SUR LES CONGRUENCES DU TROISIÈME DEGRÉ

Autor(en): **Cailler, C.**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **10 (1908)**

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **10.08.2024**

Persistenter Link: https://doi.org/10.5169/seals-10984

comme le point culminant des mathématiques à l'école. Mais il y a un fort courant, aujourd'hui, en faveur d'un usage précoce de ce calcul. On n'a pas encore précisé à quel moment il peut être commencé, mais il est prouvé qu'une connaissance minime de différentiation et d'intégration simplifie et généralise l'étude de la Géométrie analytique et de la Cinématique, sujets auxquels la tradition assigne un rang antérieur.

C. GODFREY (Osborne).

SUR LES CONGRUENCES DU TROISIÈME DEGRÉ

---

§ 1. — A propos d'un livre récent de M. G. ARNOUX[1], M. D. MIRIMANOFF[2] a présenté aux lecteurs de ce journal quelques observations sur les congruences du troisième degré et les conditions de leur résolubilité. On sait que la détermination effective des racines d'une congruence binôme s'effectue le plus souvent en calculant, dans la série des puissances de la base, un terme dont le rang est assigné par les propositions les plus simples de la théorie des nombres. Comme on peut, par une transformation linéaire, ramener l'équation du troisième degré à la forme cubique pure, on doit présumer que cette même méthode, convenablement modifiée, permettra non-seulement de discerner les cas de résolubilité de la congruence cubique, mais encore d'en trouver les racines au moins dans la majeure partie des cas. En développant cette idée, on reconnaît aisément que la théorie des congruences du troisième degré peut être rattachée à celle des suites récurrentes du second ordre à échelle de relation constante; la résolution se fait alors suivant une marche de tout point comparable à celle donnée par Gauss pour les congruences du deuxième degré.

Un ancien mémoire de G. OLTRAMARE[3] contient dans cette

---

[1] *Arithmétique graphique. Introduction à l'étude des fonctions arithmétiques.* Paris, 1906.
[2] *L'Enseign. Math.*, 1907, p. 381-384.
[3] *Journ. de Crelle*, 1853, t. 45, p. 316.

direction d'intéressants essais et un grand nombre de résultats particuliers. Mais cet auteur ne me semble pas avoir porté la méthode au degré de précision et de simplicité qu'elle doit recevoir pour devenir vraiment applicable, et ses théorèmes sont restés peu connus. On me permettra donc de revenir sur cette question après l'article de M. Mirimanoff auquel celui-ci servira de complément. Les résultats précédemment énoncés se présenteront d'ailleurs à nous d'une manière toute naturelle.

§ 2. — Commençons par rappeler succinctement les principales propriétés algébriques et numériques des récurrences du second ordre.

Soient r et s deux nombres entiers premiers entre eux, a et b les racines de l'équation $\omega^2 - r\omega - s = 0$ donnant

$$a + b = r , \quad \text{et} \quad ab = -s .$$

Nous supposons a et b inégaux, ou le discriminant

$$r^2 + 4s = (a - b)^2 \neq 0 .$$

La récurrence est définie par les termes initiaux u_0, u_1, et par la loi de formation des suivants

$$u_{n+1} = ru_n + su_{n-1} .$$

On sait que toutes les solutions de cette équation aux différences sont linéairement composées avec deux quelconques d'entre elles; nous choisirons pour celles-ci les suivantes

$$x_n = a^n + b^n , \quad \text{et} \quad y_n = \frac{a^n - b^n}{a - b} ,$$

correspondant aux valeurs initiales $x_0 = 2$, $x_1 = r$, et $y_0 = 0$, $y_1 = 1$. La seconde nous servira presque seule; la récurrence correspondante 0, 1, r, $r^2 + s$, ... sera souvent représentée par la notation $[r, s]$. La première solution se ramène d'ailleurs immédiatement à la seconde à cause de la relation $x_n y_n = y_{2n}$.

L'identité

$$(a^{m+1} - b^{m+1})(a^n - b^n) - ab(a^m - b^m)(a^{n-1} - b^{n-1}) = (a - b)(a^{m+n} - b^{m+n}) ,$$

donne la propriété fondamentale

$$y_{m+n} = y_{m+1}y_n - aby_m y_{n-1}, \tag{1}$$

$$= y_m y_{n+1} - aby_n y_{m-1}. \tag{2}$$

En y faisant $m = 2$, on retrouve la récurrence de définition

$$y_{n+2} = (a + b)y_{n+1} - aby_n ;$$

de même, si l'on pose $m = n$ ou $m = n + 1$, on aura les formules de duplication

$$y_{2n} = y_n(2y_{n+1} - (a + b)y_n), \tag{3}$$

$$y_{2n+1} = y_{n+1}^2 - aby_n^2, \tag{4}$$

dont la première s'écrit aussi

$$x_n = y_{n+1} - aby_{n-1}.$$

Par la même voie on obtiendra les formules de triplication qu'il convient de remarquer à cause de leur rapport avec les congruences du troisième degré ; ce sont

$$y_{3n} = (a^2 + ab + b^2)y_n^3 - 3(a + b)y_n^2 y_{n+1} + 3y_n y_{n+1}^2, \tag{5}$$

$$y_{3n+1} = y_{n+1}^3 - 3aby_{n+1}y_n^2 + ab(a + b)y_n^3, \tag{6}$$

$$y_{3n+2} = a^2b^2y_n^3 - 3aby_n y_{n+1}^2 + (a + b)y_{n+1}^3. \tag{7}$$

Observons enfin que l'ensemble des quantités $z_n = y_{pn+q}$, où p et q désignent des paramètres fixes, tandis que n parcourt toute la série des valeurs entières 0, 1, 2, ..., autrement dit la suite des quantités y prises de p en p à partir de y_q, forme une nouvelle récurrence du second ordre dans laquelle les quantités a^p et b^p jouent le rôle assigné précédemment à a et b eux-mêmes. En particulier, la série

$$y_0, y_p, y_{2p}, \ldots y_{np}, \ldots$$

dont tous les termes sont divisibles par y_p, a pour terme général

$$y_{np} = \frac{a^{np} - b^{np}}{a - b} = \frac{a^p - b^p}{a - b}\,\frac{a^{np} - b^{np}}{a^p - b^p} = y_p Y_n .$$

Cette suite $Y_0, Y_1, \ldots$ avec les valeurs initiales $Y_0 = 0$, $Y_1 = 1$, n'est autre que la récurrence $[a^p + b^p, -a^p b^p]$. Si D est le discriminant de cette récurrence, d celui de la suite primitive $[a + b, -ab]$, on a

$$D = (a^p - b^p)^2 \qquad d = (a - b)^2 ,$$

et par conséquent

$$D = d y_p^2 .$$

§ 3. — Passons maintenant aux propriétés arithmétiques des quantités y_n, et rappelons que les nombres $r = a + b$, et $s = -ab$, ont été supposés premiers entre eux.

Dans cette hypothèse tous les y_n sont premiers avec ab. Car x_{n-1} étant entier, on voit par l'équation

$$x_{n-1} = y_n - aby_{n-2}$$

que tout facteur commun à y_n et ab diviserait aussi x_{n-1}. Or

$$x_{n-1} = a^{n-1} + b^{n-1} = (a + b)^{n-1} - abE ,$$

E désignant un entier. Le facteur commun supposé ne saurait donc être premier avec $(a + b)$, ce qui implique contradiction.

En second lieu, deux y_n consécutifs tels que y_n, y_{n+1}, sont premiers entre eux.

Car, puisque

$$y_{n+1} = (a + b)y_n - aby_{n-1} ,$$

tout facteur commun à ces deux quantités, étant premier avec ab, devrait diviser y_{n-1}, et ainsi de suite en rétrogradant jusqu'à $y_1 = 1$.

Grâce à cette double propriété la détermination des diviseurs communs à deux nombres y_m, y_n n'offre aucune difficulté ; nous allons voir que, θ désignant le plus grand commun diviseur entre m et n, y_θ sera celui de y_m et y_n.

En effet, en vertu des égalités

$$y_{m+n} = y_{n+1}y_m - aby_n y_{m-1} ,$$
$$y_m = y_{m-n+1}y_n - aby_{m-n}y_{n-1} ,$$

on voit que tout facteur commun à y_m et y_n divisera y_{m+n} et y_{m-n}, donc aussi $y_{m\alpha-n\beta}$, α et β étant deux arbitraires. On sait que ces dernières peuvent être choisies de manière que $m\alpha - n\beta = \theta$. En outre y_θ est diviseur de y_m et de y_n; c'est donc bien le plus grand commun diviseur cherché.

Déterminons, en troisième lieu, la forme des facteurs premiers l des y_n. Observons que $\sqrt{d} = a - b$ est, en général, une irrationnelle algébrique qui disparaît de la formule

$$y_n = \frac{a^n - b^n}{a - b} = a^{n-1} + a^{n-2} b + \ldots + ab^{n-2} + b^{n-1} . \qquad (8)$$

Rien n'empêche dès lors, quand on cherche le reste de y_n selon le module l, de supprimer dans les expressions a^n ou b^n les termes, même irrationnels, qui contiennent le module en facteur. En d'autres termes, si a et a' sont deux entiers algébriques du domaine $\sqrt{d}$, quand $a' \equiv a$, on a aussi $a'^n \equiv a^n$.

Distinguons plusieurs cas et remarquons qu'aucun des facteurs l cherchés ne peut diviser ab, comme on a vu plus haut; ainsi aucun des nombres a et b ne peut être divisible par l.

1° Si l est diviseur du discriminant, on a $a \equiv b \equiv \frac{r}{2}$; par suite, le second membre de l'équation (8) donne

$$y_l \equiv 0 , \qquad (\text{mod } l)$$

et de même, comme on voit aisément,

$$y_{l^\nu} \equiv 0 \quad \text{et} \quad y_{l^\nu m} \equiv 0 . \qquad (\text{mod } l^\nu)$$

2° Si d est résidu quadratique de l, a et b sont réels (mod l), différents entre eux, et tous deux différents de zéro.

On a donc

$$a^{l-1} \equiv b^{l-1} \equiv 1 ,$$

par suite

$$y_{l-1} \equiv 0 . \qquad (\text{mod } l)$$

3° Si d est non-résidu quadratique, a et b sont des imaginaires de Galois dans le domaine $\sqrt{\text{N}}$, N désignant un non-résidu quelconque. Comme a et b sont conjugués

$$a = m + n\sqrt{\text{N}} \qquad b = m - n\sqrt{\text{N}} .$$

on aura

$$a^l \equiv m^l + n^l \mathrm{N}^{\frac{l-1}{2}} \sqrt{\mathrm{N}} \equiv b$$

et de même $b^l \equiv a$. Donc $a^{l+1} \equiv b^{l+1} \equiv ab$, par suite

$$y_{l+1} \equiv 0 . \pmod{l}$$

De là résultent deux propriétés fondamentales.

Si M est un module quelconque, premier avec ab, et décomposé en ses facteurs premiers sous la forme

$$\mathrm{M} = l^{\lambda} l'^{\lambda'} l''^{\lambda''} \ldots ,$$

il existera toujours des y_n admettant M comme diviseur.

On aura par exemple $y_n \equiv 0 \pmod{\mathrm{M}}$, si $n = \psi(\mathrm{M})$, avec

$$\psi(\mathrm{M}) = l^{\lambda-1} l'^{\lambda'-1} \ldots (l + \varepsilon)(l' + \varepsilon') \ldots ;$$

on pose $\varepsilon = 0, -1$, ou $+1$ selon que d est multiple de l, résidu quadratique, ou non-résidu de l ; autrement dit

$$-\varepsilon = \left(\frac{d}{l}\right) .$$

Le fait a été déjà établi plus haut pour $\varepsilon = 0$, puisque dans ce cas $\psi(\mathrm{M})$ est divisible par l^{λ} et y_n aussi. Si $\varepsilon = \mp 1$, on posera $\psi(\mathrm{M}) = (l \mp 1)\,\mathrm{M}'$, et $y_n = y_{l\mp 1}\,\mathrm{Y}_{\mathrm{M}'}$. Or le discriminant D de la récurrence $\mathrm{Y}_{\mathrm{M}'}$, étant égal à $d y_{l\mp 1}^2$, sera divisible par l, puisque $y_{l\mp 1}$ est divisible ; donc $\mathrm{Y}_{\mathrm{M}'}$ sera divisible par $l^{\lambda-1}$, comme on vient de le voir, et y_n le sera par l^{λ}. On prouverait de même la divisibilité par $l'^{\lambda'}$, $l''^{\lambda''}$...

Si on nomme, en second lieu, diviseurs *propres* de y_n ceux qui n'appartiennent à aucun nombre $y_{n'}$ d'indice inférieur à n, il est facile de constater que tous les facteurs premiers propres de y_n sont contenus dans la formule

$$l = np \pm 1 , \qquad (9)$$

le signe étant $+$ ou $-$ selon que d est ou n'est pas résidu quadratique de l.

En effet on a, par supposition, $y_n \equiv 0 \pmod{l}$, mais aussi

$y_{l\mp1} \equiv 0$, et si $l \mp 1$ n'était pas divisible par n, on aurait $y_\theta \equiv 0$, pour un nombre $\theta < n$, à savoir le plus grand commun diviseur de n et $l \mp 1$. La démonstration n'est évidemment pas valable pour les facteurs premiers diviseurs du discriminant ; un tel nombre l est diviseur propre de y_l.

J'ajoute qu'on pourra, dans la recherche des facteurs premiers, limiter souvent les essais exigés par la formule (9). Si, par exemple, l'indice n est impair, la formule de duplication

$$y_{2m+1} = y_{m+1}^2 - aby_m^2 ,$$

montre que les facteurs cherchés admettent ab comme résidu quadratique ; on exclura tous ceux qui ne vérifieraient pas cette condition supplémentaire.

Observons enfin que si on a $y_n \equiv 0 \pmod{l}$, on aura à cause de (2)

$$y_{pn+q} \equiv y_{n+1}^p y_q ,$$

et par conséquent

$$y_{pn+q} : y_{pn+q'} \equiv y_q : y_{q'} . \qquad \pmod{l}.$$

§ 4. — Après ces préliminaires, qui ne sont pas indispensables mais jettent une vive clarté sur ce qui suit, venons à la congruence du troisième degré

$$x^3 + px + q \equiv 0 . \qquad \pmod{l > 3}.$$

Nous adopterons, pour la résoudre, une marche analogue à celle qui donne en Algèbre la racine de l'équation cubique et conduit à la formule de Cardan. Parmi les différentes manières d'obtenir cette dernière, prenons la suivante.

J'écris la proposée sous la forme

$$x^3 - 3abx + ab(a + b) \equiv 0 , \qquad \pmod{l} \quad (10)$$

en déterminant a et b par la résolvante

$$z^2 + \frac{3q}{p} z - \frac{p}{3} \equiv 0 , \qquad \pmod{l} \quad (11)$$

dont il est aisé de trouver la relation avec les fonctions cycliques. Si x_0, x_1, x_2 représentent trois racines hypothé-

tiques de (10), et α une racine de $\alpha^2 + \alpha + 1 \equiv 0 \pmod{l}$, on trouve en effet facilement

$$z \equiv \frac{(x_0 + \alpha x_1 + \alpha^2 x_2)^3}{9p} . \qquad (12)$$

Les relations entre les racines et les coefficients de (11) donnent encore

$$ab \equiv -\frac{p}{3} , \qquad a + b \equiv -\frac{3q}{p} , \qquad (a-b)^2 \equiv \frac{4p^3 + 27q^2}{3p^2} .$$

Nous exclurons le cas où la proposée serait binôme, ou p divisible par l. Si $4p^3 + 27q^2 = \Delta$ était divisible par l, on voit que a et b seraient congrus entre eux, chacun d'eux valant $-\frac{3q}{2p} \pmod{l}$. Mais alors la congruence proposée admettrait cette même racine, car on a,

$$a^3 + pa + q \equiv a^3 - 3a^2b + ab(a+b) \equiv a(a-b)^2 \equiv 0 ,$$
$$b^3 + pb + q \equiv b^3 - 3b^2a + ab(a+b) \equiv b(a-b)^2 \equiv 0 .$$

La dite racine fonctionne, en outre, comme racine double, et ce cas est le seul où la congruence puisse posséder une racine multiple, ainsi qu'on le démontre immédiatement.

Nous le laisserons encore de côté; il ne reste dès lors plus que deux éventualités. Si 3Δ est résidu quadratique de l, a et b sont réels et distincts; si 3Δ est non-résidu, ce sont des imaginaires congruentielles dans le domaine $\sqrt{N}$; dans ce dernier cas nous élargissons le problème en essayant de résoudre la congruence dans le même domaine de rationalité. Remarquons que, quelle que soit la nature de a et b, les quantités $a + b$ ou $-\frac{3q}{p}$, ab ou $-\frac{p}{3}$, peuvent toujours être supposées entières et sans facteurs communs, puisque, r et s étant deux de leurs valeurs (mod l), la suite linéaire $r + ml$, qui est l'expression générale de la première d'entre elles, contient une infinité de nombres premiers. Nous admettrons donc constamment que r et s sont premiers entre eux.

Cela posé, et x désignant toujours une racine de (10), qui ne saurait être ni a ni b, posons

$$y \equiv \frac{x-a}{x-b} , \qquad \text{ou} \qquad x \equiv \frac{a-by}{1-y} ,$$

substitution qui transforme la proposée en

$$\alpha y^3 + \beta y^2 + \gamma y + \delta \equiv 0 ,$$

avec les valeurs suivantes des coefficients

$$\begin{aligned}
\alpha &= -(b^3 + pb + q) = -b(a-b)^2 , \\
\delta &= a^3 + pa + q = a(a-b)^2 , \\
\gamma &= -3a^2b + 3ab(b+2a) - 3ab(a+b) = 0 , \\
\beta &= 3ab^2 - 3ab(a+2b) + 3ab(a+b) = 0 .
\end{aligned}$$

La transformée est donc simplement

$$y^3 \equiv \frac{a}{b} , \qquad (\text{mod } l)$$

et sa résolution formelle donne pour x la valeur

$$x \equiv -(ab)^{1/3}(a^{1/3} + b^{1/3}) , \qquad (\text{mod } l)$$

dans laquelle on reconnaît la formule de Cardan. Il est, du reste, préférable de prendre pour la solution l'ensemble des formules

$$x \equiv \frac{a - by}{1 - y} \qquad \text{et} \qquad y^3 \equiv \frac{a}{b} .$$

Nous poserons, pour abréger, $A = \frac{a}{b}$, et nous distinguerons maintenant quatre cas.

Premier cas. — Le module l est de la forme $3m - 1$, 3Δ en est résidu quadratique, A est réel. Alors, de la condition $y^{3m-2} \equiv 1$ et de la congruence $y^3 \equiv \frac{a}{b}$, on tire

$$y \equiv \left(\frac{b}{a}\right)^{m-1} ,$$

puis, pour la seule racine de la proposée,

$$x \equiv \frac{a^m - b^m}{a^{m-1} - b^{m-1}} \equiv \frac{y_m}{y_{m-1}} .$$

La suite auxiliaire $y_0, y_1, \ldots$ est formée avec l'échelle de relation $[a + b, -ab]$; on le voit, pour résoudre (10), il sera inutile de calculer a et b. La formule de triplication (6) permet d'ailleurs de vérifier immédiatement le résultat qu'on vient d'obtenir.

Soit, comme exemple, à résoudre la congruence

$$x^3 - 3x + 3 \equiv 0 . \qquad \pmod{521}$$

On a ici $(a - b)^2 = 5$ et $\left(\frac{5}{521}\right) = 1$; ainsi la congruence n'a qu'une racine, qui vaut $x \equiv \frac{y_{174}}{y_{173}}$, la récurrence ayant comme échelle de relation [3, — 1]. On peut écrire aussi $x \equiv \frac{y_{348}}{y_{346}}$ les y étant calculés maintenant suivant la récurrence de Fibonacci [1, 1]. Dans cette dernière supposition, on a, comme on voit aisément, $y_{26} \equiv 0 \pmod{521}$, et en employant la réduction mentionnée à la fin du § 3, on obtient

$$x \equiv \frac{y_{348}}{y_{346}} \equiv \frac{y_{10}}{y_8} \equiv \frac{55}{21} \equiv 474 .$$

Comme second exemple, considérons la congruence

$$x^3 + 3x - p \equiv 0 ; \qquad \pmod{l = 3m - 1}$$

on suppose toujours $\left(\frac{p^2 + 4}{l}\right) = 1$, et on a

$$ab \equiv -1 \qquad a + b \equiv p \qquad (a - b)^2 \equiv p^2 + 4 ,$$

d'où l'on conclut, m étant pair et $m - 1$ impair,

$$a^{3m} - b^{3m} \equiv (a^m - b^m)^3 + 3(a^m - b^m) ,$$

$$a^{3m-3} - b^{3m-3} \equiv (a^{m-1} - b^{m-1})^3 - 3(a^{m-1} - b^{m-1}) ,$$

ou

$$y_{3m} \equiv (a - b)^2 y_m^3 + 3y_m ,$$

$$y_{3m-3} \equiv (a - b)^2 y_{m-1}^3 - 3y_{m-1} .$$

Mais, par suite des propriétés de divisibilité, $y_{3m-3} \equiv 1$, $y_{3m-2} \equiv 0$, $y_{3m-1} \equiv 1$, $y_{3m} \equiv p$ et enfin $x \equiv \frac{y_m}{y_{m-1}}$. On obtient ainsi le théorème que voici.

Si p est un entier tel que $p^2 + 4$ soit résidu d'un nombre premier $l = 3m - 1$, chacune des congruences

$$x^3 + 3x - p \equiv 0 ,$$
$$(p^2 + 4)y^3 + 3y - p \equiv 0 ,$$
$$(p^2 + 4)z^3 - 3z - 1 \equiv 0 ,$$

admet une seule racine (mod l), et l'on a entre ces trois racines la relation $y \equiv xz$. On prouvera, au reste, facilement que ces trois congruences se transforment l'une dans l'autre par substitution linéaire.

Deuxième cas. — Le module l est de la forme $3m + 1$, et 3Δ en est résidu quadratique, $\left(\frac{3\Delta}{l}\right) = 1$; a et b sont de nouveau réels ainsi que leur quotient A. Ce dernier devant être résidu cubique, la congruence ne sera résoluble que si $A^m \equiv 1$, autrement dit si le nombre y_m de la récurrence auxiliaire $[a + b, -ab]$ est $\equiv 0$. Quand cette condition est satisfaite, y a trois valeurs qui se suivent cycliquement, et la proposée aura trois racines.

Supposons que m ne soit pas divisible par 3, ou plus généralement, que l'indice n auquel appartient A (mod l) soit de l'une des deux formes $n = 3\mu \mp 1$, l'identité

$$A^{3\mu} \equiv A \qquad \text{ou} \qquad A^{-3\mu} \equiv A$$

montre qu'une des valeurs de y sera, selon le cas,

$$y \equiv \left(\frac{a}{b}\right)^{\mu}, \qquad \text{ou} \qquad y \equiv \left(\frac{b}{a}\right)^{\mu}.$$

Quant à x, une des trois valeurs qu'il peut prendre, sera en conséquence

$$n = 3\mu - 1 \qquad x \equiv ab\,\frac{y_{\mu-1}}{y_{\mu}} \equiv \frac{y_{2\mu}}{y_{2\mu-1}},$$

$$n = 3\mu + 1 \qquad x \equiv \frac{y_{\mu+1}}{y_{\mu}}.$$

Les deux autres racines ne s'expriment pas par la suite y_n. Soit, par exemple, la congruence

$$x^3 - 3x + 3 \equiv 0 \qquad \text{(mod 3001)}.$$

L'échelle de relation de la suite auxiliaire est [3, — 1], et la condition de possibilité est $y_{1000} \equiv 0$ (mod 3001). Si on substitue à [3, — 1], la récurrence [1, 1], la condition devient $y_{2000} \equiv 0$, et elle est satisfaite, car on trouve déjà $y_{25} \equiv 0$.

L'une des racines cherchées se présente ensuite sous la forme

$$x \equiv \frac{y_{18}}{y_{16}} \equiv \frac{2584}{987} \equiv 2207 .$$

Si n était de la forme $3^{\lambda}(3\mu \pm 1)$, et, par suite, l de la forme $3^{\lambda+1}m + 1$, les racines de la proposée ne pourraient plus s'exprimer en fonction de la récurrence auxiliaire ; mais on pourrait encore tirer avantage de la réduction à la forme monôme. En effet les racines $3^{\lambda+1}$ ièmes de l'unité existent ici, et en désignant par α l'une d'entre elles, différente de l'unité, on conclut de $A^n \equiv 1$ l'identité $A^{3\mu\pm1} \equiv \alpha^3$ et, par conséquent, pour une des valeurs de y

$$y \equiv \alpha A^{-\mu} \qquad \text{ou} \qquad y \equiv \alpha^{-1} A^{\mu} ,$$

selon le cas.

Troisième cas. — Le module l est de la forme $3m + 1$, 3Δ en est non-résidu quadratique, et $\left(\frac{3\Delta}{l}\right) = -1$; a et b sont des imaginaires de Galois de la forme $r \pm s\sqrt{N}$; A est une imaginaire de la même forme. Nous avons démontré que dans la récurrence auxiliaire $[a + b, -ab]$, le terme y_{3m+2} est divisible par l ; ainsi on a

$$A^{3m+2} \equiv 1 \qquad \text{ou} \qquad \left(\frac{a}{b}\right)^{3m+3} \equiv \frac{a}{b} .$$

Une valeur de y est donc $y \equiv \left(\frac{a}{b}\right)^{m+1}$; elle donne pour x la solution réelle

$$x \equiv ab\,\frac{y_m}{y_{m+1}} \equiv \frac{y_{2m+2}}{y_{2m+1}} ,$$

qu'on vérifiera facilement sur les formules de triplication (6) et (7).

Quant aux autres racines, elles sont nécessairement imaginaires. En effet dans le cas présent les racines cubiques de l'unité sont réelles ; si donc x_0, x_1, x_2 l'étaient, la résolvante aurait deux solutions réelles a et b, ainsi que le démontre l'égalité (12).

Prenons, comme exemple, la congruence

$$x^3 + 3x - 1 \equiv 0 \pmod{67}.$$

La condition $\left(\frac{3\Delta}{l}\right) = -1$ est satisfaite ; la récurrence auxiliaire est [1, 1]. On a donc, pour unique racine

$$x \equiv -\frac{y_{22}}{y_{23}} \equiv 40 \pmod{67}.$$

Quatrième cas. -- Le module l est de la forme $3m - 1$, 3Δ est non-résidu quadratique, ou $\left(\frac{3\Delta}{l}\right) = -1$; a et b sont ici encore des imaginaires congruentielles. Comme les racines cubiques de l'unité font partie du domaine $\sqrt{N}$, il est clair que y, et par suite x, a dans ce domaine trois racines ou aucune.

Si x admet trois valeurs, une est réelle, puisque l'existence d'une racine imaginaire entraîne celle de sa conjuguée ; je dis que les deux autres racines seront aussi réelles. Car si x_0 désigne la racine réelle et x_1, x_2 deux racines conjuguées, et que α et α^2 soient de même les racines conjuguées de $\alpha^3 \equiv 1$, les quantités

$$x_0 + \alpha x_1 + \alpha^2 x_2 \qquad \text{et} \qquad x_0 + \alpha x_2 + \alpha^2 x_1$$

seraient réelles, ainsi que a et b, en vertu de (12), ce qui contredit l'hypothèse $\left(\frac{3\Delta}{l}\right) = -1$.

La condition nécessaire et suffisante pour l'existence de ces racines est donc que A soit résidu cubique (mod l) ou que $A^{\frac{l^2-1}{3}} \equiv 1$. Cette condition s'écrit encore $A^{3m^2-2m} \equiv 1$ ou $A^m \equiv A^{-3m^2+3m}$. Mais la récurrence auxiliaire donne $y_{3m} \equiv 0$, ou $A^{3m} \equiv 1$; donc enfin la condition de possibilité prend la forme simple $A^m \equiv 1$, soit $y_m \equiv 0 \pmod{l}$.

Une fois reconnue la possibilité de la solution, on procédera pour trouver les racines comme il a été expliqué à l'occasion du deuxième cas. Ainsi, si le nombre m, ou plus généralement, si l'indice auquel appartient A (mod l) est

de la forme $3\mu \pm 1$, on aura, pour l'une des valeurs de x

$$x \equiv \frac{y_{\mu+1}}{y_\mu}, \qquad \text{ou} \qquad x \equiv ab\,\frac{y_{\mu-1}}{y_\mu} \equiv \frac{y_{2\mu}}{y_{2\mu-1}}.$$

Toutes ces propriétés peuvent être facilement contrôlées au moyen des formules de triplication (6) et (7) et des théorèmes de divisibilité énoncés §§ 3.

Soit, comme exemple, à résoudre la congruence

$$x^3 + 3x - 1 \equiv 0. \pmod{47}$$

La récurrence auxiliaire est toujours [1, 1], et son discriminant 5 est non-résidu de 47. De plus $y_{16} = 987 = 21 \times 47$. La congruence proposée a donc trois racines ; l'une d'elles sera

$$x \equiv \frac{y_6}{y_5} \equiv \frac{8}{5} \equiv 11 ;$$

les autres sont 41 et 42.

C. Cailler (Genève).

SUR LE 5me LIVRE DE GÉOMÉTRIE

Première partie.

1. — L'article intitulé « Parallélisme et translation rectiligne », publié dans le numéro du 15 septembre 1907 de la Revue *L'Enseignement mathématique* (pp. 367-381), impose de nouvelles définitions pour le parallélisme de droites et de plans et par suite un nouveau procédé de démonstration des propriétés qui les concernent. Nous nous bornerons à énoncer simplement les propositions dont la démonstration est devenue classique et surtout celles qui sont relatives à la perpendicularité d'une droite et d'un plan.

On est convenu d'appeler *surface plane* ou *plan* une sur-