les nombres *p*-adiques

par Mlle Audrey Cousin (1°S), Mlle Carine Joneaux (1°S), Mlle Sandra Lamberio (1°S), M. Olivier Chetkowski (TS), M. Loïc Jochault (TS), M. Adrien Sauvez (TS), élèves du **lycée Romain Rolland d'Ivry (94)** et M. Albert Andinaik, Mlle Hortense Disdero, Mlle Aline Bouyaud, élèves de 2nde du **lycée Pablo Picasso de Fontenay sous Bois (94)**

enseignants :
Mmes Monique Corlay, Claude Parreau
Mmes et M. Lise Bernigole, Jean-Paul Bernigole, Christiane Guedj

chercheur :
M. Olivier Piltant

coordination article : Andinaik Albert

Compte-rendu de parrainage :

Nombres p-adiques ? Que signifie ceci ? En vérité, la réponse est toute simple. Il s'agit de nombres que l'on prend dans une base de nombres premiers et infinis vers la gauche. Exemple : …125640 base 7. A travers l'étude des opérations usuelles, les élèves des lycées Pablo Picasso de Fontenay sur Seine et Romain Rolland d'Ivry nous ont permis de consolider nos connaissances sur les bases.

Félicitations aux élèves, qui connaissent leur sujet sur le bout des doigts.

NI — Les p-adiques, d'autres nombres ? 8

Le but est d'étudier des nombres inventés par les mathématiciens pour mieux comprendre les nombres habituels. Au lieu de 10 chiffres on en utilise p (p est choisi *premier*, c'est-à-dire qu'il n'est pas le résultat d'une multiplication de nombres plus petits que lui). Sur le même principe que l'écriture décimale avec virgule, on considère que les suites de chiffres (éventuellement illimitées vers la gauche) représentent des *nombres.*

Les opérations habituelles sur nombres entiers se généralisent-elles à ces nouveaux nombres ? Les divisions sont-elles possibles ?

Introduction.

Cette étude porte sur des nombres inventés par les arithméticiens, appelés nombres p-adiques . Voici leur définition :

Tout d'abord le « p » de p-adique désigne un nombre premier c'est-à-dire un entier qui n'est divisible que par 1 et par lui-même. Il représente la base de numération dans laquelle nous travaillons : p est le nombre de chiffres (ou de symboles) utilisés.

Exemple pour la base 5 ($p = 5$) : 0, 1, 2, 3, 4 sont les chiffres allant de 0 à p–1. Donc si on choisit un entier, quelconque, on peut l'écrire dans la base p. Par exemple si l'on choisit 206 comme entier, on peut écrire :

$$206 = (1\times5\times5\times5) + (3\times5\times5) + (1\times5) + 1$$

ou $206 = 1\times5^3 + 3\times5^2 + 1\times5 + 1$. On peut encore abréger cette écriture en $\overline{1311}^5$.

$\overline{1311}^5$ est l'écriture de 206 en base 5.

Donc en généralisant et en simplifiant on peut écrire tout nombre A en base p :

$$A = \overline{\ldots a_n \ldots a_4 a_3 a_2 a_1 a_0}^p$$

[NDLC : si ça ne porte pas à confusion, si le p a une valeur bien précisée par le contexte, il est tout de même plus simple d'écrire :

$$A = \ldots a_n \ldots a_4 a_3 a_2 a_1 a_0,$$

ce qui sera fait à partir de maintenant.]

On appelle « nombre p-adique » une telle écriture, illimitée vers la gauche, c'est-à-dire comportant une infinité de chiffres écrits de droite à gauche. Par exemple …1113132 (avec une infinité de 1 à gauche) est un nombre p-adique (quand $p \geq 4$).

Tout entier positif peut être vu comme un nombre p-adique, un peu particulier : on ajoute une infinité de zéros à gauche de son écriture en base p.

Maintenant que nous avons défini ce qu'est un nombre p-adique, nous pouvons vous exposer les règles d'addition et de recherche d'opposés, ainsi que les règles de multiplication et de recherche des inverses, avec pour finir les nombres périodiques.

L'addition des nombres p-adiques.

En règle générale, lorsqu'on additionne des nombres entiers usuels, exprimés en base 10, on *additionne terme à terme*. Par exemple, soient deux nombres *A* et *B*, on additionne les unités avec les unités, les dizaines avec les dizaines avec la retenue éventuelle provenant de la colonne précédente, … et ainsi de suite pour les autres termes du nombre.

Pour l'addition des nombres *p*-adiques, on procède de la même manière : on les additionne terme à terme, tout en appliquant le système des retenues. Les calculs se faisant de droite à gauche, on peut ainsi effectuer une addition.

Prenons un exemple : soient $p = 5$ et

A = …13241 avec une infinité de 1 à gauche,
B = …24122 avec une infinité de 2 à gauche.

On calcule donc en base 5 ; les chiffres a_i et b_i formant les nombres *p*-adiques *A* et *B* seront donc compris entre 0 et 4 : $0 \le a_i \le 4$ et $0 \le b_i \le 4$.

® : retenues

	®		®		
infinité de 1 à gauche	1	3	2	4	1
+ infinité de 2 à gauche	2	4	1	2	2
infinité de 3 à gauche	4	2	4	1	3

Explications :

On utilise les tables de l'addition en base 5 :

1 + 2 = 3 on pose le 3

4 + 2 = 11 on pose le 1 des unités et le 1 des "dizaines" constitue la retenue ®

® + 2 + 1 = 4 on pose le 4

3 + 4 = 12 on pose le 2 et le 1 devient une retenue

® + 1 + 2 = 4 on pose le 4.

1 + 2 = 3 et ainsi de suite pour les termes suivants …

Cas général

••••• ***Loi d'Audrey*** •••••••••••••••••••••••••••

Soient deux nombres *p*-adiques *A* et *B* écrits en base *p*.

$$A = \ldots a_n \ldots a_4 a_3 a_2 a_1 a_0$$
$$\text{et } B = \ldots b_n \ldots b_4 b_3 b_2 b_1 b_0$$

	… a_n	… a_4	a_3	a_2	a_1	a_0
+	… b_n	… b_4	b_3	b_2	b_1	b_0
	… a_n+b_n	… a_4+b_4	a_3+b_3	a_2+b_2	a_1+b_1	a_0+b_0
	… $+®_{n-1}$	…	$+®_3$	$+®_2$	$+®_1$	$+®_0$

La retenue $®_0$ correspond à la retenue éventuelle de la somme (a_0+b_0) ; elle est additionnée à la somme (a_1+b_1).

Le *n*-ème rang correspond à la somme de $(a_n+b_n) + ®_{n-1}$, l'éventuelle retenue de la colonne précédente.

••••••••••••••••••

Lorsque nous additionnons deux nombres *p*-adiques entiers naturels (donc où il n'y a à partir d'un certain rang *n*, que des zéros vers la gauche), alors l'addition de ces deux nombres revient à faire l'addition de deux entiers en base *p*.

Recherche des opposés.

Tout nombre p-adique A possède un unique opposé B tel que $A + B = 0$. On a trouvé une formule pour trouver B :

••••• ***Loi d'Hortense*** •••••••••••••••••••••••••

…	a_n	… a_4	a_3	a_2	a_1	a_0
+ …	b_n	… b_4	b_3	b_2	b_1	b_0
…	0	… 0	0	0	0	0

$a_0 + b_0 = p$ d'où $b_0 = p - a_0$
puis $a_1 + b_1 = p - 1$ $b_1 = p - 1 - a_1$
donc $a_n + b_n = p - 1$ $b_n = p - 1 - a_n$

••••••••••••••••••

Par cette formule on a trouvé que –1 en toute base s'écrit

$$\overline{\ldots(p-1)(p-1)(p-1)(p-1)}^{p}$$

Pour $p = 7$: –1 = …666666

Exemple en base 7 :

infinité de 3 *à gauche* 333321
infinité de 3 *à gauche* 333346
infinité de 0 *à gauche* 000000

On obtient une infinité de zéros. Chaque colonne donne une retenue de 1 mais le 1 n'apparaît jamais car « il est à l'infini ».

$b_0 = p - a_0 = 7 - 1 = 6$
puis $b_1 = p - 1 - a_1 = 6 - 2 = 4$
donc $b_2 = p - 1 - a_2 = 6 - 3 = 3$

Pour la soustraction au lieu d'effectuer $A - B$ on fait $A + (-B)$ en ayant cherché auparavant l'opposé de B car $A - B = A + (-B)$.

Multiplication des nombres p-adiques.

Par définition, la multiplication est une opération produit associant à deux nombres, l'un appelé multiplicande, l'autre multiplicateur, un troisième nombre appelé produit.

La multiplication de deux nombres p-adiques se fait suivant la technique habituelle de la multiplication de deux nombres entiers, comme on sait le faire habituellement. Lorsqu'on multiplie deux nombres p-adiques en base p, on obtient un nombre p-adique écrit dans la même base.

Prenons un exemple :

Prenons la base 5 : $p = 5$. On prendra pour multiplicande le nombre A = …12342 écrit avec une infinité de 1 vers la gauche et, pour multiplicateur le nombre B =…23412 écrit avec une infinité de 2 vers la gauche.

Voici la grille de **table de multiplication** modulo 5 :

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	11	13
3	0	3	11	14	22
4	0	4	13	22	31

On pose alors la multiplication et on multiplie terme à terme.

	.	.	1	2	3	4	2
×	.	.	2	4	3	1	2

On prend donc le nombre A et on le multiplie par le 2, en utilisant la grille de la table de multiplication en base 5, tout en appliquant le système des retenues.

.	.	.	11	.	1	2	3 4 2
×							2
.	.	.	22	.	3	0	2 3 4

On refait la même chose en multipliant par 1 et en décalant d'une colonne.

$$\begin{array}{r} \ldots 11\ldots 12342 \\ \times \qquad\qquad 1. \\ \hline \ldots 11\ldots 12342. \end{array}$$

On continue de la même manière pour les autres termes. Puis on additionne :

$$\begin{array}{r} \ldots\ldots\ldots\ldots 11\ \ldots\ldots 12342 \\ \times\ \ldots\ldots\ldots\ldots 22\ \ldots\ldots 23412 \\ \hline \ldots 2\ 2\ 2\ 2\ 2\ 2\ 2\ 2\ 3\ 0\ 2\ 3\ 4 \\ \ldots 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 2\ 3\ 4\ 2\ \bullet \\ \ldots 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 0\ 2\ 3\ \bullet\ \bullet \\ \ldots 3\ 3\ 3\ 3\ 3\ 4\ 3\ 1\ 3\ 1\ \bullet\ \bullet\ \bullet \\ \ldots 2\ 2\ 2\ 2\ 3\ 0\ 2\ 3\ 4\ \bullet\ \bullet\ \bullet\ \bullet \\ \ldots 2\ 2\ 2\ 3\ 0\ 2\ 3\ 4\ \bullet\ \bullet\ \bullet\ \bullet\ \bullet \\ \ldots 2\ 2\ 3\ 0\ 2\ 3\ 4\ \bullet\ \bullet\ \bullet\ \bullet\ \bullet\ \bullet \\ \ldots 2\ 3\ 0\ 2\ 3\ 4\ \bullet\ \bullet\ \bullet\ \bullet\ \bullet\ \bullet\ \bullet \\ \ldots \\ \hline (\ldots\ 1\ 4\ 1\ 4\ 1)\ \mathbf{4\ 3\ 4\ 3\ 3\ 0\ 0\ 4} \end{array}$$

Ici, avec les huit premières lignes, seuls les huit derniers chiffres de notre multiplication sont définitifs.

On peut donc en déduire un théorème, mais trop difficile à écrire car il y aurait trop de notations à adopter. [NDLC : j'ai une note de la rédaction, mais … *cette marge est trop étroite pour la contenir !*]

Grilles de multiplication modulo p.

La table modulo p est une table de multiplication dans laquelle on écrit seulement le dernier chiffre de la multiplication écrite en base p de A par B. (Dans ces tables, nous avons marqué en indice le chiffre de la retenue que l'on ajouterait pour calculer dans la numération à base p.)

Il existe deux cas :

- p **est premier ;**
- p **n'est pas premier.**

p est premier :

Il n'y a pas de zéro (autre que les résultats des nombres multipliés par zéro) car p n'est divisible que par 1 et lui-même.

Tous les chiffres de 0 à p–1 apparaissent une et une seule fois dans chaque ligne de la table (sauf celle de 0 évidemment). Si on obtenait dans la ligne de a, a différent de 0, deux fois le même résultat pour les colonnes b et c ($b > c$) on aurait $ab = ac$ + multiple de p. Donc p diviserait a ($b - c$) ce qui est impossible car p est premier, a et ($b - c$) ne sont pas des multiples de p car ils sont compris entre 1 et p–1. [et un nombre premier ne peut diviser un produit sans diviser l'un des facteurs au moins.]

$p = 5$ p premier

×	0	1	2	3	4
0	0	0	0	0	0
1	0	**1**	2	3	4
2	0	2	4	$_1\mathbf{1}$	$_1 3$
3	0	3	$_1\mathbf{1}$	$_1 4$	$_2 2$
4	0	4	$_1 3$	$_2 2$	$_3\mathbf{1}$

$p = 7$ p premier

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	**1**	2	3	4	5	6
2	0	2	4	6	$_1\mathbf{1}$	$_1 3$	$_1 5$
3	0	3	6	$_1 2$	$_1 5$	$_2\mathbf{1}$	$_2 4$
4	0	4	$_1\mathbf{1}$	$_1 5$	$_2 2$	$_2 6$	$_3 3$
5	0	5	$_1 3$	$_2\mathbf{1}$	$_2 6$	$_3 4$	$_4 2$
6	0	6	$_1 5$	$_2 4$	$_3 3$	$_4 2$	$_5\mathbf{1}$

***p* n'est pas premier :**

On trouve des zéros en plus des résultats des nombres multipliés par zéro, lorsque le chiffre est multiple d'un diviseur de p ou diviseur de p. Donc, quand p n'est pas premier, certains nombres n'ont pas d'inverse.

Par exemple : $5 \times 3 = 15 = 2 \times 6 + 3$. La retenue est 2 et le dernier chiffre 3. [On écrit $_2$3.]

$p = 6$ p non premier

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	**1**	2	3	4	5
2	0	2	4	$_1$**1**	$_1$2	$_1$4
3	0	3	$_1$0	$_1$3	$_2$0	$_2$3
4	0	4	$_1$2	$_2$0	$_2$4	$_3$2
5	0	5	$_1$4	$_2$3	$_3$2	$_4$**1**

Recherche des inverses (p premier*).*

L'inverse d'un nombre p-adique A, s'il existe, est un nombre B tel que $A \times B = 1$.

••••• ***Loi des inverses*** •••••••••••••••••••••••••

Tout nombre p-adique dont le dernier chiffre est différent de zéro admet un inverse et un seul.

••••••••••••••••••

Soit A un nombre non divisible par p (p premier). $A = \ldots a_n \ldots a_4 a_3 a_2 a_1 a_0$. On cherche donc l'inverse de A, $B = \ldots b_n \ldots b_4 b_3 b_2 b_1 b_0$ tel que :

	$\ldots a_n$	$\ldots a_4$	a_3	a_2	a_1	a_0	Nombre A
×	$\ldots b_n$	$\ldots b_4$	b_3	b_2	b_1	b_0	Inverse de A ?
	$\ldots .$	$\ldots .$	.	.	.	1	écriture de Ab_0
	$\ldots .$	$\ldots .$	.	.	c_1	0	écriture de Ab_1p
	$\ldots .$	$\ldots .$	.	c_2	0	0	écriture de Ab_2p^2
	$\ldots .$	$\ldots .$	c_3	0	0	0	écriture de Ab_3p^3
	⋮	⋮	⋮	⋮	⋮	⋮	⋮
	$\ldots$ 0	0	0	0	0	0	1

Nous allons donc chercher b_0 tel que le produit a_0b_0 se termine par 1. Pour cela, nous utilisons la grille qui nous permet de trouver b_0 correspondant à $a_0b_0 = 1$, modulo p.

• Si a_0 est le dernier chiffre de A (différent de 0), il existe un et un seul chiffre b_0 tel que $a_0b_0 = 1$ modulo p.

(En effet, ces grilles présentent toujours un seul **1** sur chaque ligne. Cela a été démontré : voir Loi d'Albert en annexe).
(Remarque : lorsque p n'est pas premier, ce n'est pas vrai.)

• $1 - Ab_0$ est multiple de p, donc $1 - Ab_0$ se termine par $c_1$0.

• On peut trouver un et un seul chiffre b_1 tel que$a_0b_1 = c_1$ modulo p (grâce à la table modulo p).

• $1 - Ab_0 - Ab_1p$ se termine par $c_2$00.

• On peut trouver un et un seul chiffre b_2 tel que$a_0b_2 = c_2$ modulo p (grâce à la table modulo p).

On a démontré que l'on pouvait trouver b_0, b_1 et b_2.

Par récurrence, on démontre que, si on trouve un b_n jusqu'à un certain rang, on peut trouver un b_{n+1}.

En effet :

• $1 - Ab_0 - Ab_1p - Ab_2p^2 - \ldots - Ab_np^n$ se termine par $c_{n+1}00\ldots0000$ (n+1 zéros).

• On peut trouver b_{n+1} tel que$a_0b_{n+1} = c_{n+1}$ modulo p (grâce à la table modulo p).

$$1 = Ab_0 + Ab_1p + Ab_2p^2 + \ldots + Ab_np^n$$
$$1 = A(b_0 + b_1p + b_2p^2 + \ldots + b_np^n)$$
$$1 = AB \text{ et } B = \ldots b_n \ldots b_4b_3b_2b_1b_0$$

Prenons un exemple :

Cherchons l'inverse du nombre p-adique A = …12231223 écrit avec une infinité de "1223" à gauche. Prenons p = 7. [On utilise la grille de multiplication en base 7.]

☞ Première étape :

```
   . . . 1223 . . . 12231223
×                        b0
-------------------------------

-------------------------------
   . . . . .  0000000000001
```

Nous effectuons le premier calcul expliqué auparavant de telle sorte que $3\times b_0 = 1$. Dans la grille, nous trouvons $b_0 = 5$.

☞ Deuxième étape : nous cherchons maintenant le chiffre b_1.

```
   . . . 1223 . . . 12231223
×                       b1 5
-------------------------------
   . . . . . . . . . . 64516451    ← A × 5
                              .

-------------------------------
   . . . . .  0000000000001
```

On effectue $1 - A \times 5$. Le résultat de la soustraction se termine par un 2. Donc, à l'aide de la grille, nous cherchons b_1 de telle sorte que $3 \times b_1$ se termine par un 2. On obtient alors $b_1 = 3$.

☞ Troisième étape : nous cherchons maintenant le chiffre b_2.

```
   . . . 1223 . . . 12231223
×                       b2 35
-------------------------------
   . . . . . . . . . . 64516451    ← A × 5
   . . . . . . . . . 40024002.     ← A × 3 × 7
                              .

-------------------------------
   . . . . .  0000000000001
```

De nouveau, nous cherchons le dernier chiffre du résultat de $1 - Ab_0 - Ab_1p$. Nous trouvons 2. Puis nous cherchons b_2 de telle sorte que $b_2 \times 3$ se termine par un 2. Donc, $b_2 = 3$.

☞ Ensuite, les prochaines étapes sont répétitives et il n'est peut-être pas nécessaire de les répéter une à une. Il faut simplement savoir qu'il faut soustraire à chaque fois, le produit du nombre *p*-adique *A* du produit précédent.

On obtient finalement :

```
   . . . 1223 . . . 12231223
×              . . . 5650335
-------------------------------
   . . . . . . . . . . 64516451 ← A×5
   . . . . . . . . . 40024002.  ← A×3×7
   . . . . . . . . 40024002. .  ← A×3×7×7
   . . . . . . . 00000000. . .  ← A×0×7×7×7
   . . . . . . 64516451. . . .  ← A×5×7×7×7×7
     et ainsi de suite . . . .
 (?) etius ed isnia te . . . .
-------------------------------
   . . . . .  0000000000001
```

[NDLR : En pratique, pour calculer b_{i+1}, on choisit tout d'abord le dernier chiffre (= le plus à droite), disons c_{i+1}, du produit $A \times b_{i+1}$ de telle manière que la somme des chiffres figurant au-dessus dans la même colonne, augmentée de la retenue éventuelle de la somme de la colonne précédente, donne pour résultat 0 (modulo 7) ; on utilise ensuite la table de multiplication pour déterminer b_{i+1} de sorte que $b_{i+1} \times 3 = c_{i+1}$.]

Division des p-adiques.

Cette méthode de recherche des inverses nous a aussi permis de faire des divisions entre deux nombres *p*-adiques, car diviser par un nombre *A*, revient à multiplier par son inverse.

Nombre p-adique périodique.

Les nombres *p*-adiques périodiques sont rationnels, c'est-à-dire sont quotient de deux entiers *p*-adiques. Pour voir cela, on utilise –1 qui s'écrit

$$\ldots(p-1)(p-1)(p-1)$$

en base *p*. En base 7 ($p = 7$), nous avons $-1 = \ldots6666$. Avec ce nombre, on peut transformer les nombres *p*-adiques périodiques de base 7.

Soit *n* le nombre *p*-adique …21212121 en base $p = 7$. *n* peut s'écrire aussi ainsi :

$$n = 21 \times \ldots01010101$$

–1 peut s'écrire également en base 7 :

$$-1 = 66 \times \ldots01010101$$

donc $n / (-1) = 21 / 66$ (écrits en base 7)
d'où $n = -21 / 66$ (écrits en base 7)

Un nombre *p*-adique périodique à partir d'un certain rang peut se transformer en *p*-adique périodique par addition ou soustraction :

Soit *n*' le nombre *p*-adique *n*' = …306306221 en base 7. Nous observons que

$$\ldots306306221 + 055 = \ldots306306306.$$

Conclusion.

Voilà ce que nous avons obtenu au cours de cette année. Nous avons remarqué que nous pouvons faire plus de choses avec les nombres *p*-adiques qu'avec les nombres entiers (par exemple les soustractions, les inverses). Nous avons lu, dans un article de *la Recherche*, que les nombres *p*-adiques sont d'une très grande utilité.

Dans certains cas, tel celui du « théorème de Fermat » (récemment démontré par Wiles, voir le Glossaire en fin de volume), la démonstration utilise plusieurs fois les nombres *p*-adiques de façon essentielle, alors que l'énoncé ne porte que sur des entiers. Pour le comprendre, il faut remarquer que pour qu'une équation ait une solution entière, il est necessaire qu'elle ait une solution *p*-adique et cela pour chaque *p* premier.

De plus les méthodes *p*-adiques n'interviennent pas qu'en mathématiques pures. On les voit maintenant apparaître dans des domaines inattendus : la physique théorique, les probabilités [NDLC : tiens ? Je croyais que c'étaient des maths pures ?] et peut-être découvrira-t-on un lien étroit avec la réalité physique.

Annexe

— Afin de démontrer que tout nombre non divisible par p a un inverse modulo p.

••••• ***Loi d'Albert*** ••••••••••••••••••••••••••••
Soit n, p premiers entre eux avec $n < p$; il existe a, b entiers tels que $a\,n + b\,p = 1$.
••••••••••••••••••

D'abord, **prenons un exemple.**

Exemple : n =13 et p = 59 ; soit à résoudre $13\,a + 59\,b = 1$.

$59 = 13 \times 4 + 7$

$$13\,a + b\,(13 \times 4 + 7) = 1$$
$$13\,(a + 4\,b) + 7\,b = 1$$
$$13\,a' + 7\,b = 1 \text{ avec } a' = a + 4\,b$$

On passe du couple (13, 59) au couple (13, 7).

$13 = 7 \times 1 + 6$

$$(7 \times 1 + 6)\,a' + 7\,b = 1$$
$$6\,a' + 7\,(a' + b) = 1$$
$$6\,a' + 7\,b' = 1 \text{ avec } b' = a' + b$$

On passe du couple (13, 7) au couple (6, 7).

$7 = 6 \times 1 + 1$

$$6(a' + b') + b' = 1$$
$$6a'' + b' = 1 \text{ avec } a'' = a' + b'$$

On passe du couple (6, 7) au couple (6, 1).

On prend $a'' = 0$ et $b' = 1$.
On trouve $a' = -1$; $b = 2$; $a = -9$.

Vérification : $-9 \times 13 + 2 \times 59 = 1$
$-117 + 118 = 1$
donc 13 a pour inverse –9 modulo 59.

Cas général

Pour résoudre ce problème, nous le ramenons donc au même problème mais avec des entiers n et p de plus en plus petits. Il nous faut effectuer pour cela une suite de transformations :

1.— (n, p) donne (n, p') avec $p' = p - k\,n$ et $0 < p' < n$

2.— (n, p') donne (n', p') avec $n' = n - k'\,p'$ et $0 < n' < p'$

Remarque : on peut avoir $p' = 0$ uniquement dans le cas où $n = 1$ puisque p et n sont premiers entre eux. On s'arrête alors au stade 1.

on peut avoir $n' = 0$ uniquement dans le cas où $p' = 1$ (de même n' et p' sont premiers entre eux ; voir plus loin).

donc on arrive à (1, 0) ou à (0, 1) ou à (n', p') avec $n' < p' < n < p$. Sinon on a un nouveau couple (n', p') avec $n' < p'$ et n', p' premiers entre eux :

Si on a $p' = \lambda\,p''$ et $n' = \lambda\,n''$ d'où
$p = k\,n + \lambda\,p''$
$n = k'\lambda\,p'' + n''\ \lambda = \lambda\,(k'p'' + n'')$
$p = k\ \lambda\ (k'\,p'' + n'') + \lambda\,p''$
$p = \lambda\,(k\,(\,k'\,p'' + n'') + p'')$

p et n sont premiers entre eux donc $\lambda = 1$ et donc p' et n' sont premiers entre eux.

En effectuant plusieurs fois les transformations précédentes on arrivera soit à (0,1) soit à (1, 0).

Réciproquement : si on a trouvé a' et b' tels que $a'\,n' + b'\,p' = 1$, on peut trouver a et b tels que $a\,n + b\,p = 1$. Donc on peut, à partir de (1, 0) ou (0, 1), revenir jusqu'à (n, p) et résoudre le problème initial.

Démonstration :

$a'\,(n - k'\,p') + b'\,p' = 1$
$a'\,n + (b' - a'k')\,p' = 1$
$a'\,n + (b' - a'k')\,(p - kn) = 1$
$(a' - b'k - a'k'k)\,n + (b' - a'\,k')\,p = 1$ avec
$a = a' - b'k - a'k'k$ et $b = b' - a'\,k$.