Arithmétique dans Z

I. Divisibilité, pgcd, ppcm et congruences

Exercice 1. — Soit $n \geqslant 1$ un entier positif. Montrer que $\sqrt{n}$ est rationnel ssi n est un carré parfait (*i.e* de la forme m^2 pour $m \in \mathbf{N}$).

Exercice 2. — Montrer que $\frac{\ln 2}{\ln 3}$ est irrationnel.

Exercice 3. — Déterminer en fonction de l'entier positif n le pgcd de n^3+n et $2n+1$.

Exercice 4. — Montrer que pour tout entier positif n la fraction $\frac{2n+1}{6n+5}$ est irréductible.

Exercice 5. — Déterminer les entiers n tels que $n-3$ divise n^3-3.

Exercice 6. — Soient a et b deux entiers tels que $7 \mid a^2+b^2$. Montrer que $7 \mid a$ et $7 \mid b$.

Exercice 7. — Soient a et b deux entiers premiers entre eux.
Montrer qu'alors $a+b$ et ab sont aussi premiers entre eux.

Exercice 8. — Soit n un entier tel que $5^3 \mid n^2$. Montrer que $5^4 \mid n^2$.

Exercice 9. — Dans un magasin, on vend des tasses par paquets de 6 et des assiettes par paquets de 8. J'organise une fête pour l'anniversaire de ma petite sœur et je veux la même quantité de tasses et d'assiettes.
Quelles sont toutes mes possibilités sur le nombre d'assiettes à acheter ?

Exercice 10. — Paramétrer les solutions (x, y) entières de l'équation $27x + 15y = 6$.

Exercice 11. — Peut-on découper une ficelle de 100 cm en morceaux de 4 cm et de 5 cm de telle sorte qu'il n'y ait aucune perte ? Combien y a-t-il de solutions ?

Exercice 12. — On considère l'algorithme de "réduction" des matrices entières vu lors de l'étude des groupes abéliens de type fini.

a) Que pensez-vous de cet algorithme appliqué sur une matrice ligne ?

b) Utiliser cet algorithme pour résoudre l'exercice *10*.

c) A quelle condition nécessaire et suffisante sur $(b_1, b_2, b_3) \in \mathbf{Z}^3$ le système suivant admet-il au moins une solution (x, y, z) *entière* ?

$$\begin{cases} 2x - y + z = b_1 \\ -2x + 4y + 2z = b_2 \\ -2x + 7y + 5z = b_3 \end{cases}$$

Exercice 13. — Soit $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ la factorisation en facteurs premiers d'un entier.
Déterminer le nombre des diviseurs de n en fonction des α_i.

Exercice 14. — Soient $a > b \geqslant 1$ deux entiers premiers entre eux.

a) Montrer qu'il existe un *unique* couple d'entiers positifs (u_0, v_0) tel que :

$$au_0 - bv_0 = 1 \quad \text{et} \quad \begin{matrix} 0 \leqslant u \leqslant b-1 \\ 0 \leqslant v \leqslant a-2 \end{matrix}$$

b) Montrer qu'il existe $N > 0$ tel que pour tout $n \geqslant N$ il existe un couple d'entiers *positifs* (u, v) tel que : $au + bv = n$.
[**Indication:** $N = ab$ convient par exemple.]

Exercice 15. — Soient $a_1, \ldots, a_n$ une famille d'entiers.

a) Montrer que l'on a $a_1 \wedge \cdots \wedge a_n = a_1 \wedge (\cdots \wedge (a_{n-1} \wedge a_n))$

b) Montrer que les a_i sont globalement premiers entre eux ss'il existe une relation de Bézout :

$$a_1 u_1 + \cdots + a_n u_n = 1.$$

Donner un exemple de a_i globalement premiers entre eux, sans qu'aucune paire a_i, a_j ne soit premiers entre eux.

c) Comment calcule-t-on efficacement le pgcd d'une famille d'entiers avec l'algorithme d'Euclide ?

Exercice 16. — Démontrer les critères de divisibilité d'un entier par 2, 3, 5 et 9.
Donner un critère de divisibilité par 7 et par 11.

Exercice 17. — Soient $m, n > 0$ deux entiers. Montrer que $\sum_{k=m}^{m+n} \frac{1}{k}$ n'est pas un entier.

[**Indication:** Considérer l'entier k ayant la plus grande valuation en 2 et montrer son unicité.]

Exercice 18. — Soit p un nombre premier ; on note $v_p(-)$ la fonction "valuation p-adique".

a) Pour $n \geqslant 1$, montrer la formule de Legendre :

$$v_p(n!) = \sum_{r \geqslant 1} E\left(\frac{n}{p^r}\right)$$

(où E désigne la fonction partie entière).

b) En déduire que pour tous $(m, n) \in \mathbf{N}^{*2}$, $\frac{(2m)!(2n)!}{m!n!(m+n)!}$ est un entier.

Exercice 19. — Quel est le chiffre des unités de l'entier 2018^{2018} ?

Exercice 20. — Soit p un nombre premier.

a) Montrer que p divise le coefficient binomial $\binom{p}{k}$ pour tout $1 \leqslant k \leqslant p-1$.

b) Montrer que $\binom{2p-1}{p} \equiv 1[p]$.

II. Anneaux $\mathbf{Z}/n$ et groupes $(\mathbf{Z}/n)^\times$, [Perrin]

Exercice 21. — Soit $n \geqslant 1$ un entier.

a) Montrer que l'anneau $\mathbf{Z}/n$ est un corps ssi n est premier.

b) En pratique, comment détermine-t-on l'inverse d'un élément non nul ?

Exercice 22. — **[Fonction d'Euler].**
Soit $n \geqslant 1$ un entier. On note $\varphi(n)$ le cardinal du groupe des inversibles de l'anneau $(\mathbf{Z}/n)$.

a) Soit $m \in \mathbf{Z}$. Montrer que les assertions suivantes sont équivalentes :

(i) $\overline{m}$ est inversible dans l'anneau $\mathbf{Z}/n$;

(ii) $\overline{m}$ est un générateur du groupe $\mathbf{Z}/n$;

(iii) m et n sont premiers entre eux.

b) Si $n = p^\alpha$ avec p premier, que vaut $\varphi(n)$?

c) On suppose que la décomposition de n en produits de facteurs premiers est $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Montrer que l'on a un isomorphisme de groupes :

$$(\mathbf{Z}/n)^\times \cong (\mathbf{Z}/p_1^{\alpha_1})^\times \times \cdots \times (\mathbf{Z}/p_k^{\alpha_k})^\times.$$

En déduire une formule pour $\varphi(n)$.

d) Montrer que $n = \sum_{d|n} \varphi(d)$.

[**Indication:** Regrouper les éléments du groupe $\mathbf{Z}/n$ selon leur ordre.]

Exercice 23. — **a)** Pour $k \geqslant 1$ fixé, montrer que l'ensemble $\{n \in \mathbf{N}, \varphi(n) = k\}$ est fini. Déterminer cet ensemble pour $k = 2^5$, $k = 2 \cdot 7^3$.

b) En déduire que $\lim_{n\to\infty} \varphi(n) = +\infty$.

Exercice 24. — Soit p un nombre premier.

a) Montrer que le groupe $(\mathbf{Z}/p)^\times$ est cyclique.
[**Indication:** Soit $d_1|\ldots|d_r$ ses facteurs invariants. Considérer les racines du polynôme $X^{d_r} - 1 \in \mathbf{Z}/p[X]$.]

b) Donner tous les générateurs des groupes $(\mathbf{Z}/5)^\times$, $(\mathbf{Z}/7)^\times$ et $(\mathbf{Z}/11)^\times$.

Exercice 25. — Soient p un nombre premier *impair* et $k > 0$ un entier. On va montrer que le groupe $(\mathbf{Z}/p^k)^\times$ est cyclique.
Soit $\rho : \mathbf{Z}/p^k \to \mathbf{Z}/p$ le morphisme de "réduction modulo p", *i.e.* : $\rho(x \mod p^k) = x \mod p$.

a) Vérifier que ρ est un morphisme d'anneaux bien défini.

b) Vérifier que ρ induit (par restriction) un morphisme de groupes $\psi : (\mathbf{Z}/p^k)^\times \to (\mathbf{Z}/p)^\times$. Montrer que ψ est surjectif.

c) En utilisant l'exercice *24*, montrer qu'il existe un élément g d'ordre $p-1$ dans $(\mathbf{Z}/p^k)^\times$.
[**Indication:** Soit x un générateur de $(\mathbf{Z}/p)^\times$, montrer qu'un élément y tel que $\psi(y) = x$ est d'ordre multiple de $p-1$ et considérer les puissances de y.]

d) Soit $\langle g\rangle$ le sous-groupe engendré par g et soit Γ le noyau de ψ. Montrer que l'application

$$\begin{array}{ccc} \langle g\rangle \times \Gamma & \to & (\mathbf{Z}/p^k)^\times \\ (a,b) & \mapsto & a \cdot b \end{array}$$

est un isomorphisme de groupes.

e) Montrer que pour tout entier $\ell \geqslant 0$, on a $(1+p)^{p^\ell} \equiv 1 + p^{\ell+1}\ [p^{\ell+2}]$.

f) Déduire de la question précédente que $\overline{1+p}$ engendre Γ.

g) En déduire que $(\mathbf{Z}/p^k)^\times$ est cyclique et même que l'élément $g \cdot \overline{(1+p)}$ en est un générateur.

h) Pour $x \in \mathbf{Z}$ et $k \geqslant 2$, montrer qu'x est générateur de $(\mathbf{Z}/p^k)^\times$ ss'il est un générateur de $(\mathbf{Z}/p^2)^\times$.
[**Indication:** Considérer les cardinaux des ensembles de générateurs de ces groupes.]

i) Soit $x \in \mathbf{Z}$ tel que $\overline{x}$ soit un générateur de $(\mathbf{Z}/p)^\times$. Montrer qu'on a l'alternative suivante : soit $\overline{x}$ soit $\overline{x+p}$ est un générateur de $(\mathbf{Z}/p^2)^\times$ et de tous les $(\mathbf{Z}/p^k)^\times$ pour tout $k \geqslant 2$.

j) Déterminer un générateur pour les groupes $(\mathbf{Z}/5^3)^\times$, $(\mathbf{Z}/7^2)^\times$ et $(\mathbf{Z}/11^{2017})^\times$.

Exercice 26. — **a)** Déterminer les groupes $(\mathbf{Z}/2)^\times$, $(\mathbf{Z}/4)^\times$ et $(\mathbf{Z}/8)^\times$. Sont-ils cycliques ?

b) Où la démonstration de l'exercice ***25*** ne marche-t-elle plus pour $p = 2$?

c) Montrer que pour tout entier $\ell \geqslant 0$, on a $(1+4)^{2^k} \equiv 1 + 2^{k+2}\ [2^{k+3}]$.

d) Montrer que pour $n \geqslant 2$ on a :

$$(\mathbf{Z}/2^n)^\times \cong (\mathbf{Z}/2) \times (\mathbf{Z}/2^{n-2})$$

Exercice 27. — Montrer que le groupe $(\mathbf{Z}/n)^\times$ est cyclique ssi $n = 2, 4, p^\alpha, 2p^\alpha$ (p premier impair).

Exercice 28. — Soit p un nombre premier impair.

a) Déterminer le nombre de carrés de $(\mathbf{Z}/p)^\times$ en considérant le morphisme de groupes $(\mathbf{Z}/p)^\times \to (\mathbf{Z}/p)^\times$, $x \mapsto x^2$.

b) Retrouver ce résultat en utilisant la structure de $(\mathbf{Z}/p)^\times$ (*c.f.* exercice 24).

c) Appliquer les deux stratégies précédentes pour déterminer le nombre de cubes dans $(\mathbf{Z}/p)^\times$ et en déduire à quelle condition -3 est un carré modulo p.

Exercice 29. — **[Carrés modulo n.]**
Soient $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ un entier décomposé en facteurs premiers et $a \in \mathbf{Z}$.

a) Montrer que a est un carré modulo n ssi pour tout i, a est un carré modulo p^{α_i}.

Dans la suite, on se concentre donc sur le cas où $n = p^\alpha$, en distinguant selon que $p = 2$ ou non. On écrit alors $a = p^r a'$ avec $a' \wedge p = 1$.

b) Si p est impair, montrer que a est un carré modulo p^α ssi (r est pair et a' est un carré modulo p) ou ($r \geqslant \alpha$).

c) Pour $\alpha \geqslant 3$, montrer que a est un carré modulo 2^α ssi (r est pair et $a' \equiv 1[8]$) ou ($r \geqslant \alpha$).

d) Montrer que -1 est un carré modulo 125 et en déterminer toutes les racines carrées dans $\mathbf{Z}/125$.
[**Indication:** Commencer par trouver les racines carrées modulo 5, puis modulo 25.]

Exercice 30. — Soit p un nombre premier impair. Soit $P \in \mathbf{Z}[X]$ le polynôme

$$P := (X+1)(X+2)\cdots(X+p-1).$$

a) Montrer que dans $\mathbf{Z}/p[X]$, on a l'égalité $\overline{P} = X^{p-1} - 1$.

b) En déduire $(p-1)! \equiv 1[p]$ (*théorème de Wilson*).

c) Pour $p \geqslant 5$, on note $\frac{a_p}{b_p}$ la fraction irréductible $\frac{a_p}{b_p} := 1 + \frac{1}{2} + \cdots + \frac{1}{p-1}$.
En considérant $P(-p)$, montrer que p^2 divise a_p (*théorème de Wolstenholme*).

Exercice 31. — Votre petit cousin, celui qui apprend ses tables de multiplication, a remarqué que dans les tables de 3 et de 7 tous les chiffres des unités sont différents.
Expliquez lui pourquoi.

Exercice 32. — Soit p un nombre premier impair.

a) Montrer que le rationnel $\frac{1}{p}$ admet un développement décimal périodique.

b) Montrer que sa période ℓ est l'ordre de 10 dans $(\mathbf{Z}/p)^\times$.

Dans toute la suite, on suppose que la période est paire et l'on note [1] $\ell = 2e$ et $\frac{1}{p} = 0, ABAB\cdots$ avec $1 \leqslant A, B \leqslant 10^e - 1$.

c) Montrer qu'on a $A + B \equiv 0[10^e - 1]$ et en déduire que $A + B = 10^e - 1$.

d) En déduire que si $p \geqslant 11$, la $\frac{p+1}{2}$ décimale de $\frac{1}{p}$ est soit 0, soit 9, selon que 10 est un carré modulo p ou non.
[**Indication:** Quel est la première décimale ? Combien y a-t-il de retenue dans l'addition $A + B = 9\ldots9$?]

III. Nombres premiers, [Gourdon]

Exercice 33. — **a)** Construire une suite de 2017 entiers consécutifs dont aucun n'est premier.

b) Même question en remplaçant *premier* par *puissance d'un nombre premier*.

Exercice 34. — Soit $n \geqslant 1$ un entier. Montrer que n est premier ss'il existe un entier $a \in \mathbf{N}$ tel que $a^{n-1} \equiv 1[n]$ et tel que pour tout $1 \leqslant k \leqslant n-2$, $a^k \not\equiv 1[n]$.

Exercice 35. — **[Nombres de Mersenne]**
Soit $k \geqslant 1$ un entier.

a) Montrer que si $2^k - 1$ est premier, alors k est premier. Un tel nombre premier est dit de *Mersenne*.

Pour tout entier $n \geqslant 1$, on pose $\theta(n) = \sum_{d|n} d$. On dit que n est parfait si $\theta(n) = 2n$.

b) Montrer que si m et n sont deux entiers premiers entre eux, alors on a $\theta(mn) = \theta(m)\theta(n)$.

c) Si $2^p - 1$ est un nombre premier de Mersenne, montrer que $2^{p-1}(2^p - 1)$ est parfait.

1. Par exemple, pour $\frac{1}{11} = 0,09\ 09\ldots$, $\ell = 2$, $A_1 = 0$ et $B_1 = 9$ et pour $\frac{1}{13} = 0,076923\ 076923\ldots$, $\ell = 6$, $A_2 = 076$ et $B_2 = 923$. Remarquer qu'on a $A_1 + B_1 = 9$ et $A_2 + B_2 = 999$.

d) Réciproquement, montrer que tout nombre parfait *pair* est de la forme précédente.

Exercice 36. — **[Nombres de Fermat]**
Soit $k \geqslant 1$ un entier.

a) Montrer que si $2^k + 1$ est premier, alors k est une puissance de 2.

b) Plus généralement, si $a \geqslant 1$ est un entier tel que $a^k + 1$ est premier, alors a est pair et k est une puissance de 2.

Exercice 37. — **[Nombres de Carmichael]**
Un entier $n \geqslant 2$ est dit *de Carmichael* si n n'est pas premier mais vérifie tout de même :

$$\forall\, a \in \mathbf{Z},\ a^n \equiv a[n].$$

a) Montrer qu'un entier $n = p_1 \dots p_k$ (les p_i étant premiers et distincts) tel que pour tout i, $p_i - 1 | n - 1$ est de Carmichael.
Vérifier que $561 = 3 \cdot 11 \cdot 17$ est de Carmichael.

b) Montrer que tout entier de Carmichael est de la forme précédente avec $k \geqslant 3$.
[**Indication:** Commencer par montrer que n est sans facteur carré. Puis, utiliser que pour p premier, $(\mathbf{Z}/p)^\times$ contient un élément d'ordre $p-1$. Enfin, montrer que $k = 2$ est impossible.]

Exercice 38. — **a)** Montrer qu'il existe une infinité d'entiers premiers congrus à 3 mod 4.
[**Indication:** Raisonner par l'absurde et utiliser qu'un entier congru à 3 mod 4 admet au moins facteur premier congru à 3 mod 4]

b) Montrer qu'il existe une infinité de nombres premiers congrus à 1 mod 4.
[**Indication:** S'ils étaient en nombre fini $p_1, \dots, p_N$, considérer un diviseur premier q de $(p_1 \cdots p_N)^2 + 1$. Remarquer que -1 est un carré modulo q.]

Exercice 39. — Soit q un nombre premier. On se propose de montrer qu'il existe une infinité de nombres premiers congrus à 1 mod q. Pour cela, on raisonne par l'absurde en supposant cet ensemble fini, disons $\{p_1, \dots, p_k\}$. On pose $a := qp_1 \cdots p_k$ et $A := \sum_{i=0}^{q-1} a^i$.

a) Soit p un diviseur premier de A. Montrer que a est inversible modulo p, puis que $\overline{a}$ est d'ordre N dans $(\mathbf{Z}/p)^\times$.

b) En déduire que $p \equiv 1[q]$ et conclure.

Exercice 40. — On note classiquement $\pi(n)$ le nombre d'entiers premiers $\leqslant n$.

a) Montrer que pour tout $n \geqslant 1$, $\prod_{\substack{p \text{ premier} \\ n+1 \leqslant p \leqslant 2n}} p$ divise le coefficient binomial $\binom{2n}{n}$.

b) En déduire que $(n+1)^{\pi(2n)-\pi(n)} \leqslant \binom{2n}{n}$.

c) En déduire que la suite $(\frac{\pi(2^k)k}{2^k})_{k \geqslant 1}$ est bornée.
[**Indication:** Majorer brutalement $\binom{2n}{n} \leqslant 2^{2n}$.]

d) En déduire que la suite $(\frac{\pi(n)\ln(n)}{n})_{n \geqslant 1}$ est bornée.

Exercice 41. — Soit $P \in \mathbf{Z}[X]$ un polynôme à coefficients entiers non constant.

a) Montrer qu'il existe une infinité d'entiers n tels que $P(n)$ n'est pas premier.
[**Indication:** Commencer par traiter le cas où le coefficient constant de P n'est ni 1, ni -1.]

b) Montrer qu'il existe une infinité de premiers p tels que $\{n \in \mathbf{Z},\ p | f(n)\}$ soit non vide.
[**Indication:** Raisonner par l'absurde.]

IV. Loi de réciprocité quadratique, [Demazure]

Exercice 42. — Soit p un nombre premier impair.

a) Montrer que 3 est un carré modulo p ssi $p \equiv \pm 1[12]$ ou bien $p = 3$.

b) Montrer que 5 est un carré modulo p ssi $p \equiv \pm 1[5]$ ou bien $p = 5$.

Exercice 43. — **[Lemme de Gauss]**
Soit $p := 2k + 1$ premier impair. On note $\mathcal{S}$ l'ensemble $\{\overline{1}, \ldots, \overline{k}\} \subset (\mathbf{Z}/p)^\times$.

a) On fixe un $a \in (\mathbf{Z}/p)^\times$. Montrer que pour tout $s \in \mathcal{S}$, il existe un unique signe $\varepsilon_a(s) \in \{\pm 1\}$ et un unique élément $s_a \in \mathcal{S}$ tel que l'on ait $sa = \varepsilon_a(s)s_a$.

b) Montrer que l'application $\mathcal{S} \to \mathcal{S}, s \mapsto s_a$ est une bijection.

c) Montrer le lemme de Gauss : $\left(\frac{a}{p}\right) = \prod_{s \in \mathcal{S}} \varepsilon_a(s)$.

[**Indication:** Calculer $\prod_{s \in S} (as)$.]

d) Pour $a = 2$, calculer $\varepsilon_2(s)$ en fonction de s.
Retrouver que 2 est un carré modulo p ssi $p \equiv \pm 1[8]$.

Exercice 44. — **[Symbole de Jacobi et test de Solovay-Strassen]**
Soit $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ la décomposition en facteurs premiers d'un entier *impair*. Le symbole de Jacobi étend formellement le symbole de Legendre : on pose pour tout $m \in \mathbf{Z}$:

$$\left(\frac{m}{n}\right) := \left(\frac{m}{p_1}\right)^{\alpha_1} \cdots \left(\frac{m}{p_k}\right)^{\alpha_k}.$$

a) Montrer que lorsque les symboles de Jacobi sont définis, on a :

i) $\left(\frac{m_1 m_2}{n}\right) = \left(\frac{m_1}{n}\right)\left(\frac{m_2}{n}\right)$ **ii)** $\left(\frac{m}{n_1 n_2}\right) = \left(\frac{m}{n_1}\right)\left(\frac{m}{n_2}\right)$

iii) $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$ **iv)** $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$

v) $\left(\frac{m}{n}\right) = (-1)^{\frac{n-1}{2}\frac{m-1}{2}}\left(\frac{n}{m}\right)$ (*loi de réciprocité de Jacobi*)

[**Indication:** Remarquer que l'on a $\frac{n-1}{2} + \frac{m-1}{2} \equiv \frac{nm-1}{2}$ [2] et $\frac{n^2-1}{8} + \frac{m^2-1}{8} \equiv \frac{n^2m^2-1}{8}$ [2].]

b) Donner un algorithme pour calculer rapidement le symbole de Jacobi (et *a fortiori* celui de Legendre).

c) Pour m et n premiers entre eux, a-t-on encore "m est un carré modulo n ssi $\left(\frac{m}{n}\right) = 1$" ?

d) Pour n impair, montrer que n est premier ssi l'on a $x^{\frac{n-1}{2}} \equiv \left(\frac{x}{n}\right)$ $[n]$ pour tout $x \in (\mathbf{Z}/n)^\times$.

[**Indication:** Pour la réciproque, remarquer que n est nécessairement de Carmichael, donc (*c.f.* exercice ***37***) sans facteur carré.]

e) Montrer que pour n non premier, pour au moins la moitié des $x \in (\mathbf{Z}/n)^\times$ on a $x^{\frac{n-1}{2}} \not\equiv \left(\frac{x}{n}\right)$ $[n]$.

[**Indication:** $\{x \in (\mathbf{Z}/n)^\times,\ x^{\frac{n-1}{2}} \equiv \left(\frac{x}{n}\right)$ $[n]\}$ est un sous-groupe de $(\mathbf{Z}/n)^\times$.]

f) En déduire un test probabiliste de primalité. Le comparer avec celui de Fermat.