

**Zeitschrift:** L'Enseignement Mathématique  
**Herausgeber:** Commission Internationale de l'Enseignement Mathématique  
**Band:** 6 (1960)  
**Heft:** 1: L'ENSEIGNEMENT MATHÉMATIQUE

**Artikel:** LES CORPS QUADRATIQUES  
**Autor:** Châtelet, A.  
**Kapitel:** CHAPITRE IV CRIBLES  
**DOI:** <https://doi.org/10.5169/seals-36342>

#### Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

#### Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

#### Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

**Download PDF:** 28.01.2026

**ETH-Bibliothek Zürich, E-Periodica, <https://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 :*

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

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 :

$$\begin{aligned} D > 0; \quad 5(2x - S)^2 > D &\Leftrightarrow x \geq r; \\ D < 0; \quad 3(2x - S)^2 > |D| &\Leftrightarrow x \geq r \end{aligned}$$

(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  $p$ :

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

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— .

$$\begin{aligned} x &\geq r; \quad p \text{ diviseur de } |F(x)|; \quad p^2 \leq |F(x)|: \\ &\Rightarrow \text{Existe } \bar{c}_p < x \quad \text{et} \quad p \text{ diviseur de } |F(\bar{c}_p)|. \end{aligned}$$

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

$$\begin{aligned} x &\geq r \quad \Rightarrow \quad p^2 \leq |F(x)| < (2x - S)^2 \\ &\Rightarrow \quad (2\bar{c}_p - S)^2 \leq p^2 < (2x - S)^2 \quad \Rightarrow \quad \bar{c}_p < x. \end{aligned}$$

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  $r-1$  ( $r-1 \leq h < H$ ), 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  $x$  ( $h < x \leq H$ ), 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:

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

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:

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

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  $h_0 \geq r-1$ ;  $h_1 > h_0$ ; ...

## 28. Exemples de calculs.

Le tableau V donne les valeurs pour  $x$  de 0 à  $H = 100$ , du trinôme  $F(x)$  déjà utilisé (tableaux I et III), de discriminant  $D = -39$ . Le *rang r* (**25**) est égal à 2.

Les *deux premières valeurs* de  $F(x)$ , ont pour diviseurs premiers **2, 3, 5**, qui sont des diviseurs de  $F(x)$ , pour les valeurs respectives :

$$0+2\lambda, \quad 1+2\lambda; \quad 0+5\lambda, \quad 4+5\lambda; \quad 1+3\lambda.$$

Il n'y a qu'une progression pour 3, qui est diviseur de  $D$ .

On a inscrit devant chaque valeur de la table, le monôme des puissances des facteurs 2, 3, 5, qui en est diviseur, de façon à calculer les quotients  $q_x$ . Les périodicités, ou les progressions sont mises en évidence par l'alignement (vertical) de ces facteurs.

Le *premier quotient*, rencontré ensuite, qui soit différent de 1 est  $F(3):2 = \mathbf{11}$ . Il est premier, on l'a inscrit devant les valeurs dont il est diviseur et qui sont données par les progressions de raison 11 et de premiers termes 3 et 7. Deux seulement  $F(51)$  et  $F(69)$  sont divisibles par une puissance supérieure de 11; les autres appartenant à des progressions de raison  $11^2$  sont extérieures à la table.

Le premier quotient obtenu ensuite, qui soit différent de 1 est  $F(6):2^2 = \mathbf{13}$ . C'est un nombre premier, diviseur de  $D$ ; il n'est obtenu que pour les valeurs d'une seule progression  $6+13\lambda$ , et seulement à la première puissance.

Les quotients suivants, jusqu'à  $F(13)$  exclus, qui devient supérieur à  $(2 \times 6 + 1)^2 = 169$ , sont égaux à 1, ou sont premiers :

$$\begin{aligned} F(7): (2 \times 3 \times 11) &= 1; & F(8): 2 &= \mathbf{41}; & F(9): (2^2 \times 5^2) &= 1; \\ F(10): (2^3 \times 3 \times 5) &= 1; & F(11): 2 &= \mathbf{71}; & F(12): 2 &= \mathbf{83}. \end{aligned}$$

On inscrit ces nombres premiers devant les valeurs de la table, dont ils sont diviseurs, et qui sont données par :

**41** pour  $x = 8, 49, 90; \quad 32, 73;$     **71** pour  $x = 11, 82; \quad 59;$   
**83** pour  $x = 12, 95; \quad 70;$

ils n'y figurent qu'à la première puissance.

Le premier quotient différent de 1, qui est rencontré ensuite est  $F(16): (2 \times 3) = \mathbf{47}$ ; il est premier et il en est de même de ceux des

quotients suivants, qui sont différents de 1, jusqu'à  $F(33)$  exclus, qui est supérieur à  $(2 \times 16 + 1)^2 = 1\ 089$ . Certains sont encore diviseurs d'autres valeurs du tableau, ce sont:

- 47** pour  $x = 16, 63; 30, 77;$     **79** pour  $x = 17, 96; 61;$   
**43** pour  $x = 20, 63; 22, 65;$     **59** pour  $x = 21, 80; 37, 96;$   
**61** pour  $x = 24, 85; 36, 97;$     **89** pour  $x = 26; 62.$

Par contre, les diviseurs premiers **281**, **383**, **137**, ne se rencontrent plus dans le tableau, limité à  $H = 100$ .

Le premier quotient rencontré ensuite, est  $F(33): 2^2 = \mathbf{283}$ ; il est premier et il en est de même de ceux des quotients suivants qui sont différents de 1 jusqu'à  $F(67)$  exclus qui est supérieur à  $(2 \times 33 + 1)^2 = 4\ 489$ . Dans ces quotients, ceux qui figurent plus d'une fois dans le tableau, limité à  $H = 100$ , sont:

- 127** pour  $x = 35; 91;$     **103** pour  $x = 47; 55;$   
**149** pour  $x = 54; 94;$     **139** pour  $x = 64; 74.$

Le premier quotient rencontré ensuite est  $F(67): (2 \times 3) = \mathbf{761}$ ; il est premier et il en est de même de tous les quotients suivants de la table, car  $(2 \times 67 + 1)^2 = 18\ 225$  est supérieur à  $F(100)$ .

Dans la table, les nombres en caractères gras sont les facteurs  $p$  rencontrés pour leur racine minimum  $\bar{c}_p$  (ou pour la première fois).

On rappelle qu'il a été indiqué ci-dessus que les nombres premiers ainsi obtenus sont ceux qui appartiennent à douze progressions arithmétiques de raison commune 39.

Le *deuxième exemple*, donné dans le tableau VI, est constitué par les valeurs pour  $x$  de  $O$  à  $H = 100$ , du trinôme, de discriminant  $D$  positif (définissant un corps réel):

$$F(x) = x^2 - 47; \quad D = (-4) \times (-47) = 188.$$

Les valeurs sont négatives et de valeurs absolues décroissantes jusqu'à  $F(6)$ ; elles sont ensuite positives et croissantes.

Le rang  $r$  est égal à 4, car:

$$5 \times (2 \times 3)^2 = 180 < 4 \times 47 < 5 \times (2 \times 4)^2 = 320.$$

Les quatre premières valeurs de  $F(x)$  ont pour diviseurs premiers: **2**, **47**, qui sont diviseurs de  $D$ , et **23**, **43**, **19**. On inscrit devant chaque valeur les monômes de ces facteurs qui en sont des diviseurs.

TABLEAU V.

$$F(x) = x^2 + x + 10 \quad D = -39 = (-3) \times 13 \quad r = 2.$$

$c$	$F(c)$	Diviseurs	$c$	$F(c)$	Diviseurs
0	10	<b>2.5</b>	25	660	2 <sup>2</sup> . 3. 5. 11
1	12	<b>2<sup>2</sup>. 3</b>	26	712	2 <sup>3</sup> . <b>89</b>
2	16	<b>2<sup>4</sup></b>	27	766	2. <b>383</b>
3	22	<b>2.</b> <b>11</b>	28	822	2. 3. <b>137</b>
4	30	<b>2.</b> <b>3. 5</b>	29	880	2 <sup>4</sup> . 5. 11
5	40	<b>2<sup>3</sup>.</b> <b>5</b>	30	940	2 <sup>2</sup> . 5. <b>47</b>
6	52	<b>2<sup>2</sup>.</b> <b>13</b>	31	1 002	2. 3. <b>167</b>
7	66	<b>2.</b> <b>3</b> <b>11</b>	32	1 066	2. <b>13.</b> <b>41</b>
8	82	<b>2.</b> <b>41</b>	33	1 432	<b>2<sup>2</sup>.</b> <b>283</b>
9	100	<b>2<sup>2</sup>.</b> <b>5<sup>2</sup></b>	34	1 200	2 <sup>4</sup> . 3. <b>5<sup>2</sup></b>
10	120	<b>2<sup>3</sup>.</b> <b>3.</b> 5	35	1 270	2. 5. <b>127</b>
11	142	<b>2.</b>	36	1 342	2. <b>11.</b> <b>61</b>
12	166	<b>2.</b>	37	1 416	2 <sup>3</sup> . 3. <b>59</b>
13	192	<b>2<sup>6</sup>.</b> <b>3</b>	38	1 492	2 <sup>2</sup> . <b>373</b>
14	220	<b>2<sup>2</sup>.</b> <b>5.</b> 11	39	1 570	2. 5. <b>157</b>
15	250	<b>2.</b> <b>5<sup>3</sup></b>	40	1 650	2. 3. <b>5<sup>2</sup></b> . 11
16	282	<b>2.</b> <b>3</b> <b>47</b>	41	1 732	2 <sup>2</sup> . <b>433</b>
17	316	<b>2<sup>2</sup>.</b> <b>79</b>	42	1 816	2 <sup>3</sup> . <b>227</b>
18	352	<b>2<sup>5</sup>.</b> 11	43	1 902	2. 3. <b>317</b>
19	390	<b>2.</b> <b>3.</b> <b>5.</b> 13	44	1 990	2. 5. <b>199</b>
20	430	<b>2.</b> 5. <b>43</b>	45	2 080	2 <sup>5</sup> . 5. <b>13</b>
21	472	<b>2<sup>3</sup>.</b> <b>59</b>	46	2 172	2 <sup>2</sup> . 3. <b>181</b>
22	516	<b>2<sup>2</sup>.</b> <b>3.</b> <b>43</b>	47	2 266	2. <b>11.</b> <b>103</b>
23	562	<b>2.</b>	48	2 362	<b>2.</b> <b>1 181</b>
24	610	<b>2.</b> 5. <b>61</b>	49	2 460	2 <sup>2</sup> . 3. 5. <b>41</b>

$c$	$F(c)$	Diviseurs	$c$	$F(c)$	Diviseurs
50	2 560	2 <sup>9</sup> . 5.	55	2 662	2. 3. <b>11<sup>3</sup></b>
51	2 662	2. 3.	52	2 766	2. 3. <b>461</b>
53	2 872	2 <sup>3</sup> . <b>359</b>	54	2 980	2 <sup>2</sup> . 5. <b>149</b>
55	3 090	2. 3. 5. <b>103</b>	56	3 202	2. <b>1 601</b>
57	3 316	2 <sup>2</sup> . <b>829</b>	58	3 432	2 <sup>3</sup> . 3. <b>11.</b> <b>13</b>
59	3 550	2. <b>5<sup>2</sup>.</b> <b>71</b>	60	3 670	2. 5. <b>367</b>
61	3 792	2 <sup>4</sup> . 3. <b>79</b>	62	3 916	2 <sup>2</sup> . <b>11.</b> <b>89</b>
63	4 042	2. <b>43.</b> <b>47</b>	64	4 170	2. 3. 5. <b>139</b>
65	4 300	2 <sup>2</sup> . 5 <sup>2</sup> . <b>43</b>	66	4 432	<b>24.</b> <b>277</b>
67	4 566	2. 3. <b>761</b>	68	4 702	2. <b>2 351</b>
69	4 840	<b>23.</b> 5. <b>11<sup>2</sup></b>	70	4 980	2 <sup>2</sup> . 3. 5. <b>83</b>
71	5 122	2. <b>13.</b> <b>197</b>	72	5 266	2. <b>2 633</b>
73	5 412	2 <sup>2</sup> . 3. <b>11.</b> <b>41</b>	74	5 560	<b>2<sup>3</sup>.</b> 5. <b>139</b>

$c$	$F(c)$	Diviseurs	$c$	$F(c)$	Diviseurs
75	5 740	2. 5. <b>571</b>	76	5 862	2. 3. <b>977</b>
77	6 016	2 <sup>7</sup> .	78	6 172	2 <sup>2</sup> . <b>1 543</b>
79	6 330	2. 3. 5. <b>211</b>	80	6 490	2. 5. 11. <b>59</b>
81	6 652	2 <sup>2</sup> . <b>1 663</b>	82	6 816	2 <sup>5</sup> . 3. <b>71</b>
83	6 982	2. <b>3 491</b>	84	7 150	2. 5 <sup>2</sup> . 11. <b>13</b>
85	7 320	2 <sup>3</sup> . 3. 5.	86	7 492	2 <sup>2</sup> . <b>1 873</b>
87	7 666	2. <b>3 833</b>	88	7 842	2. 3. <b>1 307</b>
89	8 020	2 <sup>2</sup> . 5. <b>401</b>	90	8 200	<b>23.</b> 5 <sup>2</sup> . <b>41</b>
91	8 382	2. 3. 41. <b>127</b>	92	8 566	2. <b>4 283</b>
93	8 752	2 <sup>4</sup> .	94	8 940	2 <sup>2</sup> . 3. 5. <b>149</b>
95	9 130	2. 5. 11. <b>83</b>	96	9 322	2. 59. <b>79</b>
97	9 516	2 <sup>2</sup> . 3.	98	9 712	2 <sup>4</sup> . <b>607</b>
99	9 910	2. 5. <b>991</b>	100	10 110	2. 3. 5. <b>337</b>

Les quotients suivants, pour les valeurs de  $x$ , définies par:

$$|F(x)| \leqslant (2 \times 4)^2 \Rightarrow x \leqslant 10$$

sont uniquement des valeurs, ou des moitiés de valeurs du polynôme puisqu'à l'exception du diviseur 2, la première valeur devant laquelle on a inscrit un des diviseurs précédents est  $F(16)$  divisible par 19. Ce sont:

$$\begin{aligned} F(4) &= -\mathbf{31}; & F(5):2 &= -\mathbf{11}; & F(6) &= -11; & F(7):2 &= +2; \\ F(8) &= +\mathbf{17}; & F(9):2 &= +17; & F(10) &= +\mathbf{53}. \end{aligned}$$

On les inscrit devant les valeurs suivantes de la table qu'ils divisent, éventuellement avec l'exposant convenable.

Le quotient suivant  $F(11):2 = +\mathbf{37}$  est premier; ceux qui suivent pour les valeurs de  $x$ :

$$|F(x)| \leqslant (2 \times 11)^2 \Rightarrow x \leqslant 23,$$

sont égaux à 1, ou sont premiers. Ces derniers sont encore égaux aux valeurs, ou aux moitiés des valeurs du polynôme; les seuls quotients donnés par des diviseurs déjà inscrits, à l'exception de 2, sont:

$$F(16):(19 \times 11) = +1; \quad F(22):(23 \times 19) = +1.$$

Les seuls nombres premiers ainsi obtenus qui figurent encore dans la table, limitée à  $H = 100$ , sont **37, 97, 61, 89**.

Le premier quotient suivant qui est différent de 1 est  $F(28):11 = \mathbf{67}$ , ceux qui suivent pour les valeurs de  $x$ :

$$|F(x)| \leqslant (2 \times 28)^2 \Rightarrow x \leqslant 56,$$

sont égaux à 1 ou premiers; ceux qui figurent plus d'une fois dans la table sont: **67, 127, 101, 107, 151**.

Au-delà de  $x = 56$ , tous les quotients sont premiers ou égaux à 1.

La disposition typographique est semblable à celle de l'exemple précédent, les nombres premiers obtenus pour la première fois (pour leur racine minimum) sont en caractères gras.

L'application de la loi de la réciprocité (22) montre que les nombres premiers ainsi obtenus sont ceux qui appartiennent à  $\varphi(168):2 = 46$  progressions arithmétiques, de raison commune 168 et de premiers termes: 1, 9, 11, 15, 17, 19, 21, 23, 25, 31, 35, 37, 39, 43, 49, 53, 61, 65, 67, 81, 87, 89, 91, 97, 99, 101, 107, 121, 123, 127, 135, 139, 145, 149, 151, 153, 157, 163, 165, 167, 169, 171, 173, 177, 179, 187.

TABLEAU VI.

$$F(x) = x^2 - 47 \quad D = 188 = (-4) \times (-47) \quad r = 4.$$

c		F(c)		Diviseurs	
0	-47	47		25	578
1	-46	2. 23		26	629
2	-43	43		27	682
3	-38	2. 19		28	737
4	-34	31		29	794
5	-22	2. 11			
6	-11	11		30	853
7	+ 2	2.		31	914
8	17	17		32	977
9	34	2. 17		33	1 042
10	53	53		34	1 109
11	74	2. 37		35	1 178
12	97	97		36	1 249
13	122	2. 61		37	1 322
14	149	149		38	1 397
15	178	2. 89		39	1 474
16	209	19. 11			
17	242	2. 41 <sup>2</sup>		40	1 553
18	277	277		41	1 634
19	314	2. 157		42	1 717
				43	1 802
				44	1 889
20	353	353		45	1 978
21	394	2. 197		46	2 069
22	437	23. 19		47	2 162
23	482	2. 241		48	2 257
24	529	232		49	2 354

c		F(c)		Diviseurs	
50	2 453			11.	223
51	2 554			2.	1 277
52	2 657				2. 657
53	2 762			2.	1 381
54	2 869			19.	151
55	2 978			2.	1 489
56	3 089				3 089
57	3 202			2.	1 601
58	3 317			31.	107
59	3 434			2.	17. 101
60	3 553				19. 11. 17
61	3 674			2.	11. 167
62	3 797				3 797
63	3 922			2.	53. 37
64	4 049				4 049
65	4 178			2.	2 089
66	4 309			31.	139
67	4 442			2.	2 221
68	4 577				23. 199
69	4 714			2.	2 357
70	4 853			23.	211
71	4 994			2.	11. 227
72	5 137			11.	467
73	5 282			2.	19. 139
74	5 429			61.	89

c		F(c)		Diviseurs	
75	5 578			2.	2 789
76	5 729				17. 337
77	5 882			2.	17. 173
78	6 037				6 037
79	6 194			2.	19. 163
80	6 353				6 353
81	6 514			2.	3 257
82	6 677				11. 607
83	6 842			2.	11. 311
84	7 009				4 3. 163
85	7 178			2.	37. 97
86	7 349				7 349
87	7 522			2.	3 761
88	7 697				4 3. 179
89	7 874			2.	31. 127
90	8 053				8 053
91	8 234			2.	23. 179
92	8 417				19. 443
93	8 602			2.	23. 11. 17
94	8 789				47. 11. 17.
95	8 978			2.	672.
96	9 169				53. 173
97	9 362			2.	31. 151
98	9 557				19. 503
99	9 754			2.	4 877
100	9 953				37. 269

## 29. Successions de nombres premiers.

Dans le deuxième exemple traité, les quinze premières valeurs de  $|F(x)|$  sont des nombres premiers ou des doubles de nombres premiers. Cette particularité tient à ce que les valeurs de  $|F(x)|$  pour  $x < r$ , sont des nombres premiers relativement grands, qui ne se retrouvent, par suite, dans la table, qu'à des rangs relativement éloignés. Il existe d'autres exemples de ce même phénomène.

Un exemple (bien connu, au moins depuis Euler) est constitué par les valeurs du trinôme (à discriminant  $D$  négatif):

$$F(x) = x^2 + x + 41; \quad D = -163.$$

Le tableau VII en donne les valeurs pour les valeurs entières de  $x$ , de 0 à 299; pour celles qui ne sont pas des nombres premiers, on a seulement inscrit leur décomposition en facteurs premiers.

*Les quarantes premières valeurs de  $F(x)$  sont des nombres premiers.*

Le rang  $r$  est égal à 4; les quatre premières valeurs sont les nombres premiers:

$$41, \quad 43, \quad 47, \quad 53.$$

Ils ne se retrouvent comme facteurs qu'au-delà de  $x = 39$ . On peut montrer par récurrence sur  $c$ , compris entre 4 et 39 inclus, que  $F(c)$  est un nombre premier, de racine minimum égale à  $c$ . Car, il en est ainsi pour  $F(4)$ , et, par hypothèse de récurrence, pour toute valeur  $F(x)$ ,  $x$  étant compris entre 0 inclus et  $c$  exclus; en outre la racine conjuguée du nombre premier  $F(x)$  est supérieure à 39, puisque

$$F(x) - x - 1 = x^2 + 40 \geq 40.$$

Il s'en suit que  $F(c)$  ne peut être divisible par aucun des nombres premiers  $F(x)$ , il est donc premier et de racine minimum  $c$ .

A l'exclusion des sept décompositions:

$$\begin{aligned} F(40) &= 41^2, & F(41) &= 41 \times 43, & F(44) &= 43 \times 47, \\ F(49) &= 47 \times 53, & F(56) &= 53 \times 61, & F(65) &= 61 \times 71, \\ F(76) &= 71 \times 83 \end{aligned}$$

les valeurs de  $F(40)$  à  $F(80)$ , sont des nombres premiers (soient 34 nombres premiers nouveaux).

TABLEAU VII.

 $F(x) = x^2 + x + 41$ ; discriminant: -163;  $r = 4$ .

$x$	$F(x)$	$x$	$F(x)$	$x$	$F(x)$	$x$	$F(x)$
0	41	42	1 847	84	$43 \times 167$	126	$61 \times 263$
1	43	43	1 933	85	7 351	127	$43 \times 379$
2	47	44	$43 \times 47$	86	7 523	128	16 553
3	53	45	2 111	87	$43 \times 179$	129	16 811
4	61	46	2 203	88	7 873	130	$43 \times 397$
5	71	47	2 297	89	$83 \times 97$	131	17 333
6	83	48	2 393	90	8 231	132	17 597
7	97	49	$47 \times 53$	91	$47 \times 179$	133	17 863
8	113	50	2 591	92	8 597	134	18 131
9	131	51	2 693	93	8 783	135	18 401
10	151	52	2 797	94	8 971	136	$71 \times 263$
11	173	53	2 903	95	9 161	137	18 947
12	197	54	3 011	96	$47 \times 199$	138	$47 \times 409$
13	223	55	3 121	97	9 547	139	19 501
14	251	56	$53 \times 61$	98	9 743	140	$131 \times 151$
15	281	57	3 347	99	9 941	141	20 063
16	313	58	3 463	100	10 141	142	20 347
17	347	59	3 581	101	10 343	143	$47 \times 439$
18	383	60	3 701	102	$53 \times 199$	144	20 921
19	421	61	3 823	103	10 753	145	21 211
20	461	62	3 947	104	$97 \times 113$	146	21 503
21	503	63	4 073	105	11 171	147	$71 \times 307$
22	547	64	4 201	106	11 383	148	22 093
23	593	65	$61 \times 71$	107	11 597	149	22 391
24	641	66	4 463	108	11 813	150	22 691
25	691	67	4 597	109	$53 \times 227$	151	22 993
26	743	68	4 733	110	12 251	152	23 297
27	797	69	4 871	111	12 473	153	23 603
28	853	70	5 011	112	12 697	154	23 911
29	911	71	5 153	113	12 923	155	$53 \times 457$
30	971	72	5 297	114	13 151	156	24 533
31	1 033	73	5 443	115	13 381	157	24 847
32	1 097	74	5 591	116	13 613	158	25 163
33	1 163	75	5 741	117	$61 \times 227$	159	$83 \times 307$
34	1 231	76	$71 \times 83$	118	14 083	160	25 801
35	1 301	77	6 047	119	14 321	161	$151 \times 173$
36	1 373	78	6 203	120	14 561	162	$53 \times 499$
37	1 447	79	6 361	121	$113 \times 131$	163	$41 \times 653$
38	1 523	80	6 521	122	$41 \times 367$	164	$41 \times 661$
39	1 601	81	$41 \times 163$	123	$41 \times 373$	165	27 431
40	$41^2$	82	$41 \times 167$	124	15 541	166	27 763
41	$41 \times 43$	83	7 013	125	15 791	167	28 097

TABLEAU VII. (*suite*).

$x$	$F(x)$	$x$	$F(x)$	$x$	$F(x)$	$x$	$F(x)$
168	28 433	201	<b>97 × 419</b>	234	<b>113 × 487</b>	267	71 597
169	28 771	202	41 047	235	55 501	268	<b>53 × 1 361</b>
		203	41 453	236	<b>223 × 251</b>	269	72 671
170	<b>43 × 677</b>	204	<b>41 × 1 021</b>	237	<b>47 × 1 201</b>		
171	29 453	205	<b>41 × 1 031</b>	238	56 923	270	<b>179 × 409</b>
172	<b>83 × 359</b>	206	42 683	239	<b>61 × 941</b>	271	<b>131 × 563</b>
173	<b>43 × 701</b>	207	<b>71 × 607</b>	240	57 881	272	74 297
174	30 491	208	<b>53 × 821</b>	241	58 363	273	74 843
175	30 841	209	<b>197 × 223</b>	242	<b>83 × 709</b>	274	75 391
176	31 193			243	59 333	275	75 941
177	31 547	210	44 351	244	<b>163 × 367</b>	276	76 493
178	<b>61 × 523</b>	211	44 773	245	<b>41 × 1 471</b>	277	77 047
179	32 261	212	45 197	246	<b>41 × 1 483</b>	278	<b>71 × 1 093</b>
180	32 621	214	46 051	247	61 297	279	<b>47 × 1 663</b>
181	32 983	215	<b>53 × 877</b>	248	<b>61 × 1 013</b>	280	78 721
182	33 347	216	<b>43 × 1 091</b>	249	<b>167 × 373</b>	281	79 283
183	33 713	217	<b>113 × 419</b>			282	79 847
184	<b>173 × 197</b>	218	<b>71 × 673</b>	250	62 791	283	<b>97 × 829</b>
185	<b>47 × 733</b>	219	48 221	251	<b>167 × 379</b>	284	<b>47 × 1 723</b>
186	<b>97 × 359</b>			252	<b>131 × 487</b>	285	81 551
187	<b>61 × 577</b>	220	48 661	253	64 303	286	<b>41 × 2 003</b>
188	35 573	221	49 103	254	64 811	287	<b>41 × 2 017</b>
189	35 951	222	49 547	255	<b>83 × 787</b>	288	83 273
		223	49 993	256	<b>43 × 1 531</b>	289	<b>71 × 1 181</b>
190	<b>47 × 773</b>	224	50 441	257	66 347		
191	36 713	225	50 891	258	66 863	290	84 431
192	37 097	226	51 343	259	<b>43 × 1 567</b>	291	<b>151 × 563</b>
193	37 483	227	51 797			292	85 597
194	37 871	228	52 253	260	67 901	293	86 183
195	38 261	229	52 711	261	<b>53 × 1 291</b>	294	86 771
196	38 653			262	68 947	295	<b>199 × 439</b>
197	39 047	230	53 171	263	69 473	296	<b>281 × 313</b>
198	39 443	231	53 633	264	70 001	297	88 547
199	39 841	232	<b>47 × 1 151</b>	265	<b>251 × 281</b>	298	<b>97 × 919</b>
200	40 241	233	54 563	266	<b>179 × 397</b>	299	<b>43 × 2 087</b>

Au-delà de  $F(40)$ , on inscrit les premiers nombres premiers de la table devant les valeurs qu'ils divisent, on obtient les sept décompositions indiquées; puis  $F(81) = 41 \times 163$ , qui comporte un diviseur premier non encore obtenu, ou de racine minimum 81.

A toute valeur  $F(c)$ , pour  $c$  compris entre 7 et 80 inclus, exception faite des valeurs de décomposition, on peut appliquer le raisonnement de récurrence précédent. Tout  $F(x)$ , de  $F(6)$  à  $F(c)$  exclus, étant

supposé premier, de racine minimum  $x$ , sa racine conjuguée est supérieure à 81, car:

$$F(x)-x-1 = x^2+40 \geqslant 49+40 = 89.$$

Il ne divise donc pas  $F(c)$ , qui n'étant pas divisible par les valeurs de  $F(0)$  à  $F(6)$  est un nombre premier de racine minium  $c$ .

Pour toutes les valeurs de  $x$ , au-delà de 80 et telles que:

$$F(x) \leqslant (2 \times 80 + 1)^2 \Rightarrow x \leqslant 161,$$

les quotients obtenus (après division éventuelle par les monômes des nombres premiers précédents, qui peuvent être limités aux douze premiers), sont des nombres premiers ou sont égaux à 1.

Certains sont diviseurs de valeurs ultérieures du tableau concurremment avec des nombres premiers déjà trouvés. On les inscrit et on forme les quotients qui sont tous premiers ou égaux à 1, dans la limite de la table, dont les valeurs restantes sont inférieures à  $(2 \times 161 + 1)^2$ .

On a indiqué, en caractère gras, les nombres premiers obtenus comme facteur d'une décomposition effective. Leur fréquence augmente naturellement, dans le prolongement de la table. On peut même trouver une suite de valeurs  $F(x)$ , en nombre  $H$ , arbitrairement grand, dont aucune ne soit un nombre premier.

Il suffit de prendre  $x$  compris entre  $P$  et  $P+H$ , le nombre  $P$  étant le produit des facteurs premiers qui divisent les  $H$  premières valeurs  $|F(c)|$ . Il est manifeste que chacune des valeurs  $F(x)$ , ainsi considérées est divisible par au moins un de ces nombres premiers, sans lui être égal ( $H$  étant pris au moins égal à  $r$ ).

Cependant on ne peut pas affirmer qu'il n'y a qu'un nombre fini de valeurs  $F(x)$  qui soient des nombres premiers.

Le tableau *VIII* donne *trois autres exemples*, de types différents, limités chacun aux soixante premières valeurs des trinômes.

Pour le trinôme, de discriminant  $D$  positif, impair;

$$F(x) = x^2+x-109; \quad D = 347 = (-19) \times (-23);$$

les *vingt-huit premières valeurs sont des nombres premiers*.

Pour chacune d'elles la deuxième racine est supérieure à 27;

(pour  $F(9) = -19$ , et  $F(11) = +23$ , qui sont diviseurs du discriminant, les deux progressions sont confondues).

Dans les dix-neuf valeurs suivantes, seize sont des nombres premiers, les trois autres étant des produits de nombres premiers déjà obtenus:

$$F(28) = 19 \times 37; \quad F(34) = 23 \times 47; \quad F(45) = 37 \times 53.$$

(Le raisonnement fait par récurrence dans l'exemple précédent reste valable.)

La valeur suivante  $F(47)$  est divisible par 19; mais le quotient est un nouveau nombre premier, ou de racine minimum 47.

Tous les quotients des valeurs restantes sont des nombres premiers ou sont égaux à 1.

Pour le trinôme de discriminant  $D$  positif, multiple de 4:

$$F(x) = x^2 - 83; \quad D = 332 = (-4) \times (-83)$$

2 étant diviseur du discriminant, toutes les valeurs, pour  $x$  impair sont divisibles par 2, mais non par 4.

Les vingt-quatre premières valeurs sont des nombres premiers ou des doubles de nombres premiers. Toutefois deux facteurs premiers se trouvent deux fois et un d'eux est égal à 1:

$$\begin{aligned} \mathbf{17} &= |F(7)| : 2 = F(10); & \mathbf{19} &= |F(8)| = F(11) : 2; \\ \mathbf{1} &= |F(9)| : 2. \end{aligned}$$

Dans les vingt valeurs suivantes: treize sont des nombres premiers ou des doubles de nombres premiers; les sept autres sont des produits ou des doubles de produits des nombres premiers impairs, précédemment obtenus.

Tous les quotients des valeurs restantes de la table, au-delà de  $F(43)$ , qui sont différents de 1 et de 2, sont des nombres premiers.

Pour le trinôme de discriminant négatif, multiple de 4:

$$F(x) = x^2 + 37; \quad D = -148 = (-4) \times (+37);$$

2 est encore diviseur du discriminant; toutes les valeurs pour  $x$  impair sont divisibles par 2, mais non par 4.

Les dix-huit premières valeurs, ou leurs moitiés, sont des nombres premiers. Dans les trente-huit valeurs suivantes, vingt-neuf sont des nombres premiers ou des doubles de nombres premiers; les neuf autres, ou leurs moitiés sont des produits des nombres premiers impairs déjà obtenus.

TABLEAU VIII.

$F(x) = x^2 + x - 109;$ $D = (-19) \times (-23)$		$F(x) = x^2 - 83;$ $D = (-4) \times (-83)$	
$c$	$F(c)$	$c$	$F(c)$
0	-109	30	824
1	-107	31	823
2	-103	32	947
3	-97	33	1 013
4	-89	34	$23 \times 47$
5	-79	35	1 151
6	-67	36	1 223
7	-53	37	1 297
8	-37	38	1 373
9	-19	39	1 451
10	+	40	1 531
11	23	41	1 613
12	47	42	1 697
13	73	43	1 783
14	101	44	1 871
15	131	45	$37 \times 53$
16	163	46	2 053
17	197	47	$19 \times 113$
18	233	48	2 243
19	271	49	2 341
20	311	50	2 441
21	353	51	2 543
22	397	52	2 647
23	443	53	2 753
24	491	54	2 861
25	541	55	2 971
26	593	56	3 083
27	647	57	$23 \times 139$
28		58	$3 313$
29		59	$47 \times 73$

$F(x) = x^2 + x - 83;$ $D = (-4) \times (-83)$		$F(x) = x^2 + 37;$ $D = (-4) \times (+37)$	
$c$	$F(c)$	$c$	$F(c)$
0	0	-	83
1	1	-2 $\times$ 41	30
2	2	-	2 $\times$ 439
3	3	-2 $\times$ 37	32
4	4	-	2 $\times$ 503
5	5	-2 $\times$ 29	34
6	6	-	2 $\times$ 571
7	7	-2 $\times$ 17	35
8	8	-	2 $\times$ 643
9	9	-2 $\times$ 1	39
10	+	17	29 $\times$ 37
11	23	2 $\times$ 19	34
12	47	41 $\times$ 41	41
13	73	2 $\times$ 43	42
14	101	113	43
15	131	2 $\times$ 71	43
16	163	15	17 $\times$ 109
17	197	16	2 $\times$ 971
18	233	17	2 $\times$ 103
19	271	18	19 $\times$ 107
20	311	19	2 $\times$ 1063
21	353	20	2 $\times$ 107
22	397	21	2 $\times$ 199
23	443	22	2 $\times$ 199
24	491	23	2 $\times$ 223
25	541	24	2 $\times$ 29 $\times$ 47
26	593	25	2 $\times$ 293
27	647	26	2 $\times$ 1 423
28		27	2 $\times$ 1 423
29		28	2 $\times$ 1 423

$F(x) = x^2 + 37;$ $D = (-4) \times (+37)$			
$c$	$F(c)$	$c$	$F(c)$
0	0	0	37
1	1	1	2 $\times$ 19
2	2	2	41
3	3	3	2 $\times$ 23
4	4	3	2 $\times$ 23
5	5	5	53
6	6	6	73
7	7	7	73
8	8	8	2 $\times$ 43
9	9	9	2 $\times$ 59
10	+	10	34
11	23	23	53
12	47	47	53
13	73	73	53
14	101	101	53
15	131	131	53
16	163	163	53
17	197	197	53
18	233	233	53
19	271	271	53
20	311	311	53
21	353	353	53
22	397	397	53
23	443	443	53
24	491	491	53
25	541	541	53
26	593	593	53
27	647	647	53
28		58	53
29		59	53

(à suivre)