Rudiments d'arithmétique

Exercice 3.

Essayer de réécrire les équations pour obtenir des formes factorisées (par exemple, la première peut être mise sous forme $ab = 6$).

Exercice 4.

Un diviseur commun à $n^2 + n$ et $2n + 1$ est nécessairement diviseur de tous les nombres de la forme $u(n^2 + n) + v(2n + 1)$: on peut alors choisir u et v de façon à obtenir plus de renseignements sur le diviseur.

Exercice 19.

On pourra commencer par montrer que si (x, y) est une solution telle que $x \leqslant y$ alors $x \mid y$.

Autocorrection

Autocorrection A.

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

(i) n est un multiple de 2 si et seulement si son dernier chiffre est 0, 2, 4, 6 ou 8 ;

(ii) n est un multiple de 3 si et seulement si la somme de ses chiffres est un multiple de 3 ;

(iii) n est un multiple de 4 si et seulement si le nombre obtenu en gardant ses deux derniers chiffres est un multiple de 4 ;

(iv) n est un multiple de 5 si et seulement si son dernier chiffre est 0 ou 5 ;

(v) n est un multiple de 8 si et seulement si le nombre obtenu en gardant ses trois derniers chiffres est un multiple de 8 ;

(vi) n est un multiple de 9 si et seulement si la somme de ses chiffres est un multiple de 9.

(vii) n est un multiple de 10 si et seulement si son dernier chiffre est 0 ;

(viii) n est un multiple de 11 si et seulement si la somme alternée de ses chiffres l'est.

On note $c_0, c_1, \ldots, c_r$ les chiffres de n, lus de droite à gauche. On a donc l'égalité

$$n = \sum_{i=0}^{r} c_i\, 10^i.$$

- On a l'égalité
$$n = c_0 + 10 \times \underbrace{\left(\sum_{i=1}^{r} c_i\, 10^{i-1}\right)}_{\in \mathbb{N}},$$
donc n est divisible par 2, 5 ou 10 si et seulement si c_0 l'est, ce qui démontre les points (i), (v) et (vii).
- On a l'égalité
$$n = (c_0 + 10\, c_1) + 100 \times \underbrace{\left(\sum_{i=2}^{r} c_i\, 10^{i-2}\right)}_{\in \mathbb{N}},$$
donc n est divisible par 4 si et seulement si $c_0 + 10\, c_1$ l'est, ce qui démontre le point (iii).

- On montre de la même façon le critère de divisibilité par 8 (et même par toute puissance de 2).
- On a $10 \equiv 1 \pmod 9$ et donc modulo 3, donc $n \equiv \sum_{i=0}^{r} c_i \pmod 9$ (et donc modulo 3).

  En particulier, n est divisible par 3 ou 9 si et seulement si $\sum_{i=0}^{r} c_i$ l'est, ce qui démontre les points (ii) et (vi).
- On a $10 \equiv -1 \pmod{11}$, donc $n \equiv \sum_{i=0}^{r} (-1)^i c_i$, ce qui démontre (viii) de la même façon.

Les critères montrent facilement que 14 652 est divisible par 4, 9 et 11, et donc par $4 \times 9 \times 11 = 396$. En posant la division, $14\,652 = 396 \times 37$.

Comme 37 est premier, on obtient $14\,652 = 2^2 \times 3^2 \times 11 \times 37$.

Autocorrection B.

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

(i) L'égalité $n+3 = (n+1)+2$ permet d'écrire la première équivalence de la chaîne d'équivalences

$$\begin{aligned} n+1 \mid n+3 &\Leftrightarrow n+1 \mid 2 \\ &\Leftrightarrow n+1 \in \{1,2\} \\ &\Leftrightarrow n \in \{0,2\}. \end{aligned}$$

(ii) L'égalité $n^2+3n+8 = (n+2)(n+1)+6$ permet d'écrire la première équivalence de la chaîne d'équivalences

$$\begin{aligned} n+2 \mid n^2+3n+8 &\Leftrightarrow n+2 \mid 6 \\ &\Leftrightarrow n+2 \in \{1,2,3,6\} \\ &\Leftrightarrow n+2 \in \{2,3,6\} && \text{car } n \geqslant 0 \\ &\Leftrightarrow n \in \{0,1,4\}. \end{aligned}$$

Autocorrection C.

(i) On a

$$\begin{aligned} 438 &= 8 \times 51 + 30 && (1) \\ 51 &= 1 \times 30 + 21 && (2) \\ 30 &= 1 \times 21 + 9 && (3) \\ 21 &= 2 \times 9 + 3 && (4) \\ 9 &= 3 \times 3 + 0, \end{aligned}$$

donc $\operatorname{pgcd}(438, 51) = 3$.

(ii) Par le même calcul, on obtient $\operatorname{pgcd}(151, 77) = 1$.

(iii) $\operatorname{pgcd}(1320, 720) = 120$.

(iv) $\operatorname{pgcd}(63, 17) = 1$ (la primalité de 17 rend d'ailleurs cela évident).

(v) $\operatorname{pgcd}(120, 23) = 1$ (même remarque : 23 est premier).

(vi) $\operatorname{pgcd}(8136, 492) = 12$.

Autocorrection D.

L'entier $n! + 1$ est $\geqslant 2$, donc il admet un diviseur premier $p \leqslant n! + 1$.

Il reste à montrer que $p > n$. Pour cela, il suffit de constater que si $p \leqslant n$, on a $p \mid n!$, donc on a $p \wedge (n! + 1) = p \wedge 1 = 1$, ce qui contredit la définition de p.

En particulier, on a montré que quel que soit $n \in \mathbb{N}^*$, il existait un nombre premier $p > n$. Il existe des nombres premiers arbitrairement grands, ce qui démontre qu'il existe une infinité de nombres premiers.