Arithmétique dans l'anneau $(\mathbb{Z}, +, \cdot)$

Aperçu

1. Divisibilité et division euclidienne
2. Les nombres premiers
3. Plus grand commun diviseur, algorithme d'Euclide
4. Décomposition en facteurs premiers
5. La relation de congruence

1. Divisibilité et division euclidienne
1.1 La relation « divise » dans $\mathbb{Z}$
1.2 Compatibilité avec les opérations algébriques
1.3 Division euclidienne

2. Les nombres premiers

3. Plus grand commun diviseur, algorithme d'Euclide

4. Décomposition en facteurs premiers

5. La relation de congruence

1. Divisibilité et division euclidienne
1.1 La relation « divise » dans $\mathbb{Z}$
1.2 Compatibilité avec les opérations algébriques
1.3 Division euclidienne

2. Les nombres premiers

3. Plus grand commun diviseur, algorithme d'Euclide

4. Décomposition en facteurs premiers

5. La relation de congruence

D 1 Soit $(a, b) \in \mathbb{Z}^2$. On dit que a **divise** b, et l'on note $a \mid b$ lorsqu'il existe $q \in \mathbb{Z}$ tel que $b = aq$.
Dans ce cas, on dit aussi que a est un **diviseur** de b ou que b est un **multiple** de a.

N

- On note par $a\mathbb{Z} = \{ aq \mid q \in \mathbb{Z} \}$ l'ensemble des multiples de a.
- On note $D(b) = \left\{ a \in \mathbb{N} \,\middle|\, a \mid b \right\}$ l'ensemble des diviseurs positifs de b.

E 2

1. $5 \mid 210$, $3 \mid 18$.
2. $D(6) = \{ 1, 2, 3, 6 \}$.
3. $4\mathbb{Z} = \{ \dots, -16, -12, -8, -4, 0, 4, 8, 12, 16, \dots \}$.
4. 0 est divisible par n'importe quel entier et le seul entier divisible par 0 est 0.
$$\forall a \in \mathbb{Z}, a \mid 0 \text{ et } \Big(0 \mid a \iff a = 0\Big).$$
5. Le seul diviseurs de 1 est 1, mais 1 divise tout entier relatif.
$$\forall b \in \mathbb{Z}, 1 \mid b.$$

P 3 **Lien avec la relation $\leq$**

La divisibilité est liée à l'ordre naturel sur $\mathbb{N}$ par

$$\forall b \in \mathbb{Z}, \forall a \in \mathbb{Z}, a \,\Big|\, b \implies (b = 0 \text{ ou } |a| \leq |b|)\,.$$

La réciproque est fausse.

Démonstration. Pour tout $k \geq 1$, on a $k|a| \geq |a|$. ∎

P 4 **Propriétés de la relation $\Big|$ sur $\mathbb{Z}$**

La relation $\Big|$ sur $\mathbb{Z}$ est

1. *réflexive :* $\forall a \in \mathbb{Z}, a \,\Big|\, a$;
2. *transitive :* $\forall (a,b,c) \in \mathbb{Z}^3, \left(a \,\Big|\, b \text{ et } b \,\Big|\, c\right) \implies a \,\Big|\, c$;

C 5 *Soit* $(a,b) \in \mathbb{N}^2$.

$$a \,\Big|\, b \iff b \in a\mathbb{Z} \iff b\mathbb{Z} \subset a\mathbb{Z}.$$

D 6 Soit $(a, b) \in \mathbb{Z}^2$. On dit que les entiers a et b sont associés si $\left(a \,\middle|\, b \text{ et } b \,\middle|\, a\right)$.

P 7 **Caractérisation des couples d'intiers associés**

Soit $(a, b) \in \mathbb{Z}^2$. Les assertions suivantes sont équivalentes

1. *a et b sont associés.*
2. *$a\mathbb{Z} = b\mathbb{Z}$.*
3. *$a = b$ ou $a = -b$.*

1. Divisibilité et division euclidienne
1.1 La relation « divise » dans $\mathbb{Z}$
1.2 Compatibilité avec les opérations algébriques
1.3 Division euclidienne

2. Les nombres premiers

3. Plus grand commun diviseur, algorithme d'Euclide

4. Décomposition en facteurs premiers

5. La relation de congruence

P 8 **Compatibilité avec les opérations algèbriques**

Soit $(a, b, c, d) \in \mathbb{Z}^4$.

1. *Combinaison linéaire à coefficients entiers : si* $a \mid b$ *et* $a \mid c$, *alors*

$$\forall (u, v) \in \mathbb{Z}^2 \ a \mid ub + vc.$$

   En particulier, si $a \mid b$ *et* $a \mid c$, *alors* $a \mid b + c$ *et* $a \mid b - c$.

2. *Produit : Si* $a \mid b$ *et* $c \mid d$, *alors* $ac \mid bd$.

   En particulier, si $a \mid b$ *alors pour tout* $k \in \mathbb{N}$, $a^k \mid b^k$.

3. *Multiplication/division par un entier : si* $c \neq 0$, *alors* $a \mid b \iff ac \mid bc$.

1. Divisibilité et division euclidienne

1.1 La relation « divise » dans $\mathbb{Z}$

1.2 Compatibilité avec les opérations algébriques

1.3 Division euclidienne

2. Les nombres premiers

3. Plus grand commun diviseur, algorithme d'Euclide

4. Décomposition en facteurs premiers

5. La relation de congruence

D 9

Division euclidienne dans $\mathbb{N}$

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^{\star}$. Alors il existe un unique couple d'entiers $(q, r) \in \mathbb{Z} \times \mathbb{N}$ vérifiant

$$a = bq + r \qquad \text{et} \qquad 0 \leq r < b.$$

- q est le **quotient** de la division euclidienne de a par b.
- r est le **reste** de la division euclidienne de a par b et on le note $a \mod b$..

L'opération qui remplace a par r s'appelle la **réduction modulo** b.

Démonstration. ▶ Commençons prouver l'unicité d'un couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que $a = bq + r$ et $0 \leq r < b$. Supposons l'existence de deux couples (q, r) et (q', r') vérifiant ces conditions. Alors $a = qb + r = q'b + r'$, d'où $r - r' = b(q - q')$; ainsi b divise $|r - r'|$. Puisque $0 \leq r < b$ et $0 \leq r' < b$, on en déduit $-b < r - r' < b$, c'est-à-dire $0 \leq |r - r'| < b$. Or le seul multiple de b dans $[0, b[$ est 0, on a donc $r = r'$. Puisque $r - r' = b(q - q')$ et $b \neq 0$, on a par conséquent $q = q'$.

▶ Soit $E = \{ k \in \mathbb{Z} \mid kb \leq a \}$. Cet ensemble est une partie non vide et majorée de $\mathbb{Z}$. En effet, si $a \geq 0$, $0 \in E$ et a majore E (car $b \geq 1$). Si $a < 0$, alors 0 majore E. L'ensemble E admet donc un plus grand élément q. On a donc $qb \leq a < (q + 1)b$ (sinon $q + 1 \in E$) et en posant $r = a - bq$, on a bien $0 \leq r < b$.

∎

E 10

$$\begin{array}{r|l} 543 & 17 \\ \cline{2-2} 33 & 31 \\ 16 & \end{array}$$

Ici $a = 543, b = 17, q = 31, r = 16.$

P 11 *Soit r le reste de la division euclidienne de a par b. On a*

$$b \mid a \iff r = 0.$$

1. Divisibilité et division euclidienne

2. Les nombres premiers
2.1 Définition
2.2 Crible d'Erathosthène
2.3 Ensemble des nombres premiers

3. Plus grand commun diviseur, algorithme d'Euclide

4. Décomposition en facteurs premiers

5. La relation de congruence

1. Divisibilité et division euclidienne

2. Les nombres premiers
2.1 Définition
2.2 Crible d'Erathosthène
2.3 Ensemble des nombres premiers

3. Plus grand commun diviseur, algorithme d'Euclide

4. Décomposition en facteurs premiers

5. La relation de congruence

D 12 Un **nombre premier** est un entier naturel $p \geq 2$ dont les seuls diviseurs strictement positifs sont 1 et p. On note $\mathbb{P}$ l'ensemble des nombres premiers.

Avec des quantificateurs, cela s'écrit

$$\forall (a, b) \in \mathbb{N}, p = ab \implies a = 1 \text{ ou } b = 1.$$

P 13 *Pour qu'un entier $p > 1$ soit premier, il faut et il suffit qu'il ne soit pas produit de deux entiers strictement plus grand que 1.*

T 14 **(Euclide)**
Tout entier $n > 1$ est un produit (fini) de nombres premiers. En particulier, n possède au moins un diviseur premier.

1. Divisibilité et division euclidienne

2. Les nombres premiers
2.1 Définition
2.2 Crible d'Erathosthène
2.3 Ensemble des nombres premiers

3. Plus grand commun diviseur, algorithme d'Euclide

4. Décomposition en facteurs premiers

5. La relation de congruence

P 15 *Soit $n > 1$. Si n n'est pas premier, il possède un facteur premier p tel que $p^2 \leq n$.*

A 16 Crible d'Erathosthène

Si l'entier n n'est divisible par aucun nombre premier p tel que $p^2 \leq n$, alors n est un nombre premier.

	$\boxed{2}$	$\boxed{3}$	4	$\boxed{5}$	6	$\boxed{7}$	8	9	10
$\boxed{11}$	12	$\boxed{13}$	14	15	16	$\boxed{17}$	18	$\boxed{19}$	20
21	22	$\boxed{23}$	24	25	26	27	28	$\boxed{29}$	30
$\boxed{31}$	32	33	34	35	36	$\boxed{37}$	38	39	40
$\boxed{41}$	42	$\boxed{43}$	44	45	46	$\boxed{47}$	48	49	50
51	52	$\boxed{53}$	54	55	56	57	58	$\boxed{59}$	60
$\boxed{61}$	62	63	64	65	66	$\boxed{67}$	68	69	70
$\boxed{71}$	72	$\boxed{73}$	74	75	76	77	78	$\boxed{79}$	80
81	82	$\boxed{83}$	84	85	86	87	88	$\boxed{89}$	90
91	92	93	94	95	96	$\boxed{97}$	98	99	100

1. Divisibilité et division euclidienne

2. Les nombres premiers
2.1 Définition
2.2 Crible d'Erathosthène
2.3 Ensemble des nombres premiers

3. Plus grand commun diviseur, algorithme d'Euclide

4. Décomposition en facteurs premiers

5. La relation de congruence

T 17 *L'ensemble $\mathbb{P}$ des nombres premiers est infini.*

Démonstration. Supposons que l'ensemble des nombres premiers $\mathbb{P}$ soit fini. On peut alors écrire $\mathbb{P} = \{ p_1, \dots, p_k \}$. On introduit l'entier $n = p_1 p_2 \dots p_k + 1 \geq 2$. Cet entier a un diviseur premier p. Ce nombre premier p est donc l'un des p_i. Or p divise n et divise $p_1 p_2 \dots p_k = n - 1$, donc p divise $(n-1) - n = 1$, ce qui est absurde. ∎

1. Divisibilité et division euclidienne

2. Les nombres premiers

3. Plus grand commun diviseur, algorithme d'Euclide
3.1 Plus grand commun diviseur de deux entiers
3.2 Algorithme d'Euclide
3.3 Égalité de Bézout, théorème de Gauß, lemme d'Euclide
3.4 Plus petit commun multiple de deux entiers

4. Décomposition en facteurs premiers

5. La relation de congruence

1. Divisibilité et division euclidienne

2. Les nombres premiers

3. Plus grand commun diviseur, algorithme d'Euclide
3.1 Plus grand commun diviseur de deux entiers
3.2 Algorithme d'Euclide
3.3 Égalité de Bézout, théorème de Gauß, lemme d'Euclide
3.4 Plus petit commun multiple de deux entiers

4. Décomposition en facteurs premiers

5. La relation de congruence

D 18 Soient a et b deux entiers relatifs non nuls. L'ensemble des diviseurs communs positifs de a et b admet un plus grand élément. Ce dernier est appelé **plus grand commun diviseur** de a et b et est noté $\operatorname{pgcd}(a, b)$. Ainsi,

$$\operatorname{pgcd}(a, b) = \max \left\{ d \in \mathbb{N} \;\middle|\; d \,\middle|\, a \text{ et } d \,\middle|\, b \right\}.$$

T 19 Déterminer le pgcd de 105 et 48.

D 18 Soient a et b deux entiers relatifs non nuls. L'ensemble des diviseurs communs positifs de a et b admet un plus grand élément. Ce dernier est appelé **plus grand commun diviseur** de a et b et est noté $\operatorname{pgcd}(a,b)$. Ainsi,

$$\operatorname{pgcd}(a,b) = \max\left\{ d \in \mathbb{N} \;\middle|\; d \;\middle|\; a \text{ et } d \;\middle|\; b \right\}.$$

T 19 Déterminer le pgcd de 105 et 48.

R

- Par convention $\operatorname{pgcd}(0,0) = 0$.
- On a toujours $\operatorname{pgcd}(a,0) = |a|$.
- Si $a, b \in \mathbb{Z}$, $\operatorname{pgcd}(a,b) = \operatorname{pgcd}(|a|, |b|)$.
- a divise b si, et seulement si, $\operatorname{pgcd}(a,b) = |a|$.

D 20 On dit que a et b sont **premiers entre eux** lorsque leur pgcd vaut 1.

1. Divisibilité et division euclidienne

2. Les nombres premiers

3. Plus grand commun diviseur, algorithme d'Euclide
3.1 Plus grand commun diviseur de deux entiers
3.2 Algorithme d'Euclide
3.3 Égalité de Bézout, théorème de Gauß, lemme d'Euclide
3.4 Plus petit commun multiple de deux entiers

4. Décomposition en facteurs premiers

5. La relation de congruence

T 21 *Soient des entiers a et b.*

1. *Soit k un entier, alors $\operatorname{pgcd}(a,b) = \operatorname{pgcd}(a-kb,b)$.*
2. *Si $b>0$, $\operatorname{pgcd}(a,b) = \operatorname{pgcd}(b,r)$ avec $r = a \mod b$.*
3. *Soit un entier $m>0$, alors $\operatorname{pgcd}(ma,mb) = m \times \operatorname{pgcd}(a,b)$.*
4. *Soit un entier $d>0$; si d divise a et b, soient a' et b' les entiers tels que $a = da'$ et $b = db'$. Alors d est le pgcd de a et b si, et seulement si, a' et b' sont premiers entre eux.*

A 22 Algorithme d'Euclide

On pose $a_0 = a$, $a_1 = b$, puis pour tout k jusqu'à avoir $a_{k+2} = 0$,

$$a_{k+2} = a_k \mod a_{k+1},$$

c'est-à-dire a_{k+2} est le reste dans la division euclidienne de a_k par a_{k+1}.
Alors $\operatorname{pgcd}(a, b) = a_{k+1}$.

E 23 On a $\operatorname{pgcd}(105, 48) = 3$.
En «remontant les calculs», cela permet de trouver des entiers $u, v \in \mathbb{Z}$ tels que

$$105u + 48v = 3.$$

1. Divisibilité et division euclidienne

2. Les nombres premiers

3. Plus grand commun diviseur, algorithme d'Euclide
3.1 Plus grand commun diviseur de deux entiers
3.2 Algorithme d'Euclide
3.3 Égalité de Bézout, théorème de Gauß, lemme d'Euclide
3.4 Plus petit commun multiple de deux entiers

4. Décomposition en facteurs premiers

5. La relation de congruence

T 24 **Égalité de Bézout**

Deux entiers a et b sont premiers entre eux si, et seulement si

$$\exists (u, v) \in \mathbb{Z}^2, ua + vb = 1.$$

T 25 **Lemme de Gauß**

Si a est premier avec b et a divise bc, alors a divise c.

Démonstration. Il existe des entier u, v, w tel que $ua + vb = 1$ et $bc = aw$. On peut donc écrire

$$c = uac + vbc = uac + vaw = a(uc + vw).$$

∎

T 26 **Lemme d'Euclide**

Un entier $p \geq 2$ est un nombre premier si et seulement si il vérifie la condition

$$\forall (a,b) \in \mathbb{N}^2, p \,\Big|\, ab \implies \left(p \,\Big|\, a \text{ ou } p \,\Big|\, b\right);$$

appelée lemme d'Euclide.

Démonstration. C'est un cas particulier du Lemme de Gauß. Ou bien p divise a, ou bien il est premier avec a et il divise alors b. ∎

C 27

1. *Si p premier divise $a_1 a_2 \cdots a_n$, il divise au moins l'un des facteurs.*
2. *Si p premier divise a^n, $(n \in \mathbb{N}^\star)$, alors il divise a.*

1. Divisibilité et division euclidienne

2. Les nombres premiers

3. Plus grand commun diviseur, algorithme d'Euclide
3.1 Plus grand commun diviseur de deux entiers
3.2 Algorithme d'Euclide
3.3 Égalité de Bézout, théorème de Gauß, lemme d'Euclide
3.4 Plus petit commun multiple de deux entiers

4. Décomposition en facteurs premiers

5. La relation de congruence

D 28 Soient a et b des entiers non nuls. L'ensemble des multiples communs strictement positifs de a et b admet un plus petit élément. Ce dernier est appelé **plus petit commun multiple** de a et b et est noté $\operatorname{ppcm}(a, b)$.

$$\operatorname{ppcm}(a, b) = \min \left\{ m \in \mathbb{N}^\star \;\middle|\; a \,\middle|\, m \text{ et } b \,\middle|\, m \right\}.$$

1. Divisibilité et division euclidienne

2. Les nombres premiers

3. Plus grand commun diviseur, algorithme d'Euclide

4. Décomposition en facteurs premiers
4.1 Facteurs premiers d'un entier. Le théorème de décomposition
4.2 Valuation p-adique
4.3 Applications

5. La relation de congruence

1. Divisibilité et division euclidienne

2. Les nombres premiers

3. Plus grand commun diviseur, algorithme d'Euclide

4. Décomposition en facteurs premiers
4.1 Facteurs premiers d'un entier. Le théorème de décomposition
4.2 Valuation p-adique
4.3 Applications

5. La relation de congruence

T 29 **Décomposition en facteurs premiers**

Soit $n \in \mathbb{N}$ tel que $n \geq 2$. Alors n admet une factorisation unique en facteurs premiers, à l'ordre des facteurs près, c'est-à-dire

$$\exists! m \in \mathbb{N}^{\star}, \exists!(p_1, \ldots, p_m) \in \mathbb{P}^m, p_1 \leq p_2 \leq \cdots \leq p_m \text{ et } n = p_1 p_2 \cdots p_m.$$

E 30 $90 = 9 \times 10 = 3 \times 3 \times 2 \times 5 = 2 \times 3 \times 3 \times 5 = 2 \times 3^2 \times 5.$

1. Divisibilité et division euclidienne

2. Les nombres premiers

3. Plus grand commun diviseur, algorithme d'Euclide

4. Décomposition en facteurs premiers
4.1 Facteurs premiers d'un entier. Le théorème de décomposition
4.2 Valuation p-adique
4.3 Applications

5. La relation de congruence

D 31 La décomposition de $n \geq 2$ en facteurs premiers peut également s'écrire sous la forme

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdots p_r^{\alpha_r}$$

où

- les p_i sont des nombres premiers deux à deux distincts,
- $\alpha_i \geq 1$.

Cette écriture est unique, à l'ordre des facteurs près.

- L'entier α_i est appelé **exposant** du nombre premier p_i dans la décomposition de n en facteur premier et noté $v_{p_i}(n)$.
- Si p est un nombre premier distinct de $p_1, \ldots, p_r$, on pose $v_p(n) = 0$.

On dit que $v_p(n)$ est la **valuation p-adique** de n.

P 32 *Soit $a, b \in \mathbb{N}^\star$, alors*

$$v_p(ab) = v_p(a) + v_p(b).$$

P 33 *Soit n un entier non nul qui se décompose en produit de facteurs premiers de la façon suivante*

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdots p_r^{\alpha_r}$$

Alors, les diviseurs de n dans $\mathbb{N}^\star$ sont les entiers naturels de la forme

$$d = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdot \cdots \cdots p_r^{\gamma_r}, \quad \text{avec } 0 \leq \gamma_i \leq \alpha_i \text{ pour } i = 1 \ldots r.$$

T 34 *Soient x, y deux entiers strictement positifs. Pour que x divise y, il faut et il suffit que*

$$\forall p \in \mathbb{P}, v_p(x) \leq v_p(y).$$

T 35 Quels sont les diviseurs de 90?

1. Divisibilité et division euclidienne

2. Les nombres premiers

3. Plus grand commun diviseur, algorithme d'Euclide

4. Décomposition en facteurs premiers

4.1 Facteurs premiers d'un entier. Le théorème de décomposition

4.2 Valuation p-adique

4.3 Applications

5. La relation de congruence

P 36 *Si*

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdots p_r^{\alpha_r} \qquad\qquad b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \cdots \cdots p_r^{\beta_r}$$

où les α_i et β_i sont des entiers éventuellement nuls. On a

$$\operatorname{pgcd}(a, b) = p_1^{\min(\alpha_1,\beta_1)} \times p_2^{\min(\alpha_2,\beta_2)} \times \cdots \times p_r^{\min(\alpha_r,\beta_r)}$$

T 37 Retrouver le pgcd de 105 et 48.

P 38 *Si*

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdots p_r^{\alpha_r} \qquad\qquad b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \cdots \cdots p_r^{\beta_r}$$

où les α_i et β_i sont des entiers éventuellement nuls. On a

$$\mathrm{ppcm}(a, b) = p_1^{\max(\alpha_1,\beta_1)} \times p_2^{\max(\alpha_2,\beta_2)} \times \cdots \times p_r^{\max(\alpha_r,\beta_r)}$$

P 39 *Soit de entiers $a > 0$ et $b > 0$. Si $d = \mathrm{pgcd}(a, b)$ et $m = \mathrm{ppcm}(a, b)$, alors $ab = dm$. Tout multiple commun à a et b est multiple de leur ppcm.*

Démonstration. On remarque que pour $x, y \in \mathbb{N}$, on a $x + y = \max(x, y) + \min(x, y)$. Il suffit alors de comparer les exposants de p dans ab et dm : ils sont égaux. ∎

1. Divisibilité et division euclidienne

2. Les nombres premiers

3. Plus grand commun diviseur, algorithme d'Euclide

4. Décomposition en facteurs premiers

5. La relation de congruence

5.1 La notion de congruence dans $\mathbb{Z}$

5.2 Lien avec la division euclidienne

5.3 Compatibilité avec les opérations algébriques

5.4 Petit théorème de Fermat

1. Divisibilité et division euclidienne

2. Les nombres premiers

3. Plus grand commun diviseur, algorithme d'Euclide

4. Décomposition en facteurs premiers

5. La relation de congruence

5.1 La notion de congruence dans $\mathbb{Z}$

5.2 Lien avec la division euclidienne

5.3 Compatibilité avec les opérations algébriques

5.4 Petit théorème de Fermat

D 40 Soit $a, b, n \in Z$ trois entiers. On défini la relation de congruence par

$$(a \equiv b \pmod{n}) \iff (\exists k \in \mathbb{Z}, a = b + kn) .$$

On dit que «a est **congru** à b **modulo** n». Les réels a et b diffèrent donc d'un multiple entier de n c'est-à-dire $x - y \in n\mathbb{Z}$.

E 41

- $230897 \equiv 7 \pmod{10}$.
- $17 \equiv 2 \pmod{3}$, mais aussi $17 \equiv -1 \pmod{3}$.

N Pour tous entiers a et n, on note $a+n\mathbb{Z}$ l'ensemble des entiers congrus à a modulo n. Ce sont les entiers de la forme $a+kn$, où $k \in \mathbb{Z}$. On note

$$a+n\mathbb{Z} = \{\, a+kn \mid k \in \mathbb{Z} \,\}\,.$$

E 42 L'ensemble des nombres impairs peut donc se noter $1+2\mathbb{Z}$; celui des nombres donc l'écriture décimale termine par 5 peut se noter $5+10\mathbb{Z}$.

1. Divisibilité et division euclidienne

2. Les nombres premiers

3. Plus grand commun diviseur, algorithme d'Euclide

4. Décomposition en facteurs premiers

5. La relation de congruence
5.1 La notion de congruence dans $\mathbb{Z}$
5.2 Lien avec la division euclidienne
5.3 Compatibilité avec les opérations algébriques
5.4 Petit théorème de Fermat

P 43 *Soit $a, b, r \in \mathbb{Z}$. Le reste de la division euclidienne de a par b est r si, et seulement si*

$$a \equiv r \pmod{b} \qquad \textit{et} \qquad 0 \leq r < b.$$

On a donc

$$b \,\Big|\, a \iff a \equiv 0 \pmod{b}.$$

1. Divisibilité et division euclidienne

2. Les nombres premiers

3. Plus grand commun diviseur, algorithme d'Euclide

4. Décomposition en facteurs premiers

5. La relation de congruence

5.1 La notion de congruence dans $\mathbb{Z}$

5.2 Lien avec la division euclidienne

5.3 Compatibilité avec les opérations algébriques

5.4 Petit théorème de Fermat

P 44 *Soient* $n \in \mathbb{N}^\star$, $a, b, c, d, k \in \mathbb{N}$ *et* $p \in \mathbb{N}$.

1. *Si* $a \equiv b \pmod{n}$ *et* $c \equiv d \pmod{n}$, *alors*

$$a + c \equiv b + d \pmod{n}; \qquad a - c \equiv b - d \pmod{n}; \qquad ac \equiv bd \pmod{n}.$$

2. *Si* $a \equiv b \pmod{n}$, *alors*

$$ka \equiv kb \pmod{kn}; \qquad ka \equiv kb \pmod{n}; \qquad a^p \equiv b^p \pmod{n}$$

T 45 Démontrer la proposition précédente.

1. Divisibilité et division euclidienne

2. Les nombres premiers

3. Plus grand commun diviseur, algorithme d'Euclide

4. Décomposition en facteurs premiers

5. La relation de congruence
5.1 La notion de congruence dans $\mathbb{Z}$
5.2 Lien avec la division euclidienne
5.3 Compatibilité avec les opérations algébriques
5.4 Petit théorème de Fermat

T 46 **Petit théorème de Fermat**

Soit p un nombre premier. Si $a \in \mathbb{Z}$ n'est pas multiple de p, on a

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

Un énoncé équivalent est

T 47 **Petit théorème de Fermat**

Soit p un nombre premier et $a \in \mathbb{Z}$. On a

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

Démonstration. ∎