Recherches arithmétiques.

Section Troisième

Des résidus des puissances.

45. Théorème. *Dans toute progression géométrique* $1, a, a^2, a^3$, *etc., outre le premier terme 1, il y en a encore un autre* a' *congru à l'unité suivant le module* p *premier avec* a, *l'exposant* t *étant* $< p$.

Puisque le module p est premier avec a, et par conséquent avec une puissance quelconque de a, aucun terme de la progression ne sera $\equiv 0$ (mod. p), mais chacun d'eux sera congru à quelqu'un des nombres $1, 2, 3, 4, ..., p-1$. Comme le nombre de ces derniers est $p-1$, il est évident que si l'on considère plus de $p-1$ termes de la progression, ils ne pourront pas avoir tous des résidus minima différents. Ainsi parmi les nombres $1, a, a^2, a^3, ..., a^{p-1}$, on en trouvera au moins deux congrus. Soit donc $a^m \equiv a^n$ et $m > n$, on aura, en divisant par a^n (n° 22), $a^{m-n} \equiv 1$, où $m - n < p$ et > 0.

Exemple. Dans la progression $1, 2, 4, 8$, etc. le premier terme qui est congru avec l'unité suivant le module 13, se trouve être $2^{12} = 4096$, mais suivant le module 23, on a dans la même progression, $2^{11} = 2048 \equiv 1$; de même $5^6 = 15625 \equiv 1$ (mod. 7) ; et $5^5 \equiv 3125 \equiv 1$ (mod. 11). Ainsi dans quelques cas la puissance de a congrue avec l'unité, est plus petite que a^{p-1}, et dans d'autres, il faut remonter jusqu'à la puissance $p-1$ elle-même.

46. Quand la progression est continuée au-delà du terme qui est congru à l'unité, on retrouvera les mêmes résidus qu'on avait à partir du commencement. Ainsi, soit $a^t \equiv 1$, on aura $a^{t+1} \equiv a$, $a^{t+2} \equiv a^2$, etc., jusqu'à ce qu'on parvienne au terme a^{2t}, dont le résidu minimum sera de nouveau 1, et la période des résidus recommencera. On aura ainsi une période de t résidus qui se répétera continuellement, et l'on ne pourra trouver un seul résidu qui ne fasse partie de cette période. On aura en général $a^{mt} \equiv 1$ et $a^{mt+n} \equiv a^n$; ce qui peut se présenter ainsi suivant notre notation : si $r \equiv \rho$ (mod. t), on aura $a^r \equiv a^\rho$ (mod. p).

47. Ce théorème fournit le moyen de trouver facilement les résidus des puissances, quelle que soit la grandeur de l'exposant dont elles sont affectées, en même temps qu'on découvrira la puissance congrue à l'unité. Si, par exemple, on demande le reste de la division de 3^{1000} par 13, comme $3^3 \equiv 1$ (mod. 13), on a $t = 3$, et comme d'ailleurs $1000 \equiv 1$ (mod. 3), on trouvera $3^{1000} \equiv 3$ (mod 13).

48. Si a^t est la plus petite puissance congrue à l'unité, (en exceptant $a^0 = 1$, cas que nous ne considérons pas), les t restes qui composent la période seront tous différents, comme on le voit sans difficulté par la démonstration du n° 45. Alors la proposition du n° 46 peut être renversée. Savoir, si $a^m \equiv a^n$ (mod. p), on aura $m \equiv n$ (mod. t) : car si m et n étaient incongrus suivant t, leurs résidus minima μ et ν seraient différents. Mais $a^\mu \equiv a^m$, $a^\nu \equiv a^n$; donc $a^\mu \equiv a^\nu$, c'est-à-dire, que

---

Transcription en LaTeX, ce format permettant des traductions aisées dans les multiples langues proposées par les outils de traduction automatique (ce que ne permet pas un document scanné).
Denise Vella-Chemla, mars 2024.

toutes les puissances au dessous de a^t ne seraient pas incongrues, ce qui est contre l'hypothèse.

Si donc $a^k \equiv 1 \pmod{p}$, on aura $k \equiv 0 \pmod{t}$, c'est-à-dire que k sera divisible par t.

Nous avons parlé jusqu'ici de modules quelconques, pourvu qu'ils fussent premiers avec a. À présent examinons à part les modules qui sont des nombres premiers absolus, et établissons sur ce fondement des recherches plus générales.

49. THÉORÈME. *Si p est un nombre premier qui ne divise pas a, et que a^t soit la plus petite puissance de a congrue à l'unité, l'exposant t sera $= p-1$, ou une partie aliquote de $p-1$.*

Voyez pour des exemples le n° 45.

Comme nous avons déjà prouvé que t est $= p-1$ ou $< p-1$, il reste à faire voir que dans le dernier cas il est toujours une partie aliquote de $p-1$.

1°. Rassemblons les résidus minima positifs de tous les termes, $1, a, a^2, a^3, ..., a^{t-1}$, et désignons-les par $\alpha, \alpha', \alpha''$, etc. de sorte qu'on ait $\alpha = 1, \alpha' \equiv a, \alpha'' \equiv a^2$, etc. il est visible qu'ils seront tous différents ; car si deux termes a^m, a^n donnaient les mêmes résidus, on aurait $a^{m-n} \equiv 1$ (en supposant $m > n$ et $m-n < t$) ; ce qui est absurde, puisque a^t est la plus petite puissance de a congrue à l'unité. Au reste tous les nombres $\alpha, \alpha', \alpha''$, etc. sont compris dans la série $1, 2, 3, 4, ..., p-1$, série qu'ils n'épuisent pas lorsque $t < p-1$. Nous désignerons par (A) la somme de tous ces résidus, et (A) comprendra un nombre t de termes.

2°. Prenons un nombre quelconque β, parmi ceux de la série $1, 2, 3, ..., p-1$ qui manquent dans (A). Multiplions β par $\alpha, \alpha', \alpha''$, etc. et nommons β, β', β'', etc. les résidus minima qui en proviendront, et qui seront aussi en nombre t. Ces résidus seront différents entre eux, et différeront des nombres $\alpha, \alpha', \alpha''$, etc. En effet, si la première assertion était fausse, on aurait $\beta a^m \equiv \beta a^n$, d'où l'on tire, en divisant par β, $a^m \equiv a^n$: ce qui est contre ce que nous venons de démontrer : si la dernière l'était, on aurait $\beta a^m \equiv a^n$; d'où, quand $n > m$, $\beta \equiv a^{n-m}$, c'est-à-dire que β serait congru à quelqu'un des nombres $\alpha, \alpha', \alpha''$, etc. : ce qui est contre l'hypothèse ; mais si $n < m$, on aura, en multipliant par a^{t-m}, $\beta a^t \equiv a^{t+m-n}$, ou, comme $a^t \equiv 1$, $\beta \equiv a^{t-(m-n)}$, d'où résulte la même absurdité. Désignons par (B) la somme des nombres β, β', β'', etc. qui sont en nombre t ; on aura déjà $2t$ nombres parmi ceux-ci $1, 2, 3, ..., p-1$. Donc si (A) et (B) épuisent cette série, on aura $t = \frac{p-1}{2}$.

3°. Mais s'il en manque quelques-uns, soit γ un de ceux-là. Multiplions $\alpha, \alpha', \alpha''$, etc. par γ, et soient $\gamma, \gamma', \gamma''$, etc. les résidus minima de ces produits, dont nous désignerons l'ensemble par (C) ; (C) comprendra t nombres pris dans la série $1, 2, 3, ..., p-1$ qui seront tous différents entre eux et non-compris dans (A) et (B). Les deux premières assertions se démontrent comme ci-dessus (2°) ; quant à la troisième, si l'on avait $\gamma a^m \equiv \beta a^n$, on en tirerait $\gamma \equiv \beta a^{n-m}$, ou $\gamma \equiv \beta a^{t-(m-n)}$, suivant que $m < n$ ou $> n$. Dans l'un ou l'autre cas γ serait congru à quelqu'un des nombres qui composent (B) ; ce qui serait contre l'hypothèse. On aura ainsi $3t$ nombres pris dans la série $1, 2, 3, ..., p-1$, et s'il n'en reste plus, $t = \frac{p-1}{3}$, conformément au théorème.

4°. Mais s'il en reste encore quelques-uns, on arrivera de même à une quatrième somme de

nombres (D), etc. ; et comme la série $1, 2, 3$, etc. $p-1$ est finie, on voit que l'on parviendra nécessairement à l'épuiser, et $p-1$ sera un multiple de t ; donc t sera une partie aliquote de $p-1$.

50. Puisque $\frac{p-1}{t}$ est un nombre entier, il suit qu'en élevant chaque membre de la congruence $a^t \equiv 1 \pmod{p}$ à la puissance $\frac{p-1}{t}$, on aura $a^{p-1} \equiv 1 \pmod{p}$; c'est-à-dire, que $a^{p-1}-1$ *sera toujours divisible par* p *quand* p *est premier et qu'il ne divise pas* a.

Ce théorème remarquable, tant par son élégance que par sa grande utilité, s'appelle ordinairement *théorème de Fermat*, du nom de l'inventeur. (*Fermatii opera Math. Tolosæ 1679. Fol. p. 163*) Fermat n'en a pas donné la démonstration, bien qu'il ait assuré qu'il l'avait trouvée. Euler en a le premier publié une dans la Dissertation intitulée : *Démonstration de quelques théorèmes relatifs aux nombres premiers.* (*Comm. Ac. Pétrop. T.* VIII)[1] ; elle est tirée du développement de $(a+1)^p$, qui fait voir par la forme des coefficients, que $(a+1)^p - a^p - 1$ est toujours divisible par p, et que par conséquent $(a+1)^p - (a+1)$ le sera si $a^p - a$ l'est. Or comme $1^p - 1$ est divisible par p, $2^p - 2$ le sera donc ; et partant $3^p - 3$, et généralement $a^p - a$. Donc si p ne divise pas a, on aura aussi $a^{p-1} - 1$ divisible par p. Ce que nous venons de dire suffit pour faire connaître l'esprit de la démonstration.

Lambert en a donné une semblable, (*Acta eruditorum.* 1769, p. 109). Mais comme le développement de la puissance d'un binôme semble étranger à la théorie des nombres, Euler (*Comm. nov. Petrop. T.* VIII, *p. 70*) donna une autre démonstration qui est conforme à celle que nous venons d'exposer. Dans la suite il s'en présentera encore d'autres : ici nous nous contenterons d'en donner encore une déduite du même principe que celle d'Euler. La proposition suivante, dont le théorème en question n'est qu'un cas particulier, nous sera utile pour d'autres recherches.

51. *Si* p *est un nombre premier, la puissance* p *du polynome* $a+b+c+\text{etc.}$ *est* $\equiv a^p + b^p + c^p + \text{etc.}$ *suivant le module* p.

On sait que $(a+b+c+\text{etc.})^p$ est composé de termes de la forme $Pa^\alpha b^\beta c^\gamma$ etc. où l'on a $\alpha+\beta+\gamma+$ etc.$= p$, P étant le nombre de permutations de p choses, dont α, β, γ, etc. sont respectivement égales à a, b, c, etc. Mais nous avons fait voir (n° 41) que ce nombre était toujours divisible par p, à moins que toutes les lettres ne fussent égales entre elles ; c'est-à-dire, à moins que l'un des nombres α, β, γ,etc. ne fût égal à p, et les autres égaux à zéro ; d'où il suit que tous les termes du développement, excepté a^p, b^p, etc. sont divisibles par p, et que par conséquent $(a+b+c+\text{etc.})^p \equiv a^p + b^p + c^p + \text{etc.} \pmod{p}$.

Si toutes les quantités a, b, c, etc. sont supposées $= 1$, et que leur nombre soit k, on aura $k^p \equiv k$, comme dans le n° précédent.

[1] Antérieurement (*Comm. Petr. T.* VI. *p. 106*) ce grand homme n'était pas parvenu encore au but. Dans la fameuse discussion entre Maupertuis et Konig, sur le principe de la moindre action, discussion qui les jeta dans des digressions étrangères, Konig assura qu'il avait entre les mains un manuscrit autographe de Leibniz, qui contenait une démonstration de ce théorème conforme à celle d'Euler (*Appel au Public* p. 106). Quoique nous ne voulions pas refuser de croire à ce témoignage, il est sûr cependant que Leibniz n'a jamais publié sa démonstration. (*Voyez Hist. de l'Acad. de Berlin. 1750. p. 530*).

52. Comme les nombres qui sont diviseurs de $p-1$ sont les seuls qui puissent servir d'exposants aux plus petites puissances congrues avec l'unité, on est porté à chercher si tous les diviseurs de $p-1$ jouissent de cette propriété ; et, quand on classe tous les nombres non divisibles par p suivant l'exposant de leur plus petite puissance congrue à l'unité, combien il y en a pour chaque exposant. Nous observerons d'abord qu'il suffit de considérer les nombres positifs depuis 1 jusqu'à $p-1$: il est évident en effet que les nombres congrus doivent être élevés à la même puissance pour devenir congrus à l'unité, et que par conséquent un nombre quelconque doit être rapporté au même exposant que son résidu minimum positif ; ainsi nous avons à rechercher comment les nombres $1, 2, 3, ..., p-1$, doivent être distribués sous ce point de vue, relativement aux facteurs de $p-1$. Pour abréger, si d est un des facteurs de $p-1$, entre lesquels on doit compter 1 et $p-1$, nous représenterons par ψd la multitude des nombres positifs plus petits que p, dont la puissance d est la plus petite qui soit congrue à l'unité.

53. Pour nous faire entendre plus facilement, nous présenterons d'abord un exemple. Soit $p = 19$, les nombres $1, 2, 3, ..., 18$ peuvent se distribuer de la manière suivante relativement aux diviseurs de 18 :

$$1\left\{1,\right. \quad 2\left\{18,\right. \quad 3\left\{\begin{array}{l}7\\11\end{array}\right., \quad 6\left\{\begin{array}{l}8\\12\end{array}\right., \quad 9\left\{\begin{array}{lll}4, & 5, & 6\\9, & 16, & 17\end{array}\right., \quad 18\left\{\begin{array}{lll}2, & 3, & 10\\13, & 14, & 15\end{array}\right..$$

Ainsi dans ce cas $\psi 1 = 1, \psi 2 = 1, \psi 3 = 2, \psi 6 = 2, \psi 9 = 6, \psi 18 = 6$. Avec une légère attention on voit qu'il y en a, relativement à chaque exposant, autant qu'il y a de nombres premiers avec cet exposant et non plus grands que lui, ou bien, en reprenant le signe du n° 40, que $\psi d = \varphi d$. Mais on peut démontrer généralement cette observation de la manière suivante :

1°. S'il y a un nombre a appartenant à l'exposant d, c'est-à-dire dont la puissance d soit congrue à l'unité, et les puissances inférieures incongrues, toutes les puissances de ce nombre, savoir $a, a^2, a^3, a^4, ..., a^d$, ou leurs résidus minima, auront leur puissance d congrue avec l'unité ; et comme cela peut s'exprimer en disant que les résidus minima des nombres $a, a^2, a^3, ..., a^d$ qui sont tous différents sont les racines de la congruence $x^d \equiv 1$, qui ne peut avoir plus de d racines différentes, il est évident qu'il n'y a pas de nombres autres que les résidus minima de $a, a^2, a^3, ..., a^d$, dont les puissances d soient congrues à l'unité ; d'où il suit que les nombres appartenant à l'exposant d se trouvent tous entre les résidus minima des nombres $a, a^2, a^3, ..., a^d$. On déterminera comme il suit quels ils sont et quel est leur nombre. Si k est un nombre premier avec d, toutes les puissances de a^k, dont les exposants sont $< d$, ne seront pas congrues à l'unité. Soit en effet $\frac{1}{k} \pmod{d} = m$ (voyez n° 31), on aura $a^{km} \equiv a$; donc si la puissancee e de a^k était congrue à l'unité, et que l'on eût $e < d$, on aurait aussi $a^{kme} \equiv 1$, et par conséquent $a^e \equiv 1$; ce qui est contre l'hypothèse. Il est évident, d'après cela, que le résidu minimum de a^k appartiendra à d ; mais si k a un commun diviseur δ avec d, le résidu minimum de a^k n'appartiendra pas à l'exposant d. Car $\frac{kd}{\delta}$ est divisible par d, ou bien $\frac{kd}{\delta} \equiv 0 \pmod{d}$; par conséquent $a^{\frac{kd}{\delta}} \equiv 1$; c'est-à-dire $(a^k)^{\frac{d}{\delta}} \equiv 1$. Nous conclurons de là qu'il y a autant de nombres appartenant à l'exposant d, qu'il y a de nombres premiers avec d dans la série $1, 2, 3, ..., d$. Mais il faut se souvenir que cette conclusion suppose qu'il existe déjà un nombre a appartenant à l'exposant d ; par conséquent il reste douteux s'il ne pourrait pas se faire qu'aucun nombre n'appartînt à un exposant donné, et la conclusion se réduit à $\psi d = 0$, ou $= \varphi d$.

54. 2°. Soient d, d', d'', etc. les diviseurs de $p-1$; comme tous les nombres $1, 2, 3, ..., p-1$ doivent être distribués entre ces diviseurs, on aura $\psi d + \psi d' + \psi d'' + \text{etc.} = p-1$. Mais (n° 40) nous avons démontré que $\varphi d + \varphi d' + \varphi d'' + \text{etc.} = p-1$, et du n° précédent il suit que $\psi d = 0$ ou $= \varphi d$; et par conséquent que ψd ne peut pas être $> \varphi d$; ce qui s'étend à $\psi d'$ et $\varphi d'$, etc. Si donc un ou plusieurs des nombres $\psi d, \psi d'$, etc. étaient plus petits que son correspondant parmi les nombres $\varphi d, \varphi d'$, etc., la somme des premiers ne pourrait être égale à la somme des derniers. D'où nous concluons enfin que dans tous les cas, $\psi d = \varphi d$, et que par conséquent ψd ne dépend point de la grandeur de $p-1$.

55. Il y a un cas particulier de la proposition précédente qui mérite de fixer notre attention ; le voici : *il existe toujours des nombres dont aucune puissance plus petite que* $p-1$ *n'est congrue à l'unité* ; il y en a même autant entre 1 et $p-1$, qu'il y a au-dessous de $p-1$ de nombres qui lui soient premiers. Comme il s'en faut bien que la démonstration de ce théorème soit aussi évidente qu'elle le paraît d'abord, nous en donnerons une un peu différente de celle qui précède, d'autant plus que la diversité des méthodes aide beaucoup à jeter du jour sur les points les plus obscurs.

On décomposera $p-1$ en facteurs premiers, de manière qu'on ait $p-1 = a^\alpha b^\beta c^\gamma$ etc. a, b, c, etc. étant des nombres premiers inégaux. Alors nous composerons la démonstration des deux propositions suivantes :

1°. On peut toujours trouver un nombre A, ou plusieurs appartenant à l'exposant a^α, et de même des nombres B, C, etc. appartenant aux exposants b^β, c^γ, etc.

2°. Le produit des nombres A, B, C, etc. ou le résidu minimum de ce produit appartiendra à l'exposant $p-1$; ce qui se démontre ainsi qu'il suit.

1º. Soit g un des nombres $1, 2, 3, ..., p-1$ qui ne satisfasse pas à la congruence $x^{\frac{p-1}{a}} \equiv 1 \pmod{p}$; car tous les nombres ne peuvent pas satisfaire à cette congruence, dont le degré est $< p-1$. Alors je dis que si l'on fait $g^{\frac{p-1}{a^\alpha}} \equiv h$, h ou son résidu minimum appartiendra à l'exposant a^α.

En effet il est évident que $h^{a^\alpha} \equiv g^{p-1} \equiv 1$; mais $h^{a^{\alpha-1}} \equiv g^{\frac{p-1}{a}}$, et par conséquent sera incongru à l'unité, et à plus forte raison les puissances $h^{a^{\alpha-2}}, h^{a^{\alpha-3}}$ le seront aussi. Or l'exposant de la plus petite puissance de h congrue à l'unité, c'est-à-dire l'exposant auquel h appartient, doit être un diviseur de a^α (n° 48) ; et comme a^α n'est divisible que par lui-même, ou par les puissances inférieures de a, il s'ensuit nécessairement que a^α sera l'exposant auquel b appartient. On démontrera de la même manière, qu'on peut trouver des nombres appartenant aux exposants b^β, c^γ, etc.

2°. Si nous supposons que le produit de tous les nombres A, B, C, etc. n'appartienne pas à l'exposant $p-1$, etc., mais à un exposant t plus petit, t devra être un des diviseurs de $p-1$ (n° 48), ou $\frac{p-1}{t}$ sera un entier > 1. Il suit de là que ce quotient sera un des nombres premiers a, b, c, etc., ou du moins qu'il sera divisible par quelqu'un d'eux (n° 17), par a, par exemple, car le raisonnement est le même pour les autres. t divisera ainsi $\frac{p-1}{a}$; donc le produit ABC etc. serait encore congru à l'unité, en l'élevant à la puissance $\frac{p-1}{a}$ (n° 46). Mais il est évident que tous les nombres, B, C, D, etc. (excepté A) deviennent congrus à l'unité, si on les élève à la puissance $\frac{p-1}{a}$ puisque les exposants auxquels ils appartiennent b^β, c^γ, etc. divisent $\frac{p-1}{a}$. Donc $A^{\frac{p-1}{a}}.B^{\frac{p-1}{a}}.C^{\frac{p-1}{a}}$. etc.$\equiv A^{\frac{p-1}{a}} \equiv 1$; donc

a^α doit diviser $\frac{p-1}{a}$ (n° 48), c'est-à-dire que $\frac{p-1}{a^{\alpha+1}}$ doit être entier, ce qui est absurde (n° 15). Donc enfin notre supposition ne peut subsister, c'est-à-dire que le produit ABC etc. appartient réellement à l'exposant $p-1$.

La dernière démonstration semble un peu plus longue que la première, mais elle est plus directe.

56. Ce théorème nous fournit un exemple remarquable de la circonspection dont on a besoin dans la théorie des nombres, pour ne pas regarder comme démontrées des choses qui ne le sont pas. LAMBERT, dans la Dissertation que nous avons citée plus haut, fait mention de cette proposition, mais ne dit pas un mot de la nécessité de la démontrer. Personne même n'a tenté de le faire, excepté EULER (*Comm. nov. Ac. Pétrop. T.* XVIII, *p. 85*), dans son Mémoire intitulé : *Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia.* On peut voir surtout l'art. 37, dans lequel il a parlé avec étendue de la nécessité de démontrer cette proposition. Cependant la démonstration de cet homme pénétrant présente deux défauts ; l'un tient à ce qu'il suppose tacitement, art. 31 et suivants, que la congruence $x^n \equiv 1$, (en ramenant ses raisonnements à notre notation) a réellement n racines différentes, tandis qu'il était seulement démontré que cette congruence ne peut en avoir davantage ; l'autre, à ce qu'il ne déduit que par induction la formule du n° 34.

57. Nous nommerons avec EULER, *racines primitives* les nombres qui appartiennent à l'exposant $p-1$. Si donc a est une racine primitive, tous les résidus minima des puissances $a, a^2, a^3, ..., a^{p-1}$ seront différents ; d'où l'on déduit facilement qu'ils se trouvent tous parmi les nombres $1, 2, 3, ..., p-1$ qui sont en même nombre qu'eux, c'est-à-dire que tout nombre non divisible par p est congru à quelque puissance de a. Cette propriété remarquable est d'une bien grande utilité, et peut considérablement abréger les opérations arithmétiques relatives aux congruences, à peu près de la même manière que l'introduction des logarithmes dans l'arithmétique ordinaire en abrège les opérations. Nous prendrons arbitrairement pour *base* une racine primitive a, à laquelle nous rapporterons tous les nombres non divisibles par p ; et si on a $a^e \equiv b \pmod{p}$, nous appellerons e l'*indice* de b. Par exemple, 2 est une racine primitive suivant le module 19 ; si on la prend pour base,

aux nombres	1,	2,	3,	4,	5,	6,	7,	8,	9,	10,	11,	12,	13,	14,	15,	16,	17,	18
répondront les indices	0,	1,	13,	2,	16,	14,	6,	3,	8,	17,	12,	15,	5,	7,	11,	4,	10,	9.

Au reste il est évident que pour la même base chaque nombre a plusieurs indices, mais qui seront tous congrus suivant le module $p-1$; aussi quand il sera question d'indices, ceux qui seront congrus suivant le module $p-1$, seront regardés comme équivalents, de même que les nombres sont regardés comme équivalents lorsqu'ils sont congrus suivant le module p.

58. Les théorèmes qui regardent les indices sont absolument analogues à ceux qui regardent les logarithmes.

L'indice d'un produit de tant de facteurs qu'on voudra, est congru à la somme des indices des différents facteurs, suivant le module $p-1$.

L'indice de la puissance d'un nombre est congru, suivant le module $p-1$, *au produit de l'exposant*

par l'indice du nombre donné.

Nous omettons les démonstrations à cause de leur simplicité.

On voit par là que si nous voulions construire une table qui donnât les indices de tous les nombres pour différents modules, nous pourrions nous dispenser de tenir compte de tous les nombres plus grands que le module et de tous les nombres composés. On trouvera à la fin de cet ouvrage un essai de cette table (Tab. I). Dans la première colonne sont rangés les nombres premiers et les puissances de nombres premiers depuis 3 jusqu'à 97, qui doivent être regardés comme des modules : à côté de chacun d'eux, dans la colonne suivante, les nombres pris pour bases ; suivent alors les indices des nombres premiers successifs, qui sont écrits par tranches composées de cinq chacune ; en tête se trouvent les nombres premiers disposés dans le même ordre. De sorte qu'on peut trouver facilement l'indice qui répond à un nombre premier donné, suivant un module donné.

Soit par exemple $p = 67$; l'indice de 60, en prenant 12 pour base, sera

$$\equiv 2 \text{ Ind. } 2 + \text{Ind. } 3 + \text{Ind. } 5 \text{ (mod. } 66) \equiv 58 + 9 + 39 \equiv 40.$$

59. L'indice de la valeur d'une expression quelconque $\frac{a}{b}$ (mod. p), (n° 31) est congru suivant le module $p - 1$, à la différence des indices du numérateur a et du dénominateur b, pourvu que les nombres a et b ne soient pas divisibles par p.

Soit en effet c une valeur quelconque de cette expression, on aura $bc \equiv a$ (mod. p) ; donc Ind. b + Ind. $c \equiv$ Ind. a (mod. $p - 1$), et

$$\text{Ind. } c \equiv \text{Ind. } a - \text{Ind. } b.$$

Si donc on a deux tables, dont l'une donne les indices qui répondent à chaque nombre pour un module quelconque, et dont l'autre donne les nombres qui répondent à des indices donnés, on pourra résoudre facilement toutes les congruences du premier degré, puisqu'on peut toujours les ramener à d'autres dont les modules soient premiers (n° 30).

Soit par exemple la congruence $29x + 7 \equiv 0$ (mod. 47), on aura $x \equiv \frac{-7}{29}$ (mod. 47).

De là [2]

$$\text{Ind. } x \equiv \text{Ind. } -7 - \text{Ind. } 29 \equiv \text{Ind. } 40 - \text{Ind. } 29 \equiv 15 - 43 \equiv 18 \text{ (mod. } 46);$$

or 3 est le nombre qui a pour indice 18 ; donc $x \equiv 3$ (mod. 47). Nous n'avons point ajouté la seconde table, mais on verra dans la section VI comment on peut la remplacer par une autre.

60. De même que dans le n° 31 nous avons désigné par un signe particulier, les racines des congruences du premier degré, dans ce qui va suivre, nous représenterons par un autre signe les racines des congruences à deux termes des degrés supérieurs ; et comme $\sqrt[n]{A}$ ne signifie autre chose que la racine de l'équation $x^n = A$; en ajoutant le module, $\sqrt[n]{A}$ (mod. p) représentera une racine quelconque de la congruence $x^n \equiv A$ (mod. p). Ainsi nous dirons que l'expression $\sqrt[n]{A}$ (mod. p) a autant de valeurs qu'elle en a d'incongrues suivant p ; car toutes celles qui sont congrues suivant p

[2] *Note de la transcriptrice : Gauss a pris 10 comme base.*

doivent être regardées comme équivalentes (n° 26). Au reste il est clair que si A et B sont congrus suivant p, les expressions $\sqrt[n]{A}$ (mod. p), $\sqrt[n]{B}$ (mod. p) seront équivalentes.

Maintenant si l'on fait $\sqrt[n]{A} \equiv x$ (mod. p), on aura

$$n \text{ Ind. } x \equiv \text{Ind. } A \text{ (mod. } p-1).$$

On déduit de cette congruence, d'après les règles de la section II, les valeurs de Ind. x, et de là les valeurs correspondantes de x ; mais on voit facilement que x a autant de valeurs qu'il y a de racines dans la congruence

$$n \text{ Ind. } x \equiv \text{Ind. } A \text{ (mod. } p-1);$$

donc $\sqrt[n]{A}$ n'aura qu'une valeur, quand n sera premier avec $p-1$; mais lorsque n et $p-1$, auront un commun diviseur, et que δ sera le plus grand, Ind. x aura δ valeurs incongrues suivant $p-1$, et par conséquent $\sqrt[n]{A}$ aura autant de valeurs incongrues suivant p, pourvu que Ind. A soit divisible par δ. Sans cette condition, $\sqrt[n]{A}$ n'aurait aucune valeur réelle.

Si l'on cherche par exemple les valeurs de l'expression $\sqrt[15]{11}$ (mod. 19), il faut résoudre la congruence 15 Ind. $x \equiv$ Ind. $11 \equiv 6$ (mod. 18) on trouvera [3] trois valeurs de Ind. $x \equiv 4, 10, 16$ (mod. 18), d'où il résulte $x \equiv 6, 9, 4$.

61. Quoique cette méthode soit très expéditive, quand on a les tables nécessaires, nous ne devons cependant pas oublier qu'elle est indirecte ; il sera donc utile de chercher ce que peuvent donner les méthodes directes. Nous allons exposer ici les observations que l'on peut déduire des notions précédentes ; quant à ce qui exige des considérations plus profondes, nous le réserverons pour la section VIII [4].

Nous commencerons par le cas le plus simple ; celui où $A = 1$, c'est-à-dire, dans lequel on cherche les racines de la congruence $x^n \equiv 1$ (mod. p). En prenant pour base une racine primitive quelconque, on doit avoir n Ind. $x = 0$ (mod. $p-1$). Quand n est premier avec $p-1$, cette congruence n'aura qu'une seule racine, savoir

$$\text{Ind. } x \equiv 0 \text{ (mod. } p-1) ;$$

donc, dans ce cas $\sqrt[n]{1}$ (mod. p) n'aura qu'une valeur $x \equiv 1$ (mod. p) ; mais quand n et $p-1$ ont δ pour plus grand diviseur commun, la solution complète de la congruence n Ind. $x \equiv 0$ (mod. $p-1$) sera $x \equiv 0$ (mod. $\frac{p-1}{\delta}$) (n° 30), c'est-à-dire, que Ind. x devra être congru suivant le module $p-1$ à quelqu'un des nombres $0, \frac{p-1}{\delta}, \frac{2(p-1)}{\delta}, \ldots, \frac{(\delta-1)(p-1)}{\delta}$, ou qu'il aura δ valeurs incongrues suivant le module $p-1$; donc aussi, dans ce cas, x aura δ valeurs incongrues suivant p. On voit aussi que l'expression $\sqrt[\delta]{1}$ (mod. p) a aussi δ valeurs dont les indices sont absolument les mêmes que les précédents ; donc l'expression $\sqrt[\delta]{1}$ (mod. p) est tout-à-fait équivalente à l'expression $\sqrt[n]{1}$ (mod. p), ou ce qui revient au même, la congruence $x^\delta \equiv 1$ (mod. p) et la congruence $x^n \equiv 1$ (mod. p) ont les mêmes racines ; mais la première est d'un degré inférieur à moins qu'on n'ait $\delta = n$.

Ex. $\sqrt[15]{1}$ (mod. 19) a trois valeurs, parce que 3 est le plus grand commun diviseur de 15 et 18 ; elles seront également celles de l'expression $\sqrt[3]{1}$ (mod. 19). Ces valeurs sont 1, 7, 11.

[3] *Note de la transcriptrice : Gauss a à nouveau pris comme base 10.*

[4] *Note de la transcriptrice : Il n'y a pas de Section* VIII *dans les Recherches arithmétiques.*

62. Cette réduction nous offre un grand avantage, puisqu'on n'a plus besoin de résoudre parmi les congruences de la forme $x^n \equiv 1 \pmod{p}$ que celles où n est diviseur du module diminué de l'unité. Mais nous ferons voir plus bas que les congruences de cette forme peuvent encore s'abaisser davantage, quoique ce qui précède ne suffise pas pour cela. Il y a cependant un cas que nous pouvons traiter ici à fond, celui où $n = 2$. Il est évident en effet que les valeurs de l'expression $\sqrt[n]{1} \pmod{p}$ seront $+1$ et -1, puisqu'elle n'en peut avoir plus de deux, et que $+1$ et -1 sont incongrus, à moins que le module ne soit $= 2$, cas auquel il est clair que $\sqrt{2}$ n'aurait qu'une seule valeur. Il suit de là que $+1$ et -1 sont aussi les valeurs de l'expression $\sqrt[2m]{1} \pmod{p}$, quand m est premier avec $\frac{p-1}{2}$, ce qui arrivera toujours lorsque le module sera tel que $\frac{p-1}{2}$ soit un nombre absolument premier ; par exemple, quand $p = 3, 5, 7, 11, 23$, etc., à moins que $p - 1 = 2m$, cas auquel tous les nombres $1, 2, 3, ..., p-1$ sont racines. Remarquons, comme conséquence, que l'indice de -1 est toujours $\equiv \frac{p-1}{2} \pmod{p-1}$, quelle que soit la racine primitive que l'on prenne pour base ; car $2 \text{ Ind. } (-1) \equiv 0 \pmod{p-1}$; donc $\text{Ind. } (-1)$ sera $\equiv 0$ ou $\equiv \frac{p-1}{2}$ mais 0 est toujours l'indice de $+1$, et $+1$ et -1 doivent avoir des indices différents, excepté dans le cas où $p = 2$, qu'il n'est pas nécessaire de considérer.

63. Nous avons fait voir (n° 61) que l'expression $\sqrt[n]{A} \pmod{p}$ a δ valeurs différentes ou n'en a absolument aucune, si δ est le plus grand commun diviseur des nombres n et $p - 1$. Or de même que nous avons trouvé que $\sqrt[n]{A}$ et $\sqrt[\delta]{A}$ étaient équivalentes quand on a $A \equiv 1$, nous prouverons plus généralement que l'expression $\sqrt[n]{A}$ peut toujours être ramenée à une autre $\sqrt[\delta]{B}$, à laquelle elle est équivalente. Soit en effet $x^n = A$, et t une valeur quelconque de l'expression $\frac{\delta}{n} \pmod{p-1}$ qui aura toujours (n° 31) des valeurs réelles. De la congruence $x^n \equiv A$ on déduit $x^{tn} \equiv A^t$; mais à cause de $tn \equiv \delta \pmod{p-1}$, $x^{tn} \equiv x^\delta$; donc $x^\delta \equiv A^t$. Ainsi une valeur quelconque de $\sqrt[n]{A}$ sera aussi une valeur de $\sqrt[\delta]{A^t}$; et toutes les fois que $\sqrt[n]{A}$ aura des valeurs réelles, elle sera absolument équivalente à l'expression $\sqrt[\delta]{A^t}$, puisqu'elle ne peut avoir de valeurs différentes, ni en moindre nombre. Il est vrai cependant que $\sqrt[\delta]{A^t}$ peut avoir des valeurs réelles, sans que pour cela $\sqrt[n]{A}$ en ait nécessairement.

Exemple. Si l'on cherche les valeurs de l'expression $\sqrt[21]{2} \pmod{31}$, le plus grand commun diviseur des nombres 21 et 30 est 3, et 3 est une valeur de $\frac{3}{21} \pmod{30}$; donc si $\sqrt[21]{2}$ a des valeurs réelles, elle équivaudra à l'expression $\sqrt[3]{2^3}$ ou $\sqrt[3]{8}$; ou on trouve effectivement que les valeurs de la dernière qui sont 2, 10 et 19, satisfont aussi à la première.

64. Mais afin de ne pas entreprendre inutilement cette opération, il est nécessaire de chercher le caractère auquel on pourra reconnaître si $\sqrt[n]{A}$ admet ou non des valeurs réelles. Si on a une table d'indices la chose est facile, car (n° 60) $\sqrt[n]{A}$ aura des valeurs réelles quand $\text{Ind. } A$ sera divisible par δ, en prenant pour base une racine primitive quelconque, et dans le cas contraire elle n'en aura pas ; mais on peut aussi le découvrir sans le secours de cette table. Soit en effet $k = \text{Ind. } A$, si k est divisible par δ, $\frac{k(p-1)}{\delta}$ sera divisible par $p - 1$ et réciproquement ; mais l'indice du nombre $A^{\frac{p-1}{\delta}}$ est $\frac{k(p-1)}{\delta}$; donc si $\sqrt[n]{A} \pmod{p}$ a des valeurs réelles, $A^{\frac{p-1}{\delta}}$ sera congru à l'unité ; sinon, il sera incongru. Ainsi dans l'exemple de l'article précédent, on a $2^{10} = 1024 \equiv 1 \pmod{31}$, d'où l'on conclut que l'expression $\sqrt[21]{2} \pmod{31}$ a des valeurs réelles. De même nous voyons par là que $\sqrt[2]{-1} \pmod{p}$ a toujours deux valeurs réelles, quand p est de la forme $4m + 1$, et n'en a aucune quand p est de la forme $4m + 3$, car $(-1)^{2m} = 1$ et $(-1)^{2m+1} = -1$. Ce théorème élégant qui s'énonce ordinairement ainsi : *Si p est un nombre premier de la forme $4m + 1$, on peut trouver un carré a^2 qui rende $a^2 + 1$ divisible par p ; mais si p est de la forme $4m - 1$, on ne le pourra pas*, a

été démontré de cette manière par EULER (*Comment. nov. Ac. Petrop. T.* XVIII, *p.* 112, 1773). Il en avait donné une autre démonstration bien antérieurement (*Comm. nov. T.* V, *p.* 5, 1760) ; dans une première dissertation (*T.* IV, *p. 25*), il n'était pas encore parvenu au but. LAGRANGE a depuis donné aussi une démonstration de ce théorème (*Nouv. Mém. de l'Ac. de Berlin. 1775, p. 342*). Nous en exposerons encore une différente dans la section suivante, qui sera consacrée à ce genre de considérations.

65. Après avoir examiné comment on peut réduire toutes les expressions $\sqrt[n]{A} \pmod{p}$ à d'autres dans lesquelles n soit diviseur de $p-1$, et après avoir trouvé le caractère auquel on reconnaît s'il y a des racines réelles ou non, considérons avec plus de soin les expressions $\sqrt[n]{A} \pmod{p}$, dans lesquelles n est diviseur de $p-1$. Nous ferons voir d'abord quelle est la relation qu'ont entre elles les différentes valeurs de cette expression, ensuite nous indiquerons quelques artifices au moyen desquels on peut le plus souvent trouver une des valeurs.

1°. Quand $A \equiv 1$, et que r sera une des valeurs de l'expression $\sqrt[n]{1} \pmod{p}$, ou que $r^n \equiv 1 \pmod{p}$, toutes les puissances de r seront aussi des valeurs de cette expression ; et il y en aura autant de différentes qu'il y a d'unités dans l'exposant auquel r appartient (n° 48). Si donc r est une valeur appartenant à l'exposant n, les puissances $r, r^2, r^3, r^4, ..., r^n$ (où l'unité peut remplacer la dernière) renfermeront toutes les valeurs de l'expression $\sqrt[n]{1} \pmod{p}$. Nous expliquerons plus en détail dans la section VIII [5] comment on peut trouver ces valeurs qui appartiennent à l'exposant n.

2°. Quand A est incongru à l'unité, et que l'on connaît une valeur z de l'expression $\sqrt[n]{A} \pmod{p}$, on trouve les autres de la manière suivante : soient $1, r, r^2, r^3, ..., r^{n-1}$ les valeurs de $\sqrt[n]{1}$, on aura $z, zr, zr^2, zr^3, ..., zr^{n-1}$ pour les valeurs de $\sqrt[n]{A}$; car il est évident que tous ces nombres satisferont à la congruence $x^n \equiv A$; puisqu'en effet, si zr^k est un des nombres de la suite, comme $r^k \equiv 1$ et que $z^n \equiv A$, on aura $r^{nk} \equiv 1$, et partant $z^n r^{nk} = (zr^k)^n \equiv A$. Il est aisé de juger que toutes ces valeurs sont différentes (n° 23) ; donc l'expression $\sqrt[n]{A}$ ne peut avoir d'autres valeurs, puisqu'elle ne peut en avoir plus de n. Par exemple, si une valeur de $\sqrt[n]{A}$ est z, l'autre sera $-z$. On doit conclure de ce qui précède, que l'on ne peut trouver toutes les valeurs de $\sqrt[n]{A}$, à moins qu'on ne puisse avoir toutes celles de $\sqrt[n]{1}$.

66. La seconde recherche que nous nous étions proposée, consiste à déterminer le cas où l'on peut trouver directement une valeur de l'expression $\sqrt[n]{A} \pmod{p}$, dans laquelle n est diviseur de $p-1$. Cela arrive quand il y a une valeur congrue à une puissance de A, et comme ce cas est très fréquent, il ne sera pas déplacé de s'y arrêter un instant. Soit z cette valeur, si elle existe, on aura $z \equiv A^k$ et $z^n \equiv A \pmod{p}$; donc $A \equiv A^{kn}$; et si l'on peut déterminer k de manière que cette condition soit remplie, A^k sera la valeur cherchée ; mais la condition précédente revient à celle-ci $kn \equiv 1 \pmod{t}$, t étant l'exposant auquel A appartient. Or pour que cette congruence soit possible, il faut que n soit premier avec t, et dans ce cas on aura $k = \frac{1}{n} \pmod{t}$; si au contraire t et n ont un diviseur commun, aucune valeur de z ne sera congrue à une puissance de A.

67. Mais comme il est nécessaire pour cette solution de connaître t, voyons comment il faut procéder quand on ne le connaît pas. On voit d'abord facilement que t doit être diviseur de $\frac{p-1}{n}$ lorsque $\sqrt[n]{A} \pmod{p}$ a des valeurs réelles, ce que nous supposons ici. Soit en effet y l'une quelconque de ces valeurs, on aura (n° 50) $y^{p-1} \equiv 1$, et $y^n \equiv A \pmod{p}$; en élevant à la puissance $\frac{p-1}{n}$

[5] *voir note de la transcriptrice pour la section 61.*

les deux membres de la congruence $y^n \equiv A$, on aura $y^{p-1} \equiv A^{\frac{p-1}{n}} \equiv 1$; d'ailleurs $A^t \equiv 1$; donc $\frac{p-1}{n} \equiv 0 \pmod{t}$ (n° 48). Or si $\frac{p-1}{n}$ est premier avec n, la congruence $kn \equiv 1$ pourra être résolue suivant le module $\frac{p-1}{n}$, et toute valeur de k qui y satisfera suivant ce module, y satisfera aussi (n° 5) suivant le module t diviseur de $\frac{p-1}{n}$; donc on trouvera alors ce qu'on cherchait. Si $\frac{p-1}{n}$ n'est pas premier avec n, soit q le produit des facteurs premiers de $\frac{p-1}{n}$ qui divisent en même temps n ; $\frac{p-1}{nq}$ sera premier avec n, et si la condition que t soit premier avec n a lieu, t sera aussi premier avec q, et comme il divise $\frac{p-1}{n}$, il divisera donc $\frac{p-1}{nq}$; ainsi en résolvant la congruence $kn \equiv 1 \pmod{\frac{p-1}{nq}}$, ce qui peut se faire puisque n est premier avec $\frac{p-1}{nq}$, la valeur de k satisfera aussi à la congruence, suivant le module t. Tout l'artifice consiste à trouver un nombre qui puisse remplacer t, que nous ne connaissons pas ; mais il faut se souvenir que dans le cas où $\frac{p-1}{n}$ n'est pas premier avec n, nous avons supposé n premier avec t ; et si cette condition manque, toutes les conclusions sont fausses ; c'est pourquoi, si en suivant témérairement les règles, on trouve pour z une valeur dont la puissance n ne soit pas congrue à A ; le résultat prouvera que cette condition n'a pas lieu, et que partant la méthode n'est pas applicable.

68. Mais dans ce cas même, il est souvent avantageux de faire cette recherche : elle offre l'avantage de faire trouver de vraies valeurs au moyen des fausses. Supposons en effet que les nombres k et z aient été convenablement déterminés, mais qu'on n'ait pas $z^n \equiv A \pmod{p}$. Alors si on pouvait seulement déterminer les valeurs de $\sqrt[n]{\frac{A}{z^n}} \pmod{p}$, ces différentes valeurs étant multipliées par z donneraient celles de $\sqrt[n]{A}$: en effet, si ν est une valeur de $\sqrt[n]{\frac{A}{z^n}}$ on aura $\nu^n z^n \equiv A$; mais l'expression $\sqrt[n]{\frac{A}{z^n}}$ est plus simple que $\sqrt[n]{A}$, parce que le plus souvent $\frac{A}{z^n}$ appartient à un exposant moindre que A ; car si d est le plus grand commun diviseur de t et de q, $\frac{A}{z^n} \pmod{p}$ appartiendra à l'exposant d, ce qui se démontre ainsi : puisque $z \equiv A^k$, il vient $\frac{A}{z^n}.A^{kn-1} \equiv 1 \pmod{p}$; mais $kn-1$ est divisible par $\frac{p-1}{nq}$ (n° préc.), $\frac{p-1}{n}$ l'est par t, ou $\frac{p-1}{nd}$ par $\frac{t}{d}$. D'ailleurs $\frac{t}{d}$ est premier avec $\frac{q}{d}$; donc aussi $\frac{p-1}{nd}$ est divisible par $\frac{tq}{d^2}$ ou $\frac{p-1}{nq}$ par $\frac{t}{d}$, et partant $kn-1$ par $\frac{t}{d}$, ou $(kn-1)d$ par t. Donc $A^{(kn-1)d} \equiv 1 \pmod{p}$; d'où l'on déduit facilement que $\frac{A}{z^n}$ élevé à la puissance d est congru à l'unité. Il serait facile de démontrer que $\frac{A}{z^n}$ ne peut pas appartenir à un exposant plus petit que d ; mais comme cette démonstration ne peut nous être utile, nous ne nous y arrêterons pas. Nous sommes donc certains que $\frac{A}{z^n} \pmod{p}$ appartient toujours à un plus petit exposant que A, excepté dans le cas unique où l'on aurait $d = t$.

Mais à quoi sert que $\frac{A}{z^n}$ appartienne à un plus petit exposant que A ? Il y a plus de nombres qui peuvent être A qu'il n'y en a qui peuvent être $\frac{A}{z^n}$, et quand on a occasion de résoudre plusieurs expressions de la forme $\sqrt[n]{A}$, suivant le même module, on y gagne de pouvoir tirer d'une même source la solution de plusieurs. Ainsi, par exemple, on déterminera au moins une valeur de $\sqrt[2]{A} \pmod{29}$, si l'on connait seulement les valeurs de $\sqrt[2]{-1} \pmod{29}$, qui sont ± 12 ; en effet l'on voit sans peine, par les articles précédents, que l'on déterminera d'une manière directe une valeur quand t est impair, et que d sera $= 2$ quand t est pair ; or il n'y a que -1 qui appartienne à l'exposant 2.

Exemples.

Soit $\sqrt[3]{31} \pmod{37}$; on a $p-1 = 36, n = 3, \frac{p-1}{n} = 12$, et partant $q = 3$; il faut donc qu'on ait $3k \equiv 1 \pmod{4}$, ce qui donne $k \equiv 3$. Donc $z \equiv 31^3 \pmod{37} \equiv 6$; l'on trouve effectivement

$6^3 = 31$ (mod. 37). Si les valeurs de $\sqrt[3]{1}$ (mod. 37) étaient connues, on pourrait aussi déterminer les autres valeurs de $\sqrt[3]{31}$: or les valeurs de $\sqrt[3]{1}$ (mod. 37) sont $1, 10, 26$; donc celles de $\sqrt[3]{31}$ seront $6, 23, 8$.

Soit maintenant $\sqrt[2]{3}$ (mod. 37) ; on aura $p-1 = 36, n = 2, \frac{p-1}{n} = 18$, et partant $q = 2$; donc on doit avoir $2k \equiv 1$ (mod. 9) d'où $k \equiv 5$; donc $z \equiv 3^5 \equiv 21$ (mod. 37) ; mais 21^2 n'est pas congru avec 3, mais avec 34 ; or on a $\frac{3}{34}$ (mod. 37) $\equiv -1$ et $\sqrt[2]{-1}$ (mod. 37) $\equiv \pm 6$; d'où l'on tire les vraies valeurs $\pm 6.21 \equiv \pm 15$.

Voilà à-peu-près tout ce que nous pouvions exposer ici sur la résolution de ces expressions. Il est clair que les méthodes directes deviennent souvent assez longues ; mais cet inconvénient a lieu dans presque toutes les méthodes directes de la théorie des nombres : Aussi nous n'avons pas cru devoir négliger de faire voir ce qu'on peut en attendre. Il convient aussi d'observer que les artifices particuliers qui se présentent à un homme exercé, n'entrent pas dans notre plan.

69. Revenons maintenant aux racines que nous avons appelées *primitives*. Nous avons fait voir que, si l'on prenait pour base une racine primitive quelconque, tous les nombres dont les indices sont premiers avec $p-1$, étaient aussi des racines primitives, et qu'il n'y en aurait pas d'autres, d'où nous avons conclu le nombre de ces racines (n° 53) : et comme le choix de celle que l'on prend pour base est en général arbitraire, on voit qu'ici, comme dans les logarithmes, on peut avoir plusieurs systèmes[6]. Cherchons les relations qui les lient entre eux. Soient a et b deux racines primitives, et m un autre nombre. Soit de plus Ind. $b = \beta$, quand a est pris pour base, Ind. $m \equiv \mu$ (mod. $p-1$). Soit au contraire Ind. $a = \alpha$, Ind. $m = \nu$ (mod. $p-1$) dans l'hypothèse où l'on prend b pour base ; on aura $a^\beta \equiv b$, donc $a\alpha^\beta \equiv b^\alpha \equiv a$, d'où $\alpha\beta \equiv 1$ (mod. $p-1$). On trouvera de même $\nu \equiv \alpha\mu, \mu \equiv \beta\nu$ (mod. $p-1$). Si donc on a une table d'indices construite pour la base a, on pourra facilement la changer en une autre dont la base est b. En effet, si Ind. $b \equiv \beta$ pour la base a, Ind. a sera $\equiv \frac{1}{\beta}$ (mod. $p-1$) pour la base b, et multipliant par ce nombre tous les indices de la table, on aura tous les indices pour la base b.

70. Mais quoiqu'un nombre donné puisse avoir plusieurs indices, en prenant pour base différentes racines primitives, tous ces indices auront cette propriété commune, que leur plus grand commun diviseur avec $p-1$ sera le même. En effet, A étant un nombre donné, si Ind. $A \equiv m$ pour la base a, et Ind. $A \equiv n$ pour la base b, et si leurs plus grands communs diviseurs μ et ν avec $p-1$ sont supposés inégaux ; soit $\mu > \nu$, μ ne divisera pas n ; mais si Ind. $a = \alpha$ pour la base b, on aura (art. précéd.) $n \equiv \alpha m$ (mod. $p-1$), et partant μ divisera aussi n.

On peut encore s'assurer que ce diviseur commun des indices d'un nombre donné et de $p-1$, est indépendant de la base en observant qu'il est égal à $\frac{p-1}{t}$, t étant l'exposant auquel appartient le nombre dont il s'agit. En effet, si l'indice est k pour une base quelconque, t sera le plus petit nombre (zéro excepté), qui multiplié par k, donne un produit divisible par $p-1$, ou la plus petite valeur de l'expression $\frac{0}{k}$ (mod. $p-1$) ; mais on déduit sans peine du n° 29 que cette valeur est égale au plus grand commun diviseur des nombres k et $p-1$.[7]

[6] Mais ils diffèrent en cela, que dans les logarithmes le nombre des systèmes est infini, et qu'il est ici égal au nombre des racines primitives, car les bases congrues produisent évidemment les mêmes systèmes.

[7] La dernière phrase de l'auteur ne me semble point prouver ce qu'il a avancé ; il s'y est sans doute glissé quelques

71. On démontre facilement que l'on peut toujours trouver une base telle, qu'un nombre appartenant à l'exposant t ait un indice donné à volonté. Le plus grand commun diviseur de cet indice et de $p-1$ étant $\frac{p-1}{t}$, désignons par d ce diviseur, et soit l'indice proposé $\equiv dm$; soit dn l'indice du nombre donné quand on prend pour base la racine primitive quelconque a ; on aura m et n premiers avec $\frac{p-1}{d}$ ou t. Or si e est une valeur de l'expression $\frac{dn}{dm}$ (mod. $p-1$), et en même temps premier avec $p-1$, a^e sera la racine primitive cherchée, car on aura $a^{edm} \equiv a^{dn} \equiv$ au nombre proposé (mod. p). Il nous reste à prouver que l'expression $\frac{dn}{dm}$ (mod. $p-1$) peut admettre des valeurs premières avec $p-1$; elle équivaut à $\frac{n}{m}$ (mod. $\frac{p-1}{d}$) ou $\frac{n}{m}$(mod. t), (n° 31, 2°) et toutes les valeurs en seront premières avec t ; car si une valeur e avait un diviseur commun avec t, ce diviseur devrait aussi diviser me, et partant diviser n qui est congru à me, suivant le module t, ce qui est contre l'hypothèse suivant laquelle n est premier avec t. Ainsi, quand tous les diviseurs premiers de $p-1$ divisent aussi t, toutes les valeurs de l'expression $\frac{n}{m}$ (mod. t) sont premières avec $p-1$, et leur nombre est d ; mais quand $p-1$ renferme encore d'autres facteurs premiers f, g, h, etc. qui ne divisent pas t, soit e une valeur de $\frac{n}{m}$ (mod. t), comme t, f, g, h, etc. sont premiers entre eux, on peut trouver un nombre ϵ congru à e suivant le module t, et congru, suivant f, g, h, etc., à des nombres quelconques premiers avec ceux-ci (n° 32). Ce nombre ne sera divisible par aucun facteur de $p-1$, et partant sera premier avec lui, comme il est nécessaire. On pourrait démontrer sans peine par la théorie des combinaisons, que le nombre de ces valeurs est $\frac{p-1}{t}.\frac{f-1}{f}.\frac{g-1}{g}.\frac{h-1}{h}$. etc. ; mais nous omettons cette démonstration qui ne peut nous être d'aucune utilité.

72. Quoiqu'en général on puisse prendre arbitrairement pour base une racine primitive quelconque, certains avantages particuliers peuvent faire préférer une base à toute autre. Dans la table I nous avons toujours pris 10 pour base quand il était racine primitive, et dans les autres cas nous avons choisi la base de manière que l'indice du nombre 10 fût le plus petit possible, c'est-à-dire $= \frac{p-1}{t}$, t étant l'exposant auquel 10 appartient. On en reconnaîtra l'avantage dans la sect. VI, où la même table sera employée à d'autres usages. Mais comme il peut encore rester ici quelque chose d'arbitraire, ainsi qu'on le voit par l'article précédent, nous avons toujours choisi, parmi toutes les racines primitives qui satisfont à la question, la plus petite pour base : ainsi pour $p = 73$, on a $t = 8$ et $d = 9$, ϵ a $\frac{72.2}{8.3} = 6$ valeurs qui sont $5, 14, 20, 28, 39, 40$, et nous avons pris 5 pour base.

73. La plupart des méthodes qui servent à trouver les racines primitives reposent en grande partie sur le tâtonnement. Si l'on réunit ce que nous avons dit (n° 55) avec ce que nous dirons plus bas sur la résolution de la congruence $x^n \equiv 1$, on aura à-peu-près tout ce qui peut se faire par les méthodes générales. EULER avoue (*Opuscula analyt. T. 1, p. 152.*) qu'il lui semble extrêmement difficile d'assigner ces nombres, et que leur nature doit être rangée dans les points les plus épineux de la théorie des nombres ; mais on les trouve assez facilement par la méthode suivante. Les hommes exercés préviendront facilement la longueur du calcul par beaucoup d'artifices ; mais l'usage les indique mieux que les préceptes.

1°. On prendra à volonté un nombre a premier avec le module p [8] ; et souvent le calcul devient

fautes d'impression qui lui ont échappé. Au reste je crois que l'on peut y suppléer de la manière suivante :
Puisque t est le plus petit nombre qui rende kt divisible par $p-1$, ce sera aussi celui qui rendra $\frac{kt}{d}$ divisible par $\frac{p-1}{d}$, d étant le plus grand commun diviseur entre k et $p-1$. Or $\frac{k}{d}$ et $\frac{p-1}{d}$ étant premiers entre eux, la plus petite valeur de t convenable est $\frac{p-1}{d}$; donc $\frac{p-1}{d} = t$ et $d = \frac{p-1}{t}$.(*Note du traducteur.*)

[8]Nous désignerons toujours le module par p.

plus simple lorsqu'on prend a le plus petit possible, 2 par exemple ; on déterminera sa période (n° 46), c'est-à-dire les résidus minima de ses puissances, jusqu'à ce que l'on parvienne à une puissance a^t, qui ait 1 pour résidu minimum [9]. Si l'on a $t = p-1$, a sera une racine primitive.

2°. Mais si $t < p-1$, on prendra un autre nombre b, qui ne soit pas contenu dans la période de a, et l'on cherchera de la même manière sa période. En nommant u l'exposant auquel b appartient, on voit facilement que u n'est ni égal à t, ni une de ses parties aliquotes, car dans les deux cas on aurait $b^t \equiv 1$, ce qui est impossible, la période de a renfermant tous les nombres dont la puissance t est congrue à l'unité (n° 53). Or si $u = p-1$, b sera une racine primitive ; si u n'est pas $= p-1$, mais un multiple de t, nous aurons encore l'avantage de connaître un nombre qui appartienne à un exposant plus grand, et partant nous approcherons de notre but, puisque nous cherchons le nombre qui appartient à l'exposant *maximum* ; mais si u n'est ni $= p-1$, ni multiple de t, nous pouvons trouver un nombre appartenant à un exposant plus grand que t et u ; cet exposant sera le plus petit nombre divisible à la fois par t et u. En effet, soit y ce dernier nombre ; on décomposera y en deux facteurs m et n premiers entre eux, dont l'un divise t et l'autre u [10].

Soit $a^{\frac{t}{m}} \equiv A, b^{\frac{u}{n}} \equiv B \pmod{p}$, AB appartiendra à l'exposant y ; car on voit facilement que A appartient à l'exposant m, B à l'exposant n, et par conséquent AB appartiendra à l'exposant mn, puisque m et n sont premiers entre eux, comme on peut le démontrer en suivant exactement le procédé du n° 55.

3°. Si $y = p-1$, AB sera une racine primitive, sinon on prendra de même un troisième nombre qui ne se trouve pas dans la période de AB ; ce nombre sera une racine primitive, ou bien il appartiendra à un exposant $> y$, ou bien enfin par son moyen on déterminera un nombre appartenant à un exposant $> y$: donc, comme les nombres qui résultent de la répétition de cette opération, appartiennent à des exposants qui vont toujours en augmentant, et sont néanmoins diviseurs de $p-1$, il est évident qu'on en trouvera enfin un qui appartiendra au *maximum* $p-1$, ce sera la racine primitive.

74. Eclaircissons ceci par un exemple. Soit $p = 73$, pour lequel on demande une racine primitive. Essayons d'abord le nombre 2, dont la période est

1.	2.	4.	8.	16.	32.	64.	55.	37.	1	etc.
0.	1.	2.	3.	4.	5.	6.	7.	8.	9	etc.

Donc puisque $2^9 \equiv 1$, 2 n'est pas racine primitive. Essayons le nombre 3 qui ne se trouve pas dans la période de 2, sa période est

1.	3.	9.	27.	8.	24.	72.	70.	64.	46.	65.	49.	1	etc.
0.	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12	etc.

[9] Il est aisé de voir qu'il n'est pas nécessaire de connaître ces puissances, car on peut obtenir le résidu minimum d'une puissance au moyen de la puissance précédente.

[10] On voit facilement par le n° 18 comment on peut faire cette décomposition. On décomposera y en facteurs qui soient des nombres premiers ou des puissances de nombres premiers différents ; chacun d'eux divisera t ou u, ou tous les deux. On écrira sous t ou sous u ceux qui divisent t ou u. Quant à ceux qui diviseront u et t, peu importe sous lequel on les écrive. Si l'on fait $m =$ le produit de ceux qui sont écrits sous t, $n =$ le produit de ceux qui sont écrits sous u, il est évident que m divisera t, que n divisera u et que $mn = y$.

Donc 3 n'est pas non plus racine primitive ; mais le plus petit nombre divisible à la fois par les exposants 9 et 12, auxquels 2 et 3 appartiennent, est 36, qui donne $m = 9$ et $n = 4$. Donc élevant 2 à la puissance $\frac{9}{9} = 1$, 3 à la puissance $\frac{12}{4} = 3$, le produit de ces deux puissances est 54, qui appartiendra à l'exposant 36. Si enfin on calcule la période de 54, et qu'on essaye un nombre qui n'y soit pas contenu, 5 par exemple, on trouve qu'il est racine primitive.

75. Avant d'abandonner ce sujet, nous présenterons quelques propositions qui ne nous paraissent pas indignes d'attention, à cause de leur simplicité.

Le produit de tous les termes de la période d'un nombre quelconque est $\equiv 1$ *quand leur nombre ou l'exposant auquel appartient le nombre dont il s'agit est impair, et* $\equiv -1$ *quand il est pair.*

Par exemple, pour le module 13, la période de 5 est composée des termes 1, 5, 12, 8, dont le produit $480 \equiv -1$ (mod. 13), suivant le même module, la période de 3 est composée des termes 1, 3, 9, dont le produit $27 \equiv 1$ (mod. 13).

Soit t l'exposant auquel le nombre appartient ; on peut toujours trouver (n° 71) une base pour laquelle l'indice du nombre soit $\frac{p-1}{t}$.

Or l'indice du produit de tous les termes sera

$$\equiv (1 + 2 + 3 + \text{etc.} + t - 1)\frac{p-1}{t} = \frac{(t-1)(p-1)}{2} ;$$

donc il sera $\equiv 0$ (mod. $p-1$), quand t est impair ; et $\equiv \frac{p-1}{2}$ quand t est pair. Dans le premier cas, le produit est $\equiv 1$ (mod. p) ; dans le second, $\equiv -1$ (mod. p).

76. Si le nombre du théorème précédent est une racine primitive, sa période comprendra tous les nombres $1, 2, 3, 4, ..., p-1$, dont le produit sera par conséquent toujours $\equiv -1$; car $p-1$ est toujours pair, excepté dans le cas où $p = 2$, et alors on a indifféremment $+1$ ou -1. Ce théorème élégant qu'on énonce ordinairement de cette manière : *Le produit de tous les nombres plus petits qu'un nombre premier étant augmenté de l'unité, est divisible par ce nombre premier,* a été publié par Waring qui l'attribue à Wilson (*Meditationes Algeb. Ed. 3, p. 380*) ; mais aucun des deux n'a pu le démontrer, et Waring avoue que la démonstration lui en semble d'autant plus difficile qu'il n'y a point de *notation* par laquelle on puisse exprimer un nombre premier ; pour nous, nous pensons que la démonstration de cette sorte de vérités doit être puisée dans les principes plutôt que dans la notation. Lagrange en a depuis donné une démonstration (*Nouv. Mém. de l'Ac. de Berlin, 1771*), dans laquelle il s'appuie sur la considération des coefficients que l'on trouve en développant le produit

$$(x+1)(x+2)(x+3)...(x+p-1) :$$

et il fait voir qu'en supposant ce produit

$$= x^{p-1} + Ax^{p-2} + Bx^{p-3} + \text{etc.} + Mx + N,$$

les coefficients A, B, etc. M sont divisibles par p ; or

$$N = 1.2.3...p-1.$$

Maintenant si $x = 1$, le produit est divisible par p ; mais alors il sera $\equiv 1 + N$ (mod. p), donc $1 + N$ est divisible par p.

Enfin EULER (*Opusc. analyt. T. 1, p. 329*) en a donné une démonstration qui rentre dans celle que nous venons d'exposer ; ainsi puisque de tels hommes n'ont pas cru ce sujet indigne de leurs méditations, nous espérons qu'on ne nous désapprouvera pas d'offrir encore ici une autre manière de démontrer ce théorème.

77. Nous dirons que deux nombres sont *associés*, comme l'a fait EULER, lorsque leur produit sera congru à l'unité. Cela posé, par la section précédente, tout nombre positif moindre que p, aura toujours un nombre associé moindre que p et il n'en aura qu'un ; or il est facile de prouver que parmi les nombres $1, 2, 3, ..., p-1$, il n'y a que 1 et $p-1$ qui soient eux-mêmes leurs associés, car ceux qui jouiront de cette propriété seront donnés par la congruence $x^2 \equiv 1$ qui ne peut avoir que deux racines 1 et $p-1$. Supprimant donc ces deux nombres, les autres $2, 3, 4, ..., p-2$, seront associés deux à deux ; donc leur produit sera $\equiv 1$; enfin multipliant par $p-1$, le produit de tous $1.2.3.4...p-1 \equiv p-1 \equiv -1$.

Par exemple, pour $p = 13$, les nombres $2, 3, 4, 5, ..., 11$ s'associent de la manière suivante : 2 avec 7, 3 avec 9, 4 avec 10, 5 avec 8, 6 avec 11 ; donc $2.3.4...11 \equiv 1$, et partant $1.2.3....12 \equiv 12 \equiv -1$.

78. Le théorème de WILSON peut être rendu plus général en l'énonçant comme il suit : *Le produit de tous les nombres premiers avec un nombre donné A et moindres que ce nombre, est congru suivant A, à l'unité prise positivement ou négativement.* L'unité doit être prise négativement quand A est de la forme p^m ou $2p^m$, p étant un nombre premier différent de 2, ou encore quand $A = 4$, et positivement dans tous les autres cas. Le théorème de WILSON est contenu dans le premier cas. *Exemple.* Pour $A = 15$, le produit des nombres $1, 2, 4, 7, 8, 11, 13, 14$, est $\equiv 1$ (mod. 15). Nous supprimons, pour abréger, la démonstration. Nous observerons seulement qu'on peut y parvenir comme dans l'article précédent, excepté que la congruence $x^2 \equiv 1$ peut avoir plus de deux racines, ce qui demande certaines considérations particulières. On pourrait aussi la tirer de la considération des indices, comme dans le n° 75, si l'on y joint ce que nous dirons tout à l'heure des modules composés.

79. Revenons à l'énumération des autres propositions (n° 75).

La somme de tous les termes de la période d'un nombre quelconque est $\equiv 0$.

Ainsi dans l'exemple du n° 75

$$1 + 5 + 12 + 8 = 26 \equiv 0 \text{ (mod. 13)}.$$

Soit a le nombre dont il s'agit, et t l'exposant auquel il appartient. La somme de tous les termes de la période sera

$$\equiv 1 + a + a^2 + a^3 + ... + a^{t-1} \equiv \frac{a^t - 1}{a - 1} \text{ (mod. } p) ;$$

or $a^t - 1 \equiv 0$, donc aussi $\frac{a^t-1}{a-1} \equiv 0$, si $a - 1$ n'est pas divisible par p ; il faut donc excepter ce cas, si nous voulons regarder même un seul terme comme une *période*.

80. *Le produit de toutes les racines primitives est* $\equiv 1$, excepté le cas où $p = 3$, car alors il n'y a qu'une racine primitive 2.

Si l'on prend pour base une racine primitive quelconque, les indices de toutes les racines primitives seront des nombres premiers avec $p-1$ et moindres que lui ; mais la somme de tous ces nombres, c'est-à-dire l'indice du produit de toutes les racines primitives, est $\equiv 0$ (mod. $p-1$) ; donc le produit est $\equiv 1$ (mod. p). En effet on voit facilement que si k est un nombre premier avec $p-1$, $p-1-k$ le sera aussi, et que par conséquent la somme des nombres premiers avec $p-1$ est composée de couples dont la somme est divisible par $p-1$. Il est bon d'observer que k ne peut être égal à $p-1-k$, à moins que $\frac{p-1}{2}$ ne soit premier avec $p-1$, ce qui exige que $p-1 = 2$ ou $p = 3$, cas que nous exceptons.

81. *La somme des racines primitives est* $\equiv 0$ quand $p-1$ est divisible par un carré, ou $\equiv \pm 1$ quand $p-1$ est le produit de facteurs premiers inégaux. Le signe $+$ appartenant au cas où le nombre de ces facteurs est pair, le signe $-$ au cas où il est impair.

Ex. 1°. Pour $p = 13$, on a les racines primitives $2, 6, 7, 11$ dont la somme $26 \equiv 0$ (mod. 13).
2°. Pour $p = 11$, les racines primitives sont $2, 6, 7, 8$, dont la somme $23 \equiv +1$ (mod. 11).
3°. Pour $p = 31$, les racines primitives sont $3, 11, 12, 13, 17, 21, 22, 24$, dont la somme $123 \equiv -1$ (mod. 31).

Nous avons démontré plus haut (n° 55, 2°) que si l'on a $p-1 = a^\alpha b^\beta c^\gamma$ etc., et que A, B, C, etc. soient des nombres quelconques qui appartiennent aux exposants $a^\alpha, b^\beta, c^\gamma$, etc. respectivement, tous les produits ABC etc, seront des racines primitives ; mais on peut aussi démontrer facilement qu'une racine primitive quelconque peut s'exprimer par un produit de cette espèce et d'une seule façon [11] .

Il suit de là que ces produits peuvent être pris au lieu des racines primitives ; mais, comme dans ces produits il faut combiner toutes les valeurs de A avec toutes celles de B, etc., la somme de tous ces produits sera égale au produit de la somme des valeurs de A, multipliée par la somme des valeurs de B, etc. Désignons toutes les valeurs de A, B, C, etc. par A, A', A'', etc. B, B', B'', etc. C, C', C'',

[11] On déterminera des nombres α', β', γ', etc. tels qu'on ait $\alpha' \equiv 1$ (mod. a^α) et $\equiv 0$ (mod. $b^\beta c^\gamma$ etc.) ; $\beta' \equiv 1$ (mod. b^β) et $\equiv 0$ (mod. $a^\alpha c^\gamma$ etc.), etc. (*v.* n° 32) ; donc on aura $\alpha' + \beta' + \gamma'$+etc.$\equiv 1$ (mod. $p-1$), (n° 19). Or si l'on doit exprimer une racine primitive quelconque r par un produit de la forme ABC etc. ; on prendra $A \equiv r^{\alpha'}, B \equiv r^{\beta'}, C \equiv r^{\gamma'}$, etc. A, B, C appartiendront respectivement aux exposants $a^\alpha, b^\beta, c^\gamma$, etc., et le produit ABC etc. sera $\equiv r$ (mod. p). Or il est facile de voir que A, B, C, etc. ne peuvent se déterminer d'une autre manière (1).

(1) Cette note nous semble avoir besoin de quelques éclaircissements. Il est aisé de voir que tous les nombres, excepté α', sont divisibles par a^α ; que partant leur somme l'est aussi, ou est $\equiv 0$ (mod. a^α) ; mais comme $\alpha' \equiv 1$ (mod. a^α), il vient donc $\alpha' + \beta' + \gamma'$+ etc.$\equiv 1$ (mod. a^α), de même $\alpha' + \beta' + \gamma'$+etc.$\equiv 1$ (mod. b^β), etc. ; donc $\alpha' + \beta' + \gamma'$+etc.$\equiv 1$ (mod. $a^\alpha b^\beta c^\gamma$, etc.) $\equiv 1$ (mod. $p-1$). Or si l'on fait $A \equiv r^{\alpha'}, B \equiv b^{\beta'}, C \equiv c^{\gamma'}$, etc. A, B, C, etc. appartiendront aux exposants $a^\alpha, b^\beta, c^\gamma$, etc. respectivement. En effet $A^{a^\alpha} \equiv r^{\alpha' a^\alpha} \equiv 1$ (mod. p), $\alpha' a^\alpha$ étant $\equiv 0$ (mod. $p-1$), et il est visible que l'on ne peut supposer $A^t \equiv 1$ (mod. p), t étant $< a$, et de même pour B, C, etc., car on aurait $\alpha' t \equiv 0$ (mod. $p-1$), ce qui ne peut avoir lieu à moins que t ne soit $= a^\alpha$ ou $\equiv 0$ (mod. a^α). Or il est aisé de s'assurer encore qu'on ne peut trouver de nombres A', B', C', etc. respectivement incongrus à A, B, C, etc., et qui puissent les remplacer. En effet on aurait $A' \equiv r^{\alpha''}$, α'' étant un nombre déterminé comme α' ; mais on a aussi $A \equiv r^{\alpha'}$; or comme α' et α'' sont congrus au même nombre suivant le module $p-1$, ils sont congrus entre eux suivant ce même module ; donc $r^{\alpha'} \equiv r^{\alpha''}$ (mod. p), et partant $A \equiv A'$. (*Note du traducteur.*)

etc. La somme de toutes les racines primitives sera congrue au produit $(A+A'+\text{etc.})(B+B'+\text{etc.})$ etc. ; or je dis que si $\alpha = 1$, la somme $A + A' + A''+$etc., sera $\equiv -1 \pmod{p}$, que si $\alpha > 1$, cette somme sera $\equiv 0$, et de même pour β, γ, etc. Si ces deux assertions sont démontrées, la vérité du théorème sera manifeste. En effet, quand $p-1$ est divisible par un carré, quelqu'un des exposants α, β, γ, etc. sera > 1, et partant un des facteurs dont le produit est congru à la somme des racines primitives, sera $\equiv 0$, c'est-à-dire que le produit lui-même le sera. Quand $p-1$ ne pourra être divisé par aucun carré, tous les exposants α, β, γ, etc. seront égaux à l'unité, et la somme des racines primitives sera congrue au produit d'autant de facteurs dont chacun $\equiv -1$, qu'il y a de nombres a, b, c, etc. ; donc partant le produit sera $\equiv \pm 1$, suivant qu'ils seront en nombre pair ou impair ; or ces deux assertions se prouvent ainsi qu'il suit :

1°. Quand $\alpha = 1$, et que A est un nombre appartenant à l'exposant a, les autres nombres qui appartiennent aussi à cet exposant sont $A^2, A^3, ...A^{a-1}$; or $1 + A + A^2 + A^3 + A^4 + ... + A^{a-1}$ est la somme de la période complète, et partant $\equiv 0$ (n° 79) ; donc

$$A + A^2 + A^3 + \ldots + A^{a-1} \equiv -1.$$

2°. Quand $\alpha > 1$ et que A est un nombre appartenant à l'exposant a^α, on aura les autres nombres appartenant au même exposant, si de la suite $A^2, A^3, A^4, ...A^{a^\alpha - 1}$, on retranche A^a, A^{2a}, A^{3a}, etc. (n° 53), leur somme sera donc

$$= 1 + A + A^2 + \ldots + A^{a^\alpha - 1} - (1 + A^a + A^{2a} + \ldots + A^{a^\alpha - a}) ,$$

c'est-à-dire congrue à la différence de deux périodes, et par conséquent $\equiv 0$.

82. Tout ce que nous avons exposé jusqu'à présent, suppose que le module soit un nombre premier. Il nous reste à considérer le cas où l'on prend pour module un nombre composé ; mais comme il n'en résulte pas des propriétés aussi élégantes que dans le premier cas, et qu'il n'y a pas besoin d'artifices bien délicats pour les trouver, tout se déduisant presque de la seule application des principes précédents, il serait superflu et fastidieux d'épuiser ici tous les détails. Aussi nous exposerons en peu de mots ce que ce second cas a de commun avec le premier, et ce qui lui est propre.

83. Les propositions des n^{os} 45-48 ont déjà été démontrées généralement, mais celle du n° 49 doit être changée ainsi :

Si f désigne combien il y a de nombres premiers avec m et moindres que lui, c'est-à-dire si $f = \varphi m$ (art. 38), l'exposant t de la plus petite puissance d'un nombre donné a premier avec m, qui est congrue à l'unité suivant le module m sera $= f$, ou une partie aliquote de f.

La démonstration de la proposition du n° 49 peut servir également dans ce cas-ci, en y substituant m pour p, f pour $p-1$, et au lieu des nombres $1, 2, 3, ..., p-1$, les nombres premiers avec m et moindres que lui ; ainsi nous y renvoyons le lecteur. Mais les autres démonstrations dont nous avons parlé (n^{os} 50, 51) ; ne peuvent s'appliquer à ce cas sans beaucoup d'embarras. À l'égard des propositions suivantes (n° 52 et suivants), il y a une grande différence entre les modules qui sont les puissances d'un nombre premier et ceux qui sont divisibles par plusieurs nombres premiers. Nous considérerons donc à part les modules du premier genre.

84. Si le module $m = p^n$, p étant un nombre premier, on aura $f = p^{n-1}(p-1)$, (n° 38). Or si l'on applique à ce cas les recherches contenues (n^{os} 53, 55), *mutatis mutandis* comme dans l'article précédent, on trouvera que tout ce qui y a été démontré aurait lieu également, s'il était prouvé que la congruence $x^t - 1 \equiv 0 \pmod{p^n}$, ne peut avoir plus de t racines différentes. C'est d'une proposition plus générale (n° 43) que nous avons déduit cette vérité pour un module premier : mais cette proposition n'a lieu que pour les modules premiers, et partant ne peut s'appliquer à ce cas. Nous allons donc la démontrer par une méthode particulière, et plus bas (sect. VIII[12]) nous le prouverons encore plus facilement.

85. Nous nous proposons de démontrer ce théorème : *Si le plus grand commun diviseur des nombres t et $p^{n-1}(p-1)$ est e, la congruence $x^t \equiv 1 \pmod{p^n}$ aura e racines différentes.*

Soit $e = kp^\nu$, de sorte que k ne renferme point le facteur p, et qu'il divise par conséquent $p-1$. Alors la congruence $x^t \equiv 1$ suivant le module p, aura k racines différentes, et si on les désigne par A, B, C, etc., une racine quelconque de cette même congruence, suivant le module p^n, devra être congrue à quelqu'un des nombres A, B, C, etc., suivant le module p. Or nous démontrerons que la congruence $x^t \equiv 1 \pmod{p^n}$, a p^ν racines congrues à A, autant à B, etc. suivant le module p, d'où il résultera que le nombre de toutes les racines sera kp^ν ou e, comme nous l'avons avancé. Cela posé, nous allons démontrer que

1°. Si α est une racine congrue à A, suivant le module p, $\alpha + p^{n-\nu}, \alpha + 2p^{n-\nu}, \alpha + 3p^{n-\nu}, \ldots, \alpha + p^{\nu-1}.p^{n-\nu}$ seront aussi des racines.

2°. Aucun nombre congru avec A ne pourra être racine, s'il n'est de la forme $\alpha + hp^{n-\nu}$, h étant un nombre entier quelconque ; d'où il suit qu'on aura p^ν racines différentes, et qu'on n'en aura pas davantage ; la même chose aura lien par rapport à B, C, etc.

3°. Nous ferons voir comment on peut toujours trouver une racine congrue à A suivant le module p.

86. THÉORÈME. *Si t est comme dans l'article précédent un nombre divisible par p^ν et non par $p^{\nu+1}$, on aura $(\alpha + hp^\mu)^t - \alpha^t \equiv 0 \pmod{p^{\mu+\nu}}$, et $\equiv \alpha^{t-1} hp^\mu t \pmod{p^{\mu+\nu+1}}$.* La seconde partie du théorème n'a pas lieu quand $p = 2$ et $\mu = 1$.

On pourrait déduire la démonstration de ce théorème du développement de la puissance d'un binôme, si on faisait voir que tous les termes, après le second, sont divisibles par $p^{\mu+\nu+1}$; mais comme la considération des dénominateurs des coefficients jette dans quelque embarras, nous préférons la méthode suivante :

Supposons d'abord $\mu > 1$ et $\nu = 1$, on a généralement $x^t - y^t = (x-y)(x^{t-1} + x^{t-2}y + x^{t-3}y^2 + \ldots + y^{t-1})$; donc $(\alpha + hp^\mu)^t - \alpha^t = hp^\mu\{(\alpha + hp^\mu)^{t-1} + (\alpha + hp^\mu)^{t-2} + \text{etc.} + \alpha^{t-1}\}$; mais on a $\alpha + hp^\mu \equiv \alpha \pmod{p^2}$; donc chaque terme $(\alpha + hp^\mu)^{t-1}, (\alpha + hp^\mu)^{t-2}\alpha$, etc. sera $\equiv \alpha^{t-1} \pmod{p^2}$, et par conséquent la somme de tous $\equiv t\alpha^{t-1} \pmod{p^2}$, ou bien cette somme sera de la forme $t\alpha^{t-1} + Vp^2$, V étant un nombre quelconque. Donc $(\alpha + hp^\mu)^t - \alpha^t$ sera de la forme $\alpha^{t-1} hp^\mu t + Vhp^{\mu+2}$, c'est-à-dire qu'il sera $\equiv \alpha^{t-1} hp^\mu t \pmod{p^{\mu+2}}$ et $\equiv 0 \pmod{p^{\mu+1}}$. Ainsi, pour ce cas, le théorème est démontré.

[12] *Voir note de la transcriptrice pour la section 61.*

Or si le théorème n'était pas vrai pour les autres valeurs de ν, μ restant > 1, il y aurait nécessairement une limite jusqu'à laquelle le théorème serait vrai, et passé laquelle il serait faux. Soit φ la plus petite valeur de ν qui se refuse au théorème. On voit facilement que le théorème est vrai si t est divisible par $p^{\varphi-1}$ et non par p^{φ} ; mais que si l'on substitue tp à la place de t, il ne l'est plus. On a donc $(\alpha + hp^{\mu})^t \equiv \alpha^t + \alpha^{t-1}hp^{\mu}t \pmod{p^{\mu+\varphi}}$, ou $= \alpha^t + \alpha^{t-1}hp^{\mu}t + up^{\mu+\varphi}$, u étant un nombre entier quelconque ; mais comme le théorème est déjà démontré pour $\nu = 1$, on aura $(\alpha^t + \alpha^{t-1}hp^{\mu}t + up^{\mu+\varphi})^p \equiv \alpha^{tp} + \alpha^{tp-1}hp^{\mu+1}t + \alpha^{tp-1}up^{\mu+\varphi+1} \pmod{p^{\mu+\varphi+1}}$, et partant $(\alpha + hp^{\mu})^{tp} \equiv \alpha^{tp} + \alpha^{tp-1}hp^{\mu}tp \pmod{p^{\mu+\varphi+1}}$; c'est-à-dire que le théorème est encore vrai si on substitue tp au lieu de t ou $\varphi + 1$ au lieu de φ, contre l'hypothèse ; donc le théorème est vrai pour toutes les valeurs de ν.

87. Il reste le cas où $\mu = 1$. Par une méthode absolument semblable à celle de l'article précédent, on démontrera, sans faire usage du développement du binôme, que

$$\begin{aligned}(\alpha + hp)^{t-1} &\equiv \alpha^{t-1} + \alpha^{t-2}(t-1)hp \pmod{p^2}\\ \alpha(\alpha + hp)^{t-2} &\equiv \alpha^{t-1} + \alpha^{t-2}(t-2)hp \pmod{p^2}\\ \alpha^2(\alpha + hp)^{t-3} &\equiv \alpha^{t-1} + \alpha^{t-2}(t-3)hp \pmod{p^2}, \text{ etc. ;}\end{aligned}$$

donc (puisque le nombre des termes est t) la somme sera $\equiv t\alpha^{t-1} + \frac{(t-1)t}{2}\alpha^{t-2}hp \pmod{p^2}$; mais, comme t est divisible par p, $\frac{(t-1)t}{2}$ le sera aussi, excepté le cas où $p = 2$; que nous avons exclu, et dans les autres cas, la somme sera $\equiv t\alpha^{t-1} \pmod{p^2}$, puisque $\frac{(t-1)t}{2}\alpha^{t-2}hp$ est divisible par p^2. Le reste de la démonstration est comme dans l'article précédent.

Il résulte de là généralement qu'en exceptant le cas où $p = 2$, on a $(\alpha + hp^{\mu})^t \equiv \alpha^t \pmod{p^{\mu+\nu}}$ et $(\alpha + hp^{\mu})$ *non* $\equiv \alpha^t$ pour un module qui est une puissance de p plus haute que $p^{\mu+\nu}$ pourvu toutefois que h ne soit pas divisible par p, et que p^{ν} soit la plus haute puissance de p qui divise t.

De là suivent sur-le-champ les deux premières propositions que nous nous étions proposé de démontrer (n° 85), savoir :

1°. Si $\alpha^t \equiv 1$, on aura aussi $(\alpha + hp^{n-\nu})^t \equiv 1 \pmod{p^n}$.

2º. Si un nombre α' congru à A et partant à α, suivant le module p, mais incongru à α, suivant le module, $p^{n-\nu}$, satisfaisait à la congruence $x^t \equiv 1 \pmod{p^n}$, supposons $\alpha' = \alpha + lp^{\lambda}$, de sorte que l ne soit pas divisible par p, on aura $\lambda < n - \nu$; alors $(\alpha + lp^{\lambda})^t \equiv \alpha' \pmod{p^{\lambda+\nu}}$ et non suivant p^n, qui est une puissance de p plus haute que $p^{\lambda+\nu}$; donc α' ne peut être racine de la congruence $x^t \equiv 1$.

88. Nous devions en troisième lieu trouver une racine de la congruence $x^t \equiv 1 \pmod{p^n}$, qui fut congrue à A. Il nous suffira de faire voir ici comment on peut y parvenir, si l'on connaît une racine de la congruence suivant le module p^{n-1}, puisque l'on pourra passer du module p, pour lequel A est racine, au module p^2, et de là à toutes les puissances consécutives.

Soit donc α une racine de la congruence $x^t \equiv 1 \pmod{p^{n-1}}$ et que l'on cherche une racine de la même congruence suivant le module p^n, nous la supposerons $= \alpha + hp^{n-\nu-1}$, forme qu'elle doit avoir d'après l'article précédent : nous considérerons à part le cas où $\nu = n-1$, et ν ne peut être $> n-1$. On aura donc $(\alpha + hp^{n-\nu-1})^t \equiv 1 \pmod{p^n}$; mais $(\alpha + hp^{n-\nu-1})^t = \alpha + \alpha^{t-1}htp^{n-\nu-1} \pmod{p^n}$

; si donc on détermine h de manière qu'on ait $1 \equiv \alpha^t + \alpha^{t-1} htp^{n-\nu-1}$ (mod. p^n) ; ou, comme par hypothèse $1 \equiv \alpha^t$ (mod. p^{n-1}) et que t est divisible par p^ν, de manière qu'on ait $\frac{a^t-1}{p^{n-1}} + \alpha^{t-1} h \frac{t}{p^\nu}$ divisible par p, le problème sera résolu ; or il est prouvé, dans la section précédente, que cela est toujours possible, puisque t ne peut être divisé par une puissance de p plus haute que p^ν, et que partant $\alpha^{t-1}\frac{t}{p}$ est premier avec p.

Mais si $\nu = n-1$, c'est-à-dire si t est divisible par p^{n-1} ou par une plus haute puissance de p, toute valeur A qui satisfera à la congruence $x^t \equiv 1$, suivant le module p, y satisfera aussi suivant le module p^n. Soit en effet $t = p^{n-1}\tau$, on aura $t \equiv \tau$ (mod. $p-1$) ; donc puisque $A^t \equiv 1$ (mod. p), on aura aussi $A^\tau \equiv 1$ (mod. p). Soit donc $A^\tau = 1 + hp$, on aura $A^t = (1+hp)p^{n-1} \equiv 1$ (mod. p^n), (n° 87).

89. Tout ce que nous avons démontré (n^{os} 57 et suivants) à l'aide du théorème du n° 43, a lieu pour un module qui est une puissance d'un nombre premier, et si l'on appelle *racines primitives* les nombres qui appartiennent à l'exposant $p^{n-1}(p-1)$, c'est-à-dire ceux dans la période desquels se trouvent tous les nombres non divisibles par p, il y aura également ici des racines primitives ; tout ce que nous avons dit des indices et de leur usage, ainsi que de la résolution de la congruence $x^t \equiv 1$, peut s'appliquer à ce cas : comme toutes les démonstrations n'ont aucune difficulté, il serait superflu de les répéter. Nous avons en outre fait voir comment on déduit des racines de la congruence $x^t \equiv 1$ (mod. p), celles de la congruence $x^t \equiv 1$ (mod. p^n) ; mais il faut ajouter quelque chose sur le cas où $p = 2$, que nous avions exclu dans ce qui précède.

90. *Si l'on prend pour module une puissance de 2 plus haute que la seconde, 2^n par exemple, la puissance 2^{n-2} de tout nombre impair sera 1.*

Par exemple, $3^8 = 6561 \equiv 1$ (mod. 32).

En effet tout nombre impair est de la forme $1+4h$ ou de celle-ci $-1+4h$, d'où la proposition suit immédiatement (86).

Ainsi l'exposant auquel appartient un nombre impair quelconque suivant le module 2^n, doit être un diviseur de 2^{n-2} ; ce nombre appartiendra donc à l'un des suivants $1, 2, 4, 8, ..., 2^{n-2}$; et d'ailleurs on jugera facilement auquel il appartient. Soit le nombre proposé $= 4h \pm 1$, et 2^m la plus haute puissance de 2 qui puisse diviser h (m est $= 0$ quand h est impair). Alors l'exposant auquel appartient le nombre donné sera $= 2^{n-m-2}$, si $n > m+2$; mais si $n =$ ou $< m+2$, le nombre proposé sera $\equiv \pm 1$, et partant appartiendra à l'exposant 1 ou à l'exposant 2. En effet $4h \pm 1 = \pm 1 + 2^{m+2}k$, et ce nombre élevé à la puissance 2^{n-m-2} devient congru à l'unité suivant le module p^n ; or on déduit sans peine du n° 86 que si on élevait ce nombre à une puissance de degré moindre, le résultat serait incongru à l'unité. Ainsi tout nombre de la forme $\pm 1 + 4h$, où h est impair, c'est-à-dire tout nombre de la forme $8k+3$ ou $8k+5$, appartient à l'exposant p^{n-2}.

91. Il suit de là qu'il n'y a pas dans ce cas-ci de *racines primitives*, dans le sens que nous avons donné à cette expression, c'est-à-dire qu'il n'y a pas de nombres dont la période renferme tous les nombres premiers avec le module, et plus petits que lui ; mais on voit facilement qu'il arrive ici quelque chose d'analogue. En effet toute puissance impaire d'un nombre de la forme $8k+3$ est

elle-même de la forme $8k+3$, et toute puissance paire est de la forme $8k+1$; donc aucune ne peut être de la forme $8k+5$ ou $8k+7$; donc comme la période d'un nombre de la forme $8k+3$ est composée de 2^{n-2} termes différents, dont chacun est de la forme $8k+1$ ou $8k+3$, et qu'il n'y a pas plus de 2^{n-2} de ces nombres qui soient plus petits que le module, il est évident que tout nombre de la forme $8k+1$ ou $8k+3$ est congru suivant le module 2^n, à une puissance d'un nombre quelconque de la forme $8k+3$. On peut faire voir de la même manière que la période d'un nombre de la forme $8k+5$ comprend tous les nombres de la forme $8k+1$ et $8k+5$. Si donc on prend pour base un nombre de la forme $8k+5$, on trouvera des indices réels pour tous les nombres de la forme $8k+1$ et $8k+5$ pris positivement, et pour tous les nombres de la forme $8k+3$ et $8k+7$ pris négativement : on doit encore regarder comme équivalents les indices congrus suivant 2^{n-2}. C'est ainsi qu'on doit entendre la table I, dans laquelle pour les modules 16, 32 et 64 (car il n'y a besoin d'aucune table pour le module 8), nous avons toujours pris 5 pour base. Par exemple, le nombre 19, qui doit être pris négativement, puisqu'il est de la forme $8n+3$, a pour le module 64 l'indice 7, ce qui signifie que $5^7 \equiv -19 \pmod{64}$. Si l'on prenait négativement les nombres de la forme $8n+1$ et $8n+5$, et positivement ceux de la forme $8n+3$ et $8n+7$, il faudrait leur donner des indices pour ainsi dire imaginaires ; en les introduisant dans le calcul des indices, on le réduirait à un algorithme très simple ; mais comme nous serions conduits trop loin si nous voulions traiter ce sujet en toute rigueur, nous réservons ce point pour une autre occasion, quand peut-être nous entreprendrons de traiter plus en détail la théorie des quantités imaginaires, qui nous semble jusqu'à présent n'avoir été réduite par personne à des notions claires. Les gens instruits parviendront aisément à cet algorithme ; ceux qui sont moins exercés pourront néanmoins se servir de cette table, comme ceux qui ne sont point au fait des connaissances modernes sur les logarithmes imaginaires se servent des logarithmes, pourvu qu'ils possèdent bien les principes antérieurement établis.

92. Presque tout ce qui a rapport aux résidus des puissances, suivant un module composé de plusieurs nombres premiers, peut se déduire de la théorie générale des congruences ; mais comme nous exposerons plus bas une manière de ramener les congruences dont le module est composé de plusieurs nombres premiers, à d'autres dont le module est un nombre premier, ou une puissance d'un nombre premier, nous ne nous arrêterons pas beaucoup ici sur cette matière. Nous nous contenterons d'observer que la belle propriété qui a lieu pour les autres modules, savoir : qu'il existe toujours des nombres dont la période renferme tous les nombres premiers avec le module, n'a pas lieu ici, excepté dans le seul cas où le module est double d'un nombre premier, ou d'une puissance d'un nombre premier. En effet si l'on ramène le module m à la forme $A^a B^b C^c$ etc., A, B, C, etc. étant des nombres premiers différents, qu'on fasse en outre $A^{a-1}(A-1) = \alpha, B^{b-1}(B-1) = \beta, C^{c-1}(C-1) = \gamma$, etc. et que z soit un nombre premier avec m, on aura $z^\alpha \equiv 1 \pmod{A^a}, z^\beta \equiv 1 \pmod{B^b}$, etc. ; si donc μ est le plus petit nombre divisible par α, β, γ, etc., on aura $z^\mu \equiv 1$ suivant chacun des modules A^a, B^b, etc., et partant, suivant m qui est égal à leur produit ; mais excepté le cas où m est double d'un nombre premier ou d'une puissance d'un nombre premier, on a toujours $\mu < \alpha\beta\gamma$ etc., puisque les nombres α, β, etc. ne peuvent être premiers entre eux, ayant au moins le diviseur commun 2. Ainsi la période d'aucun nombre ne peut comprendre autant de termes qu'il y a de nombres premiers avec le module, et moindres que lui, puisque leur nombre est égal au produit $\alpha\beta\gamma$ etc. Ainsi, par exemple, pour $m = 1001 = 7.11.13$, la puissance 60 d'un nombre quelconque premier avec m, est congrue à l'unité, puisque 60 est le plus petit nombre divisible à-la-fois par 6, 10 et 12. Le cas où le module est double d'un nombre premier ou d'une puissance d'un nombre premier, est tout-à-fait semblable à celui où le module est un nombre premier ou une puissance d'un nombre premier.

93. Nous avons déjà cité en plusieurs endroits les ouvrages dans lesquels les autres géomètres ont parlé du sujet que nous avons traité dans cette section-ci ; mais nous renvoyons ceux qui voudraient avoir plus de détails que le désir d'abréger ne nous a permis d'en donner, aux ouvrages suivants d'Euler, recommandables par la perspicacité qui a toujours distingué ce grand homme.

Theoremata circa residua ex divisione potestatum relicta (*Comm. nov. Petrop. T.* VII, *p.* 49).

Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia. (*Ibid. T.* XVIII, *p.* 85).

On peut y joindre les dissertations 5 et 8 des *Opuscula analytica.* T. I.