

## 23.

# Considérations générales sur les racines des nombres premiers.

(Par Mr. *Oltamare*, prof. des math. supér. à l'acad. des sciences de Genève.)

## I.

## §. 1.

Soit  $\mu$  un nombre premier quelconque, et  $x$  un nombre compris dans la suite naturelle des nombres plus petits que  $\mu$ . Élevons  $x$  successivement à toutes les puissances  $0, 1, 2, 3, \dots n, \dots (\mu-2), (\mu-1), \mu, \mu+1, \dots \mu+n-1, \dots$  nous pouvons, en représentant par  $r_{(n)}$  le reste de  $x^n$  divisé par  $\mu$ , et en nous rappelant que par le théorème de *Fermat* nous avons

$$x^{\mu-1} \equiv 1 \pmod{\mu},$$

former les deux suites infinies

$$(1.) \quad x^0, x^1, x^2, x^3, \dots x^n, \dots x^{\mu-2}, x^{\mu-1}, x^\mu, x^{\mu+1}, \dots x^{\mu+n-1}, \dots,$$

$$(2.) \quad 1, r_{(1)}, r_{(2)}, r_{(3)}, \dots r_{(n)}, \dots r_{(\mu-2)}, 1, r_{(1)}, r_{(2)}, \dots r_{(n)}, \dots$$

En examinant la suites des restes (2.), on voit que cette suite est *périodique*, qu'après un nombre  $\mu-1$  de restes on doit nécessairement retrouver l'unité, et qu'ensuite cette période de  $\mu-1$  termes se répète indéfiniment. Si tous les nombres de la période

$$(3.) \quad 1, r_{(1)}, r_{(2)}, r_{(3)}, \dots r_{(n)}, r_{(\mu-2)}$$

sont différents entr'eux, comme ils sont en nombre  $\mu-1$  et tous plus petits que  $\mu$ , ils doivent nécessairement représenter tous les nombres naturels depuis 1 à  $\mu-1$ .

Tout nombre  $x$  qui jouit de la propriété, qu'élevé à toutes les puissances  $0, 1, 2, \dots (\mu-2)$ , il donne toujours des restes différents lorsqu'on divise ces puissances par  $\mu$ , est désigné sous le nom de *racine du premier ordre ou primitive* de  $\mu$ .

Si tous les termes de la période (3.) ne sont pas différents entr'eux, il est manifeste qu'en formant la suite de ces restes, le premier reste qu'on trouvera égal à un reste déjà obtenu, devra nécessairement être l'unité; et

comme d'ailleurs le reste qui répond à la puissance  $\mu - 1$  est l'unité, il faut que la période (3.) se trouve partagée en de nouvelles périodes dont le nombre des termes de chaque période est un sous-multiple de  $\mu - 1$ ; de sorte que si l'on représente par  $m$  le nombre des périodes qui entrent dans la période (3.), et par  $n$  le nombre des termes de chacune de ces nouvelles périodes, on aura

$$mn = \mu - 1.$$

Cela posé, nous appellerons *racine du  $m^{\text{ième}}$  ordre* ou *d'un indice  $m$* , tout nombre  $x$  qui jouit de la propriété que, si on l'élève à toutes les puissances  $0, 1, 2, 3, \dots, \mu - 2$ , la suite des restes qu'on obtient en divisant ces puissances par  $\mu$ , forme  $m$  périodes semblables de  $\frac{\mu-1}{m}$  termes chacune.

## §. 2.

Considérons les deux suites (1. et 2.), et supposons que  $x$  soit une racine de l'ordre  $m$ , la série (2.) se composera de  $m$  périodes semblables, de  $\frac{\mu-1}{m}$  termes chacune.

Prenons un nombre quelconque  $\gamma$  compris dans une de ces périodes, et proposons-nous de déterminer l'indice qui répond à ce nombre. Soit, pour fixer les idées,  $\gamma = r_{(p)}$  le nombre que nous avons choisi, nous pourrions former les deux suites

$$\begin{array}{ccccccc} \gamma^0, & \gamma^1, & \gamma^2, & \gamma^3, & \dots, \\ 1, & r_{(p)}, & r_{(2p)}, & r_{(3p)}, & \dots \end{array}$$

Cela posé, on reconnaît aisément, d'après la manière dont se forment les restes successifs des puissances de  $\gamma$ :

1° Que si  $p$  est un diviseur de  $\frac{\mu-1}{m}$ , on arrivera au reste 1 après un nombre de termes égal à  $\frac{\mu-1}{mp}$ , puisque  $r_{\left(\frac{\mu-1}{m}\right)} = 1$ , et par suite que  $\gamma$  sera une racine de l'ordre  $mp$ ;

2° Que si  $q$  est le plus grand commun diviseur entre  $\frac{\mu-1}{m}$  et  $p$ , on arrivera au reste 1 après un nombre de termes égal à  $\frac{\mu-1}{mq}$ , et par suite que  $\gamma$  sera une racine dont le nombre des termes de la période sera  $\frac{\mu-1}{qm}$ , c'est-à-dire de l'ordre  $mq$ ;

3° Que si  $p$  est premier avec  $\frac{\mu-1}{m}$ , on n'arrivera au reste 1 qu'après un nombre de termes égal à  $\frac{\mu-1}{m}$ , et par suite que  $\gamma$  sera une racine dont le nombre des termes de la période sera  $\frac{\mu-1}{m}$ , c'est-à-dire de l'ordre  $m$ .

On peut conclure de là :

**Théorème I.** *Si la suite (2.) est formée au moyen d'une racine primitive  $x$  et qu'on écrive les deux suites*

$$0, 1, 2, 3, \dots p, \dots (\mu-2),$$

$$1, r_{(1)}, r_{(2)}, r_{(3)}, \dots r_{(p)}, \dots r_{(\mu-2)},$$

*$r_{(p)}$  sera une racine du nombre premier  $\mu$  d'un ordre indiqué par le plus grand commun diviseur entre  $p$  et  $\mu-1$ .*

On peut déduire de ce théorème, en admettant que tout nombre premier a une racine primitive, les conséquences suivantes :

1° Qu'un nombre premier a autant de racines de l'ordre  $m$  et plus petites que  $\mu$ , qu'il y a de nombres entiers premiers et inférieurs à  $\frac{\mu-1}{m}$  ;

2° Que si l'on connoissoit une racine primitive d'un nombre premier, on les connoitrait toutes, en élevant cette racine à toutes les puissances qui sont des nombres premiers avec  $\mu-1$  et en divisant ces puissances par  $\mu$  ;

3° Que tout nombre premier aura des racines des ordres marqués par les facteurs de  $\mu-1$ , et seulement des racines de ces ordres là ;

4° Que toute puissance  $m$  d'une racine de l'ordre  $p$  est une racine de l'ordre  $mp$ , si le nombre  $\mu$  est de la forme  $mpk+1$ , ou une racine de l'ordre donné par le plus grand commun diviseur entre  $\mu-1$  et  $mp$ , si le nombre premier est d'une autre forme.

### §. 3.

**Théorème II.** *Si  $\mu$  est un nombre premier absolu, et a une racine de ce nombre de l'ordre  $n$ , la congruence*

$$x \equiv \sqrt[n]{a} \pmod{\mu}$$

1° *Admettra une solution, et rien qu'une, si les deux nombres  $\mu-1$  et  $m$  sont premiers entr'eux ; et cette solution sera une racine de l'ordre  $n$  également.*

2° *Elle n'admettra aucune solution si les deux nombres  $\mu-1$  et  $m$  ont un plus grand commun diviseur qui n'entre pas dans  $n$  ;*

3° *Elle admettra autant de solutions que le plus grand commun diviseur entre  $\mu-1$  et  $m$  contient d'unités, si ce plus grand commun diviseur divise aussi exactement  $n$  ; de plus ces différentes solutions seront des racines de  $\mu$ , soit de l'ordre  $n$ , soit d'un ordre sous-multiple de  $n$ .*

Cette proposition très connue, n'est que l'énoncé de la réciproque de la 4<sup>ième</sup> conséquence du paragraphe précédent.

Si nous considérons l'expression

$$x \equiv \sqrt[m]{1} \pmod{\mu},$$

dont les  $m$  valeurs sont données par

$$R_k \equiv \cos \frac{2k\omega}{m} + \sqrt{-1} \sin \frac{2k\omega}{m} \pmod{\mu},$$

lorsqu'on fait dans cette formule  $k$  successivement égal à  $0, 1, 2 \dots (m-1)$ , il résultera du théorème précédent, en remarquant que 1 est évidemment de l'ordre  $\mu-1$ :

1° Que  $R_k$  sera irrationnelle pour toutes les valeurs de  $k$  différentes de 0, si  $m$  et  $\mu-1$  sont premiers entr'eux;

2° Que  $R_k$  sera rationnelle pour un nombre de valeurs de  $k$  égal au nombre qui exprime le plus grand commun diviseur entre  $\mu-1$  et  $m$ , et irrationnelle pour les autres.

#### §. 4.

Si nous supposons  $m=3$ , les différentes valeurs de  $R$  seront:

$$R \equiv 1 \pmod{\mu},$$

$$R' \equiv -\frac{1}{2} + \frac{1}{2}\sqrt{-3} \pmod{\mu},$$

$$R'' \equiv -\frac{1}{2} - \frac{1}{2}\sqrt{-3} \pmod{\mu}.$$

Par conséquent, si  $\mu=6n+1$ ,  $\mu-1$  et  $m$  seront premiers entr'eux, et les valeurs de  $R'$  et  $R''$  devront être irrationnelles.

On peut en conclure que:  $\sqrt{-3}$  est rationnelle pour tout nombre premier  $\mu$  de la forme  $6n+1$ , et irrationnelle pour tout nombre premier  $\mu$  de la forme  $6n-1$ .

En supposant  $m=3^{p-1}$ , on démontrera de même que:

*L'expression  $\sqrt[p]{-\frac{1}{2} \pm \frac{1}{2}\sqrt{-3}}$  est rationnelle pour toute valeur d'un nombre premier  $\mu$  de la forme  $2 \cdot 3^p n + 1$ , et irrationnelle pour tout nombre premier d'une autre forme.*

#### §. 5.

Si nous supposons  $m=5$ , les différentes valeurs de  $R$  seront

$$R \equiv 1 \pmod{\mu},$$

$$R' \equiv -\frac{1}{4} + \frac{1}{4}\sqrt{5} + \frac{1}{4}\sqrt{(-10-2\sqrt{5})} \pmod{\mu},$$

$$R'' \equiv -\frac{1}{4} + \frac{1}{4}\sqrt{5} - \frac{1}{4}\sqrt{(-10-2\sqrt{5})} \pmod{\mu},$$

$$R''' \equiv -\frac{1}{4} - \frac{1}{4}\sqrt{5} + \frac{1}{4}\sqrt{(-10+2\sqrt{5})} \pmod{\mu},$$

$$R^{IV} \equiv -\frac{1}{4} - \frac{1}{4}\sqrt{5} - \frac{1}{4}\sqrt{(-10+2\sqrt{5})} \pmod{\mu}.$$

Si  $\mu = 10n + 1$ , le plus grand commun diviseur entre  $\mu - 1$  et  $m$ , sera 5, et toutes les valeurs de  $R$  seront rationnelles. Or, puisque (comme nous le reconnaitrons plus loin §. 13.),  $\sqrt[5]{5}$  est rationnelle pour toute valeur de  $\mu$  de la forme  $10n + 1$ , l'expression  $\sqrt[5]{(-10 \pm 2\sqrt{5})}$  doit l'être pour toute valeur de  $\mu$  de la forme  $10n + 1$ .

Si  $\mu = 10n - 1$ ,  $\mu - 1$  et  $m$  sont deux nombres premiers entr'eux. Comme d'ailleurs  $\sqrt[5]{5}$  est rationnelle, l'expression  $\sqrt[5]{(-10 \pm 2\sqrt{5})}$  doit être irrationnelle.

Si  $\mu = 10n \pm 3$ , il est aisé de voir que  $\sqrt[5]{5}$  et  $\sqrt[5]{(-10 \pm 2\sqrt{5})}$  sont irrationnelles.

On peut conclure de là que :

*L'expression  $\sqrt[5]{(-10 \pm 2\sqrt{5})}$  est rationnelle pour toute valeur de  $\mu$  de la forme  $10n + 1$ , et irrationnelle pour tout nombre premier d'une autre forme.*

En supposant  $m = 5^{p-1}$ , on démontrera de même que :

*L'expression  $\sqrt[5^{p-1}]{[-\frac{1}{4} \pm \frac{1}{4}\sqrt{5} \pm \sqrt[5]{(-10 \mp 2\sqrt{5})}]}$  est rationnelle pour toute valeur d'un nombre premier  $\mu$  de la forme  $2 \cdot 5^p n + 1$ , et irrationnelle pour tout nombre premier d'une autre forme.*

#### §. 6.

Enfin, généralement, on peut dire que :

*En représentant par  $\alpha$  un nombre premier, et par  $R_k$  la valeur de l'expression  $\cos \frac{2k\omega}{\alpha} + \sin \frac{2k\omega}{\alpha} \sqrt{-1}$ , dans laquelle  $k$  peut prendre toutes les valeurs 1, 2, 3, ...  $\alpha - 1$ , on verra que l'expression*

$$\sqrt[\alpha^{p-1}]{R_k}$$

*sera rationnelle pour tout nombre premier de la forme  $2\alpha^p n + 1$ , et irrationnelle pour tout nombre premier d'une autre forme.*

#### §. 7.

On déduit aisément du théorème II. et de la 4<sup>ème</sup> conséquence du (§. 2.) le théorème suivant.

**Théorème III.** *Si l'on admet que toutes les racines de l'ordre  $m$  d'un nombre premier  $\mu$ , soient données par l'ensemble des solutions d'une congruence*

$$X_{(m)} = \varphi(x) \equiv 0 \pmod{\mu},$$

*la congruence, propre à donner les racines de l'ordre  $mn$ , et rien*

que les racines de cet ordre, s'obtiendra en changeant dans cette congruence  $x$  en  $\sqrt[n]{x}$ .

Réciproquement, si l'on connaît la congruence qui donne les racines de l'ordre  $mn$ , et que nous en voulions déduire celle qui donne les racines de l'ordre  $m$ , il faudra remplacer  $x$  par  $x^n$ . Mais ici on devra remarquer que la nouvelle congruence contiendra non-seulement les racines de l'ordre  $mn$ , mais aussi les racines de tous les ordres qu'on obtient en multipliant  $m$  par tous les diviseurs de  $n$ . Nous pourrions donc énoncer le théorème suivant.

### §. 8.

**Théorème IV.** *Si la congruence*

$$X_{(mn)} = \varphi(x) \equiv 0 \pmod{\mu}$$

*donne pour solutions toutes les racines de l'ordre  $mn$ , et si l'on désigne par*

$$n_1, n_2, n_3, \dots, n$$

*tous les diviseurs de  $n$ , différents de l'unité, et par*

$$X_{(mn_1)} \equiv 0 \pmod{\mu}, \quad X_{(mn_2)} \equiv 0 \pmod{\mu}, \quad \dots \quad X_{(mn)} \equiv 0 \pmod{\mu}$$

*les congruences propres à donner les racines des différents ordres  $mn_1, mn_2, \dots, m$ : la congruence qui donnera les racines de l'ordre  $m$ , et rien que les racines de cet ordre, sera*

$$X_{(m)} = \frac{\varphi(x^n)}{X_{(mn_1)} \cdot X_{(mn_2)} \cdot \dots \cdot X_{(mn)}} \equiv 0 \pmod{\mu}.$$

La détermination des congruences, propres à donner les racines d'un nombre premier  $\mu$  de tel ordre qu'on voudra, ne saurait actuellement présenter de difficultés.

### §. 9.

Si nous considérons le nombre 1, il est évident qu'en l'élevant successivement aux différentes puissances 1, 2, 3,  $\dots$ ,  $\mu - 2$ , il donnera naissance à une période d'un seul terme, et par suite ce nombre est une racine de l'ordre  $\mu - 1$ . Il est d'ailleurs aisé de reconnaître que ce nombre est la seule racine de cet ordre, de sorte que la congruence

$$X_{(\mu-1)} = x - 1 \equiv 0 \pmod{\mu}$$

est la congruence propre à donner toutes les racines, et rien que les racines de l'ordre  $\mu - 1$ .

Si actuellement nous représentons par  $2^m \alpha^s h + 1$  le nombre premier  $\mu$ ;  $m$  et  $s$  étant des nombres entiers,  $\alpha$  un nombre premier, et  $h$  un nombre impair quelconque, nous aurons en vertu du théorème précédent:

$$X_{\left(\frac{\mu-1}{2}\right)} = \frac{x^2-1}{X_{(\mu-1)}} = \frac{x^2-1}{x-1} = x+1 \equiv 0 \pmod{\mu},$$

$$X_{\left(\frac{\mu-1}{2^2}\right)} = \frac{x^2-1}{X_{\left(\frac{\mu-1}{2}\right)} X_{(\mu-1)}} = \frac{x^2-1}{(x+1)(x-1)} = x^2+1 \equiv 0 \pmod{\mu},$$

$$X_{\left(\frac{\mu-1}{2^3}\right)} = \frac{x^2-1}{X_{\left(\frac{\mu-1}{2}\right)} X_{\left(\frac{\mu-1}{2^2}\right)} X_{(\mu-1)}} = \frac{x^2-1}{(x^2+1)(x+1)(x-1)} = x^2+1 \equiv 0 \pmod{\mu},$$

$$\begin{aligned} X_{\left(\frac{\mu-1}{2^m}\right)} &= \frac{x^{2^m}-1}{X_{\left(\frac{\mu-1}{2^{m-1}}\right)} X_{\left(\frac{\mu-1}{2^{m-2}}\right)} \dots X_{(\mu-1)}} = \frac{x^{2^m}-1}{(x^{2^{m-1}}+1)(x^{2^{m-2}}+1) \dots (x-1)} \\ &= x^{2^{m-1}}+1 \equiv 0 \pmod{\mu}. \end{aligned}$$

Remarquons que la valeur de  $X_{\left(\frac{\mu-1}{2^2}\right)}$  pourrait être déduite de la valeur de

$$X_{\left(\frac{\mu-1}{2}\right)} = x+1 \equiv 0 \pmod{\mu},$$

en mettant simplement  $x^2$  à la place de  $x$ . Il en est de même des valeurs de

$$X_{\left(\frac{\mu-1}{2^3}\right)}, \quad X_{\left(\frac{\mu-1}{2^4}\right)}, \quad \dots \quad X_{\left(\frac{\mu-1}{2^m}\right)}.$$

En faisant usage de cette remarque, nous trouverons, en continuant l'application de notre théorème, la suite des congruences

$$X_{\left(\frac{\mu-1}{2^m \alpha}\right)} = \frac{x^{2^{m-1} \alpha} + 1}{X_{\left(\frac{\mu-1}{2^m}\right)}} \equiv 0 \pmod{\mu},$$

$$X_{\left(\frac{\mu-1}{2^m \alpha^2}\right)} = \frac{x^{2^{m-1} \alpha^2} + 1}{X_{\left(\frac{\mu-1}{2^m \alpha}\right)} X_{\left(\frac{\mu-1}{2^m}\right)}} \equiv 0 \pmod{\mu},$$

$$X_{\left(\frac{\mu-1}{2^m \alpha^3}\right)} = \frac{x^{2^{m-1} \alpha^3} + 1}{X_{\left(\frac{\mu-1}{2^m \alpha^2}\right)} X_{\left(\frac{\mu-1}{2^m \alpha}\right)} X_{\left(\frac{\mu-1}{2^m}\right)}} \equiv 0 \pmod{\mu},$$

$$X_{\left(\frac{\mu-1}{2^m \alpha^s}\right)} = \frac{x^{2^{m-1} \alpha^s} + 1}{X_{\left(\frac{\mu-1}{2^m \alpha^{s-1}}\right)} X_{\left(\frac{\mu-1}{2^m \alpha^{s-2}}\right)} \dots X_{\left(\frac{\mu-1}{2^m}\right)}} \equiv 0 \pmod{\mu}.$$

Et en continuant ainsi pour tous les facteurs de  $h$ , on arrivera à déterminer toutes les congruences qui donnent les racines de tel ordre qu'on voudra.

### §. 10.

Si nous appelons *racines impaires*, les racines d'un nombre premier  $\mu$  dont l'ordre est un nombre impair, et *racines paires* celles dont l'ordre est un nombre pair, nous pourrions dire :

**Théorème V.** *Les racines impaires d'un nombre premier  $\mu$  sont les racines de la congruence*

$$x^{\frac{\mu-1}{2}} + 1 \equiv 0 \pmod{\mu},$$

*et les racines paires celles de la congruence*

$$x^{\frac{\mu-1}{2}} - 1 \equiv 0 \pmod{\mu}.$$

En supposant en effet  $\mu = 2^m h$  ( $h$  étant un nombre impair), nous aurons en vertu du paragraphe précédent que les racines de l'ordre  $h$  seront les solutions de la congruence

$$x^{2^{m-1}} + 1 \equiv 0 \pmod{\mu}.$$

Si, dans cette congruence, à la place de  $x$ , nous mettons  $x^h$ , nous aurons en vertu du théorème IV, une congruence qui contiendra les racines de tous les ordres qu'on obtient en multipliant 1 par tous les diviseurs de  $h$ ; ou en d'autres termes, toutes les racines impaires. Cette nouvelle congruence est

$$x^{2^{m-1}h} + 1 = x^{\frac{\mu-1}{2}} + 1 \equiv 0 \pmod{\mu}.$$

Comme en vertu du Théorème de *Fermat* on sait que la congruence

$$x^{\mu-1} - 1 = (x^{\frac{\mu-1}{2}} + 1)(x^{\frac{\mu-1}{2}} - 1) \equiv 0 \pmod{\mu}$$

contient les racines des différents ordres de  $\mu$ , il faut que la congruence

$$x^{\frac{\mu-1}{2}} - 1 \equiv 0 \pmod{\mu}$$

contienne toutes les racines d'un ordre pair.

On reconnaîtra semblablement que toutes les racines d'un ordre  $2^q h$  ( $h$  étant un nombre impair) sont données par la congruence

$$x^{\frac{\mu-1}{2^q}} + 1 \equiv 0 \pmod{\mu}.$$

## §. 11.

Si l'on examine avec soin de quelle manière en vertu du théorème (IV.) on peut déduire de la congruence

$$x_{(2m)} \equiv 0 \pmod{\mu}$$

celle-ci :

$$x_{(m)} \equiv 0 \pmod{\mu},$$

on en conclura sur les racines paires et impaires le théorème suivant.

**Théorème VI.**  *$\mu$  étant un nombre premier de la forme  $2^m k + 1$ , et  $x$  et  $z$  deux nombres entiers qui satisfont à la congruence*

$$xz + 1 \equiv 0 \pmod{\mu}:$$

1° *Si l'un des deux nombres  $x$  ou  $z$  est une racine de  $\mu$  d'un ordre marqué par  $2^m k$ , l'autre sera une racine paire ou impaire, mais seulement d'un ordre marqué par  $2^{m-1} k$ ;*

2° *Si l'un des deux nombres  $x$  ou  $z$  est une racine de  $\mu$  d'un ordre pair ou impair marqué par  $2^{m-h'} k$  ( $h' > 1$ ), l'autre sera également une racine paire ou impaire du même ordre.*

Faisons remarquer que si  $\mu$  est de la forme  $4n + 3$ , auquel cas  $m = 1$ , en résolvant la congruence

$$xz + 1 \equiv 0 \pmod{\mu},$$

on obtient pour la valeur de l'un des deux nombres une racine impaire, et pour l'autre une racine paire d'un ordre double.

## §. 12.

Si nous appelons *racines conjuguées* deux racines dont le produit est congru à l'unité, et si nous désignons sous le nom de *racines complémentaires*, deux racines dont la somme est congrue à zéro, nous pourrions établir les théorèmes suivants.

**Théorème VII.** *Les racines conjuguées sont toujours du même ordre, quel que soit le nombre premier  $\mu$  auquel elles appartiennent.*

En effet, en posant

$$xy - 1 \equiv 0 \pmod{\mu},$$

et en désignant par  $a$  une racine primitive de  $\mu$ , les valeurs  $x \equiv a^n$ ,  $y \equiv a^{\mu-n-1}$  seront des solutions de cette congruence. Or les ordres des racines  $x$  et  $y$  seront égaux aux plus grands communs diviseurs entre  $\mu - 1$  et  $n$ ,  $\mu - 1$  et  $\mu - n - 1$ , et comme il est évident que ces plus grands communs diviseurs sont égaux, ces racines sont du même ordre.

**Théorème VIII.** *Si  $\mu$  est un nombre premier de la forme  $4m+1$ , les racines complémentaires seront toutes deux impaires ou toutes deux paires. Si elles sont impaires, elles sont du même ordre; si elles sont paires, elles peuvent être, soit du même ordre, soit d'un ordre différent d'un multiple  $2^p$ .*

*Si  $\mu$  est un nombre premier de la forme  $4m+3$ , les racines complémentaires seront, l'une d'un ordre impair, l'autre d'un ordre pair, d'un degré double de celui de la première.*

La démonstration de ce Théorème est trop simple pour qu'il soit nécessaire de nous y arrêter; il est une conséquence des théorèmes (VI. et VII.).

**Théorème IX.** *Le nombre 2 est racine impaire de tout nombre premier  $\mu$  de la forme  $8n+3$ , et racine paire de tout nombre premier  $\mu$  de la forme  $8n+1$ .*

Ce théorème est le même que celui qu'à démontré *Legendre* dans sa théorie des nombres (parag. 148).

### §. 13.

**Problème.** *Déterminer si le nombre premier  $\alpha$  est une racine paire, ou une racine impaire du nombre premier  $\mu$ .*

Si l'on connaissait les racines paires et impaires d'un nombre premier  $\alpha$ , on pourrait aisément déterminer, si  $\alpha$  est racine paire ou impaire d'un autre nombre premier  $\mu$ ; car en divisant  $\mu$  par  $\alpha$ , et en désignant par  $r$  le reste de la division, on aura par la loi de réciprocity de *Legendre* que:

*Si  $\mu$  et  $\alpha$  ne sont pas tous les deux de la forme  $4n+3$ : si  $r$  est racine paire ou impaire de  $\alpha$ ,  $\alpha$  lui-même sera une racine paire ou impaire de  $\mu$ .*

*Si  $\mu$  et  $\alpha$  sont tous deux de la forme  $4n+3$ : si  $r$  est racine paire ou impaire de  $\alpha$ ,  $\alpha$  lui-même sera, au contraire, racine impaire ou paire de  $\mu$ .*

Si nous supposons  $\alpha = 3 : 1$  sera racine paire, et 2 racine impaire; par conséquent, si  $\mu$  est des deux formes

$3n+1$	et	$4n+1$ ,	3 est racine paire,
$3n+2$	et	$4n+1$ ,	3 est racine impaire,
$3n+1$	et	$4n+3$ ,	3 est racine impaire,
$3n+2$	et	$4n+3$ ,	3 est racine paire.

Il résulte de là que:

**Théorème X. a)** *Le nombre 3 sera racine paire de tout nombre premier  $\mu$  de la forme  $12n \pm 1$ , et racine impaire de tout nombre premier de la forme  $12n \pm 5$ .*

Si nous faisons  $\alpha = 5$  : 1 et 4 seront racines paires, et 2 et 3 racines impaires. Le même raisonnement nous conduira à admettre que

**b)** *Le nombre 5 sera racine paire de tout nombre premier  $\mu$  de la forme  $10n \pm 1$ , et racine impaire de tout nombre premier de la forme  $10n \pm 3$ .*

Si nous faisons successivement  $\alpha = 7$ ,  $\alpha = 11$ ,  $\alpha = 13$ , etc., nous trouverons, en suivant la même marche que

**c)** *Le nombre 7 sera racine paire de tout nombre premier de la forme  $28n \pm 1$ , ou  $28n \pm 3$ , ou  $28n \pm 9$ ; et racine impaire de tout nombre premier de la forme  $28n \pm 5$ , ou  $28n \pm 11$ , ou  $28n \pm 13$ .*

**d)** *Le nombre 11 sera racine paire de tout nombre premier de la forme  $44n \pm 1$ , ou  $44n \pm 5$ , ou  $44n \pm 7$ , ou  $44n \pm 9$ ; ou  $44n \pm 19$ , et racine impaire de tout nombre premier de la forme  $44n \pm 3$ , ou  $44n \pm 13$ , ou  $44n \pm 15$ , ou  $44n \pm 17$ , ou  $44n \pm 21$ .*

Et généralement: *Le nombre premier  $\mu$  est racine paire de tout nombre premier  $\mu$  dont les formes sont données par une certaine suite  $4\alpha n \pm a$ , ou  $4\alpha n \pm b$ , ou etc., et racine impaire de tout nombre premier  $\mu$  dont les formes sont données par une suite  $4\alpha n \pm a'$ , ou  $4\alpha n \pm b'$ , ou etc.*

Parmi les formes de  $\mu$  qui donnent  $\alpha$  pour racine paire, on trouvera constamment la forme  $2\alpha n \pm k^2$ , et il est facile de faire voir que cela arrivera constamment. Si, en effet, on suppose  $\mu = 4\alpha n + k^2$ , et qu'on applique la loi de réciprocité, on trouve que  $\alpha$  est racine paire ou impaire de  $\mu$ , selon que  $k^2$  est racine paire ou impaire de  $\alpha$ : par suite  $\alpha$  est racine paire de  $\mu$ , car  $\mu$  est de la forme  $4n + 1$ .

Si de plus on remarque que les nombres premiers qui répondent aux deux formes  $4\alpha n \pm k^2$ , ont à la fois  $\alpha$  pour racine paire ou impaire, on pourra énoncer le théorème suivant.

**Théorème XI.** *Si  $\mu$  est un nombre premier, tel qu'en y ajoutant ou retranchant  $k^2$ , le résultat est divisible par 4: tout nombre premier différent de 2, qui divise l'expression  $\mu \pm k^2$ , est une racine paire du nombre premier  $\mu$ .*

## §. 14.

Nous pouvons, comme conséquence des théorèmes prouvés dans le paragraphe précédent, établir le théorème suivant.

**Théorème XII.**  $\mu$  et  $\alpha$  étant deux nombres premiers, et qu'en divisant  $\mu$  par  $4\alpha$ , on obtient un reste  $r$  positif ou négatif, tel que  $2\alpha - r$  soit également un nombre premier  $\nu$ :

1° Si  $\alpha$  est de la forme  $4n+1$ ,  $\alpha$  sera une racine paire ou impaire de  $\mu$ , selon qu'il sera lui-même une racine paire ou impaire de  $\nu$ .

2° Si  $\alpha$  est de la forme  $4n+3$ ,  $\alpha$  sera une racine paire ou impaire de  $\mu$ , selon qu'il sera lui-même une racine impaire ou paire de  $\nu$ .

## III.

## §. 1.

Soit  $\mu$  un nombre premier quelconque, et proposons-nous de résoudre la congruence

$$y^3 + Py^2 + Qy + R \equiv 0 \pmod{\mu}.$$

Si l'on fait disparaître le second terme de cette congruence, en posant

$$y \equiv x - \frac{1}{3}P \pmod{\mu},$$

on pourra, en désignant par  $p$  et  $q$  des nombres entiers quelconques, la mettre sous la forme

$$(1.) \quad x^3 + 3px + 2q \equiv 0 \pmod{\mu}.$$

Si l'on pose, pour abréger:

$$A \equiv \sqrt[3]{-q + \sqrt{(q^2 + p^3)}} \pmod{\mu},$$

les valeurs de  $x$  qui satisfont à la congruence (1.), seront données par les expressions analytiques:

$$(2.) \quad x' \equiv A - \frac{p}{A} \pmod{\mu},$$

$$(3.) \quad x'' \equiv -\frac{1}{2}\left(A - \frac{p}{A}\right) - \frac{1}{2}\left(A + \frac{p}{A}\right)\sqrt{-3} \pmod{\mu},$$

$$(4.) \quad x''' \equiv -\frac{1}{2}\left(A - \frac{p}{A}\right) - \frac{1}{2}\left(A + \frac{p}{A}\right)\sqrt{-3} \pmod{\mu}.$$

Cela posé, nous allons examiner quelles sont les congruences pour lesquelles ces expressions ont une valeur rationnelle ou irrationnelle, et rechercher, sous quelles formes il convient de les mettre pour en calculer les valeurs, dans le cas de la première de ces alternatives.

Nous distinguerons ici trois cas; selon que la quantité  $q^2 + p^3$  qui entre dans l'expression de  $A$ , satisfait à l'une ou à l'autre des trois congruences suivantes :

$$\begin{aligned} q^2 + p^3 &\equiv 0 \pmod{\mu}, \\ (q^2 + p^3)^{\frac{1}{2}(\mu-1)} &\equiv 1 \pmod{\mu}, \\ (q^2 + p^3)^{\frac{1}{2}(\mu-1)} &\equiv -1 \pmod{\mu}. \end{aligned}$$

### §. 2.

**Théorème I.** *Si les nombres  $p$  et  $q$  qui entrent dans la congruence proposée*

$$x^3 + 3px + 2q \equiv 0 \pmod{\mu}$$

*sont tels que l'on ait :*

$$(1.) \quad q^2 + p^3 \equiv 0 \pmod{\mu},$$

*la congruence proposée admettra trois racines rationnelles, dont deux seront égales entr'elles.*

Cette proposition est évidente si l'on remarque que l'on a identiquement, en vertu de la congruence (1.):

$$x^3 + 3px + 2q \equiv \left(x + \frac{q}{p}\right)\left(x + \frac{q}{p}\right)\left(x - \frac{2q}{p}\right) \equiv 0 \pmod{\mu},$$

d'où il résulte

$$x' \equiv +2\frac{q}{p} \pmod{\mu},$$

$$x'' \equiv -\frac{q}{p} \pmod{\mu},$$

$$x''' \equiv -\frac{q}{p} \pmod{\mu}.$$

Ces résultats pourraient d'ailleurs se déduire des expressions analytiques (2, 3 et 4.), en tenant compte de la congruence (1.) de ce paragraphe.

### §. 3.

**Théorème II.** *Si  $\mu$  est un nombre premier de la forme  $6n - 1$ , et si  $p$  et  $q$  sont deux nombres tels que l'on ait :*

$$(q^2 + p^3)^{\frac{1}{2}(\mu-1)} \equiv 1 \pmod{\mu},$$

la congruence proposée

$$x^3 + 3px + 2q \equiv 0 \pmod{\mu},$$

n'admettra qu'une seule racine rationnelle, donnée par la formule

$$x \equiv -\frac{2q}{p+2M} \pmod{\mu};$$

$M$  représentant la partie du développement de l'expression

$$[-q + \sqrt[3]{(q^2 + p^3)}]^{2n},$$

qui ne contient pas  $\sqrt[3]{(q^2 + p^3)}$  en facteur, c'est à dire :

$$\frac{1}{2} \{ [-q + \sqrt[3]{(q^2 + p^3)}]^{2n} + [-q - \sqrt[3]{(q^2 + p^3)}]^{2n} \}.$$

Puisqu'on a la congruence

$$(q^2 + p^3)^{\frac{1}{3}(\mu-1)} \equiv 1 \pmod{\mu},$$

on pourra toujours trouver une valeur de  $s$ , telle que

$$s \equiv \sqrt[3]{(q^2 + p^3)} \pmod{\mu},$$

et la valeur de  $x'$  donnée par la congruence (2. §. 1.), sera

$$x' \equiv \sqrt[3]{(s-q)} - \frac{p}{\sqrt[3]{(s-q)}} \pmod{\mu}.$$

Si maintenant on remarque que  $\mu$  est de la forme  $6n-1$ :  $\mu-1$  sera premier avec 3, et en vertu d'un théorème connu, l'expression  $\sqrt[3]{(s-q)}$  sera rationnelle; par suite la valeur de  $x'$  le sera, et la congruence proposée admettra cette valeur comme racine rationnelle.

Quant aux deux autres valeurs  $x''$  et  $x'''$  de  $x$ , il est facile de voir qu'elles sont irrationnelles; car elles se composent d'une première partie  $-\frac{1}{2} \left[ \sqrt[3]{(s-q)} - \frac{p}{\sqrt[3]{(s-q)}} \right]$  qui est rationnelle; plus d'une seconde partie, dont l'un des facteurs  $\sqrt[3]{-3}$  est toujours irrationnel (vu la forme du nombre premier  $\mu$ ) et dont l'autre  $\frac{1}{2} \sqrt[3]{(s-q)} + \frac{p}{\sqrt[3]{(s-q)}}$  est rationnel.

Pour exprimer la valeur de  $x'$  en fonction rationnelle des coefficients de la congruence proposée et du nombre premier  $\mu$ : remarquons qu'en résolvant la congruence (2. §. 1.) par rapport à  $A$ , on obtient:

$$2A \equiv 2\sqrt[3]{[-q + \sqrt[3]{(q^2 + p^3)}]} \equiv x' \pm \sqrt[3]{(x'^2 + 4p)} \pmod{\mu}.$$

Élevant à la puissance  $\mu+1=6n$  les deux membres de cette congruence, en

remarquant que :

$$\begin{aligned} x'^{\mu} &\equiv 1 \pmod{\mu}, \\ (x'^2 + 4p)^{\frac{1}{3}(\mu-1)} &\equiv 1 \pmod{\mu}, \end{aligned}$$

et en réjetant les multiples de  $\mu$ , on trouve :

$$4[-q + \sqrt[3]{(q^2 + p^3)}]^{2n} \equiv [x' \pm \sqrt[3]{(x'^2 + 4p)}]^2 \equiv 2x'^2 + 4p \pm 2x' \sqrt[3]{(x'^2 + 4p)} \pmod{\mu},$$

qu'on peut écrire :

$$x'^2 + 2p \pm x' \sqrt[3]{(x'^2 + 4p)} \equiv 2[-q + \sqrt[3]{(q^2 + p^3)}]^{2n} \pmod{\mu}.$$

Changeant le signe de  $\sqrt[3]{(q^2 + p^3)}$ , ce qui ne change pas la valeur de  $x'$ , on a :

$$x'^2 + 2p \mp x' \sqrt[3]{(x'^2 + 4p)} \equiv 2[-q - \sqrt[3]{(q^2 + p^3)}]^{2n} \pmod{\mu}.$$

Additionnant ces deux congruences, on en tire :

$$x'^2 + 2p \equiv [-q + \sqrt[3]{(q^2 + p^3)}]^{2n} + [-q - \sqrt[3]{(q^2 + p^3)}]^{2n} \pmod{\mu}.$$

En posant, pour abrégé,

$$M \equiv \frac{1}{2} \{ [-q + \sqrt[3]{(q^2 + p^3)}]^{2n} + [-q - \sqrt[3]{(q^2 + p^3)}]^{2n} \} \pmod{\mu},$$

nous aurons

$$x'^2 \equiv 2(M - p) \pmod{\mu},$$

cette valeur de  $x'^2$ , mise dans la congruence proposée, donne

$$x' \equiv -\frac{2q}{p + 2M} \pmod{\mu}.$$

#### §. 4.

**Théorème III.** *Si  $\mu$  est un nombre premier de la forme  $6n + 1$ , et si  $p$  et  $q$  sont deux nombres tels que l'on ait :*

$$(q^2 + p^3)^{\frac{1}{3}(\mu-1)} \equiv 1 \pmod{\mu},$$

*la congruence proposée*

$$x^3 + 3px + 2q \equiv 0 \pmod{\mu}$$

*admettra trois racines rationnelles, ou n'en admettra aucune, selon que la congruence*

$$(1.) \quad [-q + \sqrt[3]{(q^2 + p^3)}]^{2n} \equiv 1 \pmod{\mu}$$

*sera satisfaite, ou ne le sera pas.*

Si la quantité  $-q + \sqrt[3]{(q^2 + p^3)}$  est une racine du nombre premier  $\mu$ , d'un ordre dont l'indice soit multiple de 3, cette valeur satisfera à la congruence (1.); comme le démontre le théorème de *Fermat*, et la valeur,

$$(2.) \quad A \equiv \sqrt[3]{[-q + \sqrt[3]{(q^2 + p^3)}]} \pmod{\mu},$$

sera, en vertu d'un théorème connu, une quantité rationnelle qui admettra trois valeurs. En désignant ces trois valeurs par  $A'$ ,  $A''$  et  $A'''$ , nous aurons, comme racines de la congruence proposée :

$$(3.) \quad \begin{cases} x' \equiv A' - \frac{p}{A'} \pmod{\mu}, \\ x'' \equiv A'' - \frac{p}{A''} \pmod{\mu}, \\ x''' \equiv A''' - \frac{p}{A'''} \pmod{\mu}, \end{cases}$$

ou bien, en désignant par  $A$  une quelconque de ces trois valeurs, les expressions de  $x'$ ,  $x''$ ,  $x'''$ , données dans le (§. 1.); car  $\sqrt{-3}$  est, par la forme du nombre premier  $\mu$ , une quantité rationnelle.

Réciproquement, si  $p$  et  $q$  sont tels que la congruence (1.) soit satisfaite, la congruence proposée admettra trois solutions.

En effet, on déduit des congruences (1. et 2.):

$$A^{\mu-1} \equiv 1 \pmod{\mu}:$$

congruence qui montre que  $A$  est une quantité rationnelle, et par suite que les valeurs de  $x'$ ,  $x''$  et  $x'''$  données (§. 1.) sont rationnelles; car  $\sqrt{-3}$  l'est également.

Si la quantité  $-q + \sqrt[3]{(q^2 + p^3)}$  est une racine du nombre premier  $\mu$ , d'un ordre dont l'indice soit premier avec 3: cette valeur ne satisfera point à la congruence (1.). De plus, les trois racines  $x'$ ,  $x''$  et  $x'''$  seront irrationnelles; comme nous allons le reconnaître. En effet, la quantité  $-q + \sqrt[3]{(q^2 + p^3)}$  étant une racine du nombre premier  $\mu$  dont l'indice est premier avec 3, la valeur de

$$A \equiv \sqrt[3]{[-q + \sqrt[3]{(q^2 + p^3)}]} \pmod{\mu}$$

sera irrationnelle, conformément à un théorème connu; et par suite la valeur

$$x' \equiv A - \frac{p}{A} \pmod{\mu},$$

ne saurait devenir rationnelle que dans le cas où les parties irrationnelles de  $A$  et de  $\frac{p}{A}$  seraient égales entr'elles et où l'on aurait:

$$A \equiv \gamma + \sqrt[3]{z} \pmod{\mu},$$

$$\frac{p}{A} \equiv \gamma' + \sqrt[3]{z} \pmod{\mu};$$

$\gamma$ ,  $\gamma'$  et  $z$  représentant des quantités rationnelles.

Il résulte de ces deux congruences :

$$p - yy' \equiv (y + y')\sqrt[3]{z} + \sqrt[3]{z}^2 \pmod{\mu}.$$

Multipliant cette congruence par  $\sqrt[3]{z}$ , on trouve

$$-z \equiv -(p - yy')\sqrt[3]{z} + (y + y')\sqrt[3]{z}^2 \pmod{\mu}.$$

Éliminant  $\sqrt[3]{z}^2$  entre ces deux dernières congruences, on obtient :

$$(a.) \quad \sqrt[3]{z} \equiv \frac{z + (y + y')(p - yy')}{p - yy'(y + y')^2} \pmod{\mu}.$$

Or cette dernière congruence est absurde, car elle donne pour  $\sqrt[3]{z}$  une valeur rationnelle : la valeur de  $x'$  est donc irrationnelle.

On ne saurait objecter que le numérateur et le dénominateur peuvent être congru à zéro dans la congruence (a.), car alors il en résulterait

$$y + y' \equiv \sqrt[3]{z} \pmod{\mu};$$

ce qu'on ne saurait admettre.

Quant aux deux autres valeurs de  $x$ ,  $x''$  et  $x'''$ , il est facile de démontrer qu'elles sont également irrationnelles.

En effet, en posant pour abrégé  $z \equiv -q + \sqrt[3]{q^2 + p^3}$ , il est facile de voir que l'expression  $A - \frac{p}{A}$  peut se mettre sous la forme  $\sqrt[3]{z} + k\sqrt[3]{z}^2$ ,  $k$  étant un coefficient rationnel, et pour que  $x''$  soit rationnelle, il faut que l'on ait simultanément :

$$(b.) \quad \begin{cases} A - \frac{p}{A} \equiv \sqrt[3]{z} + k\sqrt[3]{z}^2 \pmod{\mu}, \\ \sqrt[3]{-3\left(A + \frac{p}{A}\right)} \equiv y + \sqrt[3]{z} + k\sqrt[3]{z}^2 \pmod{\mu}; \end{cases}$$

$y$  étant une quantité rationnelle.

Élévant les deux membres de ces congruences au carré, et éliminant  $A$ , on obtient :

$$(2ky + 4)\sqrt[3]{z}^2 + (4k^2z + 2y)\sqrt[3]{z} + 12p + 8kz + y^2 \equiv 0 \pmod{\mu}.$$

Multipliant cette congruence par  $\sqrt[3]{z}$ , on a :

$$(4k^2z + 2y)\sqrt[3]{z}^2 + (12p + 8kz + y^2)\sqrt[3]{z} + (2ky + 4)z \equiv 0 \pmod{\mu}.$$

Éliminant  $\sqrt[3]{z}^2$  entre ces deux congruences, on trouve :

$$\sqrt[3]{z} \equiv \sqrt[3]{-q + \sqrt[3]{q^2 + p^3}} \equiv \frac{8z - 24k^2pz - 16k^3z^2 - 12py - y^3}{8k^4z^2 - 12kpy - ky^3 - 24p - 16kz} \pmod{\mu}.$$

Or cette dernière congruence est impossible, puisqu'elle donne pour  $\sqrt[3]{z}$  une valeur rationnelle ; la valeur de  $x''$  est donc irrationnelle.

Il ne saurait arriver que le numérateur et le dénominateur fussent congrus à zéro, car alors on aurait :

$$\sqrt[3]{z} \equiv \frac{2k^2z + \gamma}{ky + 2} \pmod{\mu};$$

ce qu'on ne saurait admettre, à moins que le numérateur et le dénominateur ne fussent encore congrus à zéro, auquel cas nous aurions

$$\sqrt[3]{z} \equiv \frac{1}{k} \pmod{\mu};$$

ce qu'on ne peut admettre.

Le même raisonnement pourrait s'appliquer à  $x'''$  seulement. Au lieu des congruences (b.), il faudrait considérer les deux suivantes :

$$A - \frac{p}{A} \equiv \sqrt[3]{z} + k\sqrt[3]{z^2} \pmod{\mu},$$

$$\sqrt[3]{-3\left(A + \frac{p}{A}\right)} \equiv \gamma - \sqrt[3]{z} - k\sqrt[3]{z^2} \pmod{\mu}.$$

Réciproquement, si la congruence (1.) n'est pas satisfaite, la congruence proposée n'admet aucune racine rationnelle.

En effet, si la congruence admettait une racine rationnelle, la quantité  $A$  devrait être rationnelle; car si cette quantité ne l'était pas, les trois racines seraient irrationnelles; comme nous venons de le reconnaître. Or si  $A$  est rationnelle, on a :

$$A^{\mu-1} \equiv 1 \pmod{\mu},$$

et par suite :

$$[-q + \sqrt[3]{(q^2 + p^3)}]^{2n} \equiv 1 \pmod{\mu}.$$

Mais, par hypothèse, cette congruence n'est point satisfaite : la congruence proposée ne peut donc admettre aucune racine rationnelle.

### §. 5.

La détermination des racines de la congruence proposée est bien simple dans le cas qui nous occupe, puisqu'il suffit de calculer les trois valeurs  $A'$ ,  $A''$  et  $A'''$  de la quantité

$$A \equiv \sqrt[3]{-q + \sqrt[3]{(q^2 + p^3)}} \pmod{\mu};$$

et les trois racines seront données par les formules (3.) du paragraphe précédent, ou par les formules (2, 3 et 4.) du paragraphe 1, en prenant pour  $A$  l'une quelconque de ces trois valeurs.

Ce procédé a l'inconvénient de ne pas donner l'expression des racines en fonctions rationnelles des coefficients de la congruence proposée et du nombre premier  $\mu$ . En nous appliquant à cette détermination, nous avons pu facilement y arriver lorsque le nombre premier  $\mu$  avait l'une des deux formes  $18m+7$  et  $18m+13$ ; nous avons, au contraire, reconnu qu'il fallait distinguer plusieurs cas lorsque  $\mu$  était de la forme  $18m+1$ . Aussi, pour ne pas donner à ce mémoire trop d'étendue, nous nous contenterons d'exposer la marche à suivre dans les deux premiers cas. Pour le cas où  $\mu = 18m+1$ , nous examinerons les cas où ce nombre premier n'est pas en même temps de la forme  $54k+1$ ; il sera facile au lecteur de suppléer à l'omission que nous ferons par des considérations analogues à celles dans lesquelles nous allons entrer.

Nous devons faire observer ici que nous n'avons point cherché à exprimer les trois racines d'une même congruence en fonctions rationnelles des coefficients du nombre premier, mais seulement l'une d'elles; en second lieu nous avons regardé les expressions  $\sqrt[3]{-3}$ ,  $\sqrt[3]{p}$ ,  $\sqrt[3]{p^2}$  etc. comme rationnelles, lorsqu'il était reconnu que ces expressions l'étaient.

#### §. 6.

**Théorème IV.** *Si le nombre premier  $\mu = 6n+1$  est également de la forme  $18m+7$ , et si la congruence proposée*

$$x^3 + 3px + 2q \equiv 0 \pmod{\mu},$$

*dans laquelle  $p$  et  $q$  sont tels que l'on a*

$$(q^2 + p^3)^{\frac{1}{3}(\mu-1)} \equiv 1 \pmod{\mu},$$

*admet trois racines rationnelles: ces trois racines seront données par les formules*

$$x' \equiv 2M \pmod{\mu},$$

$$x'' \equiv -M + \sqrt[3]{-3(M^2 + p)} \pmod{\mu},$$

$$x''' \equiv -M - \sqrt[3]{-3(M^2 + p)} \pmod{\mu};$$

*$M$  représentant la partie du développement de l'expression*

$$[-q + \sqrt[3]{(q^2 + p^3)}]^{2m+1}$$

*qui ne contient pas  $\sqrt[3]{(q^2 + p^3)}$  en facteur; c'est-à-dire:*

$$\frac{1}{2} \{ [-q + \sqrt[3]{(q^2 + p^3)}]^{2m+1} + [-q - \sqrt[3]{(q^2 + p^3)}]^{2m+1} \}.$$

En vertu de la congruence (1. §. 4.) et de la forme du nombre premier  $\mu$ , on a:

$$[-q + \sqrt[3]{(q^2 + p^3)}]^{6m+3} \equiv [-q + \sqrt[3]{(q^2 + p^3)}] \pmod{\mu}.$$

Extrayant la racine troisième des deux nombres, et posant, pour abrégé :

$$[-q + \sqrt[3]{(q^2 + p^3)}]^{2m+1} \equiv M + N\sqrt[3]{(q^2 + p^3)} \pmod{\mu},$$

nous aurons :

$$[-q + \sqrt[3]{(q^2 + p^3)}]^{\frac{1}{3}} \equiv M + N\sqrt[3]{(q^2 + p^3)} \pmod{\mu}.$$

Changeant le signe de  $\sqrt[3]{(q^2 + p^3)}$ , on obtient

$$[-q - \sqrt[3]{(q^2 + p^3)}]^{\frac{1}{3}} \equiv M - N\sqrt[3]{(q^2 + p^3)} \pmod{\mu}.$$

Additionnant ces deux congruences, on obtient

$$x' \equiv 2M \pmod{\mu},$$

en remarquant que

$$x' \equiv [-q + \sqrt[3]{(q^2 + p^3)}]^{\frac{1}{3}} + [-q - \sqrt[3]{(q^2 + p^3)}]^{\frac{1}{3}} \pmod{\mu}.$$

Les valeurs de  $x''$  et  $x'''$  s'obtiennent facilement en divisant le premier membre de la congruence proposée par  $x - 2M$ , ce qui donne pour quotient,  $x^2 + 2Mx + 3p + 4M^2$  : quantité qui, congrue à zéro, donne :

$$x \equiv -M \pm \sqrt{[-3(M^2 + p)]} \pmod{\mu}.$$

### §. 7.

**Théorème V.** *Si le nombre premier  $\mu = 6n + 1$  est également de la forme  $18m + 13$ , et si la congruence proposée*

$$x^3 + 3px + 2q \equiv 0 \pmod{\mu},$$

*dans laquelle  $p$  et  $q$  sont tels que l'on a :*

$$(q^2 + p^3)^{\frac{1}{3}(\mu-1)} \equiv 1 \pmod{\mu},$$

*admet trois solutions rationnelles : les trois racines de cette congruence seront données par les formules*

$$x' \equiv \frac{1}{M + N\sqrt[3]{(q^2 + p^3)}} - p[M + N\sqrt[3]{(q^2 + p^3)}] \pmod{\mu},$$

$$x'' \equiv \frac{1}{M - N\sqrt[3]{(q^2 + p^3)}} - p[M - N\sqrt[3]{(q^2 + p^3)}] \pmod{\mu},$$

$$x''' \equiv 2M\left(p + \frac{1}{p^{6m+3}}\right) \pmod{\mu},$$

*en posant, pour abrégé :*

$$[-q + \sqrt[3]{(q^2 + p^3)}]^{2m+1} \equiv M + N\sqrt[3]{(q^2 + p^3)} \pmod{\mu}.$$

En vertu de la congruence (1. §. 4.) et de la forme du nombre premier  $\mu$ , on a :

$$-q + \sqrt[3]{(q^2 + p^3)} \equiv \frac{1}{[-q + \sqrt[3]{(q^2 + p^3)}]^{6m+3}} \pmod{\mu}.$$

Extrayant la racine troisième des deux nombres, et posant, pour abréger:

$$[-q + \sqrt[3]{(q^2 + p^3)}]^{2m+1} \equiv M + N\sqrt[3]{(q^2 + p^3)} \pmod{\mu},$$

on trouve

$$[-q + \sqrt[3]{(q^2 + p^3)}]^{\frac{1}{3}} \equiv \frac{1}{M + N\sqrt[3]{(q^2 + p^3)}} \pmod{\mu}.$$

On voit ainsi que l'expression

$$\frac{1}{M + N\sqrt[3]{(q^2 + p^3)}}$$

est l'une des trois valeurs du radical cubique  $[-q + \sqrt[3]{(q^2 + p^3)}]^{\frac{1}{3}}$ ; par conséquent l'une des racines de la congruence proposée sera:

$$x' \equiv \frac{1}{M + N\sqrt[3]{(q^2 + p^3)}} - p[M + N\sqrt[3]{(q^2 + p^3)}] \pmod{\mu}.$$

De la connaissance de cette racine on pourrait déduire les deux autres, mais il est plus simple de remarquer qu'en changeant le signe de  $\sqrt[3]{(q^2 + p^3)}$  dans la congruence (1. §. 4.), on a:

$$-q - \sqrt[3]{(q^2 + p^3)} \equiv \frac{1}{[-q - \sqrt[3]{(q^2 + p^3)}]^{6m+3}} \pmod{\mu};$$

d'où l'on déduit par un raisonnement analogue au précédent la racine

$$x'' \equiv \frac{1}{M - N\sqrt[3]{(q^2 + p^3)}} - p[M - N\sqrt[3]{(q^2 + p^3)}] \pmod{\mu}.$$

Comme d'ailleurs on sait que

$$x''' \equiv -(x' + x'') \pmod{\mu},$$

il en résultera:

$$x''' \equiv 2M\left(p + \frac{1}{p^{6m+3}}\right) \pmod{\mu},$$

en remarquant que

$$M^2 - N^2(q^2 + p^3) \equiv -p^{6m+3} \pmod{\mu}.$$

### §. 8.

Nous avons vu (§. 4.) que lorsque  $\mu$  est un nombre premier de la forme  $6n + 1$ ,  $p$  et  $q$  étant deux nombres tels que

$$(q^2 + p^3)^{\frac{1}{3}(\mu-1)} \equiv 1 \pmod{\mu},$$

la congruence

$$x^3 + 3px + 2q \equiv 0 \pmod{\mu}$$

admettait trois racines rationnelles, lorsque la congruence de condition:

$$[-q + \sqrt[3]{(q^2 + p^3)}]^{2n} \equiv 1 \pmod{\mu}$$

était satisfaite.

Si nous admettons que  $\mu$  soit de la forme  $18m+1$ , nous aurons  $2n=6m$ , et par conséquent :

$$(1.) \quad [-q + \sqrt[3]{(q^2 + p^3)}]^{6m} \equiv 1 \pmod{\mu}.$$

Or, si l'on remarque qu'en désignant par  $r$  l'une quelconque des racines primitives de  $\mu$ , on a pour les trois racines de l'unité :

$$\sqrt[3]{1} \equiv 1 \pmod{\mu},$$

$$\sqrt[3]{1} \equiv r^{+\frac{1}{3}(\mu-1)} \equiv -\frac{1}{2} + \frac{1}{2}\sqrt{-3} \pmod{\mu},$$

$$\sqrt[3]{1} \equiv r^{-\frac{1}{3}(\mu-1)} \equiv -\frac{1}{2} - \frac{1}{2}\sqrt{-3} \pmod{\mu},$$

il en résultera que si la congruence proposée admet trois solutions, nous aurons l'une des trois congruences

$$[-q + \sqrt[3]{(q^2 + p^3)}]^{2m} \equiv 1 \pmod{\mu},$$

$$[-q + \sqrt[3]{(q^2 + p^3)}]^{2m} \equiv r^{\frac{1}{3}(\mu-1)} \equiv -\frac{1}{2} + \frac{1}{2}\sqrt{-3} \pmod{\mu},$$

$$[-q + \sqrt[3]{(q^2 + p^3)}]^{2m} \equiv r^{-\frac{1}{3}(\mu-1)} \equiv -\frac{1}{2} - \frac{1}{2}\sqrt{-3} \pmod{\mu}.$$

Cela posé, nous pourrions établir les *théorèmes* suivants :

I. *Si le nombre premier  $\mu = 18m+1$  est également de la forme  $54k+19$ , et si la congruence proposée*

$$x^3 + 3px + 2q \equiv 0 \pmod{\mu},$$

*dans laquelle  $p$  et  $q$  sont tels que l'on a :*

$$(q^2 + p^3)^{\frac{1}{3}(\mu-1)} \equiv 1 \pmod{\mu},$$

$$[-q + \sqrt[3]{(q^2 + p^3)}]^{2m} \equiv 1 \pmod{\mu}$$

*admet trois racines rationnelles : l'une de ces racines sera donnée par la formule*

$$x' \equiv [-q + \sqrt[3]{(q^2 + p^3)}]^{2k+1} - \frac{p}{[-q + \sqrt[3]{(q^2 + p^3)}]^{2k+1}} \pmod{\mu}.$$

II. *Si le nombre premier  $\mu = 18m+1$  est également de la forme  $54k+19$ , et si la congruence proposée*

$$x^3 + 3px + 2q \equiv 0 \pmod{\mu},$$

*dans laquelle  $p$  et  $q$  sont tels que l'on a :*

$$(q^2 + p^3)^{\frac{1}{3}(\mu-1)} \equiv 1 \pmod{\mu},$$

$$[-q + \sqrt[3]{(q^2 + p^3)}]^{2m} \equiv r^{\pm \frac{1}{3}(\mu-1)} \pmod{\mu},$$

*admet trois racines rationnelles : l'une de ces racines sera donnée par la formule*

$$x' \equiv \frac{[-q + \sqrt[3]{(q^2 + p^3)}]^{2k+1}}{r^{\pm \frac{1}{3}(\mu-1)}} - p \frac{r^{\pm \frac{1}{3}(\mu-1)}}{[-q + \sqrt[3]{(q^2 + p^3)}]^{2k+1}} \pmod{\mu}.$$

III. Si le nombre premier  $\mu = 18m + 1$  est également de la forme  $54k + 37$ , et si la congruence proposée

$$x^3 + 3px + 2q \equiv 0 \pmod{\mu},$$

dans laquelle  $p$  et  $q$  sont tels que l'on a :

$$(q^2 + p^3)^{\frac{1}{3}(\mu-1)} \equiv 1 \pmod{\mu},$$

$$(-q + \sqrt[3]{(q^2 + p^3)})^{2m} \equiv 1 \pmod{\mu},$$

admet trois racines rationnelles : l'une de ces racines sera donnée par la formule

$$x' \equiv \frac{1}{[-q + \sqrt[3]{(q^2 + p^3)}]^{2k+1}} - p[-q + \sqrt[3]{(q^2 + p^3)}]^{2k+1} \pmod{\mu}.$$

IV. Si le nombre premier  $\mu = 18m + 1$  est également de la forme  $54k + 37$ , et si la congruence proposée

$$x^3 + 3px + 2q \equiv 0 \pmod{\mu},$$

dans laquelle  $p$  et  $q$  sont tels que l'on a :

$$(q^2 + p^3)^{\frac{1}{3}(\mu-1)} \equiv 1 \pmod{\mu},$$

$$[-q + \sqrt[3]{(q^2 + p^3)}]^{2m} \equiv r^{\pm \frac{1}{3}(\mu-1)} \pmod{\mu},$$

admet trois racines rationnelles : l'une de ces racines sera donnée par la formule

$$x' \equiv \frac{r^{\pm \frac{1}{3}(\mu-1)}}{[-q + \sqrt[3]{(q^2 + p^3)}]^{2k+1}} - p \frac{[-q + \sqrt[3]{(q^2 + p^3)}]^{2k+1}}{r^{\pm \frac{1}{3}(\mu-1)}} \pmod{\mu}.$$

Les démonstrations de ces théorèmes sont analogues à celles des théorèmes précédents, et ne présentent aucune difficulté. D'autre part, il est facile de déterminer les deux autres racines de chaque congruence par la connaissance de l'une d'elles.

Dans le cas où le nombre premier  $\mu = 18m + 1$  serait aussi de la forme  $54k + 1$ , la congruence de condition (1.) deviendrait :

$$[-q + \sqrt[3]{(q^2 + p^3)}]^{18k} \equiv 1 \pmod{\mu},$$

et il serait facile d'établir des théorèmes analogues aux précédents, en considérant les neuf racines neuvièmes de l'unité ; et ainsi de suite.

## §. 9.

Lemme I. Quel que soit le nombre premier  $\mu$  : si la congruence

$$x^3 + 3px + 2q \equiv 0 \pmod{\mu}$$

admet des racines rationnelles, elle en admettra, une seule, ou trois.

Remarquons en effet que si deux racines de cette congruence étaient rationnelles, comme la somme des trois racines est congrue à zéro: toutes les trois devraient l'être.

**Lemme II.** *Si  $\mu$  est un nombre premier quelconque,  $b$  un nombre tel que l'on ait*

$$b^{\frac{1}{2}(\mu-1)} \equiv -1 \pmod{\mu},$$

*en désignant par  $a$ ,  $r$  et  $s$  des quantités rationnelles quelconques: l'expression*

$$(1.) \quad N \equiv sM + \frac{r}{M} \pmod{\mu},$$

*dans laquelle est*

$$M \equiv \sqrt[\frac{1}{2}]{a + \sqrt{b}} \pmod{\mu},$$

*ne peut être rationnelle qu'autant qu'on a la relation*

$$(2.) \quad s\sqrt{(a^2 - b)} - r \equiv 0 \pmod{\mu}.$$

En effet, si  $N$  est rationnelle, on doit avoir par le théorème de *Fermat*:

$$N^{\mu-1} \equiv 1 \pmod{\mu},$$

et par conséquent

$$\left(sM + \frac{r}{M}\right)^{\mu-1} \equiv 1 \pmod{\mu}.$$

Multipliant les deux membres de cette congruence par  $sM + \frac{r}{M}$ , et remarquant que

$$\left(sM + \frac{r}{M}\right)^{\mu} \equiv s^{\mu}M^{\mu} + \frac{r^{\mu}}{M^{\mu}} \pmod{\mu},$$

$$s^{\mu} \equiv s \pmod{\mu},$$

$$r^{\mu} \equiv r \pmod{\mu},$$

nous obtiendrons:

$$(3.) \quad sM^{2\mu} + r \equiv sM^{\mu+1} + rM^{\mu-1} \pmod{\mu}.$$

Mais en élevant les deux membres de la congruence

$$M \equiv \sqrt[\frac{1}{2}]{a + \sqrt{b}} \pmod{\mu}$$

à la puissance  $\mu$ , en supprimant les multiples de  $\mu$  et en tenant compte de la relation

$$b^{\frac{1}{2}(\mu-1)} \equiv -1 \pmod{\mu},$$

on obtient:

$$M^{\mu} \equiv \sqrt[\frac{1}{2}]{a - \sqrt{b}} \pmod{\mu};$$

par conséquent nous aurons

$$M^{\mu+1} \equiv \sqrt[3]{(a^2 - b)} \pmod{\mu},$$

$$M^{\mu} \equiv \frac{\sqrt[3]{(a^2 - b)}}{M} \pmod{\mu},$$

$$M^{2\mu} \equiv \frac{\sqrt[3]{[(a^2 - b)^2]}}{M^2} \pmod{\mu},$$

$$M^{\mu-1} \equiv \frac{\sqrt[3]{(a^2 - b)}}{M^2} \pmod{\mu}.$$

Ces valeurs, mises dans la congruence (3.), donnent

$$[s\sqrt[3]{(a^2 - b)} - r]M^2 \equiv s\sqrt[3]{[(a^2 - b)^2]} - r\sqrt[3]{(a^2 - b)} \pmod{\mu},$$

ce que l'on peut écrire sous la forme

$$[s\sqrt[3]{(a^2 - b)} - r][M^2 - \sqrt[3]{(a^2 - b)}] \equiv 0 \pmod{\mu},$$

si nous remarquons que l'on ne peut pas poser

$$M^2 \equiv \sqrt[3]{(a^2 - b)} \pmod{\mu};$$

car il en résulterait

$$\sqrt[3]{b} \equiv -\frac{b}{a} \pmod{\mu};$$

congruence absurde, puisqu'elle donne pour  $\sqrt[3]{b}$  une valeur rationnelle; ce qui par hypothèse ne peut être admis,  $b$  étant tel que

$$b^{\frac{1}{3}(\mu-1)} \equiv -1 \pmod{\mu},$$

tandis qu'il faudrait que l'on ait

$$s\sqrt[3]{(a^2 - b)} - r \equiv 0 \pmod{\mu}.$$

#### §. 10.

**Théorème VI.** *Si  $\mu$  est un nombre premier de la forme  $6n + 1$ , et si  $p$  et  $q$  sont deux nombres tels que l'on ait*

$$(q^2 + p^3)^{\frac{1}{3}(\mu-1)} \equiv -1 \pmod{\mu},$$

*la congruence*

$$x^3 + 3px + 2q \equiv 0 \pmod{\mu}$$

*ne pourra admettre plus d'une racine rationnelle.*

En vertu du lemme I., cette proposition sera démontrée si nous prouvons que les trois racines ne peuvent être rationnelles. Si les trois racines  $x'$ ,  $x''$  et  $x'''$  sont rationnelles, la valeur de l'expression

$$A + \frac{p}{A}$$

le sera. Comme d'ailleurs  $\sqrt{-3}$  est une quantité rationnelle, puisque  $\mu$  est de la forme  $6n+1$ , il est nécessaire (vu les valeurs de  $x'$  et  $x''$ ) que l'expression

$$A + \frac{p}{A}$$

soit également rationnelle.

Or il est facile de démontrer que cette expression ne l'est pas, quelle que soit la forme du nombre premier  $\mu$ . Il suffit pour cela de faire dans la congruence (2.) du paragraphe précédent:

$$\begin{aligned} a &\equiv -q \pmod{\mu}, \\ b &\equiv q^2 + p^3 \pmod{\mu}, \\ s &\equiv 1 \pmod{\mu}, \\ r &\equiv p \pmod{\mu}, \end{aligned}$$

et nous aurons:

$$-2p \equiv 0 \pmod{\mu}:$$

congruence qu'on ne peut admettre; car il en résultera  $p \equiv 0$ , et la quantité  $\sqrt[3]{(q^2 + p^3)}$  ne serait plus irrationnelle.

### §. 11.

On peut arriver au même résultat, en remarquant que si  $x \equiv x_1 \pmod{\mu}$  est une racine rationnelle de la congruence proposée, les trois racines seront données par les expressions

$$x' \equiv x_1, \quad x'' \equiv -\frac{1}{2}x_1 + \frac{\sqrt{[-3(q^2 + p^3)]}}{x_1^2 + p}, \quad x''' \equiv -\frac{1}{2}x_1 - \frac{\sqrt{[-3(q^2 + p^3)]}}{x_1^2 + p} \pmod{\mu};$$

car on a

$$x' + x'' + x''' \equiv 0, \quad x'x'' + x'x''' + x''x''' \equiv 3p, \quad x'x''x''' \equiv -q \pmod{\mu},$$

(en vertu de la relation

$$x_1^3 + 3px_1 + 2q \equiv 0 \pmod{\mu}).$$

Il résulte de là que, comme  $\sqrt{-3}$  est une quantité rationnelle par la forme de  $\mu = 6n+1$ , l'expression  $\sqrt{[-3(q^2 + p^3)]}$  sera irrationnelle; et par suite, si  $x_1$  est irrationnelle, les valeurs de  $x'$  et  $x''$  seront irrationnelles.

### §. 12.

**Théorème VII.** *Si  $\mu$  est un nombre premier de la forme  $6n+1$ , et si  $p$  et  $q$  sont deux nombres tels que l'on ait la relation*

$$(q^2 + p^3)^{\frac{1}{3}(\mu-1)} \equiv -1 \pmod{\mu},$$

*la congruence proposée*

$$x^3 + 3px + 2q \equiv 0 \pmod{\mu}$$

admettra une solution rationnelle, ou n'en admettra aucune, selon, qu'en désignant par  $M$  la partie rationnelle du développement de l'expression

$$[-q + \sqrt[3]{(q^2 + p^3)}]^{2n},$$

la congruence

$$(2M-1)^2(M+1) \equiv -\frac{2q^2}{p^3} \pmod{\mu}$$

sera, ou ne sera pas satisfaite.

Nous avons reconnu par le théorème précédent que la congruence proposée ne pouvait admettre qu'une seule racine, donnée par l'expression

$$x \equiv \sqrt[3]{[-q + \sqrt[3]{(q^2 + p^3)}]} + \sqrt[3]{[-q - \sqrt[3]{(q^2 + p^3)}]} \pmod{\mu}.$$

En admettant que cette valeur de  $x$  est rationnelle, on pourra, en désignant par  $A$  et  $B$  des quantités également rationnelles, poser:

$$(1.) \quad \sqrt[3]{[-q + \sqrt[3]{(q^2 + p^3)}]} \equiv A + B\sqrt[3]{(q^2 + p^3)} \pmod{\mu},$$

et il en resultera

$$(2.) \quad \sqrt[3]{[-q - \sqrt[3]{(q^2 + p^3)}]} \equiv A - B\sqrt[3]{(q^2 + p^3)} \pmod{\mu}.$$

De ces deux congruences on déduit aisément:

$$(3.) \quad x \equiv 2A \pmod{\mu},$$

$$(4.) \quad A^2 - B^2(q^2 + p^3) \equiv -p \pmod{\mu}.$$

Comme le nombre premier  $\mu$  est de la forme  $6n+1$ : en élevant les deux membres de la congruence (1.) à la puissance  $\mu-1=6n$ , on aura:

$$(5.) \quad [-q + \sqrt[3]{(q^2 + p^3)}]^{2n} \equiv [A + B\sqrt[3]{(q^2 + p^3)}]^{\mu-1} \equiv \frac{A - B\sqrt[3]{(q^2 + p^3)}}{A + B\sqrt[3]{(q^2 + p^3)}} \pmod{\mu},$$

et en faisant, pour abrégér,

$$(6.) \quad [-q + \sqrt[3]{(q^2 + p^3)}]^{2n} \equiv M + N\sqrt[3]{(q^2 + p^3)} \pmod{\mu},$$

auquel cas on a

$$(7.) \quad M \equiv q^{2n} + \frac{2n-1}{2} q^{2n-2} (q^2 + p^3) + \frac{2n-1}{2} \cdot \frac{2n-2}{3} \cdot \frac{2n-3}{4} q^{2n-4} (q^2 + p^3)^2 + \dots \pmod{\mu},$$

on obtient au moyen des congruences (5. et 6.):

$$(8.) \quad \frac{A - B\sqrt[3]{(q^2 + p^3)}}{A + B\sqrt[3]{(q^2 + p^3)}} \equiv M + N\sqrt[3]{(q^2 + p^3)} \pmod{\mu},$$

et par suite

$$(9.) \quad \frac{A + B\sqrt[3]{(q^2 + p^3)}}{A - B\sqrt[3]{(q^2 + p^3)}} \equiv M - N\sqrt[3]{(q^2 + p^3)} \pmod{\mu}.$$

De ces deux congruences on déduit

$$(10.) \quad M^2 - N^2(q^2 + p^3) \equiv 1 \pmod{\mu},$$

$$(11.) \quad MA + NB(q^2 + p^3) \equiv A \pmod{\mu}.$$

Si maintenant on élimine  $B$  et  $N$  entre les congruences (4. 10. et 11.), on obtiendra :

$$(12.) \quad 4A^2 \equiv -2p(M+1) \pmod{\mu};$$

et comme par hypothèse  $x \equiv 2A$  est une racine rationnelle de la congruence proposée, on aura

$$(13.) \quad 4A^3 + 3pA + q \equiv 0 \pmod{\mu}.$$

Éliminant  $A$  entre ces deux congruences, on trouve

$$(14.) \quad (2M-1)^2(M+1) \equiv -\frac{2q^2}{p^3} \pmod{\mu}.$$

Telle est la relation qui doit exister entre les coefficients de la congruence proposée, pour que cette congruence puisse admettre une solution rationnelle.

### §. 13

**Théorème VIII.** *Si  $\mu$  est un nombre premier de la forme  $6n+1$ , et si  $p$  et  $q$  sont deux nombres tels que l'on ait la relation*

$$(q^2 + p^3)^{\frac{1}{3}(\mu-1)} \equiv -1 \pmod{\mu};$$

*tandis que la congruence proposée*

$$x^3 + 3px + 2q \equiv 0 \pmod{\mu}$$

*admet une solution rationnelle: cette solution sera donnée par la formule*

$$x \equiv \frac{2q}{p(2M-1)} \pmod{\mu};$$

$M$  représentant la partie rationnelle du développement de l'expression

$$[-q + \sqrt[3]{(q^2 + p^3)}]^{2n}$$

*par la formule du binôme.*

En effet, la seule racine rationnelle de la congruence proposée étant

$$x \equiv \sqrt[3]{[-q + \sqrt[3]{(q^2 + p^3)}]} + \sqrt[3]{[-q - \sqrt[3]{(q^2 + p^3)}]} \equiv 2A \pmod{\mu},$$

nous aurons, en vertu de la congruence (12.) du paragraphe précédent:

$$(1.) \quad x^2 \equiv -2p(M+1),$$

et par suite on a pour  $x$  les deux valeurs

$$x \equiv +\sqrt{[-2p(M+1)]} \pmod{\mu},$$

$$x \equiv -\sqrt{[-2p(M+1)]} \pmod{\mu}.$$

Il peut paraître surprenant que l'on obtienne pour  $x$  deux valeurs rationnelles, égales et de signes contraires, tandis que la congruence proposée ne peut admettre qu'une seule solution. Cette difficulté s'explique aisément si l'on remarque que,  $M$  conservant la même valeur, quel que soit le signe de  $q$ , les deux valeurs précédentes ne sont pas toutes deux racines de la congruence proposée

$$x^3 + 3px + 2q \equiv 0 \pmod{\mu},$$

mais que l'une de ces valeurs est une racine de cette congruence et l'autre appartient à la congruence

$$x^3 + 3px - 2q \equiv 0 \pmod{\mu},$$

à laquelle on pourrait appliquer le même raisonnement qui nous a conduit à la congruence (12.) du paragraphe précédent, en changeant  $q$  en  $-q$ ; ce qui n'altérerait pas cette dernière congruence.

Si nous voulons connaître celle de ces deux valeurs de  $x$  qui appartient à la congruence proposée, il suffit d'éliminer  $x^2$  entre les congruences

$$x^2 \equiv -2p(M+1) \pmod{\mu},$$

$$x^3 + 3px + 2q \equiv 0 \pmod{\mu};$$

ce qui conduit à la solution

$$x \equiv \frac{2q}{p(2M-1)} \pmod{\mu}.$$

#### §. 14.

On peut aussi démontrer les deux théorèmes que nous venons de donner, d'une manière plus simple, en remarquant que l'on a identiquement:

$$[-q + \sqrt{(q^2 + p^3)}]^\mu \equiv -q - \sqrt{(q^2 + p^3)} \pmod{\mu}.$$

Par suite on trouve

$$\begin{aligned} x &\equiv [-q + \sqrt{(q^2 + p^3)}]^{\frac{1}{3}} + [-q - \sqrt{(q^2 + p^3)}]^{\frac{1}{3}} \\ &\equiv [-q + \sqrt{(q^2 + p^3)}]^{\frac{1}{3}} + [1 + (-q + \sqrt{(q^2 + p^3)})^{\frac{1}{3}(\mu-1)}] \pmod{\mu}; \end{aligned}$$

valeur qu'on peut mettre sous la forme

$$x \equiv [-q + \sqrt{(q^2 + p^3)}]^{\frac{1}{3}} [1 + M + N\sqrt{(q^2 + p^3)}] \pmod{\mu},$$

en ayant égard à la congruence (6. §. 12.).

En changeant le signe de  $\sqrt[3]{(q^2 + p^3)}$ , ce qui n'altère pas la valeur de  $x$ , on a :

$$x \equiv [-q - \sqrt[3]{(q^2 + p^3)}]^{\frac{1}{3}} [1 + M - N \sqrt[3]{(q^2 + p^3)}] \pmod{\mu}.$$

Multipliant ces deux valeurs de  $x$ , et ayant égard à la congruence (10.) du (§. 12), on obtient (toute réduction faite)

$$x^2 \equiv -2p(M+1) \pmod{\mu}.$$

Cette valeur de  $x^2$ , mise dans la congruence proposée, donne l'équation de condition

$$(2M-1)^2(M+1) \equiv -\frac{2q^2}{p^3} \pmod{\mu}.$$

Quant à la valeur de  $x$ , on l'obtiendrait comme dans le paragraphe précédent.

### §. 15.

Si l'on remarqué que la congruence précédente peut se mettre sous la forme

$$4M^3 - 3M + 1 + \frac{2q^2}{p^3} \equiv 0 \pmod{\mu},$$

ou bien sous celle-ci :

$$z^3 - 3z + 2\left(1 + \frac{2q^2}{p^3}\right) \equiv 0 \pmod{\mu},$$

en supposant  $z = 2M$ , il en résultera que si cette dernière congruence admet une solution rationnelle, solution qui sera donnée par

$$z \equiv \frac{2\left(1 + \frac{2q^2}{p^3}\right)}{1 - 2M'} \pmod{\mu},$$

en supposant

$$(1.) \quad M' \equiv \left(1 + \frac{2q^2}{p^3}\right)^{2n} + \frac{1}{2}n \cdot \frac{2n-1}{2} \left(1 + \frac{2q^2}{p^3}\right)^{2n-2} \left[\left(1 + \frac{2q^2}{p^3}\right)^2 - 1\right] \\ + \frac{1}{2}n \cdot \frac{2n-1}{2} \cdot \frac{2n-2}{3} \cdot \frac{2n-3}{4} \left(1 + \frac{2q^2}{p^3}\right)^{2n-4} \left[\left(1 + \frac{2q^2}{p^3}\right)^2 - 1\right]^2 + \dots \pmod{\mu} :$$

la valeur de  $z$  devra être égale à  $2M$ , pour que la congruence proposée

$$x^3 + 3p + 2q \equiv 0 \pmod{\mu}$$

admette une solution rationnelle.

On voit ainsi que si la congruence proposée admet une racine rationnelle, on aura la relation

$$M(1 - 2M') \equiv 1 + \frac{2q^2}{p^3} \pmod{\mu},$$

$M$  et  $M'$  étant données par la formule (7. §. 12.) et par la formule (1.) de celui-ci.

Réciproquement, si cette congruence est satisfaite, la congruence proposée admettra une racine, donnée par la formule

$$x \equiv \frac{2q}{p(2M-1)}.$$

### §. 16.

**Théorème IX.** *Si  $\mu$  est un nombre premier de la forme  $6n-1$ , et si  $p$  et  $q$  sont deux nombres tels que l'on ait :*

$$(q^2 + p^3)^{\frac{1}{3}(\mu-1)} \equiv -1 \pmod{\mu},$$

*la congruence proposée :*

$$x^3 + 3px + 2q \equiv 0 \pmod{\mu}$$

*admettra trois racines rationnelles, ou n'en admettra aucune.*

Si nous supposons que  $x \equiv x_1 \pmod{\mu}$  soit une solution rationnelle de la congruence proposée, nous pouvons facilement reconnaître que les trois solutions seront exprimées par :

$$(1.) \quad x' \equiv x_1 \pmod{\mu},$$

$$(2.) \quad x'' \equiv -\frac{1}{2}x_1 + \frac{\sqrt{[-3(q^2 + p^3)]}}{x_1^2 + p} \pmod{\mu},$$

$$(3.) \quad x''' \equiv -\frac{1}{2}x_1 - \frac{\sqrt{[-3(q^2 + p^3)]}}{x_1^2 + p} \pmod{\mu};$$

car, en vertu de la relation

$$x_1^3 + 3px_1 + 2q \equiv 0 \pmod{\mu},$$

on a les identités :

$$\begin{aligned} x' + x'' + x''' &\equiv 0 \pmod{\mu}, \\ x'x'' + x'x''' + x''x''' &\equiv 3p \pmod{\mu}, \\ x'x''x''' &\equiv -2q \pmod{\mu}. \end{aligned}$$

Il résulte de là que, comme  $-3$  est racine impaire de tout nombre premier  $\mu$  de la forme  $6n-1$ , l'expression  $\sqrt{[-3(q^2 + p^3)]}$  sera rationnelle, et les trois racines de la congruence proposée, se composant de parties rationnelles, seront elles mêmes rationnelles.

### §. 17.

**Théorème X.** *Si  $\mu$  est un nombre premier de la forme  $6n-1$ , et si  $p$  et  $q$  sont des nombres tels que l'on ait la relation*

$$(q^2 + p^3)^{\frac{1}{3}(\mu-1)} \equiv -1 \pmod{\mu},$$

la congruence proposée

$$x^3 + 3px + 2q \equiv 0 \pmod{\mu}$$

admettra trois racines rationnelles, ou n'en admettra aucune; selon, qu'en désignant par  $M$  la partie rationnelle du développement de l'expression

$$[-q + \sqrt{(q^2 + p^3)}]^{2n-1},$$

la congruence

$$(A.) \quad Mp^2 \equiv -q \pmod{\mu}$$

sera satisfaite, ou ne le sera pas.

En désignant par  $A$  et  $B$  deux quantités rationnelles, posons:

$$(1.) \quad \sqrt[3]{[-q + \sqrt{(q^2 + p^3)}]} \equiv A + B\sqrt{(q^2 + p^3)} \pmod{\mu}.$$

Il en résultera

$$(2.) \quad \sqrt[3]{[-q - \sqrt{(q^2 + p^3)}]} \equiv A - B\sqrt{(q^2 + p^3)} \pmod{\mu}.$$

De ces deux congruences on déduit aisément:

$$(3.) \quad x \equiv 2A \pmod{\mu},$$

$$(4.) \quad A^2 + B^2(q^2 + p^3) \equiv -p \pmod{\mu}.$$

Comme le nombre premier  $\mu$  est de la forme  $6n-1$ ; en élevant les deux membres de la congruence (1.) à la puissance  $\mu-1$ , et en ayant égard à la congruence (2.), on trouvera:

$$(5.) \quad [-q + \sqrt{(q^2 + p^3)}]^{2n-1} \equiv \frac{A - B\sqrt{(q^2 + p^3)}}{[A + B\sqrt{(q^2 + p^3)}]^2} \pmod{\mu}.$$

Si nous posons, pour abréger:

$$(6.) \quad [-q + \sqrt{(q^2 + p^3)}]^{2n-1} \equiv M + N\sqrt{(q^2 + p^3)} \pmod{\mu},$$

ce qui donne

$$\begin{aligned} M &\equiv (-q)^{2n-1} + \frac{2n-1}{1} \cdot \frac{2n-2}{2} (-q)^{2n-3} (q^2 + p^3) \\ &\quad + \frac{2n-1}{1} \cdot \frac{2n-2}{2} \cdot \frac{2n-3}{3} \cdot \frac{2n-4}{4} (-q)^{2n-5} (q^2 + p^3)^2 + \dots \pmod{\mu}, \end{aligned}$$

nous aurons

$$(7.) \quad \frac{A - B\sqrt{(q^2 + p^3)}}{[A + B\sqrt{(q^2 + p^3)}]^2} \equiv M + N\sqrt{(q^2 + p^3)} \pmod{\mu}.$$

Changeant le signe de  $\sqrt{(q^2 + p^3)}$  dans cette congruence, on obtient:

$$(8.) \quad \frac{A + B\sqrt{(q^2 + p^3)}}{[A - B\sqrt{(q^2 + p^3)}]^2} \equiv M - N\sqrt{(q^2 + p^3)} \pmod{\mu}.$$

De ces deux dernières relations on tire:

$$M^2 - N^2(q^2 + p^3) \equiv -\frac{1}{p} \pmod{\mu},$$

$$[A^2 + B^2(q^2 + p^3)]M + 2ABN(q^2 + p^3) \equiv A \pmod{\mu}.$$

Eliminant  $B$  et  $N$  entre la congruence (4.) et les deux dernières, on obtient, toutes réductions faites :

$$(9.) \quad 4A^3 + 3pA \equiv Mp^2 \pmod{\mu}.$$

Cela posé : si l'on admet que la congruence proposée admette une racine rationnelle, les trois racines seront rationnelles en vertu du théorème précédent; par conséquent  $2A$  sera une quantité rationnelle qui devra satisfaire à la congruence

$$x^3 + 3px + 2q \equiv 0 \pmod{\mu};$$

on aura donc

$$4A^3 + 3pA \equiv -q \pmod{\mu}.$$

Comparant cette congruence avec celle (9.), nous aurons la relation

$$Mp^2 \equiv -q \pmod{\mu}.$$

Il résulte de là que si cette dernière congruence est satisfaite, la quantité  $2A$ , qui est rationnelle, est racine de la congruence proposée; et par conséquent il existe trois racines rationnelles, propres à satisfaire à la congruence donnée.

Si cette dernière congruence n'est pas satisfaite, il est absurde de supposer que  $2A$  soit une racine rationnelle de la congruence donnée; et par suite il ne saurait en exister aucune.

### §. 18.

Pour déterminer les racines de la congruence proposée, dans le cas où l'équation de condition (A.) du paragraphe précédent est satisfaite, on pourra avoir recours à la congruence (4.) du même paragraphe, que l'on mettra sous la forme

$$A^2 + p \equiv B^2(q^2 + p^3) \pmod{\mu}.$$

Élevant ses deux membres à la puissance  $\frac{1}{2}(\mu-1) = 3n-1$ , et remarquant que

$$B^{6n-2} \equiv B^{\mu-1} \equiv +1 \pmod{\mu},$$

$$(q^2 + p^3)^{\frac{1}{2}(\mu-1)} \equiv -1 \pmod{\mu},$$

nous aurons :

$$(A^2 + p)^{3n-1} \equiv -1 \pmod{\mu}.$$

Développant le premier membre de cette congruence par la formule du binôme, et simplifiant le résultat au moyen de la congruence

$$4A^2 + 3pA + q \equiv 0 \pmod{\mu},$$

on arrivera nécessairement à une congruence du second degré, de la forme

$$(1.) \quad LA^2 + SA + T \equiv 0 \pmod{\mu}.$$

De ces deux congruences suit

$$4SA^2 + (4T - 3pL)A - qL \equiv 0 \pmod{\mu}.$$

Éliminant  $A^2$  entre ces deux congruences, on obtient:

$$A \equiv \frac{qL^2 + 4ST}{4LT - 4S^2 - 3pL^2} \pmod{\mu};$$

et par suite une des racines de la congruence proposée sera

$$x_1 \equiv \frac{2(qL^2 + 4ST)}{4LT - 4S^2 - 3pL^2} \pmod{\mu}.$$

Les congruences (2. et 3. §. 16.) détermineront les deux autres racines.

Ce procédé ne donne pas l'expression des racines en fonctions rationnelles des coefficients de la congruence proposée et du nombre premier  $\mu$ . Nous allons présenter dans les paragraphes suivants la détermination des racines sous ce point de vue, lorsque le nombre premier a l'une des deux formes  $18m + 11$  et  $18m + 5$ ; nos recherches ayant été infructueuses pour le cas où  $\mu$  est de la forme  $18m + 17$ .

### §. 19.

**Lemme.** *Si  $\mu$  est un nombre premier de la forme  $6n - 1$ , et si la congruence*

$$x^3 + 3px + 2q \equiv 0 \pmod{\mu},$$

*dans laquelle  $p$  et  $q$  sont tels que l'on a:*

$$(q^2 + p^3)^{\frac{1}{3}(\mu-1)} \equiv -1 \pmod{\mu};$$

*admet trois racines rationnelles, on aura:*

$$(a.) \quad [-q + \sqrt[3]{(q^2 + p^3)}]^{2n} \equiv -p \pmod{\mu}.$$

Remarquons d'abord que l'on a identiquement:

$$[-q + \sqrt[3]{(q^2 + p^3)}]^\mu \equiv -q - \sqrt[3]{(q^2 + p^3)} \pmod{\mu}.$$

Par suite la valeur de  $x$ :

$$x \equiv \sqrt[3]{-q + \sqrt[3]{(q^2 + p^3)}} + \sqrt[3]{-q - \sqrt[3]{(q^2 + p^3)}} \pmod{\mu}$$

peut être écrite:

$$x \equiv [-q + \sqrt[3]{(q^2 + p^3)}]^{\frac{1}{3}} + [-q + \sqrt[3]{(q^2 + p^3)}]^{\frac{1}{3}\mu} \pmod{\mu},$$

d'où l'on tire:

$$(1.) \quad x[-q + \sqrt[3]{(q^2 + p^3)}]^{\frac{1}{3}} \equiv [-q + \sqrt[3]{(q^2 + p^3)}]^{\frac{2}{3}} + P + Q\sqrt[3]{(q^2 + p^3)} \pmod{\mu}.$$

En posant, pour abrégé :

$$(2.) \quad [-q + \sqrt[3]{(q^2 + p^3)}]^{2n} \equiv P + Q\sqrt[3]{(q^2 + p^3)} \pmod{\mu},$$

et changeant dans la congruence (1.) le signe de  $\sqrt[3]{(q^2 + p^3)}$ , on obtient

$$(3.) \quad x[-q - \sqrt[3]{(q^2 + p^3)}]^{\frac{1}{3}} \equiv [-q - \sqrt[3]{(q^2 + p^3)}]^{\frac{2}{3}} + P - Q\sqrt[3]{(q^2 + p^3)} \pmod{\mu}.$$

Additionnant les congruences (1. et 3.), on trouve

$$x^2 \equiv 2P + [-q + \sqrt[3]{(q^2 + p^3)}]^{\frac{2}{3}} + [-q - \sqrt[3]{(q^2 + p^3)}]^{\frac{2}{3}} \pmod{\mu}.$$

Si l'on remarque d'autre part que l'on a :

$$x^2 \equiv -2p + [-q + \sqrt[3]{(q^2 + p^3)}]^{\frac{2}{3}} + [-q - \sqrt[3]{(q^2 + p^3)}]^{\frac{2}{3}} \pmod{\mu},$$

il en résultera

$$(4.) \quad P \equiv -p \pmod{\mu}.$$

Changeant dans la congruence (2.) le signe de  $\sqrt[3]{(q^2 + p^3)}$ , on a

$$[-q - \sqrt[3]{(q^2 + p^3)}]^{2n} \equiv P - Q\sqrt[3]{(q^2 + p^3)} \pmod{\mu}.$$

Cette congruence, multipliée par la congruence (2.), donne

$$P^2 - Q^2(q^2 + p^3) \equiv p^{6n} \equiv p^2 \pmod{\mu}:$$

congruence qui, en vertu de la relation (4.), fait voir que

$$Q \equiv 0 \pmod{\mu}.$$

La congruence (2.) peut donc être écrite :

$$[-q + \sqrt[3]{(q^2 + p^3)}]^{2n} \equiv -p \pmod{\mu};$$

ce qu'il fallait démontrer.

## §. 20.

**Théorème XI.** *Si le nombre premier  $\mu = 6n - 1$  est également de la forme  $18m + 11$ , et si la congruence proposée*

$$x^3 + 3px + 2q \equiv 0 \pmod{\mu},$$

*dans laquelle  $p$  et  $q$  sont tels que l'on a :*

$$(q^2 + p^3)^{\frac{1}{3}(\mu-1)} \equiv -1 \pmod{\mu},$$

*admet trois racines rationnelles : ces trois racines seront données par les formules :*

$$x' \equiv 2M\sqrt[3]{p^2} \pmod{\mu},$$

$$x'' \equiv -\sqrt[3]{p^2}[M + N\sqrt[3]{(-3(q^2 + p^3))}] \pmod{\mu},$$

$$x''' \equiv -\sqrt[3]{p^2}[M - N\sqrt[3]{(-3(q^2 + p^3))}] \pmod{\mu},$$

*$M$  et  $N$  représentant la partie rationnelle et le coefficient de  $\sqrt[3]{(q^2 + p^3)}$*

du développement de l'expression  $[-q + \sqrt{(q^2 + p^3)}]^{2m+1}$  par la formule du binôme.

Si l'on remarque qu'en vertu du lemme du paragraphe précédent on a :

$$[-q + \sqrt{(q^2 + p^3)}]^{2n} \equiv -p \pmod{\mu},$$

ce que l'on peut écrire sous la forme

$$[-q + \sqrt{(q^2 + p^3)}]^{2n-1} \equiv \frac{-p}{-q + \sqrt{(q^2 + p^3)}} \equiv \frac{-q - \sqrt{(q^2 + p^3)}}{p^2} \pmod{\mu},$$

et qu'en changeant le signe de  $\sqrt{(q^2 + p^3)}$ , on aura de même :

$$[-q - \sqrt{(q^2 + p^3)}]^{2n-1} \equiv \frac{-p}{-q - \sqrt{(q^2 + p^3)}} \equiv \frac{-q + \sqrt{(q^2 + p^3)}}{p^2} \pmod{\mu},$$

que par suite les valeurs de  $x$  :

$$x' \equiv [-q + \sqrt{(q^2 + p^3)}]^{\frac{1}{3}} + [-q - \sqrt{(q^2 + p^3)}]^{\frac{1}{3}} \pmod{\mu},$$

$$x'' \equiv [-q + \sqrt{(q^2 + p^3)}]^{\frac{1}{3}}(-\frac{1}{2} - \frac{1}{2}\sqrt{-3}) + [-q - \sqrt{(q^2 + p^3)}]^{\frac{1}{3}}(-\frac{1}{2} + \frac{1}{2}\sqrt{-3}) \pmod{\mu},$$

$$x''' \equiv [-q + \sqrt{(q^2 + p^3)}]^{\frac{1}{3}}(-\frac{1}{2} + \frac{1}{2}\sqrt{-3}) + [-q - \sqrt{(q^2 + p^3)}]^{\frac{1}{3}}(-\frac{1}{2} - \frac{1}{2}\sqrt{-3}) \pmod{\mu},$$

pourront être écrites sous la forme

$$(1.) \quad x' \equiv \sqrt[3]{p^2} \{ [-q - \sqrt{(q^2 + p^3)}]^{\frac{2}{3}(n-1)} + [-q + \sqrt{(q^2 + p^3)}]^{\frac{2}{3}(n-1)} \} \pmod{\mu},$$

$$(2.) \quad x'' \equiv \sqrt[3]{p^2} \{ [-q - \sqrt{(q^2 + p^3)}]^{\frac{2}{3}(n-1)}(-\frac{1}{2} - \frac{1}{2}\sqrt{-3}) \\ + [-q + \sqrt{(q^2 + p^3)}]^{\frac{2}{3}(n-1)}(-\frac{1}{2} + \frac{1}{2}\sqrt{-3}) \} \pmod{\mu},$$

$$(3.) \quad x''' \equiv \sqrt[3]{p^2} \{ [-q - \sqrt{(q^2 + p^3)}]^{\frac{2}{3}(n-1)}(-\frac{1}{2} + \frac{1}{2}\sqrt{-3}) \\ + [-q + \sqrt{(q^2 + p^3)}]^{\frac{2}{3}(n-1)}(-\frac{1}{2} - \frac{1}{2}\sqrt{-3}) \} \pmod{\mu};$$

en posant, pour abréger :

$$[-q + \sqrt{(q^2 + p^3)}]^{2m+1} \equiv M + N\sqrt{(q^2 + p^3)} \pmod{\mu},$$

d'où résulte

$$[-q - \sqrt{(q^2 + p^3)}]^{2m+1} \equiv M - N\sqrt{(q^2 + p^3)} \pmod{\mu};$$

et si l'on remarque que  $\mu$  étant de la forme  $18m + 11$ , on aura

$$\frac{2}{3}(n-1) = 2m + 1:$$

il en résultera :

$$x' \equiv 2M\sqrt[3]{p^2} \pmod{\mu},$$

$$x'' \equiv -\sqrt[3]{p^2} [M + N\sqrt{(-3(q^2 + p^3))}] \pmod{\mu},$$

$$x''' \equiv -\sqrt[3]{p^2} [M - N\sqrt{(-3(q^2 + p^3))}] \pmod{\mu}.$$

## §. 21.

**Théorème XII.** Si le nombre premier  $\mu = 6n - 1$  est également de la forme  $18m + 5$ , et si la congruence proposée,

$$x^3 + 3px + 2q \equiv 0 \pmod{\mu},$$

dans laquelle  $p$  et  $q$  sont tels que l'on a :

$$(q^2 + p^3)^{\frac{1}{3}(\mu-1)} \equiv -1 \pmod{\mu},$$

admet trois racines rationnelles : ces trois racines seront données par les formules :

$$x' \equiv \frac{-2q}{p(2\sqrt[3]{p^2.M-1})} \pmod{\mu},$$

$$x'' \equiv \frac{-q}{p(2\sqrt[3]{p^2.M-1})} + \frac{p^2(2\sqrt[3]{p^2.M-1})\sqrt{[-3(q^2+p^3)]}}{4q^2+p^3(2\sqrt[3]{p^2.M-1})^2} \pmod{\mu},$$

$$x''' \equiv \frac{-q}{p(2\sqrt[3]{p^2.M-1})} - \frac{p^2(2\sqrt[3]{p^2.M-1})\sqrt{[-3(q^2+p^3)]}}{4q^2+p^3(2\sqrt[3]{p^2.M-1})^2} \pmod{\mu};$$

$M$  représentant la partie rationnelle du développement de l'expression

$$[-q + \sqrt{(q^2 + p^3)}]^{2m}$$

par la formule du binôme.

Si nous remarquons qu'en vertu de l'égalité  $6n - 1 = 18m + 5$ , on a :

$$\frac{2}{3}(n-1) = 2m + \frac{1}{3},$$

la valeur de  $x'$ , donnée par la congruence (1.) du paragraphe précédent, pourra s'écrire :

$$x' \equiv \sqrt[3]{p^2} \cdot \{ [-q + \sqrt{(q^2 + p^3)}]^{2m} \sqrt[3]{[-q + \sqrt{(q^2 + p^3)}]} \\ + [-q - \sqrt{(q^2 + p^3)}]^{2m} \sqrt[3]{[-q - \sqrt{(q^2 + p^3)}]} \} \pmod{\mu}.$$

En faisant pour abrégé :

$$(1.) \quad [-q + \sqrt{(q^2 + p^3)}]^{2m} \equiv M + N\sqrt{(q^2 + p^3)} \pmod{\mu},$$

et en remarquant que

$$x' \equiv \sqrt[3]{p^2} [-q + \sqrt{(q^2 + p^3)}] + \sqrt[3]{p^2} [-q - \sqrt{(q^2 + p^3)}] \pmod{\mu},$$

on obtiendra :

$$x'[1 - \sqrt[3]{p^2}(M - N\sqrt{(q^2 + p^3)})] \equiv 2\sqrt[3]{p^2} \cdot N\sqrt{(q^2 + p^3)} \sqrt[3]{[-q + (q^2 + p^3)]} \pmod{\mu}.$$

Changeant dans cette congruence le signe de  $\sqrt{(q^2 + p^3)}$ , se qui n'altère pas

la valeur de  $x'$ , on trouve:

$$x' [1 - \sqrt[3]{p^2} (M + N \sqrt[3]{(q^2 + p^3)})] \equiv -2 \sqrt[3]{p^2} \cdot N \sqrt[3]{(q^2 + p^3)} \sqrt[3]{[-q - \sqrt[3]{(q^2 + p^3)}]} \pmod{\mu}.$$

Multipliant ces deux dernières congruences membre à membre, il en résulte:

$$(2.) \quad x'^2 [(1 - \sqrt[3]{p^2} \cdot M)^2 - p \sqrt[3]{p} \cdot N^2 (q^2 + p^3)] \equiv 4p^2 \sqrt[3]{p} \cdot N^2 (q^2 + p^3) \pmod{\mu}.$$

Changeant le signe de  $\sqrt[3]{(q^2 + p^3)}$  dans la congruence (1.), on a:

$$(3.) \quad [-q - \sqrt[3]{(q^2 + p^3)}]^{2m} \equiv M - N \sqrt[3]{(q^2 + p^3)} \pmod{\mu}.$$

Multipliant membre à membre les congruences (1. et 3.), on en déduit:

$$(4.) \quad M^2 - N^2 (q^2 + p^3) \equiv p^{6m} \pmod{\mu}.$$

Comme d'ailleurs en vertu du Théorème de *Fermat* on a:

$$p^{18m+4} \equiv 1 \pmod{\mu},$$

il en résultera:

$$p^{6m+2} \equiv \sqrt[3]{p^2} \pmod{\mu},$$

$$p^{6m+1} \equiv \frac{1}{\sqrt[3]{p}} \pmod{\mu}.$$

On pourra, au moyen de ces dernières congruences, donner à la congruence (2.) la forme très simple

$$x'^2 (1 - \sqrt[3]{p^2} \cdot M) \equiv -2p (1 - p \sqrt[3]{p} \cdot M^2) \pmod{\mu},$$

si l'on remarque que

$$1 - p \sqrt[3]{p} \cdot M^2 \equiv (1 - \sqrt[3]{p^2} \cdot M)(1 + \sqrt[3]{p} \cdot M) \pmod{\mu}.$$

En substituant cette valeur dans la congruence précédente, et en supprimant le facteur  $1 - \sqrt[3]{p^2} \cdot M$ , qui, comme nous allons le reconnaître, ne peut être congru à zéro, nous aurons:

$$x'^2 \equiv -2p (1 + \sqrt[3]{p^2} \cdot M) \pmod{\mu}.$$

Si l'on remarque que la congruence proposée donne

$$x' \equiv \frac{-2q}{x'^2 + 3p} \pmod{\mu},$$

il en résulte:

$$(5.) \quad x' \equiv \frac{2q}{p(2\sqrt[3]{p^2} \cdot M - 1)} \pmod{\mu}.$$

Les valeurs de  $x''$  et  $x'''$  se déduisent trop simplement de la connaissance de  $x'$ , pour qu'il soit nécessaire de nous y arrêter.

Pour compléter la démonstration de notre théorème, il nous reste à prouver que le facteur  $1 - \sqrt[3]{p^2} \cdot M$  ne peut dans aucun cas être congru à zéro.

En effet, en supposant

$$1 - \sqrt[3]{p^2} \cdot M \equiv 0 \pmod{\mu},$$

il en résultera :

$$M \equiv \frac{1}{\sqrt[3]{p^2}} \pmod{\mu}.$$

Cette valeur de  $M$ , mise dans la congruence (4.), donne

$$N \equiv 0 \pmod{\mu};$$

on aura donc en vertu de la congruence (1.):

$$(6.) \quad [-q + \sqrt[3]{(q^2 + p^3)}]^{2m} \equiv \frac{1}{\sqrt[3]{p^2}} \pmod{\mu}.$$

D'un autre côté le lemme du (§. 19.) donne

$$[-q + \sqrt[3]{(q^2 + p^3)}]^{6m+2} \equiv -p \pmod{\mu},$$

et de ces deux congruences on tire :

$$\sqrt[3]{(q^2 + p^3)} \equiv q \pmod{\mu};$$

congruence absurde, puisque le 1<sup>er</sup> membre est irrationnel, tandis que le second ne l'est pas.

## §. 22.

On pourrait craindre que la valeur de  $x'$ , donnée par la congruence (5.) du paragraphe précédent, ne devint illusoire, en ce que pour certaines valeurs de  $p$  et  $q$  son dénominateur deviendrait congru à zéro. Or il est facile de démontrer que si  $q$  n'est pas congru à zéro, il n'est pas possible que l'on ait:

$$2\sqrt[3]{p^2} \cdot M - 1 \equiv 0 \pmod{\mu}.$$

En effet, on déduit de cette congruence

$$M \equiv \frac{1}{2\sqrt[3]{p^2}} \pmod{\mu};$$

cette valeur de  $M$  mise dans la congruence (4.), donne

$$N\sqrt[3]{(q^2 + p^3)} \equiv \frac{\pm\sqrt{-3}}{2\sqrt[3]{p^2}} \pmod{\mu};$$

on aura donc en vertu de la congruence (1.):

$$[-q + \sqrt[3]{(q^2 + p^3)}]^{2m} \equiv \frac{1}{\sqrt[3]{p^2}} \left( \frac{1}{2} \pm \frac{1}{2} \sqrt{-3} \right) \pmod{\mu}.$$

Cette congruence, combinée avec la suivante :

$$[-q + \sqrt[3]{(q^2 + p^3)}]^{6m+2} \equiv -p \pmod{\mu},$$

donne

$$q\sqrt[3]{(q^2 + p^3)} \equiv q^2 \pmod{\mu}.$$

Comme par hypothèse  $q$  n'est pas congru à zéro, on a :

$$\sqrt[3]{(q^2 + p^3)} \equiv q \pmod{\mu}:$$

congruence absurde.

### §. 23.

Voici encore un théorème analogue au théorème précédent, et qu'on pourrait lui substituer pour la détermination des racines dans la congruence proposée, dans le cas particulier qui nous occupe.

**Théorème XIII.** *Si le nombre premier  $\mu = 6n - 1$  est également de la forme  $18m + 5$ , et si la congruence proposée*

$$x^3 + 3px + 2q \equiv 0 \pmod{\mu},$$

*dans laquelle  $p$  et  $q$  sont tels que l'on a :*

$$(q^2 + p^3)^{\frac{1}{3}(\mu-1)} \equiv -1 \pmod{\mu},$$

*admet trois racines rationnelles : ces racines seront données par les formules*

$$x' \equiv \frac{2M'}{\sqrt[3]{p}} \pmod{\mu},$$

$$x'' \equiv \frac{M'}{\sqrt[3]{p}} + \frac{\sqrt[3]{-3(q^2 + p^3)}\sqrt[3]{p^2}}{4M'^2 + p\sqrt[3]{p^2}} \pmod{\mu},$$

$$x''' \equiv \frac{M'}{\sqrt[3]{p}} - \frac{\sqrt[3]{-3(q^2 + p^3)}\sqrt[3]{p^2}}{4M'^2 + p\sqrt[3]{p^2}} \pmod{\mu};$$

*$M'$  représentant la partie rationnelle que l'on obtient en développant l'expression*

$$[-q + \sqrt[3]{(q^2 + p^3)}]^{2m+1}$$

*par la formule du binôme.*

Si nous remarquons qu'en vertu de l'égalité  $6n - 1 = 18m + 5$  on a :

$$2n = 6m + 2,$$

on pourra écrire la congruence

$$[-q + \sqrt[3]{(q^2 + p^3)}]^{2n} \equiv -p \pmod{\mu}$$

sous la forme

$$[-q + \sqrt[3]{(q^2 + p^3)}]^{6m+3} \equiv -p[-q + \sqrt[3]{(q^2 + p^3)}] \pmod{\mu}.$$

Extrayant la racine troisième des deux membres, et posant, pour abrégér :

$$[-q + \sqrt[3]{(q^2 + p^3)}]^{2m+1} \equiv M' + N' \sqrt[3]{(q^2 + p^3)} \pmod{\mu},$$

nous aurons l'une des congruences

$$(a.) \quad \begin{cases} M' + N' \sqrt[3]{(q^2 + p^3)} \equiv -\sqrt[3]{p}[-q + \sqrt[3]{(q^2 + p^3)}]^{\frac{1}{3}} \pmod{\mu}, \\ M' + N' \sqrt[3]{(q^2 + p^3)} \equiv -\sqrt[3]{p}[-q + \sqrt[3]{(q^2 + p^3)}]^{\frac{1}{3}}(-\frac{1}{2} + \frac{1}{2}\sqrt{-3}) \pmod{\mu}, \\ M' + N' \sqrt[3]{(q^2 + p^3)} \equiv -\sqrt[3]{p}[-q + \sqrt[3]{(q^2 + p^3)}]^{\frac{1}{3}}(-\frac{1}{2} - \frac{1}{2}\sqrt{-3}) \pmod{\mu}. \end{cases}$$

Quelle que ce soit de ces congruences qui soit satisfaite, on en déduira, en changeant le signe des radicaux :

$$(b.) \quad \begin{cases} M' - N' \sqrt[3]{(q^2 + p^3)} \equiv -\sqrt[3]{p}[-q - \sqrt[3]{(q^2 + p^3)}]^{\frac{1}{3}} \pmod{\mu}, \\ M' - N' \sqrt[3]{(q^2 + p^3)} \equiv -\sqrt[3]{p}[-q - \sqrt[3]{(q^2 + p^3)}]^{\frac{1}{3}}(-\frac{1}{2} - \frac{1}{2}\sqrt{-3}) \pmod{\mu}, \\ M' - N' \sqrt[3]{(q^2 + p^3)} \equiv -\sqrt[3]{p}[-q - \sqrt[3]{(q^2 + p^3)}]^{\frac{1}{3}}(-\frac{1}{2} + \frac{1}{2}\sqrt{-3}) \pmod{\mu}. \end{cases}$$

En additionnant celle des congruences (a.) qui est satisfaite, avec la congruence (b.) correspondante, le second membre ne sera autre chose que  $-\sqrt[3]{p}$ , multiplié par l'une des racines de la congruence proposée; en désignant cette racine par  $x'$ , nous aurons :

$$2M' \equiv -\sqrt[3]{p} \cdot x' \pmod{\mu},$$

et par conséquent

$$x' \equiv -\frac{2M'}{\sqrt[3]{p}} \pmod{\mu}.$$

On déduit aisément de là les valeurs de  $x''$  et  $x'''$ .

#### §. 24.

**Théorème. XIV.** *Si  $\mu$  est un nombre premier de la forme  $18m+5$ , et si  $p$  et  $q$  sont deux nombres tels que l'on ait :*

$$(q^2 + p^3)^{\frac{1}{3}(\mu-1)} \equiv -1 \pmod{\mu},$$

$$M_1 p^2 \equiv -q \pmod{\mu},$$

$M_1$  représentant la partie rationnelle du développement de l'expression  $[-q + \sqrt[3]{(q^2 + p^3)}]^{6m+1}$ , en désignant par  $M$  et  $M'$  les parties rationnelles des développements des expressions  $[-q + \sqrt[3]{(q^2 + p^3)}]^{2m}$  et  $[-q + \sqrt[3]{(q^2 + p^3)}]^{2m+1}$  : nous aurons la congruence

$$(1.) \quad M' \equiv \frac{q}{\sqrt[3]{p}(\sqrt[3]{p} - 2pM)} \pmod{\mu}.$$

Ce théorème serait évident si l'on admettait que les trois valeurs de  $x'$ ,  $x''$  et  $x'''$ , données dans le paragraphe précédent, soient respectivement égales aux trois valeurs  $x'$ ,  $x''$  et  $x'''$  obtenues dans le (§. 22.); car en égalant les valeurs de  $x'$ , on obtiendrait la congruence (1.); notre théorème aura donc l'avantage d'établir cette concordance.

Si nous considérons les congruences

$$\begin{aligned} [-q + \sqrt[3]{(q^2 + p^3)}]^{6m+2} &\equiv -p \pmod{\mu}, \\ [-q + \sqrt[3]{(q^2 + p^3)}]^{2m} &\equiv M + N\sqrt[3]{(q^2 + p^3)} \pmod{\mu}, \\ [-q + \sqrt[3]{(q^2 + p^3)}]^{2m+1} &\equiv M' + N'\sqrt[3]{(q^2 + p^3)} \pmod{\mu}, \end{aligned}$$

et si nous remarquons que:

$$\begin{aligned} M^2 - N^2(q^2 + p^3) &\equiv p^{6m} \equiv \frac{1}{p\sqrt[3]{p}} \pmod{\mu}, \\ M'^2 - N'^2(q^2 + p^3) &\equiv -p^{6m+3} \equiv -p^3\sqrt[3]{p^2} \pmod{\mu}, \end{aligned}$$

nous obtiendrons:

$[M'^2 + N'^2(q^2 + p^3) + 2M'N'\sqrt[3]{(q^2 + p^3)}][M + N\sqrt[3]{(q^2 + p^3)}] \equiv -p \pmod{\mu}$ :  
congruence qu'on peut décomposer dans les deux suivantes:

$$\begin{aligned} M'^2M + N'^2M(q^2 + p^3) + 2M'N'N(q^2 + p^3) &\equiv -p \pmod{\mu}, \\ M'^2N + N'^2N(q^2 + p^3) + 2M'N'M &\equiv 0 \pmod{\mu}. \end{aligned}$$

De ces deux congruences on tire:

$$(2.) \quad 2M'^2 + p^3\sqrt[3]{p^2} \equiv -p^2\sqrt[3]{p}M \pmod{\mu},$$

et mettant dans la congruence

$$x^3 + 3px + 2q \equiv 0 \pmod{\mu}$$

pour  $x$  sa valeur  $-\frac{2M'}{\sqrt[3]{p}}$ , on obtient:

$$(4.) \quad 4M'^3 + 3p^3\sqrt[3]{p^2}M' - pq \equiv 0 \pmod{\mu};$$

éliminant  $M'^2$  entre ces deux congruences (2. et 3.), on obtient la congruence (1.).

Genève, Octobre 1852.