59.

PREUVE ÉLÉMENTAIRE DU THÉORÈME DE DIRICHLET SUR LES PROGRESSIONS ARITHMÉTIQUES DANS LES CAS OÙ LA *RAISON* EST 8 OU 12.

[*Comptes Rendus*, CVI. (1888), pp. 1278—1281, 1385—1386.]

LE principe (ou pour ainsi dire le moment intellectuel) dont nous nous servons est le suivant:

Pour démontrer que le nombre de nombres premiers d'une forme donnée est infini, cherchons à construire une progression infinie d'entiers relativement premiers entre eux, et dont chacun contiendra un nombre premier (au moins) de la forme donnée.

Dans ce qui suit, f signifie une forme fonctionnelle rationnelle entière et ne contenant que des coefficients rationnels.

LEMME I.—*Si* $u_{x+1} = fu_x$ *et si* $ff0 = f0$, *alors, r et s étant deux entiers quelconques, le plus grand diviseur commun à* u_r *et* u_s *sera un diviseur de* $f0$.

Car évidemment $u_{r+\epsilon} \equiv ff \ldots f0$ (c'est-à-dire $f^\epsilon 0$) [mod u_r]. Mais $f^\epsilon 0$, par hypothèse, $= f0$.

Conséquemment, tout diviseur de u_r et u_s sera un diviseur de $f0$.

LEMME II.—*Si* $u_{x+1} = fu_x$ *et si, de plus,* $u_1 = f0$, *le plus grand diviseur commun de* u_r *et* u_s *sera* u_t, *où t est le plus grand diviseur commun de r et s.*

(1) On aura évidemment

$$u_{s+\epsilon} \equiv u_\epsilon \pmod{u_s}.$$

Conséquemment u_t sera un diviseur de $u_{2t}, u_{3t}, \ldots, u_{mt}$ quel que soit m.

(2) Écrivons un *schéma* pareil à celui qui s'applique à la recherche du plus grand diviseur de r et s, c'est-à-dire

$$r - hs = v, \quad s - kv = w, \quad \ldots, \quad z - ly = t, \quad y - mt = 0;$$

alors, en vertu de ce qui précède, u_t sera un diviseur de u_r et u_s, et tout diviseur de u_r et de u_s sera un diviseur de u_t.

Donc, si t est le plus grand diviseur commun à r et s, u_t sera le plus grand diviseur commun à u_r et u_s, ce qui était à démontrer. Il s'ensuit que, si r est premier relativement à s, u_r et u_s auront u_1 pour leur plus grand diviseur commun.

Je vais faire l'application de ce principe: (A) aux progressions arithmétiques à la raison 8, (B) à la raison 12.

A. 1. *Cas de* $8x+3$.—Écrivons

$$u_1 = 1, \quad u_2 = 2u_1^2 + 1 = 3, \quad u_3 = 2u_2^2 + 1 = 19, \quad \ldots.$$

On démontre facilement que tout u est de la forme $8m+3$, et l'on sait que les facteurs premiers de tout u sont de la forme $8n+1$ ou $8n+3$.

Conséquemment, tout u contiendra au moins un facteur de la forme $8m+3$, et tout terme de la progression infinie

$$u_3, \quad u_5, \quad u_7, \quad u_{11}, \quad u_{13}, \quad \ldots$$

contiendra un facteur premier de la forme voulue.

De plus, en vertu du second lemme, tous ces facteurs seront distincts l'un de l'autre; car sinon u_r et u_s, où r est premier à s, auraient un facteur commun autre que u_1.

On pourrait prendre une série plus générale en écrivant u_1 égal à un produit d'un nombre quelconque de nombres premiers dont aucun n'est de la forme $8m+3$, tellement combinés que $u_1 \equiv 1 \pmod 8$; le résultat restera acquis que chaque terme de la progression des u contiendra un facteur premier de la forme $8x+3$, et que tous ces facteurs seront distincts entre eux.

A. 2. *Cas de* $8x+7$.—Écrivons

$$u_1 = 1, \quad u_2 = 2(u_1+1)^2 - 1 = 7, \quad u_3 = 2(u_2+1)^2 - 1 = 127, \quad \ldots.$$

Tout $u \equiv 7 \pmod 8$: chaque diviseur premier de tout u sera de la forme $8m+1$ ou $8m+7$. Donc il entrera dans chaque terme de la progression

$$u_2, \quad u_3, \quad u_5, \quad u_7, \quad \ldots$$

un facteur de la forme $8x+7$, et de plus, en vertu du second lemme (puisque $f0 = 1$), tous ces facteurs seront distincts.

A. 3. *Cas de* $8x+1$.—Écrivons

$$u_1 = 1, \quad u_2 = u_1^4 + 1 = 2, \quad u_3 = u_2^4 + 1 = 17, \quad \ldots.$$

Tous les facteurs de chaque u, à l'exception de 2, seront de la forme $8x+1$, et, en vertu du second lemme $u_3, u_5, u_7, u_{11}, u_{13}, u_{17}$, seront premiers entre eux.

A. 4. *Cas de* $8x+5$.—Écrivons

$$u_1 = 1, \quad u_2 = u_1^2 + 1 = 2, \quad u_3 = u_2^2 + 1 = 5,$$
$$u_4 = u_3^2 + 1 = 26, \quad u_5 = u_4^2 + 1 = 677, \quad \ldots.$$

Chaque u_{2i+1} sera de la forme $8m+5$, et chaque diviseur premier sera ou de la forme $8n+1$ ou $8n+5$, de sorte qu'il s'en trouvera un au moins de la forme $8x+5$. Donc par le second lemme la progression

$$u_3, \quad u_5, \quad u_7, \quad u_{11}, \quad u_{13}, \quad \ldots$$

contiendra un nombre infini de nombres premiers distincts de cette forme.

B. 1. *Cas de* $12x+5$.—On démontre facilement par induction que chaque terme de rang pair de la progression précédente au delà du second sera de la forme $2(24n+13)$, et chaque terme de rang impair au delà du premier de la forme $24n+5$.

Les diviseurs premiers de chaque u seront de l'une ou l'autre des six formes $24x+1$, 5, 19, 17, 13, 21.

Supposons qu'il n'existe aucun facteur premier de la forme $24x+17$ ni de la forme $24x+5$. Alors les résidus des facteurs (par rapport à 12) appartiendront au groupe 1, 9, 13, 21. Mais on voit facilement que ce groupe est un groupe fermé : car toutes ces combinaisons binaires ne font que reproduire ces mêmes nombres.

Conséquemment, tout terme de rang impair contiendra nécessairement un facteur ou de la forme $24x+5$ ou de la forme $24x+17$, et ainsi, en vertu du second lemme, on voit que la progression déjà écrite contiendra un nombre infini de nombres premiers de la forme $12n+5$.

B. 2. *Cas de* $12x+7$.—Écrivons

$$u_1 = 7, \quad u_2 = u_1^2 - u_1 + 1 = 43, \quad u_3 = u_2^2 - u_2 + 1 = 1807, \quad \ldots.$$

Les diviseurs premiers de chaque u seront de la forme $12n+1$ ou $12n+7$ et u lui-même de la forme $12m+7$. Donc, en vertu du premier lemme, la suite $u_1, u_2, u_3, u_4, \ldots$ contiendra un nombre infini de nombres premiers de la forme $12x+7$*.

B. 3. *Cas de* $12x+11$.—Écrivons

$$u_1 = -1, \quad u_2 = 3u_1^2 - 1 = 2, \quad u_3 = 3u_2^2 - 1 = 11,$$
$$u_4 = 3u_3^2 - 1 = 362, \quad \ldots.$$

Tous les u de rang impair seront de la forme $12m+11$, de sorte que leurs diviseurs premiers étant, ou de la forme $12x+1$ ou $12x+11$, il y aura un nombre infini de nombres premiers distincts contenus dans les termes de la progression

$$u_3, \quad u_5, \quad u_7, \quad u_{11}, \quad \ldots.$$

B. 4. *Cas de* $12x+1$.—Écrivons

$$u_1 = \theta^4 - \theta^2 + 1, \quad u_2 = u_1^4 - u_1^2 + 1, \quad u_3 = u_2^4 - u_2^2 + 1, \quad \ldots.$$

Chaque u, selon la loi cyclotomique, ne contiendra que des facteurs de la forme $12x+1$ et, en vertu du premier lemme, $u_1, u_2, u_3, u_4, u_5, \ldots$ seront tous

* Par un procédé analogue à celui que nous avons appliqué à la progression dont nous nous sommes servis dans les cas A. 4 et B. 1 ; on peut démontrer avec l'aide de la progression 7, 43, 1807, ..., donnée plus haut, que le nombre de nombres premiers dans la double progression arithmétique à raison 30,

7, 13, 37, 43, 67, 73, ...,

contient un nombre infini de nombres premiers : à plus forte raison cette conclusion s'applique à la double progression à raison 5

2, 3, 7, 8, 12, 13, ...

premiers entre eux: donc cette progression contiendra un nombre infini de facteurs de la forme $12x + 1$.

L'application du principe général énoncé au commencement n'est nullement astreinte aux progressions de la forme $\phi\theta$, $\phi\phi\theta$, $\phi\phi\phi\theta$, ... C'est ce que j'ai montré au Congrès scientifique d'Oran.

Au Congrès scientifique d'Oran nous avons indiqué:

(1) Une démonstration instantanée du théorème de Dirichlet pour le cas $Ax + 1$, quel que soit A, en nous servant des fonctions cyclotomiques de l'espèce ordinaire en u, en prenant pour les indices successifs A, $2A$, $3A$, ... et en donnant à u une valeur quelconque. Ces fonctions cyclotomiques sont les facteurs irréductibles des fermatiens. Par exemple, en prenant 3 pour la base des fonctions cyclotomiques, et en ôtant de chaque cyclotome dont l'indice est une puissance de 2 le *facteur singulier* 2, on obtient la progression 2, 2, 13, 5, 121, 7, 1093, ..., dont tous les termes, en omettant le second, sont premiers entre eux, et où le terme à l'indice i (le second excepté) ne contient d'autres facteurs premiers que ceux de la forme $ix + 1$. Conséquemment, en se bornant aux $i^{\text{ème}}$, $(2i)^{\text{ème}}$, $(3i)^{\text{ème}}$, $(4i)^{\text{ème}}$, ... termes, et en décomposant chacun de ces termes dans un produit de facteurs premiers distincts, la totalité de ces facteurs fournira un nombre infini de nombres premiers de la forme $ix + 1$;

(2) Une démonstration beaucoup plus cachée pour le cas $Ax - 1$, quand A est une puissance d'un nombre premier, au moyen des fonctions cyclotomiques qui se déduisent des fonctions dont nous avons parlé en les divisant par une puissance convenable de u, en exprimant le quotient comme fonction de $u + \frac{1}{u}$, disons v, et en attribuant à v une valeur constante dont la forme par rapport au module A ou bien à un multiple de A (capable de grandir indéfiniment) dépend de la forme du nombre premier dont A est une puissance, par rapport au module 8.

Plus récemment, nous avons étendu la même démonstration aux cas où A est une combinaison de puissances de 2, 3, 5, 7, de sorte qu'il nous paraît peu douteux que les propriétés cyclotomiques donnent le moyen de prouver le théorème de Dirichlet aussi bien pour le cas de $Ax-1$, comme pour le cas de $Ax+1$, quelle que soit la forme de A. Il nous semble donc qu'il y a quelque lieu d'espérer que le principe général (qu'on peut nommer constructif ou cosmothétique) peut servir à donner une démonstration pour le cas le plus général du théorème de Dirichlet. En addition à la méthode ici donnée et celle fournie par la théorie cyclotomique pour obtenir des progressions infinies de nombres relativement premiers entre eux, on peut se servir comme troisième méthode des *cumulants* (les numérateurs et dénominateurs de fractions

continues) et sans doute d'une infinité d'autres espèces de fonctions. Toute la difficulté consiste à trouver la *forme* de progression convenable à chaque cas donné.

En ce qui regarde la théorie générale des diviseurs des fonctions cyclotomiques de toute espèce, nous renvoyons à notre article, intitulé: *Excursus A: On the divisors of cyclotomic functions* [Vol. III. of this Reprint, p. 317]; et en ce qui regarde la propriété des nombres cyclotomiques de la première et seconde espèce, privés de leur *facteur singulier*, d'être relativement premiers entre eux, à un article paru dans le journal *Nature* [see pp. 591, 625 of this Volume] du mois de mars de cette année*.

* Le cas de $12x+5$ (page [622] de la Note précédente) est mal expliqué. Afin de démontrer le théorème de Dirichlet pour ce cas il suffit de remarquer que chaque terme de rang impair (après le premier) dans la progression 1, 2, 5, 26, 677, ... est de la forme $12m+5$, et chacun de ses facteurs *premiers* de la forme $4x+1$, c'est-à-dire de la forme $12x+1$ ou $12x+5$; conséquemment il contiendra au moins un facteur premier de la forme $12x+5$.