NOUVELLES ANNALES DE MATHÉMATIQUES

G. FONTENÉ

Sur une congruence extraite de la congruence binôme, facteurs premiers de certains nombres

Nouvelles annales de mathématiques 4^e série, tome 12 (1912), p. 241-260

<http://www.numdam.org/item?id=NAM_1912_4_12__241_0>

[17a]

SUR UNE CONGRUENCE EXTRAITE DE LA CONGRUENCE BINOME, FACTEURS PREMIERS DE CERTAINS NOMBRES ;

PAR M. G. FONTENÉ.

1. J'ai proposé, dans les *Nouvelles Annales*, la question suivante (2137) dont une solution a été donnée : *En désignant par p un nombre premier, par x et y deux nombres premiers entre eux, un nombre de la forme*

$$\frac{x^p - y^p}{x - y} \quad \text{ou} \quad x^{p-1} + x^{p-2}y + \ldots + y^{p-1}$$

a tous ses diviseurs premiers de la forme $P = kp + 1$, *à l'exception du diviseur p qu'il admet dans l'hypothèse* $x - y = \text{mult. } p$, *dans cette hypothèse seulement, et qu'il admet alors une seule fois* (*en supposant* $p \neq 2$).

Dans une Note relative à cette question (1911, p. 70), M. E. Cahen, se plaçant dans l'hypothèse $y = 1$, indique qu'on peut obtenir un théorème plus général en remplaçant p par un nombre non premier n, et en substituant au polynome

$$x^{p-1} - x^{p-2} + \ldots + 1$$

le polynome $f^n(x)$ qui a pour racines les racines primitives de *l'équation* binome $x^n - 1 = 0$, et dont le premier coefficient est 1.

Je n'ai pas pu savoir si ces faits sont déjà connus. Quoi qu'il en soit, M. Cahen m'ayant indiqué la règle pour les diviseurs exceptionnels, j'en ai cherché (avec y

quelconque) une démonstration que je donne ici, parce qu'elle diffère sensiblement de celle à laquelle M. Cahen était arrivé.

2. Voici d'abord, avec les notations essentielles, l'indication de la marche que nous suivrons.

Soit $n = p^{\alpha} q^{\beta} r^{\gamma} \ldots$ un nombre dont les facteurs premiers sont $p, q, r, \ldots$: nous extrairons la congruence

$$(A) \qquad x^n - y^n \equiv 0 \pmod{P},$$

P étant premier, y étant supposé connu, de la congruence

$$(B) \qquad \frac{(x^n - y^n) \times \left(x^{\frac{n}{pq}} - y^{\frac{n}{pq}}\right) \ldots \times \left(x^{\frac{n}{pqrs}} - y^{\frac{n}{pqrs}}\right) \ldots}{\left(x^{\frac{n}{p}} - y^{\frac{n}{p}}\right)\left(x^{\frac{n}{q}} - y^{\frac{n}{q}}\right) \ldots \times \left(x^{\frac{n}{pqr}} - y^{\frac{n}{pqr}}\right) \ldots} \equiv 0 \pmod{P},$$

le premier nombre étant le polynome qui a pour racines les racines primitives de *l'équation* binome $x^n - y^n = 0$, et dont le premier coefficient est 1. Cette congruence est de la forme

$$x^N + A x^{N-1} y + \ldots + A x y^{N-1} - y^N \equiv 0 \pmod{P},$$

N étant l'indicateur de n, $N = \varphi(n)$, et nous la désignerons d'une manière abrégée par l'écriture

$$f_n(x, y) \equiv 0 \pmod{P};$$

on suppose, bien entendu, y non congru à zéro suivant le module P.

Nous chercherons (II) les conditions de possibilité de la congruence (B), et cette étude nous donnera des renseignements sur les facteurs premiers d'un nombre de la forme $f_n(x, y)$, x et y étant deux nombres pre-

miers entre eux ; la recherche en question est liée à l'étude préliminaire des congruences binomes dont le module est un facteur premier de l'exposant (I).

3. Le polynome $F(x, y)$ étant homogène en x et y, si l'on considère la congruence

$$F(x, y) \equiv 0 \pmod{P},$$

y étant donné, non multiple de P, à chaque valeur de x correspond un nombre ξ tel qu'on ait

$$y \times \xi \equiv x \pmod{P},$$

puisque x n'est pas multiple de P ; c'est le lemme du théorème de Fermat. La congruence devient, après suppression du facteur y^n,

$$F(\xi, 1) \equiv 0 \pmod{P}.$$

Cela permettrait de supposer $y = 1$. J'ai préféré laisser y quelconque, en vue de la symétrie.

I. — Sur les congruences binomes dont le module est un facteur premier de l'exposant.

Nous allons considérer les congruences

$$(A') \qquad x^n - y^n \equiv 0 \pmod{p},$$

$$(B') \qquad f_n(x, y) \equiv 0 \pmod{p},$$

le module p étant un facteur premier de l'exposant n. (Nous mettons un accent pour indiquer ce fait.)

4. Théorème I. — *Le module p étant un diviseur de n, et p^α étant la plus haute puissance de p qui divise n, on a*

$$(1) \qquad x^n - y^n \equiv \left(x^{\frac{n}{p^\alpha}} - y^{\frac{n}{p^\alpha}}\right)^{p^\alpha} \pmod{p},$$

cette notation indiquant que le premier membre est identiquement congru au second, c'est-à-dire que les coefficients des termes semblables, dans les deux membres, sont congrus (mod p).

En effet, dans le développement de la puissance qui est au second membre, les coefficients des termes autres que les deux termes extrêmes contiennent le facteur p : pour $p \neq 2$, les termes extrêmes sont x^n et $-y^n$, et, pour $p = 2$, le dernier terme est y^n ou $-y^n + 2y^n$.

[J'observe à ce propos que le théorème relatif au nombre des solutions d'une congruence à module premier compte chaque solution une seule fois, la congruence $x^p - x \equiv 0 \pmod p$ ayant ses p solutions distinctes.]

3. Théorème II. — *Dans les mêmes conditions, on a*

$$f_n \quad \left(\frac{f_n}{p^\alpha}\right)^{\varphi(p^\alpha)} \qquad (\mathrm{mod}\, p); \tag{2}$$

les deux membres sont du même degré, puisque l'on a

$$\varphi(n) = \varphi\left(\frac{n}{p^\alpha}\right) \times \varphi(p^\alpha).$$

Écrivons l'identité algébrique

$$f_n(x,y) \times \left(x^{\frac{n}{p}} - y^{\frac{n}{p}}\right)\left(x^{\frac{n}{q}} - y^{\frac{n}{q}}\right) \dots \left(x^{\frac{n}{pqr}} - y^{\frac{n}{pqr}}\right) \dots$$
$$- (x^n - y^n)\left(x^{\frac{n}{pq}} - y^{\frac{n}{pq}}\right) \dots \left(x^{\frac{n}{pqrs}} - y^{\frac{n}{pqrs}}\right) \dots = 0.$$

En posant

$$\frac{n}{p^\alpha} = h,$$

le théorème I donne pour le premier terme, relative-

ment au module p,

$$(\alpha)\qquad x^{\frac{n}{p}} - \ldots = (x^h - \ldots)^{p^{\alpha-1}},$$

$$(\beta)\qquad x^{\frac{n}{q}} - \ldots = \left(x^{\frac{h}{q}} - \ldots\right)^{p^{\alpha}}, \qquad \ldots.$$

$$(\gamma)\qquad x^{\frac{n}{pq^r}} - \ldots = \left(x^{\frac{h}{q^r}} - \ldots\right)^{p^{\alpha-1}}, \qquad \ldots.$$

$$(\delta)\qquad x^{\frac{n}{q^{rs}}} - \ldots = \left(x^{\frac{h}{q^{rs}}} - \ldots\right)^{p^{\alpha}}, \qquad \ldots,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots, \qquad \ldots.$$

et, pour le second terme,

$$(\alpha')\qquad x^n - y^n = (x^h - y^h)^{p^{\alpha}}, \qquad \ldots,$$

$$(\beta')\qquad x^{\frac{n}{pq}} - \ldots = \left(x^{\frac{h}{q}} - \ldots\right)^{p^{\alpha-1}}, \qquad \ldots.$$

$$(\gamma')\qquad x^{\frac{n}{q^r}} - \ldots = \left(x^{\frac{h}{q^r}} - \ldots\right)^{p^{\alpha}}, \qquad \ldots,$$

$$(\delta')\qquad x^{\frac{n}{pq^{rs}}} - \ldots = \left(x^{\frac{h}{q^{rs}}} - \ldots\right)^{p^{\alpha-1}}, \qquad \ldots,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots, \qquad \ldots.$$

Le premier membre de l'identité algébrique ci-dessus, quand on y remplace chaque binome par la puissance de binome qui lui est identiquement congrue (mod p), se transforme en un polynome identiquement congru à zéro (mod p). Ce polynome contient le facteur

$$\left[(x^h - y^h)\left(x^{\frac{h}{q}} - \ldots\right)\ldots\left(x^{\frac{h}{q^r}} - \ldots\right)\ldots\right]^{p^{\alpha-1}},$$

dans lequel le coefficient de la plus haute puissance de x est l'unité; en supprimant ce facteur, on a encore un polynome identiquement congru à zéro (mod p), comme le montre le mécanisme de la division. On a ainsi, en remplaçant $p^{\alpha-1}(p-1)$ par $\varphi(p^{\alpha})$,

$$f_n(x,y) \times \left[\left(x^{\frac{h}{q}} - \ldots\right)\ldots\left(x^{\frac{h}{q^{rs}}} - \ldots\right)\ldots\right]^{\varphi(p^{\alpha})} - \left[(x^h - y^h)\left(x^{\frac{h}{q^r}} - \ldots\right)\ldots\right]^{\varphi(p^{\alpha})} \equiv 0, \pmod{p}.$$

Le second terme étant divisible par le polynome qui multiplie f_n, on peut, comme ci-dessus, supprimer le facteur commun, et l'on obtient

$$f_n - (f_h)^{\varphi(p^\nu)} \equiv 0 \pmod{p};$$

c'est ce qu'il fallait établir.

[Le théorème II permet de retrouver le théorème I. Le binome $x^n - y^n$ est le produit des facteurs f relatifs aux diviseurs de n. En désignant par $\lambda, \mu, \ldots$ les diviseurs de $q^\beta r^\gamma \ldots$, les diviseurs de n sont

$$\begin{array}{llll} \lambda p^\alpha, & \lambda p^{\alpha-1}, & \ldots, & \lambda p, \quad \lambda, \\ \mu p^\alpha, & \mu p^{\alpha-1}, & \ldots, & \mu p, \quad \mu, \\ \ldots, & \ldots\ldots & \ldots & \ldots \quad \ldots \end{array}$$

en appliquant le théorème II, on voit que le binome $x^n - y^n$ est identiquement congru (mod p) au produit des polynomes

$$\begin{array}{ll} (f_\lambda)^{\varphi(p^\alpha)+\ldots+\varphi(p)+1} & \text{ou} \quad (f_\lambda)^{p^\nu}, \\ (f_\mu)^{p^\alpha}, & \ldots \end{array}$$

or le produit des polynomes $f_\lambda, f_\mu, \ldots$ est le binome $x^{\frac{n}{p^\alpha}} - y^{\frac{n}{p^\alpha}}$; le binome $x^n - y^n$ est donc identiquement congru (mod p) au polynome

$$\left(x^{\frac{n}{p^\nu}} - y^{\frac{n}{p^\nu}}\right)^{p^\nu}.$$

c'est le théorème I.]

Si l'on prend en particulier $n = p^\alpha$, on a l'identité

$$x^{\frac{n}{p}(p-1)} + x^{\frac{n}{p}(p-2)}\, y^{\frac{n}{p}} + \ldots + y^{\frac{n}{p}(p-1)} \equiv (x-y)^{\frac{n}{p}(p-1)} \pmod{p}.$$

La vérification formelle se réduit à faire voir que le nombre

$$C_{p^\lambda}^{p\lambda} - (-1)^\lambda,$$

avec $P = p^{\alpha-1}$, est un multiple de p ; j'ai proposé la question dans les *Nouvelles Annales*, et M. Bricard m'en a indiqué une solution qu'il doit publier.

6. Il résulte de ce qui précède que la congruence

$$(B') \qquad f_n(x,y) \equiv 0 \pmod{p},$$

le module étant un diviseur de n, a comme solutions les solutions de la congruence

$$(b') \qquad \frac{f_n}{p^\alpha}(x,y) \equiv 0 \pmod{p},$$

extraite de la congruence binome

$$(a') \qquad x^{\frac{n}{p^\alpha}} - y^{\frac{n}{p^\alpha}} \equiv 0 \pmod{p}.$$

Nous reviendrons au n° 10 sur la question de savoir à quelle condition la congruence (b') est possible.

II. — Etude des congruences (B). Application.

7. Reprenons les congruences

$$(A) \qquad x^n - y^n \equiv 0 \pmod{P},$$
$$(B) \qquad f_n(x,y) \equiv 0 \pmod{P},$$

en vue de chercher les conditions de possibilité de la seconde. En désignant par δ le plus grand commun diviseur de n et $P-1$, la congruence (A) admet δ solutions ; ce sont les solutions de la congruence

$$(\alpha) \qquad x^\delta - y^\delta \equiv 0 \pmod{P}.$$

1° Si δ est n, c'est-à-dire si l'on a

$$P - 1 = kn, \qquad P = kn + 1,$$

la congruence (A) a n solutions ; la congruence (B) a alors N solutions.

2° Si δ n'est pas n, c'est-à-dire si P n'est pas de la forme $kn+1$, la congruence (B) ne peut avoir comme solutions que des solutions de la congruence (α) ; *en général, elle n'a pas alors de solution.*

8. Le diviseur δ n'étant pas n, la congruence (B) est comprise dans la congruence

$$\frac{x^n - y^n}{x^\delta - y^\delta} \equiv 0 \pmod{P},$$

ou, en posant $n = \delta \times \theta$, $\theta \not\equiv 1$, dans la congruence

$$x^{\delta(\theta-1)} + x^{\delta(\theta-2)}y^\delta + x^{\delta(\theta-3)}y^{2\delta} + \ldots + y^{\delta(\theta-1)} \equiv 0 \pmod{P}.$$

Si la congruence (B) admet comme solution une solution de la congruence (α), cette solution vérifie *a fortiori* la congruence qu'on vient d'écrire, et l'on doit avoir, le nombre des termes de cette congruence étant θ,

$$\theta \times y^{\delta(\theta-1)} \equiv 0 \pmod{P};$$

il faut donc que P soit un diviseur de θ, un diviseur de $\frac{n}{\delta}$. Les modules exceptionnels P, pour lesquels la congruence (B) est possible, et qui ne sont pas de la forme $kn+1$, ne peuvent donc être que des diviseurs premiers de n, soit p, q, r, ...

9. Prenons $P = p$. Le plus grand commun diviseur δ de n et $p-1$ ne peut renfermer le facteur p ; c'est un diviseur de $\frac{n}{p^\alpha}$ ou $q^\beta r^\gamma \ldots$. La congruence

$$(\alpha') \qquad x^\delta - y^\delta \equiv 0 \pmod{p}$$

est alors comprise dans la congruence

$$(a') \qquad x^{\frac{n}{p^\alpha}} - y^{\frac{n}{p^\alpha}} \equiv 0 \pmod{p},$$

et il faut voir d'abord si la congruence

$$(B') \qquad f_n(x, y) \equiv 0 \pmod{p}$$

admet des solutions de la congruence (a'). On a vu au paragraphe I que cette congruence (B') a comme solutions les solutions de la congruence

$$(b') \qquad f_{\frac{n}{p^\alpha}}(x, y) \equiv 0 \pmod{p},$$

extraite de la congruence (a').

10. A quelle condition la congruence (b') aura-t-elle des solutions? C'est une question que nous avons laissée sans réponse à la fin du paragraphe I, et que nous pouvons maintenant résoudre. En appliquant à la congruence (b') ce qu'on a dit de la congruence (B), on voit que p ne peut être un module exceptionnel pour cette congruence (b') puisqu'il n'est pas un facteur premier de $\frac{n}{p^\alpha}$. La congruence (b') n'est donc possible que si $p-1$ est divisible par $\frac{n}{p^\alpha}$ ou $q^\beta r^\gamma \ldots$,

$$p - 1 = k\frac{n}{p^\alpha} = k \times q^\beta r^\gamma \ldots,$$

ce qui exige d'abord que p soit le plus grand des facteurs premiers de n; cette congruence (b') a alors autant de solutions qu'il y a d'unités dans son degré. [Le plus grand commun diviseur de n et $p-1$ étant $\delta = \frac{n}{p^\alpha}$, la congruence (a') ne diffère pas de la congruence (a').]

Le seul module exceptionnel pour la congruence

$f_n(x, y) \equiv 0$ est donc le plus grand des facteurs premiers du nombre n, soit p, à condition encore que $p - 1$ soit divisible par $\frac{n}{p^\alpha}$, c'est-à-dire que q^β, r^γ, ... soient des diviseurs de $p - 1$; et la congruence

$$f_n(x, y) \equiv 0 \pmod{p}$$

a alors comme solutions [multiples d'ordre $\varphi(p^\alpha)$] les solutions de la congruence

$$f_{\frac{n}{p^\alpha}}(x, y) \equiv 0 \pmod{p},$$

solutions en nombre égal au degré de cette dernière congruence.

[Soit $y = 1$. On a

$$x^n - 1 = \left(\frac{x^n}{x^{p^\alpha}} - 1\right)^{p^\alpha} \pmod{p}$$

et

$$f_n(x) \equiv \left(f_{\frac{n}{p^\alpha}}\right)^{\varphi(p^\alpha)} \pmod{p}.$$

En supposant que $p - 1$ est divisible par $\frac{n}{p^\alpha}$, les racines de la congruence

$$(B') \qquad f_n(x) \equiv 0 \pmod{p},$$

racines qui sont en nombre égal au degré de cette congruence, ne sont pas racines primitives de la congruence

$$(A') \qquad x^n - 1 \equiv 0 \pmod{p},$$

laquelle n'a pas de racine primitive. Par exemple, si $n = p$, la congruence

$$x^{p-1} + \ldots - 1 \equiv 0 \pmod{p}$$

ou

$$(x - 1)^{p-1} \equiv 0 \pmod{p}$$

admet la seule racine $x = 1$, qui n'est pas racine primitive de la congruence

$$x^p - 1 \equiv 0 \pmod{p}, \quad \text{ou} \quad (x-1)^p \equiv 0 \pmod{p}.$$

Mais on peut dire que les racines de la congruence (b'), pour $y = 1$, sont les racines primitives de la congruence (a'), le module p n'étant pas exceptionnel pour l'exposant $\frac{n}{p^\alpha}$ qui ne contient pas le facteur p.]

11. De là cette conséquence, que nous avions surtout en vue :

THÉORÈME. — *Un nombre de la forme*

$$f_n(x, y),$$

x et y étant deux nombres premiers entre eux, a tous ses diviseurs premiers de la forme

$$P = kn + 1,$$

si ce n'est qu'il peut admettre comme facteur premier le plus grand des facteurs premiers de n, soit p. Il l'admet si $p - 1$ est divisible par $\frac{n}{p^\alpha}$ ou $q^\beta r^\gamma \ldots$.

$$p - 1 = k\frac{n}{p^\alpha} = k \times q^\beta r^\gamma \ldots,$$

c'est-à-dire si q^β, r^γ, ... sont des diviseurs de $p - 1$, et si l'on prend pour x et y deux nombres satisfaisant à la congruence

$$(b') \qquad f_{\frac{n}{p^\alpha}}(x, y) \equiv 0 \pmod{p},$$

extraite de la congruence

$$(a') \qquad x^{\frac{n}{p^\alpha}} - y^{\frac{n}{p^\alpha}} \equiv 0 \pmod{p};$$

avec l'hypothèse faite sur $p-1$, *la congruence* (b') *donne, pour chaque valeur de* y, *autant de valeurs de* x *qu'il y a d'unité dans son degré* [racines primitives de la congruence (a'), quand on suppose $y=1$].

En effet, si P est un diviseur premier du nombre considéré, lequel diviseur ne peut exister dans y puisqu'il devrait alors exister dans x, premier avec y, la congruence

$$f_n(x, y) \equiv 0 \pmod{P},$$

dans laquelle on donne à y la valeur qu'il a dans l'expression ci-dessus, tandis que l'on regarde x comme une inconnue, est une congruence possible, puisqu'elle est satisfaite lorsqu'on donne à x la valeur qu'il a dans l'expression.

12. *Il y aurait lieu de rechercher si le facteur exceptionnel* p, *lorsqu'il existe dans le nombre* $f_n(x, y)$, *peut y entrer plusieurs fois.*

Je montrerai plus loin que, avec $n=p^\alpha$, il n'en est rien.

13. Les diviseurs premiers de la forme $kn+1$ sont des nombres impairs; par suite, *si* n *est impair,* k est pair, et l'on a

$$P = 2k'n - 1.$$

Ce fait est en relation avec le suivant. Le nombre n étant impair, on a

$$x^{2n} - y^{2n} = (x^n - y^n)[x^n - (-y)^n];$$

par suite, le polynome $f_{2n}(x, y)$ ne diffère pas du polynome $f_n(x, -y)$, ou encore le polynome $f_n(x, y)$ ne diffère pas du polynome $f_{2n}(x, -y)$. Dès lors, si P est un diviseur régulier pour les nombres de la forme

$f_n(x, y)$, c'est aussi un diviseur régulier pour les nombres de la forme $f_{2n}(x, y)$, et l'on a

$$P = k' 2n + 1.$$

14. Le nombre premier 2 sera un diviseur exceptionnel si n est une puissance de 2, auquel cas les nombres que l'on considère sont des formes suivantes :

$$x^2 + y^2, \qquad x^4 + y^4, \qquad x^8 + y^8, \qquad \ldots$$

x et y étant impairs. Ces nombres sont d'ailleurs simplement pairs (*voir* le n° **17**).

Ce cas excepté, le polynome $f_n(x, y)$ étant

$$x^N - A x^{N-1} y + \ldots + A x y^{N-1} + y^N,$$

le coefficient du terme en $x^{\frac{N}{2}} y^{\frac{N}{2}}$ est impair; car, s'il était pair, en prenant x et y impairs, on aurait un nombre pair, ce qui n'est pas.

III. — Cas particulier.

15. La question qui se pose au n° **7**, en tenant compte des n^{os} **8** et **9**, est celle de savoir si la congruence

$$(B') \qquad f_n(x, y) \equiv 0 \pmod{p}$$

admet des solutions d'une congruence

$$(\alpha') \qquad x^\delta - y^\delta \equiv 0 \pmod{p},$$

δ étant un diviseur de $\frac{n}{p^\alpha}$. Je vais traiter cette question dans l'hypothèse $n = p^\alpha$ indépendamment des faits qui font l'objet du paragraphe I. J'en profiterai pour résoudre, dans ce cas particulier, la question posée au n° **12**.

16. Si d'abord n est un nombre premier p, les congruences (A) et (B) sont, pour reprendre tout le raisonnement,

$$(A) \qquad x^p - y^p \equiv 0 \pmod{P},$$
$$(B) \qquad x^{p-1} + x^{p-2}y + \ldots + y^{p-1} \equiv 0 \pmod{P}.$$

Si $P-1$ n'est pas multiple de p, comme la congruence (A) n'admet alors que la solution $x = y$, la congruence (B) ne peut admettre que cette solution, et elle l'admet pour $P = p$. (On ne se préoccupe pas, dans le raisonnement actuel, de l'ordre de multiplicité des solutions, qui est indifférent.) On obtient donc le théorème du n° 1, sauf à montrer que le nombre $\frac{x^p - y^p}{x - y}$, qui admet le diviseur p dans l'hypothèse $x - y = \text{mult.}\, p$ l'admet alors une seule fois. On a, en effet,

$$N = \frac{x^p - y^p}{x - y} = \frac{(y+h)^p - y^p}{h}$$
$$= py^{p-1} + \frac{p(p-1)}{1.2} y^{p-2}h + \ldots + pyh^{p-2} + h^{p-1},$$

tous les coefficients, à l'exception du dernier, étant divisibles par p ; comme on suppose h multiple de p, le second membre est divisible par p, et l'on a

$$N : p = y^{p-1} + \frac{p(p-1)}{1.2 \cdot p} y^{p-2}h + \ldots + yh^{p-2} + h^{p-1} : p ;$$

en exceptant le cas $p = 2$, tous les termes du second membre, à partir du second, sont divisibles par h, donc par p, tandis que le premier terme y^{p-1} n'est pas divisible par p, et, par suite, le quotient $N : p$ n'admet plus le facteur p.

17. Soit maintenant $n = p^\alpha$. Les congruences (A)

et (B) sont

$$(A) \qquad x^n - y^n \equiv 0 \pmod{P},$$

$$(B) \qquad \frac{x^n - y^n}{x^{\frac{n}{p}} - y^{\frac{n}{p}}} \equiv 0 \pmod{P},$$

ou, en posant

$$X = x^{\frac{n}{p}}, \qquad Y = y^{\frac{n}{p}},$$

$$[A] \qquad X^p - Y^p \equiv 0 \pmod{P},$$

$$[B] \qquad X^{p-1} + X^{p-2}Y + \ldots + Y^{p-1} \equiv 0 \pmod{P};$$

on aura, d'ailleurs, à tenir compte du fait que x et y doivent fournir des valeurs pour x et y, et il ne faudrait pas substituer à l'étude des congruences (A) et (B) l'étude pure et simple des congruences [A] et [B].

Si P n'est pas de la forme $kn + 1$, la congruence (B) ne peut admettre qu'une solution d'une congruence de la forme

$$(\alpha) \qquad x^\delta - y^\delta \equiv 0 \pmod{P},$$

δ étant une puissance de p autre que n; on verra, comme dans le cas général, que P doit être un diviseur de $\frac{n}{\delta}$, ce qui exige $P = p$.

[On peut d'ailleurs modifier un peu le raisonnement du cas général : δ étant un diviseur de $\frac{n}{p}$, la congruence écrite ci-dessus est comprise dans la congruence

$$x^{\frac{n}{p}} - y^{\frac{n}{p}} \equiv 0 \quad \text{ou} \quad X - Y \equiv 0 \pmod{P};$$

la congruence (B) ou [B] est vérifiée par $X = Y$ si $P = p$ (cas précédent).]

Mais alors, $p - 1$ étant premier avec δ, la congruence

$$(\alpha') \qquad x^\delta - y^\delta \equiv 0 \pmod{p}$$

n'admet que la solution $x = y$. La congruence (B), en dehors de l'hypothèse $P = kn + 1$, n'est donc possible que dans l'hypothèse $P = p$, et n'admet alors que la solution $x = y$.

Donc : *En désignant par n une puissance d'un nombre premier p, par x et y deux nombres premiers entre eux, un nombre de la forme*

$$\frac{x^n - y^n}{x^{\frac{n}{p}} - y^{\frac{n}{p}}} \quad \text{ou} \quad x^{\frac{n}{p}(p-1)} + x^{\frac{n}{p}(p-2)} y^{\frac{n}{p}} + \ldots + y^{\frac{n}{p}(p-1)},$$

ou encore un nombre de la forme

$$\frac{X^p - Y^p}{X - Y} \quad \text{ou} \quad X^{p-1} + X^{p-2} Y + \ldots + Y^{p-1},$$

$$X = x^{\frac{n}{p}}, \qquad Y = y^{\frac{n}{p}},$$

a tous ses diviseurs premiers de la forme $P = kn + 1$, *à l'exception du diviseur p qu'il admet dans l'hypothèse* $x - y = \text{mult. } p$, *dans cette hypothèse seulement, et qu'il admet alors une seule fois (en supposant* $n \neq 2$*).*

Pour établir ce dernier point, rappelons que, X étant premier avec Y, $X - Y$ étant multiple de p, le nombre $\frac{X^p - Y^p}{X - Y}$ admet une seule fois le facteur premier p, en exceptant le cas $p = 2$. Voyons ce qui a lieu pour $p = 2$, X et Y étant x^2 et y^2, ou x^4 et y^4, ou x^8 et y^8, ..., avec x et y impairs. Le nombre considéré est ici $X + Y$, ou $x^{\frac{n}{2}} + y^{\frac{n}{2}}$, n étant une puissance de 2 autre que 2 lui-même, de sorte que $\frac{n}{2}$ est pair ; on a alors

$$X = (2h+1)^{\frac{n}{2}} = (4h'+1)^{\frac{n}{4}} = \text{mult. } 4 + 1 ;$$

d'où

$$X + Y = (2h+1)^{\frac{n}{2}} + (2k+1)^{\frac{n}{2}} = \text{mult. } 4 + 2,$$

et ce nombre est simplement pair. Le cas $n = 2$ fait donc seul exception.

IV. — Autre cas particulier.

18. Soit encore

$$n = pq,$$

p et q étant deux nombres premiers distincts.

Avec $P = p$, δ étant un diviseur de $\frac{n}{p}$, ou q, on a $\delta = 1$ ou q, et la question est de savoir si la congruence

$$(B') \qquad \frac{(x^{pq} - y^{pq})(x - y)}{(x^q - y^q)(x^p - y^p)} \equiv 0 \pmod{p}$$

admet des solutions de l'une des deux congruences

$$(\alpha') \qquad x - y \equiv 0, \qquad x^q - y^q \equiv 0 \pmod{p}.$$

D'abord, l'hypothèse $x = y$ ne vérifie pas la congruence (B'); celle-ci peut s'écrire, en effet,

$$\frac{x^{(p-1)q} + x^{(p-2)q}y^q + \ldots + y^{(p-1)q}}{x^{p-1} + x^{p-2}y + \ldots + y^{p-1}} \equiv 0 \pmod{p},$$

et, pour $x = y$, son premier membre se réduit à $y^{(p-1)(q-1)}$. Ce point réglé, reste l'hypothèse $\delta = q$; la congruence (B') est comprise dans la congruence

$$(B', P) \qquad \frac{x^{pq} - y^{pq}}{x^q - y^q} \equiv 0 \pmod{p},$$

laquelle se décompose en deux congruences seulement: la congruence (B'), d'une part, et la congruence

$$(P) \qquad \frac{x^p - y^p}{x - y} \equiv 0 \pmod{p},$$

d'autre part. Les solutions de la congruence

$$(Q) \qquad x^q - y^q \equiv 0 \pmod{p}$$

conviennent à la congruence (B', P) ; comme les solutions de cette congruence (Q), autres que la solution $x = y$, ne vérifient pas la congruence (P), elles vérifient la congruence (B').

Cette constatation est suffisante, sans qu'il soit nécessaire de démontrer que le premier membre de la congruence (B') est identiquement congru (mod p) au polynome

$$\left(\frac{x^q - y^q}{x - y}\right)^{p-1};$$

l'ordre de multiplicité des solutions de la congruence (B') est indifférent.

V. — Remarques.

19. Remarque I. — Reprenons la congruence

$$(A) \qquad x^n - y^n \equiv 0 \pmod{P},$$

dans l'hypothèse

$$P = kn + 1;$$

elle a alors n solutions. Si G est une racine primitive du nombre premier P, de sorte qu'on ait

$$G^{kn} \equiv 1 \pmod{P},$$

l'exposant kn étant le plus petit qu'on puisse donner à G pour avoir le reste 1, on peut écrire (1)

$$y = G^{\beta},$$

---

(1) La congruence $x^n - Y \equiv 0 \pmod{P}$ a n solutions si Y est tel qu'on ait

$$Y^{\frac{P-1}{n}} \equiv 1 \pmod{P};$$

on doit avoir pour cela $Y = G^{n\beta} = (G^{\beta})^n$.

et les n valeurs de x sont

$$x = G^{\alpha}, \qquad \alpha - \beta = \text{mult. de } k = 0, k, 2k, \ldots, (n-1)k;$$

on peut encore écrire

$$y = G^{k\mu+\rho}, \qquad x = G^{\lambda+\rho}, \qquad \lambda = 0, 1, 2, \ldots, n-1.$$

La congruence (B) a alors $\varphi(n)$ solutions, pour lesquelles la différence $\alpha - \beta$ est le produit de k par un nombre premier avec n et non supérieur à n, ou encore la différence $\lambda - \mu$ est un tel nombre.

Par exemple, si n est un nombre premier p, la congruence

$$x^{p-1} + x^{p-2}y + \ldots + y^{p-1} \equiv 0 \pmod{P}.$$

en supposant

$$P = kp + 1,$$

a $p - 1$ solutions ; on peut écrire

$$y = G^{\beta}, \qquad x = G^{\alpha},$$
$$\alpha - \beta = \text{mult. de } k \qquad (\alpha > \beta),$$

ou encore

$$y = G^{k\mu+\rho},$$
$$x = G^{\lambda+\rho},$$
$$\lambda = 0, 1, 2, \ldots, n-1 \qquad (\text{sauf } \mu).$$

20. Remarque II. — Dans un article dont l'idée première appartient à M. Bricard (*Nouvelles Annales*, 1910, p. 217) j'ai étudié directement les nombres de la forme $x^2 + xy - y^2$. L'idée essentielle est que les deux congruences

$$\begin{aligned} ab - a\lambda - \lambda^2 &\equiv 0 \\ bc + b\lambda - \lambda^2 &\equiv 0 \end{aligned} \pmod{n}$$

entraînent la congruence

$$ca - c\lambda - \lambda^2 \equiv 0,$$

en supposant λ premier avec n.

Cette remarque se généralise, et, pour cinq nombres a, b, c, d, e par exemple, les deux congruences

$$abcd + abc.\lambda + ab.\lambda^2 + a.\lambda^3 + \lambda^4 \equiv 0,$$
$$bcde + bcd.\lambda + bc.\lambda^2 + b.\lambda^3 + \lambda^4 \equiv 0$$

entraînent la congruence

$$cdea - cde.\lambda + cd.\lambda^2 + c.\lambda^3 + \lambda^4 = 0$$

et, par suite, deux autres congruences analogues, λ étant premier avec le module ; il suffit, pour le voir, d'éliminer b entre les deux premières congruences ; on ordonne par rapport à b, on multiplie la seconde congruence par $a + \lambda$, la première par λ, on retranche, on divise par b qui n'est pas congru à zéro puisque λ ne l'est pas, et l'on a

$$[cde + \lambda(cd + c\lambda + \lambda^2)](a + \lambda) - a(cd + c\lambda - \lambda^2)\lambda \equiv 0;$$

les termes $a\lambda(cd + c\lambda + \lambda^2)$ disparaissent, et l'on obtient la nouvelle congruence. Mais ce point de départ ne mène ici à rien, les choses étant trop complexes.