Industrie des polynômes à valeurs entières : diviseurs, nombres premiers, « petit » théorème de Fermat, records

I – L'usine

Les mathématiciens disent : « un polynôme qui **produit**... des valeurs entières, des valeurs premières... ». Ce vocabulaire est tout à fait pertinent et on peut poursuivre l'analogie industrielle : nous sommes dans une usine, on prend une machine, pardon un polynôme P, on « entre » un entier x, on fabrique la valeur $P(x)$ et on la « sort », ou bien on appuie sur la touche "**N**" et on « sort » la suite $P(0)$, $P(1)$, $P(2)$, $P(3)$, $P(4)$, $P(5)$, $P(6)$, etc.

Si vous savez ce qu'est un polynôme, pas de problème. Si vous ne savez pas, imaginez une machine du genre : on « entre » un nombre (pour nous ce sera un entier, mais ce n'est pas obligatoire), on le multiplie par 7, on ajoute 31, et on « sort » le résultat – ou bien : on « entre » un nombre, on l'élève au carré, on ajoute 1, et on « sort » le résultat. Le nombre entré, appelé la *variable*, est traditionnellement noté x, et le résultat, appelé la *valeur* (ou la *valeur prise*), est noté $P(x)$.

Il faut savoir que la machine, pardon un polynôme P, possède des boutons de réglage pour la fabrication, avec ce que les mathématiciens appellent le degré et les coefficients du polynôme. L'ingénieur, pardon le mathématicien, se fixe des objectifs précis sur le résultat : il veut des valeurs qui soient des nombres entiers, des nombres premiers, il veut des diviseurs obligatoires, ou au contraire interdits... Alors il va tourner les boutons de réglage, pour tenter de maîtriser ce qui sort. Il peut aussi arriver qu'il tourne les boutons au hasard, et voie de temps en temps une production inattendue, alors il faut essayer de comprendre, on appelle l'expert, il arrive avec sa sacoche pleine de théorèmes, on essaie de trouver celui ou ceux qui marchent, ceux qui expliquent, qui améliorent la maîtrise de la production...

Avant de faire la visite guidée de l'usine, il faut énoncer une exigence absolue : on peut régler les polynômes comme on veut, degré, coefficients – par contre *la variable sera toujours un entier* (relatif) ; quand on dira par exemple « le polynôme P ne produit que des entiers », cela veut dire que la suite infinie (aux deux bouts) : ..., $P(-n)$, ..., $P(-3)$, $P(-2)$, $P(-1)$, $P(0)$, $P(1)$, $P(2)$, $P(3)$, ..., $P(n)$, ... ne contient que des entiers (relatifs).

L'usine des polynômes est un fournisseur attitré et important de l'usine voisine des comptes et des sommes.

Des exemples :

• le polynôme $\frac{n(n-3)}{2}$ donne le compte du nombre de diagonales d'un polygone *convexe* à n côtés ;

• le polynôme $\frac{n(n-1)(n-2)(n-3)}{24}$ donne le compte du nombre de *points d'intersection*, dans le cas où ils sont *tous distincts*, des diagonales d'un polygone *convexe* à n côtés (malgré le caractère "régulier" de la formule, ce n'est du tout évident !) ;

• le polynôme $P_1(n)=\frac{n(n+1)}{2}$ donne la somme $1+2+...+n$ des n premiers entiers (quand on connaît le résultat, ce n'est pas difficile à démontrer : il suffit de vérifier que $P_1(n)-P_1(n-1)=n$) ;

• le polynôme $P_2(n)=\frac{n(n+1)(2n+1)}{6}$ donne la somme $1^2+2^2+...+n^2$ des *carrés* des n premiers entiers (quand on connaît le résultat, ce n'est pas difficile à démontrer : il suffit de vérifier que $P_2(n)-P_2(n-1)=n^2$) ;

• etc.

II – Les diviseurs des polynômes

Une bonne question

Au fait, quels sont les polynômes qui ne produisent que des entiers (pour les valeurs entières de la variable, redisons-le) ?

↳ Éléments de réponse : les polynômes à coefficients entiers bien sûr, $24x + 7$ ou $x^2 + 1$ ou $x^n - x$. Mais aussi des polynômes à coefficients rationnels non tous entiers, comme $\frac{x(x-1)}{2}$ ou $\frac{x(x-1)(x-2)}{6}$. Alors...?

Quels diviseurs ?

Étant donné un polynôme *à coefficients entiers*, il peut arriver qu'il soit *toujours* (sous-entendu : pour les valeurs entières de la variable) divisible par un certain entier k. Si tous les coefficients du polynôme sont divisibles par k, alors k est un diviseur « apparent » du polynôme. Mais il se peut aussi que k soit un diviseur « caché » ...

Pourquoi le polynôme $x(x-1)$ est-il *toujours* divisible par 2 ?

↳ Réponse : parce que soit x soit $x-1$ est divisible par 2.

Et pourquoi le polynôme $x(x-1)(x-2)$ est-il toujours *divisible* par 6 ?

↳ Même type de réponse, mais en plus compliqué : parce qu'il est à fois toujours divisible par 2 et toujours divisible par 3. Par 2, pour la même raison que pour le précédent, et par 3, encore pour la même raison : l'un des trois entiers consécutifs x, $x-1$ et $x-2$ est divisible par 3.

Vous avez tout compris, alors dites-moi maintenant pourquoi le polynôme $x^5 - x$ est toujours divisible par 5 ?

↳ Tout n'est pas encore clair mais on peut quand même progresser un peu, notamment en "mariant" plusieurs divisibilités : si u et v sont premiers entre eux, la divisibilité d'un entier par uv est équivalente à la conjonction de la divisibilité par u et de la divisibilité par v ("conjonction" = à la fois l'un et l'autre).

Est-ce que cela va de soi ?

↳ Le « théorème de Gauss » dit que, étant donnés trois entiers a, b et c (non nuls), si a divise le produit bc et est premier avec b, alors il divise c.

↳ Corollaire du théorème de Gauss : si deux entiers u et v premiers entre eux divisent un entier w, alors leur produit uv divise w (démonstration : comme u divise w, on peut écrire $w = uz$, mais v divise $w = uz$ et est premier avec u, donc il divise z, gagné !)

↳ La divisibilité d'un entier par uv, disions-nous donc, est équivalente, *si u et v sont premiers entre eux*, à la conjonction de la divisibilité par u et de la divisibilité par v. Par conséquent, pour étudier la divisibilité des valeurs d'un polynôme par un entier d, il est nécessaire et suffisant d'étudier la divisibilité par les facteurs « primaires » de d : si par exemple $d = p^a q^b r^c$ (p, q, r premiers), on étudiera la divisibilité par p^a **et** par q^b **et** par r^c.

Attention ! Attention ! Dans le théorème de Gauss, dans son corollaire et dans tout ce qui va suivre, les entiers sont *relatifs*, et par exemple 19 et –19 sont tous les deux des nombres premiers.

On revient à $P(x) = x^5 - x$

Nous avons affirmé que ce polynôme était *toujours* divisible par 5 :

$P(0) = 0$, OK (0 est divisible par n'importe quel nombre),

$P(1) = 0$, OK,

$P(2) = 30$, OK,

$P(3) = 240$, OK,

$P(4) = 1\,020$, OK,

$P(5) = 3\,120$, OK,

$P(6) = 7\,770$, OK,

$P(7) = 16\,800$, OK,

$P(8) = 32\,760$, OK,

etc.

Une vérification numérique n'est pas une démonstration, et de toute façon, à $x = 8$, on est encore loin de l'infini ! Il nous faut un théorème, le voilà :

Théorème A

Soit P un polynôme à coefficients entiers, et M un nombre entier.

Alors, pour tout entier x et tout entier k : $P(x + k\,M) \equiv P(x) \pmod{M}$.

En particulier, si $P(x)$ est divisible par M, tous les $P(x + k\,M)$ sont divisibles par M.

Démonstration de ce théorème : voir un peu plus bas.

Utilisation n° 1 de ce théorème, démonstration que $P(x) = x^5 - x$ est toujours divisible par 5, avec $M = 5$:

$P(0)$ et $P(1)$ et $P(2)$ et $P(3)$ et $P(4)$, sont divisibles par 5, et tout entier est de la forme $x + 5\,k$ avec $x = 0$ ou 1 ou 2 ou 3 ou 4. Mais c'est une démonstration qui ne fait que démontrer dans le cas particulier de *ce* polynôme. Il y aura plus tard une *explication*, et cette explication sera *générale*.

Parenthèse for maniaques du calcul only.

On peut toujours essayer d'écrire $x^5 - x$ comme une somme

$x(x-1)(x-2)(x-3)(x-4) + 5\,R(x)$.

Il suffit de faire les calculs et on trouve

$x^5 - x = x(x-1)(x-2)(x-3)(x-4) + 5\,x(x-1)(2\,x^2 - 5\,x + 5)$.

Cela donne une *vraie* démonstration, mais malheureusement elle ne se généralise pas bien.

Utilisation n° 2 de ce théorème, démonstration qu'il n'y a aucun polynôme (non constant) qui ***ne*** donne ***que*** des nombres premiers :

On prend un entier x quelconque (0 par exemple !) et on considère $P(x) = y$. Si l'entier y n'est pas premier, le polynôme P aura pris (au moins) une valeur composée et la démonstration est terminée. Si $y = p$ premier (positif ou négatif, peu importe), on considère l'ensemble infini des $P(x + k\,p)$ pour $k \in \mathbb{Z}$. D'après le

théorème A (pour $M = p$), tous ces $P(x + k\,p)$ sont divisibles par p. Un théorème (un autre… nous ne le démontrerons pas ici – il est d'ailleurs intuitivement évident –) dit qu'un polynôme (non constant) ne peut pas prendre une infinité de fois la même valeur : donc les valeurs $P(x + k\,p)$ ne peuvent pas toutes être égales à p ou à $-p$… et il y en a donc une qui est composée (il y en a en fait une infinité).

Remarque au passage.

Il n'y a aucun polynôme (non constant) qui ne donne que des nombres premiers. Au cas où l'on aurait la naïveté de rechercher une « formule » qui ***ne*** donnerait ***que*** des nombres premiers, on voit tout de suite qu'une telle formule doit être *plus compliquée* qu'une formule polynomiale (au cas où la question vous intéresserait, sachez qu'il existe de telles formules – très très compliquées –, mais qu'aucune ne peut servir en pratique, ni pour « fournir » la liste des nombres premiers, ni même pour fournir seulement une suite de grands nombres premiers…).

Et la démonstration du théorème A ?

Si vous y tenez…! Mais il faut d'abord connaître la « formule du binôme » et aussi les coefficients « binomiaux ».

On commence par le début :

$$(a + b)^1 = a + b,$$

$$(a + b)^2 = a^2 + 2\,a\,b + b^2,$$

oui bien sûr… et puis après :

$$(a + b)^3 = a^3 + 3\,a^2 b + 3\,a\,b^2 + b^3,$$

vous avez bien dû rencontrer ça une fois dans votre vie ? Et la suite ? Vous avez deviné :

$$(a + b)^4 = a^4 + 4\,a^3 b + 6\,a^2 b^2 + 4\,a\,b^3 + b^4,$$

et ça continue… Il y a une formule générale, la f*ormule du binôme* :

$$(a+b)^n = a^n + n\,a^{n-1}\,b + \frac{n\,(n-1)}{2}\,a^{n-2}\,b^2 + \ldots + \frac{n\,(n-1)}{2}\,a^2\,b^{n-2} + n\,a\,b^{n-1} + b^n$$

Les coefficients de ce « développement » $\left(1, n, \frac{n\,(n-1)}{2}, \ldots\right)$ s'appellent les *coefficients binomiaux* et il suffit de savoir que ce sont des entiers. Prenez maintenant $a = x$ et $b = k\,M$:

$$(x + k\,M)^n = x^n + n\,x^{n-1}\,k\,M + \frac{n(n-1)}{2}x^{n-2}(k\,M)^2 + \frac{n(n-1)(n-2)}{6}x^{n-3}(k\,M)^3 + \ldots$$

Le premier terme est x^n, et chacun des termes suivants est le produit d'un coefficient binomial (un entier) par une puissance de x (un entier) par une puissance de $k\,M$ d'exposant ≥ 1 (donc un entier *divisible par* M).

Conclusion : $(x + k\,M)^n \equiv x^n \pmod{M}$.

On peut maintenant effectuer la démonstration du théorème A. On considère

$P(x) = a_0 x^t + a_1 x^{t-1} + a_2 x^{t-2} + \ldots + a_{t-1} x + a_t$ $(a_0, a_1, a_2, \ldots, a_t$ entiers).

Pour chaque indice i, on a $a_i (x + k\,M)^{t-i} \equiv a_i x^{t-i} \pmod{M}$

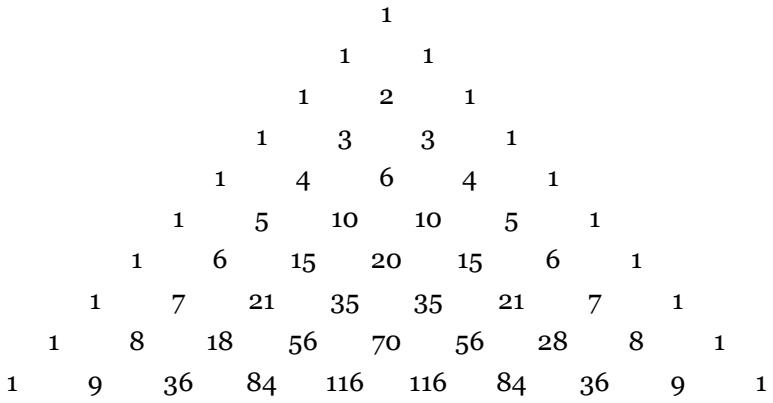
On en déduit, en additionnant tous les termes qui constituent le polynôme,

$P(x + k\,M) \equiv P(x) \pmod{M}$. Gagné !

III – Le « petit » théorème de Fermat

En préambule : le triangle arithmétique de Pascal

Regardez, regardez...



Procédé de fabrication : chaque nombre sur chaque ligne est la somme des deux qui sont au-dessus, juste à gauche et juste à droite (sauf pour les bords, encore qu'il suffise d'imaginer des "0" là où il n'y a rien pour que la règle soit générale).

Primo, vous avez reconnu les coefficients binomiaux ?

Et *secundo*, vous avez remarqué ? Pour le degré 3, tous les coefficients sauf les extrêmes (égaux à 1) sont divisibles par 3, pour le degré 5, tous les coefficients sauf les extrêmes (égaux à 1) sont divisibles par 5, pour le degré 7, tous les coefficients sauf les extrêmes (égaux à 1) sont divisibles par 7, pour le degré 11, ... calculez–les donc et voyez ! A noter que cette propriété n'est vraie que pour les degrés qui sont des nombres premiers.

Encore un théorème : si vous connaissez la formule qui donne les coefficients binomiaux $C_n^k = \binom{n}{k} = \frac{n(n-1)...(n-k+1)}{k!} = \frac{n!}{k!(n-k)!}$ pour les initiés – cette formule est en lien direct avec le triangle arithmétique de Pascal, mais c'est une autre histoire...), vous pouvez démontrer que pour un degré $n = p$ *premier*, tous les coefficients sauf les extrêmes sont divisibles par p. Pour tout k tel que $1 \leq k \leq p-1$, le numérateur de la formule est divisible par p, et le dénominateur, produit de facteurs tous inférieurs à p donc tous premiers avec p, n'est pas divisible par p (encore le théorème de Gauss !).

Le « petit » théorème de Fermat

Toutes les démonstrations en arithmétique – celle du petit théorème de Fermat comme les autres – utilisent le théorème de Gauss. Mais il y a un petit problème... Fermat (1601–1665) a vécu presque deux siècles avant Gauss (1777–1855)... Alors ?

Alors, ne croyez pas que l'on remonte dans le temps ! C'est en fait assez compliqué... En résumé : le théorème de Gauss n'est pas de Gauss mais probablement de Prestet (1648–1690).

En détail : à l'époque de Fermat, les arithméticiens utilisent ce qui s'appellera beaucoup plus tard le théorème de Gauss en le considérant comme une évidence dans la théorie de la divisibilité. Un peu plus tard, Prestet s'est rendu compte que ce n'était pas une évidence mais un théorème, et qu'il y avait une (petite) démonstration à effectuer. Et puis un jour quelqu'un a appelé théorème de Gauss le théorème de Prestet et tout le monde a oublié Prestet !

Lemme

Soit p un nombre premier. Alors, pour tous entiers a et b :

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

NOTA

Quand un ***énoncé*** est vrai, les mathématiciens ont l'habitude de l'appeler *théorème* (ou *proposition*) s'il présente un intérêt en soi, et *lemme* s'il n'a pas d'autre intérêt que d'être utilisé pour démontrer un théorème. Sans oublier bien sûr les *corollaires*, qui sont des conséquences plus ou moins immédiates d'un théorème.

Démonstration du lemme : on écrit la formule du binôme pour $n = p$ *premier* :

$$(a+b)^p = a^p + p\,a^{p-1}\,b + \frac{p\,(p-1)}{2}\,a^{p-2}\,b^2 + \ldots + \frac{p\,(p-1)}{2}\,a^2\,b^{p-2} + p\,a\,b^{p-1} + b^p$$

Tous les termes du développement autres que les termes extrêmes sont divisibles par p, ce qui donne la formule du lemme.

Théorème B (petit théorème de Fermat)

Soit p un nombre premier. Alors, pour tout entier x : $x^p \equiv x \pmod{p}$.

Autre formulation, équivalente bien sûr :

Soit p un nombre premier. Alors, pour tout entier x *non divisible par* p

$$x^{p-1} \equiv 1 \pmod{p}.$$

On peut imaginer beaucoup de démonstrations du petit théorème de Fermat. En voici une, basée sur la formule $(a+b)^p \equiv a^p + b^p \pmod{p}$ du lemme précédent :

$0^p \equiv 0$ et $1^p \equiv 1$, cela est évident et c'est un début...

Puis $2^p = (1+1)^p \equiv 1^p + 1^p \equiv 2$, et l'on voit la récurrence :
si $x^p \equiv x$, $(x+1)^p \equiv x^p + 1^p \equiv x + 1$, c'est gagné !

Pour les esprits curieux et familiers de la manipulation des congruences, on peut donner une autre démonstration :

On prend un entier x *non divisible par* p et on considère les deux ensembles
$E_1 = \{1, 2, 3, \ldots, p-1\}$ et $E_2 = \{x, 2x, 3x, \ldots, (p-1)\,x\}$.
Ces deux ensembles sont *égaux* ***modulo*** p. L'ensemble E_1 modulo p est trivialement constitué par *tous* les résidus possibles non nuls modulo p. Quant à l'ensemble E_2, tous ses éléments sont différents modulo p : on ne peut pas avoir $kx \equiv k'x \pmod{p}$, ce qui équivaudrait à $(k-k')\,x \equiv 0 \pmod{p}$ alors que $k-k'$ et x sont tous deux non nuls modulo p.

Conclusion
E_2 modulo p est lui aussi constitué par *tous* les résidus possibles non nuls modulo p (donnés dans un ordre différent), soit $E_1 \equiv E_2$ modulo p (il s'agit bien d'*égalité* d'ensembles). Donc le produit de tous les éléments de E_1 est égal au produit de tous les éléments de E_2 :
$1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \equiv x \cdot 2x \cdot 3x \cdot \ldots \cdot (p-1)\,x \pmod{p}$,
soit $1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \equiv (1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1))\,x^p \pmod{p}$.
On peut simplifier par $(p-1)!$ qui est premier avec p, et il reste $1 \equiv x^{p-1} \pmod{p}$.

Le petit théorème de Fermat possède un très grand nombre d'applications. Pour ce qui nous concerne (les polynômes), il nous *explique* pourquoi $P(x) = x^5 - x$ est toujours divisible par 5, en nous montrant que c'est une propriété arithmétique (et non pas algébrique) générale (et non pas particulière au degré 5).

Et si l'exposant n'est pas un nombre premier ?

↳ Cela nous entraînerait trop loin, en direction de l'« indicateur d'Euler ». Pour les courageux, je leur propose de démontrer *primo* que, si p est premier et x premier avec p, on a $x^{p(p-1)} \equiv 1 \pmod{p^2}$, $x^{p^2(p-1)} \equiv 1 \pmod{p^3}$, etc., *secundo* que, si p et q sont premiers et x premier avec pq, on a $x^{(p-1)(q-1)} \equiv 1 \pmod{pq}$.

Y a-t-il un grand théorème de Fermat ?

↳ Mais oui bien sûr...

On savait depuis les Grecs que $3^2 + 4^2 = 5^2$ $(9 + 16 = 25)$, que $12^2 + 5^2 = 13^2$ $(144 + 25 = 169)$, etc. Si on se réfère à l'équation générale $x^2 + y^2 = z^2$, on appelle cela des solutions d'une équation en nombres entiers (une équation « diophantienne » dans le jargon des mathématiciens – because Diophante d'Alexandrie (325 env. – 409) qui a étudié systématiquement ces problèmes).

Cette équation peut s'interpréter géométriquement : les 3 entiers x, y et z, qui constituent ce qu'on appelle parfois un « triplet de Pythagore », peuvent être pris comme les longueurs des côtés d'un triangle rectangle.

Si on prend un exposant 3 ou 4 ou plus, au lieu de l'exposant 2, l'interprétation géométrique n'est plus possible mais on rentre au cœur de la théorie des nombres. Fermat a énoncé en 1651 que l'équation diophantienne $x^n + y^n = z^n$, ne possédait, ***pour $n \geq 3$***, aucune solution entière non triviale (i.e. autre que $0^n + 0^n = 0^n$ ou $1^n + 0^n = 1^n$). Il a même affirmé qu'il savait le démontrer – mais il n'a pas donné sa démonstration (ou, c'est le plus vraisemblable, ce qu'il croyait être une démonstration). La démonstration de cette conjecture, abusivement appelée "grand" (ou "dernier") théorème de Fermat, recherchée avec passion par les professionnels et aussi par les amateurs pendant plus de 3 siècles, a été un extraordinaire ferment pour la recherche en théorie des nombres.

La démonstration, qui prend environ 200 pages, a été effectuée en 1994 par le mathématicien britannique Wiles (la conjecture s'appelle maintenant théorème de Fermat–Wiles) ; elle utilise des méthodes d'une grande abstraction et d'une haute technicité, complètement inconnues et même inimaginables à l'époque de Fermat.

IV – Les polynômes qui « donnent » des nombres premiers

Qui « donnent ... », qui « fournissent ... », qui « produisent ... », toutes ces expressions sont synonymes.

1772 : Euler

Vous connaissez « le » polynôme d'Euler : $P(x) = x^2 + x + 41$?

$P(0) = 41$ est un nombre premier, $P(1) = 43$ est un nombre premier, $P(2) = 47$ est un nombre premier, $P(3) = 53$ est un nombre premier, $P(4) = 61$ est un nombre premier, $P(5) = 71$ est un nombre premier, $P(6) = 83$ est un nombre premier, $P(7) = 97$ est un nombre premier, $P(8) = 113$ est un nombre premier, $P(9) = 131$ est un nombre premier, etc.

Et cœtera, ça veut dire quoi ? Que toutes les valeurs prises par $x^2 + x + 41$ sont des nombres premiers ? ... oui ? Vous avez perdu !! Il n'y a pas un seul polynôme qui ***ne*** donne ***que*** des valeurs premières (pour les valeurs entières de la variable, redisons-le encore). Nous l'avons déjà remarqué mais vous n'avez peut-être pas prêté suffisamment attention au passage : c'était le corollaire (appelé « utilisation n° 2 ») du théorème A.

Alors, finalement, le polynôme d'Euler ?

Quarante nombres premiers consécutifs, de $x = 0$ à $x = 39$. Vous pouvez vérifier... Et vous pouvez aussi vérifier que

$$P(40) = 40^2 + 40 + 41 = 40(40 + 1) + 41 = 41^2$$

n'est pas premier. Les petits malins remarqueront que

$$P(-1) = P(0), P(-2) = P(1), \ldots, P(-40) = P(39),$$

de sorte que le polynôme d'Euler fournit en réalité 80 nombres premiers, de $x = -40$ à $x = 39$. Mais ce n'est que du bégaiement, tous les nombres premiers sont donnés deux fois, alors on interdit cela dans la règle du jeu.

Peut-on faire mieux qu'Euler ?

La réponse est oui mais il a fallu attendre 1988 pour détrôner ce record : Fung a trouvé le polynôme $47x^2 + 9x - 5\,209$, qui fournit 43 nombres premiers consécutifs, de $x = -22$ à $x = -18$. Une remarque : l'expression "40 (ou 43) nombres premiers consécutifs" ne signifient pas qu'ils soient consécutifs dans la suite des nombres premiers mais que 40 (ou 43) valeurs du polynôme, obtenues pour 40 (ou 43) *valeurs consécutives de la variable*, sont des nombres premiers. Ce record a été battu l'année suivante par Ruby, avec le polynôme $36x^2 + 18x - 1\,801$, qui fournit 45 nombres premiers consécutifs, de $x = -33$ à $x = 11$.

Comment fait-on pour trouver des records ?

Le polynôme $16x^4 + 28x^3 - 1\,685x^2 - 23\,807x + 110\,647$, trouvé en 2000 par Dress et Landreau, fournit 46 nombres premiers consécutifs, de $x = -23$ à $x = 22$.

Comment fait-on pour trouver un tel polynôme ?

↳ Première idée de réponse : on essaye tous les polynômes

$$a_0x^4 + a_1x^3 + a_2x^2 + a_3x + a_4,$$

avec par exemple

$$|a_0| \le 50,\ |a_1| \le 500,\ |a_2| \le 5\,000,\ |a_3| \le 50\,000 \text{ et } |a_4| \le 500\,000,$$

et on teste la « primalité » de leurs valeurs entre $x = -100$ et $x = 100$.

Très mauvaise réponse !!

Cela fait $101 \cdot 1\,001 \cdot 10\,001 \cdot 100\,001 \cdot 1\,000\,001 \approx 1{,}011 \cdot 10^{20}$ polynômes à 201 valeurs chacun, soit environ $2{,}032 \cdot 10^{22}$ valeurs à calculer et à tester. Si vous mettez à 1 microseconde le temps de calcul et de test pour une valeur (ce n'est pas surestimé !), vous obtenez environ $2{,}032 \cdot 10^{16}$ secondes $\approx 2{,}352 \cdot 10^{11}$ jours ≈ 644 millions d'années.

Alors… la bonne réponse ?

↳ Ne tester qu'un infime partie des polynômes, en éliminant ceux qui sont des mauvais candidats parce qu'ils ont trop de « petits » diviseurs premiers périodiques. Si vous arrivez à éliminer 99.9999999 % des polynômes, c'est gagné ! … vous avez dit diviseurs premiers périodiques ?

Les « diviseurs premiers périodiques »

Nous allons tout expliquer sur un exemple.

Considérons un polynôme très simple et ressemblant au polynôme d'Euler, par exemple $P_7(x) = x^2 + x + 7$, et étudions sa divisibilité par les nombres premiers successifs 2, 3, 5, 7, 11, 13, …

Rappelons-nous le théorème A, il nous dit que *nous saurons tout* sur la divisibilité par p (premier) si nous regardons ce qui se passe pour p valeurs consécutives de la variable, par exemple $P(0)$, $P(1)$, $P(2)$, …, $P(p-1)$.

$P_7(0) = 7 \not\equiv 0,\ P_7(1) = 9 \not\equiv 0 \pmod 2$:

> P_7 n'est jamais divisible par 2, on dit que 2 n'est pas un diviseur premier périodique de P_7.

$P_7(0) = 7 \not\equiv 0,\ P_7(1) = 9 \equiv 0,\ P_7(2) = 13 \not\equiv 0 \pmod 3$:

> P_7 est parfois divisible par 3 (1 fois sur 3), on dit que **3** est un diviseur premier périodique de P_7.

$P_7(0) = 7 \not\equiv 0,\ P_7(1) = 9 \not\equiv 0,\ P_7(2) = 13 \not\equiv 0,\ P_7(3) = 19 \not\equiv 0,\ P_7(4) = 27 \not\equiv 0 \pmod 5$:

> P_7 n'est jamais divisible par 5, on dit que 5 n'est pas un diviseur premier périodique de P_7.

$P_7(0) = 7 \equiv 0,\ P_7(1) = 9 \not\equiv 0,\ \ldots,\ P_7(5) = 37 \not\equiv 0,\ P_7(6) = 49 \equiv 0 \pmod 7$:

> P_7 est parfois divisible par 7 (2 fois sur 7), on dit que *7* est un diviseur premier périodique de P_7.

etc.

On peut faire un petit programme pour rechercher les diviseurs premiers périodiques. Pour $P_7(x) = x^2 + x + 7$, on obtient 3, 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97, ... et, *a contrario*, pas 2, pas 5, pas 11, pas 17, pas 23, pas 29, pas 41, ...

Comment peut-on se servir des diviseurs premiers périodiques pour rechercher des polynômes record ? Encore un exemple... Oublions un instant le polynôme d'Euler avec ses 40 valeurs premières consécutives, et imaginons que nous recherchons modestement 10 valeurs premières consécutives. La méthode empirique est la suivante, étant donné un polynôme P, on regarde combien il y a de nombres premiers sur les 50 (50, pas 10) valeurs $P(0)$, $P(1)$, $P(2)$, ..., $P(49)$. S'il y en a beaucoup, il y a des chances d'en trouver 10 consécutives, s'il y en a peu, il n'y a quasiment aucune chance.

On essaye, avec $P_{17}(x) = x^2 + x + 17$, et $P_{19}(x) = x^2 + x + 19$:

diviseurs premiers périodiques de P_{17} :

17, 19, 23, 29, 37, 47, 59, 67, 71, 73, 83, ...

diviseurs premiers périodiques de P_{19} :

3, 5, 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, ...

P_{17} est un bon polynôme : aucun diviseur premier avant 17. P_{19} est une catastrophe : 1 valeur sur 3 sera divisible par 3, 2 sur 5 divisibles par 5, 2 sur 7 divisibles par 7, 2 sur 13 divisibles par 13, etc.

Vérification :

pour P_{17} : 15 valeurs premières sur 50 de $P_{17}(0)$ à $P_{17}(49)$,

pour P_{19} : 38 valeurs premières sur 50 de $P_{19}(0)$ à $P_{19}(49)$.

Voilà donc le principe : pour rechercher des polynômes record, on écrit un programme informatique qui utilise un « crible » sur les diviseurs premiers périodiques de façon à ***ne*** tester ***que*** des polynômes n'ayant que des "grands" diviseurs premiers périodiques. Principe simple, mise en œuvre délicate... et finalement des durées de calcul entre quelques semaines et quelques mois sur des « stations de travail » super-rapides !

Le record de Ruby a-t-il été battu ?

↳ Oui.

On ne trouvera vraisemblablement jamais de polynôme du *deuxième* degré qui dépasse 45 (Ruby). Par contre, il y a 8 polynômes de degré 4 qui fournissent 46 nombres premiers consécutifs, le plus simple est celui déjà donné plus haut $16\,x^4 + 28\,x^3 - 1\,685\,x^2 - 23\,807\,x + 110\,647$, de $x = -23$ à $x = 22$ (Dress et Landreau, Bordeaux, 2000). On a également trouvé un polynôme de degré 3 qui fournit 46 nombres premiers consécutifs : $66\,x^3 + 83\,x^2 - 13\,735\,x + 30\,139$, de $x = -26$ à $x = 19$ (Dress et Landreau, Bordeaux, 2001).

Souvenez-vous maintenant du début, il n'y a pas que les polynômes à coefficients entiers qui ne produisent que des entiers (pour les valeurs entières de la variable), il y a aussi des polynômes à coefficients rationnels non tous entiers. Pour des raisons qu'il serait trop compliqué d'expliquer, il n'y a aucune chance d'en trouver en degrés 2 ou 3, à nous les degrés supérieurs !

Et voici le grand record : le polynôme

$$\frac{1}{4}x^5 + \frac{1}{2}x^4 - \frac{345}{4}x^3 + \frac{879}{2}x^2 + 17\,500\,x + 70\,123$$

fournit **57** valeurs premières pour 57 valeurs consécutives de la variable, de $x = -27$ à $x = 29$ (Dress et Landreau, Bordeaux, 2003).

On peut qualifier les records précédents de records "n sur n", mais il y a aussi des records "k sur n" (avec $k < n$). Par exemple le polynôme $41\,x^2 + 33\,x - 43\,321$: 90 valeurs premières sur 100 valeurs consécutives de la variable, de $x = -57$ à $x = 42$ (Boston et Greenwood, 1995), et le polynôme $x^2 + x - 1\,354\,363$ (Dress et Olivier, Bordeaux, 1998) : 698 valeurs premières (différentes) sur 1 000 valeurs consécutives de la variable, de $x = 1\,139$ à $x = 2\,138$.

François DRESS, Université Bordeaux 1

mailto:dress@math.u-bordeaux.fr

dernière mise à jour : 31 mai 2004