

Université Paris-Saclay 2022-2023
M1 M.F., Orsay Arithmétique

T.D. 1 : Divisibilité

Les exercices soulignés sont ceux qui seront corrigés en TD ; ils sont à chercher en priorité.

Exercice 1 Soit $a \geq 2$, $m \geq 1$ et $n \geq 1$ des entiers. Calculer $\text{pgcd}(a^m - 1, a^n - 1)$ en fonction de a et de $\text{pgcd}(m, n)$.

Exercice 2 Soit $n \geq 2$ un entier. Montrer que n ne divise pas $2^n - 1$.

Exercice 3 (*Wilson*) Montrer que si p est premier alors $(p-1)! \equiv -1 \,(\text{mod}\, p)$. En déduire que si $p \equiv 1 \,(\text{mod}\, 4)$ alors -1 est un carré modulo p.

Exercice 4 (*Racines modulo p de polynômes entiers*) Soit $P \in \mathbf{Z}[X]$ un polynôme non constant. Montrer qu'il existe une infinité de premiers p tels que l'équation $P(x) \equiv 0 \,(\text{mod}\, p)$ ait une solution.

Exercice 5 (*Valuation p-adique*) Soit $n \in \mathbf{Z}$ un entier non nul et p un nombre premier. On appelle *valuation p-adique* de n et on note $v_p(n)$ le plus grand entier $k \geq 0$ tel que $p^k \mid n$. L'application v_p se prolonge sur $\mathbf{Q} \setminus \{0\}$ via la formule $v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b)$, et sur $\mathbf{Q}$ tout entier en posant $v_p(0) = \infty$.

1. Vérifier que :
   — la formule étendant v_p à un rationnel r ne dépend pas de l'écriture de r comme quotient d'entiers,
   — pour tout $x, y \in \mathbf{Q}$ on a $v_p(xy) = v_p(x) + v_p(y)$,
   — pour tout $x, y \in \mathbf{Q}$ on a $v_p(x+y) \geq \min(v_p(x), v_p(y))$, avec égalité si $v_p(x) \neq v_p(y)$.
2. Pour tout $n \geq 1$ et pour tout $k \in \{1, \ldots, p^n - 1\}$, montrer que $v_p\left(\binom{p^n}{k}\right) = n - v_p(k)$.
3. Montrer que pour tout $n \in \mathbf{N}$, on a $v_p(n!) = \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor$.
4. Montrer que pour tout $n > 1$, le rationnel $\sum_{k=1}^{n} \frac{1}{k}$ n'est pas entier.

Exercice 6 Déterminer un générateur de $(\mathbf{Z}/125\mathbf{Z})^\times$. Combien ce groupe admet-il de générateurs ?

Exercice 7 Soient $a > 0, b > 0$ des entiers. On note $d = \text{pgcd}(a, b)$ et $\ell = \text{ppcm}(a, b)$. Montrer que le système de congruences

$$\begin{cases} x \equiv y_1 \,(\text{mod}\, a) \\ x \equiv y_2 \,(\text{mod}\, b) \end{cases}$$

admet une solution $x \in \mathbf{Z}$ si et seulement si $d \mid (y_1 - y_2)$ et que dans ce cas, la classe de x modulo ℓ est unique.

Exercice 8 Soit $m > 0$ et $n > 0$ deux entiers. On suppose $m \mid n$. Montrer que l'homomorphisme naturel $(\mathbf{Z}/n\mathbf{Z})^\times \to (\mathbf{Z}/m\mathbf{Z})^\times$ est surjectif.

Exercice 9 Soit G un groupe cyclique d'ordre n. Étudier, pour $d \geq 1$ donné et $y \in G$ fixé, l'existence et le nombre de solutions à l'équation $x^d = y, x \in G$.

Que dire de la résolubilité et du nombre de solutions de la même équation dans $\mathbf{F}_p^*$?

Exercice 10 Résoudre dans $\mathbb{Z}^3$ l'équation $12x + 14y + 21z = 5$.

Exercice 11 Soit p premier, $n \geq 1$ un entier, et a un entier tel que $p \nmid a$.

1. On suppose p impair. Montrer que a est un carré modulo p^n si et seulement si a est un carré modulo p.
2. Supposons $p = 2$ et $n \geq 3$. Montrer que a est un carré modulo 2^n si et seulement si $a \equiv 1 \,(\text{mod}\, 8)$.
3. Déterminer le nombre de solutions à la congruence $x^2 \equiv 1 \,(\text{mod}\, 6125)$.
4. Montrer que le polynôme à coefficients entiers $P(X) = (X^2-13)(X^2-17)(X^2-221)$ admet des racines modulo p pour tout p mais pas de racine rationnelle.

Exercice 12

1. Soit p premier. Montrer que le polynôme $X^p - X - 1$ est irréductible dans $\mathbf{Q}[X]$ (on pourra raisonner par réduction modulo p).
2. Montrer que $X^4 + 1$ est irréductible sur $\mathbf{Q}$ mais réductible modulo p pour tout premier p.

Exercice 13 Soit $p \geq 5$ un nombre premier. Montrer que les assertions suivantes sont équivalentes :

(i) $p \equiv 1 \,(\text{mod}\, 3)$,

(ii) $\mathbf{F}_p^\times$ possède un élément d'ordre 3,

(iii) $X^2 + X + 1$ possède une racine dans $\mathbf{F}_p$,

(iv) -3 est un carré non nul modulo p.

Exercice 14 (*Lemme de Hensel*) Soit $P \in \mathbf{Z}[X]$ un polynôme unitaire, $n \geq 1$, et p un nombre premier. On suppose qu'il existe $x \in \mathbf{Z}$ tel que $P(x) \equiv 0 \,(\mathrm{mod}\, p^n)$ et $P'(x) \not\equiv 0 \,(\mathrm{mod}\, p)$. Montrer qu'il existe $\tilde{x} \in \mathbf{Z}$ tel que

$$P(\tilde{x}) \equiv 0 \,(\mathrm{mod}\, p^{2n}) \qquad \text{et} \qquad \tilde{x} \equiv x \,(\mathrm{mod}\, p^n)\,.$$

Montrer en outre que la classe de $\tilde{x}$ modulo p^{2n} est unique.

Exercice 15 (*Nombres de Carmichael*) Un *nombre de Carmichael* est un entier $n > 1$ composé (i.e. non premier) tel que pour tout $a \in \mathbf{Z}$, on a $a^n - a \equiv 0 \,(\mathrm{mod}\, n)$.

1. Montrer que n est un nombre de Carmichael si et seulement si les trois conditions suivantes sont vérifiées :
   — n est composé,
   — n est sans facteur carré,
   — pour tout premier p facteur de n on a $(p-1) \mid (n-1)$.
2. Montrer qu'un nombre de Carmichael est toujours impair et possède au moins trois facteurs premiers distincts.
3. Soit $k \geq 1$ un entier tel que $6k+1, 12k+1, 18k+1$ sont tout trois premiers (par exemple $k = 1$). Montrer que le produit $(6k+1)(12k+1)(18k+1)$ est un nombre de Carmichael.

Exercice 16 Dans cet exercice, on montre que l'équation $y^2 = x^3 + 7$ n'a pas de solutions entières. Par l'absurde, fixons une solution $(x, y) \in \mathbf{Z}^2$.

1. Quelles sont les classes possibles pour x et y modulo 4 ?
2. En utilisant l'égalité $x^3 + 8 = (x+2)(x^2 - 2x + 4)$, montrer que $x^3 + 8$ possède un facteur premier $p \equiv 3 \,(\mathrm{mod}\, 4)$ et déduire une contradiction.

Exercice 17 (*Polynômes cyclotomiques*) Soit $n \geq 1$ un entier. On note $\zeta_n := \exp(2i\pi/n)$ et on appelle *n-ème polynôme cyclotomique* le polynôme

$$\Phi_n(X) = \prod_{\substack{1 \leq k \leq n \\ \mathrm{pgcd}(k,n)=1}} (X - \zeta_n^k)\,.$$

1. Montrer que
$$X^n - 1 = \prod_{d \mid n} \Phi_d\,,$$
puis en déduire que $\Phi_n \in \mathbf{Z}[X]$ et $\sum_{d \mid n} \varphi(d) = n$.
2. Pour p premier et $r \geq 1$ entier, calculer Φ_p et Φ_{p^r}.
3. Montrer que si $\mathrm{pgcd}(m, n) = 1$ alors $\Phi_m(X^n) = \prod_{d \mid n} \Phi_{md}(X)$. En déduire que si p est premier et ne divise pas m, on a
$$\Phi_{pm}(X) = \frac{\Phi_m(X^p)}{\Phi_m(X)}\,,$$
puis calculer $\Phi_{21}(X)$.

4. Le but de cette question est de montrer que pour tout $n \geq 1$, le polynôme Φ_n est irréductible dans $\mathbf{Z}[X]$. Soit ζ une racine primitive n-ième de l'unité, et $f \in \mathbf{Z}[X]$ le facteur irréductible de Φ_n tel que $f(\zeta) = 0$. (Dans quelle mesure est-il unique ?) Écrivons $X^n - 1 = f(X)h(X)$, avec $h(X) \in \mathbf{Z}[X]$. Dans les questions (a) et (b), on suppose qu'il existe un nombre premier p ne divisant pas n tel que $f(\zeta^p) \neq 0$.
   (a) Montrer que $f(X)$ divise $h(X^p)$ dans $\mathbf{Z}[X]$.
   (b) En déduire que les réductions modulo p de f et h ne sont pas des polynômes premiers entre eux de $\mathbf{F}_p[X]$, puis que la réduction modulo p de $X^n - 1$ n'est pas sans facteur carré dans $\mathbf{F}_p[X]$.
   (c) Conclure.

Exercice 18 (*Théorème de Chevalley–Warning*) On fixe un nombre premier p.

1. Soit $m \geq 0$ un entier. Montrer que
$$\sum_{x \in \mathbf{F}_p} x^m = \begin{cases} -1 & \text{si } m \geq 1 \text{ et } (p-1) \mid m\,, \\ 0 & \text{sinon.} \end{cases}$$
2. Dans cette question on montre le *théorème de Chevalley–Warning* : soit $P_1, \ldots, P_r$ une famille de polynômes de $\mathbf{F}_p[X_1, \ldots, X_n]$ telle que $\sum_{i=1}^r \deg P_i < n$ et soit V l'ensemble des zéros communs dans $\mathbf{F}_p^n$ aux polynômes $P_1, \ldots, P_r$. Alors $\operatorname{Card} V \equiv 0 \pmod p$.
   (a) Montrer que le polynôme $P := \prod_{i=1}^r (1 - P_i^{p-1})$ coïncide sur $\mathbf{F}_p^n$ avec la fonction indicatrice de V.
   (b) On note S l'application définie par $S(Q) = \sum_{x \in \mathbf{F}_p^n} Q(x)$ pour tout $Q \in \mathbf{F}_p[X_1, \ldots, X_n]$. Vérifier que $S(P)$ est égal à $\operatorname{Card} V$ modulo p (en quel sens précisément ?).
   (c) En décomposant P sur la base des monômes $X_1^{m_1} \cdots X_n^{m_n}$, calculer $S(P)$ en utilisant la question 1. Conclure.
3. Soit $P_1, \ldots, P_r$ vérifiant les hypothèses du théorème de Chevalley–Warning. On suppose en outre les P_i homogènes. Montrer que les polynômes P_i admettent dans $\mathbf{F}_p^n$ un autre zéro commun que $(0, \ldots, 0)$.