Tous les exercices sont indépendants et peuvent être traités dans un ordre quelconque. Le polycopié du cours est le seul docuemnt autorisé. La note maximale pourra être atteinte sans que tous les exercices soient traités.

Exercice 1. *Soit p un nombre premier impair. Montrer que les deux nombres complexes $i^{(p-1)/2}(1+i)2^{(p-1)/2}$ et $1+i^p$ appartiennent à $\mathbb{Z}[i]$ et sont égaux modulo $p\mathbb{Z}[i]$. En déduire $\left(\frac{2}{p}\right)$.*

Exercice 2. *a) Existe-t-il un corps de nombres K de degré ≥ 3 tel que tout élément de $\mathbb{Z}_K^\star$ soit un cube dans $\mathbb{Z}_K^\star$?*
b) Existe-t-il un corps de nombres K de degré 2 tel que tout élément de $\mathbb{Z}_K^\star$ soit un cube dans $\mathbb{Z}_K^\star$?

Exercice 3. *Soit $P = X^4 - X^2 - 2X + 3$. Factoriser P sur $\mathbb{F}_2$ et $\mathbb{F}_3$. Ce polynôme est-il irréductible sur $\mathbb{Z}$?*

Exercice 4. *Soit (E) l'équation*

$$2x^4 = y^4 - 17z^4$$

d'inconnues $(x, y, z) \in \mathbf{Z}^3$. L'objet du problème est de montrer que (E) n'a pas de solutions non triviales. Et l'on considère par l'absurde une telle solution (x, y, z).
a) Montrer qu'alors (E) admet une solution, toujours notée (x, y, z), à coordonnées globalement premières entre elles.
b) Montrer que 2 est un carré modulo 17.
c) Montrer que x n'est pas multiple de 17.
d) Montrer que x n'est pas un carré modulo 17.
e) Soit p un nombre premier impair qui divise x (on a donc $p \neq 17$). Montrer que 17 est un carré modulo p, puis que p est un carré modulo 17.
f) Montrer que x est un carré modulo 17, et conclure.

Exercice 5. *On pose*

$$A(n) = \left(\begin{array}{c} 2n \\ n \end{array} \right) = \prod_{p \leq 2n} p^{a_p} \ ,$$

démontrer

$$a_p = \sum_{m=1}^{\infty} \left(\left[\frac{2n}{p^m} \right] - 2 \left[\frac{n}{p^m} \right] \right) \ .$$

a) Soit $p \leq n$ un facteur premier de $A(n)$, montrer que $p \leq \frac{2n}{3}$ (pour n assez grand, que l'on précisera).
b) Soit p un facteur premier de $A(n)$ tel que $a_p \geq 2$; montrer que $p \leq \sqrt{2n}$.
c) On admettra que $\theta(n) \leq 2n\log(2)$, pour $n \geq 1$, où $\theta(x) = \sum_{p \leq x} \log(p)$. On suppose qu'il n'y a pas de nombre premier compris entre n et $2n$. Montrer que $\log(A(n)) \leq \frac{4}{3}n + \sqrt{2n}\log(2n)$.
d) Montrer que $A(n) \geq 2^{2n}/n$ et en déduire qu'il existe au moins un nombre premier compris entre n et $2n$ si $n \geq 1000$.
e) Démontrer l'inégalité $\theta(n) \leq 2n\log(2)$.

Exercice 6. *On note μ le fonction de Möbius ($\mu(n) = 0$ s'il existe $m \geq 2$ tel que $m^2 \mid n$, $\mu(n) = 1$ si n a un nombre pair de diviseurs premiers et $\mu(n) = -1$ si n admet un nombre impair de diviseurs premiers).*
a) Montrer que la série $S = \sum_{n \geq 1} \frac{\mu(n)}{n}$ est convergente.
b) Montrer $S = 0$.

Le corollaire 7.25 du cours affirme que le groupe des classes $C(K)$ est engendré par les classes d'idéaux maximaux de norme $\leq c = \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|\mathrm{disc(K)}|}$; on admettra que l'on peut en fait prendre $c = \left(\frac{4}{\pi}\right)^{r_2} \frac{d!}{d^d} \sqrt{|\mathrm{disc(K)}|}$, où d est le degré de K.

Exercice 7. *a) Soit $K = \mathbb{Q}[X]/(X^4 - X - 1)$ et u la classe de X dans le quotient. Calculer le discriminant de K.*
b) Montrer que $\mathbb{Z}_K = \mathbb{Z}[u]$.
c) Calculer le nombre de plongements réels r_1 de K et le nombre de plongements complexes r_2 à conjugaison près.
d) Montrer que le groupe des classes d'idéaux $C(K)$ est engendré par les classes d'idéaux maximaux de norme au plus 2.
e) Montrer que $\mathbb{Z}_K$ est principal.
f) Vérifier que $X - 3$ divise $X^4 - X - 1$ dans $\mathbb{F}_7[X]$. Est-ce qu'il existe un élément $a \in \mathbb{Z}_K$ de norme ± 7 ? Si oui, y en a-t-il une infinité ? Existe-t-il un élément de norme $+7$?

Exercice 8. *Soit A l'anneau $\mathbb{Z}[X]/(X^3 - 5)$ et notons u la classe de x dans A. Nous notons K le corps des fractions de A.*
a) calculer le discriminant de A.
b) Donner des générateurs pour les idéaux maximaux de A contenant 3.
c) Donner des générateurs pour les idéaux maximaux de A contenant 5.
d) Montrer que A est l'anneau des entiers de K (au dessus de 3 on pourra faire la substitution $x = y + 2$).
e) Montrer tout élément du groupe des classes d'idéaux est représenté par un idéal de norme au plus 7.
f) Donner une majoration du cardinal du groupe des classes d'idéaux.
g) Est-ce que l'équation $a^3 + 5b^3 + 25c^3 - 15abc = 1$ a des solutions dans $\mathbb{Z}$ autres que $(1, 0, 0)$?

Exercice 9. *Montrer que la série $\sum_{k=0}^{\infty} p^k$ converge dans $\mathbb{Q}_p$ et calculer sa limite.*

Exercice 10. *Soit $f(x) = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{Z}_p[X]$. On suppose que $v_p(a_i) \geq 1$ pour $i \leq n-1$ et $v_p(a_0) = 1$. Montrer que $f(x)$ est irréductible sur $\mathbb{Q}_p[X]$. En déduire pour $m \geq 1$ le degré sur $\mathbb{Q}_p$ de ζ_{p^m}, où ζ_{p^m} est une racine de l'unité, primitive d'ordre p^m.*