Développement : Somme de deux carrés

1. Historique : — *Énoncé par Fermat en 1640 et démontré une première fois par Euler, ce théorème compte beaucoup de démonstrations différentes et intéressante, dont la "one-sentence proof" de Zagier et une très récente (2016) par des considérations de partitionnement. Nous prenons ici une preuve apportée par A. Thue en 1902.*

2. Lemme 1. — *Énoncé* : L'équation $s^2 \equiv -1\,(p)$, pour p premier admet :

- Une solution (triviale) si $p = 2$
- Deux solutions si si $p \equiv 1\,(4)$
- Aucune solution si $p \equiv 3\,(4)$

Démonstration :

- Évident pour $n = 2$ où $-1 = 1$
- On considère désormais que $p > 2$ et on se place dans $\mathbb{Z}/p\mathbb{Z}*$ (de cardinal $p-1$).
- A chaque x on fait correspondre les quatre éléments suivants *éventuellement répétés* : $x, -x, x^{-1}, -x^{-1}$
- $x = -x$ est impossible car la caractéristique n'est pas 2.
- $x = x^{-1}$ a toujours deux uniques solutions $x = 1$ et $x = -1 = p-1$
- Enfin, $x = -x^{-1}$ (ie $x^2 = -1$) peut avoir deux solutions (notées x_0 et $p - x_0$) ou aucune solution.
- Les classes d'équivalences sont alors $\{1, -1\}$, $\{x_0, -x_0\}$, les autres quadruplets distincts.
- Lorsque nous avons une paire (x_0, $p - x_0$), nous avons donc $p - 1 = 2 + 2 + 4k$ et donc $p \equiv 1\,(4)$.
- Lorsque nous n'avons pas de paire (x_0, $p - x_0$), nous avons donc $p - 1 = 2 + 4k$ et donc $p \equiv 3\,(4)$.

3. Applications au passage. —

- Rem : on vient de montrer que les diviseurs premiers impairs de tout nombre M^2+1 sont congrus à 1 modulo 4. Il y a donc une infinité de tels nombres premiers car si p_k en était le plus grand élément, $(\Pi_{1\leq j\leq k}\, p_k)^2 + 1$ exhiberait une contradiction.
- Rem : on peut construire plus simplement une contradiction à un ppe des premiers congrus à 3 modulo 4, ppe que l'on noterait encore p_k en s'appuyant sur $2^2\Pi_{1\leq j\leq k}\, p_k - 1$
- $x^2 + y^2 \equiv -1\,(p)$ a toujours une solution si p est premier. En effet :
  - lorsque x, y balayent $\mathbb{Z}/p\mathbb{Z}^*$, x^2 et $1 - y^2$ balayent chacun $E(p/2)+1$ éléments distincts.
  - Ces deux sous-ensembles ne sauraient être disjoints puisqu'inclus dans $\mathbb{Z}/p\mathbb{Z}^*$ qui a $p-1$ éléments.

4. Lemme 2 : impossibilité pour p premier congru à 3 modulo 4. — *Démonstration* :

- Sq $p = a^2 + b^2$.
- Si a est pair, $a^2 \equiv 0\,(mod : 4)$ et idem pour b
- Si a est impair, $a^2 = (2k+1)^2 = 4k^2 + 4k + 1$, donc $a \equiv 1\,(mod : 4)$ et idem pour b.
- Nous avons donc 3 possibilités de résidu en sommant a^2 et b^2 : $0+0=0$, $0+1=1$ et $1+1=2$
- Comme p est premier, la seule possibilité est 1. C'est une condition nécessaire.
- CQFD

5. Lemme 3 : existence pour p premier congru à 1 modulo 4. — *Énoncé* : Tout nombre premier congru à 1 modulo 4 est la somme de deux carrés. *Démonstration* :

- Considérons l'ensemble des paires $z_1, z_2 \in \{0, 1, 2, \cdots, E(\sqrt{p})\}$
- Nous avons $(E(\sqrt{p})+1)^2$ valeurs possibles.
- Comme $\forall x$, $E(x)+1 > x$, on plus de p paires et donc, $\forall s \in \mathbb{Z}$, la famille des $z_1 - sz_2$ aura au moins un doublon modulo p.
- Soient x_1, y_1 et x_2, y_2 un de ces doublons, vérifiant donc que au moins une des deux valeurs $(x_1 - x_2)$ ou $(y_1 - y_2)$ est non nulle.
- On a donc $x_1 - sy_1 \equiv x_2 - sy_2\,(mod : p)$, avec $x_1, y_1, x_2, y_2 \in \{0, 1, 2, \cdots, E(\sqrt{p})\}$.
- Et donc aussi $(x_1 - x_2) \equiv s(y_1 - y_2)\,(mod : p)$.
- En posant $x = |x_1 - x_2|$ et $y = |y_1 - y_2|$, on a toujours $x, y \in \{0, 1, 2, \cdots, E(\sqrt{p})\}$ et on a $x \equiv \pm sy\,(mod : p)$.
- Et donc aussi : $x^2 \equiv s^2 y^2$
- Comme $p \equiv 1\,(mod : 4)$, le lemme 1 s'applique et prenons s solution à $s^2 \equiv -1\,(mod : p)$.
- Nous avons donc $x^2 \equiv -y^2\,(mod : p)$ ie $\exists k x^2 + y^2 = kp$
- Mais $0 < x^2 + y^2 < 2p$ donc forcément $x^2 + y^2 = p$
- CQFD

6. Théorème : condition d'existence de deux carrés dont la somme fait n. — *Énoncé* : Un nombre entier est la somme de deux carrés ssi la valuation p-adique pour les facteurs premiers congrus à 3 modulo 4 est paire.

Démonstration : nous parlerons de 'représentable' lorsqu'une somme de deux carrés existe.

Condition Suffisante :

- 1 et 2 sont représentables : $1 = 1^2 + 0^2$ et $2 = 1^2 + 1^2$
- Les nombres premiers de la forme $4k+1$ aussi (cf lemme 3).
- Le produit de deux nombres représentables l'est aussi. En effet, si $n_1 = a_1^2 + b_1^2$ et $n_2 = a_2^2 + b_2^2$, $n_1 n_2 = (a_1 a_2 + b_1 b_2)^2 + (a_1 b_2 - a_2 b1)^2$
- Si n est représentable, nz^2 l'est aussi.
- Condition Suffisante : les règles précédentes permettent de calculer la décomposition de proche en proche lorsque la condition est vérifiée (à condition de résoudre les $4k+1$ nécessaires).
- Exe : $90 = 2*3*3*5$. $2 = 1+1; 5 = 4+1$. Donc $2\times 5 = (1.2+1.1)^2 + (1.1-1.2)^2 = 3^2 + 1^2$. Puis $9^2 + 3^2 = 90$.

Condition Nécessaire :

- Sq $n = x^2 + y^2$ et que $\exists p = 4m + 3$ divisant n, ie $n \equiv 0\,(mod : p)$.
- Mq $p|x$. Dans le cas contraire, x est inversible dans $\mathbb{Z}/p\mathbb{Z}$ et alors en multipliant par $(x^{-1})^2$, on obtient $0 \equiv (1 + (xy)^2)\,(mod : p)$, ce qui est impossible (cf "Applications au passage").
- Donc $p2|x^2$
- Pour les mêmes raisons, $p^2|y^2$.
- Et donc $p^2|n$, CQFD.

Leçons

- Equations diophantiennes
- Dénombrements

) *Sources : D. Perrin - Proofs from THE BOOK*

December 16, 2017

Bruno Nitrosso, EPP et candidat libre