FST Mulhouse.

Licence 1 Maths-Info

Mathématiques : ARITHMETIQUE-ALGEBRE

Elisabeth REMM

Chapitre 3

Congruence - Equations diophantiennes

1. La relation de congruence

1.1. **Définition de la congruence modulo p.** Soit p un entier positif donné.

Définition 1. *Soient m et n deux entiers. n dit que m est congru à n modulo p et on écrit*

$$m \equiv n \pmod{p}$$

ou parfois pour raccourcir l'écriture

$$m \equiv n \ [p]$$

si p divise la différence $m - n$.

Ceci est aussi équivalent à dire que m et n ont les mêmes restes dans la division euclidienne par p. Cette relation est appelée la relation de congruence modulo p.

Exemples

(1) $18 \equiv 13 \pmod{5}$

(2) $m = 2k \equiv 0 \pmod{2}$, où $k \in \mathbb{Z}$.

(3) $m = 2k + 1 \equiv 1 \pmod{2}$, où $k \in \mathbb{Z}$.

Théorème 1. *La relation de congruence modulo p est une relation d'équivalence.*

Démonstration. Elle est en effet

(1) Réflexive car $m - m$ a pour reste 0 dans la division par p.

(2) Symétrique car si $m - n$ a pour reste 0 il en esr aussi de même de $n - m$ dans la division par p,

(3) Transitive. En effet si m_1 est congru à m_2 modulo p et m_2 congru à m_3 modulo p, alors $m_1 - m_2$ est divisible par p, c'est-à-dire $m_1 - m_2 = kp$, $m_2 - m_3$ est aussi divisible par p, soit $m_2 - m_3 = k_2 p$. Aisni

$$m_1 - m_3 = m_1 - m_2 + m_2 - m_3 = kp + k_1 p = (k + k_1)p$$

et $m - m_2$ est aussi divisible par p soit m_1 congru à m_3 modulo p, ce qui montre la transitivité. La relation de congruence modulo p est donc Réflexvie, Symétrique et Transitive. C'est une relation d'équivalence.

1.2. **Addition,soustraction et multiplication de nombres congruents.** Nous allons regarder le comportement de cette relation par rapport aux opérations arithmétiques ordinaires.

Proposition 1. *Soit p un entier positif donné et soient m_1, m_2, n_1, n_2 des entiers tels que*

$$m_1 \equiv m_2 \pmod{p}, \quad n_1 \equiv n_2 \pmod{p}.$$

Alors

(1) $m_1 + n_1 \equiv m_2 + n_2 \pmod{p}$,

(2) $m_1 - n_1 \equiv m_2 - n_2 \pmod{p}$,

(3) $m_1 n_1 \equiv m_2 n_2 \pmod{p}$

Démonstration. La démonstration est facile et laissée au lecteur. Il suffit de se servir des hypothèses :

$$m_1 - m_2 = k_1 p, \quad n_1 - n_2 = k_2 p.$$

La troisième propriété est un peu plus délicate à établir. On écrit

$$m_1 n_1 - m_2 n_2 = m_1 n_1 - m_1 n_2 + m_1 n_2 - m_2 n_2 = m_1(n_1 - n_2) + (m_1 - m_2)n_2$$

ce qui permet de conclure.

Par contre, pour la division les choses sont moins simples. Nous y reviendrons en fin de cours dans l'étude de certaines structures algébriques.

1.3. **L'ensemble des classes d'équivalence.** Considérons la relation d'équivalence modulo p. Soit m un entier. Sa classe d'équivalence est par définition le sous-ensemble de $\mathbb{Z}$, noté $\mathrm{cl}(m)$ et défini comme suit :

$$\mathrm{cl}(m) = \{n \in \mathbb{Z},\ n \equiv m \pmod{p}\}.$$

Proposition 2. *Pour p entier positif donné, il existe p classes d'équivalence pour la relation de congruence modulo p, à savoir*

$$\mathrm{cl}(0), \mathrm{cl}(1) \cdots, \mathrm{cl}(p-2), \mathrm{cl}(p-1).$$

Démonstration. En effet, si r est le reste de la division de m par p, alors $0 \leq r < p$ et $m \equiv r \pmod{p}$. Comme les restes de la division par p sont les entiers positifs compris entre 0 et $p-1$, on en déduit qu'il y a au plus p classes d'équivalence, celles décrites dans la proposition. Il reste à montrer que ces classes forment une partition de $\mathbb{Z}$. Il est clair que la réunion de ces classes est l'ensemble $\mathbb{Z}$. Montrons que leurs intersections sont vides. Si $n \in \mathrm{cl}(r_1)$ et $n \in \mathrm{cl}(r_2)$ alors le reste de la division de n par p est r_1 et r_2, ce qui implique $r_1 = r_2$ et donc $\mathrm{cl}(r_1) = \mathrm{cl}(r_2)$.

On note $\mathbb{Z}/p\mathbb{Z}$ l'ensemble quotient associé à cette relation, c'est-à-dire l'ensemble des classes d'équivalence. On en déduit

$$\mathbb{Z}/p\mathbb{Z} = \{\mathrm{cl}(0), \mathrm{cl}(1) \cdots, \mathrm{cl}(p-2), \mathrm{cl}(p-1)\}.$$

Par soucis de simplification d'écriture, nous adopterons l'écriture suivante

$$\mathrm{cl}(m) = \overline{m}^{(p)}$$

ou si la précision de p est superflue, car sous-entendue

$$\mathrm{cl}(m) = \overline{m}.$$

Les opérations sur les classes s'écrivent alors

$$\overline{m} + \overline{n} = \overline{m+n}, \quad \overline{m} \cdot \overline{n} = \overline{mn}$$

mais en prenant garde qu'il s'agit toujours de la congruence modulo le même entier.

Exemples.

(1) $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$.

(2) $\mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}\}$.

(3) $\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$.

Comme ces ensembles sont finis et munis de deux opérations $+$ et $\times$, nous pouvons dresser les tables de ces opérations.

Exemples.

(1) Dans $\mathbb{Z}/2\mathbb{Z}$ les tables d'addition et de multiplication s'écrivent

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

,

$\times$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

(2) Dans $\mathbb{Z}/3\mathbb{Z}$ les tables d'addition et de multiplication s'écrivent

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

,

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

(3) Dans $\mathbb{Z}/4\mathbb{Z}$ les tables d'addition et de multiplication s'écrivent

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

,

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Nous étudierons plus en détail les propriétés de ces opérations dans le dernier chapitre consacré aux structures algébriques.

2. Applications : les preuves par 3, 5 et 9

2.1. **Quelques calculs avec la congruence.** Nous avons vu, ci-dessus, la relation : soit p un entier positif donné et soient m_1, m_2, n_1, n_2 des entiers tels que $m_1 \equiv m_2 \pmod{p}$, $n_1 \equiv n_2 \pmod{p}$, alors

$$m_1 n_1 \equiv m_2 n_2 \pmod{p}.$$

Nous en déduisons immédiatement

Proposition 3. *Soit p un entier positif donné et soient m_1, m_2 des entiers tels que $m_1 \equiv m_2 \pmod{p}$, alors pour tout $k \in \mathbb{N}$*

$$m_1^k \equiv m_2^k \pmod{p}.$$

Exemples.

(1) Modulo 3 : Nous savons que $10 \equiv 1 \pmod{3}$. Nous en déduisons que pour tout $k \in \mathbb{N}$,

$$10^k \equiv 1 \pmod{3}$$

et aussi

$$10^k + 2 \equiv 1 + 2 \pmod{3}.$$

Mais comme $2 + 1 = 3 \equiv 0 \pmod{3}$, nous obtenons, pour tout $k \in \mathbb{N}$,

$$10^k + 2 \equiv 0 \pmod{3}$$

et donc $10^k + 2$ est divisible par 3.

(2) Modulo 7 : Nous voulons simplifier l'expression $93^{1002} + 93^{1001} + 93^{1000} \pmod{7}$. Considérons l'entier 93. On vérifie sans peine que $93 \equiv 2 \pmod{7}$. Nous en déduisons que pour tout entier k, $93^k \equiv 2^k \pmod{7}$. Mais $2^3 \equiv 1 \pmod{7}$. Ceci implique

$$2^{999} \equiv 1 \pmod{7},\ 2^{1000} \equiv 2 \pmod{7},\ 2^{1001} \equiv 4 \pmod{7},\ 2^{1002} \equiv 1 \pmod{7}.$$

Ainsi

$$3^{1002} + 93^{1001} + 93^{1000} \equiv (2 + 4 + 1) \equiv 0 (\text{mod } 7).$$

2.2. **La preuve par 3 ou par 9.** Considérons un nombre entier n écrit sous sa forme décimale :

$$n = a_1 a_2 \cdot a_p$$

avec $a_i \in \{0, 1, 2, \cdots, 9\}$. Par exemple $n = 5432$, alors $a_1 = 5, a_2 = 4, a_3 = 3, a_4 = 2$. Cette écriture est équivalente à

$$n = a_1 \cdot 10^{p-1} + a_2 \cdot 10^{p-2} + \cdots + a_{p-1} \cdot 10 + a_p.$$

Par exemple $5432 = 5 \cdot 10^3 + 4 \cdot 10^2 + 3 \cdot 10 + 2$. Mais nous avons $10 \equiv 1 (\text{mod } 3), 10^2 \equiv 1 (\text{mod } 3)$ et donc plus généralement, pour tout $k \in \mathbb{N}$:

$$10^k \equiv 1 (\text{mod } 3).$$

Ainsi

$$n = a_1 \cdot 10^{p-1} + a_2 \cdot 10^{p-2} + \cdots + a_{p-1} \cdot 10 + a_p \equiv a_1 + a_2 + \cdots + a_p \pmod{3}.$$

De même nous avons $10 \equiv 1 \pmod{9}$ et donc pour tout entier k, $10^k \equiv 1 \pmod{9}$. Nous aurons donc aussi

$$n = a_1 \cdot 10^{p-1} + a_2 \cdot 10^{p-2} + \cdots + a_{p-1} \cdot 10 + a_p \equiv a_1 + a_2 + \cdots + a_p \pmod{9}.$$

On en déduit la règle de divisibilité :

Proposition 4. *(1) Un nombre entier n est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3.*

(2) Un nombre entier n est divisible par 9 si et seulement si la somme de ses chiffres est divisible par 9.

2.3. **La preuve par 11.** D'après ce que nous venons de voir, les critères de divisibilité par un entier p repose sur l'étude de $10^k \pmod p$. Ici $p = 11$ et $10 \equiv -1 \pmod{11}, 10^2 \equiv 1 \pmod{11}$, $10^3 \equiv -1 \pmod{11}$, ce qui donne en général

$$10^{2k} \equiv 1 \pmod{11},\ 10^{2k+1} \equiv -1 \pmod{11}.$$

Ainsi

$$n = a_1 \cdot 10^{p-1} + a_2 \cdot 10^{p-2} + \cdots + a_{p-1} \cdot 10 + a_p \equiv (-1)^{p-1}a_1 + (-1)^{p-2}a_2 - a_{p-1} + a_p.$$

Proposition 5. *Un nombre est divisible par 11 lorsque la différence entre la somme des chiffres de rang pair et la somme des chiffres de rang impair est un multiple de 11.*

Prenons par exemple $n = 5432$. Nous avons

$$5432 \equiv -5 + 4 - 3 + 2 = -2 = 9 \ (\mod 11).$$

De meme $25432 \equiv 2 - 5 + 4 - 3 + 2 = 0 \ (\mod 11)$ et donc ce nombre est divisible par 11.

2.4. **Quelques autres règles de divisibilité.** On pourra, à titre d'exercices, démontrer de manière analogue d'autres règles de divisibilté

Proposition 6. *(1) Un nombre est divisible par 4 lorsque les deux chiffres de droite forment un nombre multiple de 4.*

(2) Un nombre est divisible par 5 lorsque le chiffre des unités est 0 ou 5.

(3) Un nombre est divisible par 8 lorsque les trois chiffres de droite forment un nombre multiple de 8.

Il existe également un critère de divisibilité par 7, mais cela commence à devenir peu simple à utiliser. On séparer ce nombre par tranches de trosi chiffres en partant des unités et d'insérer alternativement des $-$ et des $+$ entre les tranches. On effectue l'opération ainsi écrite et ce résultat est divisible par 7 si et seulement le nombre de départ l'est.

3. Congruence modulo un nombre premier

Dans cette partie nous allons nous intéresser à la congruence modulo p lorsque p est un nombre premier. Nous verrons en dernière partie du cours que les ensembles $\mathbb{Z}/p\mathbb{Z}$ ont des structures algébriques différentes lorsque p est premier ou pas. Nous avons ci-dessus étudier les tables de multiplications de $\mathbb{Z}/p\mathbb{Z}$ pour $p = 2, 3$ et $p = 4$. Nous pouvons remarque sur ces exemples une différence de structure entre $\mathbb{Z}/4\mathbb{Z}$ et les deux autre $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z}$. En effet dans $\mathbb{Z}/4\mathbb{Z}$, il existe un élément non nul dont le carré est nul. En effet on a

$$(\overline{2}^{(4)})^2 = \overline{0}^{(4)}.$$

Cette propriété est fausse dans $\mathbb{Z}/2\mathbb{Z}$ car $(\overline{1}^{(2)})^2 = \overline{1}^{(2)}$ et dans $\mathbb{Z}/3\mathbb{Z}$ car $(\overline{1}^{(3)})^2 = \overline{1}^{(3)}$ et $(\overline{2}^{(3)})^2 = \overline{1}^{(3)}$. Dans ces deux ensembles on a aussi la propriété plus générale :

$$x \cdot y = 0 \Rightarrow x = 0 \text{ ou } y = 0$$

propriété qui est bien entendu fausse dans $\mathbb{Z}/4\mathbb{Z}$, nous l'avons vu pour $x = y = \overline{2}^{(4)}$.

3.1. L'ensemble $\mathbb{Z}/p\mathbb{Z}$ lorsque p est premier.

Proposition 7. *Soit p un nombre premier. Alors l'équation*

$$x \cdot y = 0,\ x, y \in \mathbb{Z}/p\mathbb{Z}$$

a pour seules solutions $x = 0$ ou $y = 0$.

Démonstration. En effet soient $x, y \in \mathbb{Z}/p\mathbb{Z}$. Il existe des entiers m et n, $m < p$ et $n < p$ tels que $x = \overline{m}^{(p)}$ et $y = \overline{n}^{(p)}$. Alors

$$x \cdot y = \overline{m}^{(p)} \cdot \overline{n}^{(p)} = \overline{mn}^{(p)}.$$

Supposons $x \cdot y = 0$, c'est-à-dire $\overline{mn}^{(p)} = \overline{0}^{(p)}$. Alors le produit mn est dans la classe de 0 ce qui est équivalent à dire que mn est congru est 0 modulo p ou encore que mn est divisible par p. Comme p est premier, d'après le théorème de Gauss, alors soit m est divisible par p soit n est divisible par p, soit $\overline{m}^{(p)} = \overline{0}^{(p)}$), soit $\overline{n}^{(p)} = \overline{0}^{(p)}$. D'où la proposition.

Remarque : la réciproque est aussi vraie : si p n'est pas premier, il existe dans $\mathbb{Z}/p\mathbb{Z}$ deux éléments non nuls x et y tels que $x \cdot y = 0$. En effet si p n'est pas premier, il existe m et n diviseurs de p autres que 1 et p tels que $p = mn$. On en déduit que $\overline{m}^{(p)} \cdot \overline{n}^{(p)} = \overline{mn}^{(p)} = \overline{0}^{(p)}$.

3.2. Le théorème de Fermat.

Théorème 2. *Soit p un nombre premier et $a \in \mathbb{Z}$ un entier non multiple de p. Alors*

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

Démonstration. Commençons par démontrer le lemme suivant, souvent appelé identité de Frobenius

Lemme 1. *Soit p un nombre premier. Alors pour tout x et y dans $\mathbb{Z}$, on a*

$$(x + y)^p \equiv x^p + y^p \pmod{p}.$$

En effet si nous développons $(x + y)^p$, par exemple par récurrence, nous voyons que

$$(x + y)^p = x^p + a_{p-1,1}x^{p-1}y + \cdots + a_{p-k,k}x^{p-k}y^k + \cdots + a_{1,p-1}xy^{p-1} + y^p$$

et chacun des coefficients $a_{p-k,k}$ est entier. Or nous avons vu que ces coefficients ne sont rien d'autre que les coefficients binomiaux

$$a_{p-k,k} = \binom{p-k}{p} = \frac{p!}{(p-k)!k!}.$$

On en déduit que ces coefficients binomiaux sont tous entiers. Or

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

soit

$$(k!)\binom{p-k}{p} = p(p-1)\cdots(p-k+1).$$

On en déduit que p divise l'entier $(k!)\binom{p}{p-k}$. Or nous avons supposé p premier. Ceci implique que soit p divise 2, soit divise 3, soit divise k soit divise $\binom{p-k}{p}$. Mais $k < p$. Donc la seule possibilité est p divise $\binom{p-k}{p}$ ce qui implique

$$\binom{p-k}{p} \equiv 0 \pmod{p}.$$

D'où le lemme. Revenons à la démonstration du théorème. Montrons tout d'abord par récurrence sur a que pour tout $a \in \mathbb{N}$,

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

(1) L'identité est vraie pour $a = 0$.

(2) Supposons que cette identité soit vraie pour l'entier a. Alors d'après le lemme ci-dessus

$$(a+1)^p \equiv a^p + 1^p \pmod{p}.$$

Mais par hypothèse de récurrence

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

On en déduit

$$(a+1)^p \equiv a + 1 \pmod{p}.$$

(3) La propriété étant alors vérifiée pour $a + 1$, elle est vraie pour tout $a \in \mathbb{N}$.

Supposons à présent $a \in \mathbb{Z}$. Il existe toujours un entier positif b tel que $a \equiv b \pmod{p}$. Ainsi $a^p \equiv b^p \pmod{p}$ et donc $a^p \equiv b \pmod{p}$ ce qui implique $a^p \equiv a \pmod{p}$. Ainsi pour tout $a \in \mathbb{Z}$,

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

Ceci s'écrit aussi

$$a^p - a = a(a^{p-1} - 1) \equiv 0 \pmod{p}.$$

Mais nous supposons que a n'est pas un multiple de p. Comme p divise $a(a^{p-1} - 1)$, comme il ne divise pas a, il divise $a^{p-1} - 1$. Ceci s'écrit aussi

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

D'où le théorème.

4. Equations diophantiennes

Une équation diophantienne est une équation polynomiale à une ou plusieurs inconnues

$$P(x_1, \cdots, x_n) = 0$$

où P est un polynôme à n inconnues et à coefficients dans $\mathbb{Z}$. Le problème est de chercher les solutions entières à une telle équation. Ce type de problème est extrêmement difficile et on n'a guère de résultats généraux. Une des plus célèbres équations diophantiennes est certainement l'équation de Fermat

$$x^2 + y^n - z^n = 0.$$

Pour $n = 2$, on retrouve l'identité de Pythagore $x^2 + y^2 = z^2$, et on en connaît des solutions entières (exemple $x = 3, y = 4, z = 5$). Il y en a même une infinité. Le problème posé par Fermat (qui affirmait l'avoir résolu) était de montrer que pour $n > 2$, l'équation $x^n + y^n = z^n$

n'avait pas de solution entière. Ce problème a été entièrement résolu en 1994 par Andrew Wiles, après 357 ans d'efforts de la part de nombreux mathématiciens. Nous allons étudier ici quelques cas très particuliers et surtout accessibles.

4.1. **L'équation diophantienne** $ax + by = c$**,** $a, b, c \in \mathbb{Z}$**.**

Théorème 3. *Soient $a, b \in \mathbb{Z}^*$ et soit $c \in \mathbb{Z}$. L'équation diophantienne*

$$ax + by = c$$

admet au moins une solution si et seulement si c est un multiple du PGCD de a et deb.

Démonstration. Montrons que la condition est nécessaire. Supposons que l'équation $ax+by = c$ admette une solution : il existe donc deux entiers m et n tels que

$$am + bn = c.$$

Soit $d = PGCD(a, b)$. Par définition, d divise a, d divise b. Il divise donc toute combinaison linéaire à coefficients entiers. Ainsi d divise $am + bn$. On en déduit donc que d divise c.

Montrons que la condition est suffisante. Supposons donc que $d = PGCD(a, b)$ divise c et montrons que l'équation à au moins une solution (x, y) avec x et y dans $\mathbb{Z}$. L'identité de Bezout appliquée au couple (a, b) implique l'existence de deux entiers u et v tels que

$$au + bv = d.$$

Or d divise c, c'est-à-dire il existe un entier k tel que $c = kd$. Ainsi

$$k(au + bv) = kd = c$$

et donc $(x = ku, v = kv)$ est une solution de $ax + by = c$. D'où le théorème.

Exemples.

(1) Considérons l'équation diophantienne

$$15x + 33y = 14.$$

Nous avons $PGCD(15, 33) = 3$. Or 14 n'est pas un multiple de 3. L'équation diophantienne donnée n'a pas de solutions (en nombres entiers bien entendu).

(2) Considérons l'équation diophantienne

$$66x + 45y = 6.$$

Nous avons $66 = 2 \times 3 \times 11$ et $45 = 3^2 \times 5$. Ainsi $PGCD(66, 45) = 3$ et il divise 6. L'équation admet une solution que nous allons chercher en s'inspirant de la démonstration précédente. Cherchons l'identité de Bézout relative à 66 et 45. Pour cela utilisons l'algorithme d'Euclide.

$$66 = 45 \times 1 + 21$$
$$45 = 21 \times 2 + 321 = 3 \times 7 + 0$$

et le PGCD de 66 et 45 est bien 3. "Remontons ces identités en partant de l'avant dernière donnant le PGCD :

$$45 = 21 \times 2 + 3 \text{ soit } 3 = 45 - 21 \times 2$$
$$66 = 45 \times 1 + 21, \text{ soit } 21 = 66 - 45 \times 1$$
$$3 = 45 - 21 \times 2 \text{ soit } 3 = 45 - (66 - 45) \times 2$$
$$3 = 66 \times (-2) + 45 \times 3.$$

L'identité de Bézout s'écrit donc

$$66 \times (-2) + 45 \times 3 = PGCD(66, 45).$$

Comme $c = 6 = 2 \times 3$, on en déduit

$$66 \times (-4) + 45 \times 6 = 2 \times PGCD(66, 45) = 6.$$

Une solution est donnée par $x = -4$ et $y = 6$.

Le problème restant est celui de trouver toutes les solitions de $ax + by = c$ avec $c = k \cdot PGCD(a, b)$. Soit (x_0, y_0) une solution particulière de $ax + by = c$, avec $x_0, y_0 \in \mathbb{Z}$, donnée par exemple en utilisant l'identité de Bézout. Si (x_1, y_1) est aussi une solution avec $x_1, y_1 \in \mathbb{Z}$, alors on a

$$\begin{cases} ax_0 + by_0 = c, \\ ax_1 + by_1 = c. \end{cases}$$

Nous en déduisons

$$a(x_1 - x_0) + b(y_1 - y_0) = 0.$$

Soit d le PGCD de a et b. Posons $a = da', b = db'$. L'équation précédente est équivalente à

$$a'(x_1 - x_0) = b'(y_0 - y_1)$$

avec $PGCD(a', b') = 1$. Le théorème de Gauss implique alors, comm a' est premier avec b' que a' divise $y_0 - y_1$). De même, b' divise $(x_1 - x_0)$. Ainsi, il existe des entiers k et k' tels que

$$\begin{cases} y_1 - y_0 = ka', \\ x_1 - x_0 = k'b'. \end{cases}$$

Ainsi, toute autre solution (x_1, y_1) avec $x_1, y_1 \in \mathbb{Z}$ est donnée par

$$\begin{cases} y_1 = y_0 + ka', \\ x_1 = x_0 + kb'. \end{cases}$$

Mais $a'x_1 + b'y_1' = 1$ implique aussi

$$a(x_0 + k'b) + b'(y_0 + ka) - 1 = 0 = a'x_0 + b'y_0 + (k + k')a'b' - 1 = (k + k')a'b'.$$

Ainsi $k + k' = 0$ et donc

$$\begin{cases} y_1 = y_0 + ka', \\ x_1 = x_0 - kb'. \end{cases}$$

Proposition 8. *Considérons l'équation diophantienne $ax + by = c$ où c est un multiple de $PGCD(a, b)$. Si (x_0, y_0) est une solution de cette équation, $x_0, y_0 \in \mathbb{Z}$, alors toute autre solution (x_1, y_1) avec $x_1, y_1 \in \mathbb{Z}$ est de la forme*

$$\begin{cases} y_1 = y_0 + ka', \\ x_1 = x_0 - kb' \end{cases}$$

avec $k \in \mathbb{Z}$ et $a = a'PGCD(a, b),\ b = b'PGCD(a, b)$.

4.2. **L'équation de Fermat-Pythagore $x2+y^2 = z^2$.** Le problème consiste à trouver toutes les solutions $(x, y, z) \in \mathbb{Z}^3$ vérifiant l'équation

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

Nous savons, pour avoir étudier quelques triangles rectangles, que cette équation admet des solutions, par exemple $(x = 3, y = 4, z = 5)$ est une solution, $(x = 5, y = 12, z = 13)$ en est une autre. Comment les trouver toutes. Il est clair que si $(x_0, y_0, z_0) \in \mathbb{Z}^3$ est une solution, alors $(\pm x_0, \pm y_0, \pm z_0)$ sont aussi des solutions. Nous pouvons donc nous contenter de chercher les solutions positives.

Définition 2. *Une solution positive* $(_0, y_0, z_0)$ *in*$\mathbb{N}^3$ *est dite primitive si* $PGCD(x_0, y_0, z_0) = 1$.

Notons que pour calculer en général le PGCD de trois entiers (x_0, y_0, z_0), on peut commencer par calculer le PGCD de deux de ces nombres, par exemple $d_1 = PGCD(x_0, y_0)$, puis le PGCD du dernier des trois nombres avec le PGCD venant d'être calcullé, ici dans l'exemple, on calculerait $d = PGCD(z_0, d_1)$. Mias dans le càs présent, où de plus (x_0, y_0, z_0) sont une solution de l'équation de Fermat-Pythagore, nous avons la simplification suivante :

Lemme 2. *Si* (x_0, y_0, z_0) *est une solution de l'équation de Fermat-Pythagore* $x^2 + y^2 = z^2$, *alors les propositions suivantes sont équivalentes*

(1) x_0, y_0, z_0 *sont premiers entre eux, c'est-à-dire* $PGCD(x_0, y_0, z_0) = 1$,

(2) x_0, y_0 *sont premiers entre eux,*

(3) x_0, z_0 *sont premiers entre eux,*

(4) y_0, z_0 *sont premiers entre eux,*

Démonstration. Il est clair que si $PGCD(x_0, y_0) = 1$, alors $PGCD(x_0, y_0, z_0) = 1$. De même $PGCD(x_0, z_0) = 1$ ou $PGCD(y_0, z_0) = 1$ implique $PGCD(x_0, y_0, z_0) = 1$. Supposons maintenant $PGCD(x_0, y_0, z_0) = 1$ et montrons que $PGCD(x_0, y_0) = 1$,$PGCD(x_0, y_0) = 1$ et $PGCD(y_0, z_0) = 1$. Soit d un diviseur commun de x_0 et y_0 : $x_0 = dx_1, y_0 = dy_1$, $x_1, y_1 \in \mathbb{N}$. Alors

$$x_0^2 + y_0^2 = d^2(x_1^2 + y_1^2) = z_0^2$$

et donc d^2 divise z_0^2 et d divise z_0. Ainsi d est un diviseur commun à x_0, y_0, z_0 et par hypothèse $d = 1$. Nous en déduisons que $PGCD(x_0, y_0) = 1$. De même pour $PGCD(x_0, z_0)$ et $PGCD(y_0, z_0)$.

Corollaire 1. *Si* (x_0, y_0, z_0) *est une solution positive primitive de l'équation* $x^2+y^2 = z^2$, *alors les entiers* x_0, y_0, z_0 *sont premiers deux à deux.*

Considérons (x_0, y_0, z_0) une solution positive primitive et étudions la parité de ces entiers.

(1) Si un entier n est pair alors $n^2 \equiv 0 \bmod 4$ et si $m = 2k + 1$ est impair alors $m^2 = 4k^2 + 4k + 1 \equiv 1 \bmod 4$.

(2) Si x_0 et y_0 sont impairs, alors $x_0^2 + y_0^2 \equiv 2 \bmod 4$ et Z_0^2 est, d'après la remarque ci-dessus congrus à 0 ou à 1 modulo 4. Donc ceci est impossible

(3) Ainsi x_0 et y_0 sont de parité différente.

(4) On peut donc supposé x_0 pair , y_0 impair et $PGCD(x_0, y_0) = 1$.

Ceci implique que z_0 est lui aussi impair. Nous avons

$$y_0^2 = z_0^2 - x_0^2 = (z_0 - x_0)(z_0 + x_0)$$

et les entiers $y_0, (z_0 - x_0), (z_0 + x_0)$ sont tous pairs. On en déduit l'équation entre entiers

$$\frac{y_0}{2}^2 = \frac{z_0 - x_0}{2}\frac{z_0 + x_0}{2}.$$

Lemme 3. *Les entiers* $\frac{z_0 - x_0}{2}$ et $\frac{z_0 + x_0}{2}$ *sont premiers entre eux.*

En effet si d est un diviseur commun, alors il divise la somme $\frac{z_0 - x_0}{2} + \frac{z_0 + x_0}{2} = z_0$ et la différence $\frac{z_0 - x_0}{2} - \frac{z_0 + x_0}{2} = x_0$. Ainsi d est un diviseur commun à x_0 et z_0 qui sont supposées premiers, donc $d = 1$, d'où le lemme.

Ainsi comme $\frac{y_0}{2}^2 = \frac{z_0 - x_0}{2}\frac{z_0 + x_0}{2}$, le carré de l'entier $\frac{y_0}{2}$ apparaît comme un produit de deux nombres premiers. Or on ale résultat suivant, que nous démontrerons en exercice :

Lemme 4. *Soient a, b, c des entiers strictement positifs tels que*

$$a^2 = bc$$

avec $PGCD(b, c) = 1$, alors b et c sont aussi des carrés.

On en déduit qu'il existe des entiers strictement positifs m et n tels que

$$\frac{z_0 - x_0}{2} = m^2, \ \frac{z_0 + x_0}{2} = n^2.$$

Ainsi $z_0 = m^2 + n^2, \ x_0 = m^2 - n^2$ ce qui donne aussi $y_0 = 2mn$.

Théorème 4. *Les solutions positives primitives de $x^2 + y^2 = z^2$ sont données par*

$$x_0 = m^2 - n^2, \quad y_0 = 2mn, \quad z_0 = m^2 + n^2$$

où m, n sont des entiers strictement positifs premiers entre eux et $m > n$.

Evidemment on peut permuter les rôles de x_0 et y_0.

Ainsi, pour trouver les solutions primitives, et donc les autres par multiplication par un entier, il suffit de choisir m et n :

(1) Si $m = 2, n = 1$, nous avons $(x_0, y_0, z_0) = (3, 4, 5)$.
(2) Si $m = 3, n = 2$, nous avons $(x_0, y_0, z_0) = (5, 12, 13)$.
(3) Si $m = 4, n = 1$, nous avons $(x_0, y_0, z_0) = (15, 8, 17)$.
(4) Si $m = 4, n = 3$, nous avons $(x_0, y_0, z_0) = (7, 24, 25)$.
(5) Si $m = 5, n = 2$, nous avons $(x_0, y_0, z_0) = (21, 20, 29)$.
(6) Si $m = 5, n = 3$, nous avons $(x_0, y_0, z_0) = (16, 30, 34)$.

5. Résolution des équations sur les congruences

Nous nous intéressons à résoudre des équations du type

$$ax \equiv b \pmod{p}$$

où p est un entier donné strictement positif ainsi que les constantes a et b, ou plus généralement des systèmes du type

$$\begin{cases} a_1x \equiv b_1 \pmod{p} \\ a_2x \equiv b_2 \pmod{p} \end{cases}$$

où a_1, a_2, b_1, b_1 et p sont des entiers donnés et p strictement positif. On cherche bien entendu des solutions dans $\mathbb{Z}$.

5.1. **Etude de l'équation** $ax \equiv b \pmod{p}$**.** L'équation $ax \equiv b \pmod{p}$ s'écrit aussi $ax = b+kp$ ou bien

$$ax - kp = b$$

est donc du type Bézout. Elle implique donc que b est un multiple du PGCD de a et de p. En effet, posons $d = PGCD(a, p)$. On obtient alors $a = da_1$ et $p = ddp_1$ avec $a_1, p_1 \in \mathbb{Z}^*$. D'où

$$da_1x - kdp_1 = b$$

soit

$$d(a_1x - kp_1) = b$$

et d est un diviseur de b. Nous en déduisons

Proposition 9. *Soit l'équation* $ax \equiv b \pmod{p}$*. Soit* $d = PGCD(a, p)$*. Si* d *ne divise pas* b *alors l'équation donnée n'a pas de solutions. Si* d *divise* b*, alors l'équation donnée a des solutions.*

Démonstration. Il nous reste à démontrer la deuxième partie de cette proposition. Reprenons la dernière équation ci-dessus

$$d(a_1x - kp_1) = b.$$

Si b est un multiple de d, il s'écrit $b = db_1$ avec $b_1 \in \mathbb{Z}^*$. En remplaçant dans l'équation précédente, nous obtenons

$$a_1x - kp_1 = b_1$$

avec $PGCD(a_1, p_1) = 1$. Cette équation est équivalente à

$$a_1x \equiv b_1 \bmod p_1 \quad \text{et} \quad PGCR(a_1, p_1) = 1.$$

L'identité de Bézout assure l'existence d'un couple d'entiers u et v tels que

$$a_1u + p_1v = 1.$$

Toute autre couple $u, v)$ vérifiant cette identité est de la forme

$$u' = u + np_1,\ v' = v - na_1,\ n \in \mathbb{Z}.$$

On en déduit que les solutions de $a_1x \equiv b_1 \bmod p_1$ son données par

$$x = u + np_1,\ n \in \mathbb{Z}.$$

D'où la proposition.

Remarque. La démonstration ci-dessus nous donne une méthode de résolution de $ax \equiv b \pmod{p}$ lorsque b est un multiple de $PGCD(a, p)$.

(1) Si $d = PGCD(a, p)$ (d peut être égal à 1), alors en posant $a = a_1 d,\ p = p_1 d$ et $b = db_1$, on se ramène à l'équation
$$a_1 x \equiv b_1 \pmod{p_1}.$$
(2) Comme a_1 et p_1 sont premiers entre eux, on explicite l'identité de Bézout
$$a_1 u + p_1 v = 1.$$
(3) Les solutions sont données par
$$x = du + np_1,\ n \in \mathbb{Z}.$$

Exemple. Soit à résoudre
$$6x \equiv 9 \pmod{15}.$$
On a $d = PGCD(6, 15) = 3$ et $b = 9$ est un multiple de $d = 3$. Les solutions sont donc données en résolvant
$$2x \equiv 3 \pmod{5}.$$
L'identité de Bézout relative au couple $(2, 5)$ s'écrit
$$2 \times (-2) + 5 \times (1) = 1$$
soit $u = -2$ et $v = 1$. On en déduit les solutions de l'équation proposées
$$x = -2 \times 3 + 5n = -6 + 5n,\ n \in \mathbb{Z}.$$
Ainsi $\cdots, -16, -11, -6, 4, 9, 14, 19, \cdots$

5.2. **Systèmes de congruence.** Nous pouvons trouver dans la littérature un grand nombre d'énigmes qui se résolvent via l'approche que nous allons présenter ici. Par exemple, en voici une : *Un pâtissier a préparé des bredala avec 1 kilo de farine, chacun des bredala pesant au moins 10 grammes. Il veut ranger ces gateaux dans une boite, de manière bien ordonnée. Mais s'il range ses gateaux sur deux rangées, il lui reste un gateau non rangé. S'il fait 3, 4, 5 ou 6 rangées, il lui en reste toujours 1. Combien de gateaux a-t-il fabriqué ?.*

Les systèmes "mathématiques" qui nous intéressent ici s'écrivent, pour les plus simples :

Soient donnés $a, b \in \mathbb{Z}$ et $m, n \in \mathbb{N}^*$. Existe -t-il une ou plusieurs solutions au système
$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

Le théorème suivant, appelé théorème des restes chinois, suite à l'étude de l'énigme "*Soient des objets en nombre inconnu. Si on les range par 3 il en reste 2. Si on les range par 5, il en reste 3 et si on les range par 7, il en reste 2. Combien a-t-on d'objets ?* " par un mathématicien chinois, permet da savoir les conditions pour avoir des solutions. Une fois vérifiées les hypothèses de ce théorème, la recherche des solutions se fait de manière classique, via l'identité de Bézout.

Théorème 5. *Soient $a, b \in \mathbb{Z}$ et m, n des entiers supérieurs ou égal à 2. Alors si m et n sont premiers entre eux, le système de congruence*
$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$
admet des solutions.

Démonstration. Le système donné est est équivalent à

$$\begin{cases} x = a + km \\ x = b + k'n \end{cases}$$

avec $k, k' \in \mathbb{Z}$. Nous en déduisons

$$a - b = k'n - km.$$

Ceci est une équation diophantienne linéaire. Nous avons vu qu'il existait des solutions si et seulement si m et n étaient premiers entre eux. D'où le théorème.

La résolution des équations diophantiennes nous permet alors de trouver les solutions du système de congruence.

Proposition 10. *Supposons m et n premiers entre eux. Alors les solutions du système de congruence*

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

sont données par

$$x = x_0 + kmn$$

où x_0 est une solution particulière.

Exemple. Soit à résoudre le système de congruence

$$\begin{cases} x \equiv 5 \pmod{11} \\ x \equiv 7 \pmod{15} \end{cases}$$

Comme $m = 11$ et $n = 15$ sont premiers entre eux, ce système admet des solutions. Nous avons vu que la solution générale est obtenue dès que l'on connait une solution particulière. On a

$$x = 5 + 11k = 7 + 15k'$$

d'où

$$11k - 15k' = 2.$$

Cherchons la relation de Bézout entre 11 et 15 qui est par exemple donnée par l'algorithme d'Euclide :

$$15 = 11 + 4,\ 11 = 4 \times 2 + 3,\ 4 = 3 + 1$$

et donc $PGCD(15, 11) = 1$. Redévissons cet algorithme :

$$4 - 3 = 1, 4 - (11 - 4 \times 2) = 4 \times 3 - 11 = (15 - 11) \times 3 - 11 = 15 \times 3 - 11 \times 4.$$

Ainsi

$$1 = 15u + 11v$$

s'écrit

$$1 = 15 \times 3 - 11 \times 4.$$

Ceci implique

$$2 = 15 \times (6) + 11 \times (-8).$$

On en déduit

$$k = -8,\ k' = 6$$

et donc une solution particulière est

$$x_0 = 5 + 11 \times (-8) = -83.$$

La solution générale est donc

$$x = 9 - 83 + 165k, \quad k \in \mathbb{Z}.$$

EXERCICES

Exercice 1. Calculer, en utilisant le théorème de Fermat

$$2004^{2005} \pmod{13}.$$

Exercice 2. Soit a un entier pair strictement positif. Soit p un nombre premier qui divise $a^2 + 1$.

(1) Montrer que p est de la forme $4n + 1$. (on pourra utiliser le théorème de Fermat)

(2) En déduire qu'il existe une infinité de nombre premier de la forme $4n + 1$. (On pourra faire un raisonnement par l'absurde).

(3)

bf Exercice. Résoudre le système de congruence

$$\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \end{cases}$$

bf Exercice. Résoudre le système de congruence

$$\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 1 \pmod 3 \\ x \equiv 1 \pmod 4 \\ x \equiv 1 \pmod 5 \\ x \equiv 1 \pmod 6 \end{cases}$$

En déduire la solution de l'épigme du pâtissier et de ses gâteaux. **Exercice.** Résoudre **Exemple.** Soit à résoudre le système de congruence

$$\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \end{cases}$$