# Pourquoi chercher en arithmétique aujourd'hui ?

Bertrand Rémy

ENS de Paris, le 15 juillet 2021

# Motivation «quotidienne» : cryptage RSA

Problème : notre but est de pouvoir procéder au chiffrement et au déchiffrement (= codage et décodage) sécurisé d'information à transmettre. Par exemple :

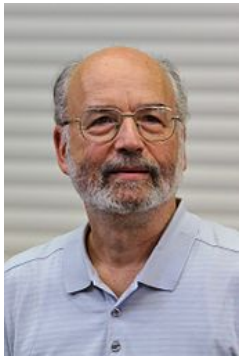
1. recevoir un message codé qui ne peut être lu que par moi ;
2. authentifier un message par ma signature certifiée.

Une méthode consiste à utiliser les propriétés des nombres entiers, en particulier les nombres premiers et l'opération de division euclidienne. C'est la raison pour laquelle nous allons faire une digression sur l'arithmétique des nombres entiers.

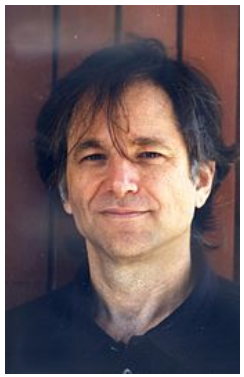
Les recettes sont relativement simples à expliquer, mais les justifications scientifiques relèvent de recherches mathématiques et informatiques qui sont encore d'actualité.

# Les inventeurs du cryptage RSA

Ronald Rivest



Adi Shamir



Leonard Adleman

# Arithmétique. Les nombres

Dans cet exposé, il va être question d'**arithmétique** : c'est une branche des mathématiques qu'on appelle aussi la **théorie des nombres**.

En mathématique, on utilise beaucoup les nombres pour contrôler des grandeurs (des tailles d'ensembles, des valeurs de fonctions) : la plupart du temps les nombres sont des **outils**. Pour calculer de plus en plus efficacement, on est même amené à construire des ensembles de nombres de plus en plus grands.

Les collégiens et lycéens apprennent successivement à travailler avec les nombres entiers naturels (0; 1; 2; etc.), puis les nombres entiers relatifs (on ajoute -1; -2; etc.), puis les nombres rationnels, qui sont les fractions de nombres entiers (par exemple : $\frac{3}{2}$, $\frac{4}{7}$, $\frac{-5}{8}$ etc.).

Et il y en a d'autres (les nombres réels, complexes) !

# Arithmétique. La discipline de recherche

Mais en arithmétique, les nombres sont les **objets d'étude** et pas seulement les outils : c'est même la définition de cette discipline des mathématiques. On se pose beaucoup de questions sur les nombres et certaines d'entre elles peuvent sembler abstraites, gratuites, arbitraires...

Plutôt que chercher à expliquer les arguments qui convainquent un mathématicien de réfléchir à un problème d'arithmétique, j'ai fait les choix suivants :

1. décrire des questions élémentaires de théorie des nombres ;
2. mentionner quelques retombées dans la vie quotidienne de réponses, même partielles, à ces questions.

C'est une sorte de grand écart entre des spéculations intellectuelles et des applications très concrètes.

# Arithmétique. Les nombres entiers et leurs multiples

Pour partir de questions vraiment élémentaires, on ne va manipuler que des nombres entiers.

On dispose d'opérations de calcul : **addition**, **soustraction**, **multiplication** ; on a aussi une notion d'**ordre** sur les nombres : on sait les comparer puisqu'on peut toujours dire lequel de deux nombres est le plus grand.

Il y a une autre façon de ⟪comparer⟫ des nombres, qui ne fonctionne que partiellement, mais qui va être très intéressante pour nous : c'est la **relation de divisibilité**.

Par exemple : 3 *divise* 21 car on peut écrire 21 comme un multiple entier de 7 puisque $21 = 3 \times 7$.

En général, on dit qu'un entier $m$ **divise** un autre entier $n$ s'il existe un troisième entier $k$ tel que $n = m \times k$ ; on dit aussi que $n$ est un **multiple** de $m$.

# Arithmétique. La division euclidienne

Si $d$ est un nombre entier, une façon de décider si un nombre est multiple de $d$ consiste à effectuer sa division avec reste entier.

Plus précisément, on se donne en plus de $d$ un nombre entier $N$. La **division euclidienne de $N$ par $d$** est l'écriture (unique) :

$$N = q \times d + r$$

où l'on impose que le **reste** $r$ soit un nombre entier ($\geqslant 0$) plus petit que $d$.

De façon imagée : si on se donne $N$ jetons, le nombre $q$ est le nombre maximal de paquets de $d$ jetons que l'on peut former et il reste $r$ jetons hors paquets.

On remarque que le fait que $N$ est un multiple de $d$ (ou encore est divisible par $d$) se traduit par le fait que le reste $r$ ci-dessus vaut 0.

# Arithmétique. Les nombres premiers

On en vient aux vedettes du jour : les **nombres premiers**.

Voici la définition : *un nombre premier, c'est un nombre entier positif qui a exactement deux diviseurs, qui sont alors 1 et lui-même*.

Exemple : 2; 3; 5; 7; 11; 13; 17; 19; 23; 29; 31; 37; 41; 43; 47; 53; 59; 61; 67; 71; 73; 79; 83; 89; 97 etc.

Les nombres premiers sont les blocs élémentaires de l'étude des nombres entiers du point de vue de la divisibilité : *tout nombre entier s'écrit comme produit de nombres premiers, et la décomposition est unique à l'ordre des facteurs près*.

Exemple : $153153 = 3^2 \times 7 \times 11 \times 13 \times 17$.

# Le truc arithmétique du cryptage

Choisir deux **très grands nombres premiers** $p$ et $q$ et former le nombre $n = p \times q$ : c'est la taille maximale des messages à transmettre et à recevoir.

Mathématiquement (c'est de l'arithmétique du 17e et du 18e siècle), on sait trouver des entiers $e$ et $d$ qui ont la propriété suivante : *à chaque fois qu'on se donne un entier $M$ plus petit que $n$, si on calcule $M^{de} = (M^e)^d = (M^d)^e$ (c'est $M$ multiplié avec lui-même $d \times e$ fois) et qu'on effectue la division euclidienne de $M^{de}$ par $n$, on retrouve le nombre $M$ !*

Précautions et instructions :

1. garder jalousement pour soi la décomposition $n = p \times q$ et le nombre $d$ ;
2. diffuser les nombres $n$ et $e$ à ceux dont on veut recevoir des informations cryptées.

# La recette de cryptage

Procédures d'envoi :

1. Pour recevoir un message $M$, je demande de m'envoyer le reste de la division euclidienne de $M^e$ par $n$, appelé $C$.
2. Pour envoyer un message $M$, j'envoie le reste de la division euclidienne de $M^d$ par $n$, appelé $C$.

Procédures de réception :

1. Dans le cas 1, je calcule le reste de la division euclidienne de $C^d$ par $n$ pour recevoir $M$.
2. Dans le cas 2, mon destinataire calcule le reste de la division euclidienne de $C^e$ par $n$ pour recevoir $M$.

Dans les deux cas, l'information transmise visible publiquement est le message crypté $C$ (pas $M$) mais à la fin $M$ est reconstitué là où il faut (chez moi ou chez le destinataire que j'ai choisi).

# Exemple de cryptage et décryptage (merci à Wikipedia)

Je prends $p = 3$ et $q = 11$, et donc $n = 33$ (dans la pratique, il faut des nombres premiers gigantesques, mais on veut ici des calculs raisonnables). La théorie mathématique (le petit théorème de Fermat ci-dessous) dit qu'on peut prendre $e = 3$ et $d = 7$. L'information que je transmets à l'interlocuteur est $n = 33$ et $e = 3$. Je garde pour moi la décomposition $n = 3 \times 11$ et $d = 7$.

Le message que mon interlocuteur veut m'envoyer se traduit par le nombre $M = 4$ (inférieur à 33). Par les informations que je lui ai données ($n$ et $e$, appelées *clé publique*), mon interlocuteur sait que ce qu'il a à faire : calculer $4^3 = 64$ et prendre le reste par la division euclidienne par 33, soit 31. Il m'envoie alors le message crypté $C = 31$.

Pour le décrypter, je calcule $31^7 = 27512614111$ et je fais la division euclidienne par 33 : le reste vaut $M = 4$.

# Le petit théorème de Fermat

À la base de la détermination des entiers $e$ et $d$, il y a un énoncé de Pierre de Fermat et qui est a priori surprenant :

**Théorème.—** *Soit $p$ un nombre premier. Alors pour tout nombre entier $M$, le nombre premier $p$ divise la différence $M^p - M$.*

Exemples : $5^3 - 5 = 120$ est divisible par 3 ; $(-3)^7 + 3 = -2184$ est divisible par 7 et $2^{97} - 2 = 158456325028528675187087900670$ est divisible par 97.

Pierre de Fermat

# L'ensemble des nombres premiers

Derrière tout ça, il y a le fait que l'on commence à bien comprendre l'ensemble des nombres premiers, même s'il reste encore extrêmement mystérieux.

1. Depuis les Grecs, on sait prouver que cet ensemble est infini.
2. Depuis Fermat et Euler, on sait justifier l'existence de $e$ et $d$ comme ci-dessus.
3. Il est crucial de pouvoir fabriquer des nombres premiers de plus en plus grands.
4. Il est crucial qu'il n'existe pas d'algorithme de décomposition en facteurs premiers trop efficace à ce jour (c'est un problème très difficile – on a de la marge).

Si un jour on conçoit des ordinateurs avec des capacités de calcul bien supérieures, il faudra penser à autre chose...

# Produire des nombres premiers

Pour revenir à des questions de recherche, voici une liste de questions actuelles concernant la production de nombres premiers :

1. Existe-t-il une infinité de nombres premiers $p$ tels que $p+2$ soit lui aussi premier (on parle de *nombres premiers jumeaux*)?
2. Existe-t-il une infinité de nombres premiers de la forme $2^n+1$ avec $n$ entier (on parle de *nombres premiers de Fermat*) ?
3. Existe-t-il une infinité de nombres premiers de la forme $2^n-1$ avec $n$ entier (on parle de *nombres premiers de Mersenne*) ?

Exemples de gros nombres premiers : $2^{43112609}-1$ (qui a au moins $10^7$ chiffres en écriture décimale), et même $2^{57885161}-1$.

# Les progressions arithmétiques

Voici un résultat très récent d'existence de « paquets » de nombres premiers (appelés *progressions arithmétiques*).

**Théorème (B. Green, T. Tao et T. Ziegler).**— *Soit $k$ un nombre entier. Alors il existe une infinité de couples de nombres entiers $a$ et $b \geqslant 1$ tels que $a, a+b, a+2b, \ldots, a+kb$ soient tous premiers. On peut même être très précis sur la « densité » de ces couples $(a, b)$ parmi les couples d'entiers.*

Tamar Ziegler
(Hebrew University, Jerusalem)

# Problèmes élémentaires d'arithmétique

Voici un autre problème arithmétique, dont la formulation est élémentaire, mais qui a des développements très contemporains.

Questions : *est-ce que tout nombre entier* $\geqslant 0$ *se casse en somme de* $n = 2$ *carrés de nombres entiers ? Même question pour* $n = 3$ *et* $n = 4$.

- (Euler, 1755) Un nombre premier impair (i.e. $\neq 2$) est somme de 2 carrés si, et seulement si, il est congru à 1 modulo 4.
- (Lagrange, 1770) Tout nombre entier $\geqslant 0$ est somme d'au plus 4 carrés.
- (Legendre, 1798) Un nombre entier $\geqslant 0$ est somme d'au plus 3 carrés si, et seulement si, il n'est *pas* de la forme $4^a(8b + 7)$ pour $a, b \in \mathbf{N}$.

# Commentaires et prolongements

Le premier énoncé, qui porte sur les nombres premiers, permet en gros résoudre la question générale. Pour voir cela, il suffit de constater que le fait d'être une somme de deux carrés est une propriété stable par produit :

$$\left(a^2+b^2\right)\left(c^2+d^2\right)=(ac-bd)^2+(ad+bc)^2=(ac+bd)^2+(ad-bc)^2.$$

Les énoncés des réponses sans démonstration ont souvent été formulés bien avant (pour $n=2$ : Girard, 1634 ; cas $n=4$ apparemment affirmé dès l'Antiquité).

Remarquons aussi que la réponse au cas $n=4$ rend les questions pour $n \geqslant 5$ sans intérêt.

L'étape suivante est alors plus quantitative : *pour un entier* $\geqslant 0$ *donné, compter le nombre de ses écritures en somme de n carrés*.

# Distribution de points sur la sphère $S^2$

On va s'intéresser au cas $n = 3$.

Pour $k \geqslant 0$ notons $N(k)$ le nombre d'écritures de $k$ comme somme de trois carrés. Le théorème de Legendre se formule alors comme suit :

*$N(k) \neq 0$ si et seulement si $k$ n'est pas de la forme $4^a(8b + 7)$.*

On dit alors que $k$ est « bon » . Une première amélioration est :

*$N(k)$ tend vers $+\infty$ quand $k$, bon, tend vers $+\infty$.*

Remarquons maintenant que si $(x, y, z)$ satisfait $x^2 + y^2 + z^2 = k$, alors le triplet normalisé $(\frac{x}{\sqrt{k}}, \frac{y}{\sqrt{k}}, \frac{z}{\sqrt{k}})$ est un point de la sphère unité $S^2$. Un théorème récent de théorie analytique des nombres (Duke, 1988), affirme :

*À la limite, quand $k$ bon tend vers $+\infty$,*
*les points $(\frac{x}{\sqrt{k}}, \frac{y}{\sqrt{k}}, \frac{z}{\sqrt{k}})$ se répartissent uniformément sur $S^2$.*

# Applications

« *Quand* $k$, *non congru à* $0$, $-1$ *ou* $4$ *modulo* $8$, *tend vers* $+\infty$, *les points* $(\frac{x}{\sqrt{k}}, \frac{y}{\sqrt{k}}, \frac{z}{\sqrt{k}})$ *pour lesquels* $x^2 + y^2 + z^2 = k$, *se répartissent uniformément sur* $S^2$. »

Simuler le hasard est un problème profond, qui a d'innombrables applications dans la vie de tous les jours. Ce théorème dit en quelque sorte qu'on peut simuler la répartition de points au hasard sur la sphère $S^2$ au moyen de la résolution d'un problème de pure arithmétique.