22. Nombres premiers décomposables dans le corps.

l'existence d'idéaux canoniques, non inscrits, de racine positive minimum $\overline{c}$ (ou $\overline{c'}+m$) et de norme m:

$\overline{c}$:	7, 27;	9, 24;	9, 57;	10, 75;	11, 42;	11, 95;
m:	34	33	66	85	53	106 ;
$\overline{c}$:	15, 195;	16, 215;	17, 120;	17, 257;	18, 85;	
m:	210	241	137	274	103	
$\overline{c}$:	18, 291;	19,154;	19,327;	20, 35;	20, 57;	20, 365;
m:	309	173	346	55	77	385
c :	21, 50;	21, 121;	21,192;	21,405;	22, 45;	22, 447.
m:	71	142	213	426	67	469

22. Nombres premiers décomposables dans le corps.

On peut caractériser, à priori, les nombres premiers qui sont des diviseurs des valeurs de la table. En utilisant des propriétés de la Théorie élémentaire des nombres et, plus spécialement la *loi de réciprocité quadratique* [1]), on peut démontrer que:

en plus des diviseurs du discriminant, *les nombres premiers, pour qui la congruence fondamentale est possible*, —ou qui sont *normes de deux idéaux premiers*, du premier degré, conjugués— —ou décomposables en le produit de ces deux idéaux— *sont ceux qui appartiennent à certaines progressions arithmétiques*, dont la raison commune est la valeur absolue $|D|$, du discriminant du corps, et qui sont en nombre $\varphi(|D|)$ |2.

La congruence fondamentale (**1**), caractérisée par le nombre entier d, est *possible ou impossible suivant que*, d et, par suite, *le discriminant* D (égal à d, ou à $4d$) *est congru, ou n'est pas congru*, mod. p, au carré d'un nombre entier.

On peut représenter cette propriété de D, relative au nombre premier p, par le *symbole de* LEGENDRE. Il peut être construit en

---

[1]) Ces propriétés sont notamment exposées dans les ouvrages français: J.-A. SERRET, *Algèbre supérieure*, 3e édition, 1866 et suivantes; section III, ch. 2; E. BOREL et J. DRACH, d'après des leçons de J. TANNERY, *Introduction à la théorie des Nombres et à l'Algèbre supérieure*, 1894, 1re partie, ch. IV; J. TANNERY, *Leçons d'Arithmétique*, 1896, ch. XIV, § 5; E. CAHEN, *Eléments de la Théorie des Nombres*, 1900 — Théorie des Nombres — tome second, 1924, ch. XVI. On trouvera dans ces ouvrages la définition de la fonction — ou indicateur — d'EULER $\varphi(n)$.

utilisant l'indice de D, défini par une racine primitive g, mod. p:

$$g^{\text{ind. } D} \equiv D, \quad (\text{mod. } p) \quad \Rightarrow \quad \left(\frac{D}{p}\right) = (-1)^{\text{ind. } D}.$$

Ce symbole est égal à $+1$, *ou à* -1, suivant que l'exposant ind. D, (défini mod. $p-1$) est pair ou impair —ou que D est congru ou n'est pas congru à un carré— donc *suivant que la congruence fondamentale est possible ou impossible.*

L'expression du symbole met en évidence son caractère multiplicatif: il est égal au produit des symboles des facteurs (entiers positifs ou négatifs) d'une décomposition de D en produit:

$$D = \Pi\delta_i \quad \Rightarrow \quad (-1)^{\text{ind. } D} = (-1)^{\Sigma(\text{ind. } \delta_i)} = \Pi\left(\frac{\delta_i}{p}\right).$$

Il est commode de décomposer D en un produit de facteurs δ_i, comprenant éventuellement un facteur, noté δ_1, égal à -4, ou $+8$, ou -8, et des facteurs premiers impairs, différents, chacun étant affecté d'un signe convenable, de façon qu'il soit congru à $+1$, mod. 4. [Exemples: -3, $+5$, -7, -11, $+13$, ...]

L'examen des divers cas montre que ceci est possible:

1. *d impair*, positif ou négatif, *congru à* $+1$, mod. 4. Alors D est égal à d; sa valeur absolue est égale à un produit de facteurs premiers impairs différents. Le nombre de ceux qui sont congrus à -1, mod. 4, est pair ou impair, suivant que d est positif ou négatif; on peut donc les affecter du signe —. Exemples:

$d = -3;\ +5;\ +21;\ -15;\ +65;\ \ldots$
$D = -3;\ +5;\ (-3)\times(-7);\ (-3)\times(+5);\ (+5)\times(+13);\ \ldots$

2. *d impair*, positif ou négatif, congru à -1, mod. 4. Alors D est égal à $4d$; on conserve le signe de D, en affectant 4 du signe —. Exemples:

$d = -1;\ +3;\ -5;\ -21;\ \ldots$
$D = -4;\ (-4)\times(-3);\ (-4)\times(+5);\ (-4)\times(-3)\times(-7);\ \ldots$

3. *d pair*, positif ou négatif. Alors $D = 4d$ a un facteur 8 qu'on affecte du signe $+$ ou —, suivant les signes affectés éventuellement aux autres facteurs. Exemples:

$d = +2;\ -2;\ +6;\ -6;\ +10;\ \ldots$
$D = +8;\ -8;\ (-8)\times(-3);\ (+8)\times(-3);\ (+8)\times(+5);\ \ldots$

Pour calculer les divers symboles, ainsi considérés, on peut utiliser la *loi de réciprocité*, bornée au cas d'un facteur δ, impair et congru à $+1$, mod. 4, ou égal à -4, $+8$, ou -8. Elle est alors exprimée par les égalités:

δ impair premier, congru à $+1$, mod. 4: $\left(\frac{\delta}{p}\right) = \left(\frac{p}{|\delta|}\right)$;

$\left(\frac{-4}{p}\right) = +1$ ou -1, suivant que $p \equiv +1$ ou -1, (mod. 4);

$\left(\frac{+8}{p}\right) = +1$ ou -1, suivant que $\begin{cases} p \equiv +1 \text{ ou } -1, \\ \text{ou} \\ p \equiv +3 \text{ ou } -3, \end{cases}$ (mod. 8);

$\left(\frac{-8}{p}\right) = +1$ ou -1, suivant que $\begin{cases} p \equiv +1 \text{ ou } +3, \\ \text{ou} \\ p \equiv -1 \text{ ou } -3, \end{cases}$ (mod. 8).

Il en résulte que, pour chaque facteur δ, considéré (y compris -4, $+8$, et -8), le symbole a la même valeur pour des nombres premiers p, congrus entre eux, mod. $|\delta|$ et, pour le calculer, on peut remplacer p par tout nombre congru, mod. $|\delta|$; notamment par le reste de sa division par $|\delta|$ (compris entre 1 et $|\delta|$ et premier avec $|\delta|$).

Les facteurs $|\delta_i|$ étant premiers entre eux, deux à deux, pour que des nombres soient simultanément congrus, suivant chacun d'eux, il faut et il suffit qu'ils soient congrus suivant leur produit $|D|$.

Les valeurs simultanées des symboles des facteurs δ_i et par suite celle de leur produit sont donc les mêmes pour tous les nombres premiers appartenant à une même progression arithmétique, de raison $|D|$; —donc congrus, mod. $|D|$— .

Dans les $\varphi(|\delta_i|)$ valeurs, incongrues, mod. $|\delta_i|$:

$|\delta_i|$ impair, $\varphi(|\delta_i|) = |\delta_i| - 1$; $\varphi(4) = 2$; $\varphi(8) = 4$;

la moitié ont un *symbole de* LEGENDRE positif. Un raisonnement simple de récurrence montre qu'il en est de même pour les

$\varphi(|D|) = \Pi\varphi(|\delta_i|)$ valeurs incongrues, mod. $|D| = \Pi|\delta_i|$.

Il y a $\varphi(|D|) : 2$ progressions pour lesquelles le symbole de

LEGENDRE est positif; les nombres premiers qui leur appartiennent sont ceux qui sont normes d'idéaux premiers conjugués distincts —ou diviseurs des valeurs du tableau, non diviseurs de $|D|$.

Le tableau III donne un exemple de calcul de ces progressions pour le corps de discriminant —39 (tableau I). On a calculé directement, sans utiliser les indices, les classes, mod. 3 et mod. 13, qui sont congrues à des carrés.

On obtient ainsi 12 progressions arithmétiques, on donne les premiers nombres premiers (inférieurs à 500) qui leur appartiennent;

TABLEAU III.

Corps de discriminant $D = -39 = (-3)\times(+13)$; $\varphi(39) = 24$.

Classes mod. 3: $1^2 \equiv 2^2 \equiv 1$,

Mod. 13: $\begin{cases} 1^2 \equiv 12^2 \equiv 1; & 2^2 \equiv 11^2 \equiv 4; & 3^2 \equiv 10^2 \equiv 9 \\ 4^2 \equiv 9^2 \equiv 3; & 5^2 \equiv 8^2 \equiv 12; & 6^2 \equiv 7^2 \equiv 10. \end{cases}$

$p \equiv a$ mod. 39	mod. 3	mod. 13	$\left(\frac{-3}{p}\right) = \left(\frac{a}{3}\right)$	$\left(\frac{13}{p}\right) = \left(\frac{a}{13}\right)$	$\left(\frac{-39}{p}\right)$
1	1	1	+1	+1	+1
2	2	2	—1	—1	+1
4	1	4	+1	+1	+1
5	2	5	—1	—1	+1
7	1	7	+1	—1	—1
8	2	8	—1	—1	+1
10	1	10	+1	+1	+1
11	2	11	—1	—1	+1
14	2	1	—1	+1	—1
16	1	3	+1	+1	+1
17	2	4	—1	+1	—1
19	1	6	+1	—1	—1
20	2	7	—1	—1	+1
22	1	9	+1	+1	+1
23	2	10	—1	+1	—1
25	1	12	+1	+1	+1
28	1	2	+1	—1	—1
29	2	3	—1	+1	—1
31	1	5	+1	—1	—1
32	2	6	—1	—1	+1
34	1	8	+1	—1	—1
35	2	9	—1	+1	—1
37	1	11	+1	—1	—1
38	2	12	—1	+1	—1

chacun d'eux est la norme de deux idéaux canoniques conjugués; dont l'un a une racine minimum positive c, indiquée entre parenthèses; la racine minimum de l'autre est $-1-c$ (ainsi qu'il est indiqué dans le tableau I, pour les premiers de ces idéaux, de normes 2 et 5):

$1+39\lambda$: 79 (17); 157 (39); 313 (141);
$2+39\lambda$: 2 (0); 41 (8); 197 (71); 353 (145); 431 (192);
$4+39\lambda$: 43 (20); 199 (44); 277 (66); 433 (41);
$5+39\lambda$: 5 (0); 83 (12); 239 (102); 317 (43);
$8+39\lambda$: 47 (16); 281 (23); 359 (53);
$10+39\lambda$: 127 (35); 283 (33); 439 (209);
$11+39\lambda$: 11 (3); 89 (26); 167 (31); 401 (89); 479 (169);
$16+39\lambda$: 211 (79); 367 (60);
$20+39\lambda$: 59 (21); 137 (28); 293 (113); 449 (189);
$22+39\lambda$: 61 (24); 139 (64); 373 (38);
$25+39\lambda$: 103 (47); 181 (46); 337 (100);
$32+39\lambda$: 71 (11); 149 (54); 227 (42); 383 (27); 461 (52).

Le tableau IV donne de même un exemple de calcul des progressions pour le corps de discriminant $+60$ (tableau II).

TABLEAU IV.

$F(x) = x^2-15$; $D = +60 = (-4)\times(-3)\times(+5)$; $\varphi(60) = 16$.

mod. 60	1	7	11	13	17	19	23	29	31	37	41	43	47	49	53	59
mod. 4	1	3	3	1	1	3	3	1	3	1	1	3	3	1	1	3
$\left(\frac{-4}{p}\right)$	+	−	−	+	+	−	−	+	−	+	+	−	−	+	+	−
mod. 3	1	1	2	1	2	1	2	2	1	1	2	1	2	1	2	2
$\left(\frac{-3}{p}\right)$	+	+	−	+	−	+	−	−	+	+	−	+	−	+	−	−
mod. 5	1	2	1	3	2	4	3	4	1	2	1	3	2	4	3	4
$\left(\frac{5}{p}\right)$	+	−	+	−	−	+	−	+	+	−	+	−	−	+	−	+
$\left(\frac{60}{p}\right)$	+	+	+	−	+	−	−	−	−	−	−	+	−	+	+	+

On obtient 8 progressions arithmétiques, dont on donne encore les premiers nombres premiers (inférieurs à 500), ainsi que la norme minimum positive de l'un des idéaux dont ils sont la norme:

$1+15\lambda$: 61 (25); 181 (14); 241 (16); 421 (65);
$7+15\lambda$: 7 (1); 67 (22); 127 (53); 307 (130); 367 (105); 487 (224);
$11+15\lambda$: 11 (2); 71 (21); 131 (43); 191 (46); 251 (39); 311 (126); 431 (51); 491 (83);
$17+15\lambda$: 17 (7); 137 (17); 197 (58); 257 (23); 317 (40);
$43+15\lambda$: 43 (12); 103 (18); 163 (34); 223 (98); 283 (79); 463 (101);
$49+15\lambda$: 109 (48); 229 (106); 349 (109); 409 (158);
$53+15\lambda$: 53 (11); 113 (44); 173 (19); 233 (99); 293 (111); 353 (108);
$59+15\lambda$: 59 (29); 179 (33); 239 (60); 359 (71); 419 (68); 479 (203).

Il y a une infinité de nombres premiers vérifiant les conditions précédentes, donc d'*idéaux premiers du premier degré*, dans tout corps quadratique.

On peut le démontrer en s'inspirant du raisonnement arithmétique qui est utilisé couramment pour démontrer l'existence d'une infinité de nombres premiers. On forme le produit C, des m premiers nombres premiers p_i, à l'exception des diviseurs du discriminant D. Le nombre entier C^2-D admet un diviseur premier p, supérieur à tous les p_i, et qui vérifie la condition imposée [1]).

23. Congruence et classes d'idéaux.

De même qu'on a construit le groupe quotient $\mathcal{G}|\mathfrak{L}$, des classes du groupe $\mathcal{G}(\theta)$, relativement au sous-groupe $\mathfrak{L}$, des

[1]) Cette propriété résulte aussi du *théorème de la progression arithmétique*, qui affirme l'existence d'une infinité de nombres premiers dans chacune des progressions arithmétiques, construites comme il a été dit, de raison $|D|$ et dont les premiers termes sont premiers avec $|D|$. Ceci montre aussi bien l'existence d'une infinité d'idéaux premiers du second degré —ou de nombres premiers ne vérifiant pas la condition imposée—. On pourrait aussi en donner une démonstration directe, mais sans distinguer l'appartenance des normes aux différentes progressions.