Arithmétique 2

Questions de cours
Montrez l'existence d'un PGCD.
Montrez le théorème de Bezout.

---

1. Congruences

Exercice 1.1. *Résoudre* $3x \equiv 2 \mod 10$ *puis* $2x \equiv 3 \mod 12$.

Exercice 1.2 (Problème de Sun Tzu)**.**
Soient des objets dont on ignore le nombre. En les comptant 3 par 3 il en reste 2 ; en les comptant 5 par 5, il en reste 3 et en les comptant 7 par 7, il en reste 2. Combien y a-t-il d'objets ?

Exercice 1.3.
(1) *Montrer que* $2^{12} \equiv 1 \mod 13$
(2) *Donner la liste des puissances de* 2 *modulo* 13.
(3) *Résoudre dans* $\mathbb{Z}$, $6x^2 \equiv 5 \mod 13$.

2. PGCD, PPCM

Exercice 2.1. *Vérifier que pour tout* $(a, b) \in \mathbb{Z}^2$, $(a \wedge b)(a \vee b) = ab$.

Exercice 2.2. *Résoudre dans* $\mathbb{Z}$: $x \wedge y = 5$, $x \vee y = 60$.

Exercice 2.3. *Résoudre dans* $\mathbb{Z}$: $x \wedge y = 7$, $x \vee y = 210$.

Exercice 2.4. *Résoudre dans* $\mathbb{Z}$: $x \wedge y = 12$, $x + y = 420$.

Exercice 2.5. *Résoudre dans* $\mathbb{Z}$: $x \vee y = 252$, $xy = 1512$.

Exercice 2.6. *Résoudre dans* $\mathbb{Z}$: $(x \vee y) - (x \wedge y) = 187$.

Exercice 2.7. *Montrez que si* (a, b, q, r) *sont quatre entiers relatifs tels que* $a = bq + r$ *alors* $b \wedge r = a \wedge b$. *En déduire un algorithme (celui d'Euclide) pour calculer* $a \wedge b$ *ainsi qu'un algorithme pour déterminer les pairs* $(u, v) \in \mathbb{Z}^2$ *telles que* $au + bv = a \wedge b$.

Exercice 2.8. *Soit* $(u_n)_{n\in\mathbb{N}}$ *la suite de Fibonacci. On veux montrer que* $u_n \wedge u_m = u_{n\wedge m}$.
(1) *Montrer que* $u_{n+1} \wedge u_n = 1$.
(2) *si* $m > n > 0$ *exprimer* u_m *en fonction de* u_n, u_{n-1}, u_{m-n+1} *et* u_{n-m}.
(3) *En déduire que pour* $d \in \mathbb{N}$, $(d|u_m$ *et* $d|u_n) \Leftrightarrow (d|u_{m-n}$ *et* $d|u_n)$.
(4) *Montrer que l'algorithme d'Euclide donne le résultat cherché.*

Exercice 2.9. *Montrer que pour tout triplet de nombres entiers* (a, b, c), *on a* $a \wedge (b \wedge c) = (a \wedge b) \wedge c$. *Notons* d *cet entier. Montrer qu'un entier* n *est divisible par* d *si et seulement si il existe trois entiers relatifs* u, v, w *tels que* $n = au + bv + cw$.

3. Équations diophantiennes

Exercice 3.1. *Résoudre dans $\mathbb{Z}$ puis $\mathbb{N}$ l'équation $3x - 4y = 7$.*

Exercice 3.2. *Résoudre dans $\mathbb{Z}$ puis $\mathbb{N}$ l'équation $12x - 10y = 4$.*

Exercice 3.3. *Résoudre dans $\mathbb{Z}$ puis $\mathbb{N}$ l'équation $x^2 + y^2 = 3z^2$.*

Exercice 3.4. *Factoriser le polynôme $x^3+3xy+y^3-1$ et résoudre dans $\mathbb{Z}$ l'équation $x^3+3xy+y^3 = 1$.*

Exercice 3.5. *Résoudre dans $\mathbb{N}$ l'équation $x^4 + x^2 + 1 = y^2$.*

Pour le mardi 3 octobre 12:00

Exercice 4.6. *Pour $n \in \mathbb{N}^*$, on note d_n le nombre de diviseurs (positifs) de n.*

(1) *Montrer que si $a \wedge b = 1$ alors $d_{ab} = d_a d_b$.*
(2) *Calculer d_n en fonction de la décomposition de n en produit de facteurs premiers.*
(3) *Est-il vrai que n est un carré si et seulement si d_n est impair ?*
(4) *Montrer que $(\prod\limits_{d|n} d)^2 = n^{d_n}$.*

Exercice 4.7. *Pour $n \in \mathbb{N}^*$, on note $\varphi(n)$ le nombre d'entiers positifs plus petits que n et premiers à n. (φ est l'indicatrice d'Euler.)*

(1) *Montrer que si $a \wedge b = 1$ alors $\varphi(ab) = \varphi(a)\varphi(b)$.*
(2) *Montrer que si p est premier et a est entier strictement positif alors $\varphi(p^a) = p^{a-1}(p-1)$.*
(3) *Montrer que $\frac{\varphi(n)}{n} = \prod\limits_{\substack{p \text{ premier} \\ p|n}} (1 - \frac{1}{p})$.*
(4) *Est-il vrai que $\sum\limits_{d|n} \varphi(d) = n$?*
(5) *Montrer que si p et q sont deux premiers distincts et $n \equiv 1 \mod (p-1)(q-1)$ alors $x^n \equiv x \mod pq$.*
(6) *En déduire que si $x^5 \equiv 2 \mod 14$ alors $x \equiv 2^5 \mod 14$.*