Zeitschrift: L'Enseignement Mathématique

Band: 44 (1998)

Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: PARTICULAR CASE OF DIRICHLET'S THEOREM ON ARITHMETIC PROGRESSIONS

Bibliographie

Autor: Sedrakian, Naïri / Steinig, John

DOI: https://doi.org/10.5169/seals-63892

By (10), (11) and Lemma 1,

$$q \mid m^{(m,\,q-1)} - 1\,. \tag{12}$$

Suppose now that (8) does not hold. Then $(m, q-1) \mid \dfrac{m}{p_i}$ for some i, $1 \le i \le s$, whence by (12),

$$q \mid m^{m/p_i} - 1 \tag{13}$$

and therefore

$$\frac{m^m - 1}{m^{m/p_i} - 1} = \sum_{\nu=0}^{p_i-1} (m^{m/p_i})^\nu \equiv p_i \pmod{q}\,. \tag{14}$$

But (14) is impossible, for with (9) it implies that $p_i = q$, contradicting the fact that q does not divide m. This concludes the proof of the theorem.

REMARK. Several elementary proofs of this special case of Dirichlet's theorem are known; see [1], [2, §11.3], [4, §48], [5], [6], [7, §6.1A], [8, Ch. 6,5], [9], [10] and the references in [7, pp. 241–245]. They involve, more or less explicitly, the cyclotomic polynomials, say $\Phi_n(x)$. Although the proof we have given here does not require any knowledge of these polynomials, the integer N defined in (7) is in fact equal to $\Phi_m(m)$, as can be seen with Lemmas 1 and 2 and the identity [2, p. 181]

$$\Phi_n(x) = \prod_{d|n} \left(x^{n/d} - 1\right)^{\mu(d)},$$

where μ is the Möbius function (see also [4], §46).

REFERENCES

[1] ESTERMANN, T. Note on a paper of A. Rotkiewicz. *Acta Arithmetica 8* (1963), 465–467.

[2] HASSE, H. *Vorlesungen über Zahlentheorie.* 2. Auflage. Springer-Verlag (Berlin, Göttingen, Heidelberg, New York), 1964.

[3] LE BESGUE, V.-A. *Introduction à la théorie des nombres.* Mallet-Bachelier (Paris), 1862.

[4] NAGELL, T. *Introduction to Number Theory.* 2nd edition. Chelsea Publishing Co. (New York), 1964.

[5] NIVEN, I. and B. POWELL. Primes in certain arithmetic progressions. *Amer. Math. Monthly 83* (1976), 467–469.

[6] ROTKIEWICZ, A. Démonstration arithmétique de l'existence d'une infinité de nombres premiers de la forme $nk+1$. *L'Enseignement Math. (2) 7* (1961), 277–280.

[7] SHAPIRO, H. N. *Introduction to the Theory of Numbers.* John Wiley & Sons, Inc. (New York), 1983.

[8] SIERPIŃSKI, W. *Elementary Theory of Numbers.* 2nd edition (ed. A. Schinzel). North-Holland (Amsterdam, New York, Oxford) and PWN (Warszawa), 1988.

[9] SCHUR, I. Über die Existenz unendlich vieler Primzahlen in einigen speziellen arithmetischen Progressionen. *Sitzber. der Berliner Math. Ges. 11* (1912), 40–50. Reproduced in *Gesammelte Abhandlungen II* (ed. A. Brauer and H. Rohrbach), 1–11. Springer-Verlag (Berlin, Göttingen, New York), 1973.

[10] WENDT, E. Elementarer Beweis des Satzes, dass in jeder unbegrenzten arithmetischen Progression $my+1$ unendlich viele Primzahlen vorkommen. *J. für die reine und angewandte Math. 115* (1895), 85–88.

(Reçu le 30 juin 1997; version révisée reçue le 30 avril 1998)

Naïri Sedrakian

c/o Vardan Akopian
8, rue Francis de Croisset, A406
F-75018 Paris
France
e-mail: hakobian@ann.jussieu.fr

John Steinig

Section de mathématiques
Université de Genève
C.P. 240
CH-1211 Genève 24
Switzerland

vide-leer-empty