II. ESSAI

THÉORÈME DE BACHET

I. Congruences. Théorèmes de Fermat et de Wilson

(En réponse à une demande formulée par un collègue, A. Buquet *nous donne ici une démonstration difficilement accessible dans les ouvrages courants, et n'utilise que les éléments d'arithmétique de la classe de Mathématiques Elémentaires. Nous pensons que cette étude pourra intéresser d'autres collègues que l'auteur de la question relative au « théorème de Bachet »).*

Pour exprimer que deux nombres entiers a et b ont le même reste de division par un même troisième c, il est équivalent d'affirmer que a est un multiple de c augmenté de b ou que a et b sont congrus suivant le module c, ce qui est noté de façon courante respectivement par $a = \mathcal{M}\, c + b$ ou $a \equiv b \pmod{c}$.

Un des chapitres fondamentaux de la théorie des nombres est l'étude des congruences à inconnues lorsque le module est donné. Si la notation des congruences est employée ici, il n'est fait aucun appel à des résultats, même classiques, non montrés directement à l'aide des éléments d'arithmétique du programme de Mathématiques Elémentaires.

Résoudre la congruence $f(x) \equiv 0 \pmod{P}$ où $f(x)$ est un polynôme de degré n à coefficients entiers positifs, négatifs ou nuls : $a_n x^n + \ldots + a_1 x + a_0$, c'est trouver toutes les valeurs entières qu'il faut attribuer à x pour que le polynôme prenne une valeur numérique multiple du module entier P.

Si une valeur x_0 convient, il en est de même pour tous les termes de la progression arithmétique de raison P de terme général $u_k = x_0 + KP$, illimitée dans les deux sens, car $f(x_0 + KP) - f(x_0)$ est manifestement multiple de P quel que soit l'entier K. On dit que les termes de cette progression forment *une classe de solutions*. On peut se borner, pour résoudre une telle congruence, à essayer les termes de la suite $(0, 1, 2, \ldots, P-1)$. Les propriétés de telles congruences sont les plus simples lorsque le module P est premier absolu ; c'est ce qui sera toujours supposé par la suite.

Théorème 1. — *Tout polynôme de degré n à coefficients entiers*

$$f(x) = a_n x^n + \ldots + a_1 x + a_0$$

multiple d'un nombre premier P *pour n valeurs distinctes* $x_1, x_2, \ldots, x_n$ *prises dans la suite* $(0, 1, 2, \ldots, P-1)$ *peut être mis sous la forme*

$$f(x) = a_n g_n(x) + b_n g_{n-1}(x) + b_{n-2}\, g_{n-2}(x) + \ldots + b_2 g_1(x) + b_1$$

où $b_1, b_2, \ldots, b_n$ *sont nuls ou multiples de* P *et* $g_i(x)$ *désigne le produit*

$$(x - x_1)\,(x - x_2) \ldots (x - x_i).$$

Divisons $f(x)$ par $(x - x_1)$; on a $f(x) = (x - x_1)\, Q_1(x) + b_1$. $Q_1(x)$ est un polynôme à coefficients entiers et b_1, égal à $f(x_1)$, est multiple de P ou occasionnellement nul. Si l'on remplace x par x_2 dans cette identité, il vient

$$f(x_2) = (x_2 - x_1)\, Q_1(x_2) + b_1 ;$$

$f(x_2)$ et b_1 étant multiples de P, il en est de même du produit $(x_2 - x_1)\, Q_1(x_2)$. Comme le facteur $x_2 - x_1$, qui est en valeur absolue au plus égal à $P - 1$ ne peut être multiple de P, c'est l'autre facteur $Q_1(x_2)$ qui est égal à un multiple b_2 de P. Pour une raison analogue, $Q_1(x)$ est aussi multiple de P pour $x = x_3, x_4, \ldots x_n$. Divisons $Q_1(x)$ par $x - x_2$, il vient $Q_1(x) = (x - x_2)\, Q_2(x) + b_2$, le quotient $Q_2(x)$ étant aussi à termes entiers.

$Q_2(x_2)$ et b_2 étant multiples de P, il en est de même de $(x_3 - x_2)\, Q_2(x_3)$;

$x_2 - x_3$ ne pouvant l'être, c'est le facteur $Q_2(x_3)$ qui est égal à un multiple b_3 de P (s'il n'est pas nul). $Q_3(x)$ est également multiple de P pour $x = x_4, x_5, \ldots, x_n$.

Par divisions successives on définit des quotients $Q_1(x)$, $Q_2(x)$, .., $Q_n(x)$ de degrés $n-1$, $n-2$, ..., 0 et des multiples de P : b_1, b_2, ..., b_n liés par la relation de récurrence $Q_{i-1}(x) = (x - x_i)\, Q_i(x) + b_i$.

Le dernier quotient $Q_n(x)$, de degré nul, est égal à A_n. L'élimination de $Q_1(x)$, $Q_2(x)$, .., $Q_{n-1}(x)$ conduit à la relation de l'énoncé.

THÉORÈME 2. — *Si un polynôme à coefficients entiers de degré n est multiple d'un nombre premier* P *pour plus de n valeurs distinctes de x prises dans la suite* (0, 1, 2, .., P — 1) *ses coefficients sont nuls ou multiples de* P.

Dans l'identité du théorème précédent remplaçons x par une valeur supplémentaire x_{n+1} rendant aussi $f(x)$ multiple de P. Le produit

$$a_n(x_{n+1} - x_1)(x_{n+1} - x_2)\ldots(x_{n+1} - x_n)$$

doit être multiple de P. Ce ne peut être aucun des facteurs $(x_{n+1} - x_i)$. c'est donc a_n et le théorème s'ensuit.

THÉORÈME 3. — *La congruence* $f(x) \equiv 0$ (*mod.* P) *où* P *est un nombre premier et* $f(x)$ *un polynôme de degré n dont les termes sont des nombres entiers non tous multiples de* P *ou nuls, ne peut admettre plus de n classes distinctes de solutions.*

Les P classes distinctes possibles comprennent les P termes de la suite (0, 1, 2, .., P — 1). S'il existait plus de n classes distinctes de solutions, on se trouverait dans les conditions du théorème précédent et tous les coefficients de $f(x)$ seraient, en contradiction avec l'hypothèse, tous multiples de P ou nuls.

Ainsi, on peut dire qu'en général une congruence de degré n à module premier admet au plus n classes de solutions distinctes. Si ce maximum est atteint de façon banale avec la congruence $g(x) \equiv$ (mod. P) avec $g(x) = (x-1)(x-2)\ldots(x-n)$, il est aussi atteint dans le cas du polynôme $x^{P-1} - 1$, comme cela résulte du

THÉORÈME 4 (DE FERMAT). — *Etant donné un nombre premier* P *et un nombre a non multiple de* P. *l'expression* $a^{P-1} - 1$ *est multiple de* P.

Divisons par a les P — 1 produits a, $2a$, $3a$, .., $(P-1)a$, ce qui introduit des quotients et des restes définis par les relations

$$(1) \qquad ka = Pq_k + r_k \qquad (k = 1, 2, \ldots, P-1).$$

Deux restes quelconques, r_i et r_j sont différents, car leur égalité entraînerait

$$ia - Pq_i = ja - Pq_j \quad \text{et} \quad (i-j)\,a = P(q_i - q_j),$$

P devrait alors diviser a ou $(i-j)$ ce qui est impossible, $i-j$ étant en valeur absolue inférieur à P. Les restes r_k en nombre P — 1 sont donc dans leur ensemble les nombres 1, 2, .., P — 1. En multipliant membre à membre les égalités (1) on obtient $(P-1)!\, a^{P-1} = \mathcal{M}P + (P-1)!$ et $(P-1)!\,(a^{P-1} - 1) = \mathcal{M}P$, ce qui entraîne $a^{P-1} - 1 = \mathcal{M}P$.

THÉORÈME 5 (DE WILSON). — *Si* P *est un nombre premier, l'expression* $(P-1)! + 1$ *est multiple de* P.

Les deux congruences $f(x) = x^{P-1} - 1 \equiv 0$ (mod. P) et

$$g(x) = (x-1)(x-2)\ldots(x-P+1) \equiv 0 \text{ (mod. P)}$$

admettent l'une et l'autre les P — 1 classes de solutions distinctes

$$KP + 1,\ KP + 2,\ \ldots,\ KP + P - 1$$

et il en est de même de la congruence de degré P — 2

$$h(x) = g(x) - f(x) \equiv 0 \text{ (mod. P)}.$$

D'après le théorème 2, tous les coefficients du polynôme $h(x)$, supposé ordonné, sont multiples de P ou nuls. Si P est impair, il s'ensuit que la somme des termes de la suite (1, 2, 3, .., P — 1) est multiple de P, ainsi que les sommes de leurs produits 2 à 2, 3 à 3, .., P — 2 à P — 2. Il en est de même du terme constant $(P-)! + 1$, ce qui démontre la proposition, qui est aussi vérifiée pour P = 2, puisque $1! + 1 = 2$.

II. Restes et résidus quadratiques

Une congruence du second degré de la forme particulière $x^2 - a \equiv 0$ suivant un module premier impair $P = 2N + 1$ admet au plus deux classes de solutions. La discussion de sa possibilité suivant les valeurs de a conduit à une notion très importante en théorie des nombres. *On appelle reste quadratique du nombre premier impair* $P = 2N + 1$ *tout nombre* R *de la suite* $(1, 2, \ldots, 2N - 1, 2N)$ *pour lequel* $x^2 - R = \mathcal{M}P$, *c'est-à-dire pour lequel la congruence* $x^2 \equiv R$ *est possible*. On appelle *résidu quadratique* tout terme de la progression $R + KP$, progression nommée *classe résiduelle*. *On appelle non reste tout nombre* S *de la même suite* $(1, 2, \ldots, 2N)$ *pour lequel la congruence* $x^2 \equiv S$ *est impossible*. La congruence est également impossible pour tous les termes de la progression $s = S + KP$. Tout terme s est nommé *non résidu*, leur ensemble forme *une classe non résiduelle*.

Pour $P = 3$ on a une classe résiduelle $3K + 1$ et une classe non résiduelle $3K + 2$ (ou $3K - 1$) ; pour $P = 7$ on a trois classes résiduelles $7K + 1$, $7K + 2$, $7K + 4$ et trois classes non résiduelles $7K + 3$, $7K + 5$, $7K + 6$. Pour $P = 13$ on a six restes 1, 3, 4, 9, 10, 12 et six non restes 2, 5, 6, 7, 8, 11.

Théorème 6. — *Les restes de division par un nombre premier impair* $P = 2N + 1$ *des carrés des nombres de* 1 *à* N *sont distincts et sont dans l'ordre inverse les restes de division par* P *des carrés des nombres de* $N + 1$ *à* $2N$. *Le nombre* P *admet* N *classes résiduelles et* N *classes non résiduelles*.

Il suffit d'étudier les restes R_i de division par P des carrés consécutifs de 1^2 à $(2N)^2$, car $(n + KP)^2$ donne le même reste que n^2. Soient $R_1, R_2, \ldots, R_n$ les restes de division relatifs à la première moitié de ces carrés. Ils sont tous distincts, car $R_i - R_j = (i - j)(i + j)$ ne peut être multiple de P, $i + j$ et $|i - j|$ étant au plus égaux à $2N - 1$ sont inférieurs à P. Chacun d'eux est égal à un seul des restes $R_{N+1}, \ldots, R_{2N}$ provenant de la seconde moitié des carrés, car de

$$(2N + 1 - i)^2 - i^2 = (2N + 1)(2N + 1 - 2i) = \mathcal{M}P,$$

suit $R_i = R_{2N+1-i}$. Il y a donc exactement N restes et par suite N non restes et autant de classes résiduelles et non résiduelles.

Théorème 7. — *Pour qu'un nombre* r *soit résidu quadratique d'un nombre premier impair* $P = 2N + 1$, *il faut et il suffit que* $r^N - 1$ *soit multiple de* P ; *pour qu'un nombre* s *soit un non résidu, il faut et il suffit que* $s^N + 1$ *soit multiple de* P.

Il suffit de faire la démonstration pour un reste et un non reste puisque

$$(n + KP)^N \pm 1 = \mathcal{M}P + n^N \pm 1.$$

Pour la totalité des restes et des non restes, c'est-à-dire pour nombre a de la suite $(1, 2, \ldots, 2N)$, et d'après le théorème 4 de Fermat $a^{2N} - 1 = \mathcal{M}P$ ou encore $(a^N - 1)(a^N + 1) = \mathcal{M}P$. L'un des facteurs $a^N - 1$ et $a^N + 1$ est donc multiple de P et jamais les deux puisque leur différence 2 ne peut être multiple de P.

Si a est un reste R_i, on a $i^2 = \mathcal{M}P + R_i$ entraînant $R_i^N = \mathcal{M}P + i^{2N}$ et $R_i^N - 1 = \mathcal{M}P + i^{2N} - 1$. D'après le théorème de Fermat, $i^{2N} - 1$ est multiple de P et il en est donc de même de $R_i^N - 1$. La congruence $x^N - 1 \equiv 0 \pmod{P}$ admet donc pour solutions les N classes résiduelles distinctes $KP + R_i$ et ne peut admettre d'après le théorème 3 d'autres solutions. Lorsque a est égal à un non reste S le produit $(S^N - 1)(S^N + 1)$ est multiple de P sans que $S^N - 1$ le soit. C'est le facteur $S^N + 1$ qui est multiple de P et la totalité des classes de solutions de la congruence $x^N + 1 \equiv 0 \pmod{P}$ est fournie par les N classes non résiduelles.

Théorème 8. — *Le produit de deux résidus ou de deux non résidus est un résidu ; le produit d'un résidu par un non résidu est un non résidu.*

Soient r et r' deux résidus et s et s' deux non résidus ; on a

$$r^N = \mathcal{M}P+1,\ r'^N = \mathcal{M}P+1,\ s^N = \mathcal{M}P-1,\ s'^N = \mathcal{M}P-1$$

d'où l'on déduit par multiplication :

$$(rr')^N = \mathcal{M}P+1,\ (ss')^N = \mathcal{M}P+1,\ (rs)^N = \mathcal{M}P-1$$

ce qui, d'après le théorème 7 démontre la proposition.

III. Décomposition en somme de carrés

Théorème 9. — *Un produit de sommes de deux carrés est une somme de deux carrés ; un produit de sommes de quatre carrés est une somme de quatre carrés.*

Cela résulte des identités

$$(a^2+b^2)\ (a'^2+b'^2) = (aa'+bb')^2 + (ab'-a'b)^2,$$

$$(a^2+b^2+c^2+d^2)\ (a'^2+b'^2+c'^2+d'^2) = (aa'+bb'+cc'+dd')^2 + (ab'-ba'-cd'+dc')^2 + (ac'+bd'-ca'-db')^2 + (ad'-bc'+cb'-da')^2.$$

Théorème 10. — *Si le produit d'un nombre premier* P *par un nombre n inférieur à* P *est égal à une somme de deux carrés, il existe un nombre n' inférieur à n tel que le produit* Pn' *soit égal à une somme de deux carrés.*

Soit $Pn = a^2 + b^2$; en divisant a et b par n et en prenant les restes minima en valeur absolue on obtient des nombres a', b', a'', b'' vérifiant les conditions

$$a'' = a - na',\ b'' = b - nb',\ |a''| \leqslant \frac{n}{2},\ |b''| \leqslant \frac{n}{2},\ \text{d'où}\ a''^2 + b''^2 \leqslant \frac{n^2}{2} < n^2.$$

Alors $a''^2 + b''^2 = a^2 + b^2 - 2(aa' + bb')n + (a'^2 + b'^2)n^2$ est égal à un multiple nn' de n si $n' = P - 2(aa' + bb') + (a'^2 + b'^2)n < n$. Le produit P$n'$ est bien une somme de deux carrés,

$$Pn' = P^2 - 2(aa' + bb')P + (a^2 + b^2)\ (a'^2 + b'^2) = (P - aa' - bb')^2 + (ab' - a'b)^2$$

Il s'agit bien de deux carrés et non d'un seul (cas où la démonstration serait illusoire), car si l'un des deux carrés était nul, l'autre serait un multiple KP de P, ce qui entraînerait $n' = K^2P \geqslant P$ et $n > n' \geqslant P$ en contradiction avec l'hypothèse.

Théorème 11. — *Si un nombre premier* P *divise une somme de deux carrés inférieure à son carré* P^2, *il est lui-même égal à une somme de deux carrés.*

Il existe alors un nombre $n < P$, tel que $Pn = a^2 + b^2$ et par suite on est assuré de l'existence d'un nombre $n_1 < n$ et d'une décomposition $Pn_1 = a^2_1 + b^2_1$. Le théorème est vérifié si $n_1 = 1$, sinon on peut trouver n_2 tel que $n_2 < n_1 < n < P$ et une décomposition $Pn_2 = a^2_2 + b^2_2$ avec une conclusion analogue. On peut ainsi former une suite décroissante $n_1, n_2, \ldots$ qui se termine par un terme égal à 1, ce qui vérifie la proposition.

Théorème 12. — *Si le produit d'un nombre premier* P *par un nombre entier n inférieur à* P *est égal à une somme de 2, 3 ou 4 carrés, il existe un nombre entier n' inférieur à n, tel que le produit* Pn' *soit égal à une somme de 2, 3 ou 4 carrés.*

Soit $Pn = a^2 + b^2 + c^2 + d^2$; en divisant a, b, c, d par n et en prenant les restes minima en valeur absolue, on obtient quatre quotients a', b', c', d' et quatre restes a'', b'', c'', d'' vérifiant les conditions

$a'' = a - na'$, $b'' = b - nb'$, $c'' = c - nc'$, $d'' = d - nd'$ où $|a''|$, $|b''|$, $|c''|$, $|d''|$ sont inférieurs ou égaux à $\frac{n}{2}$. La somme $\Sigma a''^2 = \Sigma a^2 - 2n\Sigma aa' + n^2\Sigma a'^2$ est égale à un multiple nn' de $n' = P - 2\Sigma aa' + n\Sigma a'^2 \leqslant n$.

Si $n' < n$, il vient

$$Pn' = (p - \Sigma aa')^2 + (ab' - ba' - cd' + dc')^2 + (ac' + bd' - ca' - db')^2 + (ad' - bc' + cb' - da')^2.$$

Si $n' = n$, cette décomposition ne peut convenir. Dans ce cas n est un nombre pair $2n''$ et les nombres a, b, c, d se répartissent en deux couples de même parité. Si

a et b sont de même parité, il en est de même de c et d. A la place de n' on prendra $n'' = \frac{n}{2} < n$, avec la décomposition

$$Pn'' = \left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2 + \left(\frac{c+d}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2.$$

Les carrés sont au nombre de 2, 3 ou 4 ; s'il n'y avait qu'un seul carré (cas où la démonstration serait illusoire), ce carré serait un multiple KP de P. On aurait n' ou $n'' = K^2P \geqslant P$ et n ne serait pas inférieur à P.

THÉORÈME 13. — *Si un nombre premier* P *divise une somme de 2, 3 ou 4 carrés inférieure à son carré* P^2, *il est lui-même égal à une somme de 2, 3 ou 4 carrés.*

On peut déterminer une suite de décompositions $Pn_i = \Sigma a^2_i$, où les nombres n_1, n_2, ... vont en décroissant, le dernier étant égal à 1.

THÉORÈME 14. — *Tout nombre premier de la forme* $4n + 1$ *est égal à une somme de deux carrés.*

Pour un tel nombre premier $P = 2N + 1 = 4n + 1$, N est pair et puisque $(-1)^N = (-1)^{2n} = 1$, d'après le théorème 7 le nombre -1 est un résidu quadratique. Le nombre $P - 1$ est donc un reste et il existe un nombre i (théorème 6) au plus égal à N tel que $i^2 - (P - 1) = \mathcal{M}P$, ou encore $i^2 + 1 = \mathcal{M}P$. Le nombre P qui divise $i^2 + 1 \leqslant N^2 + 1 < P^2$ se trouve dans les conditions d'application du théorème 11, il est somme de deux carrés.

THÉORÈME 15. — *Tout nombre premier de la forme* $4n + 3$ *est égal à une somme de 3 ou 4 carrés.*

Pour un tel nombre premier $P = 2N + 1 = 4n + 3$, $N = 2n + 1$ est impair et $(-1) = -1$. D'après le théorème 7, le nombre -1 est un non résidu et, par suite, $P - 1$ est un non reste.

Dans la suite (1, 2, 3, .., 2N) le premier terme est un reste et le dernier $2N = P - 1$ est un non reste. Il existe donc deux termes consécutifs h et $h + 1$ dont le premier est un reste et le second un non reste, le produit des deux non résidus $h + 1$ et -1 soit $-h - 1$ est, d'après le théorème 8, un résidu. Il existe donc, d'après le théorème 6, deux nombres i et j au plus égaux à N, tels que

$$i^2 - h = \mathcal{M}P, \quad j^2 + h + 1 = \mathcal{M}P, \text{ d'où } i^2 + j^2 + 1 = \mathcal{M}P.$$

Avec $P = 7$ on pourra prendre $h = 2$, $i = 3$, $j = 2$, $i^2 + j^2 + 1 = 7 \times 2$.

Comme $i^2 + j^2 + 1 \leqslant N^2 + N^2 + 1 < P^2$, le théorème 15 est applicable et P est somme de 2, 3 ou 4 carrés. Mais il ne peut être la somme de deux carrés seulement ; ces carrés de parités différentes conduiraient à

$$P = (2p + 1)^2 + (2q)^2 = 4k + 1 \neq 4n + 3.$$

THÉORÈME 16 (DE BACHET). — *Tout nombre entier est égal à une somme de quatre carrés, dont certains peuvent être nuls.*

Tout nombre entier N peut être décomposé en un produit de facteurs premiers qui sont, soit 2, soit de la forme $4n + 1$, soit de la forme $4n + 3$, tous décomposables en sommes de 2, 3 ou 4 carrés. D'après le théorème 9, N peut être décomposé en somme de 2, 3 ou 4 carrés. Le plus petit nombre demandant 4 carrés est

$$7 = 2^2 + 1^2 + 1^2 + 1^2.$$

A. BUQUET, *professeur au Lycée, St-Quentin (Aisne).*

A. BUQUET nous donne en outre les références suivantes :

1° Démonstration élémentaire du théorème de Bachet, par A. MATROT (Vuibert et Nony).

2° Exercices d'analyse numérique, par V.-A. LEBESGUE, 1859 (Leiberck-Faraguet, 11, rue de Seine, Paris).

3° Théorie des nombres ordinaires et algébriques, par H. LAURENT (Naud, Paris).

D'autre part, notre collègue MARTY (Nay, Basses-Pyrénées) nous indique celles-ci :

4° Traité d'arithmétique, par HUMBERT, 1893 (Nony et C^ie).

5° Les nombres premiers, par E. BOREL, collection « Que sais-je ? », n° 571, P.U.F.