6. Congruence fondamentale (module composé).

l'existence d'un zéro est équivalente à celle d'un nombre entier $(2c—S)$, dont le carré est congru à D, mod. p.

Pour le *module premier* $p = 2$, il n'y a que deux classes d'entiers, représentés respectivement par 0 et 1; il suffit de former les valeurs qu'elles donnent à $F(x) = x^2+x+N$:

$$F(0) \equiv F(1) \equiv N, \quad (\text{mod. } 2);$$

d'où la condition d'existence.

2. Pour un *module premier impair* p, *diviseur de* D, l'expression de $4F(x)$ est congrue à:

$$4F(x) = (2x—S)^2—D \equiv (2x—S)^2, \quad (\text{mod. } p);$$

elle montre qu'il existe un et un seul zéro c, mod. p, qui rend $(2c—S)$ divisible par p. Suivant le cas, il est congru à:

$$c \equiv 0, \quad \text{si } S = 0; \qquad c \equiv \frac{p—1}{2}, \quad \text{si } S = —1.$$

Pour le *module* 2, lorsque D est pair, S est nul, la congruence:

$$x^2+N \equiv 0, \quad (\text{mod. } 2)$$

a une et une seule solution (zéro double), congrue à:

$$0, \quad \text{si } N \text{ est pair}; \qquad 1, \quad \text{si } N \text{ est impair}.$$

Pour $p = 1$, la propriété est triviale, il n'y a qu'une seule classe, formée de tous les nombres entiers et elle est zéro double de $F(x)$.

6. Congruence fondamentale (module composé).

On considère d'abord un *module primaire* —ou puissance d'un nombre premier > 1— .

Théorème de la congruence fondamentale pour un module primaire. Relativement à un *module* p^h, puissance (d'exposant h, entier positif), d'un nombre premier p, différent de 1, le polynôme fondamental $F(x)$:

1° *n'a pas de zéro*, pour tout exposant h, s'il n'en a pas pour $h = 1$ —ou si la congruence est impossible, mod. p— ;

2° *n'a pas de zéro*, pour h supérieur à 1, s'il a un *zéro double* pour $h = 1$ —ou si D est divisible par p— ;

3° a un et un seul *couple de zéros conjugués, incongrus*, s'il en est ainsi pour $h = 1$ —ou si la congruence est possible, mod. p; et p non diviseur de D— .

Les trois conditions suffisantes énumérant tous les cas possibles, le théorème exprime une *propriété caractéristique d'existence des zéros.*

1. S'il existe un zéro c_h, mod. p^h, il l'est, à fortiori, mod. p; c'est la propriété contraposée de l'énoncé.

2. Dans le cas d'un *module premier impair* p, différent de 1, diviseur du discriminant D, on peut encore utiliser $4F(x)$. Tout zéro, c, mod. p^h, l'est, à fortiori, mod. p; il rend $(2x—c)$ divisible par p et $(2x—S)^2$ divisible par p^2, d'où la congruence:

$$4F(c) = (2c—S)^2—D \equiv —D, \quad (\text{mod. } p^2).$$

L'existence d'un zéro c, mod. p^h, pour $h > 1$; donc, à fortiori, mod. p^2; entraînerait la divisibilité de D par p^2, ce qui est contraire à la définition du polynôme fondamental, dont le discriminant ne peut avoir de facteur carré impair.

Dans le cas du *module* 2^h et d'un polynôme de *discriminant pair*, donc de la forme x^2+N, tout zéro, mod. 2^h, donc, à fortiori mod. 2, ne peut être que de la forme:

$$0+2\lambda, \quad \text{si } N \text{ est pair}; \qquad 1+2\lambda, \quad \text{si } N \text{ est impair.}$$

Les valeurs de $F(x)$, pour ces nombres, sont congrues à

$$(2\lambda)^2+N \equiv N, \qquad (1+2\lambda)^2+N \equiv 1+N, \quad (\text{mod. } 4).$$

L'existence d'un zéro; mod. 2^h, pour $h > 1$; donc, à fortiori, mod. 4; entraînerait la divisibilité de N, ou de $1+N$, par 4; ce qui est aussi contraire à la définition du polynôme fondamental (**1**), puisque, dans le premier cas $N = —d$, est sans diviseur carré, et que dans le second cas $1+N = 1—d$ n'est pas divisible par 4.

3. On peut établir la propriété par récurrence sur h, en supposant qu'il existe un et un seul couple de zéros, c_h c'_h, conjugués, incongrus, mod. p^h (ce qui est vrai pour $h = 1$). S'il en existe mod. p^{h+1}, ils le sont, à fortiori, mod. p^h, donc de l'une des formes:

$$c_h+\lambda p^h, \qquad \text{ou} \qquad c'_h+\lambda' p^h; \qquad \lambda,\lambda' \text{ entiers.}$$

On calcule les valeurs qu'ils donnent à $F(x)$; pour le premier:

$$F(c_h+\lambda p^h) \equiv F(c_h)+\lambda p^h.\dot{F}(c_h), \quad (\text{mod. } p^{h+1});$$

on a supprimé des termes du développement en λ, qui sont multiples de p^{2h}, donc à fortiori, de p^{h+1}. La valeur ainsi obtenue est divisible par p^h, il suffit de chercher si son quotient par cette puissance peut être divisible par p, d'où la congruence:

$$|F(c_h): p^h|+\lambda.\dot{F}(c_h) \equiv 0, \quad (\text{mod. } p).$$

Or c_h étant zéro, mod. p_h, l'est aussi mod. p et il ne peut être double, en raison de la propriété 2, précédente. La dérivée, coefficient de λ, n'est donc pas nulle, mod. p, cette équation du premier degré en λ a une et une seule solution, qui peut être désignée par λ_h, on obtient ainsi un zéro déterminé:

$$c_{h+1} \equiv c_h+\lambda_h p^h, \quad (\text{mod. } p^{h+1}).$$

On obtient de même un zéro déterminé $c'_h+\lambda'_h.p^h$, de la deuxième forme; ces deux zéros sont incongrus, puisque leur différence:

$$c_{h+1}-c'_{h+1} \equiv c_h-c'_h, \quad (\text{mod. } p^h)$$

n'étant pas divisible par p^h, ne peut l'être par p^{h+1}. Comme ce sont les deux seuls zéros, ils sont conjugués et leur somme est congrue à S.

L'application de la récurrence, depuis $h = 1$, permet d'écrire ces zéros, en partant des zéros, mod. p:

$$\left.\begin{aligned} c_{h+1} &\equiv c_1+\lambda_1 p+\ldots+\lambda_h p^h, \\ c'_{h+1} &\equiv c'_1+\lambda'_1 p+\ldots+\lambda'_h p^h; \end{aligned}\right\} \quad (\text{mod. } p^{h+1}).$$

La somme de ces deux développements, limités à l'indice k, est congrue à S, mod. p^{k+1} [1].

THÉORÈME de la congruence fondamentale pour un module composé. — Pour un module égal au produit de plusieurs puissances de nombres premiers différents:

$$m = \Pi m_i; \quad m_i = p_i^{hi}; \quad p^i \text{ premier} \neq 1; \quad i \text{ de } 1 \text{ à } s;$$

le polynôme fondamental a des couples de zéros conjugués si et seulement si:

1° pour tout facteur premier p_i, *diviseur du discriminant* D, *l'exposant* h_i *est égal à* 1 ($m_i = p_i$);

2° pour tout facteur premier p_j, *premier avec* D, *la congruence, mod.* p_j, *est possible* —ou le polynôme a deux zéros conjugués incongrus— .

Si ces deux conditions sont remplies et si $s' \leqslant s$ est le nombre de facteurs premiers p_j (ou m_j) premiers avec D, il y a $2^{s'}$ *zéros incongrus*. Si s' n'est pas nul, ils sont répartis en $2^{s'-1}$ *couples de zéros conjugués*; si $s' = 0$; ils se réduisent à un *zéro double*; m étant d'ailleurs alors diviseur de D.

Les conditions sont *nécessaires*: si l'une, au moins, n'était pas vérifiée pour un facteur m_i, ou m_j, le polynôme n'aurait pas de zéro relativement à ce facteur, donc, à fortiori, relativement au module m, qui en est un multiple.

Les conditions sont *suffisantes*: pour chaque facteur m_i, diviseur de D, le polynôme $F(x)$ a un zéro c_i (double); pour chaque facteur m_j, premier avec D, il a deux zéros (conjugués) c_j et c_j'. Tout zéro c de $F(x)$, mod. m, doit alors vérifier l'un des systèmes de s congruences:

$$c \equiv c_i, \quad (\text{mod. } m_i); \qquad c \equiv c_j \quad \text{ou} \quad c \equiv c_j', \quad (\text{mod. } m_j).$$

---

[1]) La démonstration de cette existence aurait pu être faite sans utiliser nommément la dérivée $\dot{F}(x)$. Sous la forme adoptée, elle est valable pour un polynôme $F(x)$, de degré quelconque, à coefficients entiers et normé. Si ce polynôme a, relativement à un module premier p, un zéro c, qui n'annule pas sa dérivée $\dot{F}(x)$, il a, relativement à tout module p^h (h entier positif), un zéro c^h congru à c, mod. p. Cette propriété, qui peut encore être énoncée sous une forme plus générale (existence d'un polynôme, de degré quelconque diviseur de $F(x)$), est connue sous le nom de *lemme de* HENSEL.

Chacun des systèmes a une solution déterminée, mod. m, puisque les s modules m_i sont premiers entre eux deux à deux et que leur produit est égal à m [1].

Dans la formation d'un système de congruences, pour chacun des s' modules m_j, premiers avec D, on peut choisir entre deux congruences. Il y a donc bien $2^{s'}$ systèmes, d'où le nombre de zéros indiqué. Leur répartition en couples conjugués en résulte; on passe d'ailleurs d'un zéro c à son conjugué c', en changeant le choix dans chacune des congruences, mod. m_j.

Pour m diviseur de D et sans facteur carré, il n'y a qu'un système de s congruences, qui détermine un zéro double. Il peut être obtenu par les règles suivantes:

$$\begin{array}{ll} D \text{ impair; } m \text{ impair} & \\ D = 4d;\ d \text{ impair, } m \text{ pair:} & c \equiv (m+S):2 \begin{cases} \equiv (m-1):2, & (\text{mod. } m); \\ \equiv m:2, & (\text{mod. } m); \end{cases} \\ D = 4d;\ m \text{ diviseur de } d; & c \equiv 0, \quad (\text{mod. } m). \end{array}$$

7. Idéaux canoniques.

L'extension de la théorie de la *divisibilité* (arithmétique) à un corps quadratique $\mathbf{R}(\theta)$ et au domaine de ses entiers (algébriques) $\mathbf{E}(\theta)$ a conduit à considérer, dans $\mathbf{R}(\theta)$, des sous-ensembles particuliers, appelés *idéaux*.

On peut donner d'un idéal une *définition constructive*, en le caractérisant par deux de ses éléments, convenablement choisis, qui en constituent une *base canonique* et, à partir desquels, il est

---

[1]) La résolution d'un système de deux congruences:

$$x \equiv a_1, \quad (\text{mod. } m_1) \qquad x \equiv a_2, \quad (\text{mod. } m_2);$$

est équivalent à la résolution de l'équation en λ:

$$a_1 + \lambda m_1 \equiv a_2, \quad (\text{mod. } m_2);$$

elle est possible et déterminée si m_1 et m_2 sont premiers entre eux et la solution du système est de la forme:

$$a_1 + (\lambda_1 + u m_2) \times m_1 = b + u \times (m_1 \times m_2);$$

elle est déterminée, [module $m = m_1 \times m_2$].

Cette construction s'étend, de proche en proche, ou par récurrence sur s, à un système de s congruences dont les modules sont premiers entre eux deux à deux.