Exercice 6.7.1

Indication. — Attention, ici Fermat ne s'applique pas

Exercice 6.7.2

Indication. — chiffre des unités = reste modulo 10
on pensera à réduire 123456 modulo 10

Exercice 6.7.3

Indication. — On pourra par exemple décomposer $56 = 50 + 6$ et appliquer la formule du binôme

Exercice 6.7.4

Indication. — chiffre des dizaines = chiffres des dizaines du reste modulo 100

Exercice 6.8

Indication. — Trois derniers chiffres = reste modulo 1000
Si 10 divise a, alors pour tout $n \geqslant 3$, on a $a^n = 0 \pmod{1000}$

Exercice 6.9

Indication. — Algorithme d'Euclide pour le calcul du pgcd ; pour le ppcm on pourra utiliser la proposition 6.4.4.1 du cours

Exercice 6.10

Indication. — Algorithme d'Euclide étendu (exemple p. 77 et remarque p. 78 du cours)

Exercice 6.11

Indication. — Pour 6.11.1, algorithme d'Euclide étendu (exemple p. 77 et remarque p. 78 du cours)
Pour 6.11.2, le d trouvé au 6.11.1 ne divise pas 15

Exercice 6.12

Indication. — Se rappeler que si a est un entier pair, il existe un entier b tel que $a = 2b$ et si a est un entier impair, il existe un entier b tel que $a = 2b+1$. Prendre alors le carré...

Le début de 6.12.3(a) découle des deux premières questions et de la compatibilité des congruences à l'addition. Pour la fin de 6.12.3(a), regarder les carrés modulo 8.

Dans 6.12.3(b), on précise qu'on demande de montrer que $ab+bc+ac$ n'est pas un carré modulo 4. Commencer par travailler modulo 8 en utilisant 6.12.2.

Exercice 6.13

Indication 1. — On peut essayer d'utiliser le corollaire 6.4.2 du cours. On peut aussi essayer d'utiliser le fait que deux entiers a et b sont premiers entre eux si et seulement si pour tout nombre premier p, p ne divise pas a ou p ne divise pas b (énoncé dont la structure logique favorise les aisonnements par l'absurde)

Indication 2. — En utilisant le corollaire 6.4.2 : pour 6.13.1 écrire une identité de Bezout pour a et b et essayer d'en déduire une identité de Bezout pour a et $a+b$. Pour 6.13.2 écrire une identité de Bezout pour a et b, une identité de Bezout pour a et c, et les multiplier terme à terme. Pour 6.13.3 écrire une identité de Bezout pour a et b, et l'élever à une puissance bien choisie pour obtenir (grâce à la formule du binôme) une identité de Bezout pour a^k et b^l

Exercice 6.14

Indication. — La réponse est non, et un argument de divisibilité permet de le montrer. Rappelons que la somme des entiers de 1 à 30 est $\frac{30(30+1)}{2}$

Exercice 6.15

Indication. — On peut essayer d'utiliser le corollaire 6.4.2 du cours. On peut aussi (ce qui revient un peu au même) essayer d'appliquer l'algorithme d'Euclide. Pour 6.15.1 on pourra par exemple commencer par essayer d'appliquer Euclide à $3(8n+7)$ et $6n+5$.

Exercice 6.16

Indication. — Pour 6.16.1, trouver une solution particulière (a_0, b_0) avec Euclide étendu (ou directement). Si (a,b) est une solution quelconque, en déduire une relation entre $a-a_0$ et $b-b_0$ qu'on pourra étudier à l'aide du lemme de Gauss.

Même chose pour 6.16.2 (pour la solution particulière, on pourra partir de celle obtenue en 6.16.1)

Pour 6.16.3, penser à la situation de 6.11.2