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 6.
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 11.
La valuation p-adique d'un entier n est un cardinal – celui de $\left\{k \in \mathbb{N}^* \,\middle|\, p^k \mid n\right\}$ – et il est toujours possible d'écrire un cardinal comme une somme de 1...

Exercice 18.
On pourra commencer par montrer que si (x, y) est une solution telle que $x \leqslant y$ alors $x \mid y$.

Exercice 28.
Pour la première question, on pourra essayer de traduire hypothèse et conclusion en termes du groupe multiplicatif $(\mathbb{F}_p^\times, \cdot)$.

Exercice 38.
Pour la première question, on pourra réutiliser la vieille idée de mise sous forme canonique.

Pour la question 2(d), en partant de la solution $x_0 = 1$ de (E_5), par exemple, on pourra chercher une solution de (E_{25}) de la forme $x = 1 + 5\xi$. On vérifiera en effet que l'équation (E_{25}) se ramène ainsi à une équation du premier degré en ξ, facile à résoudre.

Il faudra également argumenter qu'on « attrape » ainsi toutes les solutions de (E_{25}).

Autocorrection

Autocorrection A.

(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 $438 \wedge 51 = 3$.

On remonte le calcul pour obtenir notre relation de Bézout :

$$
\begin{aligned}
3 &= 21 - 2 \times 9 && \text{(d'après (4))} \\
&= 21 - 2 \times (30 - 21) && \text{(d'après (3))} \\
&= 3 \times 21 - 2 \times 30 \\
&= 3 \times (51 - 30) - 2 \times 30 && \text{(d'après (2))} \\
&= 3 \times 51 - 5 \times 30 \\
&= 3 \times 51 - 5 \times (438 - 8 \times 51) && \text{(d'après (1))} \\
&= 43 \times 51 - 5 \times 438.
\end{aligned}
$$

(ii) Par le même calcul, on obtient $151 \wedge 77 = 1$ et $1 = 51 \times 77 - 26 \times 151$.

(iii) $1320 \wedge 720 = 120$ et $120 = 2 \times 720 - 1320$.

(iv) $63 \wedge 17 = 1$ (la primalité de 17 rend d'ailleurs cela évident) et $1 = 19 \times 63 - 26 \times 46$.

(v) $120 \wedge 23 = 1$ (même remarque : 23 est premier) et $1 = 47 \times 23 - 9 \times 120$.

(vi) $8136 \wedge 492 = 12$ et $12 = 215 \times 492 - 13 \times 8136$ (les calculs sont un peu pénibles).

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.

Soit $n \in \mathbb{N}^*$. On a l'égalité

$$n^4 - n^2 = n^2(n^2 - 1) = n^2(n - 1)(n + 1).$$

- Déjà, l'entier $n^4 - n^2$ est divisible par le produit $(n - 1)n(n + 1)$ de trois entiers consécutifs. L'un de ces trois entiers est nécessairement multiple de 3, donc $3 \mid n^4 - n^2$.
- Ensuite, distinguons deux cas :
  - Si n est pair, on peut trouver $m \in \mathbb{N}$ tel que $n = 2m$. On a alors $n^2 = 4m^2$, donc n^2 est multiple de 4, ce qui entraîne que $n^4 - n^2$ l'est également.
  - Si n est impair, les deux facteurs $n - 1$ et $n + 1$ sont pairs, donc $n^4 - n^2$ est un multiple de 4.

  Ainsi, $4 \mid n^4 - n^2$.

Comme 3 et 4 sont premiers entre eux, le lemme de Gauss entraîne que $12 \mid n^4 - n^2$.

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.

Autocorrection E.

On a $2 \times 3 \times 5 \times 7 = 210$. En faisant les produits de trois de ces quatre nombres, on obtient

$$3 \times 5 \times 7 = 105, \qquad 2 \times 5 \times 7 = 70, \qquad 2 \times 3 \times 7 = 42 \qquad \text{et} \qquad 2 \times 3 \times 5 = 30.$$

Ainsi, pour tous $a, b, c, d \in \mathbb{Z}$, le nombre $N = 105a + 70b + 42c + 30d$ vérifie

$$\begin{cases} N \equiv 105a \equiv a \pmod 2 \\ N \equiv \ 70b \equiv b \pmod 3 \\ N \equiv \ 24c \equiv 2c \pmod 5 \\ N \equiv 30d \equiv 2d \pmod 7. \end{cases}$$

Il reste ainsi à « corriger » les deux facteurs 2 surnuméraires, en utilisant les inverses de 2 modulo 5 et 7.

Comme $2 \times 3 \equiv 1 \pmod 5$ et $2 \times 4 \equiv 1 \pmod 7$, le nombre $n = 105a + 70b + 126c + 120d$ est congru à a, b, c et d modulo 2, 3, 5 et 7 respectivement.

Ainsi, $(\lambda, \mu, \nu, \xi) = (105, 70, 126, 120)$ convient.

Autocorrection F.

On va calculer 2^{70} et 3^{70} modulo 13.

- On a $3^3 = 27 \equiv 1 \pmod{13}$, donc $3^{70} = (3^3)^{23} \times 3 \equiv 3 \pmod{13}$.
- D'après le petit théorème de Fermat, $2^{12} \equiv 1 \pmod{13}$, donc $2^{70} \equiv 2^{10} \pmod{13}$. On a en fait $2^5 = 32 \equiv 6 \pmod{13}$, donc $2^{10} \equiv 36 \equiv -3 \pmod{13}$.

On en déduit $2^{70} + 3^{70} \equiv 0 \pmod{13}$, ce qui conclut.