27. Calcul des diviseurs premiers.

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **6 (1960)**

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **21.07.2024**

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

CHAPITRE IV

CRIBLES

27. Calcul des diviseurs premiers.

Les propriétés des idéaux canoniques, dans un corps quadratique, et des idéaux réduits, peuvent être interprétées sous la forme de propriétés des *nombres premiers* (rationnels), analogues à celles du « crible d'Eratosthène ». On reprend, en se plaçant à ce point de vue, les constructions et définitions déjà indiquées, en sorte que le chapitre actuel peut être considéré comme indépendant des autres.

On forme, pour les valeurs entières de x, croissantes à partir de 0, *la suite des valeurs d'un trinôme du second degré :*

$$F(x) = x^2+Sx+N; \quad \begin{cases} S = -1; & N \text{ quelconque;} \\ S = 0; & N \not\equiv +1; \pmod 4; \end{cases}$$

sous la réserve que *le discriminant* $D = S^2-4N$, *n'ait pas de facteur carré*, à l'exclusion de 4 (si $S = 0$); et ne soit pas égal à $+4$.

On se propose de chercher *les facteurs premiers qui sont des diviseurs des valeurs de cette suite.*

A cet effet, on détermine un *rang* r, tel que pour tout x, au moins égal à r:

$$|F(x)| < (2x-S)^2.$$

Cette condition est d'ailleurs équivalente, suivant le cas (**25**) à:

$$D>0; \quad 5(2x-S)^2>D \Leftrightarrow x\geqslant r;$$
$$D<0; \quad 3(2x-S)^2>|D| \Leftrightarrow x\geqslant r$$

(dans le cas de D positif, $F(x)$ est négatif, notamment pour toutes les valeurs de x strictement inférieures à r).

On appelle **racine minimum** $\bar{c}_p$, d'un nombre (entier rationnel) premier p, *la plus petite valeur entière de* x (nulle ou positive) s'il en existe, *telle que* $|F(x)|$ *soit divisible par* p.

Les valeurs de x pour lesquelles $|F(x)|$ est divisible par p (zéros de la congruence fondamentale; (**5**), sont alors les termes de deux progressions arithmétiques, de raison p:

$$\bar{c}_p+\lambda p; \quad S—\bar{c}_p+(\lambda+1)p; \qquad (\lambda \text{ entier } \geqslant 0).$$

Ces deux progressions sont confondues si $2\bar{c}_p—S = p$; alors p est diviseur du discriminant.

Ces propriétés résultent de la construction des idéaux (**7** et **21**) les valeurs de x sont les racines des deux idéaux canoniques conjugués, de norme p, donc premiers et de produit égal à l'idéal principal (p). On peut aussi les établir directement comme conséquences de l'étude de la *congruence fondamentale* (**5**) pour un module premier.

On peut alors prendre comme base de l'algorithme du crible, la propriété fondamentale suivante.

Pour chaque valeur de x, au moins égale au rang r, *si un nombre premier* p *est diviseur de* $F(x)$ *et si son carré est au plus égal à* $|F(x)|$, *sa racine minimum* $\bar{c}_p$ *est* (strictement) *inférieure à* x —ou il est diviseur d'une valeur antérieure du tableau— .

$$x \geqslant \mathrm{r}; \ p \text{ diviseur de } |F(x)|; \ p^2 \leqslant |F(x)|: \\ \Rightarrow \text{ Existe } \bar{c}_p < x \quad \text{et} \quad p \text{ diviseur de } |F(\bar{c}_p)|.$$

On peut vérifier directement cette propriété en conjuguant la définition de r et la limitation de p^2:

$$x \geqslant r \quad \Rightarrow \quad p^2 \leqslant |F(x)| < (2x—S)^2 \\ \Rightarrow \quad (2\bar{c}_p—S)^2 \leqslant p^2 < (2x—S)^2 \quad \Rightarrow \quad \bar{c}_p < x.$$

On peut aussi bien considérer l'idéal canonique de norme p, de racines $x+\lambda p$ et sa racine minimum (non négative) $\bar{c}_p$. S'il est réduit, $\bar{c}_p$ est inférieur à r, donc à x. S'il n'est pas réduit $|F(\bar{c}_p)|$ est inférieur à p^2, de sorte que x ne peut être égal à $\bar{c}_p$, donc lui est supérieur.

On choisit un nombre h, au moins égal à $r-1$ ($r-1 \leqslant h < H$), on considère les h premières valeurs de la suite et on décompose chacune d'elles en un produit de facteurs premiers p.

On détermine, pour chacune des valeurs successives de x ($h < x \leqslant H$), les puissances des nombres premiers p, précédemment obtenus, qui divisent exactement $|F(x)|$; on forme, pour chaque x, le quotient q_x de $|F(x)|$ par le produit de ces puissances.

1. *Le premier quotient* q_c, ainsi obtenu ($c > h$), *qui soit différent de* 1 *est un nombre premier.*

2. *Les quotients suivants*, pour les valeurs de x, ($h < x < h_1$), vérifiant la condition (c déterminé comme il vient d'être dit):

$$|F(x)| < (2c-S)^2;$$

sont égaux à 1, *ou sont des nombres premiers.*

1. Quel que soit le diviseur premier p, du quotient q_c, il n'est pas diviseur d'une valeur antérieure $|F(x)|$, sa racine minimum est c et p^2 est supérieur à $|F(c)|$ (c étant au moins égal à r). Donc:

$$p^2 > |F(c)| \geqslant q_c.$$

Or il y a au plus un diviseur de q_c, dont le carré lui est supérieur; de sorte que si q_x est différent de 1, il est égal à son seul facteur premier p.

2. Si un quotient q_x, pour $x > c$, est différent de 1 et n'est pas premier, il admet au moins un facteur premier p_1 dont le carré lui est au plus égal. Ce facteur ne divise aucune des valeurs antérieures à $F(c)$ et sa racine minimum c_1 est au moins égale à c, de sorte que:

$$(2c-S)^2 \leqslant (2c_1-S)^2 \leqslant p_1^2 \leqslant q_x \leqslant |F(x)|.$$

Ce quotient q_x ne peut donc être obtenu que pour une valeur de x, au delà des limites fixées par l'énoncé.

Ces règles peuvent s'appliquer par récurrence ascendante à des suites de valeurs croissantes $h_0 \geqslant r-1$; $h_1 > h_0$; ...