Corrigés — Arithmétique dans $\mathbb{Z}$

Chapitre 9

Solution 1.

1. $21 = 15 + 6$; $15 = 2 \times 6 + 3$; $6 = 2 \times 3 + 0$. PGCD $= 3$. Remonter : $3 = 15 - 2 \times 6 = 15 - 2(21 - 15) = 3 \times 15 - 2 \times 21$. Bézout : $u = -2, v = 3$.
2. $54 = 2 \times 24 + 6$; $24 = 4 \times 6 + 0$. PGCD $= 6$. $6 = 54 - 2 \times 24$. $u = 1, v = -2$.

Solution 2.

1. $7 \times (-1) + 4 \times 2 = 1$. Solution particulière $(-1, 2)$. Général : $x = -1 + 4k, y = 2 - 7k$.
2. $\mathrm{PGCD}(15, 10) = 5 \mid 20$. Simplifier : $3x + 2y = 4$. $3 \times 2 + 2 \times (-1) = 4$. Général : $x = 2 + 2k, y = -1 - 3k$.
3. $\mathrm{PGCD}(3, 5) = 1 \mid 7$. $3 \times (-1) + 5 \times 2 = 7$. Général : $x = -1 + 5k, y = 2 - 3k$... non, $x = -1 + 5\frac{k}{1} = -1 + 5k$ et $y = 2 - 3k$.

Solution 3.

Par Fermat $(p = 11)$: $a^{\{10\}} \equiv 1 \bmod 11$ pour a premier avec 11.

1. $2^{\{10\}} \equiv 1$.
2. $3^{\{11\}} = 3 \times 3^{\{10\}} \equiv 3 \times 1 = 3$.
3. $5^{\{20\}} = \left(5^{\{10\}}\right)^2 \equiv 1^2 = 1$.

Solution 4.

Inverse de 4 modulo 13 : $4 \times 10 = 40 = 3 \times 13 + 1$, donc 10. $x \equiv 70 \equiv 5 \bmod 13$.

Solution 5.

$n^3 - n = n(n - 1)(n + 1)$: trois entiers consécutifs, donc divisible par 2 et par 3 (trois entiers consécutifs contiennent un multiple de chaque), donc par 6.

Solution 6.

Fermat pour $p = 5$: montrer $a^5 \equiv a \bmod 5$. Récurrence sur $a \geq 0$: $0^5 = 0$ ✓. Hérédité : supposer $a^5 \equiv a$. Alors $(a + 1)^5 = a^5 + 5a^4 + 10a^3 + 10a^2 + 5a + 1 \equiv a + 1 \bmod 5$ (tous les coefficients binomiaux intermédiaires sont multiples de 5). Pour $a < 0$: inversion.

Solution 7.

$2^3 = 8 \equiv 1 \bmod 7$. $2^{\{100\}} = 2^{3 \times 33 + 1} = \left(2^3\right)^{\{33\}} \times 2 \equiv 2 \bmod 7$. Reste : 2.

Solution 8.
$17 = 13 + 4$; $13 = 3 \times 4 + 1$; $4 = 4 \times 1$. $1 = 13 - 3 \times 4 = 13 - 3(17 - 13) = 4 \times 13 - 3 \times 17$. $a = 4, b = -3$. Multiplier par 5 : $13 \times 20 + 17 \times (-15) = 5$. Particulière $(20, -15)$.

Solution 9.
Pour $8 \mid n^2 - 1$: $n = 2k + 1$, $n^2 - 1 = 4k(k + 1)$, avec $k(k + 1)$ pair, donc $8 \mid n^2 - 1$. Pour $3 \mid n^2 - 1$: n impair. Si $n \equiv 0 \bmod 3$, n divisible par 3 et impair, possible pour $n = 3$ etc. Alors $n^2 - 1 \equiv -1$, non divisible par 3. Contre-exemple : $n = 3$, $n^2 - 1 = 8$, non divisible par 24. **L'énoncé est incorrect** : c'est $24 \mid (n^2 - 1)$ pour n impair ET non multiple de 3, soit $n \equiv \pm 1 \bmod 6$.