$\mathbb{Z}/n\mathbb{Z}$

1 Congruences

1.1 Définition

$\exists k \in \mathbb{Z}$ t.q. $b = a + kn$

Définition. Soit $n \in \mathbb{N}^*$. Pour $a, b \in \mathbb{Z}$, on dit que a **est congru à** b **modulo** n si et seulement si $n \mid b - a$. On note $a \equiv b\ [n]$ ou parfois $a \equiv b \bmod n$.

Proposition. La relation de congruence modulo n est un relation d'équivalence sur $\mathbb{Z}$.

1.2 Compatibilité avec les lois

Proposition. Soit $n \in \mathbb{N}^*$, $a, b, c, d \in \mathbb{Z}$. On a alors :

$$\left.\begin{array}{l} a \equiv b\ [n] \\ c \equiv d\ [n] \end{array}\right\} \implies a + c \equiv b + d\ [n]$$

$$\left.\begin{array}{l} a \equiv b\ [n] \\ c \equiv d\ [n] \end{array}\right\} \implies ac \equiv bd\ [n]$$

Corollaire. Si $a \equiv b\ [n]$, alors pour tout $k \in \mathbb{N}$, $a^k \equiv b^k\ [n]$.

Exemple. Justifier le critère de divisibilité par 3 : la somme des chiffres dans l'écriture en base 10 est divisible par 3.

2026

$2+0+2+6 = 10$

$10 = 1$

$3 \nmid 1$ donc $3 \nmid 2026$

Soit $n \in \mathbb{N}$. $\exists d, \exists a_0, \dots, a_d \in [\![0, 9]\!]$ t.q. $n = \sum_{k=0}^{d} a_k 10^k$

$10 \equiv 1\ [3]$ donc $\forall k$ $10^k \equiv 1^k\ [3]$

$$\text{donc } \forall k \quad a_k 10^k \equiv a_k \quad [3]$$

$$\text{donc} \quad n \equiv \sum_{k=0}^{d} a_k \quad [3]$$

$$\text{donc } 3 \mid n \iff n \mid \sum_{k=0}^{d} a_k$$

1.3 Le petit théorème de Fermat

Petit théorème de Fermat.

Soit p un nombre premier, a un entier non multiple de p. Alors :

$$a^{p-1} \equiv 1 \ [p]$$

Preuve : Montrons par récurrence sur $a \in \mathbb{N}$:

$$a^p \equiv a \ [p]$$

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

avec $p \mid \binom{p}{k} = \dfrac{p!}{k!(p-k)!} \in \mathbb{N}$

$$= p \cdot \frac{(p-1)!}{k!(p-k)!} \notin \mathbb{N}$$

- $k \binom{p}{k} = p \binom{p-1}{k-1}$ avec $k \in [\![1, p-1]\!]$

  $\binom{p}{k} \in \mathbb{N}$ et $\binom{p-1}{k-1} \in \mathbb{N}$

  k et p premiers entre eux et $p \mid k \binom{p}{k}$

  donc par le lemme de Gauss, $p \mid \binom{p}{k}$

- $0^p \equiv 0 \ [p]$

- Soit $a \in \mathbb{N}$, on suppose $a^p \equiv a \ [p]$

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

  $\equiv a + 1 + 0 \ [p]$

Ainsi $\forall a \in \mathbb{N}, \quad a^p \equiv a \ [p]$

Supposons maintenant que a n'est pas multiple de p.

$$a^p - a \equiv 0 \ [p]$$

ie $a(a^{p-1} - 1) \equiv 0 \ [p]$

donc $p \mid a(a^{p-1} - 1)$

or p premier, $a \notin p\mathbb{Z}$

donc $a \wedge p = 1$

donc par le lemme de Gauss

$$p \mid a^{p-1} - 1$$

ie $a^{p-1} \equiv 1 \ [p]$

---

2 L'anneau $\mathbb{Z}/n\mathbb{Z}$

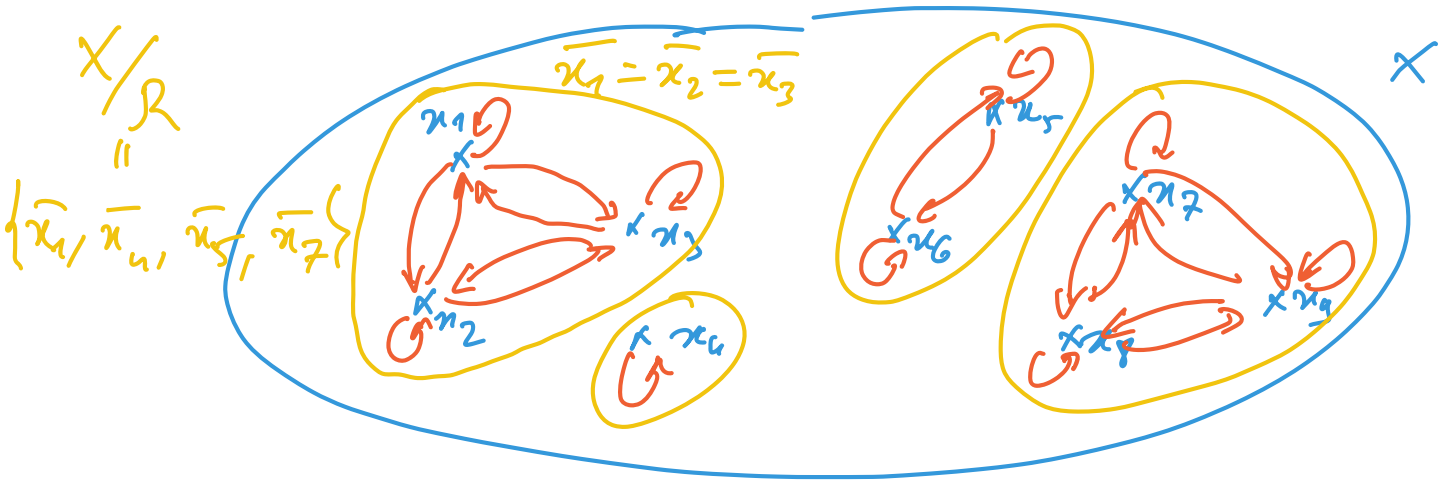
2.1 Complément : ensemble quotient

Définition. Soit X un ensemble et $\mathcal{R}$ une relation d'équivalence sur X. Pour $x \in X$, on appelle **classe d'équivalence de x pour la relation $\mathcal{R}$**, et on note $\overline{x}$, l'ensemble des éléments $y \in X$ tels que $y\mathcal{R}x$:

$$y \in \overline{x} \iff y\mathcal{R}x$$

Proposition. Si $y \in \overline{x}$, alors $\overline{y} = \overline{x}$. On dit que y **est un représentant de la classe d'équivalence** $\overline{x}$.

Proposition. Les classes d'équivalences pour $\mathcal{R}$ forment une partition de X : elles sont non vides, deux à deux disjointes et leur réunion est X.



2.2 L'ensemble $\mathbb{Z}/n\mathbb{Z}$

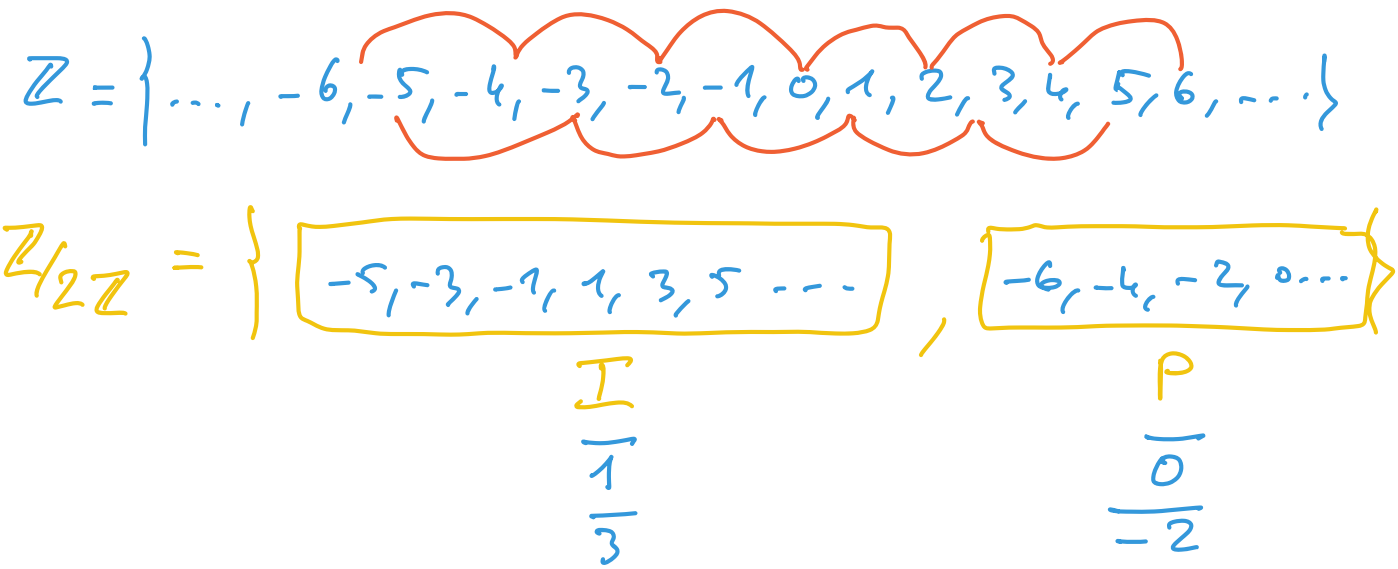
Définition. Soit $n \geqslant 2$. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble quotient de $\mathbb{Z}$ par la relation de congruence modulo n.

Exemple. Pour $n = 2$, on a :

$$\mathbb{Z}/2\mathbb{Z} = \{I, P\} = \{\overline{0}, \overline{1}\}$$

Proposition. Soit $n \geqslant 2$. L'ensemble $\mathbb{Z}/n\mathbb{Z}$ est un ensemble à n élément, que l'on peut décrire ainsi :

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$$



$$\mathbb{Z}/7\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$$
$$= \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{-3}, \overline{-2}, \overline{-1}\}$$

2.3 Structure d'anneau

Rappel. Pour $n \geqslant 2$, il existe une unique loi de groupe sur $\mathbb{Z}/n\mathbb{Z}$, encore notée $+$, pour laquelle l'application $k \mapsto \overline{k}$ soit un morphisme de groupes, i.e. :

$\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$

$$\forall a, b \in \mathbb{Z},\ \overline{a+b} = \overline{a} + \overline{b}$$

Remarque. *Si l'on considère $x, y \in \mathbb{Z}/n\mathbb{Z}$ et que l'on veut parler de $x+y$, on envisage donc $a, b \in \mathbb{Z}$ qui sont des représentants des classes d'équivalence x et y : $\overline{a} = x$ et $\overline{b} = y$. Alors :*

$$x + y = \overline{a+b}$$

Proposition. Pour $n \geqslant 2$, il existe une unique loi interne sur $\mathbb{Z}/n\mathbb{Z}$, notée $\times$, pour laquelle l'application :

$$\begin{array}{ccc} \mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ k & \mapsto & \overline{k} \end{array}$$

vérifie :

$$\forall a, b \in \mathbb{Z},\ \overline{a \times b} = \overline{a} \times \overline{b}$$

Alors $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif, dont l'unité est $\overline{1}$.

Exemple. Dresser la table d'addition de $\mathbb{Z}/5\mathbb{Z}$.
Dresser la table de multiplication de $\mathbb{Z}/5\mathbb{Z}$, de $\mathbb{Z}/6\mathbb{Z}$.

Remarque. *Notons bien que :*

$$\begin{array}{ccc} \mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ k & \mapsto & \overline{k} \end{array}$$

est un morphisme surjectif de l'anneau $(\mathbb{Z}, +, \times)$ sur l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.

• La loi $\times$ est ainsi bien définie

Soit $x, y \in \mathbb{Z}/n\mathbb{Z}$ $\quad x \times y = ?$

avec $a, b \in \mathbb{Z}$ tq $x = \overline{a}$ et $y = \overline{b}$

$x \times y = \overline{a \times b}$ par déf.

Le résultat est indép du choix des représentants de x et y

Soit $a_1, b_1 \in \mathbb{Z}$ tq $x = \overline{a_1}$ et $y = \overline{b_1}$

ie $a_1 \equiv a \ [n]$

$b_1 \equiv b \ [n]$

donc $a_1 \times b_1 \equiv a \times b \ [n]$

ie $\overline{a_1 \times b_1} = \overline{a \times b}$

- $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif.
- $\times$ est une loi de composition interne

associative

$$\begin{aligned}(\bar{a} \times \bar{b}) \times \bar{c} &= (\overline{a \times b}) \times \bar{c} && \times\ \mathbb{Z}/n\mathbb{Z} \\ &= \overline{(a \times b) \times c} && \times\ \mathbb{Z} \\ &= \overline{a \times (b \times c)} && \times \text{ associative} \\ &= \bar{a} \times \overline{(b \times c)} \\ &= \bar{a} \times (\bar{b} \times \bar{c})\end{aligned}$$

distributive sur $+$

[...]

admet un neutre $\bar{1}$

$$\begin{aligned}\bar{a} \times \bar{1} &= \overline{a \times 1} \\ &= \bar{a} && \text{car 1 neutre de } \times \text{ dans } \mathbb{Z}\end{aligned}$$

$\times$ est commutative

ıple. Dresser la table d'addition de $\mathbb{Z}/5\mathbb{Z}$.
Dresser la table de multiplication de $\mathbb{Z}/5\mathbb{Z}$, de $\mathbb{Z}/6\mathbb{Z}$.

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$					
$\bar{1}$					
$\bar{2}$					$\bar{1}$
$\bar{3}$					
$\bar{4}$					

$\bar{2} + \bar{4} = \overline{2+4}$

$= \bar{1}$ car $6 \equiv 1$ [5]

×	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$		$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$			$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$				$\bar{4}$	$\bar{2}$
$\bar{4}$					$\bar{1}$

$\bar{2} \times \bar{4} = \overline{2 \times 4}$

$= \bar{8}$

$= \bar{3}$

Ce sont les carrés modulo 5

Résoudre : $a^2 = 3$ [5]

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$		$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	
$\bar{2}$			$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$				$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$					$\bar{4}$	$\bar{2}$
$\bar{5}$						$\bar{1}$

$\bar{2} \times \bar{3} = \bar{0}$

$\bar{2}$ et $\bar{3}$ sont des diviseurs de $\bar{0}$

Anneau non intègre

2.4 Calcul dans $\mathbb{Z}/n\mathbb{Z}$

Remarque. *On travaille dans $\mathbb{Z}/n\mathbb{Z}$, où $n \geqslant 2$.*
Pour $k, a \in \mathbb{Z}$, que représentent :

$$k\,\overline{a},\ \overline{ka} \text{ et } \overline{k}\,\overline{a}$$

Exemple. Est-ce que l'écriture suivante, dans l'anneau $\mathbb{Z}/17\mathbb{Z}$, a du sens ?

$$\overline{15} \times (\overline{3})^{-1} = \overline{5}$$

Remarque. *On évite de dire : « soit $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ », mais plutôt : « soit $x \in \mathbb{Z}/n\mathbb{Z}$ et a un représentant de x, c'est-à-dire tel que $x = \overline{a}$. »*
En particulier, si on définit :

$$f : \mathbb{Z}/n\mathbb{Z} \to \ldots$$

on peut vouloir écrire $\overline{a} \mapsto f(a)$, c'est-à-dire définir $f(x)$ en utilisant un représentant de x. Mais il faut bien justifier qu'alors, la définition est indépendante du choix du représentant :

$$\overline{a} = \overline{b} \implies f(a) = f(b)$$

$k = 7$

$7\overline{a} = \overline{a} + \overline{a} + \overline{a} + \overline{a} + \overline{a} + \overline{a} + \overline{a}$

$\overline{7a} = \overline{a+a+a+a+a+a+a}$ (=)

$\overline{7}\,\overline{a} = \overline{7 \times a}$ (=)

Exemple. Est-ce que l'écriture suivante, dans l'anneau $\mathbb{Z}/17\mathbb{Z}$, a du sens ?

$$\overline{15} \times (\overline{3})^{-1} = \overline{5}$$

$\overline{15} \times (\overline{3})^{-1} = \overline{(15 \times 3^{-1})}$ $\quad 3^{-1} \notin \mathbb{Z}$

$= \overline{5}$

$\overline{15} \times (\overline{3})^{-1}$

1ère question : est-ce que $\overline{3}$ est inversible

on cherche $x = \overline{a}$ tq $x \times \overline{3} = \overline{1}$

on remarque que $\overline{6}$ convient

donc $\overline{3}$ inversible et $(\overline{3})^{-1} = \overline{6}$

Alors :

$$\overline{15} \times (\overline{3})^{-1} = \overline{15} \times \overline{6}$$

$$= \overline{15 \times 6}$$

$$= \overline{90} \qquad 90 = 85 + 5$$

$$= \overline{5}$$

Exemple. Résoudre, dans $\mathbb{Z}/11\mathbb{Z}$, l'équation :

$$x^2 - \overline{6}x + \overline{5} = \overline{0}$$

Inconnue : $x \in \mathbb{Z}/11\mathbb{Z}$

poser : $x = \overline{a}$

$$x^2 - \overline{6}x + \overline{5} = (x - \overline{3})^2 - \overline{4}$$

x solution $\Leftrightarrow (x - \overline{3})^2 = \overline{4}$

Calculons les carrés dans $\mathbb{Z}/11\mathbb{Z}$:

$$\overline{0}^2 = \overline{0}$$

" $\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, -\overline{1}, -\overline{2}, -3, -\overline{4}, -5\}$

$$\overline{1}^2 = (-\overline{1})^2 = \overline{1}$$

$$\overline{2}^2 = (-\overline{2})^2 = \overline{4}$$

$$\overline{3}^2 = (-\overline{3})^2 = \overline{9}$$

$$\overline{4}^2 = (-\overline{4})^2 = \overline{5}$$

$$\overline{5}^2 = (-\overline{5})^2 = \overline{3}$$

x solution $\Leftrightarrow \begin{cases} x - \overline{3} = \overline{2} \\ \text{ou} \\ x - \overline{3} = -\overline{2} \end{cases}$

$\Leftrightarrow \begin{cases} x = \overline{5} \\ \text{ou} \\ x = \overline{1} \end{cases}$

Exemple. Résoudre, dans $\mathbb{Z}/31\mathbb{Z}$, l'équation :

$$x^2 - \overline{11}x - \overline{1} = \overline{0}$$

$-\overline{11} = \overline{20}$

x solution $\iff x^2 - \overline{11}\,x - \overline{1} = \overline{0}$

$\iff (x + \overline{10})^2 - \overline{101} = \overline{0}$

$\iff (x + \overline{10})^2 = \overline{8}$

Carrés dans $\mathbb{Z}/31\mathbb{Z}$:

$\overline{0}^2 = \overline{0}$

$(-\overline{1})^2 = \overline{1}^2 = \overline{1}$

$\overline{2}^2 = \overline{4}$

$\overline{3}^2 = \overline{9}$

$\overline{4}^2 = \overline{16}$

$\overline{5}^2 = \overline{25}$

$\overline{6}^2 = \overline{5}$

$\overline{7}^2 = \overline{18}$

$\overline{8}^2 = \overline{2}$

$\overline{9}^2 = \overline{19}$

$\overline{10}^2 = \overline{7}$

$\overline{11}^2 = -\overline{3} = \overline{28}$

$$\overline{12}^2 = \overline{20}$$

$$\overline{13}^2 = \overline{15}$$

$$\overline{14}^2 = \overline{196} = \overline{10}$$

$$(-\overline{15})^2 = \overline{15}^2 = \overline{225} = \overline{8}$$

Bref : x sol $\Leftrightarrow$ $\begin{cases} x + \overline{10} = \overline{15} \\ \text{ou} \\ x + \overline{10} = -\overline{15} \end{cases}$

$\Leftrightarrow$ $\begin{cases} x = \overline{5} \\ \text{ou} \\ x = -\overline{25} = \overline{6} \end{cases}$

Exemple. Discuter, suivant les valeurs de $a \in \mathbb{Z}/13\mathbb{Z}$, le nombre de solutions de l'équation :

$$x^2 + x + a = \overline{0}$$

x sol $\iff$ $x^2 - \overline{12}x + a = \overline{0}$

$\iff$ $(x - \overline{6})^2 = \overline{10} - a$

on cherche les carrés dans $\mathbb{Z}/13\mathbb{Z}$

et les valeurs de a tq $\overline{10} - a$ soit un carré.

$\overline{0}^2 = \overline{0}$

$(-\overline{1})^2 = \overline{1}^2 = \overline{1}$

$(-\overline{2})^2 = \overline{2}^2 = \overline{4}$

$(-\overline{3})^2 = \overline{3}^2 = \overline{9}$

$(-\overline{4})^2 = \overline{4}^2 = \overline{3}$

$(-\overline{5})^2 = \overline{5}^2 = -\overline{1} = \overline{12}$

$(-\overline{6})^2 = \overline{6}^2 = \overline{10}$

Donc : • Si $\overline{10} - a = \overline{0}$ ie $a = \overline{10}$

alors unique solution $x = \overline{6}$

• Si $\overline{10} - a = \overline{1}, \overline{4}, \overline{9}, \overline{3}, \overline{12}, \overline{10}$

alors 2 solutions

• Sinon :

pas de solutions

Remarque :

ex 2 : Dans $\mathbb{Z}/3\mathbb{Z}$

$$(x+\bar{10})^2 = \bar{8} = (\bar{15})^2$$

$$\Leftrightarrow (x+\bar{10}+\bar{15})(x+\bar{10}-\bar{15}) = \bar{0}$$

$$\Leftrightarrow (x+\bar{25})(x-\bar{5}) = \bar{0}$$

$$\Rightarrow x = -\bar{25} \quad \text{ou} \quad x = \bar{5}$$

nécessite l'intégrité de $\mathbb{Z}/3\mathbb{Z}$

Proposition. Pour p premier, calculer $\mathrm{Card}(A)$ où :

$$A = \left\{ x^2,\ x \in \left(\mathbb{Z}/p\mathbb{Z}\right)^* \right\}$$

3 Inversibles de $\mathbb{Z}/n\mathbb{Z}$

Théorème.

Soit n entier, $n \geqslant 2$. Les éléments inversibles de $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ sont les classes $\overline{k}$ où $k \in \{0, \dots, n-1\}$ est premier avec n.

Remarque. *Ce sont les générateurs du groupe cyclique* $(\mathbb{Z}/n\mathbb{Z}, +)$.

Preuve :

⇐ Soit $k \in \{0, \dots, n-1\}$ tq $k \wedge n = 1$

Par lettre de Bézout

$\exists u, v \in \mathbb{Z}$ tq $ku + vn = 1$

donc $ku \equiv 1 \ [n]$

ie $\overline{k}\,\overline{u} = \overline{1}$ dans $\mathbb{Z}/n\mathbb{Z}$

Donc $\overline{k}$ est inversible (d'inverse $\overline{u}$)

Remarque : calcul d'inverse dans $\mathbb{Z}/n\mathbb{Z}$

⟶ Bézout. (Gauss)

⇒ Soit $k \in \{0, \dots, n-1\}$ tq $\overline{k}$ inversible.

donc $\exists u \in \mathbb{Z}$ tq $\overline{k}\,\overline{u} = \overline{1}$

donc $ku \equiv 1 \ [n]$

ie $\exists v \in \mathbb{Z}$ tq $ku = 1 - nv$

Bref $ku + nv = 1$

Bézout ⟶ $k \wedge n = 1$

Notation : On note $(\mathbb{Z}/n\mathbb{Z})^*$ l'ensemble des inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

Remarque : on trouve aussi les notations $(\mathbb{Z}/n\mathbb{Z})^\times$ $\mathcal{U}(\mathbb{Z}/n\mathbb{Z})$

Attention : $(\mathbb{Z}/n\mathbb{Z})^* \neq \mathbb{Z}/n\mathbb{Z} \setminus \{\bar{0}\}$

$\mathbb{Z}^* = \{-1, 1\}$

$\mathbb{Z} \setminus \{0\} = \{-7, -6, \dots, -1, 1, 2, 3, \dots\}$

Définition. On note $\varphi(n)$ le nombre d'inversibles de $(\mathbb{Z}/n\mathbb{Z}, +, \times)$:

$$\varphi(n) = \text{Card}\left(\{k \in \{0, \dots, n-1\},\ k \wedge n = 1\}\right)$$

φ s'appelle **l'indicatrice d'Euler**.

Remarque. *On convient que* $\varphi(1) = 1$.

$\varphi(n) = \text{Card}\left((\mathbb{Z}/n\mathbb{Z})^*\right)$

Théorème.

Les trois propriétés suivantes sont équivalentes :

(*i*) $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps ;

(*ii*) $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau intègre ;

(*iii*) n est premier.

Notation. Pour p nombre premier, on note $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$.

Preuve :

(i) ⇒ (ii) Tout corps est un anneau intègre

(iii) ⇒ (i) On suppose n premier

Rappel : un corps est un anneau commutatif où tout élément non nul est inversible.

Soit $x \in \mathbb{Z}/n\mathbb{Z}$, $x \neq \overline{0}$

Il existe $a \in \{1, \dots, n-1\}$ tq $x = \overline{a}$

Comme n premier,

$$n \wedge a = 1$$

donc par le th précédent, $\overline{a}$ est inversible

dans $\mathbb{Z}/n\mathbb{Z}$ ie x est inversible.

(ii) ⇒ (iii) par contraposée.

On suppose $n = pq$ où $p, q \geq 2$

Alors $\overline{p} \times \overline{q} = \overline{pq} = \overline{0}$

avec $2 \leq p, q \leq n-1$ donc $\overline{p} \neq \overline{0}$, $\overline{q} \neq \overline{0}$

Donc $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre.

Théorème d'Euler.

Soit $n \geqslant 2$. Si $a \wedge n = 1$, alors $a^{\varphi(n)} \equiv 1\ [n]$.

Remarque. *Lorsque n est premier, on reconnaît le petit théorème de Fermat.*

Si n premier, $(\mathbb{Z}/n\mathbb{Z})^* = \mathbb{Z}/n\mathbb{Z} \setminus \{\bar{0}\}$

car $\mathbb{Z}/n\mathbb{Z}$ est un corps

donc $\varphi(n) = n-1$

donc $a^{n-1} \equiv 1\ [n]$

Th d'Euler :

a, n tq $a \wedge n = 1$.

$\bar{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$

donc $x \longmapsto \bar{a}\,x$ permutation de $(\mathbb{Z}/n\mathbb{Z})^*$

$$\overline{\prod_{x \in (\mathbb{Z}/n\mathbb{Z})^*} x} = \overline{\prod_{x \in (\mathbb{Z}/n\mathbb{Z})^*} \bar{a}\,x}$$

$$= \bar{a}^{\operatorname{Card}(\mathbb{Z}/n\mathbb{Z})^*} \overline{\prod_{x \in (\mathbb{Z}/n\mathbb{Z})^*} x}$$

$$= \bar{a}^{\varphi(n)} \overline{\prod_{x \in (\mathbb{Z}/n\mathbb{Z})^*} x}$$

Comme $\overline{\prod_{x \in (\mathbb{Z}/n\mathbb{Z})^*} x}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$

il reste $\overline{1} = \bar{a}^{\varphi(n)}$

Résultat en passant

Soit $(A, +, \times)$ un anneau fini commutatif.

Mque A est un corps $\Leftrightarrow$ A est intègre

$\Rightarrow$ toujours vrai

$\Leftarrow$ Soit $a \in A$, $a \neq 0$

On cherche $x \in A$ tq $ax = 1$

On note $u : A \longrightarrow A$

$$x \longmapsto ax$$

- u est un morphisme de groupes

$$u(x+y) = a(x+y)$$

$$= ax + ay$$

$$= u(x) + u(y)$$

• $x \in \ker(u) \iff ax = 0$

$\iff x = 0$ car $a \neq 0$ et A intègre

donc u injectif, de $A \to A$ avec A fini, donc u bijectif

donc u surjectif.

Donc $\exists x \in A$ tq $u(x) = 1$

ie $ax = 1$

Donc a est inversible, d'inverse x.

4 Le théorème chinois

4.1 Présentation du problème chinois

Exemple.

1. Déterminer une relation de Bézout entre 14 et 25.
2. Déterminer x_1 et x_2 dans $\mathbb{Z}$ tels que :

$$\begin{cases} x_1 \equiv 1\ [14] \\ x_1 \equiv 0\ [25] \end{cases} \quad \text{et} \quad \begin{cases} x_2 \equiv 0\ [14] \\ x_2 \equiv 1\ [25] \end{cases}$$

3. Utiliser x_1 et x_2 pour déterminer une solution du système :

$$\begin{cases} x \equiv 2\ [14] \\ x \equiv 3\ [25] \end{cases}$$

4. Déterminer toutes les solutions du système précédent.

Remarque. *Pourquoi le système :*

$$\begin{cases} x \equiv 2\ [26] \\ x \equiv 3\ [38] \end{cases}$$

n'a pas de solution ?

$25 = 1 \times 14 + 11$

$14 = 1 \times 11 + 3$

$11 = 3 \times 3 + 2$

$3 = 1 \times 2 + 1$

$1 = 3 - 1 \times 2$

$= 3 - 1 \times (11 - 3 \times 3)$

$= -11 + 4 \times 3$

$= -11 + 4 (14 - 11)$

$= 4 \times 14 - 5 \times 11$

$= 4 \times 14 - 5(25 - 14)$

$= -5 \times 25 + 9 \times 14$

Donc $\underline{1 = -5 \times 25 + 9 \times 14}$

2. Déterminer x_1 et x_2 dans $\mathbb{Z}$ tels que :

$$\begin{cases} x_1 \equiv 1\ [14] \\ x_1 \equiv 0\ [25] \end{cases} \quad \text{et} \quad \begin{cases} x_2 \equiv 0\ [14] \\ x_2 \equiv 1\ [25] \end{cases}$$

3. Utiliser x_1 et x_2 pour déterminer une solution du système :

$$\begin{cases} x \equiv 2\ [14] \\ x \equiv 3\ [25] \end{cases}$$

4. Déterminer toutes les solutions du système précédent.

(2) $1 \equiv -5 \times 25 + 9 \times 14 \quad [14]$

donc $x_1 = -5 \times 25$ convient

$= -125$

De même $x_2 = 9 \times 14$ convient

$= 126$

(3) $x_0 = 2x_1 + 3x_2$ convient.

$= -2 \cdot 125 + 3 \cdot 126$

$= 128$

(4) x sol $\iff \begin{cases} x \equiv 2\ [14] \\ x \equiv 3\ [25] \end{cases}$

$$\Leftrightarrow \begin{cases} x \equiv x_0 \ [14] \\ x \equiv x_0 \ [25] \end{cases}$$

$$\Leftarrow \begin{cases} x - 128 \equiv 0 \ [14] \\ x - 128 \equiv 0 \ [25] \end{cases}$$

$$\Leftrightarrow \begin{cases} 14 \mid x - 128 \\ 25 \mid x - 128 \end{cases}$$

$14 \wedge 25 = 1$

$$\Leftarrow 14 \times 25 \mid x - 128$$

$$\Leftrightarrow \exists k \in \mathbb{Z} \text{ tq}$$

$$x = 128 + k\,350$$

Remarque :

$$1 = -5 \times 25 + 9 \times 14$$

donc :

$$(\overline{25})^{-1} = (\overline{-5}) \quad \text{dans } \mathbb{Z}/14\mathbb{Z}$$

et $(\overline{14})^{-1} = \overline{9}$ dans $\mathbb{Z}/25\mathbb{Z}$

On peut noter $\overline{25} = (25 \bmod 14)$

$$= [25]_{14}$$

La sol particulière est

$$x_0 = 2 \times 9 \times 14 + 3 \times -5 \times 25$$

↑ inverse de $\overline{14}$ dans $\mathbb{Z}/25\mathbb{Z}$

↑ inverse de $\overline{25}$ dans $\mathbb{Z}/14\mathbb{Z}$

Dans $\mathbb{Z}/25\mathbb{Z}$

$$\overline{x_0} = \overline{2} \times \overline{1} + \overline{0}$$

Dans $\mathbb{Z}/14\mathbb{Z}$

$$\overline{x_0} = \overline{0} + \overline{3} \times \overline{1}$$

4.2 Structure d'anneau produit

Définition. Soit $(A, +, *)$ et $(B, +, \star)$ deux anneaux. On définit **l'anneau produit** en munissant le produit cartésien $A \times B$ des lois :

$$(a, b) + (a', b') = (a + a', b + b')$$
$$(a, b) \times (a', b') = (a * a', b \star b')$$

Proposition. Muni de cette structure, $A \times B$ est un anneau.

Remarque. *On peut étendre cette définition et cette proposition au cas d'un nombre fini d'anneaux.*

4.3 À propos de la notation

Remarque. *Pour $a \in \mathbb{Z}$, on note $\overline{a}$ l'élément de $\mathbb{Z}/n\mathbb{Z}$ qui est la classe de a. Mais si on travaille à la fois dans $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z}$, la notation devient ambiguë.*

Notation. Pour $n \geqslant 2$ et $a \in \mathbb{Z}$, on note :

$$(a \bmod n) \text{ ou } [a]_n$$

la classe de a modulo n, que l'on note aussi $\overline{a}$ lorsqu'il n'y a pas d'ambiguité.

Exemple. Préciser le diagramme de l'application :

$$\phi \,:\, a \mapsto (a \bmod 14, a \bmod 25)$$

Est-ce un morphisme d'anneaux ?
Quel est son noyau ?

4.4 Le théorème chinois

Théorème chinois.

Soit m, n entiers $\geqslant 2$, premiers entre eux. Alors l'application :

$$\begin{array}{rccc} u: & \mathbb{Z}/mn\mathbb{Z} & \to & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ & a \bmod mn & \mapsto & (a \bmod m, a \bmod n) \end{array}$$

est correctement définie, et est un isomorphisme d'anneaux.

Remarque. *Si l'on dispose d'une relation de Bézout :*

$$mu + nv = 1$$

l'isomorphisme réciproque est :

$$(a \bmod m, b \bmod n) \mapsto (anv + bmu \bmod mn)$$

Preuve :

- Mque u est bien définie

Soit $x \in \mathbb{Z}/mn\mathbb{Z}$

$a \in \mathbb{Z}$ tq $x = \overline{a}^{mn} = [a]_{mn}$

On a posé $u(x) = (\overline{a}^{m}, \overline{a}^{n})$

$= ([a]_m, [a]_n)$

Soit $b \in \mathbb{Z}$ tq $x = [b]_{mn}$

$[a]_{mn} = [b]_{mn}$

donc $mn \mid b-a$

donc $m \mid b-a$ et $n \mid b-a$

donc $[a]_m = [b]_m$ et $[a]_n = [b]_n$

donc l'expression de $u(x)$ est indépendante

du choix du représentant x

• u est un morphisme d'anneaux.

$$u(x+y) = u(x) + u(y)$$

$$u(x \times y) = u(x) \times u(y)$$

$$u(1) = 1$$

$x \in \mathbb{Z}/mn\mathbb{Z}$, $x = [a]_{mn}$

$y \in \mathbb{Z}/mn\mathbb{Z}$, $y = [b]_{mn}$

$$x \times y = [ab]_{mn}$$

$$u(x \times y) = \left([ab]_m, [ab]_n \right)$$

$$= \left([a]_m \times [b]_m, [a]_n \times [b]_n \right)$$

$$= \left([a]_m, [a]_n \right) \times \left([b]_m, [b]_n \right)$$

par déf de l'anneau produit

$$= u(x) \times u(y)$$

• injectif.

Soit $x \in \mathbb{Z}/mn\mathbb{Z}$, $a \in \mathbb{Z}$ tq $x = [a]_{mn}$

$x \in \ker u \iff u(x) = 0$

$\iff \left([a]_m, [a]_n \right) = (\bar{0}, \bar{0})$

$\iff \begin{cases} a \equiv 0 \quad [m] \\ a \equiv 0 \quad [n] \end{cases}$

$\iff \begin{cases} m \mid a \\ n \mid a \end{cases}$

$\Leftrightarrow \quad mn \mid a \quad$ car $m \wedge n = 1$

$\Leftrightarrow \quad [a]_{mn} = \overline{0}$

$\Leftarrow \quad x = \overline{0}$

Donc $\ker u = \{\overline{0}\}$

ie u est injectif

- $\text{Card } \mathbb{Z}/mn\mathbb{Z} = mn$

$$\text{Card}\left(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}\right) = \text{Card } \mathbb{Z}/m\mathbb{Z} \times \text{Card } \mathbb{Z}/n\mathbb{Z} = m \times n$$

Donc u est un isomorphisme d'anneaux.

Corollaire. Soit m, n entiers $\geqslant 2$, premiers entre eux. Alors le système de congruences :

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

admet au moins une solution $x_0 \in \mathbb{Z}$.
L'ensemble des solutions est $x_0 + mn\mathbb{Z}$.

Preuve : x sol $\Leftrightarrow \begin{cases} [x]_m = [a]_m \\ [x]_n = [b]_n \end{cases}$

$\Leftrightarrow \quad u([x]_{mn}) = ([a]_m, [b]_n)$

$\Leftrightarrow \quad [x]_{mn} = u^{-1}([a]_m, [b]_n)$

unique solution dans $\mathbb{Z}/mn\mathbb{Z}$

Les solutions "entières" sont donc définies modulo mn.

Allons plus loin ! Exprimons x_0.

$m \wedge n = 1$

dans $\mathbb{Z}/m\mathbb{Z}$, $\overline{n}$ ($= [n]_m$) est inversible.

on note $\overline{v}$ ($= [v]_m$) son inverse

De même, dans $\mathbb{Z}/n\mathbb{Z}$ $\overline{m}$ ($= [m]_n$) inversible,

on note $\overline{u}$ ($= [u]_n$) son inverse

On pose $x_0 = a\,v\,n + b\,u\,m$

donc $[x_0]_m = [a]_m \times \underbrace{[v]_m [n]_m}_{1}$

i.e. $x_0 \equiv a \ [m]$

de même $x_0 \equiv b \ [n]$

Bref : Pour expliciter x_0, on cherche un inverse à $\overline{m}$ dans $\mathbb{Z}/n\mathbb{Z}$ et à $\overline{n}$ dans $\mathbb{Z}/m\mathbb{Z}$ par l'identité de Bézout.

Généralisation. Soit $n_1, \ldots, n_k$ entiers $\geqslant 2$, deux à deux premiers entre eux, alors :

$$\begin{array}{rcl} \mathbb{Z}/(n_1 \ldots n_k)\mathbb{Z} & \to & \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z} \\ a \bmod n_1 \ldots n_k & \mapsto & (a \bmod n_1, \ldots, a \bmod n_k) \end{array}$$

est correctement définie, et est un isomorphisme d'anneaux.

Exemple. Résoudre le système de congruences :

$$\begin{cases} n \equiv 4 \ [5] \\ n \equiv 1 \ [7] \end{cases}$$

$$\begin{cases} x \equiv 3 \quad [17] & m_1 = 17 \\ x \equiv 4 \quad [11] & m_2 = 11 \\ x \equiv 5 \quad [6] & m_3 = 6 \end{cases}$$

m_1, m_2, m_3 deux à deux premiers entre eux.

On pose $N = m_1 m_2 m_3 = 17 \times 11 \times 6$

$= 187 \times 6$

$= 1122$

et $x_0 = 3 \times \underbrace{11 \times 6 \times y_1}_{\substack{1 \bmod 17 \\ 0 \bmod 11 \\ 0 \bmod 6}} + 4 \times \underbrace{17 \times 6 \times y_2}_{\substack{0 \bmod 17 \\ 1 \bmod 11 \\ 0 \bmod 6}} + 5 \times \underbrace{17 \times 11 \times y_3}_{\substack{0 \bmod 17 \\ 0 \bmod 11 \\ 1 \bmod 6}}$

$[y_1]_{17} = [11 \times 6]_{17}^{-1} = [\cdots] = 8$

$[y_2]_{11} = [17 \times 6]_{11}^{-1} = [\cdots] = 4$

$[y_3]_6 = [17 \times 11]_6^{-1} = [\cdots] = 1$

(Bézout 3 fois)

donc $x_0 = 3 \times 11 \times 6 \times 8$

$+ 4 \times 17 \times 6 \times 4$

$+ 5 \times 17 \times 11 \times 1 = 785$

Or par le th chinois

$$u : \mathbb{Z}/1122\mathbb{Z} \longrightarrow \mathbb{Z}/17\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$$
$$[a]_{1122} \longmapsto ([a]_{17}, [a]_{11}, [a]_6)$$

est un isomorphisme d'anneaux

$$u^{-1}([3]_{17}, [4]_{11}, [5]_6)$$
$$= [785]_{1122}$$

donc $\exists k \in \mathbb{Z}$ tq $x = 785 + k\,1122$

5 Indicatrice d'Euler

Rappel. Pour $n \geqslant 2$, $\varphi(n)$ désigne le nombre d'inversibles de $(\mathbb{Z}/n\mathbb{Z}, +, \times)$, ou encore le nombre d'entiers premiers avec n parmi $\{0, \dots, n-1\}$, ou encore le nombre de générateurs du groupe cyclique $(\mathbb{Z}/n\mathbb{Z}, +)$.

Théorème d'Euler. Soit n entier, $n \geqslant 2$ et $a \in \mathbb{Z}$. Si a est premier avec n, alors $a^{\varphi(n)} \equiv 1\ [n]$.

Corollaire (petit théorème de Fermat). Soit p un nombre premier. Pour tout a non multiple de p, $a^{p-1} \equiv 1\ [p]$.

Théorème.

Soit $m, n \in \mathbb{N}^*$. Si m et n sont premiers entre eux, alors :

$$\varphi(mn) = \varphi(m)\varphi(n)$$

Preuve.

Par le théorème chinois :

$$\text{ie : } \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

est un isomorphisme d'anneaux donc

$$\text{ie } \left(\left(\mathbb{Z}/mn\mathbb{Z}\right)^*\right) = \left(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}\right)^*$$
$$= \left(\mathbb{Z}/mn\mathbb{Z}\right)^* \times \left(\mathbb{Z}/n\mathbb{Z}\right)^*$$

et $\operatorname{Card}\left(\mathbb{Z}/mn\mathbb{Z}\right)^* = \operatorname{Card}\left(\mathbb{Z}/m\mathbb{Z}\right)^* \times \operatorname{Card}\left(\mathbb{Z}/n\mathbb{Z}\right)^*$

ie $\varphi(mn) = \varphi(m)\varphi(n)$

On retient : φ est "multiplicative" sous l'hypothèse $m \wedge n = 1$

Proposition. Si p est premier et $k \in \mathbb{N}^*$, alors :

$$\varphi(p^k) = p^k - p^{k-1}$$

Preuve :

$\varphi(p^k)$ = nb d'inversibles de $\mathbb{Z}/p^k\mathbb{Z}$

Soit $x \in \mathbb{Z}/p^k\mathbb{Z}$

$a \in \{1, \dots, p^k\}$ tq $x = \overline{a}$

x non inversible dans $\mathbb{Z}/p^k\mathbb{Z}$

$\iff a \wedge p^k \neq 1$

$\iff p \mid a$ car p premier

$\iff a = p$ ou $2p$ ou $\dots$ $p^{k-1} \cdot p$

Donc il y a p^{k-1} non inversibles dans $\mathbb{Z}/p^k\mathbb{Z}$

Donc $\varphi(p^k) = p^k - p^{k-1}$

Théorème.

Soit $n \geqslant 2$ un entier. On a :

$$\varphi(n) = n \prod_{\substack{p \text{ premier} \\ p|n}} \left(1 - \frac{1}{p}\right)$$

Exemple. Calculer $\varphi(36)$.

Preuve : On écrit

$$n = \prod_{i=1}^{d} p_i^{k_i}$$

où $p_1, \dots, p_d$ sont des nb premiers distincts

$k_1, \dots, k_d$ sont des entiers ≥ 1

$$\varphi(n) = \varphi\left(\prod_{i=1}^{d} p_i^{k_i}\right)$$

$$= \prod_{i=1}^{d} \varphi\left(p_i^{k_i}\right)$$

car les $p_i^{k_i}$ sont 2 à 2 premiers entre eux

$$= \prod_{i=1}^{d} \left(p_i^{k_i} - p_i^{k_i - 1}\right)$$

$$= \prod_{i=1}^{d} p_i^{k_i} \times \prod_{i=1}^{d} \left(1 - \frac{1}{p_i}\right)$$

$$= n \prod_{\substack{p \mid n \\ p \text{ premier}}} \left(1 - \frac{1}{p}\right)$$

$\varphi(36)$: calculer par 2 méthodes.

M1 $36 = 2^2 \times 3^2$

donc $\varphi(36) = 36 \times \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)$

$= 6 \times (1)(2)$

$= 12$

M2 $\varphi(36) = \varphi(9 \times 4)$

$= \varphi(9)\varphi(4)$ $\quad 9 \wedge 4 = 1$

$= \varphi(3^2)\varphi(2^2)$

$= (9-3)(4-2)$

$= 12$

M3 $\bar{0}$ $\bar{1}$ $\bar{2}$ $\bar{3}$ $\bar{4}$ ---

$\bar{a}$ inversible $\iff a \wedge 36 = 1$

$(\mathbb{Z}/36\mathbb{Z})^* = \{\bar{1}, \bar{5}, \bar{7}, \bar{11}, \bar{13}, \bar{17}, \bar{19}, \bar{23}, \bar{25}, \bar{29}, \bar{31}, \bar{35}\}$