a été **conjecturé** par Gauss vers 1800, et est un problème assez difficile. Il a fallu pratiquement un siècle et les travaux géniaux de B. Riemann en 1853, pour que finalement en 1898, deux mathématiciens J. Hadamard et De La Vallée Poussin prouvent indépendamment la conjecture de Gauss, qu'on appelle maintenant le **théorème des nombres premiers**.

Le problème de comptage des premiers est pourtant loin de s'arrêter là. Pour éviter d'utiliser la fonction logarithme, qui n'est pas connue de tout le monde, posons le problème différemment.

D'après le *théorème fondamental* tout entier est, de manière unique, produit de nombres premiers. Parmi tous les entiers jusqu'à N, mettons d'un coté ceux qui sont produit d'un nombre **pair** de nombres premiers et de l'autre ceux qui sont produit d'un nombre **impair** (on peut soit compter les répétitions, soit ne pas les compter, ça n'a pas d'importance si on compte de la même manière des deux cotés).

Par exemple, si $N = 20$, les entiers produits d'un nombre pair (en comptant les répétitions) sont 1, 4, 6, 9, 10, 14, 15, 16, et ceux qui sont produits d'un nombre impair sont 2, 3, 5, 7, 8, 11, 12, 13, 17, 18, 19, 20.

Il est raisonnable de penser que les entiers sont distribués équitablement entre les deux types de nombres, et c'est effectivement vrai. Ce n'est pourtant pas si facile que ça à montrer puisque c'est en fait équivalent au théorème des nombres premiers.

Mais on peut se poser une question plus précise: appellons $h(N)$ la différence entre le nombre d'entiers jusquà N produit d'un nombre pair de premiers, et ceux produit d'un nombre impair. Effectivement $h(N)$ est "négligeable" par rapport à N en un sens mathématique précis. Mais quelle est la **taille** de $h(N)$?

La célèbre **Conjecture de Riemann** (ou **Hypothèse de Riemann**) dit que $h(N)$ n'est pas beaucoup plus grand que $\sqrt{N}$. Ceci est certainement la plus célèbre et la plus importante de toutes les questions mathématiques actuelles, a un nombre incalculable de conséquences (dont un prix de 1 million de dollars pour sa résolution), et pourtant apparemment nous ne sommes pas plus près de sa solution qu'il y a un siècle.

On peut résumer la discussion précédente en termes "probabilistes": les nombres premiers sont répartis de manière très irrégulière à petite échelle; à grande échelle ils sont répartis régulièrement, et l'hypothèse de Riemann affirme que les fluctuations autour de leur moyenne est aussi petite que possible, ce qu'on est loin de savoir démontrer.

Autre résultat de "régularité" beaucoup plus facile mais surprenant, mais toutefois qui nécessite une compréhension de la notion de **produit infini**: considèrons la quantité:

$$P = \frac{1}{2} \times \frac{3}{2} \times \frac{2}{3} \times \frac{4}{3} \times \frac{4}{5} \times \frac{6}{5} \times \frac{6}{7} \times \frac{8}{7} \times \frac{10}{11} \times \frac{12}{11} \times \dots ,$$

où les facteurs successifs sont de la forme $(p-1)/p$ et $(p+1)/p$ pour les nombres premiers p par ordre croissant.

Vu la répartition irrégulière des nombres premiers, il n'y a aucune raison de penser que P ait une valeur particulière. Et pourtant il est relativement facile de montrer que

$$P = \frac{6}{\pi^2}$$

(où $\pi = 3.14159...$ comme d'habitude). Dans un contexte légèrement différent, ceci est l'un des plus beaux et importants résultats d'analyse du 18ième siècle, conjecturé par J. Bernoulli et démontré par L. Euler, sans conteste le plus grand mathématicien du 18ième.

2. Autour du Théorème de Fermat

2.1. **Fermat.** Pierre de Fermat (17ième siècle) a été l'un des grands physiciens et mathématiciens de son siècle. Son célèbre "grand théorème" (qu'il n'avait certainement pas démontré) affirme que si $n \geq 3$ une puissance n-ième ne peut pas être (non trivialement) une somme de deux puissances n-ièmes, contrairement à ce qui se passe pour $n = 2$ ($3^2 + 4^2 = 5^2$), et il a fallu les efforts de très nombreux mathématiciens, culminant en 1995, donc 350 ans après son énoncé, avec la démonstration du théorème par A. Wiles, aidé de R. Taylor.

Mais ce n'est pas de ce théorème dont je veux parler mais d'un théorème beaucoup plus simple, qu'on appellera ici simplement le théorème de Fermat, et qui est intimement lié aux nombres premiers.

2.2. **Le Théorème de Fermat: Énoncé et Démonstration.** Ce théorème dit la chose suivante: soit p un **nombre premier**, et a un entier non divisible par p. Alors le reste de la division par p de a^{p-1} (a à la puissance $p-1$, c'est-à-dire multiplié par lui-même $p-1$ fois) est toujours égal à 1 (à quoi est-il égal si a est divisible par p ?).

Ce théorème est très facile à montrer. Je le démontre en illustrant par un exemple.

Prenons $p = 11$ et $a = 5$, et calculons les restes successifs de la division par p de $1 \times a$, $2 \times a$, etc..., jusqu'à $10 \times a$ ($10 = p - 1$): on trouve (faites le!):

$$5,\ 10,\ 4,\ 9,\ 3,\ 8,\ 2,\ 7,\ 1,\ 6.$$

Comme on le voit, il s'agit à nouveau des entiers de 1 à 10 dans le désordre: c'est très facile de montrer que ce sera le cas pour tout p premier et a non divisible par p.

Faisons alors le **produit** de ces quantités. D'une part, de la manière dont cela a été construit, le reste de la division par p du produit sera égal à celui de

$$(1 \times a) \times (2 \times a) \times \cdots \times (10 \times a) = 10! \times a^{10} = (p-1)!a^{(p-1)} ,$$

où $n!$ (factorielle n) signifie $n! = 1 \times 2 \times \cdots \times n$.

D'autre part, puisqu'on a obtenu les entiers dans le désordre, c'est aussi le reste de la division par p de

$$5 \times 10 \times 4 \times \cdots \times 6 = 10! = (p-1)! .$$

Il en résulte que p doit diviser la différence, égale à $(p-1)!(a^{p-1} - 1)$, donc d'après la deuxième définition des nombres premiers, il doit diviser l'un des facteurs, et comme p ne divise évidemment pas $1, 2, \ldots, p-1$, il en résulte qu'il divise $a^{p-1} - 1$, ce qui est exactement le théorème de Fermat.

Remarque. On utilise la notation $a \equiv b \pmod{p}$, appelée **congruence** pour dire que $a - b$ est divisible par p, ou encore que les restes de la division de a et b par p sont égaux. C'est une notation très pratique. Par exemple, le théorème de Fermat ci-dessus dit que $a^{p-1} \equiv 1 \pmod{p}$. Pour éviter l'utilisation de cette notion, j'utiliserai la formulation plus lourde consistant à dire que les restes de division par p sont égaux, mais il est beaucoup plus élégant de retranscrire en termes de congruences. D'ailleurs, dans la démonstration ci-dessus, nous avons utilisé implicitement le fait que si $a \equiv b \pmod{p}$ et $c \equiv d \pmod{p}$ alres $ac \equiv bd \pmod{p}$: montrez le!

2.3. **Calculabilité.** Avant de passer aux applications, il est crucial de se poser la question suivante: le théorème de Fermat donne une condition *nécessaire* pour que p soit premier, mais est-ce que cette condition est facilement vérifiable numériquement ?

De fait, a^{p-1} devient rapidement un très grand nombre, donc comment vérifie-t-on que le reste de sa division avec p est égal à 1 ?

Il y a deux réponses, complémentaires, à cette question.

Tout d'abord, en supposant qu'on calcule naivement a^{p-1} comme $a \times a \times \cdots$ ($p-1$ fois), ce qu'on ne fera **pas**, voir ci-dessous, à chaque fois qu'on fait un produit on prend le reste de la division par p. Donc nous n'aurons jamais de nombres plus grands que p^2, ce qui est raisonnable.

Par exemple, bien que $2^{16} = 65536$ ait 5 chiffres, on calcule $2 \times 2 \times 2 \times 2 \times 2 = 32$, qu'on divise par $p = 17$, ce qui donne 15, puis (par exemple) encore trois fois ce même produit (ce qui fait 15 facteurs 2 en tout), ce qui donne $15 \times 15 \times 15$, ce qu'on calcule comme $15 \times 15 = 225$, reste 4, puis $4 \times 15 = 60$, reste 9. Enfin, comme il faut 16 facteurs 2 et pas 15, on remultiplie encore par 2, ce qui fait 18, reste 1 comme prévu (ce n'est pas grave si vous n'avez pas suivi, tout d'abord il vaut mieux que vous fassiez le calcul vous-même, et ensuite nous allons voir une bien meilleure méthode).

Cet exemple nous conduit à découvrir la deuxième réponse: au lieu de calculer un produit de 16 facteurs comme ci-dessus, on va plutôt calculer $a = 2^2$, puis $b = a^2 = 2^4$, puis $c = b^2 = 2^8$, puis finalement $d = c^2 = 2^{16}$, soit en tout 3 multiplications au lieu de 15 (même si notre astuce ci-dessus en a réduit le nombre). On trouve, toujours en prenant le reste de la division par 17:

$a = 4$, $b = 16$, $c = 256$, donc $c = 1$, $d = 1$, facile!

Ici, nous sommes dans le cas le plus favorable où $p-1$ est une puissance de 2. Mais même dans le cas général une méthode semblable est applicable en utilisant l'écriture en système **binaire** de $p-1$. Léxercice ci-dessous explique ceci:

Exercice: en écrivant $42 = 32 + 8 + 2$ (écriture en base 2 de 42), montrer qu'on peut calculer le reste de la division de a^{42} par 43 en n'utilisant que 7 multiplications (et restes de division), au lieu de 41 par la méthode naive.

3. Applications du Théorème de Fermat

Le théorème de Fermat a de très nombreuses applications en théorie des nombres et en cryptographie. En voici quelques unes.

3.1. **Première Application: Développement Décimaux.** Cette première application n'est pas très utile mais nous permet de démarrer doucement.

Regardons le développement décimal de la fraction 1/7: on a

$$1/7 = 0.142857142857142857142857142857142857\cdots$$

On constate que le développement est **périodique**, ce qui est le cas du développement décimal de **toute** fraction (ce n'est pas difficile à montrer, justement en utilisant le théorème de Fermat!), donc rien de très étonnant. Notez toutefois que la **période** est ici égale à $6 = 7 - 1$, et c'est en effet Fermat: en exercice, en utilisant le théorème de Fermat, montrer

que si p est un nombre premier différent de 2 et 5, la période du développement décimal de $1/p$ est un diviseur de $p-1$ (elle peut être plus petite que $p-1$: donner un exemple).

Mais il y a plus: regardez la table de multiplication suivante:

$$\begin{aligned}
1 \times 142857 &= 142857\\
2 \times 142857 &= 285714\\
3 \times 142857 &= 428571\\
4 \times 142857 &= 571428\\
5 \times 142857 &= 714285\\
6 \times 142857 &= 857142\\
7 \times 142857 &= 999999\ .
\end{aligned}$$

A part la dernière ligne, également intéressante, les résultats s'obtiennent tous en faisant une permutation circulaire des chiffres.

- Expliquez ce phénomène.
- Montrer qu'il se produit aussi par exemple pour $p = 17$.

3.2. **Deuxième Application: les Nombres de Mersenne.** Depuis le moyen-âge on s'est aperçu que l'on pouvait **construire** de grands nombres premiers par la formule suivante:

$$M_n = 2^n - 1\ ,$$

et M_n s'appelle le n-ième **nombre de Mersenne** (moine qui vivait au début du 17ème siècle). Il est facile de voir que pour que M_n soit premier il faut (condition **nécessaire**, mais pas suffisante comme on va le voir) que n soit lui-même premier: en effet, si d est un diviseur de n autre que 1 et n (qui existent si n n'est pas premier), alors on montre facilement que que $M_d = 2^d - 1$ est un diviseur de M_n autre que 1 et M_n (montrez-le!).

Donc on se restreint à $n = p$ premier. On trouve $M_2 = 3$, premier, $M_3 = 7$, premier, $M_5 = 31$, premier, $M_7 = 127$, premier, mais $M_{11} = 2047 = 23 \times 89$ n'est **pas** un nombre premier. Toutefois on ne se décourage pas, et $M_{13} = 8191$ est à nouveau premier.

En 2013 on connait 48 nombres de Mersenne premiers, le plus grand correspond à $n = 5788561$, et a plus de 17 millions de chiffres décimaux (c'est le plus grand nombre premier connu explicitement).

Mais là n'est pas notre propos. Revenons à M_{11}: pour s'apercevoir qu'il n'est pas premier, on peut bien sûr diviser par 2, 3, etc..., jusqu'à ce qu'on s'apercoive que 23 le divise, ce qui fait en tout 9 essais. Mais grâce au théorème de Fermat, il suffit d'en faire un seul!: le résultat est le suivant.

Théorème. Soit p un nombre premier, $M_p = 2^p - 1$ le nombre de Mersenne correspondant, et q un diviseur premier de M_p. Alors le reste de division de q par $2p$ est égal à 1.

Par exemple, dans notre cas $p = 11$, le reste de la division par 22 doit être égal à 1, donc le tout premier diviseur à essayer est 23 (bien sûr ce n'est pas toujours aussi facile).

Nous allons montrer ce théorème. Tout d'abord, puisque q est premier, et évidemment non divisible par 2 (M_p est impair!), d'après Fermat le reste de la division de 2^{q-1} par q vaut

1. D'un autre coté, comme q divise $M_p = 2^p - 1$, le reste de la division de 2^p par q est *aussi* égal à 1.

Nous faisons maintenant un raisonnement **par l'absurde**. Nous avons vu dans la définition des nombres premiers que soit $q-1$ est divisible par p, soit $q-1$ et p sont premiers entre eux. Supposons donc que nous sommes dans ce dernier cas. D'après le théorème d'Euclide étendu (voir ci-dessus), il existe donc des entiers u et v tels que $u(q-1) + vp = 1$, d'où:

$$(2^{q-1})^u \times (2^p)^v = 2 \, .$$

Comme le reste de la division par q de 2^{q-1} et de 2^p est égal à 1, il en va de même du reste de la division de 2 par q, ce qui est clairement impossible vu que $q \geq 3$, donc que le reste de la division de 2 par q est 2.

Cette contradiction montre que p doit diviser $q-1$, et comme $q-1$ est pair, c'est même $2p$ qui doit diviser $q-1$.

Anecdote personelle: bien sûr tous les calculs se font sur ordinateur. Quand j'étais au lycée, le plus petit Mersenne dont on savait (par des méthodes dont je parlerai plus bas) qu'il n'était pas premier, mais dont on ne connaissait pourtant aucun facteur, était $M_{101} = 2^{101} - 1$, un nombre de 31 chiffres décimaux. Grâce au théorème ci-dessus, on sait que pour trouver un diviseur q il suffit d'essayer ceux dont le reste de la division par 202 est 1. Autant vous dire que j'ai essayé à la main sans succès!

(En quelques millisecondes, sans même utiliser ce théorème, un ordinateur trouve le facteur $7432339208719 = 36793758459 \times 202 + 1$, je pouvais toujours essayer!).

Pour ceux qui aiment vraiment ce genre d'exercices, noter que l'on peut encore diviser par 2 le temps de recherche d'un facteur: on a le théorème supplémentaire suivant.

Sous les mêmes hypothèses, q nombre premier divisant $2^p - 1$. Alors le reste de la division de q par 8 est égal à 1 ou à 7 (jamais à 3 ou à 5, rappelons que q est impair).

Montrer cela est un peu plus difficile: on remarque tout d'abord que si $x = 2^{(p+1)/2}$ on a $x^2 = 2^{p+1} = 2 \times 2^p$, donc que le reste de la division de x^2 par q est égal à 2 (puisque celui de 2^p est égal à 1). Maintenant un résultat pas complètement évident de Gauss (1798) dit que le reste de la division d'un carré par un nombre premier q ne peut être égal à 2 que si q est comme ci-dessus.

3.3. **Troisième Application: les Tests de Non Primalité.** Nous souhaiterions déterminer si un entier donné p est premier ou non. Comme nous le verrons dans un paragraphe ultérieur, une première idée est naturellement de diviser p par 2, 3, etc... pour vérifier si p est ou non divisible par un "petit" entier. Si ce n'est pas le cas, on peut commencer à penser que p pourrait être premier, et c'est là où le théorème de Fermat nous vient en aide; c'est probablement son application la plus importante, en particulier à cause de son lien avec la cryptographie.

Choisissons par exemple comme base $a = 2$. Le théorème de Fermat nous dit que si p est un nombre premier au moins égal à 3 le reste de la division de 2^{p-1} par p est égal à 1. C'est bien, mais se peut-il que ceci arrive également quand p n'est **pas** un nombre premier ? Quelques essais à la main ne trouvent pas de contre-exemples. Et pourtant il y en a: regardons $p = 341 = 11 \times 31$, donc pas un nombre premier. On a $p - 1 = 340$. Or d'après Fermat justement, on sait que $2^{10} - 1$ est divisible par 11, et en fait on vérifie que $2^{10} - 1 = 3 \times 11 \times 31$, donc il est même divisible par $341 = 11 \times 31$. Il en résulte que le reste

de la division par 341 de $2^{p-1} = 2^{340} = (2^{10})^{34}$ est encore égal à 1, donc 341, qui n'est pas premier, se comporte *comme* un nombre premier vis-à-vis du théorème de Fermat: on dit que c'est un nombre **pseudo-premier** à base 2.

Ces nombres sont-ils rares ou non ? Une expérimentation numérique sur ordinateur montre que les seuls nombres pseudo-premiers à base 2 jusqu'à 1000 sont les trois nombres 341, 561 et 645, alors qu'il y a 168 nombres premiers, donc 2% "d'erreur". Jusqu'à 10^6 il y a 244 nombres pseudo-premiers à base 2 pour 78498 nombres premiers, donc 0.3%. Sachant que le reste de la division par p de a^{p-1} peut se calculer rapidement (voir ci-dessus), ceci donne une méthode très rapide pour vérifier qu'un nombre est "presque" premier, avec une probabilité d'erreur assez faible: c'est ce qu'on appelle un test de **non-primalité**: on calcule le reste de a^{p-1}: si ce n'est pas égal à 1, p n'est **pas** un nombre premier. C'est comme ceci qu'on peut vérifier très facilement que (par exemple) $2^{101} - 1$ n'est pas premier. Et pourtant, cela ne nous donne **pas la moindre** indication d'un diviseur différent de lui-même et de 1, situation assez remarquable!

On peut améliorer la situation, c'est-à-dire faire que la probabilité d'erreur soit plus faible. Par exemple on peut demander que p soit un pseudo-premier à la fois à base 2, et à base 3. Il n'y a alors plus que 66 pseudo-premiers jusqu'à 10^6 au lieu de 244. Mais ce n'est toujours pas suffisant.

Pour faire vraiment mieux, il faut une autre idée, basée sur la deuxième définition des nombres premiers: d'après celle-ci, si p est premier et divise $x^2 - 1 = (x-1) \times (x+1)$ alors p divise $x-1$ ou $x+1$. En d'autres termes, si le reste de la division de x^2 par p vaut 1, celui de la division de x par p doit valoir 1 ou $p-1$.

Regardons par exemple le cas de $p = 341$ qui n'est pas premier, mais qui est pseudo-premier à base 2. Nous avons vu que si $x = 2^5 = 32$, on a $x^2 = 2^{10} = 1024 = 3 \times 341 + 1$, donc le reste de la division de x^2 par 341 est bien égal à 1. Et bien sûr celui de la division de $x = 32$ lui-même est égal à 32, qui n'est ni 1 ni $p - 1 = 340$, ce qui élimine la possibilité que 341 soit premier.

Ceci conduit au test de non-primalité le plus utile, qui s'appelle le **test de Miller–Rabin**: on procède comme suit. On calcule le reste de 2^{p-1}. Si ce n'est pas 1, p n'est pas premier. Si c'est 1, on regarde $2^{(p-1)/2}$, dont le reste doit être 1 ou $p-1$. Si ce n'est pas le cas, p n'est pas premier. Si le reste est $p-1$, on dit que p a passé le test (ce qui ne signifie bien sûr pas que p est premier). Si le reste est 1, on peut peut-être recommencer: si $(p-1)/2$ est pair (ce qui arrive une fois sur 2), on calcule alors $2^{(p-1)/4}$, et à nouveau son reste doit être 1 ou $p-1$, et on continue de la même manière. Si on ne peut plus recommencer (par exemple à la première étape quand $(p-1)/2$ est impair), on dit aussi que p a passé le test.

Un p non premier qui "passe le test" s'appelle un pseudo-premier **fort** à base 2. Bien sûr rien ne nous oblige à utiliser la base 2: on peut en utiliser d'autres. Et là il y a un **théorème**: si on utilise k bases choisies au hasard (ou bien simplement les bases $a = 2$, 3,...), et que p passe tous les tests, il y a une probabilité inférieure à $1/4^k$ que p ne soit pas premier. Donc si $k = 20$ par exemple, la probabilité est infime.

Ce test (et certaines améliorations) est très largement utilisé, mais j'insiste sur le fait que c'est un test de NON primalité qui élimine pratiquement tous les nombres non premiers, mais il ne prouvera JAMAIS qu'un nombre EST effectivement premier.

4. Conclusion: Tests de Primalité

Nous avons vu que le théorème de Fermat et ses raffinements permettent de fabriquer des tests de **nonprimalité** très efficaces. On peut aussi l'utiliser pour obtenir des tests de **primalité**, mais il faut se fatiguer un peu plus.

On a par exemple le théorème suivant, dû à Pocklington et Lehmer (vers 1930), dont la démonstration n'est pas très difficile:

Théorème. Soit $p \geq 2$ un entier. Supposons que pour tout diviseur premier q de $p-1$ on puisse trouver un entier a_q tel que le reste de la division de a_q^{p-1} par p soit égal à 1 (c'est nécessaire sinon p n'est pas premier), et tel que $a_q^{(p-1)/q} - 1$ et p soient **premiers entre eux**, ce qui se teste aisément grâce à l'algorithme d'Euclide. Alors p est premier.

Jusqu'en 1978, ce test (et des tests similaires et améliorés) était le seul disponible pour **prouver** qu'un nombre de grande taille est premier (pour les petits nombres il suffit de faire un nombre suffisant de divisions). Toutefois il possède un grave défaut: il faut connaître tous les diviseurs premiers q de $p-1$, c'est à dire **factoriser** $p-1$. Or comme nous le verrons ci-dessous, ceci est beaucoup plus difficile, donc souvent le test est inapplicable.

Un tournant s'est produit à partir de 1978 jusqu'en 1986 avec les travaux de Adleman, Pomerance, Rumely, moi-même, Lenstra, puis Atkin et Morain, ce qui a permis de développer des tests de **primalité** extrêmement efficaces: on peut maintenant facilement **prouver** la primalité d'un nombre de 1000 chiffres décimaux, et avec un peu plus de difficulté, de 5000 chiffres. Les méthodes employées utilisent des outils mathématiques beaucoup plus sophistiqués (corps cyclotomiques, sommes de Gauss et de Jacobi pour le test APRCL, courbes elliptiques pour le test d'Atkin–Morain).

L'histoire des tests de primalité s'est plus ou moins terminée avec le travail de Agrawal–Kayal–Saxena (AKS) en 2002 qui ont donné le premier test de primalité qui prend un temps **polynomial** en le nombre de chiffres de p; de plus, il est plus élémentaire que les tests mentionnés ci-dessus. Toutefois, malgré un certain nombre d'améliorations apportées successivement par H. Lenstra, C. Pomerance, puis D. Bernstein, il n'est toujours pas compétitif **en pratique** par rapport aux tests ci-dessus, donc il est pour l'instant d'intérêt théorique et pédagogique.

5. Factorisation

5.1. **Introduction.** Nous en venons maintenant à l'autre coté du sujet, la **factorisation**. Voyons d'abord de quoi il s'agit. Nous nous donnons un entier N, et (après avoir éventuellement regardé si N est divisible par 2, 3, et 5 par exemple pour éliminer des cas évidents), grâce aux tests de **non-primalité** on s'assure soit que N n'est certainement **pas** un nombre premier, soit qu'il est presque certainement premier. Dans ce dernier cas, nous appliquons alors un test de **primalité**, souvent plus délicat, pour prouver que N est effectivement premier (il se peut bien entendu qu'il ne le soit pas, mais c'est excessivement rare).

Si nous découvrons que N est un nombre premier, notre travail est terminé. Sinon, en dehors de cas assez simples nous aurons montré que N n'est pas un nombre premier, sans pourtant avoir la moindre idée d'un diviseur de N autre que 1 et N (par exemple, si le reste de la division de 2^{N-1} par N n'est pas égal à 1).

Le problème de la **factorisation** consiste donc à trouver un tel diviseur (on peut ensuite travailler sur les morceaux et obtenir la décomposition complète en produit de nombres premiers). Disons tout de suite que c'est **beaucoup plus difficile**.

Tout d'abord une remarque d'ordre "philosophico-mathématique". Prouver qu'un entier N est un nombre premier (réponse à la question: oui ou non) necessite une **rigueur mathématique absolue**. Il faut une véritable démonstration, que l'on puisse vérifier, etc...

Par contre, pour factoriser un nombre vous avez parfaitement le droit d'aller voir une voyante qui vous donne un facteur: **aucune rigueur** n'est nécessaire, puisque si on vous dit que d est un facteur de N, vous effectuez simplement la division N/d pour vérifier que le reste est nul.

On peut donc utiliser une multitude d'approches pour factoriser, y compris les plus baroques. Noter qu'il m'arrive parfois de recevoir des lettres d'amateurs me disant qu'ils ont trouvé une méthode merveilleuse pour factoriser, et si je leur réponds, je leur envoie un grand nombre construit spécialement, et je leur demande de le factoriser, et la correspondance s'arrête là.

Nous verrons également ci-dessous que la difficulté de la factorisation est à la base de la méthode de chiffrement **RSA**, donc est fondamentale en cryptographie.

5.2. **Divisions Successives.** Nous avons donc un entier N dont nous savons qu'il n'est pas premier, et nous voulons trouver un facteur. La première méthode qui vient à l'esprit est de diviser successivement N par 2, 3, 4,... jusqu'à $N-1$ pour voir si un reste est nul. On peut facilement améliorer cette méthode en remarquant que si d est un diviseur de N, alors $N = d \times (N/d)$ et N/d est aussi un diviseur de N, et si on choisit pour d le plus petit diviseur de N autre que 1 on aura donc $d \leq N/d$, soit $d^2 \leq N$, donc $d \leq \sqrt{N}$. Il suffit donc de diviser N par les entiers de 2 à $\sqrt{N}$, ce qui est bien entendu beaucoup plus rapide. A la main on peut faire ceci raisonnablement jusqu'à $N = 10^4 = 10000$, et sur ordinateur, $N = 10^{18}$ prend moins de 90 secondes par exemple.

Cette méthode, appellée naturellement méthode des **divisions successives** peut encore être améliorée: par exemple, une fois testé que N n'est pas divisible par 2 (est impair), il est évidemment inutile de diviser N par 4, 6, etc... Idéalement, il faudrait diviser N seulement par des nombres premiers. Mais comme il est encombrant de calculer et stocker une telle table, on se contente de diviser par des entiers qui eux-mêmes ne sont divisibles ni par 2 ni par 3 par exemple, ce qui (après avoir essayé 2 et 3 eux-mêmes) donne la suite de diviseurs potentiels 5, 7, 11, 13, 17, 19, 23, 25, etc..., avec écarts successifs 2, 4, 2, 4, etc... Cette méthode est déjà environ 3 fois plus rapide que la méthode la plus naïve (38 secondes au lieu de 90 pour $N = 10^{18}$).

C'est toutefois une méthode limitée par nature, son temps d'exécution étant en gros proportionnel à $\sqrt{N}$, donc même sur ordinateur limitée à des nombres d'une vingtaine de chiffres décimaux.

Noter que Fermat a inventé une méthode alternative de factorisation qui peut donner de bons résultats quand la méthode ci-dessus échoue ou est trop longue, mais la méthode de Fermat est également en $\sqrt{N}$.

5.3. **Utilisation du Théorème de Fermat: la Méthode $p-1$.** Nous avons vu la très grande utilité du théorème de Fermat dans les tests de non-primalité et de primalité. Peut-être paradoxalement (puisqu'il s'occupe principalement de nombres premiers), on peut également l'employer très utilement pour factoriser, bien que, contrairement à la méthode précédente, on ne trouve pas systématiquement un facteur.

Rappelons tout d'abord la notion de PGCD (plus grand commun diviseur): si a et b sont des entiers, le plus grand entier d qui divise à la fois a et b s'appelle le PGCD de a et de b, mais il possède une propriété plus **forte**: si e est un diviseur commun à a et b, alors par définition $e \leq d$, mais en fait on a beaucoup mieux: e est un **diviseur** de d.

D'autre part, **l'algorithme d'Euclide** mentionné ci-dessus permet très rapidement de calculer un PGCD **sans factoriser** a et b, je ne donne pas les détails, très classiques.

L'idée de l'utilisation du théorème de Fermat est alors la suivante. Soit p un facteur premier de N. D'après le théorème de Fermat, nous savons d'une part que p divise $a^{p-1}-1$, et d'autre part par hypothèse p divise N. Il en résulte que p divise le PGCD de $a^{p-1}-1$ et N, qu'on peut aisément calculer grâce à l'algorithme d'Euclide. Il est possible que ce PGCD d soit plus grand que p, mais cela n'a aucune importance, puisque d divise N on aura quand même trouvé un diviseur de N autre que 1 et pratiquement toujours autre que N (au passage noter qu'on ne calcule **jamais** a^{p-1} lui-même, mais son reste de division par N comme expliqué ci-dessus, pour n'avoir que des nombres de taille raisonnable).

Il semble donc qu'on ait trouvé une méthode (très efficace) pour factoriser N, mais bien sûr pour l'instant c'est un leurre: on ne peut pas calculer $a^{p-1}-1$ sans connaître p, ça à donc l'air d'un cercle vicieux.

Mais pas tout à fait: faisons l'hypothèse que $p-1$ soit lui-même un produit de puissances de nombres premiers pas trop grands. Par exemple, supposons que les puissances de premiers divisant $p-1$ soient plus petites qu'une certaine borne B: il en résulte que $p-1$ divise $B!$, produit des entiers de 1 à B. Si on écrit $B! = (p-1)q$, on a donc

$$a^{B!} = (a^{p-1})^q \ ,$$

donc le reste de la division de $a^{B!}$ par p est aussi égal à 1, donc p divise le PGCD de $a^{B!}-1$ et N. Il n'y a donc plus de cercle vicieux puisqu'on peut se donner B.

Pour des raisons évidentes cette méthode s'appelle la méthode $p-1$, et est due à J. Pollard, mathématicien britannique qui a inventé un grand nombre de très utiles méthodes de factorisation.

J'ai présenté la méthode de la manière la plus primitive, mais en fait on utilise toujours au moins deux améliorations. Premièrement, au lieu de prendre $B!$, on prend le **plus petit commun multiple** (PPCM) des entiers de 1 à B, ce qui améliore considérablement le temps d'execution. Deuxièmement, si $p-1$ n'a pas que des petits facteurs premiers, il arrive beaucoup plus souvent qu'il ait beaucoup de petits facteurs premiers, et un seul facteur premier nettement plus grand. On peut modifier l'algorithme pour prendre ceci en compte.

Donnons un exemple. Soit $N = 39916801279417607$, et choisissons $B = 12$, disons. En réduisant modulo N à chaque étape, on trouve immédiatement (sur ordinateur) que le reste de la division par N de $2^{B!}$ est égal à $R = 28730708527905607$. Nous utilisons alors l'algorithme d'Euclide pour calculer le PGCD de $R-1$ avec N, et on trouve également immédiatement que celui-ci est égalà 39916801, qui est donc un facteur (en fait premier) de

N. Le temps de trouver ce facteur a été négligeable, alors que si on avait fait une recherche systématique par divisions successives, cela aurait pris beaucoup plus de temps.

J'insiste sur le fait que cette méthode, assez simple en fait, permet de trouver certains facteurs, mais n'est pas du tout systématique.

5.4. **La Méthode Rho de Pollard.** Revenons à des méthodes systématiques de factorisation. Il a fallu attendre 1974, ce qui est incroyablement tard, pour voir apparaître une méthode de factorisation plus rapide que $\sqrt{N}$, en $\sqrt[3]{N}$, due à S. Lehman. Bien qu'élémentaire, cette méthode est assez compliquée à expliquer et n'a qu'un intérêt historique.

Une méthode tout à fait remarquable et à la fois techniquement beaucoup plus simple et de plus en $\sqrt[4]{N}$, ce qui est encore plus rapide, et due aussi a Pollard: c'est la méthode ρ, pour une raison que nous verrons plus bas.

Présentons d'abord l'algorithme sous la forme d'une boite noire, sans aucune explication.

Algorithme ρ de Pollard. Soit à factoriser le nombre N. Poser $x \leftarrow 1$, $y \leftarrow 1$, puis répéter $x \leftarrow x^2+1$, $y \leftarrow y^4+2y^2+2$ (restes de la division par N), puis calculer par l'algorithme d'Euclide le PGCD de $x-y$ avec N jusqu'à ce qu'il soit différent de 1 et N, ce qui donne bien un diviseur de N.

Ultrasimple et magique, n'est-il pas ?

Prenons un exemple: soit à factoriser $N = 1147$. On obtient successivement $(x,y) = (1,1)$, $(2,5)$, $(5,677)$, $(26,677)$, et le PGCD de $677-26$ avec 1147, calculé par Euclide, est égal à 31, donc facteur de N. Comme on le voit, c'est très rapide.

Expliquons pourquoi ça marche. Tout d'abord, notons que la formule pour y peut sécrire $y \leftarrow (y^2+1)^2+1$. Donc y est exactement la même suite que x, mais qui va deux fois plus vite: x vaut successivement (en oubliant la division par N) 1, 2, 5, 26, 677, 458330, 210066388901,... alors que y vaut 1, 5, 677, 210066388901, les mêmes nombres de 2 en 2.

On peut donc espérer que nous ayons ce qu'on appelle deux **marches aléatoires** parmi les entiers de 0 à $N-1$, le fait d'élever au carré et d'ajouter 1 semblant être une opération assez au hasard. La deuxième marche va deux fois plus vite que la première, et après un certain nombre de pas, a de bonnes chances de tomber à nouveau sur la même valeur que la première. C'est un résultat peut être pas complètement intuitif de probabilités: on peut s'attendre à ce que les deux marches aléatoires se mettent à coïncider après environ $\sqrt{N}$ étapes (voir ci-dessous le jeu du kangourou sauvage et apprivoisé).

Pour l'instant rien à voir avec la factorisation. Mais soit p un diviseur premier de N, qu'on peut toujours supposer plus petit que $\sqrt{N}$ en prenant le plus petit, puisqu'on suppose N non premier. Puisque p divise N, il est clair que le fait de réduire modulo N (reste de la division par N) ne change pas le reste de la division par p. Donc au lieu de considérer les marches aléatoires comme étant modulo N, elles sont aussi **implicitement** (car on ne connait pas encore p) modulo p. Mais si elles coïncident modulo p, ce qu'elles doivent faire après environ $\sqrt{p}$ étapes, cela signifie que les restes de division de x et y par le nombre inconnu p sont les mêmes, donc que p divise $x-y$, et comme p divise N, le PGCD de $x-y$ et N sera divisible par p, donc pas égal à 1, et presque certainement pas N non plus, ce qui explique pourquoi l'algorithme marche. De plus, comme $p \leq \sqrt{N}$, on a $\sqrt{p} \leq \sqrt[4]{N}$, comme annoncé.

Si vous dessinez le comportement de l'une des marches aléatoires modulo p, il y a d'abord une "queue" non périodique, puis un cycle périodique, qui ensemblent forment la lettre grecque rho ρ, d'où le nom de la méthode.

Noter aussi que la méthode est sensible à la taille du plus petit diviseur p de N: plus il est petit, plus c'est rapide. Ce n'est PAS le cas de toutes les méthodes de factorisation (d'ailleurs déjà la méthode $p-1$ vue ci-dessus n'est pas tellement sensible à la taille de p mais plutôt à la taille des facteurs de $p-1$, ce qui est assez différent).

Bien qu'ancienne (1975) cette méthode est toujours utilisée, vu sa simplicité. Il est possible de remplacer x^2+1 par d'autres fonctions, mais pas n'importe lesquelles. On peut par exemple prendre x^2-1 ou x^2+2, mais on ne peut **pas** prendre x^2 (c'est pratiquement évident) ni x^2-2 (c'est moins évident, et dû à l'identité $(z+1/z)^2-2=z^2+1/z^2$).

5.5. **Parenthèse: Le Jeu des Kangourous.** Je suppose que la plupart des lecteurs auront entendu parler du **paradoxe des anniversaires**, qui comme tout paradoxe n'en est pas un une fois expliqué: bien qu'il y ait 365 jours dans l'année, dans une classe de 23 élèves, il y a plus d'une chance sur 2 que deux élèves ait le même anniversaire (si la classe a 35 élèves, la probabilité est de 81%). Ce nombre 23 est proche de la racine carrée de 365 (environ 19), ce qui est phénomène très fréquent en probabilité.

Le jeu du Kangourou est basé sur une idée semblable. Supposons qu'il y ait un kangourou sauvage qui saute à chaque fois en ligne droite une distance de 1 à 10 pas, le nombre de pas qu'il doit faire à chaque fois étant indiqué à l'endroit où il tombe, sauf la première fois où il choisit comme il veut. Comment rattraper ce kangourou en obéissant aux mêmes règles que lui ? Il n'y a même pas à réfléchir: on prend un kangourou apprivoisé qui saute deux fois plus vite (mais le même nombre de pas), et on lui dit de faire la même chose: le paradoxe du kangourou nous dit qu'assez rapidement le kangourou apprivoisé sera exactement dans les traces du kangourou sauvage.

Tour de cartes correspondant: prenez deux (mieux, trois) jeux de 52 cartes dans lesquels vous enlevez les RDV pour qu'il n'y ait que des cartes de 1 à 10. Vous dites à un ami de choisir dans sa tête un nombre entre 1 et 10, puis de placer devant lui les cartes (ouvertes) une à une jusqu'à ce nombre, et sans hésiter, continuer à la manière du kangourou, c'est à dire de continuer à prendre le nombre de cartes indiqué sur la carte où il est tombé, et ainsi de suite jusqu'à ce que le paquet soit épuisé. Votre ami doit seulement se souvenir de la dernière carte où il est tombé (sans vous le dire ni hésiter).

Comment trouver cette carte ? Pas de problème, faites la même chose que lui, choisissez un nombre au hasard entre 1 et 10, etc... La dernière carte sur laquelle vous tomberez sera presque certainement la même que la sienne.

5.6. **Méthodes Modernes de Factorisation.** Depuis la méthode ρ de Pollard, un très grand nombre de méthodes de plus en plus efficaces ont été inventées. La plupart (mais pas toutes!) utilisent des notions mathématiques, mais également informatiques, plus ou moins sophistiqués.

Je cite les plus utiles, sans essayer d'expliquer leur fonctionnement, mais en donnant quelques explications sur leurs limitations.

• La méthode des **courbes elliptiques** (ECM en anglais), introduite par H. Lenstra. Cette méthode est la seule méthode autre que la méthode ρ a être principalement sensible au diviseur premier p de N cherché. Bien qu'elle utilise la notion mathématique de courbe elliptique, elle est relativement simple à expliquer et à programmer, si l'on accepte un certain nombre de résultats.

• La méthode du **crible quadratique** de C. Pomerance et autres. Cette méthode est basée sur des principes extrêmement simples que je pourrais expliquer dans le cadre de cet article, mais est extrêmement complexe et technique à mettre en œuvre, nécessitant également de solides notions informatiques.

• La méthode du **crible algébrique** de J. Pollard, qui est la méthode la plus rapide actuellement connue pour factoriser des nombres qui n'ont aucune raison d'avoir de petits facteurs premiers, par exemple les nombres RSA (voir plus bas). Encore plus technique que la précédente, mais bien sûr vu son utilité ça vaut le coup. Cette méthode utilise des notions mathématiques un peu plus avancées (corps de nombres, groupes de classes, unités, etc...) mais même connaissant ces notions il est hors de question pour un amateur d'essayer de la programmer, vu sa complexité.

Pour donner une idée, il est maintenant raisonnable de factoriser des nombres de 160 à 180 chiffres décimaux, et avec de très gros efforts, 220 chiffres. Il est pour l'instant absolument impossible (sauf coup de chance improbable) de factoriser un nombre de 350 chiffres, disons. En particulier, les fabriquants de cartes à puces qui utilisent RSA (voir ci-dessous) choisissent maintenant pour la plupart des nombres de 2048 bits, c'est à dire plus de 600 chiffres décimaux.

6. Cryptographie

Pour terminer, parlons de cryptographie, et plus précisément de l'application de la théorie des nombres (et en particulier des nombres premiers) à la science des codes secrets.

6.1. **Cryptographie à Clef Secrète.**

Les premiers codes secrets, utilisés depuis l'antiquité, étaient de simples codes de permutation: par exemple remplacer A par B, B par C, etc..., ce qui rend déjà le message "illisible" (le mot "nous" se transforme en "opvt"), mais est beaucoup trop facile à déchiffrer. Il y a des variantes un peu plus difficiles à déchiffrer (exemple en exercice), mais cela fait très longtemps qu'on ne les utilise plus.

Un mode de chiffrement beaucoup plus efficace utilise une "clef secrète". Si par exemple on décide d'utiliser telle page de telle édition de tel livre, la permutation peut se faire en fonction des lettres rencontrées dans cette page. Par exemple si la clef secrète est "abracadabra" (donc numéros (1)(2)(18)(1)(2)(1)(4)(1)(2)(18)(1) dans l'ordre alphabétique), on peut crypter en utilisant successivement une permutation de 1, puis 2, puis 18, puis 1,... lettres. Ceci devient quasiment indéchiffrable si l'on ne possède pas la clef secrète.

De très nombreuses améliorations et transformations ont été apportées à cette idée naïve, mais l'un des problèmes qui reste est le transport de la clef secrète elle-même.

L'état actuel de la cryptographie à clef secrète est le suivant: le protocole utilisé au niveau international (car imposé par les US) s'appelle le DES, inventé en Belgique; il est très rapide,

mais necessite la transmission par d'autres moyens d'une clef secrète. Il est considéré comme très sûr.

6.2. **Cryptographie à Clef Publique.** L'invention de la crytographie à clef publique à la fin des années 1970 provient d'un paradoxe (comme d'habitude apparent): tout le problème de la transmission de la clef secrète serait réglé si on rendait cette clef publique! Ceci est évidemment ridicule puisqu'une fois qu'on connait la clef, on peut aisément décoder.

Et pourtant ceci n'est pas vrai. Dans le contexte expliqué ci-dessus où la clef sert simplement à décaler les lettres, effectivement connaître la clef de codage permet très facilement de décoder. Mais que se passerait-il si on pouvait créer une méthode de codage utilisant une clef, telle que la connaissance de cette clef ne permette **pas** de décoder ?

Le problème de la primalité et factorisation apporte une première réponse à ce problème (il y en a d'autres, telles que par exemple l'utilisation de **logarithmes discrets**): choisissons deux **grands** nombres premiers p et q: grâce aux tests de primalité, c'est très facile à faire (il faut moins d'une seconde pour créer des nombres premiers de 200 chiffres décimaux, disons), et posons $N = p \times q$. Gardons précieusement secrets nos nombres p et q, mais rendons public le nombre N.

Imaginons que l'on trouve une méthode de **codage** utilisant le nombre N, sans avoir besoin de connaître ses facteurs p et q, mais par contre que pour décoder il soit absolument nécessaire de les connaître. Nous avons alors gagné. En effet, tout interlocuteur désirant nous addresser un message codé peut le faire en utilisant N, puisque N est **public**. Par contre, nous seuls sommes capable de déchiffrer le message puisqu'il faut connaître p et q pour cela.

On peut faire encore mieux, car un interlocuteur peut facilement se faire passer pour quelqu'un d'autre (c'est la base du **phishing**): supposons que Monsieur H, qui a sa méthode de **C**odage publique C_H et de **D**écodage ultra-secrète D_H veuille communiquer avec Monsieur Z, qui a les méthodes correspondantes C_Z et D_Z.

Si M est le message à envoyer de H à Z, H envoie le message codé

$$M' = C_Z(D_H(M)) \ :$$

il peut le faire puisque il connait D_H (il est seul à le connaître), et qu'il connait aussi C_Z qui est **public**. Puisque

$$M = C_H(D_Z(M')) \ ,$$

Z peut récuperer le message car il connait D_Z (il est seul à le connaître), et il connait C_H qui est public.

L'avantage énorme de cette méthode un peu plus complexe est que maintenant le message est **authentifié**: si vous réfléchissez bien, vous verrez qu'il est impossible (sauf évidemment si les secrets se sont éventés) que le message soit lu par un autre que Z (il faut D_Z), mais également il est impossible que ce message provienne de quelqu'un d'autre que H (il faut D_H).

6.3. **La Méthode RSA.** Reste à trouver une méthode de codage utilisant seulement N, mais dont la méthode de décodage nécessite p et q. Une fois que l'on a cette idée c'est très facile, mais les premiers à en avoir eu l'idée, qu'ils ont breveté et qui vaut des milliards de dollars, sont Rivest, Shamir et Adleman, d'où le nom de RSA.

Prenons un exemple simple. Choisissons nos grands premiers p et q tels que le reste de leur division par 3 soit égal à 2. Pour **coder** un message M, on le transforme d'abord en un nombre (par exemple $a = 01$, $b = 02$, etc...), que nous appellerons encore M pour simplifier, et comme message codé M' nous calculons le reste de la division par N de M^3. Bien noter que pour faire ce codage nous n'avons besoin que de N lui-même, pas de ses facteurs p et q.

Celà peut sembler paradoxal, mais prendre une "racine cubique" modulo N est essentiellement impossible sans connaître p et q. Par contre, grâce au théorème de Fermat c'est facile quand on les connait:

Cherchons un exposant e tel que le reste de la division par N de $(M')^e$ soit le message initial M. On a (modulo N)

$$(M')^e = M^{3e} = M \times M^{3e-1} \ .$$

Si on peut choisir e tel que $3e-1$ soit divisible par $p-1$ et par $q-1$, alors d'après le théorème de Fermat les restes de la division de M^{3e-1} par p et par q seront égaux à 1, en d'autres termes p et q divisent $M^{3e-1}-1$, donc également leur produit $N = pq$ (on choisit p et q distincts), donc pour récuperer M il suffit de calculer le reste de la division par N de $(M')^e$.

Choisir e est très facile: comme nous avons pris soin que le reste de la division par 3 de p et de q soit égal à 2 on peut par exemple prendre

$$e = \frac{2(p-1)(q-1)+1}{3} \ :$$

c'est bien un entier d'après le choix de p et q, et évidemment $3e-1 = 2(p-1)(q-1)$ est bien divisible par $p-1$ et par $q-1$.

Noter qu'en pratique la méthode RSA ne sert pas directement à coder de longs messages, car c'est une méthode relativement lente (pensez aux milliards de transactions par seconde qui se font de part le monde), mais plutôt par exemple à coder les clefs secrètes utilisées par les techniques beaucoup plus rapides à clef secrètes. C'est donc une méthode complémentaire mais essentielle.

Enfin notons que cela fait de nombreuses années que les experts indiquent qu'il faudrait remplacer RSA par une méthode beaucoup plus moderne et beaucoup plus efficace, car nécessitant des clefs publiques beaucoup plus courtes: la **cryptographie sur courbes elliptiques**. Par exemple nous avons indiqué que par sécurité il est maintenant nécessaire d'utiliser des clefs RSA publiques de 2048 bits (617 chiffres décimaux), alors que pour une sécurité équivalente, l'utilisation des courbes elliptiques ne nécessite que des clefs de 224 bits (68 chiffres décimaux). Mais l'inertie des décideurs devant le coût prohibitif du changement empêche cette reconversion.

7. Logiciels

Voici les URLs de deux logiciels libres (et donc gratuits) destinés aux professionnels de la théorie des nombres. Malgré tout, je vous conseille de télécharger au moins **Pari/GP**, assez léger, qui est facile d'accès et vous permettra de vous amuser longtemps avec les nombres.

Pari/GP: développé sous ma direction à Bordeaux depuis 25 ans, et maintenant sous la direction de Karim Belabas et Bill Allombert. Possède son propre langage de programmation, assez facile d'accès pour un non informaticien.

`http://pari.math.u-bordeaux.fr`

Disponible sur toutes plateformes (PC, Mac, Linux), et sur tablettes et smartphones Android sous le nom de `paridroid`.

Sage: dveloppé sous la direction de W. Stein a Seattle depuis 8 ans. Gigantesque logiciel contenant de manière relativement intégrée à peu près tous les logiciels libres (dont Pari/GP bien sûr) ayant un rapport avec la théorie des nombres, la combinatoire, l'algèbre, la géométrie algébrique, etc... Son langage de programmation est essentiellement **Python**.

`http://www.sagemath.org`

Université Bordeaux I, Institut de Mathématiques de Bordeaux, UMR 5251 du CNRS, 351 Cours de la Libération, 33405 TALENCE Cedex, FRANCE