ARITHMETIQUE DANS $\mathbb{Z}$

I) Divisibilité dans $\mathbb{Z}$

Diviseurs, multiples

Définition: Soit $(a,b) \in \mathbb{Z}^2$. On dit que **b est un diviseur de a** (ou que **a est un multiple de b)** ssi $\exists m \in \mathbb{Z} \mid a = b \times m$. On pourra noter $b \mid a$, qui est lu : "b divise a"

Remarque: La relation de divisibilité dans $\mathbb{Z}$ est réflexive, transitive mais elle n'est pas antisymétrique (ni symétrique d'ailleurs). Par contre, il s'agit bien d'une relation d'ordre dans $\mathbb{N}$.

Définition: Soit $(a,b) \in \mathbb{Z}^2$. On dit que **a et b sont associés** ssi $a \mid b$ et $b \mid a$.

Remarque: On a alors $a = b$ ou $a = -b$

Division euclidienne dans $\mathbb{Z}$

Théorème : Division euclidienne $\forall (a,b) \in \mathbb{Z} \times \mathbb{N}^*, \exists ! (q,r) \in \mathbb{Z}^2 \mid a = bq + r$ et $0 \leq r < b$

Définition: Dans la division euclidienne de a par b, on appelle q **le quotient**, r **le reste**, a le dividende et b le diviseur.

Dem: Soit $(a,b) \in \mathbb{Z} \times \mathbb{N}^*$. **Existence**. Soit $A = \{p \in \mathbb{Z} \mid bp \leq a\}$.

- ✔ $A \neq \varnothing$ car la suite $(-nb)_{n \in \mathbb{N}}$ diverge vers $-\infty$
- ✔ A est majorée. En effet : Si $a \leq 0$, $\forall p \in A$, $p \leq 0$.

Si $a > 0$, $\forall p \in A$, $p \leq a$ (car si $p > a$, alors $bp \geq p > a$)

Donc A est une partie non vide et majorée de $\mathbb{Z}$ donc A possède un plus grand élément. Soit q ce plus grand élément.

On a : $qb \leq a$ et $(q+1)b > a$. Ainsi, en posant $r = a - bq$, on a : $0 \leq r < b$

On a bien établi l'existence du couple (q,r) tel que $a = bq + r$ et $0 \leq r < b$

Unicité. Supposons : $\exists (q,r,q',r') \in \mathbb{Z}^4 \mid a = bq + r = bq' + r'$ et $0 \leq r < b$ et $0 \leq r' < b$.

On a alors : $r' - r = b(q - q') \Rightarrow |r' - r| = b|q - q'|$

Si $q \neq q'$, $|q - q'| \geq 1$ et donc $b|q - q'| \geq b$. Mais alors $|r' - r| \geq b$ ce qui est impossible car $(r,r') \in [0,b[^2$. Ainsi $q = q'$ et alors $r = r'$. On a bien l'unicité du couple (q,r).

Remarque: On peut prolonger la division euclidienne à un couple (a,b) d'entiers relatifs avec b non nul. $\forall (a,b) \in \mathbb{Z} \times \mathbb{Z}^*, \exists ! (q,r) \in \mathbb{Z}^2 \mid a = bq + r$ et $0 \leq r < |b|$

II) PGCD

PGCD de deux entiers naturels

Définition: Soit $(a,b) \in \mathbb{N}^2$, $(a,b) \neq (0,0)$. On appelle **PGCD de a et de b** le plus grand élément (pour la relation $\leq$) de l'ensemble des diviseurs communs à a et b. On le note $a \wedge b$ ou pgcd(a,b). On convient pgcd(0,0) = 0

Remarque: Cet élément existe bien. En effet l'ensemble des diviseurs communs à a et b est une partie de $\mathbb{Z}$, non vide (car contient 1) et majorée (par max(a,b)) : cette partie de $\mathbb{Z}$ possède donc bien un plus grand élément.

Algorithme d'Euclide

Théorème : Soit $(a,b) \in \mathbb{N}^2$, $(a,b) \neq (0,0)$. L'ensemble des diviseurs communs à a et à b est l'ensemble des diviseurs de $a \wedge b$.

Dem: On notera lorsque n est un entier naturel, D(n) l'ensemble des diviseurs de n.

1) Si b = 0, on a : $a \wedge b = a$ et $D(b) = \mathbb{Z}$, donc $D(a) \cap D(b) = D(a)$.

2) Si a = 0, on a : $a \wedge b = b$ et $D(a) \cap D(b) = D(b)$

3) Sinon, quitte à échanger a et b, on peut supposer $0 < b \leq a$.

On effectue la division euclidienne de a par b : $\exists (q_1, r_1) \in \mathbb{Z}^2 \mid a = b q_1 + r_1$ avec $0 \leq r_1 < b$

* Si d divise a et b alors d divise r_1 et b

* Si d divise r_1 et b alors d divise a et b

Ainsi $D(a) \cap D(b) = D(r_1) \cap D(b)$. On réitère le procédé : $b = r_1 q_2 + r_2$ et $D(a) \cap D(b) = D(r_1) \cap D(r_2)$

On crée ainsi une suite $r_0 = b, r_1, r_2, ..., r_p$ tant que $r_p \neq 0$ telle que: $\forall k \leq p-1$, $D(a) \cap D(b) = D(r_k) \cap D(r_{k+1})$

et $0 \leq r_p < r_{p-1} < ... < r_1 < b$. Cette suite d'entiers étant décroissante strictement, il existe un rang p tel que $r_{p+1} = 0$ et $r_p \neq 0$. On a alors que r_{p-1} est un multiple de r_p . Donc $D(r_{p-1}) \cap D(r_p) = D(r_p)$

Aussi $D(a) \cap D(b) = D(r_p)$ où r_p est le dernier reste non nul dans l'algorithme d'Euclide.

Mais alors, r_p est un diviseur commun à a et à b et c'est le plus grand diviseur commun à a et à b

Exemple: $25 \equiv 10\ [15]$, $15 \equiv 5\ [10]$ et $10 \equiv 0\ [5]$ Donc $25 \wedge 15 = 5$

Remarque: Le théorème précédent permet de dire que le PGCD de a et de b est non seulement le plus grand diviseur commun à a et b pour la relation $\leq$ mais également pour la divisibilité (les diviseurs communs à a et à b sont tous des diviseurs de $a \wedge b$)

Remarque: Les diviseurs des entiers n et – n étant les mêmes, la notion de PGCD (et l'algorithme d'Euclide) se prolonge au cas de deux entiers relatifs

Relation de Bézout

Théorème : Soit $(a,b) \in \mathbb{Z}^2$. Alors $\exists (u,v) \in \mathbb{Z}^2$ | $au + bv = a \wedge b$

Dem: Soit $d = a \wedge b =$ pgcd(a,b). En reprenant l'algorithme d'Euclide depuis la fin, on a : $d = r_p = r_{p-2} - q_p r_{p-1}$ donc d est la somme d'un multiple de r_{p-1} et d'un multiple de r_{p-2}.

Or $r_{p-1} = r_{p-3} - q_{p-1} r_{p-2}$ donc d est la somme d'un multiple de r_{p-2} et d'un multiple de r_{p-3} . En remontant les calculs, d est la somme d'un multiple de a et d'un multiple de b. $\exists (u,v) \in \mathbb{Z}^2$ | $au + bv = d = a \wedge b$

Exemple: Trouver un couple $(u,v) \in \mathbb{Z}^2$ tel que $512\,u + 421\,v = 1$. On a

	1	4	1	1	1	2
512	**421**	91	57	34	23	11
91	57	34	23	11	1	

D'où : $1 = 23 - 2 \times 11 = 23 - 2\,(34 - 23) = 3 \cdot 23 - 2 \cdot 34 = 3 \cdot (57 - 34) - 2 \cdot 34 = 3 \cdot 57 - 5 \cdot 34 = 3 \cdot 57 - 5 \cdot (91 - 57) = 8 \cdot 57 - 5 \cdot 91 = 8 \cdot (421 - 4 \cdot 91) - 5 \cdot 91 = 8 \cdot 421 - 37 \cdot 91$ Ainsi : $1 = 45 \cdot 421 - 37 \cdot 512$

Algorithme d'Euclide étendu: On veut trouver une méthode systématique pour trouver des coefficients de Bézout. L'idée est de reprendre l'algorithme d'Euclide en notant r_k les différents restes dans l'algorithme d'Euclide, et de trouver deux suites d'entiers u_k et v_k pour lesquels on a $r_k = a\ u_k + b\ v_k$

Comme on a affaire à une récurrence double ($r_{p-1} = r_{p-3} - q_{p-1} r_{p-2}$), on va plutôt doubler le nombre de variables dans l'algorithme. On prendra 6 variables, r, r', u, u', v et v' telles qu'à chaque étape, on ait $r = a\,u + bv$, $r' = a\,u' + b\,v'$ (ce qui correspondra aux relations $r_k = a\,u_k + b\,v_k$ et $r_{k+1} = a\,u_{k+1} + b\,v_{k+1}$).

L'initialisation est donnée par : $r \leftarrow a$, $u \leftarrow 1$, $v \leftarrow 0$, $r' \leftarrow b$, $u' \leftarrow 0$, $v' \leftarrow 1$

Tant que r' est non nul, on calcule le quotient q de r par r' et on effectue les nouvelles affectations :

$(r, u, v, r', u', v') \leftarrow (r', u', v', r - q\,r', u - q\,u', v - q\,v')$ *Attention : affectations simultanées ici*

Lorsque le processus s'arrête, donc lorsque r' s'annule, r contient le dernier reste non nul de la division euclidienne (donc PGCD(a, b)) et comme à chaque étape, $r = au + bv$, u et v contiennent les deux coefficients de Bézout que nous cherchions.

III) Entiers premiers entre eux

Définition: Soit deux entiers relatifs a et b. On dit que **a et b sont premiers entre eux** si leur PGCD est égal à 1

Théorème de Bézout

Théorème de Bézout : Soit $(a,b) \in \mathbb{Z}^2$. $a \wedge b = 1 \Leftrightarrow \exists (u,v) \in \mathbb{Z}^2$; $au + bv = 1$

Dem: On sait d'abord, d'après la relation de Bézout, que si $a \wedge b = 1$, $\exists (u,v) \in \mathbb{Z}^2$; $au + bv = 1$

Réciproquement, si $\exists (u,v) \in \mathbb{Z}^2$; $au + bv = 1$. Soit alors d le pgcd de a et b. d divise a donc il divise aussi au. De même, d divise bv. Aussi d divise la somme qui vaut 1. Or d est en entier naturel, donc $d = 1$.

Lemme de Gauss : Soit $(a,b,c) \in \mathbb{Z}^3$ | a divise bc et $a \wedge b = 1$. Alors a divise c

Dem: On a $a \wedge b = 1 \Rightarrow \exists\ (u,v) \in \mathbb{Z}^2$ | $a\,u + b\,v = 1$. D'où : $auc + bvc = c$.

Or a divise bcv et auc donc leur somme qui est c.

Propriété : Soit $(a,b,c) \in \mathbb{Z}^3$ | a divise c, b divise c et $a \wedge b = 1$ Alors ab divise c

Dem: On a $a \wedge b = 1 \Rightarrow \exists\ (u,v) \in \mathbb{Z}^2$ | $a\,u + b\,v = 1$. D'où : $auc + bvc = c$.

Or c est un multiple de a donc bvc est un multiple de ab. De même auc est un multiple de ab. Aussi c est un multiple de ab

Propriété : Soit $(a,b,c)\in\mathbb{Z}^3$ tels que $a \wedge b = 1$ et $a \wedge c = 1$ Alors $a \wedge bc = 1$

Dem: On a $a\wedge b = 1 \Rightarrow \exists\ (u,v) \in\mathbb{Z}^2 \mid a\,u + b\,v = 1$. De même, $\exists\ (\delta,\gamma) \in\mathbb{Z}^2 \mid a\,\delta + c\,\gamma = 1$
D'où : $1 = a\,(ua\delta + uc\gamma + \delta bv) + bc\,(v\gamma)$. Ainsi par Th. Bézout, a et bc sont premiers entre eux.

PGCD d'un nombre fini d'entiers

Définition: Soit $(a_1,a_2, \ldots, a_n)\in\mathbb{Z}^n$, n entiers non tous nuls. On appelle **PGCD de $(a_1,a_2, \ldots, a_n)$** le plus grand élément (pour la relation $\leq$) de l'ensemble des diviseurs communs à a_1, a_2, … et a_n. On le note $\text{pgcd}(a_1,a_2, \ldots, a_n)$. On convient $\text{pgcd}(0,0,..,0) = 0$

Remarque: Cet élément existe bien. En effet l'ensemble des diviseurs communs à $(a_1,a_2, \ldots, a_n)$ est une partie de $\mathbb{Z}$, non vide (car contient 1) et majorée (par $\max(a_1,a_2, \ldots, a_n)$) : cette partie de $\mathbb{Z}$ possède donc bien un plus grand élément.

Définition: Soit $(a_1,a_2, \ldots, a_n)\in\mathbb{Z}^n$. On dit que **$a_1$, a_2, … et a_n sont premiers entre eux dans leur ensemble** si $\text{pgcd}(a_1,a_2, \ldots, a_n) = 1$.

On dit que **a_1, a_2, … et a_n sont premiers entre eux deux à deux** ssi pour tout couple (i, j), avec $i \neq j$, $\text{pgcd}(a_i,a_j) = 1$

Exemple: Les entiers 15, 20, 12 sont premiers entre eux dans leur ensemble mais pas premiers entre eux deux à deux.

Relation de Bézout

Théorème : Soit $(a_1,a_2, \ldots, a_n)\in\mathbb{Z}^n$. Alors
$\exists\ (u_1,u_2, \ldots, u_n)\in\mathbb{Z}^n \mid a_1 u_1 + a_2 u_2 + \ldots + a_n u_n = \text{pgcd}(a_1, a_2, \ldots, a_n)$

Dem: On procède par récurrence sur le nombre d'entiers constituant la famille, en constatant que le pgcd de $(a_1,a_2, \ldots, a_n)$ est le pgcd de a_n et de $\text{pgcd}(a_1,a_2, \ldots, a_{n-1})$.

IV) PPCM

PPCM

Définition: Soit a et b deux entiers relatifs dont au moins un est non nul. On appelle **PPCM de a et de b (ou ppcm(a,b))** le plus petit entier naturel multiple commun à a et b. On le note **$a \vee b$**

Remarque: Cet élément existe bien. En effet l'ensemble des multiples naturels communs à a et b est une partie de $\mathbb{N}$, non vide (car contient $|a \times b|$) : cette partie de $\mathbb{N}$ possède donc bien un plus petit élément.

Théorème : Soit $(a,b)\in\mathbb{Z}^2$ tel que $a \wedge b = 1$. $a \vee b = |ab|$

Dem: * Si c multiple commun de a et b, alors d'après Gauss, c est un multiple de ab donc de |ab|.
* Si c est un multiple de |ab| alors c'est clairement un multiple de a et de b.

Théorème : Soit $(a,b)\in\mathbb{Z}^2$. $\text{pgcd}(a,b) \times \text{ppcm}(a,b) = |ab|$

Dem: Soit $d = \text{pgcd}(a,b)$. Soit a_1 et b_1 les quotients de a et b par d. Par définition de d, a_1 et b_1 sont premiers entre eux. D'où d'après la propriété précédente, $\text{ppcm}(a,b) = d \times \text{ppcm}(a_1, b_1) = d\,|a_1\,b_1|$

Ainsi, $\text{pgcd}(a,b) \times \text{ppcm}(a,b) = d^2\ |a_1\,b_1| = |ab|$.

Application: Tout rationnel possède une représentation irréductible, c'est à dire sous la forme $\frac{a}{b}$ avec a et b premiers entre eux (et $b > 0$) : il suffit de simplifier les deux termes de la fraction par leur PGCD

Pour trouver un dénominateur commun de deux irrationnels, on prend le ppcm des dénominateurs

V) Nombres premiers

Nombres premiers

Définition: On appelle **nombre premier** tout entier $p \geq 2$ n'ayant pour diviseurs positifs que 1 et lui-même. Un entier ≥ 2 non premier est appelé **composé**

Propriété : Soit $(a, p) \in \mathbb{Z}^2$ avec p nombre premier. Alors soit $a \wedge p = 1$ soit p divise a.

Dem: Soit d = pgcd(a,b). d est un diviseur positif de p. On a donc : soit d = 1 auquel cas a et p sont premiers entre eux. Soit d = p auquel cas p divise a.

Remarque: On en déduit une méthode pour obtenir les nombres premiers inférieurs à une valeur donnée : le **crible d'Eratosthène** que l'on programmera en informatique. On écrit dans un tableau les entiers compris entre 2 et la borne n. On conserve le premier nombre non rayé (ici 2) et on raye tous ses autres multiples. Puis on passe au suivant (ici 3) et on raye tous les multiples non encore rayés etc… Une fois considéré les nombres jusqu'à $\sqrt{n}$, tous les nombres restants sont premiers.

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

Remarque: On en déduit une conséquence du théorème de Gauss pour les nombres premiers : Si p est un nombre premier et a et b sont deux entiers. Alors **si p divise ab et p ne divise pas a, alors p divise b**. (On connait ce résultat sous le terme de lemme d'Euclide)

Infinité de nombres premiers

Théorème : Tout entier $n \geq 2$, possède au moins un facteur premier.

Dem: Soit P_n la propriété de récurrence : " n possède au moins un facteur premier"

- P_2 vraie ? 2 possède un facteur premier : lui-même. **P_2 est vraie**
- Soit $n \geq 2$. On suppose $\forall k \in [\![2, n]\!]$, P_k vraie. P_{n+1} est-elle également vraie ? On a : $n + 1 \geq 2$. De deux choses l'une : ○ soit n + 1 est premier, auquel cas il possède bien un facteur premier
  ○ soit n + 1 n'est pas premier. Auquel cas, on peut trouver deux entiers naturels d et q tous deux différents de 1 et de n + 1 tels que : n + 1 = d q
  Mais alors, q est dans $[\![2, n]\!]$ donc, comme P_q est vraie, on en déduit que q possède un facteur premier… facteur premier qui divise aussi n + 1.
  On en déduit que **P_{n+1} est vraie**

➢ Ainsi on a montré que P_2 est vraie et que, pour tout $n \geq 2$, $\forall k \in [\![2, n]\!]$, P_k vraie entraine P_{n+1} vraie. Aussi, par le théorème de récurrence forte, on a : $\forall n \in \mathbb{N}, n \geq 2 \Rightarrow P_n$ vraie

Théorème : L'ensemble des nombres premiers est infini.

Dem: Supposons par l'absurde que l'ensemble des nombres premiers est fini.
Notons $p_1, p_2, \ldots$ et p_n tous les nombres premiers. On pose $N = p_1 p_2 .. p_n + 1$.

Cet entier N est supérieur ou égal à 2 et il possède donc au moins un facteur premier. Mais, par le théorème de Bézout, on montre aisément que N est premier avec chacun des nombres premiers p_1, p_2, … et p_n. Ainsi, tous les facteurs premiers de N sont en dehors de la liste des nombres premiers p_1, p_2, … p_n, ce qui est impossible car elle était censée représentée tous les nombres premiers. Contradiction

Théorème (théorème fondamental de l'arithmétique) : Tout entier $n \geq 2$, s'écrit de manière unique (à l'ordre près), comme produit de nombres premiers.

Dem: Existence. Soit P_n : " n s'écrit comme produit de nombres premiers"

- P_2 vraie ? 2 s'écrit comme produit d'un nombre premier : lui-même. **P_2 est vraie**
- Soit $n \geq 2$. On suppose $\forall k \in [\![2, n]\!]$, P_k vraie. P_{n+1} est-elle également vraie ? On a : $n + 1 \geq 2$. Deux cas : ○ soit $n + 1$ est premier, auquel cas il s'écrit bien comme produit de nombres premiers
  ○ soit $n + 1$ n'est pas premier. Auquel cas, on peut trouver deux entiers naturels d et q tous deux différents de 1 et de $n + 1$ tels que : $n + 1 = d\,q$
  Mais alors, d et q sont dans $[\![2, n]\!]$ donc, comme P_d et P_q sont vraies, on en déduit que d et q s'écrivent comme produit de nombres premiers, et donc $n + 1$ est aussi produit de nombres premiers
  On en déduit que **P_{n+1} est vraie**

➢ Ainsi on a montré que P_2 est vraie et que, pour tout $n \geq 2$, $\forall k \in [\![2, n]\!]$, P_k vraie entraine P_{n+1} vraie.
Aussi, par le théorème de récurrence forte, on a : $\forall n \in \mathbb{N}, n \geq 2 \Rightarrow P_n$ vraie

Unicité. Supposons que l'entier n possède deux décompositions en produit de facteurs premiers. Quitte à multiplier ces écritures par des termes du type p^0 pour p premier, et à réordonner les écritures, on peut supposer que l'on a écrit n sous les formes : $n = \prod_{k=1}^{q} p_k^{\alpha_k} = \prod_{k=1}^{q} p_k^{\beta_k}$ où les p_1, p_2, … p_q sont des nombres premiers 2 à 2 distincts et les α_1, α_2, … α_q et les β_1, β_2, … β_q sont des sont des entiers naturels.
Montrer l'unicité de la décomposition revient alors à montrer que pour tout k entre 1 et q, $\alpha_k = \beta_k$.
Soit alors un entier m entre 1 et q. Quitte à échanger les deux écritures, on peut supposer $\alpha_m \leq \beta_m$.
En simplifiant l'égalité $\prod_{k=1}^{q} p_k^{\alpha_k} = \prod_{k=1}^{q} p_k^{\beta_k}$ par $p_m^{\alpha_m}$, on obtient $\prod_{\substack{k=1 \\ k \neq m}}^{q} p_k^{\alpha_k} = p_m^{\beta_m - \alpha_m} \prod_{\substack{k=1 \\ k \neq m}}^{q} p_k^{\beta_k}$
Mais alors, p_m ne divise pas le premier terme car les p_k sont distincts 2 à 2. Il ne doit donc pas diviser non plus le second membre. Aussi $\alpha_m = \beta_m$

Valuation p-adique

Définition: Soit p un nombre premier et n un entier naturel. On appelle **valuation p-adique de n** l'entier $q \geq 0$ tel que p^q divise n et p^{q+1} ne divise pas n. On note cette valuation p-adique sous la forme : $v_p(n)$.

Remarque: Cet entier existe bien. En effet l'ensemble des entiers k tels que p^k divise n est une partie de $\mathbb{N}$, non vide (car contient 0) et majorée (par n car $p^n \geq 2^n > n$) : cette partie de $\mathbb{N}$ possède donc bien un plus grand élément : $v_p(n)$

Propriété : Soit p un nombre premier et n un entier naturel. Alors p divise n ssi $v_p(n) \geq 1$

Dem: Cela provient directement de la définition.

Application: Soit a et b deux entiers. pour déterminer le pgcd de a et de b il suffit de décomposer a et b en produit de facteurs premiers et de ne conserver que les facteurs premiers communs aux deux décompositions et ce avec la valuation p-adique la plus petite.

Pour le ppcm, il suffira de prendre tous les facteurs premiers intervenant et avec la valuation p-adique maximale rencontrée.

VI) Congruences

Relation de congruence modulo n

Définition: Soit n un entier relatif. On définit **la relation de congruence modulo n sur $\mathbb{Z}$** par : $\forall (a, b)\in\mathbb{Z}^2$, $a \equiv b\ [n] \Leftrightarrow$ n divise a – b

Remarque: La relation de congruence modulo 0 est l'égalité.
La relation de congruence modulo – n est la même que la congruence modulo n. On pourra ainsi travailler avec des congruence modulo n > 0.

Propriété : Soit $n\in\mathbb{N}^*$. La relation de congruence modulo n est une relation d'équivalence.

Dem: Cela a déjà été vu

Propriété : Soit $n\in\mathbb{N}^*$. La relation de congruence modulo n est stable par addition et multiplication i.e. : $\forall(a, b, c, d) \in\mathbb{Z}^4$, avec $a \equiv b\ [n]$ et $c \equiv d\ [n]$, on a : $a + c \equiv b + d\ [n]$ et $ac \equiv bd\ [n]$.

Dem: Il suffit d'écrire (a + c) – (b + d) = (a – b) + (c – d) somme de multiples de n, ainsi que ac – bd = a (c – d) + d (a – b) somme de multiples de n.

Petit théorème de Fermat

Théorème : Soit p un nombre premier. Alors :

1) $\forall n\in\mathbb{Z}$, $n^p \equiv n\ [p]$
2) **pour tout entier a non divisible par p, on a : $a^{p-1} \equiv 1\ [p]$ (th Fermat)**

Dem: 1) Soit P_n : " $n^p \equiv n\ [p]$ "

- P_0 vraie ? $0^p = 0$ car p > 1, donc on a bien $0^p \equiv 0\ [p]$. **P_0 est vraie**
- Supposons P_n vraie. P_{n+1} est-elle également vraie ? On a, d'après la formule du binôme,

$$(n + 1)^p – n^p – 1 = \sum_{k=1}^{p-1} \binom{p}{k} n^k .$$ Or p divise $\binom{p}{k}$ lorsque $k\in[\![1, p - 1]\!]$ car : $k\binom{p}{k} = p\binom{p-1}{k-1}$

Ainsi $(n + 1)^p \equiv n^p + 1\ [p]$. Mais comme P_n est vraie, on en déduit : $(n + 1)^p \equiv n^p + 1\ [p]$: **P_{n+1} vraie**

- Ainsi on a montré que P_0 est vraie et que, pour tout $n\geq 0$, P_n vraie entraine P_{n+1} vraie. Aussi, par le théorème de récurrence, on a : $\forall n \in\mathbb{N}$, P_n vraie i.e. $\forall n\in\mathbb{N}$, $n^p \equiv n\ [p]$

Ce résultat se prolonge au cas où n est un entier négatif. En effet, si p = 2, on a bien n et n^2 de même parité. Si p > 2, alors p est impair et donc $n^p = -|n|^p \equiv -|n|\ [p] \equiv n\ [p]$

2) Soit a un entier non divisible par p. On a, d'après le point précédent, p divise $a^p – a$ c'est-à-dire que p divise $a(a^{p-1} – 1)$. Or p est premier à a, donc d'après Gauss, p divise $a^{p-1} – 1$

Remarque: Il existe des nombres impairs composés q tels que $2^{q-1} \equiv 1\ [q]$. Par exemple 341 vérifie cette propriété. On dit que 341 est pseudopremier en base 2.

Il existe même des nombres q qui sont pseudopremiers pour toutes les bases premières à q : on appelle ces nombres les nombres de Carmichael. Le plus petit d'entre eux étant 561.

L'existence de ces nombres de Carmichael empêche celle d'un test de divisibilité pratique : p premier s'il divise $a^{p-1} – 1$ pour toute entier a entre 2 et p – 1 premier à p. Néanmoins si l'on cherche les nombres premiers compris entre deux valeurs données, plutôt que d'effectuer le test de primalité complet sur tous les nombres, on peut commencer par un test de divisibilité de $a^{p-1} – 1$ par p pour quelques valeurs de a, puis n'effectuer le test de primalité complet que sur les valeurs restantes.