Lycée Bascan de Rambouillet
Introduction à l'exposé de Daniel Perrin
Fermat, Mersenne, factorisation et nombres parfaits à la BNF,
conférences *Un texte, un mathématicien.*
14 mars 2018.

Premiers et parfaits, notes d'exposé

1 Nombres premiers, décomposition des nombres

Définition d'un nombre premier, début de la liste.
Comment les reconnaître ? Eratosthène et $\sqrt{n}$ [en passant, critères de divisibilité par $2, 3, (4), 5, (9), 11, (25)$].

Théorème fondamental de l'arithmétique, fondé sur la division euclidienne : tout nombre entier naturel se décompose *de manière unique* en un produit de nombres premiers.
Commentaire sur la primalité des nombres : test algorithmiquement très coûteux, évocation de RSA.

Retour à l'énigme. Réactions aux réponses des élèves. Maple, limites des machines (mêmes performantes).

2 Une application : les triplets pythagoriciens

[Intervention du théorème fondamental de l'arithmétique et de la géométrie]
Triplets pythagoriciens (triangles rectangles à côtés entiers), dont le célèbre $3, 4, 5$ des maçons ; en trouver d'autres ? Les trouver tous ?

Pour trouver les solutions entières de $x^2 + y^2 = z^2$, on peut réduire l'étude au cas où $x, y, z \geq 1$ et sont deux à deux premiers entre eux.

Diviser par z^2, utiliser la paramétrisation unicursale du cercle $c = \frac{1-t^2}{1+t^2}$, $s = \frac{2t}{1+t^2}$, se convaincre que $c, s \in \mathbb{Q}$ si, et seulement si $t \in \mathbb{Q}$.
[Si c est rationnel, t^2 est rationnel ; si s est aussi rationnel, t l'est également.]
On obtient un infinité de solutions, toutes décrites à partir des $t = \frac{p}{q}$, fractions irréductibles :

$$(x, y, z) = (p^2 - q^2, 2pq, p^2 + q^2),$$

quitte à diviser par 2 (les pgcd deux à deux de ces trois nombres sont simultanément 1 ou 2 ; le voir en supposant qu'un nombre premier divise deux d'entre eux : il vaut 2 ou est diviseur commun de p et q).

Quelques exemples. Maple.

3 Nombres de Mersenne

[Sont intervenus dans la course aux nombres premiers]
Nombre de Mersenne : ce sont les nombres de la forme $M_n = 2^n - 1$.

Si $n = ab$, alors $2^n - 1$ est divisible par $2^a - 1$ ce qui empêche M_{ab} d'être premier.
[Partir de la formule $X^b - 1 = (X - 1)(X^{b-1} + \cdots + X + 1)$, substituer X^a à X.]
Ainsi, les nombre de Mersenne premiers sont à rechercher parmi les $2^p - 1$ où p est premier.

Essais, tableau des premiers nombres de Mersenne de la forme $2^p - 1$:

p	$2^p - 1$	factorisation de $2^p - 1$
2	3	**3**
3	7	**7**
5	31	**31**
7	127	**127**
11	2047	23×89
13	8191	**8191**
17	131071	**131071**
19	524287	**524287**
23	8388607	47×178481
29	536870911	$233 \times 1103 \times 2089$
31	2147483647	**2147483647**
37	137438953471	223×616318177
41	2199023255551	13367×164511353
43	8796093022207	$431 \times 9719 \times 2099863$
47	140737488355327	$2351 \times 4513 \times 13264529$
53	9007199254740991	$6361 \times 69431 \times 20394401$
59	576460752303423487	$179951 \times 3203431780337$
61	2305843009213693951	**2305843009213693951**
67	147573952589676412927	$193707721 \times 761838257287$
71	2361183241434822606847	$228479 \times 48544121 \times 212885833$
73	9444732965739290427391	$439 \times 2298041 \times 9361973132609$
79	604462909807314587353087	$2687 \times 202029703 \times 1113491139767$
83	9671406556917033397649407	$167 \times 57912614113275649087721$
89	618970019642690137449562111	**618970019642690137449562111**
97	158456325028528675187087900671	$11447 \times 13842607235828485645766393$
etc		

On ne sait pas si l'ensemble des nombres de Mersenne premiers est fini.

4 Nombres parfaits

[Une (autre) question ouverte très simple à énoncer.]
Définition d'un nombre parfait : la somme des diviseurs égale le double.

Euclide : si $2^p - 1$ est premier, alors $2^{p-1}(2^p - 1)$ est (pair et) parfait. [Preuve.]
Euler : si n est pair et parfait, il est de la forme $\frac{M_p(M_p+1)}{2}$ ci-dessus.

[Une preuve : soit $n = 2^v m$ un nombre parfait, où $v \geq 1$ et m impair. Les diviseurs de n sont les $2^w d$ où $0 \leq w \leq v$ et où d est un diviseur (nécessairement impair) de m. On note $\sigma(x)$ la somme des diviseurs de l'entier naturel non nul x. Ainsi, $\sigma(n) = \left(2^{v+1} - 1\right)\sigma(m) = 2n = 2^{v+1}m$. On retient de cela que $\frac{\sigma(m)}{m} = \frac{2^{v+1}}{2^{v+1}-1}$. Comme cette dernière fraction est irréductible, si D est le pgcd de m et de $\sigma(m)$, on obtient que $\sigma(m) = D2^{v+1}$ et $m = D\left(2^{v+1} - 1\right)$. En particulier, $\sigma(m) = m + D$. Or, parmi les diviseurs de m, figurent $m \neq 1$, D et 1 qui ne peuvent donc pas être distincts. Cela impose que $D = 1$, ce qui prouve que $m = 2^{v+1} - 1$ est un nombre premier ($\sigma(m) = m + 1$) de Mersenne et que n est de la forme attendue.]

On ne sait pas si l'ensemble des nombres parfaits pairs est fini (c'est la même question que plus haut !). Le début de la liste des nombres parfaits : 6, 28, 496, 8128, 33550336, 8589869056, 137438691328, 2305843008139952128, 2658455991569831744654692615953842176, *etc.*
On ne sait pas s'il existe des nombres parfaits impairs, mais on a montré[1] qu'il n'en existe aucun qui soit inférieur à 10^{1500}.

[1] P. Ochem et M. Rao, 2012.