

A NOTE ON LINNIK'S THEOREM ON QUADRATIC NON-RESIDUES

PAUL BALISTER, BÉLA BOLLOBÁS, JONATHAN D. LEE, ROBERT MORRIS,
AND OLIVER RIORDAN

ABSTRACT. We present a short and purely combinatorial proof of Linnik's Theorem: for any $\varepsilon > 0$ there exists a constant C_ε such that for any N , there are at most C_ε primes $p \leq N$ such that the least positive quadratic non-residue modulo p exceeds N^ε .

1. INTRODUCTION

In 1941, Linnik [7] developed the Large Sieve and used it (in [8]) to prove that for any $\varepsilon > 0$ there is a constant C_ε such that for all N , there are at most C_ε primes $p \leq N$ such that the least quadratic non-residue modulo p exceeds N^ε . The Large Sieve was subsequently developed as a theorem about quasi-independent functions by Rényi [10, 11, 12, 13], and as a theorem on duality and an approximate Plancherel identity by Bombieri [2] and Roth [14]. Modern presentations include [3, 5].

The techniques of these proofs are ultimately analytic, and relate Fourier analysis on the circle to the discrete Fourier transform on $\mathbb{Z}/p\mathbb{Z}$. In this paper, we present a direct combinatorial (or 'elementary') proof of Linnik's Theorem, based on an explicit (and extremely simple) combinatorial sieve. To deduce Linnik's Theorem using this sieve we will need only a (very weak) estimate on smooth numbers, which itself has a simple combinatorial proof (see [1]). In particular, we avoid using standard results such as the Prime Number Theorem, which despite having an elementary proof (see [6]), is far deeper than the result we wish to show.

2. THE COMBINATORIAL SIEVE

The following simple combinatorial inequality is the key ingredient of our proof.

Lemma 1. *For any sets $A_1, \dots, A_d \subseteq [n] = \{1, 2, \dots, n\}$,*

$$(d+1)^2 \left| \bigcap_{i=1}^d A_i \right| \leq (d+1)^2 n - 4d \sum_{i=1}^d |A_i^c| + 4 \sum_{i \neq j} |A_i^c \cap A_j^c|.$$

Proof. Suppose $x \in [n]$ is in ℓ of the sets A_i^c . Then on the right-hand side it is counted

$$(d+1)^2 - 4d\ell + 4\ell(\ell-1) = (d+1-2\ell)^2 \geq 0$$

times and, if it is in all of the sets A_i , it is counted exactly $(d+1)^2$ times. □

3. LINNIK'S THEOREM

A positive integer m is called y -smooth if for any prime p dividing m , $p \leq y$; we write $\Psi(n, y)$ for the number of y -smooth numbers in the set $\{1, \dots, [n]\}$. For any prime number p , let n_p be the least positive quadratic non-residue modulo p .

Theorem 2. Fix $N > B \geq 2$ with N an integer. Let $\mathcal{P} = \{p \leq N : p \text{ is prime and } n_p > B\}$ and let $d = |\mathcal{P}|$. Then $(d+1)\Psi(N^3, B) \leq (5 + dB^{-2})N^3$.

Proof. Fix n (to be chosen later) and, for each $p_i \in \mathcal{P}$, let $A_i = \{x \in [n] : \left(\frac{x}{p_i}\right) = 1\}$. Each A_i contains all primes less than or equal to B . Furthermore, if $x, y \in A_i$ and $xy \leq n$, then $xy \in A_i$. Hence,

$$\left| \bigcap_{i=1}^d A_i \right| \geq \Psi(n, B).$$

The set A_i^c contains all integers up to n in $(p_i + 1)/2$ of the congruence classes modulo p_i , so

$$|A_i^c| \geq \frac{n}{2} \left(1 + \frac{1}{p_i}\right) - p_i,$$

and hence

$$4d \sum_{i=1}^d |A_i^c| \geq 2d^2 n + 2dn \sum_{p \in \mathcal{P}} \frac{1}{p} - 4d \sum_{p \in \mathcal{P}} p.$$

By the Chinese Remainder Theorem, when $i \neq j$ the set $A_i^c \cap A_j^c$ contains all integers up to n in $(p_i + 1)(p_j + 1)/4$ of the congruence classes modulo $p_i p_j$. Thus

$$|A_i^c \cap A_j^c| \leq \frac{n}{4} \left(1 + \frac{1}{p_i}\right) \left(1 + \frac{1}{p_j}\right) + p_i p_j,$$

and hence

$$4 \sum_{i \neq j} |A_i^c \cap A_j^c| \leq d(d-1)n + 2(d-1)n \sum_{p \in \mathcal{P}} \frac{1}{p} + n \sum_{p, q \in \mathcal{P}, p \neq q} \frac{1}{pq} + 4 \sum_{p, q \in \mathcal{P}, p \neq q} pq.$$

Hence, by Lemma 1,

$$\begin{aligned} (d+1)^2 \Psi(n, B) &\leq (d+1)^2 n - 2d^2 n - 2dn \sum_{p \in \mathcal{P}} \frac{1}{p} + 4d \sum_{p \in \mathcal{P}} p \\ &\quad + d(d-1)n + 2(d-1)n \sum_{p \in \mathcal{P}} \frac{1}{p} + n \sum_{p, q \in \mathcal{P}, p \neq q} \frac{1}{pq} + 4 \sum_{p, q \in \mathcal{P}, p \neq q} pq \\ &\leq (d+1)n + 4d \sum_{p \in \mathcal{P}} p + n \sum_{p, q \in \mathcal{P}, p \neq q} \frac{1}{pq} + 4 \sum_{p, q \in \mathcal{P}, p \neq q} pq. \end{aligned}$$

Note that $n_p \leq p$, and so each $p \in \mathcal{P}$ is at least B and at most N . Hence

$$(d+1)^2 \Psi(n, B) \leq (d+1)n + 4d^2 N + \frac{nd^2}{B^2} + 4d^2 N^2.$$

We now fix $n = N^3$. Then, as $d \leq N$,

$$(d+1)^2 \Psi(N^3, B) \leq (d+1)N^3 + 4N^3 + d^2 B^{-2} N^3 + 4dN^3,$$

and so $(d+1)\Psi(N^3, B) \leq (5 + dB^{-2})N^3$ as claimed. \square

One of the earliest results on $\Psi(n, y)$ was obtained by Dickman [4] in 1930. To deduce Linnik's Theorem we will need only the following weak version of his result.

Lemma 3. *For any $u > 0$, there exists a constant $c_u > 0$ such that*

$$\Psi(n, n^{1/u}) \geq c_u n$$

for all real $n \geq 1$.

An elementary proof can be found in [1], based in turn on an elementary proof (inspired by one given by Erdős) of a very weak form of Merten's Theorem, namely the inequality $\sum_{n^{1-\varepsilon} < p \leq n} \frac{1}{p} \geq \varepsilon + o(1)$.

Corollary 4 (Linnik's Theorem). *Fix $\varepsilon > 0$. Then there is a constant C_ε such that for all N there are at most C_ε primes $p \leq N$ with $n_p > N^\varepsilon$.*

Proof. By Lemma 3, applied with $u = 3/\varepsilon$ and $n = N^3$, we have that $\Psi(N^3, N^\varepsilon) \geq c_{3/\varepsilon} N^3$. By Theorem 2, the number d of primes $p \leq N$ with $n_p > B = N^\varepsilon$ satisfies

$$d\Psi(N^3, N^\varepsilon) \leq (d+1)\Psi(N^3, N^\varepsilon) \leq 5N^3 + dN^{3-2\varepsilon}.$$

Thus

$$d \leq \frac{5N^3}{\Psi(N^3, N^\varepsilon) - N^{3-2\varepsilon}} \leq \frac{5}{c_{3/\varepsilon} - N^{-2\varepsilon}},$$

which is bounded as $N \rightarrow \infty$. \square

ACKNOWLEDGEMENT

The work of the first two authors was partially supported by NSF grant DMS 1600742, and work of the second author was also partially supported by MULTIPLEX grant 317532. The work of the fourth author was partially supported by CNPq (Proc. 303275/2013-8) and FAPERJ (Proc. 201.598/2014). The research in this paper was carried out while the third, fourth and fifth authors were visiting the University of Memphis.

REFERENCES

- [1] P. Balister, B. Bollobás, J.D. Lee, R. Morris and O. Riordan, A note on Linnik's Theorem on quadratic non-residues, arXiv:1712.07179.
- [2] E. Bombieri, On the large sieve, *Mathematika*, **12** (1965), 201–225.
- [3] A.C. Cojocaru and M.R. Murty, An introduction to sieve methods and their applications, London Mathematical Society Student Texts, **66**, Cambridge University Press, 2006.
- [4] K. Dickman, On the frequency of numbers containing prime factors of a certain relative magnitude, *Ark. Mat. Astron. Fys.*, **22** (1930), 1–14.

- [5] J.B. Friedlander and H. Iwaniec, *Opera de cribro*, American Mathematical Society Colloquium Publications, vol. 57, American Mathematical Society, Providence, RI, 2010.
- [6] D. Goldfeld, The elementary proof of the Prime Number Theorem: an historical perspective, In: *Number Theory* (Chudnovsky D., Chudnovsky G., Nathanson M., eds), pp. 179–192, Springer, New York, 2004.
- [7] U.V. Linnik, The large sieve, *C. R. (Doklady) Acad. Sci. URSS (N.S.)*, **30** (1941), 292–294.
- [8] U.V. Linnik, A remark on the least quadratic non-residue, *C. R. (Doklady) Acad. Sci. URSS (N.S.)*, **36** (1942), 119–120.
- [9] F. Mertens, Ein Beitrag zur analytischen Zahlentheorie, *J. Reine Angew. Math.*, **78** (1874), 46–62.
- [10] A. Rényi, On the representation of an even number as the sum of a single prime and a single almost-prime number, *Doklady Akad. Nauk SSSR (N.S.)*, **56** (1947), 455–458.
- [11] A. Rényi, Un nouveau théorème concernant les fonctions indépendantes et ses applications à la théorie des nombres, *J. Math. Pures Appl.*, **28** (1949), 137–149.
- [12] A. Rényi, On the large sieve of Ju.V. Linnik, *Compos. Math.*, **8** (1951), 68–75.
- [13] A. Rényi, New version of the probabilistic generalization of the large sieve, *Acta Math. Acad. Sci. Hung.*, **10** (1959), 217–226.
- [14] K.F. Roth, On the large sieves of Linnik and Rényi, *Mathematika*, **12** (1965), 1–9.

DEPARTMENT OF MATHEMATICAL SCIENCES, UNIVERSITY OF MEMPHIS, MEMPHIS TN 38152, USA
Email address: pbalistr@memphis.edu

DEPARTMENT OF PURE MATHEMATICS AND MATHEMATICAL STATISTICS, UNIVERSITY OF CAMBRIDGE, WILBERFORCE ROAD, CAMBRIDGE CB30WB, UK; *and* DEPARTMENT OF MATHEMATICAL SCIENCES, UNIVERSITY OF MEMPHIS, MEMPHIS TN 38152, USA; *and* LONDON INSTITUTE FOR MATHEMATICAL SCIENCES, 35A SOUTH ST., MAYFAIR, LONDON W1K 2XF, UK
Email address: b.bollobas@dpmms.cam.ac.uk

MICROSOFT RESEARCH, REDMOND, USA
Email address: jonatlee@microsoft.com

IMPA, ESTRADA DONA CASTORINA 110, JARDIM BOTÂNICO, RIO DE JANEIRO, RJ, BRAZIL
Email address: rob@impa.br

MATHEMATICAL INSTITUTE, UNIVERSITY OF OXFORD, RADCLIFFE OBSERVATORY QUARTER, WOODSTOCK ROAD, OXFORD OX2 6GG, UK
Email address: riordan@maths.ox.ac.uk