Une équation diophantienne est une équation polynomiale à coefficients entiers dont on cherche les solutions entières.
Références : R. Descombes, Éléments de théorie des nombres ; D. Duverney Théorie des nombres.

Corrigé :

Exercice 1. (L'équation de Pell).
Soit d un entier strictement positif qui n'est pas le carré d'un nombre entier.

a) Montrer que $\sqrt{d}$ est irrationnel.

b) Montrer qu'il existe un entier $n \neq 0$ tel que l'équation $x^2 - dy^2 = n$ possède une infinité de solutions. (Utiliser le théorème de l'exercice 2)
On fixe un tel entier dans la suite de l'exercice.

c) Montrer qu'il existe des solutions distinctes (x_1, y_1) et (x_2, y_2) de l'équation $x^2 - dy^2 = n$ telles que $x_1 \equiv x_2 \pmod{n}$ et $y_1 \equiv y_2 \pmod{n}$.

d) Écrire la fraction $(x_1 + y_1\sqrt{d})/(x_2 + y_2\sqrt{d})$ sous la forme $x_3 + y_3\sqrt{d}$. Montrer que x_3 et y_3 sont entiers et vérifient $(x_3)^2 - d(y_3)^2 = 1$.

e) Soit $(u, v) \in \mathbb{N}^2$ une solution de l'équation $x^2 - dy^2 = 1$ où $v > 0$ est minimal. Soit $(x, y) \in \mathbb{N}^2$ une autre solution. Si $y > 0$, simplifier $(x + y\sqrt{d})/(u + v\sqrt{d})$ et construire une solution $(x', y') \in \mathbb{N}^2$ telle que $0 < y' < y$.

f) Montrer que les solutions de l'équation $x^2 - dy^2 = 1$ sont de la forme $(\pm x_k, \pm y_k)$, pour $k \in \mathbb{Z}$, où x_k et y_k sont déterminés par la relation $x_k + y_k\sqrt{d} = (u + v\sqrt{d})^k$. (Utiliser la méthode de descente infinie)

a) Si $\sqrt{d} = m/n$ alors $m^2 = dn^2$, et tout nombre premier divise d avec exposent pair. Alors d est un carré.
b) Par le théorème de l'exercice 2 il existe une infinité de couples $(p, q) \in \mathbb{N}^* \times \mathbb{N}^*$ telles que $|p - q\sqrt{d}| < 1/q$. Alors $|p + q\sqrt{d}| < 2q\sqrt{d} + 1/q$ et

$$|p^2 - dq^2| < 2\sqrt{d} + 1.$$

Comme $p^2 - dq^2$ ne prend que des valeurs entières, il existe un entier n tel que on ait $p^2 - dq^2 = n$ pour une infinité de $(p, q) \in \mathbb{N}^* \times \mathbb{N}^*$.
c) Il n'y a qu'un nombre fini des couples $x \pmod{n}, y \pmod{n}$.
d) $x_3 = (x_1x_2 - dy_1y_2)/n$, $y_3 = (x_2y_1 - x_1y_2)/n$. x_3 est entier puisque $x_1x_2 - dy_1y_2 \equiv x_1^2 - dy_1^2 \equiv n \equiv 0 \pmod{n}$. Pareil pour y_3. $(x_3)^2 - d(y_3)^2 = 1$ par la multiplicativité de la norme $N(x+y\sqrt{d}) = (x^2 - dy^2)^2$ dans $\mathbb{Q}[\sqrt{d}]$.
e) $0 = x^2(dv^2+1) - u^2(dy^2+1) = d(xv - uy)(xv + uy) + d(y^2 - v^2)$. Soit $x' + y'\sqrt{d} = (x+y\sqrt{d})/(u+v\sqrt{d})$ Alors

$$y' = yu - xv = \frac{y^2 - v^2}{xv + uy} < y.$$

et $y' > 0$ si $y > v$.
f) Par la multiplicativité de la norme, $x_k + y_k\sqrt{d} = (u + v\sqrt{d})^k$ est une solution. Inversement, etant donné une solution (x, y). Si $y = 0$ alors on peut prendre $k = 0$. Sinon, par e), si on divise $x + y\sqrt{d}$ par $(u + v\sqrt{d})$ on diminue y qui reste strictement positive si $y > v$.

Exercice 2.

a) Soit α irrationnel. Montrer que pour tout entier $Q > 1$, il existe un rationnel p/q tel que $1 \leq q < Q$ et $0 < |q\alpha - p| \leq 1/Q$. (Utiliser le principe des tiroires)

b) Montrer le resultat suivant :
Théorème (Dirichlet). Soit α irrationnel. Alors il existe une suite infinie de rationnels $P_k, /Q_k$ vérifiant

$$0 < |\alpha - P_k/Q_k| \leq 1/Q_k^2.$$

Considérons les $Q+1$ nombres 0, 1, $j\alpha - j[\alpha]$, $j = 1, \ldots, Q-1$, (où [x] désigne la partie entière de x). Ces $Q+1$ nombres sont contenus dans $[0,1]$ alors, par le principe des tiroires, il en existe deux contenus dans le même sous-intervalle de longueur $1/Q$. Alors il existe $0 \leq a_1 < a_2 \leq Q-1$, $a_i \in \mathbb{N}$ et des entiers b_1, b_2 tels que

$$0 < |(a_2 - a_1)\alpha + (b_2 - b_1)| \leq 1/Q.$$

Alors pour $p = b_2 - b_1$ et $q = a_2 - a_1$ nous avons

$$0 < |\alpha - p/q| < 1/(qQ) < 1/q^2.$$

Posons alors $P_1 = p$ et $Q_1 = q$. Supposons que nous avons construit $P_1/Q_1, \cdots, P_m/Q_m$. Soit Q tel que $1/Q < |\alpha - P_k/Q_k|$ pour $k = 1, \ldots, m$. Par (a) il existe un rationnel p/q, $0 < q < Q$ tel que $|\alpha - p/q| < 1/(qQ)$. D'où $|\alpha - p/q| < 1/q^2$ et $|\alpha - p/q| < |\alpha - P_k/Q_k|$ pour $k = 1, \ldots, m$ donc $p/q \neq P_k/Q_k$ pour $k = 1, \ldots, m$. Posons $P_{m+1} = p$ et $Q_{m+1} = q$.

Exercice 3. *(Equations diophantiennes du premier du premier degré)*

a) Résoudre dans $\mathbb{Z}$ l'équation : $3x + 4y = c$ pour $c = 0, 1, 6$.

b) Montrer que l'équation $ax + by = c$, $a, b, c \in \mathbb{Z}$, $a \neq 0$, $b \neq 0$, admet une solution entière ssi le $pgcd(a, b)$ divise c

c) Résoudre dans $\mathbb{Z}$ l'équation : $15x + 6y + 10z = 1$.

d) Montrer que l'ensemble des solutions de $AX = B$ où $A \in \mathcal{M}_{n,p}(\mathbb{Z})$ et $B \in \mathbb{Z}^n$ est soit vide soit de la forme : une solution particulière plus un sous-réseau de $\mathbb{Z}^p$ de rang $p - rg(A)$.

a) $c = 0$: $x = 4k, y = -3k$, $k \in \mathbb{Z}$
$c = 1$: $x = 4k - 1, y = -3k + 1$, $k \in \mathbb{Z}$
$c = 6$: $x = 4k + 2, y = -3k$, $k \in \mathbb{Z}$.
b) par Bezout
c) D'abord nous alons résoudre $15x + 6y + 10z = 0$. Rappelons que par le théorème de la base adaptée si $A \in M_{n,m}(\mathbb{Z})$ alors il existe une base de $\mathbb{Z}^n$ et une de $\mathbb{Z}^m$ dans lesquelles $A = \begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}$, où $D = diag(d_1, \ldots, d_r)$, et $d_1, \ldots, d_r$ sont non nuls vérifient $d_1 | \cdots | d_r$.. Dans notre cas la matrice $(15, 6, 10)$ est équivalente dans la base $(-1, 1, 1), (4, -5, -3), (6, -5, -6)$ de $\mathbb{Z}^3$ à la matrice $(1, 0, 0)$. Alors les solutions sont $k(4, -5, -3) + l(6, -5, -6)$, $k, l \in \mathbb{Z}$.
$(x, y, z) = (-1, 1, 1)$ donne une solution particulière de $15x + 6y + 10z = 1$. Alors les solutions sont $(-1, 1, 1) + k(4, -5, -3) + l(6, -5, -6)$, $k, l \in \mathbb{Z}$.
d) résulte du théorème de la base adaptée