Zeitschrift: L'Enseignement Mathématique
Band: 9 (1907)
Heft: 1: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: THÉORIE ÉLÉMENTAIRE DES RÉSIDUS QUADRATIQUES
Kapitel: Exercices.
Autor: Aubry, A.
DOI: https://doi.org/10.5169/seals-10133

4° Si $p = 4 + 1$, p a $\frac{p-1}{4}$ résidus biquadratiques (n° 4, VII).

5° Si $p = 8 + 1$, -1 est résidu biquadratique, ainsi que 4 et -4 (id.).

6° On démontre comme au n° précédent que, pour $p = 4 + 1$, la congruence des résidus biquadratiques est $x^{\frac{p-1}{4}} \equiv 1$, et, de là, que les $p - 1$ premiers entiers se partagent en quatre classes d'un nombre égal de termes, qui sont les racines des quatre congruences

$$x^{\frac{p-1}{4}} \equiv \pm 1 , \qquad x^{\frac{p-1}{4}} \equiv \pm f .$$

Exercices.

1. Etant donné le théorème de Fermat, si on appelle résidus et non-résidus de p les nombres qui lui sont inférieurs et qui donnent respectivement $r^m \equiv 1$ et $\rho^m \equiv -1$, on a les propositions suivantes :

Le produit de deux résidus ou de deux non-résidus est congru à un résidu et celui d'un résidu par un non-résidu l'est à un non-résidu.

Le nombre p a m résidus et m non-résidus[1].

Les résidus sont les restes de la division par p des m premiers carrés.

2. Si $p = 4 + 1$ divise $a^2 \pm kb^2$, il divise aussi $x^2 \mp ky^2$. Quelque soit k, $p = 4 - 1$ divise $x^2 + ky^2$ ou $x^2 - ky^2$. Si p divise $a^2 - kb^2$ et $c^2 - ld^2$, il divise également $x^2 - aly^2$. Si p ne divise ni $x^2 - ky^2$ ni $x^2 - ly^2$, il divise $x^2 - kly^2$. (Lagrange).

3. $B^2 - R$ étant divisible par A et $R - r$ l'étant par p, p divise ou ne divise pas A selon que r est résidu ou non-

[1] Soient n le nombre des résidus et ν celui des non-résidus. Les produits ρr, $\rho r'$, ... donneront n non-résidus différents; par suite $n \leq \nu$. La multiplication de ρ par les ν non-résidus donnerait ν résidus différents. Donc $n \leq \nu$ et $n = \nu = m$.

Cette démonstration est beaucoup plus simple que celle de Matrot (J. E. 1893, p. 74).

résidu. Ce théorème sert, dans certains cas, à décomposer les grands nombres en leurs facteurs. (Gauss [1]).

4. Le produit des résidus est $\equiv \mp 1$ et celui des non-résidus $\equiv \pm 1$, selon que $p = 4 \pm 1$. De là, le *théorème de Wilson*, que représente la congruence

$$(p-1)! + 1 \equiv 0 ,$$

et cette autre congruence, due à Libri,

$$\frac{(p-1)!}{a} + a^{p-2} \equiv 0 .$$

5. Si $p = 4 - 1$, $m! \equiv \pm 1$ selon que p a un nombre impair ou un nombre pair de résidus inférieurs à $\frac{p}{2}$ (Lejeune-Dirichlet).

6. Si $p = 4 + 1$, $(m!)^2 + 1 \equiv 0$ (Lagrange).

7. p diyise toujours $rx^2 - r'y^2$ et $\rho x^2 - \rho' y^2$, mais jamais $rx^2 - \rho y^2$. $p = 4 + 1$ divise $rx^2 + \rho y^2$ et non $rx^2 + r'y^2$ ni $\rho x^2 + \rho' y^2$; le contraire a lieu pour $p = 4 - 1$. (Euler).

8. Si $(b^2 - 4ac)$ est résidu, la congruence $ax^2 + bx + c \equiv 0$ a deux racines (Gauss). Plus généralement, la même chose a lieu si $a(b^2 - 4ac)$ est résidu (Cauchy).

9. Si $p = 4 + 1$, on a $(1 + \rho)(1 + \rho') \ldots \equiv 2$ et si $p = 4 - 1$, $(1 + r)(1 + r') \ldots \equiv 2$ (Stieltjès).

10. Pour $p = 4 + 1$, la suite $1 + \rho$, $1 + \rho'$, ... comprend $\frac{p-1}{4}$ résidus et autant de non-résidus. Si $p = 4 - 1$, la suite $1 + r$, $1 + r'$, ... comprend $\frac{p-3}{4}$ résidus et $\frac{p+1}{4}$ non-résidus (Stieltjès).

---

[1] Ainsi on a $93019 = 305^2 - 6$; comme le montre la table des résidus, 6 n'est pas résidu des nombres 7, 11, 13, 17, 31, 37, 41, 53, 61, 71, 79, 83: aucun de ces nombres ne divise donc 93019.

Or $2.93019 = 432^2 - 586$. Le reste 11 de la division de 586 par 23 est non-résidu de 23 ; donc 23 ne divise pas 93019. Le reste 27 de la division de 586 par 43 est de même non-résidu de 43, donc 43 ne divise pas 93019.

$3.93019 = 529^2 - 784 = 529^2 - 28^2 = 501.257$, d'où $93019 = 167.257$, ce qui termine le calcul. Autrement, on continuerait ainsi . $5.93019 = 682^2 - 29$; or 29 n'est résidu d'aucun des nombres 31, 37, 41, 43, 47, 61, 73, 79, 97, ... On déterminerait ainsi successivement d'autres facteurs premiers impossibles à admettre et on n'aurait plus qu'à essayer les divisions par les quelques facteurs inférieurs à $\sqrt{93019}$ qu'on n'aurait pu éliminer.

On voit l'intérêt qu'il y aurait à posséder une table des résidus des nombres premiers jusqu'à 10.000, ou même plus loin, comme le souhaitait Gauss.

11. Si ni $p-1$ ni m ne sont résidus, il y a au moins un résidu r tel que $-r-1$ soit également résidu. (Matrot).

12. Appelons *variation* la succession d'un résidu (ou non-résidu) et d'un non-résidu (ou résidu). La suite $1,2,3,\ldots p-1$, présente un nombre pair ou impair de variations selon que $p = 4 \pm 1$. (Stieltjès).

13. Si $p = 4 - 1$, la congruence $x^2 \equiv a$ a les deux racines $x \equiv \pm a^{\frac{p+1}{4}}$; si $p = 8 + 5$ et que $a^{\frac{p-1}{4}} \equiv 1$, ses racines sont $x \equiv \pm a^{\frac{p+3}{8}}$ (Legendre).

Si $p = 8 + 5$ et que $a^{\frac{p-1}{4}} \equiv -1$, les deux racines sont $x \equiv \pm a^{\frac{p+3}{8}}\, m\,!$ (Mathews).

14. *Lemme de Gauss.* Soit μ le nombre des restes obtenus en divisant par p les m premiers multiples de a, et ne conservant de ces restes que ceux qui sont plus grands que m ; on a :

$$a^m = (-1)^{\mu}$$

15. On a aussi, avec Eisenstein,

$$a^m = \prod_1^m \frac{\sin \frac{2ka\pi}{p}}{\sin \frac{2k\pi}{p}},$$

et avec Liouville,

$$a^m = (-1)^{mn} \prod_1^n (\alpha^k - \alpha^{-k})^{p-1}.$$

Dans cette dernière formule $a = 2n + 1$ et α désigne une racine imaginaire de l'équation $x^p - 1 = 0$.

16. Le nombre μ est de même parité que le produit

$$\prod \left(\frac{h}{p} - \frac{k}{a}\right)\left(\frac{h}{p} + \frac{k}{a} - \frac{1}{2}\right)$$

h variant de 1 à m et k de 1 à $\frac{a-1}{2}$ (Kronecker).

17. Appelons, avec Lagrange, $E\omega$ la partie entière du nombre non entier ω, et posons

$$f(a,b) = E\frac{a}{b} + E\frac{2a}{b} + E\frac{3a}{b} + \ldots + E\frac{\frac{b-1}{2}a}{b},$$

$$4r_n = p + \left(4n - p - 2pE\frac{2n}{p}\right)(-1)^{E\frac{2n}{p}},$$

on aura :

$$f(1,b) = 0\ ,\ f(a+b,b) = \frac{b^2-1}{8} + f(a,b) \qquad \text{(Tchebichef).}$$

$$r_a \cdot r_{2a} \cdot r_{3a} \ldots r_{ma} \equiv a^m m!\,(-1)^{f(2a,p)} \qquad \text{(id.)}$$

$$a^m \equiv (-1)^{f(2a,p)} \equiv 2^m (-1)^{f(a+p,p)} \qquad \text{(id.)}$$

$$a^m \equiv (-1)^{f(a,p)}\ . \qquad \text{(Gauss).}$$

18. Etendre la notion des résidus aux restes de carrés divisés par un nombre composé P. En particulier, si a est résidu de p, il l'est de p^n. Le nombre p^n a mp^n résidus. (Gauss).

Soit le nombre $P = ax^2 + bxy + cy^2$, où x et y sont premiers entre eux $(b^2 - 4ac)$ est résidu de P. (Gauss).

A. Aubry (Beaugency, Loiret).