Introduction aux équations diophantiennes

Choukri Saâd

Stage de Novembre 2018

0- Table des matières

1 Généralités **2**

2 Méthodes élémentaires de résolution **2**
2.1 Factorisations, décompositions . . . 2
2.2 Utilisation de la récurrence . . . 5
2.3 Méthode de la représentation paramétrique . . . 6
2.4 Utilisation du discriminant d'un trinôme . . . 6
2.5 Principe de la descente infinie . . . 8
2.6 L'équation $x^2 - y^2 = n$ . . . 9
2.7 Exercices . . . 9
2.8 Solutions des exercices . . . 10

3 Résolution à l'aide des congruences, inégalités **11**
3.1 Utilisation des congruences . . . 11
3.2 Utilisation des inégalités . . . 14
3.3 Exercices . . . 15
3.4 Solutions des exercices . . . 15

4 Équations diophantiennes linéaires **16**
4.1 L'équation $ax + by = c$ . . . 16
4.2 Autres équations diophantiennes linéaires . . . 16
4.3 Exercices . . . 16
4.4 Solutions des exercices . . . 16

5 Équations diophantiennes quadratiques, cubiques **16**
5.1 Triplets pythagoriciens . . . 16
5.2 L'équation $x^4 + y^4 = z^4$ . . . 16
5.3 Équations de Pell . . . 16
5.4 Autres équations diophantiennes quadratiques . . . 16
5.5 Équations cubiques . . . 16
5.6 Exercices . . . 16
5.7 Solutions des exercices . . . 16

6 Construction de solutions, Vietta Jumping **16**
6.1 Construction des solutions . . . 16
6.2 Vietta Jumping . . . 16
6.3 Exercices . . . 16
6.4 Solutions des exercices . . . 16

7 Florilège d'équations de tout genre **16**
7.1 Exercices . . . 16
7.2 Solutions des exercices . . . 16

1- Généralités

Une équation diophantienne est une équation à coefficients entiers dont on cherche des solutions entières. Il n'existe pas de méthode générale pour résoudre une équation diophantienne. Cependant, il existe plusieurs techniques et approches pour attaquer une équation diophantienne. Dans ce cours on va découvrir plusieurs techniques à savoir les méthodes élémentaires de résolution, l'utilisation des congruences, l'utilisation des inégalités, équations diophantiennes linéaires et finalement les équations diophantiennes quadratiques et cubiques.

Définition. On appelle une équation diophantienne une équation de la forme

$$f(x_1, x_2, ..., x_n) = 0$$

où f est une fonction à n variables avec $n \geq 2$. Si f est une fonction polynomiale à coefficients entiers, on dit que l'équation est une équation algébrique diophantienne.

En théorie des équations diophantiennes, trois questions principales se posent,
- L'équation est-elle résoluble ?
- Dans le cas où l'équation est résoluble, le nombre de solutions est il fini ou infini ?
- Dans le cas où l'équation est résoluble, déterminer toutes les solutions.

Notez qu'en général, les équations diophantiennes font intervenir plusieurs et souvent un grand nombre d'inconnues. Notez également que les techniques utilisées pour aborder les équations diophantiennes sont très souvent radicalement différentes des techniques d'attaque pour les équations algébriques.

2- Méthodes élémentaires de résolution

Les propriétés des entiers et les notions de divisibilité sont essentielles dans la résolution des équations diophantiennes.

2.1- Factorisations, décompositions

Pour résoudre des équations diophantiennes, on a besoin de savoir plusieurs identités remarquables que nous allons présenter par la suite.

Soit a et b des nombres réels et n un entier naturel non nul. Alors

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + ... + ab^{n-2} + b^{n-1}) = (a-b)\sum_{p=0}^{n-1} a^p b^{n-1-p}$$

Démonstration. Si $b = 0$ ou si $a = b$, c'est évident. Supposons que $b \neq 0$, alors en posant $c = a/b$ il s'agit de montrer que

$$c^n - 1 = (c-1)(c^{n-1} + c^{n-2} + ... + c + 1)$$

en utilisant les suites géométriques pour $c \neq 1$, ce qui est vrai puisque

$$1 + c + ... + c^{n-1} = \frac{1-c^n}{1-c}$$

Soit a et b des nombres réels et n un entier naturel impair, alors

$$a^n + b^n = (a+b)(a^{n-1} - ab^{n-2} + ... + ab^{n-2} - b^{n-1}) = (a+b)\sum_{p=1}^{n-1}(-1)^p a^p b^{n-1-p}$$

Démonstration. On a

$$a^n + b^n = a^n - (-b)^n = (a-(-b))\sum_{p=1}^{n-1} a^p(-b)^{n-1-p} = (a+b)\sum_{p=1}^{n-1}(-1)^p a^p b^{n-1-p}$$

en utilisant l'identité précédente.

Soit a et b des nombres réels et n un entier naturel non nul,

$$a^{2^n} - b^{2^n} = (a-b)\times(a+b)\times(a^2+b^2)\times(a^4+b^4)\times\ldots\times(a^{2^{n-1}}+b^{2^{n-1}}) = (a-b)\times\prod_{p=1}^{n-1}(a^{2^p}+b^{2^p})$$

Démonstration. On procède par récurrence pour montrer cette identité. Pour $n = 1$, c'est trivial. Supposons l'identité vraie pour le rang $n \geq 1$ et montrons qu'elle est vraie pour le rang $n+1$. Soient a et b des nombres réels, on a

$$(a^{2^{n+1}}-b^{2^{n+1}}) = [(a^{2^n})^2-(b^{2^n})^2] = (a^{2^n}-b^{2^n})\times(a^{2^n}+b^{2^n}) = (a-b)\times\prod_{p=1}^{n-1}(a^{2^p}+b^{2^p})\times(a^{2^n}+b^{2^n}) = (a-b)\times\prod_{p=1}^{n}(a^{2^p}+b^{2^p})$$

d'où le résultat est vrai pour le rang $n+1$. Donc l'identité est vrai pour tous réels a et b et pour tout entier naturel non nul n.

Donnons une identité remarquable très importante appelé l'identité de *Sophie Germain*.

Soient a et b des nombres réels, alors

$$a^4 + 4b^4 = (a^2+2b^2+2ab)(a^2+2b^2-2ab)$$

Démonstration. Soient a et b des nombres réels, alors

$$a^4 + 4b^4 + 4a^2b^2 - 4a^2b^2 = (a^2+2b^2)^2 - (2ab)^2 = (a^2+2b^2+2ab)(a^2+2b^2-2ab)$$

D'où l'identité.

Soit a un nombre réel, alors

$$a^4 + 1 = (a^2+\sqrt{2}a+1)(a^2-\sqrt{2}a+1)$$

Démonstration. Soit a un nombre réel, on a

$$a^4 + 1 = a^4 + 2a^2 + 1 - 2a^2 = (a^2+1)^2 - (\sqrt{2}a)^2 = (a^2+1+\sqrt{2}a)(a^2+1-\sqrt{2}a)$$

D'où l'identité.

Soient a, b et c des nombres réels, on a

$$a^3+b^3+c^3-3abc = (a+b+c)(a^2+b^2+c^2-ab-bc-ca)$$

Démonstration. Soient a, b et c des nombres réels, en développant le côté de droite on trouve le côté de gauche.

Soient a et b deux nombres réels, et n un entier naturel non nul, on a

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

Démonstration. Si $b = 0$, on a bien sur la formule. Supposons $b \neq 0$, en divisant les deux membres de l'égalité par b^n, on trouve

$$(c+1)^n = \sum_{k=0}^{n} \binom{n}{k} c^k \qquad (*)$$

où $c = a/b$. Montrons par un argument combinatoire la formule $(*)$. Notons c_k le coefficient de c^k où $0 \leq k \leq n$ dans le développement de $(c+1)^n$. Nous obtenons c^k en effectuant $\underbrace{c \times c \times ... \times c}_{k}$, donc c_k est le nombre de manières de choisir k, $(1+c)$ parmi n, $(1+c)$ dans le produit $(1+c)^n$, il s'en suit que $c_k = \binom{n}{k}$. D'où $(*)$.

Voyons par la suite des exemples simples sur la résolution des équations diophantiennes en utilisant les factorisations.

(Maroc 2018) Déterminer tous les couples d'entiers naturels (x, y) tels que,

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{5}$$

Soit (x, y) une solution éventuelle de l'équation ci-dessus. L'équation ci-dessus est équivalente à

$$5x + 5y - xy = 0$$

i.e.

$$5x - xy + 5y = (5-y)x + 5y - 25 = -25$$

qui est équivalente à

$$(x-5)(y-5) = 25$$

Ceci est équivalent à

$$\begin{cases} x-5 = 1 \\ y-5 = 25 \end{cases} \quad \begin{cases} x-5 = 25 \\ y-5 = 1 \end{cases} \quad \begin{cases} x-5 = 5 \\ y-5 = 5 \end{cases}$$

c-à-d

$$\begin{cases} x = 6 \\ y = 30 \end{cases} \quad \begin{cases} x = 30 \\ y = 6 \end{cases} \quad \begin{cases} x = 10 \\ y = 10 \end{cases}$$

Donc

$$S = \{(5,5), (6,30), (30,6)\}$$

Trouver tous les entiers naturels x et n tels que

$$2^n + 1 = x^2$$

On passe le 1 de l'autre côté de l'égalité et on factorise,

$$(x-1)(x+1) = 2^n$$

Donc $x-1$ et $x+1$ sont des puissances de 2, or les seules puissances de 2 qui différent de 2 sont 2 et 4, il vient que $x = 3$ et par suite $2^n + 1 = 9$, donc $n = 3$. Réciproquement le couple $(3, 3)$ est une solution. Donc l'unique solution du problème est $(3, 3)$.

(Inde) Déterminer les solutions entières positives de l'équation

$$(xy-7)^2 = x^2+y^2$$

L'équation est équivalente à l'équation

$$(xy-6)^2 + 13 = (x+y)^2$$

i.e.

$$[xy-6-(x+y)] \times [xy-6+(x+y)] = -13$$

Ce qui donne le système d'équations

$$\begin{cases} xy-6-(x+y) = -1 \\ xy-6+(x+y) = 13 \end{cases} \qquad \begin{cases} xy-6-(x+y) = -13 \\ xy-6+(x+y) = 1 \end{cases}$$

Ce qui est équivalent à

$$\begin{cases} x+y = 7 \\ xy = 12 \end{cases} \qquad \begin{cases} x+y = 7 \\ xy = 0 \end{cases}$$

Donc

$$S = \{(3,4),(4,3),(0,7),(7,0)\}$$

(Maroc 2018) Soit p un nombre premier et a et n deux entiers naturels satisfaisant l'équation

$$2^p + 3^p = a^n$$

Montrer que $n = 1$.

Il évident que le cas $n = 0$ amène à une absurdité. Si $p = 2$, on a alors $a^n = 13$ et par suite $n = 1$. Supposons que p est un nombre premier impair, on a

$$(2+3) \times (2^{p-1} - 3 \times 2^{p-2} + ... + 3^{p-2} \times 2 - 3^{p-1}) = a^n$$

Donc 5 divise a^n et puisque 5 est un nombre premier, alors 5 divise a. Supposons que $n \geq 2$, alors 25 divise $a^n = a^2 \times a^{n-2}$. Par suite

$$2^{p-1} - 3 \times 2^{p-2} + ... + 3^{p-2} \times 2 - 3^{p-1} \equiv 0 \pmod 5$$

Mais on a $2 \equiv -3 \pmod 5$, donc

$$3^{p-1} - 3^{p-1} + ... + (-1)^{\frac{p-1}{2}} 3^{\frac{p-1}{2}} 2^{\frac{p+1}{2}} + ... + 3^{p-1} - 3^{p-1} \equiv 0 \pmod 5$$

Donc 5 divise $3^{(p-1)/2} \times 2^{(p+1)/2}$, ce qui est impossible puisque $5 \wedge 2 = 5 \wedge 3 = 1$. En conclusion $n = 1$.

2.2- Utilisation de la récurrence

Le raisonnement par récurrence est un outil très efficace pour résoudre des équations diophantiennes. Voyons des exemples par la suite.

Montrer que pour tout entier $n \geq 3$ l'équation

$$\frac{1}{x_1} + \frac{1}{x_2} + ... + \frac{1}{x_n} = 1$$

admet des solutions entières strictement positives distincts deux à deux.

Pour $n = 3$, le résultat est vrai puisque $1/2 + 1/3 + 1/6 = 1$. Supposons que le résultat est vrai pour un rang k, on a

$$\frac{1}{x_1} + \frac{1}{x_2} + ... + \frac{1}{x_k} = 1$$

et par suite

$$\frac{1}{2} + \frac{1}{2x_1} + ... + \frac{1}{2x_k} = 1$$

Donc le $(n+1)$-uplet $(2, 2x_1, ..., 2x_k)$ pour le rang $k+1$. D'où le résultat par principe de récurrence.

2.3- Méthode de la représentation paramétrique

Il peut arriver que les solutions entières d'une équation diophantienne peuvent s'exprimer en fonction de quelques paramètres. La méthode de la représentation paramétrique permet de montrer l'existence d'une infinité de solution de l'équation diophantienne. Voyons quelques exemples permettant d'illustrer cette méthode.

(Tournoi des villes) Montrer qu'il existe une infinité de triples d'entiers tels que

$$x^3 + y^3 + z^3 = x^2 + y^2 + z^2$$

En prenant $z = -y$ l'équation devient $x^3 = x^2 + 2y^2$ et puis en prenant $y = mx$ avec $m \in \mathbb{Z}$, l'équation devient $x = 1 + 2m^2$. Ainsi on a une famille infinie de solutions donnée par

$$\begin{cases} x = 2m^2 + 1 \\ y = m(2m^2 + 1) \\ z = -m(2m^2 + 1) \end{cases} \quad \text{où} \quad m \in \mathbb{Z}$$

Déterminer les triplets (x, y, z) d'entiers naturels non nuls tels que

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{z}$$

L'équation donnée est équivalente à $z = \dfrac{xy}{x+y}$. On pose $x \wedge y = d$, alors $x = dn$ et $y = dm$ avec $n \wedge m = 1$. Donc $z = \dfrac{dmn}{m+n}$, donc $m + n$ divise dmn et puisque $(m+n) \wedge mn = 1$, par le lemme de Gauss $m + n$ divise d, i.e. $d = k(m+n)$ où $k \in \mathbb{N}^*$. En conclusion les solutions sont données par

$$\begin{cases} x = km(m+n) \\ y = kn(m+n) \\ z = kmn \end{cases} \quad avec \quad k, m, n \in \mathbb{N}^*$$

2.4- Utilisation du discriminant d'un trinôme

Commençons par donner une proposition concernant les trinômes unitaires à coefficients dans $\mathbb{Z}$.

Soient $a, b \in \mathbb{Z}$, alors l'équation

$$x^2 + ax + b = 0$$

admet une solution dans $\mathbb{Z}$ si et seulement son discriminant est un carré parfait.

Démonstration. Soient a et b deux entiers relatifs. Supposons que l'équation $x^2 + ax + b$ admet une solution dans $\mathbb{Z}$, soit x_0 cette solution et soit x_1 la seconde solution. On sait que $x_0 + x_1 = -a$, donc $x_1 \in \mathbb{Z}$ et on a $x_0 x_1 = b$. Le discriminant de l'équation $x^2 + ax + b = 0$ est

$$\Delta = a^2 - 4b = (x_0 + x_1)^2 - 4x_0x_1 = (x_0 - x_1)^2$$

qui est évidemment un carré parfait. D'où la condition nécessaire. Réciproquement, supposons que le discriminant Δ de l'équation x^2+ax+b est un carré parfait, i.e. $\Delta = a^2-4b = k^2$ et par suite les solutions de l'équation $x^2+ax+b=0$ sont

$$x_0 = \frac{-a+k}{2}, \quad x_1 = \frac{-a-k}{2}$$

Sachant que $a^2-4b=\alpha^2$, i.e. $4b = a^2-\alpha^2 = (a-\alpha)(a+\alpha)$ donc l'un des deux entiers $a-\alpha$ et $a+\alpha$ est pair, il s'en suit que a et α ont la même parité, et par suite les deux entiers $a-\alpha$ et $a+\alpha$ sont pairs. Par suite les deux solutions x_0 et x_1 sont des entiers, d'où la condition suffisante.

Déterminer tous les entiers naturels n tels que $n+1$ divise n^2-2n+3.

On peut résoudre ce petit problème en utilisant uniquement des arguments de divisibilité. Mais on va utiliser la proposition précédente. Soit n un entier naturel éventuel vérifiant la condition ci-dessus. Alors il existe k entier naturel tel que $n^2-2n+3 = k(n+1)$, ce qui est équivalent à $n^2-(k+2)n+3-k=0$, cette équation admet une solution en vertu de notre hypothèse, donc son discriminant est un carré parfait, c-à-d

$$(2+k)^2-4(3-k) = \alpha^2$$

Ce qui est équivalent à

$$(k+4)^2-\alpha^2 = (k+4-\alpha)(k+4+\alpha) = 24$$

Les solutions de cette équation sont $(k,\alpha)=(1,1)$ et $(k,\alpha)=(3,5)$. Il s'en suit que $n\in\{0,1,2,5\}$, réciproquement il s'agit bien de solutions du problème.

(États unis) Déterminer les solutions entières non nuls de l'équation

$$(x^2+y)(x+y^2) = (x-y)^3$$

L'équation diophantienne ci-dessus est équivalente à

$$2y^2+(x^2-3x)y+3x^2+x=0$$

Cette équation admet une solution si et seulement si sont discriminant $x(x+1)^2(x-8)$ est un carré parfait, il s'en suit que $x(x-8)$ est un carré parfait, i.e. $x(x-8)=z^2$ donc $(x-4)^2-z^2=16$. Ceci fournit $x\in\{-1,8,9\}$ et alors $(x,y)\in\{(-1,-1),(8,-10),(9,-10),(9,-21)\}$. La réciproque donne

$$S = \{(-1,-1),(8,-10),(9,-10),(9,-21)\}$$

(Maroc 2016) Trouver tous les nombres premiers p et q vérifiant

$$p^3+p = q^2+q$$

Soit (p,q) une solution éventuelle. Il est clair que les deux nombres premiers p et q sont différents et que $p<q$ et en particulier p et q sont premiers entre eux. D'autre part p divise $q(q+1)$, et par le lemme de Gauss p divise $q+1$. On pose $q+1=kp$, i.e. $q=kp-1$ et en substituant dans l'équation de base on trouve

$$p^3+p = q^2+q = (kp-1)^2+(kp-1) = k^2p^2-2kp+kp = k^2p^2-kp$$

Ce qui est équivalent à

$$p^2-k^2p+kp+1 = p^2-(k^2-k)p+1=0$$

Donc le discriminant de cette équation est un carré parfait, i.e.

$$(k^2-k)^2-4=\alpha^2$$

où α est un entier naturel. Ceci fournit les systèmes d'équations

$$\begin{cases} k^2-k+\alpha=4 \\ k^2-k-\alpha=1 \end{cases} \quad \begin{cases} k^2-k+\alpha=1 \\ k^2-k-\alpha=4 \end{cases} \quad \begin{cases} k^2-k+\alpha=2 \\ k^2-k-\alpha=2 \end{cases}$$

Ce qui implique que

$$2k^2-2k-5=0, \quad 2k^2-2k-4=0$$

La première équation n'admet pas de solution entière puisque sont discriminant n'est pas un carré parfait. La seconde équation à pour solutions entières -1 et 2, donc $k=2$ et par suite

$$q+1=2p$$

En substituant dans l'équation de base on trouve

$$p^3+p=(2p-1)^2+2p-1=4p^2-2p$$

i.e.

$$p^2-4p+3=0$$

Donc $p=3$, et par suite $q=5$. Réciproquement le couple $(3,5)$ s'agit bien d'une solution du problème. Alors

$$S=\{(3,5)\}$$

2.5- Principe de la descente infinie

La *descente infinie* est une méthode introduite et abondamment utilisée par Fermat. Le but est de prouver qu'une certaine équation diophantienne n'admet pas (ou très peu) de solutions. Pour cela on part d'une solution hypothétique et on construit une nouvelle strictement plus petite dans un certain sens. On obtiendrait ainsi une suite strictement décroissante de solutions, ce qui n'est en général pas possible.
Un premier exemple qui illustre cette idée est l'irrationalité de $\sqrt{2}$. On est à nouveau amené à considérer le problème.

Existe t-il des entiers naturels non nuls a et b tels que

$$a^2=2b^2$$

On prouve que a est pair puis que b l'est aussi, on voit que $(a/2,b/2)$ est une nouvelle solution. D'autre part, puisque $b\neq 0$, alors $b/2<b$. Ainsi si l'on part d'une solution (a_0,b_0) avec $b_0\neq 0$, on peut construire une nouvelle solution (a_1,b_1) avec $b_1<b_0$. Puis on continue, on construit $(a_2,b_2),(a_3,b_3)$, et ainsi de suite. On construit ainsi une suite (b_n) telle que

$$b_0>b_1>b_2>b_3>...$$

Ce qui constitue une contradiction, car il n'existe une suite de nombres entiers naturels qui est strictement décroissante. En effet on a la proposition.

Il n'existe pas une suite d'entiers naturels qui est strictement décroissante.

Démonstration. Par absurde, soit (u_n) une suite d'entiers naturels qui est strictement décroissante. On considère l'ensemble $A=\{u_n \mid n\in\mathbb{N}\}$, l'ensemble A est une partie non vide de $\mathbb{N}$, elle admet donc un plus petit élément qu'on note $m=u_p$, puisque la suite (u_n) est strictement décroissante alors $u_{p+1}<u_p$, mais $u_{p+1}\in A$ ce qui contredit le caractère minimal de u_p. D'où la proposition.

Trouver les entiers x,y et z tels que

$$x^3+9y^3=z^3$$

On part d'une solution éventuelle (x, y, z) distincts du triplet $(0, 0, 0)$. L'équation implique que x est un multiple de 3. Mais alors $x = 3x'$ et l'équation devient après simplification par 3,

$$3x'^3 + y^3 = 9z'^3$$

et on déduit de cela que z est un multiple de 3. On écrit $z = 3z'$, l'équation devient

$$3x'^3 + y^3 = 9z'^3$$

et on obtient que y est multiple de 3. Posons $y = 3y'$, on vérifie que le triplet (x', y', z') est encore solution de l'équation de base et qu'il est plus petit que le triplet (x, y, z) dans le sens

$$| x' | + | y' | + | z' | < | x | + | y | + | z |$$

Le principe de la descente infinie permet alors de conclure que l'unique solution de l'équation de départ est le triplet $(0, 0, 0)$.

2.6- L'équation $x^2 - y^2 = n$

A n entier naturel non nul fixé, on considère l'équation $x^2 - y^2 = n$ d'inconnues $x, y \in \mathbb{N}$. Puisque $(x + y) + (x - y) = 2x$ pair, alors les deux entiers $x + y$ et $x - y$ ont même parité. S'ils sont tous les deux impairs, alors n est impair, et s'ils sont tous les deux pairs, n est divisible par 4. Par conséquent, l'équation ne peut avoir de solution que si n est impair ou si n est divisible par 4. Soit (x, y) une solution éventuelle de l'équation, alors $x - y$ est un diviseur de n, notons le d et par suite $x + y = n/d$, il vient que $x = \frac{1}{2}\left(\frac{n}{d} + d\right)$ et $y = \frac{1}{2}\left(\frac{n}{d} - d\right)$.
Il y a donc autant de solutions que d'entiers naturels d et n/d sont des diviseurs de n de même parité. Écrivons $n = 2^{v_2(n)}m$ avec m impair. Si $v_2(n) = 0$, alors n'importe quel diviseur de n convient, et si $v_2(n) \geq 2$ alors d est de la forme $2^j d'$ avec $1 \leq j \leq r - 1$ et d' divise m.
Par exemple, pour $n = 2016 = 2^5 \times 3^2 \times 7$, d est de la forme $2^j d'$ avec $1 \leq j \leq 4$ et $d' \in \{1, 3, 7, 9, 21, 63\}$.

> Définition. Soit n un entier relatif et x un entier naturel non nul. On désigne par $v_x(n)$ le plus grand exposant avec lequel x divise n, autrement dit $v_x(n) = \max\{p \in \mathbb{N}, x^p \mid n\}$, $v_x(n)$ est dite la valuation $x-$adique de n.

Il ne s'agit que d'une définition qu'on a utilisé dans ce qui précède. On détaillera plus sur les valuations $x-$adiques et leurs propriétés prochainement.
Dans la suite nous allons donner une propriété très utile.

> Soient a, b et c trois entiers relatifs et $m \geq 2$ un entier tels que $ab = c^m$, supposons que a et b sont premiers entre eux, alors il existe α et β des entiers relatifs tels que $a = \alpha^m$ et $b = \beta^m$.

Démonstration. Soit p un nombre premier divisant a, il s'agit de montrer que l'exposant α_p de p dans la décomposition primaire de a est un multiple de m. Puisque p divise ab, alors c^m est un multiple de p et il en est de même pour c, notons γ_p l'exposant de p de la décomposition primaire de c, on a alors $\gamma_p \geq 1$ (car p divise c), il s'en suit que $v_p(ab) = v_p(c^m)$, i.e. $v_p(a) = v_p(c^m)$ et alors $\alpha_p = m\gamma_p$. D'où le résultat.

2.7- Exercices

1. (a) Prouver que le produit de deux entiers non nuls consécutifs ne peut pas être un carré parfait.
   (b) Prouver que le produit de trois entiers consécutifs non nuls ne peut pas être un carré parfait.
   (c) Prouver que le produit de quatre entiers consécutifs non nuls ne peut pas être un carré parfait.
2. (France 2002) On considère 2002 rationnels $x_1, x_2, ..., x_{2002}$ tels que pour tout sous-ensemble I de $\{1, 2, ..., 2002\}$ de cardinal 7, il existe un sous-ensemble de cardinal 11 vérifiant,

$$\frac{\sum_{i \in I} x_i}{7} = \frac{\sum_{j \in J} x_j}{11}$$

   Montrer que tous les x_i sont égaux.

3. (Biélorussie 1999) Prouver qu'il existe une infinité de triplets de rationnels non entiers positifs tels que

$$\{x^3\} + \{y^3\} = \{z^3\}$$

où $\{t\} = t - \lfloor x \rfloor$ désigne la partie décimale de t.

4. (Italie 1994) Trouver tous les entiers x et y pour lesquels

$$y^2 = x^3 + 16$$

5. (OIM 1981) Soient m et n deux entiers tels que $1 \leq n, m \leq 1981$ vérifiant

$$(n^2 - mn - m^2)^2 = 1$$

Quel est le maximum de $n^2 + m^2$?

2.8- Solutions des exercices

1. (a) Donnons d'abord un lemme, si n et $n+1$ sont des carrés parfaits, alors $n = 0$. En effet Supposons $n = a^2$ et $n+1 = b^2$, donc $(b-a)(b+a) = 1$ et alors $b-a = b+a = 1$ et par suite $a = 0$, donc $n = 0$. Supposons qu'il existe deux entiers consécutifs n et $n+1$ tels que $n(n+1)$ soit un carré parfait. Puisque n et $n+1$ sont premiers entre eux, alors tous les deux sont des carrés parfaits et par suite $n = 0$ en vertu du lemme précédent. Ce qui est absurde. Une autre méthode consiste à remarquer que l'équation d'inconnue n n'admet pas de solution puisque son discriminant ne peut pas être un carré parfait.
   ➛*Le même argument s'applique pour montrer que le produit de deux entiers ne peut pas être une puissance parfaite.*

   (b) Supposons que $(n-1)n(n+1)$ est un carré parfait, comme n et n^2-1 sont premiers entre eux, ils doivent tous les deux être des carré parfaits, mais n^2-1 ne peut être un carré parfait que si $n = -1, 1$ alors le produit $n(n-1)(n+1)$ est nul, ce qui est absurde.

   (c) Il suffit de remarquer que

$$(n-1)n(n+1)(n+2) = (n-1)(n+2)n(n+1) = (n^2+n-2)(n^2+n) = (n^2+n)^2-2(n^2+n) = (n^2+n-1)^2-1$$

   puisque $(n^2+n-1)^2$ est un carré parfait, alors le produit de quatre entiers naturels non nuls consécutifs ne peut être un carré parfait.

2. Quitte à multiplier tous les x_i par un même facteur, on peut supposer que tous les x_i sont des entiers. Quitte à permuter les x_i, on peut supposer que x_1 est le plus petit d'entre eux. Posons $y_i = x_i - x_1 \geq 0$. On a $y_1 = 0$ et la famille des y_i vérifie la même hypothèse que la famille des x_i. Soit $i \in \{2, ..., 2002\}$ un entier. Notons I un sous ensemble de $\{2, ..., 2002\}$ de cardinal 7 contenant i et I' l'ensemble I obtenu en remplaçant i par 1. Par hypothèse, il existe des ensembles J et J' de cardinal 11 tels que,

$$11\sum_{i\in I} y_i = 7\sum_{j\in J} y_j, \quad 11\sum_{i\in I'} y_i = 7\sum_{j\in J'} y_j$$

   En soustrayant ces deux égalités, on voit que $11y$, est un multiple de 7 et donc d'après le lemme de Gauss, il en est de même de y_i, et cela pour tout i. La famille des $y_i/7$ est encore solution du problème. Le principe de descente infinie assure que l'unique solution est alors $y_i = 0$ pour tout i. Cela entraîne bien que tous les x_i sont égaux.

3. On trouve en premier en lieu une solution particulière $(x_0, y_0, z_0) = (3/5, 4/5, 6/5)$. Comme un dénominateur commun de x_0^3, y_0^3 et z_0^3 est 125, si on multiplie x_0^3, y_0^3 et z_0^3 par 125, on ne changera pas la partie décimale. On cherche donc des cubes congrues à 1 modulo 125. Les nombres $(125k+1)^3$ s'imposent. On est finalement amené à considérer les nombres

$$x = x_0(125k+1), \quad y = y_0(125k+1), \quad z = z_0(125k+1)$$

   dont il est facile de vérifier qu'il conviennent.

4. Soit (x, y) une éventuelle solution de l'équation $y^2 = x^3 + 16$, qui s'écrit encore $(y-4)(y+4) = x^3$. Si y est impair, alors $y-4$ et $y+4$ sont premiers entre eux et donc ils sont des cubes parfaits impairs distants de 8, ce qui n'existe pas. Donc $y = 2y'$ est pair, et par suite $x = 2x'$ est pair aussi. L'équation devient donc

$$(y'+2)(y'-2) = 2x'^3$$

Donc $y'+2$ ou $y'-2$ est pair, puisque $y'+2$ et $y'-2$ ont même parité, alors ils sont tous les deux pairs, et par suite y' est pair, il s'en suit que x' est également est pair. Donc on peut récrire $y'=2s$ et $x'=2t$. Il vient $(s+1)(s-1)=4t^3$, par suite $s+1$ et $s-1$ sont pairs, donc $s=2u+1$ est impair, et l'on obtient finalement $u(u+1)=t^3$. Puisque u et $u+1$ sont premiers entre eux, cela impose que tous les deux soient des cubes, et par suite $u=-1$ ou 0 et $t=0$. En remontant, on trouve que l'équation de base possède exactement deux solutions $(0,-4)$ et $(0,4)$.

5. L'examen des premiers cas suggère que les couples de nombres de Fibonacci sont solutions, $(1,2),(2,3),(3,5),(5,8),...$ Il est facile de le vérifier de manière générale. En effet, si (m,n) convient alors

$$(m+n)^2-n(m+n)=m^2+2mn+n^2-mn-2n^2=-(n^2-mn-m^2)$$

et donc $(n,m+n)$ convient aussi. En calculant les termes de la suite de Fibonacci ≤ 1981,

$$1,2,3,8,13,21,34,55,89,144,233,377,610,987,1597$$

On obtient que m^2+n^2 peut atteindre 1597^2+987^2. On aimerait que cette valeur soit effectivement le maximum cherché. Pour le voir, il suffit d'effectuer l'opération $(m,n)\to(n,m+n)$ dans l'autre sens ! En effet, soit (m,n) une solution avec $1\leq m<n$, alors $(n-m,m)$ aussi. En itérant ce procédé, on se ramène nécessairement à une solution de la forme $(1,n)$. Or pour $m=1$ l'équation devient $n^2-n=0,2$ dont la seule solution strictement positive est $n=2$. Il en résulte que toutes les solutions sont obtenues à partir de $(1,2)$ par itération de $(m,n)\to(n,m+n)$, donc sont toutes de la forme (F_{n-1},F_n). Finalement, le maximum possible de m^2+n^2 est exactement 1597^2+987^2.
➛*Ne vous inquiétez, c'est un problème* 3 *de l'olympiade internationale.*

3- Résolution à l'aide des congruences, inégalités

L'utilisation des congruences et les inégalités et parfois les deux sont des outils très puissant dans la résolution des équations diophantiennes. Dans cette partie, on va voir plusieurs exemples et exercices dont la solution est amené à utiliser ces outils.

3.1- Utilisation des congruences

La maîtrise des propriétés des congruences est fondamentale avant d'introduire cette partie. Une méthode souvent efficace, pour prouver qu'une équation diophantienne n'a *pas de solution* est de considérer la même équation modulo un entier N et de prouver qu'il n'y a pas de solution dans cette nouvelle situation. Pour cela nous allons commencer par donner quelques propriétés sur les congruences modulo des entiers.

[Théorème de Fermat] Soit a un entier et p un nombre premier, alors

$$a^p\equiv a \pmod p$$

Avant de démontrer ce théorème, on introduit d'abord un lemme qui lui aussi est très utile.

Soit p un nombre premier et $1\leq k\leq p-1$, alors p divise $\binom{p}{k}$.

En effet, on sait que

$$k\binom{p}{k}=k\times\frac{p!}{k!(p-k)!}=p\times\frac{(p-1)!}{(k-1)!(p-1-k+1)}=p\binom{p-1}{k-1}$$

Par suite, p divise $k\binom{p}{k}$, et puisque k et p sont premiers entre eux (car un nombre premier est premier avec tous les entiers naturels non nuls qui lui sont inférieurs), donc par le lemme de Gauss p divise $\binom{p}{k}$. D'où le lemme. Revenons à la démonstration du théorème de Fermat.

Démonstration. On procède par récurrence sur $a \in \mathbb{N}$, pour $a = 0$ c'est évident, supposons le résultat vrai pour un rang a et montrons le pour le rang $a+1$, on sait que

$$(a+1)^p = a^p + 1 + \sum_{k=1}^{p-1} \binom{p}{k} a^k \equiv a^p + 1 \equiv a + 1 \pmod{p}$$

Ce qui achève la récurrence. Pour le cas $a \in \mathbb{Z}^-$, si $p = 2$ on a clairement 2 divise $a^2 - a$, sinon p est impair et alors $a^p \equiv a \pmod{p}$ puisque $(-a)^p \equiv -a \pmod{p}$ (car $-a \in \mathbb{N}$).

On a un corollaire très important, appelé petit théorème de Fermat ou *petit Fermat*.

Soit a un entier et p un nombre premier ne divisant pas a, on a la congruence

$$a^{p-1} \equiv 1 \pmod{p}$$

Démonstration. D'après le théorème de Fermat, on a

$$a^p \equiv a \pmod{p}$$

Puisque p est un nombre premier ne divisant pas a, alors a et p sont premiers entre eux, ce qui est équivalent à que a soit inversible modulo p. En *divisant* la congruence ci-dessus par a, on trouve $a^{p-1} \equiv a \pmod{p}$. D'où le résultat.

(Maroc 2018) Soient a, b et c des entiers. Montrer l'équivalence

$$30 \mid a^5 + b^5 + c^5 \iff 30 \mid a + b + c$$

Pour trouver le résultat, il suffit de montrer par exemple que

$$a^5 + b^5 + c^5 \equiv a + b + c \pmod{30}$$

D'après le petit théorème de Fermat, on a pour tout entier x, $x^5 \equiv x \pmod{5}$ et $x^2 \equiv x \pmod{2}$ et $x^3 \equiv x \pmod{3}$, donc $x^5 = x \pmod{5}$ et $x^5 = x \times (x^2)^2 \equiv x \times x^2 \equiv x^2 \equiv x \pmod{2}$ et aussi $x^5 = x^3 \times x^2 \equiv x \times x^2 \equiv x^3 \equiv x \pmod{3}$, finalement puisque $5, 3$ et 2 sont premiers entre eux deux à deux, alors $x^5 \equiv x \pmod{30}$ pour tout entier x, d'où

$$a^5 + b^5 + c^5 \equiv a + b + c \pmod{30}$$

On en déduit le résultat.

Dans la suite de cette partie on donnera un peu de propositions sur les puissances modulo quelques entiers. Commençons par une proposition très importante.

Le carré d'un entier est toujours congru à 0 ou 1 modulo 4.

Démonstration. La preuve est facile, en effet on a $x \equiv 0, 1, 2, 3 \pmod{4}$ et en élevant au carré, on obtient $x^2 \equiv 0, 1, 4, 9 \pmod{4}$ et d'où le résultat.

Existe t-il des entiers a, b tels que

$$a^2 + b^2 = 463$$

On regarde l'équation ci-dessus modulo 4, on a d'après la proposition précédente

$$a^2 + b^2 \equiv 0, 1, 2 \pmod{4}$$

mais $463 \equiv 3 \pmod{4}$, donc un tel couple (a, b) solution de l'équation n'existe pas.

Le carré d'un entier est congru à 0 ou 1 modulo 3.

Démonstration. On sait que $x \equiv 0, 1, 2 \pmod 3$ et donc $x^2 \equiv 0, 1 \pmod 3$. Un autre argument consiste à remarquer que si 3 ne divise pas x, alors le petit théorème de Fermat fournit $x^2 \equiv 1 \pmod 3$.

Le carré d'une entier est congru à 0 ou 1 modulo 12.

Démonstration. Il suffit de remarquer que $12 = 4 \times 3$ et appliquer les deux lemmes précédents.

Donnons le dernier lemme de cette partie concernant les congruences modulo 8.

Le carré d'un entier est congru à $0, 1$ ou 4 modulo 8.

Démonstration. Un tableau de congruence suffit.

Existe t-il des entiers a, b et c tels que

$$a^2 + b^4 + c^8 = 10^{2018} + 15$$

Regardons l'équation modulo 8, les entiers a^2, b^4 et c^8 sont des carrés, d'après le lemme précédent, on a la somme de trois carrés ne peut pas être congru à 7 modulo 8, sachant que $10^{2018} + 15$ est congru à 7 modulo 8. Un tel triplet (a, b, c) solution de l'équation ne peut exister.

Finissons cette partie par des exemples.

(Balkan) Trouver tous les entiers x et y tels que

$$y^5 - 4 = x^2$$

Comme les exposants qui interviennent dan l'équation sont 2 et 5, il peut être intéressant de l'examiner en réduction modulo un nombre premier p tels que 2 et 5 divisent $p - 1$. Le premier qui se présente est $p = 11$. Les puissances cinquièmes modulo 11 sont $0, 1$ et -1, donc le second membre de l'équation est congru à $7, 8$ ou 6 modulo 11. Par ailleurs les carrés modulo 11 sont $0, 1, 4, 9, 5$ et 3. Il en résulte immédiatement que l'équation n'a pas de solution.

Trouver tous les couples d'entiers (x, y) satisfaisant l'équation suivante

$$x^2 - y! = 2001$$

Quand $y \geq 7$, on a 7 divise $y!$ et donc $x^2 \equiv 2001 \equiv 6 \pmod 7$. Mais on a le tableau de congruence,

x	$x^2 \pmod 7$
0	0
1	1
2	4
3	2
4	2
5	4
6	1

Donc l'équation n'a pas de solution. Par suite $y \leq 6$. Notons que le plus petit carré supérieur à 2001 est $2025 = 45^2$, cela fournit deux solutions $(45, 4)$ et $(-45, 4)$, cela couvre tous les cas avec $y \leq 4$. Si $y = 5$, on obtient $x^2 = 2001 + 5! = 2121$, donc 3 divise x et par suite 9 divise $x^2 = 2121$ ce qui n'est pas possible. Supposons maintenant que $y = 6$, on obtient $x^2 = 2001 + 6! = 2721$ qui n'a pas de solution par le même argument précédent. En conclusion les seules solutions de l'équation suggérée sont $(45, 4)$ et $(-45, 4)$.

Montrer que l'équation

$$(x+1)^2 + (x+2)^2 + ... + (x+2001)^2 = y^2$$

n'a pas de solutions entières.

On pose $x = z - 1001$ l'équation devient

$$(z-1000)^2 + ... + (z-1)^2 + z^2 + (z+1)^2 + ... + (z+1000)^2 = y^2$$

Il s'en suit que

$$2001z^2 + 2(1^2 + 2^2 + ... + 1000^2) = y^2$$

i.e.

$$2001z^2 + 1000 \times 1001 \times 667 = y^2$$

Le membre de gauche est congru à 2 modulo 3. Ce qui n'est pas possible car le membre de droite est un carré parfait.

3.2- Utilisation des inégalités

L'utilisation des majorations, des minorations peuvent s'avérer utile dans certaines situations, dans cette dernière partie de ce chapitre on va voir de nombreux exemples dont la résolution se fait en utilisant des inégalités. Contrairement aux parties précédentes, pas de théorie dans cette partie.

(Maroc 2018) Trouver tous les entiers naturels x et y tels que

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{5}$$

Soient (x, y) solution éventuelle de l'équation ci-dessus. Les entiers naturels x et y jouent des rôles symétrique, on peut alors supposer que $x \leq y$, il vient

$$\frac{1}{5} \leq \frac{1}{x} + \frac{1}{y} \leq \frac{2}{x}$$

Par conséquent $x \leq 10$. Sachant que $1/5 \geq 1/x$ d'après l'équation de base, alors $x \geq 5$. En substituant x par les valeurs $5, 6, 7, 8, 9, 10$, on trouve $S = \{(5, 30), (10, 10), (30, 5)\}$.

(Russie) Déterminer tous les pairs d'entiers naturels (x, y) vérifiant

$$x^3 - y^3 = xy + 61$$

Soit (x, y) une solution éventuelle de l'équation ci-dessus. Il est clair que $x \neq y$. Puisque x et y jouent des rôles symétriques, on peut supposer que $x > y$, on a

$$x^3 - y^3 = (x-y)(x^2 + xy + y^2) = xy + 61$$

Donc, $x^2 + y^2 + xy \leq xy + 61$ ou encore $x^2 + y^2 \leq 61$ et alors $y \leq 5$ car $2y^2 < x^2 + y^2 \leq 61$. En examinons les valeurs de y on trouve que l'unique solution de l'équation proposée est $(6, 5)$.

(Maroc 2015) Trouver tous les entiers naturels n et m tels que $(m+n)^2$ divise $4(mn+1)$.

Soit (n,m) un couple vérifiant la condition ci-dessus. Puisque $(m+n)^2$ divise $4(mn+1)$, alors $(m+n)^2 \leq 4mn+4$, i.e. $(m-n)^2 \leq 4$ et alors $\mid m-n \mid \leq 2$. Donc $m-n=-2,-1,0,1,2$. Si $m-n=0$, i.e. $m=n$, alors $4n^2 \mid 4n^2+4$ et alors $n^2 \mid 1$, donc $n=1$ et par suite $n=m=1$. Si $m=n+1$, alors $(2n+1)^2 \mid 4(n^2+n+1)$ et par suite $(2n+1)^2 \mid 3$, i.e. $(2n+1)^2=0$ et alors $n=0$ et par suite $m=n+1=1$. Pour $m=n+2$, on vérifie facilement que tous les couples $(n,n+2)$ sont solutions du problème. En conclusion

$$S=\{(0,1),(1,0),(1,1),(n,n+2),(n+2,n) \mid n \in \mathbb{N}\}$$

3.3- Exercices

1. Quelle est la valeur minimale positive de 12^m-5^n pour m et n des entiers strictement positifs ?
2. Soient $m,n \geq 1$ des entiers. Montrer que 3^m+3^n+1 n'est pas un carré parfait.
3. Trouver tous les entiers $x,y \geq 1$ tels que $3^x-2^y=7$.
4. Trouver tous les entiers $n \geq 1$ tels que $2^n+12^n+2014^n$ soit un carré parfait.
5. Montrer que tout entier relatif peut s'écrire comme la somme de cinq cubes d'entiers relatifs d'une infinité de manières différentes.
6. (Saint Petersbourg 1997) Soient x,y et z des entiers strictement positifs tels que $2x^x+y^y=3z^z$. Montrer que $x=y=z$.

3.4- Solutions des exercices

1. Soit $x=12^m-5^n$ le minimum cherché. On a $x \equiv -5^n \pmod 6$ et alors x n'est divisible par 3, ni par 3. De même x n'est pas divisible par 5. Par conséquent, on a $x \geq 7=12-5$ ou $x=1$. Il reste à exclure le cas $x=1$. Pour cela, on peut remarquer que
$$12^n-5^n \equiv -1 \pmod 4$$
Donc le minimum cherché est 7.
2. On travaille modulo 8, on remarque que 3^m+3^n+1 est congru à $3,5$ ou 7 modulo 8. Or un carré est congru à $0,1$ ou 4 modulo 8, ce qui conclut.
3. On vérifie que $y=1$ donne la solution $x=2$, et que $y=2$ ne donne pas de solution. On suppose donc $y \geq 3$. Il est judicieux de travailler modulo 8, on doit avoir $3^x \equiv 7 \pmod 3$. Or une puissance de 3 n'est jamais congrue à 7 modulo 8.
4. Regardons l'expression modulo 3, $2^n+12^n+2014^n \equiv (-1)^n+1 \pmod 3$. Comme un carré n'est jamais congru à 2 modulo 3, on en déduit que n est impair, on en déduit que n est impair. Regardons ensuite l'expression modulo 7,
$$2^n+12^n+2014^n \equiv 2^n+(-2)^n+5^n \equiv 5^n \pmod 7$$
Lorsque n est impair, 5^n ne peut être congru qu'à $3,5$ ou 6 modulo 7. Or un carré est congru $0,1,2$ ou 4 modulo 7. Il n'existe donc pas d'entiers $n \geq 1$ tels que $2^n+12^n+2014^n$ soit un carré parfait.
5. Partons de la formule
$$(t+1)^3+(t-1)^3+(-t)^3+(-t)^3=6t$$
qui prouve déjà que tout multiple de 6 peut s'écrire comme somme de quatre cubes. Soit n un entier. On veut réussir à écrire n d'une infinité de façons comme somme de cinq cubes. Mais d'après ce qui précède, chaque fois que l'on arrive à trouver un cube congru à $-n$ modulo 6, on obtient une telle écriture. Or on vérifie facilement que tout résidu modulo 6 est un cube car pour tout $a \in \mathbb{Z}$, on a $a^3 \equiv a \pmod 6$. D'où le résultat, car un entier peut s'écrire comme une infinité de façons telle qu'il soit un cube modulo 6, en effet
$$a \equiv a^3 \equiv a^9 \equiv ... \equiv a^{3^k} \equiv ... \pmod 6$$
6. Si $z=1$, il est clair que $x=y=1$. Supposons $z \geq 2$, et supposons qu'on a pas $x=y=z$. Soit $t=\max(x,y)$, on a $t>z$, donc $t \geq z+1$. Si $t=x$, alors
$$2x^x \geq 2(z+1)^{z+1} > 2z^{z+1} \geq 4z^z$$
Ce qui n'est pas possible. Maintenant, supposons $t=y$, on aura
$$y^y \geq (z+1)^z > z^{z+1}+(z+1)z^z=(2z+1)z^z \geq 5z^z$$
Ce qui est également pas possible. En conclusion, on a $x=y=z$.

4- Équations diophantiennes linéaires

4.1- L'équation $ax + by = c$

4.2- Autres équations diophantiennes linéaires

4.3- Exercices

4.4- Solutions des exercices

5- Équations diophantiennes quadratiques, cubiques

5.1- Triplets pythagoriciens

5.2- L'équation $x^4 + y^4 = z^4$

5.3- Équations de Pell

5.4- Autres équations diophantiennes quadratiques

5.5- Équations cubiques

5.6- Exercices

5.7- Solutions des exercices

6- Construction de solutions, Vietta Jumping

6.1- Construction des solutions

6.2- Vietta Jumping

6.3- Exercices

6.4- Solutions des exercices

7- Florilège d'équations de tout genre

7.1- Exercices

7.2- Solutions des exercices

7- Références

[1] Les olympiades de mathématiques, Tarik Belhaj Soulami, Ellipses, 1999.

[2] Cours d'arithmétiques, Pierre Bornsztein, Xavier Caruso, Pierre Nolin, Mehdi Tibouchi, Décembre 2004.

[3] Théorie des nombres III, Thomas Huber, Avril 2016.

[4] Théorie des nombres aux olympiades des mathématiques, Tarik Al Seayri, équipe saoudite de préparation aux OIM, 2011.

[5] Problems from the book, Titu Andreescu, XYZ Press 2008.

[6] A introduction to Diophantienne equations, Titu Andreescu, Birkhauser 2010.

[7] Olympiad Number Theory Through Challenging Problems, Justin Stevens, Third edition.

[8] Équations diophantiennes modulo N, Igor Kortchemski.