Annals of Mathematics

An Elementary Proof of Dirichlet's Theorem About Primes in an Arithmetic Progression
Author(s): Atle Selberg
Source: *Annals of Mathematics*, Second Series, Vol. 50, No. 2 (Apr., 1949), pp. 297-304
Published by: Annals of Mathematics
Stable URL: http://www.jstor.org/stable/1969454
Accessed: 12-02-2018 13:26 UTC

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact support@jstor.org.

Your use of the JSTOR archive indicates your acceptance of the Terms & Conditions of Use, available at http://about.jstor.org/terms

Annals of Mathematics is collaborating with JSTOR to digitize, preserve and extend access to *Annals of Mathematics*

This content downloaded from 131.183.72.12 on Mon, 12 Feb 2018 13:26:56 UTC
All use subject to http://about.jstor.org/terms

ANNALS OF MATHEMATICS
Vol. 50, No. 2, April, 1949

AN ELEMENTARY PROOF OF DIRICHLET'S THEOREM ABOUT PRIMES IN AN ARITHMETIC PROGRESSION

BY ATLE SELBERG

(Received August 18, 1948)

1. A classical theorem by Dirichlet asserts that every arithmetic progression $ky + l$, where the positive integers k and l are relatively prime, represents infinitely many primes as y runs over the positive integers.

The object of this paper is to give a new and more elementary proof of this theorem. More elementary in the respect that we do not use the complex characters mod k, and also in that we consider only finite sums.

More precisely the theorem that is proved in this paper is the following:

For every positive integer k, there exist positive numbers C_k and x_0 depending only on k, such that, when $(k, l) = 1$ we have

$$\sum_{\substack{p \leqq x \\ p \equiv l(k)}} \frac{\log p}{p}^{1} > C_k \log x, \qquad \text{for} \qquad x > x_0. \tag{1.1}$$

The value we will obtain for the C_k could easily be improved, but this is of little interest.

2. Notations. We write in the following, supposing the k fixed,

$$S_l(x) = \sum_{\substack{p \leqq x \\ p \equiv l(k)}} \frac{\log p}{p}, \qquad Q_l(x) = \frac{S_l(x)}{\log x}. \tag{2.1}$$

Further $\mu(d)$ denotes the Möbius function, and

$$\lambda_d = \lambda_{d,x} = \mu(d) \log^2 \frac{x}{d}. \tag{2.2}$$

We make use of the formulas

$$\sum_{p \leqq x} \frac{\log p}{p} = \log x + O(1), \tag{2.3}$$

and, $\pi(x)$ denoting the number of primes $\leqq x$

$$\pi(x) = O\left(\frac{x}{\log x}\right), \tag{2.4}$$

which are both well known results, which can be proved elementary.

Finally $\chi(n)$ will always denote a real, non-principal character mod k.

3. In this paragraph we shall prove some important inequalities for $Q_l(x)$.

[1] Here and in the following, p always denotes prime numbers, the same holds for q and r.

This content downloaded from 131.183.72.12 on Mon, 12 Feb 2018 13:26:56 UTC
All use subject to http://about.jstor.org/terms

We start with the expression

$$\theta_n = \theta_{n,x} = \sum_{d/n} \lambda_d$$

where n is a positive integer and the summation is extended over all divisors d of n. We shall prove that

$$\theta_n = \begin{cases} \log^2 x, & \text{for } n = 1, \\ \log p \cdot \log x^2/p, & \text{for } n = p^\alpha, \quad \alpha \geqq 1, \\ 2 \log p \log q, & \text{for } n = p^\alpha q^\beta, \quad \alpha \geqq 1, \quad \beta \geqq 1, \\ 0, & \text{for all other } n. \end{cases} \tag{3.1}$$

This follows immediately when we remark, that it is clearly enough to prove it for quadrat-frei numbers. Writing $n = p_1 p_2 \cdots p_i$ where the primes are different from each other, one has

$$\theta_{p_1 p_2 \cdots p_i, x} = \theta_{p_1 p_2 \cdots p_{i-1}, x} - \theta_{p_1 p_2 \cdots p_{i-1}, x/p_i},$$

from which the result follows at once by induction.

Hence, for $(l, k) = 1$

$$\begin{aligned} \sum_{\substack{n \leqq x \\ n \equiv l(k)}} \theta_n &= \sum_{\substack{p^\alpha \leqq x \\ p^\alpha \equiv l(k)}} \log p \cdot \log \frac{x^2}{p} + \sum_{\substack{p^\alpha q^\beta \leqq x \\ p^\alpha q^\beta \equiv l(k)}} \log p \log q^2 \\ &+ O(\log^2 x) = \sum_{\substack{p \leqq x \\ p \equiv l(k)}} \log^2 p + \sum_{\substack{pq \leqq x \\ pq \equiv l(k)}} \log p \log q + O\left(\sum_{p \leqq x} \log p \cdot \log \frac{x}{p}\right) \\ &+ O\left(\log x \sum_{\substack{p^\alpha \leqq x \\ \alpha \geqq 2}} \log p\right) + O\left(\sum_{\substack{p^\alpha q^\beta \leqq x \\ \alpha \geqq 2}} \log p \log q\right) + O(\log^2 x) \\ &= \sum_{\substack{p \leqq x \\ p \equiv l(k)}} \log^2 p + \sum_{\substack{pq \leqq x \\ pq \equiv l(k)}} \log p \log q + O(x), \end{aligned} \tag{3.2}$$

where the O-terms are easily estimated by means of (2.4) and (2.3).

On the other hand we have

$$\sum_{\substack{n \leqq x \\ n \equiv l(k)}} \theta_n = \sum_{\substack{d \leqq x \\ (d,k)=1}} \lambda_d \sum_{\substack{d/n \\ n \leqq x \\ n \equiv l(k)}} 1 = \frac{x}{k} \sum_{\substack{d \leqq x \\ (d,k)=1}} \frac{\lambda_d}{d} + O\Big(\sum_{d \leqq x} |\lambda_d|\Big) = \frac{x}{k} \sum_{\substack{d \leqq x \\ (d,k)=1}} \frac{\lambda_d}{d} + O(x),$$

since

$$\sum_{d \leqq x} |\lambda_d| \leqq \sum_{d \leqq x} \log^2 \frac{x}{d} = O(x).$$

---

[2] We may omit the factor 2 before this sum by counting $p^\alpha q^\beta$ as different from $q^\beta p^\alpha$.

This content downloaded from 131.183.72.12 on Mon, 12 Feb 2018 13:26:56 UTC
All use subject to http://about.jstor.org/terms

Comparing this with (3.2) we get

$$\sum_{\substack{p \leqq x \\ p \equiv l(k)}} \log^2 p + \sum_{\substack{pq \leqq x \\ pq \equiv l(k)}} \log p \log p = \frac{x}{k} \sum_{\substack{d < x \\ (d,k)=1}} \frac{\lambda_d}{d} + O(x).^3$$

By summing over all residues l mod. k and observing that for $(l, k) > 1$ the left-hand side of the above formula is $O(x)$ by (2.4), we get if $\varphi(k)$ denotes Eulers function,

$$\sum_{\substack{p \leqq x \\ p \equiv l(k)}} \log^2 p + \sum_{\substack{pq \leqq x \\ pq \equiv l(k)}} \log p \log q$$

(3.3)

$$= \frac{1}{\varphi(k)} \{ \sum_{p \leqq x} \log^2 p + \sum_{pq \leqq x} \log p \log q \} + O(x).$$

From this we deduce by partial summation

$$\sum_{\substack{p \leqq x \\ p \equiv l(k)}} \frac{\log^2 p}{p} + \sum_{\substack{pq \leqq x \\ pq \equiv l(k)}} \frac{\log p \log q}{pq} = \frac{1}{\varphi(k)}$$

(3.4)

$$\left\{ \sum_{p \leqq x} \frac{\log^2 p}{p} + \sum_{pq \leqq x} \frac{\log p \log q}{pq} \right\} + O(\log x) = \frac{1}{\varphi(k)} \log^2 x + O(\log x),$$

the last form being obtained by summing $\sum_{p \leqq x} \log^2 p/p$ and $\sum_{p \leqq x} \log p/p$ $\sum_{q \leqq x/p} \log q/q$ by means of (2.3).

In the same way we deduce from (3.3) that

$$\sum_{\substack{p \leqq x \\ p \equiv l(k)}} \frac{\log^3 p}{p} + \sum_{\substack{pq \leqq x \\ pq \equiv l(k)}} \frac{\log p \log q}{pq} \log pq = \frac{2}{3\varphi(k)} \log^3 x + O(\log^2 x),$$

or

$$\sum_{\substack{p \leqq x \\ p \equiv l(k)}} \frac{\log p^3}{p} + 2 \sum_{\substack{pq \leqq x \\ pq \equiv l(k)}} \frac{\log p \log^2 q}{pq} = \frac{2}{3\varphi(k)} \log^3 x + O(\log^2 x), \tag{3.5}$$

writing now

$$\sum_{\substack{pq \leqq x \\ pq \equiv l(k)}} \frac{\log p \log^2 q}{pq} = \sum_{\substack{p < x \\ p \nmid k}} \frac{\log p}{p} \sum_{\substack{q \leqq x/p \\ q \equiv l\bar{p}(k)}} \frac{\log^2 q}{q},$$

where $\bar{p}$ is determined by $p\bar{p} \equiv 1(k)$. Using now (3.4) for the last sum we get:

$$\sum_{\substack{pq \leqq x \\ pq \equiv l(k)}} \frac{\log p \log^2 q}{pq} = \frac{1}{\varphi(k)} \sum_{p \leqq x} \frac{\log p}{p} \log^2 \frac{x}{p} - \sum_{p \leqq x} \frac{\log p}{p}$$

$$\sum_{\substack{qr \leqq x/p \\ qr \equiv l\bar{p}(k)}} \frac{\log q \log r}{qr} + O\left(\sum_{p \leqq x} \frac{\log p}{p} \log x \right)$$

$$= -\sum_{\substack{pqr \leqq x \\ pqr \equiv l(k)}} \frac{\log p \log q \log r}{pqr} + \frac{1}{3\varphi(k)} \log^3 x + O(\log^2 x),$$

[3] It is possible to estimate this series elementary, one finds it is $2^1/\varphi(k) \log x + O(1)$. From the resulting formula one can give an elementary proof of the prime-number theorem.

This content downloaded from 131.183.72.12 on Mon, 12 Feb 2018 13:26:56 UTC
All use subject to http://about.jstor.org/terms

since one easily deduces from (2.3) that

$$\sum_{p\leqq x}\frac{\log p}{p}\log^2\frac{x}{p}=\tfrac{1}{3}\log^3 x+O(\log^2 x).$$

Inserting the above result in (3.5) one gets

$$\sum_{\substack{p\leqq x\\ p\equiv l(k)}}\frac{\log^3 p}{p}=2\sum_{\substack{pqr\leqq x\\ pqr\equiv l(k)}}\frac{\log p\log q\log r}{pqr}+O(\log^2 x). \tag{3.6}$$

Again from (3.4) we deduce that

$$\sum_{\substack{p\leqq x\\ p\equiv l(k)}}\frac{\log^2 p}{p}\leqq\frac{1}{\varphi(k)}\log^2 x+O(\log x),$$

from which we easily find, by partial summation,

$$\sum_{\substack{p\leqq x\\ p\equiv l(k)}}\frac{\log p}{p}\leqq\frac{2}{\varphi(k)}\log x+O(\log\log x). \tag{3.7}$$

Now by (3.7)

$$\begin{aligned}\sum_{\substack{pq\leqq x\\ pq\equiv l(k)}}\frac{\log p\log q}{pq}&\leqq\sum_{\substack{p\leqq x^{1/3}\\ pq\equiv l(k)}}\sum_{q\leqq x^{1/3}}\frac{\log p\log q}{pq}+2\sum_{x^{1/3}<p\leqq x}\frac{\log p}{p}\sum_{\substack{q\leqq x/p\\ q\equiv l\bar{p}(k)}}\frac{\log q}{q}\\ &\leqq\sum_{\substack{p\leqq x^{1/3}\\ pq\equiv l(k)}}\sum_{q\leqq x^{1/3}}\frac{\log p\log q}{pq}+\frac{4}{\varphi(k)}\sum_{x^{1/3}<p\leqq x}\frac{\log p}{p}\log\frac{x}{p}\\ &\quad+O\left(\log\log x\sum_{p\leqq x}\frac{\log p}{p}\right)=\sum_{\substack{p\leqq x^{1/3}\\ pq\equiv l(k)}}\sum_{q\leqq x^{1/3}}\frac{\log p\log q}{pq}\\ &\quad+\frac{8}{9\varphi(k)}\log^2 x+O(\log x\log\log x,\end{aligned}$$

by (2.3). Inserting this in (3.4) we get

$$\sum_{\substack{p\leqq x\\ p\equiv l(k)}}\frac{\log^2 p}{p}\geqq\frac{1}{9\varphi(k)}\log^2 x-\sum_{\substack{p\leqq x^{1/3}\\ pq\equiv l(k)}}\sum_{q\leqq x^{1/3}}\frac{\log p\log q}{pq}+O(\log x\log\log x),$$

or, for $x>x_0$

$$\log x\sum_{\substack{p\leqq x\\ p\equiv l(k)}}\frac{\log p}{p}>\frac{1}{10\varphi(k)}\log^2 x-\sum_{\substack{p\leqq x^{1/3}\\ pq\equiv l(k)}}\sum_{q\leqq x^{1/3}}\frac{\log p\log q}{pq},$$

from which

$$\log x\cdot S_l(x)>\frac{1}{10\varphi(k)}\log^2 x-\sum_{mm'\equiv l(k)}S_m(x^{1/3})S_{m'}(x^{1/3}),$$

This content downloaded from 131.183.72.12 on Mon, 12 Feb 2018 13:26:56 UTC
All use subject to http://about.jstor.org/terms

where the sum is taken over all pairs of residues mod. k with $mm' \equiv l(k)$. Dividing by $\log^2 x$ we get

$$(3.8) \qquad Q_l(x) > \frac{1}{10\varphi(k)} - \frac{1}{9} \sum_{mm' \equiv l(k)} Q_m(x^{1/3}) Q_{m'}(x^{1/3}), \quad \text{for} \quad x > x_0.$$

In a similar way, we get from (3.6) that

$$(3.9) \qquad Q_l(x) \geqq \frac{2}{27} \sum_{mm'm'' \equiv l(k)} Q_m(x^{1/3}) Q_{m'}(x^{1/3}) Q_{m''}(x^{1/3}) - O\left(\frac{1}{\log x}\right).$$

(3.7) gives

$$(3.10) \qquad Q_l(x) \leqq \frac{2}{\varphi(k)} + O\left(\frac{\log \log x}{\log x}\right).$$

4. We now proceed to prove the following

LEMMA 1. *For every real, nonprincipal character* χ mod k *we have*

$$\sum_{\substack{p \leqq x \\ \chi(p)=1}} \frac{\log p}{p} > \frac{1}{9} \log x \quad \textit{for} \quad x > x_0.$$

We make use of the fact, which can be deduced from the law of reciprocity for the quadratic residue symbols, that to each χ there exist an integer D which is not a square and $|D| < k^2$, such that for all primes p we have $\chi(p) = (D/p)$ where (D/p) is the ordinary quadratic residue symbol.[4] What we shall prove then is

$$(4.1) \qquad \sum_{\substack{p \leqq x \\ (D/p)=1}} \frac{\log p}{p} > \frac{1}{9} \log x \quad \text{for } x > x_0.$$

We consider the product

$$(4.2) \qquad P = \prod_{\substack{|u| \leqq \sqrt{x/2} \\ |v| \leqq \sqrt{x/2p}}}' |u^2 - Dv^2|$$

where the dash $\prod'$ indicates that the term $u = 0$, $v = 0$ is omitted. It is easily seen that for $x > x_0$

$$(4.3) \qquad \log P > \frac{x}{\sqrt{D}} \log x.$$

Let us estimate the exponent of the highest power of a prime p which divides P. First suppose that $(D/p) = 1$. We try to estimate how many solutions the congruence

$$u^2 - Dv^2 \equiv 0(p),$$

[4] See for instance Dirichlet-Dedekind: Vorlesungen über Zahlentheorie, the beginning of §135.

This content downloaded from 131.183.72.12 on Mon, 12 Feb 2018 13:26:56 UTC
All use subject to http://about.jstor.org/terms

has in the given range for u and v. We suppose that there is a solution (u_o, v_o),[5] then we see that if (u, v) is another we have

$$(uv_o)^2 - (u_o v)^2 \equiv 0(p),$$

or one of the congruences

$$uv_o \pm u_o v \equiv 0(p),$$

must be satisfied. The number of solutions in the given range for u and v of these congruences is easily estimated to be less than

$$\frac{4x}{p\sqrt{D}} + O\left(\sqrt{\frac{x}{p}}\right).$$

Thus at most $8x/(p\sqrt{D}) + O(\sqrt{x/p})$ of the numbers $u^2 - Dv^2$ contain the prime p as a factor, and in the same manner, we prove that at most

$$\frac{8x}{p^\alpha\sqrt{D}} + O\left(\sqrt{\frac{x}{p^\alpha}}\right)$$

of the $u^2 - Dv^2$ contain the factor p^α. Thus the product P contains p to a power less than

$$\frac{8}{p-1}\frac{x}{\sqrt{D}} + O\left(\sqrt{\frac{x}{p}}\right) = \frac{8}{p}\frac{x}{\sqrt{D}} + O\left(\sqrt{\frac{x}{p}}\right).$$

On the other hand if $(D/p) = -1$, we easily see, that since p has to divide both u and v in order to divide $u^2 - Dv^2$, the product P will contain p to a power less than

$$O\left(\frac{x}{p^2}\right).$$

Finally if $(D/p) = 0$, or p/D, we have that P contains p to a power less than

$$O\left(\frac{x}{p}\right).$$

These results give

$$\begin{aligned}\log P &\leqq 8\frac{x}{\sqrt{D}}\sum_{\substack{p\leqq x\\(D/p)=-1}}\frac{\log p}{p} + O\left(\sqrt{x}\sum_{p\leqq x}\frac{\log p}{\sqrt{p}}\right)\\ &\quad + O\left(x\sum_{p\leqq x}\frac{\log p}{p^2}\right) + O\left(x\sum_{p/D}\frac{\log p}{p}\right)\\ &= 8\frac{x}{\sqrt{D}}\sum_{\substack{p\leqq x\\(D/p)=1}}\frac{\log p}{p} + O(x).\end{aligned}$$

[5] (u_o, v_o) is assumed to be a nontrivial solution, i.e. $(u_o, p) = (v_o, p) = 1$.

This content downloaded from 131.183.72.12 on Mon, 12 Feb 2018 13:26:56 UTC
All use subject to http://about.jstor.org/terms

Comparing this with (4.3) we get

$$\sum_{\substack{p \leqq x \\ (D/p)=1}} \frac{\log p}{p} + O(1) > \tfrac{1}{6} \log x,$$

or

$$\sum_{\substack{p \leqq x \\ (D/p)=1}} \frac{\log p}{p} > \tfrac{1}{6} \log x \quad \text{for} \quad x > x_0,$$

which proves our lemma.

5. LEMMA 2. *Suppose that we have a set of different residues* $m_1, m_2, \cdots m_h$ mod k, *such that they all are relatively prime to* k. *Further suppose that* $h \geqq \frac{1}{2}(\varphi(k))$, *and that to each real character* χ mod k, *we can find an* m *in the set with* $\chi(m) = 1$. *Let* $(l, k) = 1$, *and suppose that there is a* m *and* m', *not necessarily different, belonging to the set for which* $mm' \equiv l(k)$. *Then we can find a triple of residues belonging to the set* (m, m', m'')[6] *such that*

$$mm'm'' \equiv l(k).$$

Assume that always

$$m_{i_1} m_{i_2} m_{i_3} \not\equiv l(k),$$

or

$$m_{i_1} m_{i_2} \not\equiv l\bar{m}_{i_3}(k). \tag{5.1}$$

Since the left-hand side can assume at least h different[7] values and the right-hand side h different values, we see that the lemma is true for $h > \frac{1}{2}(\varphi(k))$. Thus we will assume $h = \frac{1}{2}(\varphi(k))$. Then we see from (5.1) that the product $m_{i_1} m_{i_2}$ can assume only h different values. Writing $n_i = m_i \bar{m}_1$ the same will be the case with the h residues $n_1 = 1, n_2, \cdots, n_h$. From this we see that these residues form a group with respect to multiplication. We then define a real character $\chi(n)$ which is 1 for $n_1, n_2, \cdots, n_h$ and -1 for the other h residues. For this character we would have for $i = 1, 2, \cdots, h$,

$$\chi(m_i) = \chi(m_1).$$

According to the assumption, there is at least one m_i with $\chi(m_i) = 1$, so that for all m_i, $\chi(m_i) = 1$. From this we get $\chi(l) = \chi(m)\chi(m') = 1$ so that both 1 and l will be found in the set of m_i, since $1.1.l \equiv l(k)$, this contradicts (5.1) so our lemma is completely proved.

6. We are now able to prove the theorem stated in section 1. More precisely we will show that

$$Q_l(x) > \frac{1}{(20)^4(\varphi(k))^6} \quad \text{for} \quad x > x_0. \tag{6.1}$$

[6] The m and m' do not necessarily mean the same residues as in the preceding congruence.

[7] When we say different we mean different mod k.

This content downloaded from 131.183.72.12 on Mon, 12 Feb 2018 13:26:56 UTC
All use subject to http://about.jstor.org/terms

Let us assume that

$$Q_l(x) < \frac{1}{30\varphi(k)}, \tag{6.2}$$

for some large x. From (3.10) we see that since by (2.3),

$$\sum_n Q_n(x^{1/3}) = 1 + O\left(\frac{1}{\log x}\right),$$

we can find at least $\frac{1}{2}(\varphi(k))$ values m for which

$$Q_m(x^{1/3}) > \frac{1}{20(\varphi(k))^2} \quad \text{for} \quad x > x_0 .$$

Further from Lemma 1, for any real non-principal character

$$\sum_{\chi(n)=1} Q_n(x^{1/3}) > \tfrac{1}{9} \quad \text{for} \quad x > x_0 ,$$

so that there exist at least one $Q_m(x1/3) > \frac{1}{2}(9\varphi(k))$ with $\chi(m) = 1$. Finally from (3.8) and (6.2),

$$\sum_{nn' \equiv l(k)} Q_n(x^{1/3})Q_{n'}(x^{1/3}) > \frac{1}{15\varphi(k)},$$

so that there exists at least one pair of residues m, m' with $mm' \equiv l(k)$ and

$$Q_m(x^{1/3})Q_{m'}(x^{1/3}) > \frac{1}{15(\varphi(k))^2}$$

or by (3.10)

$$Q_m(x^{1/3}) > \frac{1}{31\varphi(k)} > \frac{1}{20(\varphi(k))^2}, \qquad Q_{m'}(x^{1/3}) > \frac{1}{20(\varphi(k))^2}.$$

Thus we can find a set of different residues mod k, $m_1, m_2, \cdots, m_h$ with $h \geqq \frac{1}{2}(\varphi(k))$ so that

$$Q_{m_i}(x^{1/3}) > \frac{1}{20(\varphi(k))^2}$$

for $i = 1, 2, \cdots, h$, and that further to each real character χ there is a m_i with $\chi(m_i) = 1$, and finally there exist residues m, m' belonging to this set, such that $mm' \equiv l(k)$.

From Lemma 2 we then conclude that there exist residues m, m', m'' in this set with $mm'm'' \equiv l(k)$. Then (3.9) gives

$$Q_l(x) \geqq \frac{2}{27} Q_m(x^{1/3})Q_{m'}(x^{1/3})Q_{m''}(x^{1/3}) - O\left(\frac{1}{\log x}\right) > \frac{1}{(20)^4(\varphi(k))^6},$$

for $x > x_0$, which proves our theorem.

THE INSTITUTE FOR ADVANCED STUDY

This content downloaded from 131.183.72.12 on Mon, 12 Feb 2018 13:26:56 UTC
All use subject to http://about.jstor.org/terms