Contrôle continu du 22 octobre

Corrigé

Exercice 1 –

1.1. On a les dentités $2^6 = 63 + 1 = 9 \cdot 7 + 1$ et le reste est égal à 1.

1.2. En tenant compte du point précédent, on a les congruences

$$9^{43} \equiv 2^{43} \equiv 2 \cdot 2^{42} \equiv 2 \cdot (2^6)^7 \equiv 2 \cdot 1^7 \equiv 2 \pmod 7.$$

Le reste est donc égal à 2.

2. Si l'entier 133 n'est pas premier, il possède un diviseur $d > 1$ inférieur ou égal à $\sqrt{133} < 12$. Une vérification directe amène à la factorisation $133 = 7 \cdot 19$.

3. On obtient facilement la factorisation $540 = 2^2 \cdot 3^3 \cdot 5$, ce qui amène aux identités $v_2(540) = 2, v_3(540) = 3, v_5(540) = 1$ et $v_p(540) = 0$ pour tout nombre premier $p > 5$.

4. En posant $n = 2m+1$, on obtient l'identité $n^2 = 4m(m+1)+1$. L'entier $m(m+1)$ étant toujours pair, on en déduit que $n^2 - 1$ est divisible par 8.

5. On a les identités

$$\begin{aligned} 75 = 2 \cdot 37 + 1 = 2(4 \cdot 9 + 1) + 1 = 8 \cdot 9 + 2 + 1 = 8(8 + 1) + 2 + 1 = \\ = 64 + 8 + 2 + 1 = 1 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2 + 1. \end{aligned}$$

L'écriture de 75 en base 2 est donc 1001011.

Exercice 2 –

1. L'algorithme d'Euclide amène au tableau suivant :

	1	1	1	9	1	1	2	
308	202	106	96	10	6	4	2	0
1	0	1	-1	2	-19	21	-40	
0	1	-1	2	-3	29	-32	61	

En particulier, le pgcd de 308 et 202 est égal à 2.

2. D'après le tableau ci-dessus, on obtient l'identité de Bézout

$$-40 \cdot 308 + 61 \cdot 202 = 2,$$

d'où la solution particulière $(-40, 61)$.

3. La solution générale (x, y) est donnée par

$$\begin{cases} x = x_0 + d^{-1}bn = 101n - 40, \\ \\ y = y_0 - d^{-1}an = 61 - 154n, \end{cases}$$

avec n entier.

Exercice 3 –

1. Le groupe G étant cyclique d'ordre 20, les ordres possibles de ses éléments sont les diviseurs de 20, soit $1, 2, 4, 5, 10$ et 20.
2. D'après le cours, il existe une bijection entre les sous-groupes de G et les diviseurs de son ordre. On obtient donc 6 sous-groupes.
3. Le groupe G possède $\varphi(20) = \varphi(4)\varphi(5) = 2 \cdot 4 = 8$ générateurs.
4. Les générateurs de G sont les classes des entiers naturels inférieurs ou égaux à 20 premiers avec 20, ce qui donne les éléments $\bar{1}, \bar{3}, \bar{7}, \bar{9}, \overline{11}, \overline{13}, \overline{17}$ et $\overline{19}$.
5. Pour tout élément $x = (a, b)$ de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$, on a les identités

$$10x = (10a, 10b) = (0, 0) = 0,$$

ce qui implique que l'ordre de x divise 10. Il s'en suit que $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$, qui est d'ordre 20, n'est pas cyclique et ne peut donc pas être isomorphe à G.

Exercice 4 –

1. Le groupe G est d'ordre $\varphi(14) = \varphi(2)\varphi(7) = 6$. Ses éléments étant les classes des entiers naturels inférieurs ou égaux à 14 et premiers avec 14, on obtient l'identité $G = \{\bar{1}, \bar{3}, \bar{5}, \bar{9}, \overline{11}, \overline{13}\}$.
2. D'après le théorème de Lagrange, l'ordre de la classe de 3 divise 6. Les entiers $3^1 = 3, 3^2 = 9$ et $3^3 = 27$ n'étant pas congrus à 1 modulo 14, le seul ordre possible est 6.
3. Le groupe G étant d'ordre 6, le point précédent affirme qu'il est cyclique, engendré par la classe de 3.
4. Les éléments $x \in G$ vérifiant $x^2 = \bar{1}$ sont les éléments de l'unique sous-groupe d'ordre 2 de G, engendré par la classe $\bar{3}^3 = \overline{27} = \overline{13}$. On a donc $x = \bar{1}$ ou $x = \overline{13}$. De manière analogue, les éléments vérifiant l'identité $x^3 = \bar{1}$ sont les éléments du seul sous-groupe d'ordre 3 de G, engendré par $\bar{3}^2 = \bar{9}$, ce qui donne $\bar{1}, \bar{9}$ et $\bar{9}^2 = \overline{81} = \overline{11}$.

5.1. Le groupe G étant abélien, pour tout $x, y \in G$, on a les identités

$$f(xy) = (xy)^p = x^p y^p = f(x)f(y),$$

et l'application f est donc un homomorphisme.

5.2. Le noyau de f est formé par les éléments $x \in G$ tels que $x^p = \bar{1}$. En particulier, le l'ordre d de x divise p. De plus, le théorème de Lagrange affirme que d divise 6. Les entiers 6 et p étant premiers entre eux, on en déduit l'identité $d = 1$, d'où la relation $x = \bar{1}$. L'homomorphisme f est alors injectif et, le groupe G étant fini, il est également surjectif, donc bijectif.