CHAPITRE 3 : CONGRUENCES ET ARITHMÉTIQUE MODULAIRE

1. Congruences

Définition 1.1. Soit m, a, b entiers. On dit que a *est congru à* b *modulo* m si m divise $a - b$. (On dit aussi que "a et b sont congrus modulo m".) En symboles

$$a \equiv b \pmod{m} \iff m \mid a - b \iff \exists k \in \mathbb{Z} \text{ avec } a - b = kn.$$

Par exemple on a $2 \equiv 8 \pmod 3$ car 3 divise $2 - 8 = -6$. On a $a \equiv 0 \pmod 2$ si et seulement si 2 divise $a - 0 = a$, c'est à dire ssi a est pair. On a $a \equiv 1 \pmod 2$ ssi il existe k avec $a - 1 = 2k$ et donc $a = 2k + 1$ est impair. Similairement on a

$$\begin{aligned} a \equiv 2 \pmod 5 &\iff a = 5k + 2 \text{ avec } k \text{ entier}, \\ a \equiv 1 \pmod 4 &\iff a = 4k + 1 \text{ avec } k \text{ entier}, \\ a \equiv 3 \pmod 4 &\iff a = 4k + 3 \text{ avec } k \text{ entier}. \end{aligned}$$

Surtout on a

$$\boxed{a \equiv 0 \pmod n \iff a = nk \text{ avec } k \text{ entier.} \iff a \text{ est un multiple de } n}$$

Quelques propriétés de la congruence

Théorème 1.2. *Soit a, b, c, a', b', n entiers. Les énoncés suivants sont vrais :*
(a) (Reflexivité) $a \equiv a \pmod n$.
(b) (Symétrie) $a \equiv b \pmod n$ *implique* $b \equiv a \pmod n$.
(c) (Transitivité) $a \equiv b,\ b \equiv c \pmod n$ *implique* $a \equiv c \pmod n$.
(d) $a \equiv a',\ b \equiv b' \pmod n$ *implique* $a \pm a' \equiv b \pm b' \pmod n$.
(e) $a \equiv a',\ b \equiv b' \pmod n$ *implique* $aa' \equiv bb' \pmod n$.
(f) *Si d est un diviseur commun de a, b et n, alors* $a \equiv b \pmod n$ *implique* $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{n}{d}}$.
(g) *Si d divise n, alors* $a \equiv b \pmod n$ *implique* $a \equiv b \pmod d$.

Donc les règles de manipulation des congruences contiennent la plupart des règles de manipulations d'égalités entre entiers pour l'addition, la soustraction, et la multiplication. Mais pour la division (et la simplification des congruences), c'est plus compliqué.

Exemple : $2 \equiv 16$ et $3 \equiv 10 \pmod 7$ impliquent $2 \cdot 3 \equiv 16 \cdot 10$ et donc $6 \equiv 160 \pmod 7$.

Preuve. (a) $a - a = 0 = 0n$.
(b) $a - b = kn \Longrightarrow b - a = -kn$.
(c) $a - b = kn,\ b - c = \ell n \Longrightarrow a - c = (a - b) + (b - c) = (k + \ell)n$.
(d) Laissée comme exercice.
(e) $a - a' = kn,\ b - b' = \ell n \Longrightarrow ab - a'b' = ab - a'b + a'b - a'b' = (a - a')b + a'(b - b') = (kb + a'\ell)n$.
(f) Laissée comme exercice.
(g) Si $d \mid n$ et $n \mid a - b$, alors $d \mid a - b$. □

Théorème 1.3. *Soient n et a entiers avec $n \geq 1$. Alors a est congru modulo n à exactement un des nombres $0, 1, 2, \ldots, n - 1$.*

Donc chaque entier est congru à 0 ou 1 modulo 2, mais pas aux deux. Chaque entier est congru à 0, 1 ou 2 modulo 3, mais pas à plus qu'un parmi les trois. Etc.

Preuve. Par la division euclidienne, on peut écrire $a = qn + r$ avec q, r entiers et $0 \leq r \leq n-1$. Et $a \equiv r \pmod{n}$ car leur différence est qn. Donc a est congru à un des nombres $0, 1, 2, \ldots, n-1$.

Supposons maintenant que a est congrus à deux nombres r et s parmi $0, 1, \ldots, n-1$. Par symétrie et transitivité r et s sont aussi congrus, et il existe k entier avec $r - s = kn$. Or on a $0 \leq r < n$ et $-n < -s \leq 0$, donc $-n < r - s = kn < n$ et en divisant par n, $-1 < k < 1$. Comme k est entier, on a $k = 0$ et $r = s$. □

2. Les congruences $ax \equiv b \pmod{n}$.

On cherche les solutions x de congruences commes $7x \equiv 11 \pmod{31}$ et en général $ax \equiv b \pmod{n}$. On considère d'abord le cas où a et n sont premiers entre eux, comme 7 et 31.

Théorème 2.1. *Si a et n sont premiers entre eux, alors il existe une solution x de $ax \equiv b \pmod{n}$, et c'est unique modulo n.*

Existence. On cherche une relation de Bezout $7u + 31v = \pm 1$ par l'algorithme d'Euclide étendu.

		+	−	+	−	+
	a_i			4	2	3
	u_i	31	7	3	1	0
-7	p_i	0	1	4	9	31
$+31$	q_i	1	0	1	2	7

On trouve $31 \cdot 2 - 7 \cdot 9 = -1$. Modulo 31, on a $31 \equiv 0$, donc cela devient $7 \cdot 9 \equiv 1 \pmod{31}$. On multiplie par 11 donnant $7 \cdot 9 \cdot 11 \equiv 7 \cdot 99 \equiv 11 \pmod{31}$, et on réduit modulo 31 par la division euclidienne $99 = 3 \cdot 31 + 6$. Donc $99 \equiv 6$ et $7 \cdot 6 \equiv 11 \pmod{31}$. Finalement pour tout $x \equiv 6 \pmod{31}$ on aura aussi $7x \equiv 11 \pmod{31}$.

A noter que dans la relation de Bezout on utilise le numérateur 9 et le dénominateur 2 de l'avant-dernière réduite de $\frac{31}{7}$, avec ***signes opposés***.

La même méthode marche pour toute congruence $ax \equiv b \pmod{n}$ tant que a et n sont premiers entre eux.

Unicité. En général, si a et n sont premiers entre eux, et on a $ax \equiv b$ et $ay \equiv b \pmod{n}$, alors on a $ax \equiv ay \pmod{n}$ par transitivité, et donc $ax - ay \equiv 0$ et $a(x-y) \equiv 0 \pmod{n}$. Donc n divise $a(x-y)$. Mais a et n sont premiers entre eux. Donc par le lemme de Gauss, n doit diviser $x - y$, et donc x et y sont congrus modulo n.

Le cas où a et n non premiers entre eux.

Théorème 2.2. *Il existe une solution x de $ax \equiv b \pmod{n}$ si et seulement si $d = \text{pgcd}(a, n)$ divise b. La solution x est unique modulo $\frac{n}{d}$.*

La condition que d divise b est nécessaire, c'est à dire, si la congruence a une solution, alors d divise b. En effet, si on a $ax \equiv b \pmod{n}$, alors il existe k entier avec $ax - b = kn$ et $b = ax - kn$. Comme d divise a et n, il divise aussi $ax - kn = b$.

La condition que d divise b est suffisante aussi, c'est à dire, si d divise b, alors la congruence a une solution. En effet, si d divise b, alors en appliquant l'algorithme d'Euclide étendu à n

et a, on trouve $u = (-1)^N p_{N-1}$ et $v = (-1)^{N-1} q_{N-1}$ avec $au + vn = d$. Cela donne $au \equiv d \pmod{n}$. En multipliant par $\frac{b}{d}$ on trouver $a(u\frac{b}{d}) \equiv b \pmod{n}$.

La congruence $ax \equiv b \pmod{n}$ est équivalente à $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$ avec $\frac{a}{d}$ et $\frac{n}{d}$ premiers entre eux. Comme les solutions de cette dernière congruence sont uniques modulo $\frac{n}{d}$, les solutions de $ax \equiv b \pmod{n}$ sont uniques modulo $\frac{n}{d}$ aussi.

Deux exemples :

(1) Dans la congruence $36x \equiv 80 \pmod{90}$, on a $\text{pgcd}(36, 90) = 18$, mais 18 ne divise pas 80. Donc il n'y a pas de solution.

(2) Pour résoudre $125x \equiv 275 \pmod{450}$, on applique l'algorithme d'Euclide étendu à 450 et 125

		+	−	+	−	+	−
	a_i			3	1	1	2
	u_i	450	125	75	50	25	0
−125	p_i	0	1	3	4	7	18
+450	q_i	1	0	1	1	2	5

On trouve $125(-7) + 450 \cdot 2 = 25$, et donc $125(-7) \equiv 25 \pmod{450}$. Maintenant on multiplie par $\frac{275}{25} = 11$, donnant $125(-77) \equiv 275 \pmod{450}$. La solution est unique modulo $\frac{450}{25} = 18$, donc la solution est $x \equiv -77 \pmod{18}$ ou bien $x \equiv 13 \pmod{18}$.

3. Le théorème chinois

Le théorème chinois. *Soit m et n des entiers premiers entre eux. Alors quelque soit a et b entiers il existe des solutions simultanées de $x \equiv a \pmod{m}$ et $x \equiv b \pmod{n}$, et cette solution x est unique modulo mn.*

Unicité. Soit x une solution simultanée des deux congruences, et soit y un deuxième entier. Alors y est aussi une solution des deux congruences ssi on a $x \equiv y \pmod{m}$ et $x \equiv y \pmod{n}$. Alors $m \mid x - y$ et $n \mid x - y$, ce qui équivaut à ce que $\text{ppcm}(m, n) \mid x - y$ ou $x \equiv y \pmod{\text{ppcm}(m, n)}$. Mais comme m et n sont premiers entre eux, on a $\text{ppcm}(m, n) = mn$. Donc y est aussi une solution des deux congruences ssi $x \equiv y \pmod{mn}$.

Existence. On cherche une relation de Bezout $\boxed{mu + nv = 1}$. Alors on a $nv = 1 - mu$ et $mu = 1 - nv$. Il s'ensuit qu'on a

$$nv \equiv 1 \pmod{m}, \qquad nv \equiv 0 \pmod{n},$$
$$mu \equiv 0 \pmod{m}, \qquad mu \equiv 1 \pmod{n}.$$

Il s'ensuit que si on prend $\boxed{x = anv + bmu}$ on a bien $x \equiv a \cdot 1 + b \cdot 0 \equiv a \pmod{m}$ et $x \equiv a \cdot 0 + b \cdot 1 \equiv b \pmod{n}$.

Faisons un exemple. Cherchons les x avec $x \equiv 11 \pmod{18}$ et $x \equiv 25 \pmod{77}$. On cherche une relation de Bezout $18u + 55v = 1$.

		+	−	+	−	+	−	+
	a_i			4	3	1	1	2
	u_i	77	18	5	3	2	1	0
−18	p_i	0	1	4	13	17	30	77
+77	q_i	1	0	1	3	4	7	18

On a $18 \cdot 30 + 77(-7) = 1$ avec $u = 30$ et $v = -7$. La solution est $x \equiv 11 \cdot 77(-7) + 25 \cdot 18 \cdot 30 \equiv 7571$. Comme on a $18 \cdot 77 = 1386$, les solutions sont $x \equiv 7571 \equiv 641 \pmod{1386}$.

Quand m et n ne sont pas premiers entre eux, on a le théorème suivant.

Théorème 3.1. *Soit m et n entiers naturels, et $d = \text{pgcd}(m, n)$. Alors il existe une solution simultanée x de $x \equiv a \pmod m$ et $x \equiv b \pmod n$ si et seulement si on a $a \equiv b \pmod d$. La solution x est unique modulo $\text{ppcm}(m, n)$.*

Existence. Soit $y = x - a$. On cherche y vérifiant $y \equiv 0 \pmod m$ et $y \equiv b - a \pmod n$. Par le lemme de Bezout il existe u et v avec $mu + nv = d$. On a donc $mu \equiv 0 \pmod m$ et $mu \equiv d \pmod n$. Comme on a $a \equiv b \pmod d$, le nombre $\frac{b-a}{d}$ est entier. On prend $y = mu\frac{b-a}{d}$ et donc $x = a + mu\frac{b-a}{d}$ comme solutions.

Unicité. Similaire au cas où m et n sont premiers entre eux.

4. Systèmes de représentants modulo n

Définition 4.1. Une famille de n entiers $a_1, \ldots, a_n$ telle que tout entier est congru à modulo n à exactement un des a_i est *un système de représentants modulo n.*

Donc $0, 1, 2, 3, 4$ est un système de représentants modulo 5. On peut substituer 5 pour 0, car ils sont congrus modulo 5, et $1, 2, 3, 4, 5$ est un système de représentants modulo 5. Les entiers congrus à $1, 2, 3, 4 \pmod 5$ y restent ; les entiers congrus à 0 sont congrus aussi à 5. Similairement on peut passer de $0, 1, 2, 3, 4$ à $0, 1, 2, -2, -1 = -2, -1, 0, 1, 2$ car $3 \equiv -2$ et $4 \equiv -1 \pmod 5$. Les entiers congrus à $0, 1, 2$ continuent à l'être, ceux congrus à 3 sont congrus à -2, et ceux congrus à 4 sont congrus à -1.

En général, si on prend certains nombres $a_1, a_2, \ldots, a_r$ de la liste $0, 1, 2, \ldots, n-1$ et on les remplace par $b_1, b_2, \ldots, b_r$ avec $a_i \equiv b_i \pmod n$ pour tout i, alors on a toujours un système de représentants modulo n.

Théorème 4.2. *Soient n et a entiers avec $n \geq 1$.*

(a) *Si $n = 2k + 1$ est impair, alors a est congru modulo n à exactement un des n entiers $-k, \ldots, -1, 0, 1, \ldots, k$.*

(b) *Si $n = 2k$ est pair, alors a est congru modulo n à exactement un des n entiers $-(k-1), \ldots, -1, 0, 1, \ldots, k-1, k$.*

Dans les deux cas a est congru modulo n à exactement un entier ρ avec $-\frac{n}{2} < \rho \leq \frac{n}{2}$.

Preuve. Le théorème précédent dit que chaque entier a est congru modulo n à exactement un entier r avec $0 \leq r < n$. Si $0 \leq r \leq \frac{n}{2}$, on pose $\rho = r$. Sinon, on a $\frac{n}{2} < r < n$, et on pose $\rho = r - n$, et on a $-\frac{n}{2} < \rho < 0$, et on a toujours $a \equiv r \equiv r - n \equiv \rho \pmod n$. Donc a est congru modulo n à exactement un entier dans $\left]-\frac{n}{2}, 0\right[\cup \left[0, \frac{n}{2}\right] = \left]-\frac{n}{2}, \frac{n}{2}\right]$. □

Théorème 4.3. *Soit $a_1, a_2, \ldots, a_n$ une famille de n entiers avec la propriété que $a_i \not\equiv a_j \pmod n$ pour tout $i \neq j$. Alors $a_1, a_2, \ldots, a_n$ est un système de représentants modulo n.*

Preuve. Considérons l'application

$$\begin{aligned} \{a_1, a_2, \ldots, a_n\} &\longrightarrow \{0, 1, 2, \ldots, n-1\} \\ a_i &\longmapsto \text{reste de la division euclidienne de } a_i \text{ par } n. \end{aligned}$$

Aucun entier parmi $\{0, 1, 2, \ldots, n-1\}$ n'a plus qu'un antécédent, car si a_i et a_j avait le même reste r, on aurait $a_i \equiv r \equiv a_j \pmod n$, qui est exclu par hypothèse sauf pour $i = j$. Donc l'application est injective. Une application injective entre deux ensembles du même cardinal fini est toujours bijective. Donc chaque entier k parmi $\{0, 1, 2, \ldots, n-1\}$ a exactement un antécédent qu'on notera a_{i_k}.

Maintenant tout entier est congru modulo n à exactement un entier k parmi $\{0, 1, 2, \ldots, n-1\}$ et à exactement un entier a_{i_k} parmi $\{a_1, a_2, \ldots, a_n\}$. □

5. Les carrés modulo n

Chercher les carrés modulo n signifie chercher les nombres k parmi $0, 1, \ldots, n-1$ pour lesquels il existe un a avec $a^2 \equiv k \pmod{n}$. Comme $a \equiv b \Longrightarrow a^2 \equiv b^2 \pmod{n}$, on peut se restreindre par le théorème 4.2 aux a avec $-\frac{n}{2} < a \leq \frac{n}{2}$. Mais comme $(-a)^2 \equiv a^2 \pmod{n}$, on peut même se restreindre aux a positifs dans cette liste, c'est à dire à $0, 1, \ldots, \left[\frac{n}{2}\right]$.

Les carrés modulo n sont les restes de la division euclidienne par n de $0^2, 1^2, 2^2, \ldots, \left[\frac{n}{2}\right]^2$.

Par exemple, modulo 10 on a

$$0^2 \equiv 0, \qquad 1^2 \equiv 1, \qquad 2^2 \equiv 4, \qquad 3^2 \equiv 9, \qquad 4^2 \equiv 6, \qquad 5^2 \equiv 5 \pmod{10}$$

Donc 0, 1, 4, 5, 6, 9 sont des carrés modulo 10, mais 2, 3, 7, 8 ne sont pas des carrés modulo 10. La représentation décimale d'un carré termine toujours en 0, 1, 4, 5, 6 ou 9.

Modulo 4 on a $0^2 \equiv 0$, $1^2 \equiv 1$, et $2^2 \equiv 0 \pmod{4}$. Modulo 8 on a

$$0^2 \equiv 0, \qquad 1^2 \equiv 1, \qquad 2^2 \equiv 4, \qquad 3^2 \equiv 1, \qquad 4^2 \equiv 0 \pmod{8}.$$

D'où :

Théorème 5.1. (a) *Tout carré est congru à* 0 *ou* 1 *modulo* 4.
(b) *Tout carré est congru à* 0, 1, *ou* 4 *modulo* 8.

Théorème 5.2. (a) *Aucun nombre de la forme* $4k+3$ *n'est la somme de deux carrés* a^2+b^2.
(b) *Aucun nombre de la forme* $8k+7$ *n'est la somme de trois carrés* $a^2+b^2+c^2$.

Preuve du théorème 5.2. (a) L'énoncé est équivalent à $a^2 + b^2 \not\equiv 3 \pmod{4}$ pour tout a et b entiers. Mais on a $a^2 \equiv 0$ ou 1, et $b^2 \equiv 0$ ou 1 (mod 4). Donc $a^2 + b^2$ est congru à $0+0$ ou $0+1$ ou $1+0$ ou $1+1$ modulo 4. Les valeurs possibles sont 0, 1, 2 seules. Et 3 n'est pas atteint comme une valeur de $a^2 + b^2 \pmod{4}$.
(b) Exercice. □

6. Arithmétique modulo un premier p

Théorème 6.1. *Soit* p *premier. Si* $ab \equiv 0 \pmod{p}$, *alors* $a \equiv 0$ *ou* $b \equiv 0 \pmod{p}$.

C'est une réécriture du théorème : "Si p est premier et $p \mid ab$, alors $p \mid a$ ou $p \mid b$."

Corollaire 6.2. *Soit* p *premier, et* $c \not\equiv 0 \pmod{p}$. *Si* $ac \equiv bc \pmod{p}$, *alors* $a \equiv b \pmod{p}$.

Preuve. Si $ac \equiv bc \pmod{p}$, alors $(a-b)c \equiv 0 \mod p$. Par le théorème, on a $a - b \equiv 0$ ou $c \equiv 0 \pmod{p}$. Mais par hypothèse, on a $c \not\equiv 0 \pmod{p}$. Donc c'est $a - b \equiv 0$ et ensuite $a \equiv b \pmod{0}$. □

Corollaire 6.3. *Soit* p *premier. Si* $a^2 \equiv b^2 \pmod{p}$, *alors* $a \equiv \pm b \pmod{p}$.

A noter que si on remplace le premier p par un entier quelconque, les conclusions du théorème et du corollaires devient fausses. Par exemple on a $4 \cdot 2 \equiv 0 \pmod{8}$, mais $4 \not\equiv 0$ et $2 \not\equiv 0 \pmod{8}$. Et on a $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{8}$, mais $1 \not\equiv \pm 3 \pmod{8}$. Mais 8 n'est pas premier.

Preuve. De $a^2 \equiv b^2 \pmod{p}$ on déduit $a^2 - b^2 \equiv 0$ et $(a-b)(a+b) \equiv 0 \pmod{p}$. Le théorème précédent montre alors que $a-b \equiv 0$ ou $a+b \equiv 0 \pmod{p}$. D'où $a \equiv b$ ou $a \equiv -b \pmod{p}$. □

Théorème 6.4. *Soit p premier et a entier avec $a \not\equiv 0 \pmod{p}$. Alors pour tout c il existe une solution x de la congruence $ax \equiv c \pmod{p}$, et cette solution est unique modulo p.*

Preuve. Pour p premier, la condition $a \not\equiv 0 \pmod{p}$ implique que a et p sont premiers entre eux. Donc le théorème actuel est le cas particulier du théorème 2.1 avec $n = p$ un premier. □

On a dit que $0, 1, 2, \ldots, p-1$ forment un système de représentants modulo p. Si on supprime le 0 et on prend le produit des autres on trouve $1 \cdot 2 \cdot 3 \cdots (p-1) \not\equiv 0 \pmod{p}$ par le théorème 6.1 car aucun des facteurs n'est congru à 0.

Soit $0, a_1, a_2, \ldots, a_{p-1}$ un autre système de représentants modulo p contenant 0. Alors pour chaque k parmi $1, \ldots, p-1$ il y a exactement un i_k parmi $1, 2, \ldots, p-1$ tel que $k \equiv a_{i_k} \pmod{p}$. De plus $i_k \neq i_j$ pour $k \neq j$. Donc on a

$$\begin{aligned} a_1 \cdot a_2 \cdot a_3 \cdots a_{p-1} &\equiv a_{i_1} \cdot a_{i_2} \cdot a_{i_3} \cdots a_{i_{p-1}} && \text{on permute les facteurs} \\ &\equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p} && \text{car } a_{i_1} \equiv 1,\ a_{i_2} \equiv 2, \text{ etc.} \end{aligned}$$

On a montré

Lemme 6.5. *Soit p premier et $0, a_1, \ldots, a_{p-1}$ un système de représentants modulo p contenant 0. Le produit de ses membres non nuls vérifie $a_1 \cdot a_2 \cdots a_{p-1} \equiv 1 \cdot 2 \cdots (p-1) \equiv (p-1)! \pmod{p}$.*

Théorème 6.6. *Soit p premier et $a \not\equiv 0 \pmod{p}$. Alors on a $a^{p-1} \equiv 1 \pmod{p}$.*

Par exemple, modulo 7 on a $1^6 \equiv 1$, $2^6 = 64 \equiv 1$, $3^6 = 729 \equiv 1$, $4^6 \equiv 4096 \equiv 1$, $5^6 = 15625 \equiv 1$, $6^6 = 46656 \equiv 1 \pmod{7}$.

Preuve. Considérons les p entiers

$$a \cdot 0 = 0,\ a \cdot 1,\ a \cdot 2,\ \ldots\ ,\ a \cdot (p-1).$$

Dans cette liste on a $a \cdot i \not\equiv a \cdot j \pmod{p}$ pour $i \neq j$, car on a $i \not\equiv j \pmod{p}$ pour $i \neq j$ (vu que $0, 1, \ldots, p-1$ est un systéme de représentants modulo p) et on a le corollaire 6.2. Donc c'est un système de représentants modulo p (théorème 4.3). Par le lemme, on a donc

$$(a \cdot 1)(a \cdot 2) \cdots (a \cdot (p-1)) \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}.$$

En regroupant cela donne

$$a^{p-1}\,(p-1)! \equiv (p-1)! \equiv 1\,(p-1)! \pmod{p}.$$

Or $(p-1)! \not\equiv 0 \pmod{p}$ car aucun de ses facteurs n'est pas $\equiv 0$ et on a le théorème 6.1. Donc on peut simplifier par $(p-1)!$ dans la congruence (corollaire 6.2) et trouver $a^{p-1} \equiv 1 \pmod{p}$. □

Théorème de Fermat. *Soit p premier et a entier. Alors $a^p \equiv a \pmod{p}$.*

Preuve. On deux cas : soit $a \not\equiv 0 \pmod{p}$, soit $a \equiv 0 \pmod{p}$.

Dans le premier cas, on applique le théorème précédent et on trouve $a^{p-1} \equiv 1$ et $a^p \equiv a \cdot a^{p-1} \equiv a \cdot 1 \equiv a \pmod{p}$.

Dans le second cas, on a $a^p \equiv 0^p \equiv 0 \equiv a \pmod{p}$. □

Soit maintenant p premier. On veut évaluer $(p-1)!$ modulo p comme suit.

Par par le théorème 6.4, associé à chaque entier $x \in \{1, 2, \ldots, p-1\}$ est un entier y avec $xy \equiv 1 \pmod{p}$, et cet y est unique modulo p. On peut prendre cet y dans $\{1, 2, \ldots, p-1\}$. (On appelle cet y *l'inverse de x modulo p.*) Si à x on associe y par cette procédure, alors à y on associe x car $xy \equiv 1 \pmod{p}$ se lit aussi $yx \equiv 1 \pmod{p}$. Donc on peut diviser $\{1, 2, \ldots, p-1\}$ en des sous-ensembles $\{x_i, y_i\}$ disjoints avec $x_i y_i \equiv 1$. Par exemple, pour $p = 11$ ces sous-ensembles sont

$$\{1\},\ \{2,6\},\ \{3,4\},\ \{5,9\},\ \{7,8\},\ \{10\}.$$

Tous ces sous-ensembles sont de cardinal 2 sauf quand on a un $\{x\}$ avec x associé à lui-même, c'est-à-dire $xx =\equiv 1 \pmod{p}$. Ce sont les x vérifiant $x^2 \equiv 1^2 \pmod{p}$ donc par le corollaire 6.3 les x avec $x \equiv \pm 1 \pmod{p}$, donc $x = 1$ et $x = p-1 \equiv -1 \pmod{p}$.

Maintenant calculons $(p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-1)$ en regroupant le produit selon ces sous-ensembles. Pour $p = 11$ on a

$$\begin{aligned} 10! &= 1 \cdot (2 \cdot 6) \cdot (3 \cdot 4) \cdot (5 \cdot 9) \cdot (7 \cdot 8) \cdot 10 \\ &\equiv 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot (-1) && \pmod{11} \\ &\equiv -1. \end{aligned}$$

Pour un premier $p \geq 3$ général (on traite $p = 2$ à part), on a une division de $\{1, \ldots, p-1\}$ en deux sous-ensembles $\{1\}, \{p-1\}$ de cardinal 1, et $\frac{p-3}{2}$ sous-ensembles $\{x_i, y_i\}$ de cardinal 2. On trouve

$$\begin{aligned} (p-1)! &= 1 \cdot (x_1 \cdot y_1) \cdot (x_2 \cdot y_2) \cdots (x_{\frac{p-3}{2}} \cdot y_{\frac{p-3}{2}}) \cdot (p-1) \\ &\equiv 1 \cdot 1 \cdot 1 \cdots 1 \cdot (-1) && \pmod{p} \\ &\equiv -1. \end{aligned}$$

On a montré le théorème suivant pour les premiers $p \geq 3$. Le cas du premier $p = 2$ est facile.

Théorème de Wilson. *Pour tout premier p on a $(p-1)! \equiv -1 \pmod{p}$.*

Maintenant $p \geq 3$ un premier, nécessairement impair (pourquoi ?), et soit $a \not\equiv 0 \pmod{p}$. Selon le théorème 6.6 on a $\left(a^{\frac{p-1}{2}}\right)^2 \equiv a^{p-1} \equiv 1 \equiv 1^2 \pmod{p}$, et donc selon le corollaire 6.3 on a $a^{\frac{p-1}{2}} \equiv 1$ ou $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. A quoi ces deux cas correspondent-ils ?

Or si $a \not\equiv 0$ est un carré modulo p, c'est-à-dire s'il existe $b \not\equiv 0$ avec $b^2 \equiv a \pmod{p}$, alors on a

$$a^{\frac{p-1}{2}} \equiv \left(b^2\right)^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \pmod{p}$$

par le théorème 6.6.

Mais que se passe-t-il si a n'est pas un carré modulo p ?

Donc fixons un $a \not\equiv 0 \pmod{p}$ qui n'est pas un carré modulo p. On va raisonner comme dans la démonstration du théorème de Wilson. Par le théoréme 6.4, pour chaque $x \not\equiv 0 \pmod{p}$ il existe un $y \not\equiv 0$ avec $xy \equiv a \pmod{p}$ et cet y est unique modulo p. Donc associé à chaque $x \in \{1, 2, \ldots, p-1\}$ est un unique $y \in \{1, 2, \ldots, p-1\}$ avec $xy \equiv a \pmod{p}$, et si y est associé à x, alors x est associé à y. Donc on peut encore diviser $\{1, 2, \ldots, p-1\}$ en une réunion disjointe de sous-ensembles $\{x_i, y_i\}$ de nombres avec $x_i y_i \equiv a \pmod{p}$. Ces sous-ensembles sont de cardinal 2 sauf quand on a un x_i qui est associé à lui-même, ce qui correspond à $x_i x_i \equiv x_i^2 \equiv a \pmod{p}$. Aucun tel x_i auto-associé n'existe sous nos hypothèses, car on a

supposé a non carré modulo p. Donc tous les sous-ensembles $\{x_i, y_i\}$ de $\{1, 2, \ldots, p-1\}$ sont de cardinal 2, et il y a $\frac{p-1}{2}$ tels sous-ensembles. On trouve donc

$$\begin{aligned} -1 \equiv (p-1)! &= (x_1 \cdot y_1) \cdot (x_2 \cdot y_2) \cdot (x_3 \cdot y_3) \cdots (x_{\frac{p-1}{2}} \cdot y_{\frac{p-1}{2}}) \\ &\equiv a \cdot a \cdot a \cdots a \qquad \left(\tfrac{p-1}{2} \text{ fois}\right) \qquad \pmod p \\ &\equiv a^{\frac{p-1}{2}}. \end{aligned}$$

Conclusion :

Théorème 6.7. *Soit $p \geq 3$ premier, et $a \not\equiv 0 \pmod p$. Alors on a*

$$a^{\frac{p-1}{2}} \equiv \begin{cases} 1 \pmod p & \text{si } a \text{ est un carré modulo } p, \\ -1 \pmod p & \text{si } a \text{ n'est pas un carré modulo } p, \end{cases}$$

La conséquence de ce théorème que nous utiliserons dans ce cours est le théorème suivant.

Théorème 6.8. *Soit p un premier.*
(a) -1 *est un carré modulo p si et seulement si p est de la forme $p = 2$ ou $p = 4k + 1$.*
(b) -1 *n'est pas un carré modulo p si et seulement si p et de la forme $p = 4k + 3$.*

Donc -1 est un carré modulo p pour $p = 2$, 5, 13, 17, 29, 37, 41, 53, 57, ... et n'est pas un carré modulo p pour $p = 3$, 7, 11, 19, 23, 31, 43, 47, 59, ...

Preuve. Montrons d'abord les implications

$$\begin{aligned} p = 2 \text{ ou } p = 4k+1 &\implies -1 \text{ est un carré modulo } p, \\ p = 4k+3 &\implies -1 \text{ n'est pas un carré modulo } p, \end{aligned}$$

Pour $p = 2$ on a $-1 \equiv 1 \equiv 1^2 \pmod 2$. Pour $p \geq 3$ on applique le théorème 6.7. Pour $p = 4k+1$ on a $(-1)^{\frac{p-1}{2}} \equiv (-1)^{2k} \equiv 1 \pmod p$, donc -1 est un carré modulo p pour $p = 4k + 1$. Pour $p = 4k + 3$, on a $(-1)^{\frac{p-1}{2}} \equiv (-1)^{2k+1} \equiv -1 \pmod p$, donc -1 n'est pas un carré modulo p pour $p = 4k + 3$.

Maintenant les contraposées des deux implications ci-dessus donnent les implications inverses.

$$\begin{aligned} p = 4k+3 &\impliedby p \neq 2 \text{ et } p \neq 4k+1 &&\impliedby -1 \text{ n'est pas un carré modulo } p, \\ p = 2 \text{ ou } p = 4k+1 &\impliedby p \neq 4k+3 &&\impliedby -1 \text{ est un carré modulo } p. \end{aligned}$$

□

Références

[1] M. Demazure. *Cours d'algèbre : Primalité. Divisibilité. Codes.* Nouvelle Bibliothèque Mathématique, 1. Cassini, Paris, 1997.

[2] G. Hardy and E. Wright. *Introduction à la théorie des nombres.* Paris : Vuibert ; Paris : Springer., 2007. Traduit de l'anglais par François Sauvageot.

[3] A. Y. Khinchin. *Continued fractions.* Dover Publications Inc., Mineola, NY, 1997. Traduit du russe. Réédition de la traduction américaine de 1964 [University of Chicago Press, Chicago].

[4] D. E. Knuth. *The Art of Computer Programming. Vol. 2 : Seminumerical Algorithms.* Boston : Addison-Wesley, 3rd edition, 1998.

[5] H. W. Lenstra, Jr. Solving the Pell equation. *Notices Amer. Math. Soc.*, 49(2) :182–192, 2002.

[6] W. J. LeVeque. *Topics in number theory. Vol. I, II.* Dover Publications Inc., Mineola, NY, 2002. Reprint of the 1956 original [Addison-Wesley Publishing Co., Inc., Reading, Mass.].

[7] I. Niven. *Irrational numbers*. The Carus Mathematical Monographs, No. 11. The Mathematical Association of America. Distributed by John Wiley and Sons, Inc., New York, N.Y., 1956.

[8] I. Niven and H. S. Zuckerman. *An introduction to the theory of numbers*. John Wiley & Sons, New York-Chichester-Brisbane, 4th edition, 1980.

[9] A. Weil. *Number theory for beginners*. Springer-Verlag, New York, 1979. Avec la collaboration de Maxwell Rosenlicht.