Semaine 11 - Arithmétique dans $\mathbb{Z}$

Valentin De Bortoli
email : valentin.debortoli@gmail.com

1 Carrés parfaits

1 Le tableau suivant récapitule les valeurs de m modulo 8 et celles de m^2 qui découlent :

0	1	2	3	4	5	6	7
0	1	4	1	0	1	4	1

Donc aucun nombre de la forme $8n+k$ avec $k \in \{2,3,5,6,7\}$ ne peut être un carré parfait. $N = (n-2)^2 + (n-1)^2 + n + (n+1)^2 + (n+2)^2 = 5n^2 + 10 = 5(n^2+2)$. Donc 5 divise N et donc 5^2 aussi. Ce qui signifie que $n^2 = 5m + 3$ avec $m \in \mathbb{N}$.

0	1	2	3	4
0	1	4	4	1

2 Implication et primalité

Soit p un nombre premier.

1 On écarte le cas $p = 3$. Dans les autres cas, p est congru à un ou deux modulo trois. Si il est congru à un alors $8p^2 + 1$ est divisible par trois et donc non premier. Si il est congru à deux alors $8p^2 + 1$ est encore divisible par trois donc non premier. Donc le seul cas qu'il reste est $p = 3$. Dans ce cas $8 \times 9 + 1 = 73$ qui est premier tout comme 71.

3 Puissance et nombres premiers entre eux

1 On raisonne par récurrence. Au rang un la propriété est triviale. Pour l'hérédité on considère

$$\begin{aligned}(1+\sqrt{2})^{n+1} &= (1+\sqrt{2})(a_n + b_n\sqrt{2}) \\ &= a_n + 2b_n + (a_n + b_n)\sqrt{2}\end{aligned}$$

Ainsi $(a_n, b_n) \in \mathbb{N}^2$.

2 Encore une fois procédons par récurrence. C'est vrai au rang un. Ensuite on considère $(a_n + 2b_n) \wedge (a_n + b_n) = b_n \wedge (a_n + b_n) = \wedge b_n \wedge a_n = 1$.

4 Équations et arithmétique

1 Résoudre dans $\mathbb{Z}^2$ les équations suivantes :

1

$$\begin{cases} x + y = 56 \\ x \vee y = 105 \end{cases}$$

2

$$\begin{cases} x \wedge y = x - y \\ x \vee y = 72 \end{cases}$$

3 $x \vee y - x \wedge y = 243$

5 Nombres de Fermat

1 Si $m = qr$ avec q impair alors $-2^m = ((-2^r))^q$ et donc $1 + 2^m = 1 - ((-2^r))^q$. Ainsi N est divisible par $1 + 2^r$.

2 Soit $m > n$ et p un diviseur premier de F_n. On a $2^{2^n} = -1[p]$. Supposons que p est aussi un diviseur premier de F_m alors on a aussi $2^{2^m} = -1[p]$. Mais $2^{2^m} = \left(2^{2^n}\right)^{2^{m-n}}$ avec 2^{m-n} qui est pair et donc $2^{2^m} = 1[p]$. Ainsi $A = -1[p]$ ce qui est valide si et seulement si $p = 2$ or il est évident que 2 ne divise pas F_n.

3 $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$. Ces nombres sont effectivement premiers. Fermat avait conjecturé que tous les F_n étaient premiers. Euler a réfuté cette conjecture. En effet $F_5 = 65537$ est divisible par 641. On a depuis réussi à montrer que tous les nombres de Fermat de F_5 à F_32 sont composés. On ignore tout de F_{33} et des suivants (il faut bien se rendre compte que ce sont là des nombres prodigieusement grands et qu'il est inenvisageable de les stocker sur ordinateurs. Par exemple F_{33} s'écrit en base décimale avec plus de mille milliards de chiffres...). On pense que c'est cette conjecture qui a poussé Fermat à penser qu'il possédait une démonstration de son grand théorème (voir remarque de l'exercice 7). Malgré l'échec de cette conjecture les nombres de Fermat sont très utiles. Par exemple les seuls polygones réguliers à n côtés constructibles à la règle et au compas sont ceux tels que n est une puissance de deux ou une puissance de deux multipliée par des nombres de Fermat distincts (théorème de Gauss-Wantzel).

1 Soit $N = 2^m + 1$. Montrer que si N est premier alors m est une puissance de 2.

2 On note $F_n = 2^{2^n} + 1$ le n-ième nombre de Fermat. Montrer que deux nombres de Fermat distincts sont premiers entre eux.

3 A votre avis, ces nombres sont-ils premiers ?

6 Nombres de Mersenne

1 Soit $N = a^m - 1$. Montrer que si N est premier alors $a = 2$ et m est un nombre premier

2 On note $M_n = 2^{p_n} - 1$ le n-ième nombre de Mersenne (où p_n est une énumération des nombres premiers). Montrer que deux nombres de Mersenne distincts sont premiers entre eux.

Remarque : les plus grands nombres premiers trouvés à ce jour sont des nombres de Mersenne. En cette fin de décembre 2016 le plus grand nombre premier identifié est un nombre de Mersenne. Il comporte 22 338 618 chiffres (projet GIMPS).

7 Triplets pythagoriciens

On appelle triplet pythagoricien tout triplet $(x, y, z) \in \mathbb{Z}^3$ tel que $x^2 + y^2 = z^2$.

1 Exhiber un tel triplet.

2 Montrer que l'on peut se restreindre au cas où x, y et z sont premiers entre eux dans leur ensemble.

3 Montrer qu'alors ils sont premiers entre eux deux à deux.

4 Dans ce cas, montrer que deux sont impairs et que z est impair. On suppose alors que $y = 2y'$ et x et z impairs.

5 On pose $X = \frac{x+z}{2}$ et $Z = \frac{z-x}{2}$. Montrer que $X \wedge Z = 1$ et que X et Z sont des carrés parfaits.

6 En déduire l'ensemble des triplets pythagoriciens.

Remarque : il n'existe pas de solutions si l'exposant est strictement supérieur à 2. Il s'agit du grand théorème de Fermat que celui-ci pensait avoir montré. Une démonstration rigoureuse a été donnée par Wiles en 1995 après de nombreuses années de recherche.

8 Factorielle et arithmétique

1 Soit $k \in [\![0, n]\!]$, montrer que $\binom{n}{k}$ est un entier.

2 Soit $k \wedge n = 1$ montrer que n divise $\binom{n}{k}$.

3 Soit p un nombre premier. Montrer que $\forall k \in [\![0, p-1]\!]$, p divise $\binom{p}{k}$.

9 Suite de Fibonacci et arithmétique

On considère la suite de Fibonacci définie par $u_0 = 0$, $u_1 = 1$ et $u_{n+2} = u_{n+1} + u_n$.

1 Montrer que $u_{n+1}u_{n-1} - u_n^2 = (-1)^n$. En déduire que $u_{n+1} \wedge u_n = 1$ si $n \in \mathbb{N}^*$.

2 Montrer que $\forall (m, n) \in \mathbb{N}^* \times \mathbb{N},\ u_{m+n} = u_{m-1}u_n + u_m u_{n+1}$. On pourra commencer par le cas $m = 1$ et le cas $m = 2$ puis raisonner par récurrence.

3 En déduire que $u_n \wedge u_m = u_{n \wedge m}$.

10 Exo Ulm