Arithmétique dans $\mathbb{Z}$

1 Questions de cours

1. Montrer que tout entier est produit de nombre premier.
2. Montrer que les sous-groupes de $\mathbb{Z}$ sont exactement les $n\mathbb{Z}$.
3. Soient $a_1, \ldots, a_n$ des entiers premiers entre eux deux à deux, et b un entier.
   Montrer que $\forall i \in \{1, \ldots, n\},\ a_i \mid b$ *si et seulement si* $a_1 \cdots a_n \mid b$.

2 Applications

1. Déterminer le pgcd de 33 et 24, et établir une relation de Bezout.
2. Déterminer le pgcd de 37 et 27, et établir une relation de Bezout.
3. Déterminer le pgcd de 270 et 105, et établir une relation de Bezout.

3 Exercices

1. Soit p un nombre premier.
   Montrer que $\forall k \in [\![1, p-1]\!],\ p \mid \binom{p}{k}$, et en déduire que
   $$\forall n \in \mathbb{Z},\ p \mid n^p - n.$$
2. Montrer qu'il existe 1000 entiers consécutifs non premiers. Généraliser.
3. Soit p un nombre premier $\geqslant 5$. Montrer que $p^2 - 1$ est divisible par 24.
4. Montrer que $\sqrt{2}$ n'est pas un nombre rationnel.
5. Soit $n \in \mathbb{N}$. Montrer que les entiers
   $$a_i = i \times n! + 1,\ i \in [\![1, n+1]\!]$$
   sont deux à deux premiers entre eux.
6. On appelle *partition* d'un ensemble E un ensemble $P = \{A_i \mid i \in I\}$, où
   – I est un ensemble ;
   – $A_i \subseteq E$;
   – $\forall i \neq j \in I,\ A_i \cap A_j = \emptyset$;
   – $\bigcup_{i \in I} A_i = E$.
   Donner une partition $\{A_i \mid i \in \mathbb{N}\}$ de $\mathbb{N}$ où chaque A_i est infini.

7. Soit $(F_n)_n$ la suite de Fibonacci, définie par $F_0 = 0, F_1 = 1$ et

$$\forall n \in \mathbb{N},\ F_{n+2} = F_{n+1} + F_n.$$

(i) Montrer que pour tout entier $n > 0$,

$$F_{n+1}F_{n-1} - F_n^2 = (-1)^n.$$

En déduire que F_n et F_{n+1} sont premiers entre eux.

(ii) Montrer que pour tous $n > 0$ et $p \in \mathbb{N}$, on a

$$F_{n+p} = F_pF_{n+1} + F_{p-1}F_n.$$

En déduire que

$$\text{pgcd}(F_n, F_p) = \text{pgcd}(F_{n+p}, F_p).$$

(iii) Montrer que

$$\forall (n,p) \in \mathbb{N}^2,\ \text{pgcd}(F_n, F_p) = F_{\text{pgcd}(n,p)}.$$

8. Soit $n \in \mathbb{N}$.

(i) Montrer qu'il existe un unique couple $(a_n, b_n) \in \mathbb{N}^2$ tel que

$$(1+\sqrt{2})^n = a_n + b_n\sqrt{2}.$$

On explicitera a_n et b_n.

(ii) Montrer que a_n et b_n sont premiers entre eux.

4 Corrections

4.1 Applications

1. On a $24 \wedge 33 = 3$ et $3 \times 33 - 4 \times 24 = 3$.
2. On a $37 \wedge 27 = 1$ et $-11 \times 37 + 11 \times 27 = 1$.
3. On a $270 \wedge 105 = 15$ et $2 \times 270 - 5 \times 105 = 15$.

4.2 Exercices

1. (a) On a
$$\binom{p}{k} = \frac{p}{k}\binom{p-1}{k-1},$$
d'où
$$k\binom{p}{k} = p\binom{p-1}{k-1}.$$
Or p est premier et $k < p$ sont $k \wedge p = 1$, et donc par théorème de Gauß
$$p \mid \binom{p}{k}.$$

   (b) Par récurrence sur n :
   $n = 0$: C'est bon.
   $n \to n+1$: On a
$$(n+1)^p - n - 1 = n^p - n + \sum_{k=1}^{p-1} \binom{p}{k} n^k.$$
   Par la question précédente, p divise la somme, et p divise $n^p - n$ par hypothèse de récurrence.

2. On pose pour tout $k \in \{2, \ldots, 1001\}$
$$x_k = 1001! + k.$$
Les x_k sont 1000 entiers consécutifs, et pour tout $k \in \{2, \ldots, 1001\}$ on a $k \mid x_k$. Donc les x_k ne sont pas premiers. On généralise en posant $x_k = (n+1)! + k$.

3. On a $p^2 - 1 = (p-1)(p+1)$. Comme p est impair, $p-1$ et $p+1$ sont deux entiers pairs consécutifs, et donc l'un est divisible par 2, l'autre par 4. Donc $8 \mid p^2 - 1$.
   De plus, $p-1, p, p+1$ sont trois entiers consécutifs, et donc l'un d'eux est divisible par 3 ; comme p est premier $\geqslant 5$, ça ne peut pas être p. Donc $3 \mid p^2 - 1$.
   Comme 3 et 8 sont premiers entre eux,
$$3 \times 8 = 24 \mid p^2 - 1.$$

4. Supposons que $\sqrt{2}$ est rationnel : on a p et q deux entiers positifs premiers entre eux, $q \neq 0$ tels que
$$\sqrt{2} = \frac{p}{q}.$$
Mais alors $2q^2 = p^2$, et donc p est pair. On écrit $p = 2k$.
On a alors $4k^2 = 2q^2$, et donc $2k^2 = q^2$. Donc q^2 et donc q est aussi pair, ce qui contredit $p \wedge q = 1$.

5. Supposons qu'il existe i et j distincts tels que a_i et a_j ne soient pas premiers entre eux : ils ont un diviseur commun premier, soit d. Alors
$$d \mid a_i - a_j = (i-j) \times n!.$$
Donc comme d est premier, d divise $i - j$ ou d divise $n!$. En particulier $d \leqslant n$, et donc $d \mid n!$. Comme $d \mid i \times n! + 1$, on a aussi $d \mid 1$. D'où une contradiction.

6. Soit $(p_i)_{i\in\mathbb{N}}$ une énumération croissante des nombres premiers. On pose pour tout $i \in \mathbb{N}$
$$A_i = \{p_0^{a_0} \times \cdots \times p_i^{a_i} \mid a_0, \ldots, a_i \in \mathbb{N},\ a_i \geqslant 1\}$$
(on rajoute 0 et 1 dans n'importe lequel des A_i, par exemple A_0).
On a, d'après le théorème de décomposition unique en nombre premiers, $\cup_i A_i = \mathbb{N}$. De plus, soient i et j deux entiers distincts, par exemple $i > j$. Supposons $A_i \cap A_j \neq \emptyset$, et soit alors $x \in A_i \cap A_j$.
Alors on peut écrire x de deux façons
$$x = p_0^{a_0} \times \cdots \times p_i^{a_i} = p_0^{b_0} \times \cdots \times p_j^{b_j}.$$
Mais alors x est à la fois un multiple de p_i et non un multiple de p_i. D'où une contradiction.

7. (i) On montre la relation par récurrence sur n. En posant $U_n = (-1)^n F_{n-1}$, on a
$$U_{n+1}F_n + U_n F_{n+1} = 1,$$
et on conclut par théorème de Bezout.

   (ii) On montre la relation par récurrence sur n. Puis, on montre que $\mathscr{D}(F_n, F_p) = \mathscr{D}(F_{n+p}, F_p)$.
   ($\subseteq$) : Si d divise F_n et F_p, d'après la relation juste montrée, d divise F_{n+p}.
   ($\supseteq$) : Soit d un diviseur de F_p et F_{n+p}. Alors d divise aussi $F_{p-1}F_n$, et comme F_p et F_{p-1} sont premiers entre eux, d et F_{p-1} sont premiers entre eux. Par théorème de Gaußon a donc d divise F_n.

   (iii) Soient m et n deux entiers, $n \neq 0$. On écrit la division euclidienne de m par n :
$$m = nq + r,\ 0 \leqslant r \leqslant n-1.$$

En itérant le résultat de la question précédente, on a

$$\begin{aligned}\mathrm{pgcd}(F_n, F_r) &= \mathrm{pgcd}(F_n, F_{r+n}) \\ &= \cdots \\ &= \mathrm{pgcd}(F_n, F_{r+nq}) \\ &= \mathrm{pgcd}(F_n, F_m)\end{aligned}$$

Considérons $d = \mathrm{pgcd}(m, n)$, et $a_0 \geqslant a_1 \geqslant \cdots > a_m = d > 0$ la suite des restes non nuls dans l'algorithme d'Euclide. On a

$$\begin{aligned}\mathrm{pgcd}(F_m, F_n) &= \mathrm{pgcd}(F_{a_0}, F_{a_1}) \\ &= \mathrm{pgcd}(F_{a_1}, F_{a_2}) \\ &= \cdots \\ &= \mathrm{pgcd}(F_{a_m}, 0) \\ &= F_{\mathrm{pgcd}(m,n)}\end{aligned}$$

8. (i) Pour l'unicité, c'est évident. Pour l'existence :

$$\begin{aligned}(1+\sqrt{2})^n &= \sum_{k=0}^{n} \binom{n}{k} (\sqrt{2})^k \\ &= \sum_{l=0}^{E(n/2)} \binom{n}{2l} 2^l + \sqrt{2} \times \sum_{l=0}^{E((n-1)/2)} \binom{n}{2l+1} 2^l\end{aligned}$$

(ii) On peut refaire le calcul précédent et montrer que

$$(1-\sqrt{2})^n = a_n - b_n\sqrt{2}.$$

On a donc en multipliant $(1-\sqrt{2})^n \times (1+\sqrt{2})^n$:

$$(-1)^n = a_n^2 - 2b_n^2,$$

c'est-à-dire, en posant $u_n = (-1)^n a_n$ et $v_n = 2 \times (-1)^{n+1} b_n$:

$$a_n u_n + b_n v_n = 1.$$

Par théorème de Bezout, on a $a_n \wedge b_n = 1$.