ANNALES SCIENTIFIQUES DE L'É.N.S.

ANDRÉ ROUSSEL

Sur le rattachement de certaines questions d'arithmétique à un principe d'extremum

Annales scientifiques de l'É.N.S. 3^e série, tome 63 (1946), p. 45-79

<http://www.numdam.org/item?id=ASENS_1946_3_63__45_0>

© Gauthier-Villars (Éditions scientifiques et médicales Elsevier), 1946, tous droits réservés.

L'accès aux archives de la revue « Annales scientifiques de l'É.N.S. » (http://www.elsevier.com/locate/ansens) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

SUR LE RATTACHEMENT

DE

CERTAINES QUESTIONS D'ARITHMÉTIQUE

A UN PRINCIPE D'EXTREMUM

PAR M. ANDRÉ ROUSSEL.

1. On peut rattacher de nombreux problèmes d'arithmétique à un principe d'extremum.

Nous nous proposons dans cet article de donner une application de cette méthode qui semble encore inédite.

Ce premier travail sera consacré à l'obtention de théorèmes traduisant sous une forme analytique relativement simple, des conditions nécessaires et suffisantes pour qu'un entier p soit premier. Notre point de départ sera le suivant :

Pour que p entier soit premier, il faut et il suffit que pour tout x appartenant à l'intervalle fermé $(2, p-1)$, *on ait*

$$u = \cos^2 \pi x \cos^2 \frac{\pi p}{x} < 1, \tag{1}$$

car on ne pourrait avoir

$$u = 1$$

que si les équations

$$\cos^2 \pi x = 1, \qquad \cos^2 \frac{\pi p}{x} = 1$$

avaient une solution commune en x; d'après la première des conditions précédentes, cette solution commune, x, serait un entier compris entre 2 et $p-1$ qui diviserait p d'après la seconde.

Soit alors $M(p)$ le maximum absolu de u quand x varie dans l'intervalle fermé $(2, p-1)$. La fonction u étant continue, la condition (1) équivaut à

$$M(p) < 1, \tag{1'}$$

et (1') exprime la condition nécessaire et suffisante pour que p soit premier.

Or il est clair que la méthode classique pour calculer M, ou pour traduire (1) par une condition ne dépendant que de p seul ne saurait aboutir ici. Ce procédé consisterait, en effet, à résoudre l'équation

$$u' = 0,$$

et à comparer entre elles les valeurs de u correspondant à ses racines. Il aboutirait finalement à réintroduire la définition purement arithmétique du nombre premier, à savoir que de tous les quotients $\frac{p}{k}(k \neq 1, p)$ aucun ne doit être entier et ne nous avancerait donc à rien.

Nous sommes ainsi conduit, à propos de la question que nous examinons, à poser le problème général suivant :

Existe-t-il d'autres procédés, en dehors de la méthode élémentaire classique que nous venons de rappeler, pour déterminer l'extremum absolu d'une fonction ?

Cette question ne semble par avoir été étudiée et nous ne connaissons dans cet ordre d'idées, qu'un théorème de Riesz qui soit antérieur à nos travaux actuels sur ce sujet.

Voici l'énoncé de cette proposition qui est très intéressante.

Soit $f(x)$ une fonction continue, non négative dans un intervalle fini (a, b). On a

$$\max f(x) = \lim_{m=\infty} \left\{ \int_a^b [f(x)]^m \, dx \right\}^{\frac{1}{m}}.$$

Ce théorème fournit ce que l'on pouvait appeler *un moyen direct* de calculer le maximum absolu de $f(x)$ et l'obtention de propositions analogues serait très importante à divers titres, et en particulier par le fait qu'elle auraient de nombreuses applications en théorie des nombres comme nous le montrerons dans ce travail et dans d'autres en préparation (1).

Nous avons d'ailleurs obtenu d'autres résultats dans cet ordre d'idées (*voir* la note citée), mais dans ce premier Mémoire nous utiliserons le théorème de Riesz, ou plutôt nous nous en inspirerons en nous bornant ici à mentionner le problème général ci-dessus.

Pour être complet, nous allons donner la démonstration de ce théorème de Riesz, quoique ce ne soit pas strictement nécessaire à l'exposé qui va suivre et qui contient tout ce qui est nécessaire à son intelligence, mais l'intérêt de cette proposition peu connue et le caractère très simple de sa démonstration nous paraissent justifier ce rappel.

---

(1) A. ROUSSEL, *Sur un procédé de traduction analytique de propriétés arithmétiques* (*C. R. Acad. Sc.*, t. 219, 1944, p. 568.

Soit donc $f(x)$ continue, non négative et non identiquement nulle dans l'intervalle (a, b). On supposera $a < b$. A tout ε positif on peut faire correspondre un sous-intervalle (α, β) de (a, b) tel que dans (α, β) ou $(\alpha < \beta)$ on ait

$$f(x) \geqq \mathrm{M} - \frac{\varepsilon}{2},$$

M étant le maximum absolu de f dans (a, b).

Il vient donc

$$\int_\alpha^\beta \left(\mathrm{M} - \frac{\varepsilon}{2}\right)^m dx < \int_\alpha^\beta [f(x)]^m dx < \int_a^b [f(x)]^m dx < \int_a^b \mathrm{M}^m dx.$$

Posons, pour simplifier,

$$\mathrm{I}_m = \int_a^b [f(x)]^m dx,$$

on a donc

$$(\beta - \alpha)\left(\mathrm{M} - \frac{\varepsilon}{2}\right)^m < \mathrm{I}_m < (b - a)\mathrm{M}^m,$$

d'où

$$(\beta - \alpha)^{\frac{1}{m}}\left(\mathrm{M} - \frac{\varepsilon}{2}\right) < \mathrm{I}^{\frac{1}{m}} < (b - a)^{\frac{1}{m}}\mathrm{M}.$$

α et β dépendant en général de ε, mais non de m, quand m tend vers $+\infty$, les quantités

$$(\beta - \alpha)^{\frac{1}{m}} \quad \text{et} \quad (b - a)^{\frac{1}{m}}$$

tendent vers un.

On peut alors trouver un nombre m_0 assez grand, tel que l'inégalité

$$m \geqq m_0$$

entraîne

$$\mathrm{M} - \varepsilon < \mathrm{I}_m^{\frac{1}{m}} < \mathrm{M} + \varepsilon,$$

ε étant arbitraire, cela revient à dire que si m tend vers $+\infty$, $\mathrm{I}_m^{\frac{1}{m}}$ a une limite et que cette limite est égale à M.

Le théorème dont nous venons de rappeler la démonstration est susceptible de diverses généralisations. Il s'étend ainsi sans peine aux fonctions de plusieurs variables. En outre f peut être supposée seulement intégrable au sens de Lebesgue, M désignant alors sa borne supérieure dans (a, b). On établirait, de même, la proposition un peu plus générale

$$\mathrm{M} = \lim_{m=+\infty} \left\{ \frac{\int_a^b [f(x)]^m g(x)\, dx}{\int_a^b g(x)\, dx} \right\}^{\frac{1}{m}} \qquad (g \geqq 0),$$

mais nous n'insisterons pas ici sur ces propositions que ne constituent pas des généralisations essentielles du théorème, et nous ne parlerons pas des modifications à peu près évidentes qu'il y a lieu de faire subir à son énoncé pour en déduire un procédé de détermination du *minimum absolu* de f.

Ces préliminaires étant posés, nous allons maintenant aborder le sujet de cette étude.

2. Revenons au problème posé au début du paragraphe précédent. Soit p *un entier que nous supposerons premier.* Considérons la fonction u définie par la relation (1). Son maximum M est alors inférieur à 1 au sens strict. Nous allons trouver d'abord une limite supérieure de M, elle-même inférieure à 1.

Nous commencerons par préciser la valeur maximum de

$$\cos^2 \frac{\pi p}{x}$$

quand x varie dans un intervalle $\left(k - \frac{\alpha}{p}, k + \frac{\alpha}{p}\right)$, k désignant un entier appartenant à l'intervalle fermé $(2, p-1)$ et α un nombre compris entre 0 et 1 qui sera précisé dans la suite.

Pour k égal à 2, on ferait varier x seulement dans l'intervalle $\left(2, 2 + \frac{\alpha}{p}\right)$ et pour $k = p - 1$, dans l'intervalle $\left(p - 1 - \frac{\alpha}{p}, p - 1\right)$.

Effectuons la division de p par k

$$p = kq + r \qquad \text{avec } 1 \leq r \leq k - 1,$$

d'où

$$\cos^2 \frac{\pi p}{k} = \cos^2 \frac{\pi r}{k}.$$

Or

$$\frac{1}{p} < \frac{1}{p-1} \leq \frac{1}{k} \leq \frac{r}{k} \leq \frac{k-1}{k} = 1 - \frac{1}{k} \leq 1 - \frac{1}{p-1} < 1 - \frac{1}{p},$$

et l'arc

$$\frac{\pi r}{k}$$

est compris entre les arcs supplémentaires

$$\frac{\pi}{p-1} \quad \text{et} \quad \pi - \frac{\pi}{p-1}.$$

Donc

$$\cos^2 \frac{\pi r}{k} < \cos^2 \frac{\pi}{p-1} < \cos^2 \frac{\pi}{p}.$$

Par conséquent pour k compris entre 2 et $p - 1$, on a

$$\cos^2 \frac{\pi p}{k} \leq \cos^2 \frac{\pi}{p-1} < \cos^2 \frac{\pi}{p}. \tag{2}$$

Ce résultat appelle deux remarques :

1° il subsiste si p n'est pas premier pourvu que k ne divise pas p;

2° si N désigne un nombre au moins égal à p, on a, dans les mêmes conditions,

$$\cos^2\frac{\pi p}{k} < \cos^2\frac{\pi}{N}. \tag{2'}$$

Soit maintenant la fonction

$$y = \cos^2\frac{\pi p}{x}.$$

On a

$$y' = \frac{2\pi p}{x^2}\sin\frac{2\pi p}{x},$$

d'où

$$|y'| \leq \frac{2p\pi}{x^2} \leq \frac{2p\pi}{4} < 2p$$

Quand x varie dans l'intervalle $\left(k-\frac{\alpha}{p},\ k+\frac{\alpha}{p}\right)$, on a sûrement

$$\cos^2\frac{\pi p}{x} \leq \cos^2\frac{\pi p}{k} + 2p\frac{2\alpha}{p},$$

d'où

$$\cos^2\frac{\pi p}{x} \leq \cos^2\frac{\pi}{p-1} + 4\alpha. \tag{3}$$

Dans le second membre de (3), on peut d'ailleurs remplacer $\cos^2\frac{\pi}{p-1}$ par une quantité supérieure, $\cos^2\frac{\pi}{p}$ ou $\cos^2\frac{\pi}{N}$, par exemple.

Nous allons chercher à déterminer α de façon que

$$\cos^2\frac{\pi}{p-1} + 4\alpha < 1-\lambda, \tag{4}$$

λ étant un nombre compris entre 0 et 1 que nous préciserons prochainement. L'inégalité (4) peut s'écrire

$$4\alpha < \sin^2\frac{\pi}{p-1} - \lambda. \tag{5}$$

Or on voit facilement que, pour $0 \leq x \leq \frac{\pi}{2}$, on a

$$\sin x > \frac{2}{\pi}x,$$

la portion correspondante de la courbe $y = \sin x$ restant au-dessus de la droite de coefficient angulaire égal à $\frac{2}{\pi}$. Donc, pour les mêmes valeurs de x,

$$\sin^2 x > \frac{4}{\pi^2}x^2.$$

Par conséquent

$$\sin^2\frac{\pi}{p-1} > \frac{4}{(p-1)^2} > \frac{4}{p^2}.$$

L'inégalité (5) sera vraie, *a fortiori*, si

$$4\alpha < \frac{4}{(p-1)^2} - \lambda.$$

Nous prendrons alors

$$\lambda = \frac{2}{(p-1)^2};$$

(5) et (6) seront alors vraies en prenant

$$\alpha \leq \frac{1}{2(p-1)^2}.$$

Finalement, si x varie dans l'intervalle $\left(k - \frac{\alpha}{p},\ k + \frac{\alpha}{p}\right)$ avec

$$\alpha = \frac{1}{2(p-1)^2},$$

on aura

$$\cos^2\frac{\pi p}{x} \leq 1 - \frac{2}{(p-1)^2}, \tag{6}$$

ou encore, N désignant un nombre supérieur ou égal à p,

$$\cos^2\frac{\pi p}{x} < 1 - \frac{2}{N^2}. \tag{6'}$$

Si p n'est pas premier ces résultats subsistent pourvu que k ne soit pas un de ses diviseurs (autre que 1 et p).

Ceci posé, il est facile de trouver, pour p premier, une limite supérieure $M(p)$, inférieure à 1 quand x varie dans tout l'intervalle $(2, p-1)$.

Soient deux entiers consécutifs k et $k+1$ de cet intervalle; prenons autour de chacun d'eux un intervalle d'amplitude δ telle que

$$\frac{\delta}{2} = \frac{\alpha}{p} = \frac{1}{2p(p-1)^2}.$$

Quand x varie dans l'intervalle (x_1, x_2) où

$$x_1 = k + \frac{\delta}{2}, \qquad x_2 = k + 1 - \frac{\delta}{2}.$$

On a

$$\cos^2\pi x < \cos^2\frac{\pi\delta}{2} = \cos^2\frac{\pi}{2p(p-1)^2}.$$

Or

$$\cos^2\frac{\pi}{2p(p-1)^2} = 1 - \sin^2\frac{\pi}{2p(p-1)^2} < 1 - \frac{4}{\pi^2}\,\frac{\pi^2}{4p^2(p-1)^4},$$

donc quand x varie dans (x_1, x_2), on a

$$\cos^2 \pi x < 1 - \frac{1}{p^2(p-1)^4}$$

et, *a fortiori*

$$u = \cos^2 \pi x \cos^2 \frac{\pi p}{x} < 1 - \frac{1}{p^2(p-1)^4}. \tag{7}$$

Ce résultat reste valable quand x varie dans tout l'intervalle fermé $(k, k+1)$, car dans les parties de ce dernier intervalle non comprises dans (x_1, x_2), c'est-à-dire dans les intervalles $\left(k, k+\frac{\alpha}{p}\right)$ et $\left(k+1-\frac{\alpha}{p}, k+1\right)$, on a, d'après (6),

$$u \leq \cos^2 \frac{\pi p}{x} < 1 - \frac{2}{(p-1)^2} < 1 - \frac{1}{p^2(p-1)^4},$$

car, pour $p \geq 3$,

$$\frac{2}{(p-1)^2} > \frac{1}{p^2(p-1)^4}.$$

Le nombre k étant un entier quelconque compris entre 2 et $p-1$, l'inégalité (7) est vraie dans *tout* l'intervalle fermé $(2, p-1)$. On voit donc que :

La condition nécessaire et suffisante pour que l'entier p soit premier est que pour toute valeur de x appartenant à l'intervalle fermé $(2, p-1)$, *on ait*

$$u = \cos^2 \pi x \cos^2 \frac{\pi p}{x} \leq 1 - \frac{1}{p^2(p-1)^4}. \tag{7'}$$

Nous venons de démontrer que la condition était nécessaire.

Elle est évidemment suffisante, car si elle est vraie, p est sûrement premier, sinon u atteindrait la valeur *un* et ne resterait donc pas toujours inférieur à un nombre inférieur à l'unité.

On peut remplacer dans le second membre de (7') la fraction

$$\frac{1}{p^2(p-1)^4}$$

par une quantité plus petite, par exemple

$$\frac{1}{p^6} \quad \text{ou} \quad \frac{1}{N^6},$$

cette dernière comportant la supposition $p \leq N$, et la condition nécessaire et suffisante pour que p soit premier peut se traduire par

$$u = \cos^2 \pi x \cos^2 \frac{\pi p}{x} < 1 - \frac{1}{p^6} \qquad (2 \leq x \leq p-1), \tag{8}$$

ou, si $p \leq N$,

$$u = \cos^2 \pi x \cos^2 \frac{\pi p}{x} < 1 - \frac{1}{N^6} \qquad (2 \leq x \leq p-1). \tag{8'}$$

On peut encore remplacer les premiers membres de (7'), (8) et (8') par M(p), cette notation désignant, comme nous l'avons déjà indiqué, le maximum absolu de la fonction u quand x varie de 2 à $p-1$.

Terminons ce paragraphe en indiquant une limite inférieure de M(p). Faisons $x=3$, dans u. Alors

$$\frac{p}{3}=q+\frac{r}{3}, \qquad r=1 \text{ ou } 2,$$

d'où

$$u(3)=\cos^2 3\pi \cos^2\frac{\pi p}{3}=\frac{1}{4}.$$

Donc

$$\mathrm{M}(p)\geqq\frac{1}{4}. \tag{9}$$

3. Considérons maintenant la fonction

$$u=\cos^2\pi x\cos^2\frac{\pi p}{x} \qquad (2\leqq x\leqq p-1), \tag{10}$$

p étant, pour le moment du moins, un entier quelconque. Nous avons

$$u'=-2\pi\sin\pi x\cos\pi x\cos^2\frac{\pi p}{x}+2\pi\frac{p}{x^2}\cos^2\pi x\cos\pi\frac{p}{x}\sin\pi\frac{p}{x}$$

ou

$$u'=-\pi\sin 2\pi x\cos^2\frac{\pi p}{x}+\frac{\pi p}{x^2}\cos^2\pi x\sin\frac{2\pi p}{x},$$

$$|u'|<\pi+\frac{\pi p}{4}=\pi\frac{p+4}{4}<p+4\leqq 2p, \tag{11}$$

car nous pouvons sans inconvénients supposer $p\geqq 4$.

Considérons la courbe (C) représentant les variations de la fonction définie par (10). Soient toujours M le maximum absolu de u dans l'intervalle fermé $(2, p-1)$ et μ un nombre positif arbitraire mais inférieur à M. Cette dernière condition sera certainement satisfaite si l'on prend $\mu<\frac{1}{4}$, d'après l'inégalité (9). Il existe au moins un intervalle compris dans $(2, p-1)$ où l'on a

$$\mathrm{M}-\mu\leqq u\leqq \mathrm{M}, \tag{12}$$

soient (x_0, M) les coordonnées du point K de C correspondant au maximum de u. Par K menons la droite D de coefficient angulaire $2p$. Elle ne rencontre C qu'au seul point K et sa portion comprise entre K et l'axe des x est tout entière au-dessous de C. Si nous considérons alors le triangle rectangle déterminé par les trois droites

$$x=x_0; \qquad y=\mathrm{M}-\mu, \tag{D}$$

la base ν de ce triangle est telle que

$$\nu = \frac{\mu}{2p} \tag{13}$$

(c'est de la base parallèle à Ox dont il est question). Il est alors clair que les inégalités (12) sont satisfaites au moins pour un intervalle de Ox d'amplitude supérieure à ν. (Ceci suppose le maximum M_1 atteint pour une valeur $x_0 \neq 2$, mais dans ce cas la même conclusion subsisterait en remplaçant D par une droite analogue mais de pente $-2p$.)

4. Soit maintenant l'expression

$$I_m = \left\{ \int_2^{p-1} \cos^{2m} \pi x \cos^{2m} \frac{\pi p}{x}\, dx \right\}^{\frac{1}{m}}. \tag{14}$$

On a

$$I_m \leq \left\{ \int_2^{p-1} M^m\, dx \right\}^{\frac{1}{m}} = (p-3)^{\frac{1}{m}} M;$$

d'autre part, μ étant un nombre positif quelconque, inférieur à M, on a

$$\cos^{2m} \pi x \cos^{2m} \frac{\pi p}{x} > (M - \mu)^m$$

sur un intervalle au moins égal à $\frac{\mu}{2p}$ d'après (13). Il vient donc

$$\int_2^{p-1} \cos^{2m} \pi x \cos^{2m} \frac{\pi p}{x}\, dx > (M - \mu)^m \frac{\mu}{2p}.$$

On a finalement la double inégalité

$$(M - \mu) \left(\frac{\mu}{2p} \right)^{\frac{1}{m}} < I_m < M (p-3)^{\frac{1}{m}},$$

ou encore

$$(M - \mu) \left(\frac{\mu}{2p} \right)^{\frac{1}{m}} - M < I - M < M (p-3)^{\frac{1}{m}} - M. \tag{15}$$

Occupons-nous d'abord de la seconde des inégalités (15). Cherchons à déterminer m de façon que

$$M (p-3)^{\frac{1}{m}} - M < 2\mu, \tag{16}$$

la valeur de μ devant être précisée ultérieurement. Posons

$$(p-3)^{\frac{1}{m}} = 1 + \beta \qquad (\beta > 0),$$

(16) équivaut à

$$p < \frac{2\mu}{M}. \tag{17}$$

On a toujours $M \leq 1$, donc

$$\frac{2\mu}{M} \geq 2\mu.$$

Pour satisfaire à (17) et par suite à (16), il suffira de prendre

$$\beta < 2\mu,$$

ou

$$(p-3)^{\frac{1}{m}} - 1 < 2\mu; \tag{18}$$

Or

$$(p-3)^{\frac{1}{m}} - 1 = e^{\frac{\operatorname{Log}(p-3)}{m}} - 1 < \frac{1}{m}\operatorname{Log}(p-3)\, e^{\frac{\operatorname{Log}(p-3)}{m}}. \tag{19}$$

Prenons

$$m > \operatorname{Log} p > \operatorname{Log}(p-3). \tag{20}$$

Alors

$$e^{\frac{\operatorname{Log}(p-3)}{m}} < e^1 < 3,$$

et (19) donne, d'après (20),

$$(p-3)^{\frac{1}{m}} - 1 < \frac{3\operatorname{Log} p}{m};$$

pour satisfaire à (16), il suffira de prendre

$$\frac{3\operatorname{Log} p}{m} < 2\mu$$

ou

$$m > \frac{3}{2}\frac{\operatorname{Log} p}{\mu}, \tag{21}$$

(21) entraînera (20) puisque μ est inférieur à 1 et par conséquent entraînera aussi (16).

Nous prendrons

$$2\mu = \frac{1}{2p^6}. \tag{22}$$

De sorte que, si

$$m \geq 6p^6 \operatorname{Log} p, \tag{23}$$

On aura, d'après (15),

$$I_m < M + \frac{1}{2p^6}. \tag{24}$$

Remarquons que si l'on supposait

$$p \leq N,$$

et si l'on remplaçait la valeur (22) de μ par

$$\frac{1}{2N^6},$$

(16) sera alors satisfaite, à condition de prendre

$$m \geqq 6N^6 \operatorname{Log} N, \tag{25}$$

et (24) deviendrait (pour $p \leqq N$)

$$I_m < M + \frac{1}{2N^6}. \tag{26}$$

Si p est maintenant supposé premier, (24) et (26) donnent, pour m satisfaisant aux inégalités (23) ou (25),

$$I_m < 1 - \frac{1}{2p^6} \tag{27}$$

ou

$$I_m < 1 - \frac{1}{2N^6}. \tag{28}$$

Il suffit pour le voir de se reporter aux inégalités (8) et (8′). Il y a lieu de noter que les inégalités (27) et (28) ont lieu au sens strict.

Nous allons maintenant montrer que, si p n'est pas premier, on peut prendre m assez grand pour que l'on ait

$$I_m > 1 - \frac{1}{2p^6}. \tag{29}$$

Pour cela, considérons la première des inégalités (15) et cherchons à partir de quelles valeurs de m on a

$$-2\mu_1 < (M - \mu_1)\left(\frac{\mu_1}{2p}\right)^{\frac{1}{m}} - M, \tag{30}$$

μ_1 étant un nombre positif inférieur à M $\left(\text{cette condition étant sûrement remplie si } \mu_1 < \frac{1}{4}\right)$, qui sera précisé par la suite.

Posons

$$\left(\frac{\mu_1}{2p}\right)^{\frac{1}{m}} = 1 - \alpha \qquad (\alpha > 0),$$

l'inégalité (30) équivaut à

$$\alpha < \frac{\mu_1}{M - \mu_1}, \tag{31}$$

et (31) sera satisfaite si l'on a

$$\alpha < \mu_1. \tag{32}$$

Car le dénominateur du second membre de (31) est inférieur à un. Nous avons alors, en vertu de la première inégalité (15),

$$I_m > M - 2\mu_1 = 1 - 2\mu_1, \tag{33}$$

puisque nous supposons actuellement p non premier, ce qui entraîne $M = 1$. Prenons

$$2\mu_1 = \frac{1}{2p^6},$$

il faut déterminer m de façon que

$$\alpha = 1 - \left(\frac{1}{8p^7}\right)^{\frac{1}{m}} < \frac{1}{4p^6}. \tag{34}$$

Or

$$\alpha = 1 - \left(\frac{1}{8p^7}\right)^{\frac{1}{m}} = 1 - e^{\frac{1}{m}\operatorname{Log}\frac{1}{8p^7}} < \frac{1}{m}\left|\operatorname{Log}\frac{1}{8p^7}\right| e^{\left|\frac{1}{m}\operatorname{Log}\frac{1}{8p^7}\right|}.$$

Prenons

$$\frac{1}{m}\left|\operatorname{Log}\frac{1}{8p^7}\right| < 1,$$

c'est-à-dire

$$m > \operatorname{Log}(8p^7), \tag{35}$$

d'où

$$\alpha < \frac{1}{m}\left|\operatorname{Log}\frac{1}{8p^7}\right| e^1 < \frac{3}{m}\operatorname{Log}(8p^7);$$

(35) étant supposée satisfaite, il suffira pour satisfaire à (34) de prendre

$$\frac{3}{m}\operatorname{Log}(8p^7) < \frac{1}{4p^6}$$

ou

$$m > 4p^6 \operatorname{Log}(8p^7). \tag{36}$$

Or (36) entraîne (34). Donc, si m satisfait à l'inégalité (36), l'inégalité (33) sera satisfaite et l'on aura

$$I_m > 1 - \frac{1}{2p^6}.$$

Si, nous plaçant toujours dans le cas où p n'est pas premier, on prenait

$$2\mu_1 = \frac{1}{2N^6},$$

l'inégalité

$$m > 4N^6 \operatorname{Log}(8N^7) \tag{37}$$

entraînerait

$$I_m > 1 - \frac{1}{2N^6}.$$

D'autre part

$$4p^6 \operatorname{Log}(8p^7) > 6p^6 \operatorname{Log} p;$$

le second membre de cette dernière inégalité n'est autre que le second membre de (23).

Donc, finalement, si l'on prend pour m un nombre satisfaisant à la condition (36), on aura, si p est premier,

$$I_m < 1 - \frac{1}{2p^6}$$

et si p n'est pas premier

$$I_m > 1 - \frac{1}{2p^6}.$$

Si l'on considère les entiers p inférieurs à un même nombre fixe N, d'ailleurs quelconque, la condition (37) entraînerait, si p est premier,

$$I_m < 1 - \frac{1}{2N^6}$$

et, dans le cas contraire,

$$I_m > 1 - \frac{1}{2N^6}.$$

Nous sommes ainsi conduit à énoncer les deux théorèmes suivants

Pour que le nombre entier p soit premier, il faut et il suffit que l'on ait

$$\int_2^{p-1} \cos^{2m} \pi x \cos^{2m} \frac{\pi p}{x}\, dx < \left(1 - \frac{1}{2p^6}\right)^m, \tag{38}$$

où m désigne un nombre fixe, puis arbitrairement une fois pour toutes parmi ceux qui satisfont à la condition

$$m \geqq 4p^6 \operatorname{Log}(8p^7).$$

Si l'on considère seulement les nombres entiers inférieurs à un nombre donné N, d'ailleurs arbitraire, on obtient l'énoncé suivant :

Pour que l'entier $p \leqq N$ *soit premier, il faut et il suffit que l'on ait*

$$\int_2^{p-1} \cos^{2m} \pi x \cos^{2m} \frac{\pi p}{x}\, dx < \left(1 - \frac{1}{2N^6}\right)^m, \tag{39}$$

m désignant un nombre fixe, choisi arbitrairement une fois pour toutes parmi ceux qui satisfont à la condition

$$m \geqq 4N^6 \operatorname{Log}(8N^7).$$

L'intérêt du second énoncé consiste en ce que l'exposant m peut être pris indépendant de p. Insistons sur le fait qu'il suffit de savoir que (38) ou (39)

est vraie pour *une seule valeur de m* [pourvu que celle-ci satisfasse à la condition appropriée, (36) ou (37) suivant qu'il s'agit du premier énoncé ou du second] pour pouvoir affirmer que p est premier.

Remarque. — Si $p \geqq 4$, on a

$$\operatorname{Log}(8p^7) = \operatorname{Log}8 + 7\operatorname{Log}p < 4p;$$

cette inégalité est vraie pour $p = 4$. En effet

$$\operatorname{Log}8 + 7\operatorname{Log}4 < 13 < 4 \times 4.$$

La dérivée du premier membre de la relation à démontrer est égale à $\frac{7}{p}$ et reste inférieure à celle du second membre qui est 4. Il en résulte que ce premier membre reste inférieur au second pour $p > 4$, puisque cette circonstance se présente pour $p = 4$ et en vertu de la relation entre leurs dérivées.

On pourra donc, dans les énoncés précédents, remplacer m par une quantité plus grande et prendre ainsi

$$m \geqq 16p^7$$

dans le premier énoncé et

$$m \geqq 16\mathrm{N}^7$$

dans le second. On pourrait même se borner à prendre

$$m \geqq p^9 \qquad \text{ou} \qquad m > \mathrm{N}^9$$

car, pour $p \geqq 4$, on a

$$p^2 \geqq 16 \qquad \text{et} \qquad p^9 > 16p^7.$$

5. Il est facile de généraliser les considérations précédentes et d'en tirer une condition nécessaire et suffisante pour que deux entiers r et s $(r < s)$ soient premiers entre eux.

En effet, pour que r et s soient premiers entre eux, il faut et il suffit que l'on ait

$$v = \cos^2\pi x \cos^2\frac{\pi r}{x}\cos^2\frac{\pi s}{x} < 1, \tag{40}$$

quand x varie dans l'intervalle $(2, s)$, intervalle qu'on pourrait d'ailleurs réduire à $(2, r)$; mais nous conserverons le premier intervalle, ce qui permet d'obtenir un peu plus de simplicité.

Nous allons développer l'étude de la condition (40). Supposons r et s premiers entre eux. On démontre d'abord, comme au paragraphe 2, que si k est un entier quelconque, on a toujours dans cette hypothèse

$$\cos^2\frac{\pi r}{k}\cos^2\frac{\pi s}{k} < \cos^2\frac{\pi}{s}. \tag{41}$$

soit alors la fonction

$$y = \cos^2 \pi \frac{r}{x} \cos^2 \pi \frac{s}{x}.$$

On a

$$|y'| < \pi \frac{r+s}{4} < 2s,$$

et l'on voit facilement, comme plus haut, que, si x varie dans l'intervalle

$$\left(k - \frac{\alpha}{s}, k + \frac{\alpha}{s}\right) \qquad \text{avec } \alpha = \frac{1}{2s^2},$$

on aura, au sens strict,

$$\cos^2 \frac{\pi r}{x} \cos^2 \frac{\pi s}{x} < 1 - \frac{2}{s^2}, \tag{42}$$

et, en achevant le raisonnement comme au paragraphe 3, on voit facilement que, dans *tout l'intervalle* $(2, s)$, *on aura*

$$v = \cos^2 \pi x \cos^2 \frac{\pi r}{x} \cos^2 \frac{\pi s}{x} < 1 - \frac{1}{s^6}. \tag{43}$$

On peut dire que cette condition (43) exprime une condition nécessaire et suffisante pour que r et s soient premiers entre eux : elle est bien nécessaire d'après ce que nous venons de voir et elle est suffisante, car si r et s n'étaient pas premiers entre eux, v atteindrait au moins une fois la valeur 1.

Remarquons enfin que le maximum de v, *a priori* non nul, est supérieur à $\frac{1}{16}$. Il suffit pour le voir de remplacer x par 3 dans l'expression de v. Ceci posé, un calcul facile montre que

$$v' < 3s. \tag{44}$$

Si M désigne alors le maximum de v quand x varie dans $(2, s)$ et μ un nombre positif inférieur à M $\left(\text{ce qui aura lieu si l'on prend } \mu < \frac{1}{16}\right)$, la double inégalité

$$M - \mu \leq v \leq M \tag{45}$$

sera, en vertu de (44), satisfaite sur un intervalle de Ox d'amplitude au moins égale à

$$\nu = \frac{\mu}{3s}.$$

Posons alors

$$\mathcal{J}_m = \left\{ \int_2^s \cos^{2m} \pi x \cos^{2m} \frac{\pi r}{x} \cos^{2m} \frac{\pi s}{x} dx \right\}^{\frac{1}{m}}.$$

On a

$$(M - \mu)\left(\frac{\mu}{3s}\right)^{\frac{1}{m}} - M < \mathcal{J}_m - M < M(s-2)^{\frac{1}{m}} - M. \tag{46}$$

Raisonnons comme au paragraphe 4, et considérons d'abord la seconde des inégalités (46). On montre que, si

$$m \geqq 6s^6 \operatorname{Log} s, \tag{47}$$

on aura

$$\mathcal{I}_m < \mathrm{M} + \frac{1}{2s^6}.$$

De sorte que, si r et s sont premiers entre eux,

$$\mathcal{I}_m < 1 - \frac{1}{2s^6}; \tag{48}$$

si maintenant r et s ne sont pas premiers entre eux, on montre, comme au paragraphe 4 que l'on peut prendre m assez grand pour que

$$\mathcal{I}_m > 1 - \frac{1}{2s^6}. \tag{49}$$

Il suffit pour cela, de reprendre le raisonnement employé pour démontrer l'inégalité (29) en observant que $2p$ doit être maintenant remplacé par $3s$.

r et s n'étant pas premiers entre eux, l'inégalité (49) sera satistaite à condition de faire

$$m \geqq 4\left(\frac{3s}{2}\right)^6 \operatorname{Log}\left[8\left(\frac{3s}{2}\right)^7\right],$$

ou, plus simplement,

$$m \geqq 30s^6 \operatorname{Log}(70s^7). \tag{50}$$

Remarquons que (50) entraîne (47). On peut donc résumer ainsi les résultats obtenus :

Pour que r et s soient premiers entre eux, il faut et il suffit que l'on ait

$$\int_2^s \cos^{2m}\pi x \cos^{2m}\frac{\pi r}{x} \cos^{2m}\frac{\pi s}{x}\, dx < \left(1 - \frac{1}{2s^6}\right)^m, \tag{51}$$

m désignant un nombre fixe, astreint seulement à satisfaire à la condition

$$m \geqq 30s^6 \operatorname{Log}(70s^7);$$

s est ici supposé désigner le plus grand des deux nombres r et s.

Si l'on considère les nombres r, s inférieurs à un nombre N d'ailleurs quelconque, on pourrait encore, en raisonnant toujours comme dans les 4 premiers paragraphes, remplacer cet énoncé par le suivant :

Pour que les entiers r et s, inférieurs à N, *soient premiers entre eux, il faut et il suffit que l'on ait*

$$\int_2^{\mathrm{N}} \cos^{2m}\pi x \cos^{2m}\frac{\pi r}{x} \cos^{2m}\frac{\pi s}{x}\, dx < \left(1 - \frac{1}{2\mathrm{N}^6}\right)^m, \tag{52}$$

m désignant un nombre fixe choisi arbitrairement une fois pour toutes parmi les valeurs de m qui vérifient l'inégalité

$$m \geq 30\,N^6 \operatorname{Log}(70\,N^7).$$

On pourrait faire sur ces énoncés des remarques analogues à celles qui terminent le paragraphe 4.

Insistons sur le fait qu'il suffit pour la validité des théorèmes que (51) et (52) soient vraies pour *une seule valeur de m*, à condition que celle-ci satisfasse aux inégalités convenables figurant dans leurs énoncés.

Il y a lieu de noter ici que la limite supérieure de l'intégrale (52) peut être prise égale à N, donc indépendante de r et de s, alors que, dans l'énoncé analogue du paragraphe 4 l'intégrale correspondante (39) avait sa limite supérieure égale à $p-1$. Cela provient du fait que si r et s sont premiers entre eux, il n'existe aucune valeur de x (sauf 1) qui soit entière et divise à la fois r et s, tandis qu'un nombre premier est divible par lui-même et l'unité, d'où la nécessité de prendre dans (39) la limite supérieure de l'intégrale inférieure à p.

Il n'est pas difficile d'étendre les résultats précédents au cas de n nombres entiers $r_1, r_2, \ldots, r_n$. Soit à exprimer que n entiers distincts $r_1, r_2, \ldots, r_n$ sont premiers entre eux dans leur ensemble. Désignons, pour simplifier, par N un nombre supérieur à tous les précédents.

Pour que $r_1, r_2, \ldots, r_n$ soient premiers entre eux dans leur ensemble, il faut et il suffit que

$$(53) \qquad w = \cos^2\pi x \cos^2\frac{\pi r_1}{x}\cos^2\frac{\pi r_2}{x}\cdots\cos^2\frac{\pi r_n}{x} < 1,$$

quand x varie dans l'intervalle (2, N).

En appliquant les méthodes précédentes, on voit d'abord que la condition (53) peut se remplacer par

$$w < 1 - \frac{1}{N^6}.$$

Soit alors

$$(54) \qquad K_m = \left\{\int_2^N \cos^{2m}\pi x \cos^{2m}\frac{\pi r_1}{x}\cdots\cos^{2m}\frac{\pi r_n}{x}\,dx\right\}^{\frac{1}{m}}.$$

On démontrerait ici, en reprenant nos raisonnements antérieurs, que μ désignant un nombre positif quelconque, inférieur au maximum M de w dans (2, N), on a

$$(55) \qquad (M-\mu)\left[\frac{\mu}{(n+1)N}\right]^{\frac{1}{m}} - M < K_m - M < M(N-2)^{\frac{1}{m}} - M.$$

On verrait d'ailleurs immédiatement que

$$M > \left(\frac{1}{4}\right)^n,$$

en faisant $x = 3$ dans l'expression de w. Mais il y a lieu de noter que la première des équations (55) ne sera utilisée que dans le cas où M est égal à 1, de sorte qu'il suffira de prendre toujours

$$\mu < 1.$$

Remarquons que (55) se déduit de (15) en y remplaçant, à droite $2p$ par $(n+1)\mathrm{N}$, et, à gauche $p-1$ par N. On voit alors facilement qu'il suffit de remplacer dans (36), $2p$ par $(n+1)\mathrm{N}$, ce qui donne

$$m \geqq \frac{1}{2^4}(n+1)^6 \mathrm{N}^6 \operatorname{Log}\frac{(n+1)^7 \mathrm{N}^7}{2^4} \tag{56}$$

pour obtenir le théorème suivant :

Pour que n entiers $r_1, r_2, \ldots, r_n$ inférieurs à un même nombre N *soient premiers entre eux dans leur ensemble, il faut et il suffit que l'on ait*

$$\int_2^N \cos^{2m}\pi x \cos^{2m}\frac{\pi r_1}{x} \cdots \cos^{2m}\frac{\pi r_n}{x}\, dx < \left(1 - \frac{1}{2\mathrm{N}^6}\right)^m,$$

m désignant un nombre pris une fois pour toutes d'une façon arbitraire parmi ceux qui satisfont à la condition

$$m \geqq \frac{1}{2^4}(n+1)^6 \mathrm{N}^6 \operatorname{Log}\frac{(n+1)^7 \mathrm{N}^7}{2^4}.$$

6. L'idée qui nous a guidé et consistant à rattacher à un principe d'extremum la question étudiée peut être appliquée de bien des façons. Nous en indiquerons ici quelques-unes, en nous bornant toujours au problème qui consiste à traduire analytiquement la propriété pour un entier d'être un nombre premier. Il existe un théorème fini correspondant au théorème de Riesz et qui est le suivant :

Soit $a_1, a_2, \ldots, a_n$ un nombre *fini* quelconque de quantités *positives*. L'expression

$$\left\{\sum_{k=1}^{k=n} a_k^m\right\}^{\frac{1}{m}}$$

tend vers une limite quand m augmente indéfiniment, et cette limite est égale au plus grand des nombres a_k.

La démonstration de cette proposition est très simple. Nous reviendrons sur celle-ci dans le paragraphe suivant. L'exposé que nous allons donner actuellement, tout en s'inspirant du théorème cité, se suffira entièrement à lui-même.

Soit p un entier quelconque. Posons

$$S_m = \cos^{2m}\frac{\pi p}{2} + \cos^{2m}\frac{\pi p}{3} + \dots \cos^{2m}\frac{\pi p}{p-1} \tag{56}$$

ou

$$S_m = \sum_{k=2}^{k=p-1} \cos^{2m}\frac{\pi p}{k}.$$

D'après ce que nous avons vu au début [inégalité (2)], si k ne divise pas p, on a

$$\cos^2\frac{\pi p}{k} \leq \cos^2\frac{\pi}{p} = 1 - \sin^2\frac{\pi}{p} \leq 1 - \frac{4}{\pi^2}\left(\frac{\pi}{p}\right)^2 = 1 - \frac{4}{p^2}.$$

Supposons p premier. Il vient alors

$$S_m < (p-2)\cos^{2m}\frac{\pi}{p} < (p-2)\left(1 - \frac{4}{p^2}\right)^m,$$

d'où

$$S^{\frac{1}{m}} < (p-2)^{\frac{1}{m}}\left(1 - \frac{4}{p^2}\right). \tag{57}$$

Je me propose de déterminer m de façon que

$$(p-2)^{\frac{1}{m}}\left(1 - \frac{4}{p^2}\right) < 1 - \frac{2}{p^2}. \tag{58}$$

Il suffit de prendre m tel que

$$(p-2)^{\frac{1}{m}} < \frac{1 - \frac{2}{p^2}}{1 - \frac{4}{p^2}} < 1 + \frac{2}{p^2-4} \tag{59}$$

ou

$$e^{\frac{\operatorname{Log}(p-2)}{m}} - 1 < \frac{2}{p^2-4}. \tag{60}$$

Or, si x est un nombre positif quelconque, on a

$$e^x - 1 < x\,e^x.$$

Donc (60) et (59) seront satisfaites si l'on a

$$\frac{\operatorname{Log}(p-2)}{m} e^{\frac{\operatorname{Log}(p-2)}{m}} < \frac{2}{p^2-4}. \tag{61}$$

Prenons déjà

$$\frac{\operatorname{Log}(p-2)}{m} < 1 \tag{62}$$

et (61), donc (59) seront satisfaites en prenant

$$\frac{\operatorname{Log}(p-2)}{m}\times 3<\frac{2}{p^2-4},$$

car alors

$$e^{\frac{\operatorname{Log}(p-2)}{m}}<e<3,$$

ce qui donne :

$$m>\frac{3}{2}(p^2-4)\operatorname{Log}(p-2). \tag{63}$$

Or, p étant supposé supérieur à 2, l'inégalité (63) entraîne (62) et finalement (58). On voit donc que si m vérifie l'inégalité (63), on aura, d'après (57) et (58),

$$S_m^{\frac{1}{m}}<1-\frac{2}{p^2}<1. \tag{64}$$

Supposons maintenant que p ne soit pas premier, il vient alors

$$S_m\geqq 1, \tag{65}$$

d'où

$$S_m^{\frac{1}{m}}\geqq 1. \tag{65'}$$

Ainsi, la condition (64) *qui peut s'écrire*

$$S_m<\left(1-\frac{2}{p^2}\right)^m \tag{66}$$

exprime la condition nécessaire et suffisante pour que p soit un nombre premier, l'exposant m étant pris arbitrairement parmi les nombres qui satisfont à l'inégalité :

$$m>\frac{3}{2}(p^2-4)\operatorname{Log}(p-2). \tag{63}$$

On peut encore dire :

Pour que p soit premier, il faut et il suffit que l'inégalité (63) *entraîne*

$$S_m<1; \tag{67}$$

cette dernière condition étant entendue au sens strict [égalité des deux membres de (67) exclu].

La validité de cette conclusion suppose seulement que (67) *ait lieu pour une seule valeur de m pourvu que celle-ci satisfasse à* (63).

Supposons p premier : il est clair alors que (66) entraîne (67) et la condition est bien nécessaire. Elle est suffisante. Supposons (67) vérifiée pour une valeur de m satisfaisant à (63). Le nombre p est premier, sinon (65) aurait lieu, ce qui est contradictoire avec la supposition précédente.

Remarque. — Si, comme nous l'avons fait dans les paragraphes précédents, nous considérons seu ement les entiers p inférieurs à un même nombre N pouvant d'ailleurs être pris arbitraire, on montrerait facilement, en reprenant les raisonnements ci-dessus que, *pour que le nombre entier p satisfaisant à*

$$p \leq N$$

soit premier, il faut et il suffit que

$$S_m < \left(1 - \frac{2}{N^2}\right)^m, \tag{68}$$

m étant un nombre fixe pouvant être pris arbitrairement parmi ceux qui satisfont à

$$m > \frac{3}{2}(N^2 - 4)\,\mathrm{Log}(N - 2). \tag{69}$$

Les inégalités (68) et (69) sont respectivement les analogues des inégalités (66) et (63).

La condition (68) peut d'ailleurs être remplacée par

$$S_m < 1, \tag{70}$$

pourvu que m satisfasse toujours à (69). L'intérêt de l'inégalité (68) est d'être plus précise que l'inégalité (70).

7. Ceci posé, nous allons transformer l'expression de S_m. L'emploi de *formules sommatoires* permet de transformer de façons très diverses des expressions de ce type. Nous nous bornerons ici à indiquer comment une application simple des éléments de la théorie des fonctions de variables complexes permet d'obtenir une transformation intéressante de S_m. Le procédé que nous allons appliquer est étroitement apparenté d'ailleurs aux méthodes conduisant aux formules sommatoires.

Soit dans le plan complexe (z) un contour fermé C auquel on impose seulement de contenir à son intérieur les points de l'axe réel ayant pour abscisses les nombres entiers allant de 2 à $p-1$, à l'exclusion des autres points d'*abscisses entières de cet axe*. On a alors

$$S_m = \frac{1}{2i}\int_c \cos^{2m}\frac{\pi p}{z}\cot \pi z\, dz, \tag{71}$$

et l'on peut appliquer à cette expression de S_m les conclusions du paragraphe 6.

On a ainsi le théorème suivant :

Pour que le nombre entier p tel que

$$p \leq N$$

soit premier, il faut et il suffit que si m désigne un exposant fixe, pris arbitrairement parmi les nombres qui satisfont à l'inégalité

$$m > \frac{3}{2}(N^2 - 4)\,\mathrm{Log}(N - 2),$$

on ait

$$\frac{1}{2i}\int_c \cos^{2m}\frac{\pi p}{z}\cot\pi z\,dz < 1.$$

Nous nous bornerons actuellement à ces résultats, quoiqu'il soit manifeste, d'une part, qu'une intégrale telle que (71) soit susceptible d'une étude beaucoup plus poussée, et que d'autre part la méthode que nous employons dans ce paragraphe, pour exprimer qu'un nombre p est premier, soit, elle aussi, susceptible de s'étendre à beaucoup d'autres questions.

Remarque. — Reprenons l'expression (56) de S_m, c'est-à-dire

$$S_m = \sum_{k=2}^{k=p-1} \cos^{2m}\frac{\pi p}{k},$$

quand on fait tendre m vers $+\infty$, le terme

$$\cos^{2m}\frac{\pi p}{k}$$

tend vers zéro ou reste égal à 1 suivant que k ne divise pas ou divise p. Si donc n est le nombre des diviseurs de p, autres que 1 et p, on voit que S_m *tend vers n quand m tend vers* $+\infty$.

Soit C le contour fermé du plan complexe z défini antérieurement. On a

$$n = \lim_{m=\infty}\frac{1}{2i}\int_c \cos^{2m}\frac{\pi p}{z}\cot\pi z\,dz, \tag{72}$$

et la condition nécessaire et suffisante pour que p soit premier deviendra donc

$$\lim_{m=+\infty}\frac{1}{2i}\int_c \cos^{2m}\frac{\pi p}{z}\cot\pi z\,dz = 0. \tag{73}$$

La supériorité de l'énoncé précédent sur cette dernière proposition provient de ce que m peut y recevoir une valeur fixe, évitant ainsi l'étude du passage à la limite dans (73).

8. Nous allons encore appliquer d'une manière différente le principe d'extremum dont nous indiquerons quelques applications dans le présent article.

Notre point de départ sera tout à fait élémentaire. Nous partirons en effet de la définition même des nombres premiers. Celle-ci peut s'énoncer de la façon suivante :

Pour que $p > 2$ soit premier, il faut et il suffit que le plus petit des nombres

$$A_{k,k'} = \left(\frac{p}{k} - k'\right)^2, \tag{74}$$

obtenus en donnant à k et k' toutes les valeurs entières allant de 2 à $p-1$ (valeurs extrêmes comprises), soit différent de zéro.

Précisons encore : Si p est premier, la division de p par k donne

$$\frac{p}{k} = q + \frac{r}{k} \tag{75}$$

et la fraction qui figure au second membre de (75) est au moins égale à

$$\frac{1}{k} > \frac{1}{p},$$

car on a évidemment

$$1 \leq r \leq k-1 < p-1.$$

Il en résulte facilement alors

$$A_{k,k'} > \frac{1}{p^2}. \tag{76}$$

Pour que p soit premier, il est donc nécessaire que le plus petit des A soit supérieur au second membre de (76), et cette condition est suffisante, car si elle est satisfaite aucun des nombres

$$\left(\frac{p}{k} - k'\right)^2 \qquad (k, k' = 2, \ldots, p-1)$$

ne peut être nul.

On a, d'autre part,

$$A < 4p^2$$

et la condition (76) est équivalente à la suivante

$$0 < A'_{k,k'} = 4p^2 - A_{k,k'} < 4p^2 - \frac{1}{p^2}, \tag{76'}$$

où k et k' prennent indépendamment l'un de l'autre, toutes les valeurs entières allant de 2 à $p-1$. Cherchons alors, quel est, dans ces conditions, le plus grand des nombres $A'_{k,k'}$ dont nous désignerons la valeur par M. Remarquons, d'abord, que, pour que p soit premier, il faut et il suffit que

$$M < 4p^2 - \frac{1}{p^2}. \tag{77}$$

Cette condition (77) peut, d'ailleurs se remplacer par toute condition de la forme

$$M < 4p^2 - \alpha, \tag{78}$$

où α désigne un nombre quelconque tel que

$$0 \leq \alpha \leq \frac{1}{p^2}, \tag{79}$$

car (78), *prise au sens strict* équivaut à

$$A_{k,k'} > 0, \tag{80}$$

qui exprime que A ne peut s'annuler, donc que p est premier : l'inégalité (80), nécessaire pour que p soit premier est aussi suffisante.

Or, d'après ce que nous avons vu au paragraphe 6, relativement au théorème fini correspondant à celui de Riesz, on a

$$M = \lim_{m=\infty} \left\{ \sum_{k=2}^{k=p-1} \sum_{k'=2}^{p-1} A'^m \right\}^{\frac{1}{m}}.$$

Posons donc

$$S_m = \sum_{k=2}^{k=p-1} \sum_{k'=2}^{k'=p-1} \left[4p^2 - \left(\frac{p}{k} - k' \right)^2 \right]^m. \tag{81}$$

Pour que p soit premier, il faut et il suffit que

$$\lim S_m^{\frac{1}{m}} < 4p^2 - \alpha, \tag{82}$$

où

$$0 \leq \alpha \leq \frac{1}{p^2}.$$

Si l'on prend $\alpha = 0$ dans (82), il doit être bien entendu que l'on suppose cette inégalité vérifiée au sens strict.

Il est maintenant nécessaire, comme nous l'avons fait au paragraphe 6 pour une autre question, d'étudier de plus près la façon dont $S_m^{\frac{1}{m}}$ tend vers sa limite.

Nous allons envisager le problème d'une façon générale. Soient alors

$$a_1, \quad a_2, \quad \ldots, \quad a_n$$

un nombre quelconque, n, de quantités *positives*. Soit a la plus grande de celles-ci.

Nous avons

$$a^m < a_1^m + a_2^m + \ldots a_n^m < n a^m,$$

d'où

$$a < (a_1^m + a_2^m + \ldots + a_n^m)^{\frac{1}{m}} < n^{\frac{1}{m}} a,$$

ou encore

$$0 < \left(\sum_i a_i^m \right)^{\frac{1}{m}} - a < \left(n^{\frac{1}{m}} - 1 \right) a.$$

Or

$$n^{\frac{1}{m}} - 1 = e^{\frac{\operatorname{Log} n}{m}} - 1 < \frac{\operatorname{Log} n}{m} e^{\frac{\operatorname{Log} n}{m}}.$$

Prenons déjà

$$m > \operatorname{Log} n$$

d'où

$$e^{\frac{\operatorname{Log} n}{m}} < e^1 < 3.$$

Il vient alors

$$0 < \left(\sum_{i=1}^{i=n} a_i^m \right)^{\frac{1}{m}} - a < 3 \frac{\operatorname{Log} n}{m} a,$$

soit K un nombre fixe tel que

$$a_i \leq K \qquad (i = 1, 2, \ldots, n).$$

On a donc, *a fortiori*,

$$0 < \left(\sum_{i=1}^{i=n} a_i^m \right)^{\frac{1}{m}} - a < \frac{3 K \operatorname{Log} n}{m}.$$

Soit ε un nombre positif arbitraire. Prenons à la fois

$$m > \operatorname{Log} u \qquad \text{et} \qquad m > \frac{3 K \operatorname{Log} n}{\varepsilon}, \tag{83}$$

il viendra

$$0 < \left(\sum_{i=1}^{i=n} a_i^m \right)^{\frac{1}{m}} - a < \varepsilon.$$

Appliquons ceci à la question que nous étudions actuellement. Nous pouvons trouver un nombre m_0 tel que l'inégalité

$$m > m_0$$

entraîne

$$0 < S_m^{\frac{1}{m}} - M < \frac{1}{p^2}. \tag{84}$$

D'après ce que nous venons d'exposer, il suffira de prendre

$$m > m_0 > \frac{3 \times 4 p^2 \operatorname{Log}(p-2)^2}{\frac{1}{p^2}} = 12 p^4 \operatorname{Log}(p-2), \tag{85}$$

car, ici, on peut faire dans les inégalités (83)

$$K = 4p^2; \qquad n = (p-2)^2; \qquad \varepsilon = \frac{1}{p^2}.$$

Choisissons arbitrairement un nombre m vérifiant (85). On voit facilement que, pour que p soit premier, il faut et il suffit que

$$S_m^{\frac{1}{m}} < 4p^2. \tag{86}$$

La condition est nécessaire; en effet, si p est premier, on a

$$M < 4p^2 - \frac{1}{p^2},$$

d'après (77); donc, dans ce cas, d'après (84)

$$S_m^{\frac{1}{m}} < M + \frac{1}{p^2} < 4p^2.$$

La condition est suffisante, car, puisque

$$M < S_m^{\frac{1}{m}},$$

l'inégalité

$$S_m^{\frac{1}{m}} < 4p^2$$

entraînera

$$M < 4p^2,$$

et cette dernière inégalité, prise au sens strict (la possibilité pour les deux membres d'être égaux étant donc formellement exclue) entraîne bien que p est premier comme nous l'avons vu un peu plus haut.

On a donc le théorème suivant :

Pour que le nombre entier p soit premier, il faut et il suffit que l'on ait

$$S_m < 4^m p^{2m}, \tag{87}$$

m désignant un nombre pris arbitrairement une fois pour toutes parmi ceux qui satisfont à la condition

$$m > 12p^4 \operatorname{Log}(p-2).$$

Remarques. — 1° Comme nous l'avons souvent fait, considérons seulement les nombres p tels que

$$p \leqq N,$$

N étant un nombre arbitraire fixe. Posons

$$S'_m = \sum_{k=2}^{k=p-1} \sum_{k'=2}^{k'=p-1} \left[4N^2 - \left(\frac{p}{k} - k' \right)^2 \right]^m, \tag{88}$$

en reprenant les raisonnements précédents, on voit facilement que :

Pour que p soit premier, il faut et il suffit que l'on ait

$$S'_m < 4^m N^{2m},$$

m désignant un nombre fixe choisi arbitrairement une fois pour toutes parmi ceux qui satisfont à l'inégalité

$$m > 12 N^4 \operatorname{Log}(N-2).$$

Ce dernier énoncé est plus simple que le précédent, l'exposant m ne dépendant pas de p, qui figure lui-même d'une façon plus simple dans l'expression de S'_m que dans celle de S_m.

2° On a toujours, quel que soit p entier,

$$0 < 1 - \frac{1}{4p^2}\left(\frac{p}{k} - k'\right)^2 \leq 1 \qquad (k,\ k' = 2,\ \ldots,\ p-1),$$

le terme intermédiaire de cette inégalité ne pouvant être égal à 1 que si p n'est pas premier, k désignant alors un de ses diviseurs autres que 1 et p.

Si donc nous considérons la somme

$$s_m = \sum_{k=2}^{p-1} \sum_{k'=2}^{p-1} \left[1 - \frac{1}{4p^2}\left(\frac{p}{k} - k'\right)^2\right]^m, \tag{89}$$

on voit que, p étant fixe, s_m *tend vers zéro quand m tend vers l'infini si p est premier, et, dans le cas contraire, vers le nombre n des diviseurs de p, la somme* s_m *renfermant alors n termes égaux à* s_m.

On a un énoncé analogue pour la somme :

$$s'_m = \sum_{k=2}^{p-1} \sum_{k'=2}^{p-1} \left[1 - \frac{1}{4N^2}\left(\frac{p}{k} - k'\right)^2\right]^m,$$

où

$$p \leq N.$$

Ces derniers énoncés sont plus simples en apparence que ceux que nous venons de donner plus haut, mais le passage à la limite qui y figure les rend au contraire à certains points de vue plus complexes que les précédents dans lesquels l'exposant m était fixe.

L'intérêt des considérations ci-dessus réside en partie dans le fait que les sommes S_m, S'_m, s_m, s'_m peuvent recevoir une forme simple en utilisant les éléments de la théorie des fonctions de variables complexes.

Dans le plan d'une variable complexe x, soit C un contour fermé coupant l'axe réel en deux points seulement x_1 et x_2 tels que

$$1 < x_1 < 2 \qquad \text{et} \qquad p-1 < x_2 < p.$$

On peut prendre, par exemple,

$$x_1 = \frac{3}{2} \qquad \text{et} \qquad x_2 = p - \frac{1}{2}.$$

C renferme à son intérieur tous les points dont les affixes sont les nombres entiers compris entre 2 et $p-1$, valeurs extrêmes comprises.

Soit, de même, dans le plan d'une seconde variable complexe y un contour fermé C′ rencontrant le nouvel axe réel en deux points seulement dont les affixes y_1 et y_2 satisfont aux conditions

$$1 < y_1 < 2 \qquad \text{et} \qquad p-1 < y_2 < p.$$

On peut prendre encore ici

$$y_1 = \frac{3}{2} \qquad \text{et} \qquad y_2 = p - \frac{1}{2}$$

par exemple.

Le contour C′ renferme à son intérieur tous les points du plan complexe (y) dont les affixes sont les nombres entiers successifs allant de 2 à $p-1$. Les sommes S_m, S'_m, s_m, s'_m peuvent alors être mises sous des formes très simples par application des théorèmes généraux relatifs aux fonctions analytiques. Ainsi la théorie des résidus donne immédiatement

$$S'_m = -\frac{1}{4}\int_c \int_{c'} \left[4N^2 - \left(\frac{p}{x} - y\right)^2\right]^m \cot \pi x \cot \pi y \, dx \, dy,$$

les autres sommes S_m, s_m, s'_m auraient des expressions analogues.

En tenant compte de ce que nous venons d'exposer, les théorèmes antérieurement démontrés dans ce paragraphe prennent une forme intéressante. On a, par exemple, la proposition suivante :

Pour que le nombre entier $p \leq N$ *soit premier, il faut et il suffit que l'on ait*

$$\int_c \int_{c'} \left[4N^2 - \left(\frac{p}{x} - y\right)^2\right]^m \cot \pi x \cot \pi y \, dx \, dy > -4^{m+1} N^{2m},$$

m désignant un nombre choisi arbitrairement une fois pour toutes, parmi ceux qui satisfont à la condition

$$m > 12 N^4 \operatorname{Log}(N-2),$$

et encore

L'intégrale

$$I = -\frac{1}{4}\int_c \int_{c'} \left[1 - \frac{1}{4N^2}\left(\frac{p}{x} - y\right)^2\right]^m \cot \pi x \cot \pi y \, dx \, dy$$

tend vers une limite quand m tend vers l'infini. Cette limite est égale au nombre des diviseurs de p compris entre 2 *et* $p-1$ *si les contours* C *et* C′ *sont choisis comme plus haut.*

De sorte que, pour que p soit premier, il faut et il suffit que la limite de I soit nulle.

9. Indiquons maintenant une autre façon d'appliquer les idées du paragraphe précédent.

Nous partirons de la remarque élémentaire suivante : pour que p soit premier, il faut et il suffit qu'aucun des nombres

$$\frac{(p-1)!}{p}k \qquad (k=1, 2, \ldots, p-1)$$

soit entier (1).

1° La condition est nécessaire. Si p est premier, il est premier avec 2, ..., $p-1$, k, et ne saurait donc diviser leur produit.

2° La condition est suffisante. Supposons en effet

$$\frac{(p-1)!\,k}{p}$$

non entier. Alors k ne divise pas p. Car, s'il en était autrement, le quotient

$$\frac{p}{k}=q$$

serait un entier inférieur à p qui figurerait donc dans $(p-1)!$ et

$$\frac{(p-1)!}{q}=\frac{(p-1)!}{p}k$$

serait entier, contrairement à l'hypothèse. Alors p n'étant pas divisible par aucun des nombres 2, 3, ..., $p-1$ est premier.

Exprimer que p est premier revient donc à exprimer que la plus petite des quantités :

$$B_{k,k'}=\left[\frac{(p-1)!}{p}k-k'\right]^2,$$

où

$$k=1, 2, \ldots, p-1; \qquad k'=1, 2, \ldots, (p-1)!$$

n'est pas nulle. On verrait d'ailleurs facilement, comme dans le paragraphe 8, que cette condition équivaut encore ici à

$$B_{k,k'}\geqq\frac{1}{p^2},$$

(1) On sait même, avec plus de précision, que, pour que p soit premier, il faut et il suffit que p *ne divise pas* $1\,2\ldots(p-1)$.

Nous n'utiliserons pas cette proposition (quoique certaines des considérations qui vont suivre en seraient simplifiées), car nous ne voulons, conformément au but de ce travail, ne faire appel ici, en fait de théorie des nombres, qu'aux propriétés et aux définitions fondamentales.

d'ailleurs

$$B_{k,k'} < 4[(p-1)!]^2 < 4(p!)^2.$$

On raisonnerait alors comme plus haut. Considérons seulement les nombres p majorés par un même nombre N d'ailleurs quelconque.

Pour que p soit premier, il faut et il suffit que :

$$\lim_{m=\infty} \left\{ \sum_{k=1}^{p-1} \sum_{k'=1}^{(p-1)!} \left[4(N!)^2 - \left[\frac{(p-1)!}{p} k - k' \right]^2 \right] \right\}^{\frac{1}{m}} \leq 4(N!)^2 - \frac{1}{N^2},$$

et l'on peut raisonner sur ce résultat comme plus haut.

On pourrait ainsi assigner une valeur m_0 de l'exposant m, dépendant seulement, dans le cas actuel, de N et non de p, et telle que, m étant un nombre pris arbitrairement une fois pour toutes et astreint seulement à être supérieur à m_0, la condition précédente serait équivalente à

$$\sum_{k=1}^{p-1} \sum_{k'=1}^{(p-1)'} \left\{ 4(N!)^2 - \left[\frac{(p-1)!}{p} k - k' \right]^2 \right\}^m < 4^m (N!)^{2m},$$

l'inégalité étant entendue au sens strict.

Signalons enfin que, pour exprimer que p est premier, on pourrait encore écrire

$$\lim_{m=\infty} \sum_{k=1}^{p-1} \sum_{k'=1'}^{(p-1)'} \left\{ 1 - \frac{1}{4(N!)^2} \left[\frac{(p-1)!}{p} k - k' \right]^2 \right\}^m = 0;$$

les sommes doubles précédentes dépendent de p d'une manière plus compliquée que les sommes analogues du numéro 8. Par contre, k et k' y figurent d'une façon plus simple et la théorie des nombres de Bernoulli permettrait de transformer leurs expressions en effectuant les sommations indiquées (1). Il y a là un sujet de recherches s'étendant d'ailleurs à d'autres questions que celles étudiées dans ce travail et que nous nous bornerons à mentionner ici.

Ajoutons encore que les sommes doubles figurant ci-dessus peuvent se transformer en intégrales doubles par le procédé que nous avons indiqué au paragraphe précédent. Cette transformation pouvant d'ailleurs être rattachée à

---

(1) Conformément à la remarque de la page 76, quand on se borne à chercher une condition nécessaire et suffisante pour que p soit premier, on peut faire $k = 1$ et l'on aurait une sommation simple au lieu d'une sommation double. Ainsi on aurait la proposition suivante :

Pour que p soit premier, il faut et il suffit que :

$$\lim_{m=\infty} \sum_{k'=1}^{(p-1)!} \left\{ 1 - \frac{1}{4(N!)^2} \left[\frac{(p-1)!}{p} - k' \right]^2 \right\}^m = 0.$$

Des remarques analogues sont applicables aux transformations des sommes doubles précédentes, dans le cas particulier actuel, en supposant toujours comme le théorème rappelé dans la note précédente pour que p soit premier, il faut et il suffit que $(p-1)!$ ne soit pas divisible par p.

celle dont nous indiquions la possibilité par l'introduction des formules sommatoires et des nombres de Bernoulli.

Il pourrait y avoir intérêt, dans ce dernier cas surtout, à modifier un peu l'expression de nos sommes doubles. Bornons-nous à donner la proposition suivante qui découle immédiatement de ce que nous venons d'exposer :

Pour que p soit premier, il faut et il suffit que l'on ait

$$0 = \lim_{m=\infty} \int_C \int_{C'} \left\{ 1 - \frac{1}{4(N!)^2} \left[\frac{(p-1)!}{p} x - y \right]^2 \right\}^m \cot \pi x \cot \pi y \, dx \, dy,$$

C et C′ étant deux contours fermés définis d'une façon analogue à ceux que nous avons fait intervenir au paragraphe précédent.

Remarque. — Pour exprimer que p est premier, on pourrait aussi considérer les nombres

$$\frac{1}{1+\left(\frac{p}{k}-k'\right)^2} \qquad (k, k' = 2, 3, \ldots, p-1);$$

le plus grand d'entre eux doit être *inférieur* à 1 (condition nécessaire et suffisante). On serait donc conduit à introduire la somme

$$S_{1,m} = \sum_{k=2}^{p-1} \sum_{k'=2}^{p-1} \left[\frac{1}{1+\left(\frac{p}{k}-k'\right)^2} \right]^m,$$

et la condition précédente deviendrait

$$\lim_{m=\infty} S_{1,m}^{\frac{1}{m}} < 1.$$

De même, soit

$$S_{2,m} = \sum_{k=1}^{p-1} \sum_{k'=1}^{(p-1)!} \left\{ \frac{1}{1+\left[\frac{(p-1)!}{p} k - k' \right]^2} \right\}^m;$$

le fait que p est premier se traduirait encore par

$$\lim S_{2,m}^{\frac{1}{m}} < 1.$$

On pourrait reprendre, sur ces nouvelles sommes, des raisonnements analogues à ceux que nous avons déjà faits, mais les transformations en intégrales doubles sont moins simples.

Une application plus serrée de la théorie des fonctions de variables complexes aux intégrales rencontrées au cours de cette étude est possible, et il existe des techniques permettant de les transformer de façons très diverses. Il y a là un sujet de recherches que nous nous bornerons encore à mentionner ici et dont l'intérêt paraît certain.

Nous nous proposons d'ailleurs de revenir sur ce point dans un travail ultérieur, ainsi que sur les développements qu'appelleraient les considérations par lesquelles nous allons terminer ce travail.

10. On peut encore, en revenant au début du paragraphe précédent, formuler l'énoncé suivant :

Pour que p soit premier, il faut et il suffit que la fonction

$$\varphi(x) = \cos^2 \pi x \cos^2 \pi \frac{(p-1)!}{p} x \qquad (1 \leq x \leq p-1)$$

reste inférieure à 1 *en valeur absolue* (1).

Cet énoncé est analogue à celui qui nous a servi de point de départ au paragraphe 1 et l'on pourrait développer à son sujet des considérations semblables.

Ainsi, le maximum absolu de φ dans $(1, p-1)$ est

$$\lim_{m=\infty} \left\{ \int_1^{p-1} \cos^{2m} \pi x \cos^{2m} \pi \frac{(p-1)!}{p} x \, dx \right\}^{\frac{1}{m}}.$$

Donc, *pour que p soit premier, il faut et il suffit que*

$$\lim_{m=\infty} \left\{ \int_1^{p-1} \cos^{2m} \pi x \cos^{2m} \pi \frac{(p-1)!}{p} x \, dx \right\}^{\frac{1}{m}} < 1;$$

---

(1) Si l'on voulait faire appel à la proposition que nous avons déjà rappelée en note, à savoir que pour que p soit premier, il faut et il suffit qu'il ne divise pas $(p-1)!$: on pourrait au lieu de supposer que x varie dans tout l'intervalle fermé $(1, p-1)$ supposer qu'il varie seulement dans un intervalle tel que $(1 \leq x \leq a)$, où a désigne un nombre arbitraire inférieur à p. On pourrait prendre ainsi $a < 2$. Cette remarque est applicable à tout ce qui suit. En outre, en prenant $a - 1$ assez petit on pourrait remplacer l'énoncé ci-dessus par le suivant : *pour que p soit premier, il faut et il suffit que*

$$\max \text{ de } \cos^2 \pi \frac{(p-1)!}{p} x < 1 \qquad (1 \leq x \leq a),$$

d'où

$$\lim_{m=\infty} \left\{ \int_1^{a} \cos^{2m} \pi \frac{(p-1)!}{p} x \, dx \right\}^{\frac{1}{m}} < 1.$$

En adoptant le point de vue de la théorie des équations, on pourrait encore dire que pour $a - 1$ assez petit, l'équation

$$\sin \pi \frac{(p-1)!}{p} z = 0$$

ne doit pas avoir de racines dans l'intervalle fermé $(1, a)$. Ces indications paraissent faciles à développer. Ceci aboutirait probablement au théorème de Wilson.

L'inconvénient du point de vue actuel est de supposer qu'on prend pour point de départ un théorème d'arithmétique pure déjà relativement élevé. L'intérêt des considérations plus générales développées paragraphe 10 et dans le reste de cet article n'est pas diminué par la remarque actuelle ou les remarques analogues antérieurement faites.

en étudiant de plus près l'intégrale précédente, on pourrait éviter le passage à la limite et obtenir un énoncé analogue à celui du paragraphe 4, relations (38) et (39).

Considérons encore la somme

$$\sigma_m = \sum_{k=1}^{k=p-1} \cos^{2m}\pi \frac{(p-1)!}{p} k.$$

Les remarques d'un caractère très élémentaire faites au début du paragraphe précédent montrent que σ_m tend vers une limite quand m tend vers $+\infty$ et que cette limite est nulle si p est premier, supérieur à 1 dans le cas contraire. Une application simple de la formule des résidus donne facilement

$$\sigma_m = \frac{1}{2i}\int_C \cos^{2m}\pi \frac{(p-1)!}{p} z \cot \pi z \, dz,$$

C désignant un contour fermé renfermant à son intérieur la partie de l'axe réel sur laquelle sont situés les points dont les affixes sont les nombres entiers allant de 1 à $p-1$ et ne contenant pas d'autre point d'affixe entière.

La condition nécessaire et suffisante pour que p soit premier se traduira donc par

$$\lim_{n=\infty} \frac{1}{2i}\int_C \cos^{2m}\pi \frac{(p-1)!}{p} z \cot \pi z \, dz = 0;$$

l'intégrale précédente paraît facile à étudier et l'on doit sans doute aboutir à retrouver l'énoncé du théorème de Wilson sous la forme suivante : pour que p soit premier, il faut et il suffit que

$$\sin \pi \frac{(p-1)! + 1}{p} = 0.$$

L'étude dont nous indiquons ici la possibilité ne semble pas avoir été faite malgré l'extrême simplicité de son point de départ qui, quoique apparaissant ici comme un cas particulier de l'idée générale développée en partie dans cet article, pouvait facilement être trouvée de façon indépendante.

En résumé, les idées qui ont servi de base à ce travail sont les suivantes :

Après avoir remarqué que de nombreuses questions d'arithmétique pouvaient être rattachées à un principe d'extremum en envisageant les entiers comme réalisant le maximum de $\cos^2 \pi x$, nous avons pris un cas très particulier : le problème d'exprimer, par une condition analytique assez simple, la propriété pour un entier d'être un nombre premier. Nous avons alors étudié cette question en restant systématiquement dans un ordre d'idées que l'on peut dire issu du théorème de Riesz rappelé au début. Mais l'idée fondamentale de traduire des propriétés de nature arithmétique par des conditions d'extremum

a une généralité beaucoup plus grande et peut être traitée par d'autres méthodes, si bien que cet article quoique contenant quelques énoncés assez simples ne constitue qu'un premier travail touchant un domaine très vaste.

Pour finir, nous donnerons un exemple d'une autre façon d'appliquer les idées précédentes, mais en envisageant toujours le même problème : celui d'exprimer que p est premier, mais en abandonnant les considérations plus ou moins issues du théorème de Riesz. Nous nous bornerons d'ailleurs ici à des indications très brèves. La condition

$$\cos^2\pi x \cos^2\frac{\pi p}{x} < 1 \qquad (2 \leq x \leq p-1),$$

qui est la condition nécessaire et suffisante pour que p soit premier équivaut à l'énoncé suivant :

Pour que p soit premier, il faut et il suffit que

$$f(z) = \cos\pi z \cos\frac{\pi p}{z} \pm 1 = 0 \tag{90}$$

n'ait pas de racines *réelles* dans l'intervalle $(2, p-1)$. Il est facile de traduire cela analytiquement. Soit dans le plan de la variable complexe (z), le rectangle R ayant deux côtés parallèles à Oy dont les équations respectives sont

$$x = \frac{3}{2} \qquad \text{et} \qquad x = p - \frac{1}{2}.$$

Les côtés parallèles à Ox ayant respectivement pour équations :

$$y = -\delta \qquad \text{et} \qquad y = +\delta,$$

en prenant δ assez petit, R ne contiendra pas d'autres racines que les racines réelles de $f(z)$, s'il en existe. Une discussion facile permettrait de préciser la valeur de δ. En désignant par Γ le contour de R, la condition nécessaire et suffisante pour que p soit premier s'exprime par

$$\frac{1}{2\pi i}\int_\Gamma \frac{f'(z)}{f(z)}dz = 0.$$

Mêmes remarques au sujet de l'équation

$$g(z) \equiv \cos\pi z \cos\pi\frac{(p-1)!}{p} z \pm 1 = 0; \tag{91}$$

l'absence de racines réelles dans $(1, p-1)$ entraîne que p est premier et inversement.

On peut adopter, pour exprimer l'absence de racines réelles dans un certain intervalle, un point de vue de fonctions de variables réelles. On sait, en effet, que le nombre n des racines de

$$f(x) = 0$$

comprises dans (a, b) est

$$(92) \qquad n = -\frac{1}{\pi}\int_a^b \frac{\varepsilon(ff''-f'^2)}{f^2+\varepsilon f'^2}\,dx + \frac{1}{\pi}\operatorname{arc\,tang}\frac{\varepsilon f'(b)}{f(b)} - \frac{1}{\pi}\operatorname{arc\,tang}\frac{\varepsilon f'(a)}{f(a)},$$

les arc tang étant compris entre $\left(-\frac{\pi}{2}\text{ et }+\frac{\pi}{2}\right)$ et ε une quantité constante quelconque.

Ce théorème (¹) se démontre d'ailleurs sans peine, en remarquant que la primitive correspondant à l'intégrale qui figure dans (92) est

$$\operatorname{arc\,tang}\left[\frac{\varepsilon f'(x)}{f(x)}\right].$$

Toutefois, le théorème que nous venons ainsi de rappeler suppose que toutes les racines de $f(z)$ sont simples. Il faut donc modifier un peu les expressions de f et g définies par (90) et (91) afin de pouvoir leur appliquer cette proposition, car si $f=0$, par exemple, a des racines réelles, celles-ci sont doubles. Cette modification est facile : on peut toujours trouver un nombre α^2 assez voisin de 1, pour que, si p est premier, l'équation

$$\cos^2\pi x\cos^2\frac{\pi p}{x} - \alpha^2 = 0$$

n'ait pas de racines réelles comprises dans $(2, p-1)$, et que dans le cas contraire, ses racines réelles soient *simples*. Une discussion facile, mais un peu longue, permettrait d'assigner une valeur pour α^2.

Il suffit alors d'appliquer la formule (92) en y faisant

$$n=0; \qquad a=\frac{3}{2}; \qquad b=p-\frac{1}{2}$$

et

$$f(x)=\cos\pi x\cos\frac{\pi p}{x}\pm\alpha.$$

Des considérations analogues pourraient être développées pour

$$g(x)=\cos\pi x\cos\pi\frac{(p-1)!}{p}x\pm\beta.$$

L'intérêt des formules ainsi obtenues consiste dans la possibilité d'appliquer aux intégrales qui y figurent un procédé de calcul, soit par développement en série, soit par une méthode d'approximation.

(¹) *Cf.* E. PICARD, *Nombre de racines communes à plusieurs équations* (*Journ. de Math. pures et appliquées*, t. 8, 1892, p. 12).