PARTICULAR CASE OF DIRICHLET'S THEOREM ON ARITHMETIC PROGRESSIONS

Autor(en): **Sedrakian, Naïri / Steinig, John**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **44 (1998)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **21.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-63892

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

L'Enseignement Mathématique, t. 44 (1998), p. 3–7

A PARTICULAR CASE OF DIRICHLET'S THEOREM ON ARITHMETIC PROGRESSIONS

by Naïri SEDRAKIAN and John STEINIG

Dirichlet's theorem on primes in an arithmetic progression states that if a and m are relatively prime integers, there exist infinitely many primes p such that $p \equiv a \pmod{m}$. We give here an elementary proof of the case in which $a = 1$.

We use the following notation. If $x_1, \ldots, x_r$ are positive integers, with $r \geq 2$, $(x_1, \ldots, x_r)$ denotes their greatest common divisor and $[x_1, \ldots, x_r]$ their least common multiple. For $r = 1$, we set $(x_1) := x_1$ and $[x_1] := x_1$.

The proof rests on three lemmas.

LEMMA 1. *If m and $a_1, \ldots, a_r$ are integers, with $m > 1$ and $a_i \geq 1$ for $1 \leq i \leq r$, then*

$$(1) \qquad \bigl(m^{a_1} - 1, \ldots, m^{a_r} - 1\bigr) = m^{(a_1, \ldots, a_r)} - 1 .$$

Proof. The case $r = 1$ is trivial. The case $r = 2$ can be established by computing $(m^{a_1} - 1, m^{a_2} - 1)$ with the euclidean algorithm; the computation runs parallel to that of (a_1, a_2). One can then continue by induction, using the associative property

$$(x_1, \ldots, x_r) = \bigl((x_1, \ldots, x_{r-1}), x_r\bigr) .$$

(For a different proof of the case $r = 2$, see [8], p. 26.)

LEMMA 2. *If* $x_1, \dots, x_r$ *are positive integers, then*

$$[x_1, \dots, x_r] = \frac{\prod_i (x_i) \prod_{i<j<k} (x_i, x_j, x_k) \cdot \dots}{\prod_{i<j} (x_i, x_j) \prod_{i<j<k<\ell} (x_i, x_j, x_k, x_\ell) \cdot \dots}, \tag{2}$$

where the numerator on the right hand side is the product of the gcd's of $x_1, \dots, x_r$, *taken* n *at a time for odd* $n = 1, 3, \dots$; *the denominator is the product of the gcd's of* $x_1, \dots, x_r$, *taken* n *at a time for even* $n = 2, 4, \dots$. *There are* 2^{r-1} *factors in the numerator and* $2^{r-1} - 1$ *in the denominator.*

Proof. The case $r = 1$ is trivial. For $r = 2$, identity (2) is the familiar

$$[x_1, x_2] = \frac{x_1 x_2}{(x_1, x_2)} . \tag{3}$$

One can continue by induction, using (3) and the associative and distributive properties

$$[x_1, \dots, x_r] = \big[[x_1, \dots, x_{r-1}], x_r\big] ,$$

respectively

$$\big([x_1, \dots, x_{r-1}], x_r\big) = \big[(x_1, x_r), \dots, (x_{r-1}, x_r)\big] .$$

(Identity (2) is due to V.-A. Le Besgue ([3], pp. 51–53), whose proof consists in showing that any prime divides both sides of (2) to the same power.)

LEMMA 3. *Let* m *be an integer,* $m > 1$; *let* $p_1, \dots, p_r$ *be distinct primes which divide* m. *Then*

$$\big[m^{m/p_1} - 1, \dots, m^{m/p_r} - 1\big] < m^m - 1 . \tag{4}$$

Proof. Since $m^m - 1$ is divisible by each integer $m^{m/p_i} - 1$ $(i = 1, \dots, r)$, it is divisible by their least common multiple. Hence (4) will be proved if we can show that

$$\big[m^{m/p_1} - 1, \dots, m^{m/p_r} - 1\big] = m^m - 1 \tag{5}$$

is impossible. To this end, we rewrite the left hand side of (5) by setting $x_i = m^{m/p_i} - 1$ in Lemma 2, and then apply Lemma 1 to the gcd's which occur. Since $p_1, \dots, p_r$ are distinct primes, we have

$$(x_{i_1}, \dots, x_{i_t}) = m^{m/p_{i_1} \cdot \dots \cdot p_{i_t}} - 1 \qquad \text{if } 1 \le i_1 < \dots < i_t \le r .$$

This will bring (5) to the form

$$\prod_{j=1}^{k}(m^{n_j}-1)=\prod_{j=k+1}^{2k}(m^{n_j}-1)\,, \tag{6}$$

with $k=2^{r-1}$ and $n_1=\frac{m}{p_1\cdot\ldots\cdot p_r}<n_j \quad (j\geq 2)$.

But (6) would imply that

$$(-1)^{k-1}(m^{n_1}-1)\equiv(-1)^k \pmod{m^{n_1+1}}\,,$$

that is, $m^{n_1+1}\mid m^{n_1}$; this is impossible, since $m>1$. This concludes the proof.

We can now prove the

THEOREM. *Let* m *be an integer,* $m>1$. *There exist infinitely many primes* p *such that* $p\equiv 1 \pmod{m}$.

Proof. By a familiar argument [10], it suffices to prove the existence, for each $m>1$, of at least one prime $p\equiv 1\pmod{m}$. (If $p_1\equiv 1\pmod{m}$ and $p_2\equiv 1\pmod{p_1m}$, then $p_2\equiv 1\pmod{m}$ and $p_2\geq p_1m+1>p_1$.)

Now let m be an integer, $m>1$, and let $p_1,\ldots,p_s$ be its distinct prime divisors. Define the integer N by

$$N:=\frac{m^m-1}{\left[m^{m/p_1}-1,\ldots,m^{m/p_s}-1\right]}\,. \tag{7}$$

Then $N>1$ by Lemma 3. Let q be any prime divisor of N; we shall show that

$$q\equiv 1 \pmod{m}\,. \tag{8}$$

Since $q\mid N$, we have

$$q\;\Big|\;\frac{m^m-1}{m^{m/p_i}-1} \quad \text{for } i=1,\ldots,s \tag{9}$$

and

$$q\mid m^m-1\,. \tag{10}$$

It follows from (10) that q does not divide m, whence

$$q\mid m^{q-1}-1\,. \tag{11}$$

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]

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

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.* 2^{nd} 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