[16] L. Carlitz, *Arithmetic properties of generalized Bernoulli numbers*, J. Reine Angew. Math. 202 (1959), pp. 174–182.
[17] S. Chowla, *On some formulae resembling the Euler–Maclaurin sum formula*, Norske Vid. Selsk. Forh. (Trondheim) 34 (1961), pp. 107–109.
[18] Harold Davenport, *Multiplicative Number Theory*, Chicago 1967.
[19] D. Davies and C. B. Haselgrove, *The evaluation of Dirichlet L-functions*, Proc. Royal Soc. London Ser. A 264 (1961), pp. 122–132.
[20] G. Lejeune Dirichlet, *Sur l'usage des intégrales définies dans la sommation des séries finies ou infinies*, J. Reine Angew. Math. 17 (1837), pp. 57–67; *G. Lejeune Dirichlet's Werke*, Berlin 1889, vol. 1, pp. 257–270.
[21] Cecil E. Duncan, *On the asymptotic behavior of trigonometric sums*, Second communication, Koninklijke Nederlandse Akademie van Wetenschappen, Proceedings (A) 60 (1957), pp. 369–373; Indag. Math. 19 (1957), pp. 369–373.
[22] Paul Epstein, *Zur Theorie allgemeiner Zetafunktionen*, Math. Ann. 56 (1902), pp. 615–644.
[23] — *Zur Theorie allgemeiner Zetafunktionen. II*, Math. Ann. 63 (1907), pp. 205–216.
[24] Tomlinson Fort, *Finite Differences and Difference Equations in the Real Domain*, Oxford 1948.
[25] F. B. Hildebrand, *Introduction to Numerical Analysis*, New York 1956.
[26] L. K. Hua, *Additive Theory of Prime Numbers*, Translations of Mathematical Monographs, vol. 13, Amer. Math. Soc., Providence, Rhode Island 1965.
[27] C. Jordan, *Calculus of Finite Differences*, Budapest 1939; 2nd ed., New York 1947.
[28] Konrad Knopp, *Theory and Application of Infinite Series*, London 1951.
[29] E. Landau, *Vorlesungen über Zahlentheorie*, Leipzig 1927; reprinted New York 1947, 3 vols.
[30] G. Landsberg, *Zur Theorie der Gauss'schen Summen und der linearen Transformationen der Thetafunctionen*, J. Reine Angew. Math. 111 (1893), pp. 234–253.
[31] Heinrich-Wolfgang Leopoldt, *Eine Verallgemeinerung der Bernoullischen Zahlen*, Abh. Math. Sem. Univ. Hamburg 22 (1958), pp. 131–140.
[32] M. Lerch, *Zur Theorie der Gauss'schen Summen*, Math. Ann. 57 (1903), pp. 554–567.
[33] R. Lipschitz, *Untersuchung der Eigenschaften einer Gattung von unendlichen Reihen*, J. Reine Angew. Math. 105 (1889), pp. 127–156.
[34] Kurt Mahler, *Eine Bemerkung zum Beweis der Eulerschen Summenformel*, Mathematica (Zutphen) (B) 7 (1938), pp. 33–42.
[35] L. J. Mordell, *Some applications of Fourier series in the analytic theory of numbers*, Proc. Cambridge Philos. Soc. 24 (1928), pp. 585–596.
[36] W. D. Munro, *Note on the Euler–Maclaurin formula*, Amer. Math. Monthly 65 (1958), pp. 201–203.
[37] Niels Erik Nörlund, *Vorlesungen über Differenzenrechnung*, Die Grundlehren der mathematischen Wissenschaften, 13, Berlin 1924; New York 1954.
[38] A. M. Ostrowski, *On the remainder term of the Euler–Maclaurin formula*, J. Reine Angew. Math. 239/240 (1970), pp. 268–286.
[39] Hans Rademacher, *Topics in Analytic Number Theory*, Berlin 1973.
[40] J. Barkley Rosser and Lowell Schoenfeld, *Approximation of the Riemann zeta-function* (to appear).
[41] E. C. Titchmarsh, *The Theory of Functions*, 2nd ed., London 1939.
[42] — *The Theory of the Riemann Zeta-function*, Oxford 1951.

Received on 27. 11. 1973 (495)

ACTA ARITHMETICA
XXVIII (1975)

An asymptotic inequality concerning primes in contours for the case of quadratic number fields

by

DOUGLAS HENSLEY (Minneapolis, Minn.)

Introduction. Our main result is an extension to quadratic number fields of the result that, assuming Schinzel's Hypothesis H, $\pi(x+y)$ sometimes exceeds $\pi(x)+\pi(y)$ (cf. [6], [15]).

To be concrete and definite, we will at first concentrate on the Gaussian integers. Later we show what modifications are needed to carry over to other quadratic number fields.

For any "reasonable" bounded region S in the complex plane we ask whether, as S expands homothetically, there must appear Gaussian integers y for which the translate by y of our region contains more prime Gaussian integers than the region itself.

Let us temporarily assume Hypothesis H. We may then state our principle result in the following form:

THEOREM 1. *If S is not "logarithmically centered on zero"* (definition to follow), *then*

(1) *For all sufficiently large x there exist arbitrarily large Gaussian integers y for which the translate $xS+y$ contains more prime Gaussian integers than xS.*

Remark. Since on the average there will be fewer primes in $xS+y$ as $|y|$ increases, (1) states that there are exceptions to this average behavior, and that thick clusters of primes will occur arbitrarily far from the origin. Of course, these clusters may be few and far between.

DEFINITION. A *logarithmic center* of a region S is a complex number α which minimizes $f(\alpha) = \int_S \log|z-\alpha|\,d\text{area}$; S is *logarithmically centered* if zero is a logarithmic center of S.

Remark. It is easy to show that minimizing $f(\alpha)$ maximizes (as $x\to\infty$),

$$\mathrm{Li}[x(S-\alpha)] = \frac{2}{\pi}\int_{x(S-\alpha)\cap\{|z|>2\}} \frac{d\,\text{area}}{\log|z|}. \tag{2}$$

Now the "prime number theorem for Gaussian integers in contours" gives the integral $\mathrm{Li}[x(S-a)]$ as a sharp estimate for $\pi[x(S-a)]$, the number of Gaussian primes in $x(S-a)$. The form we use, which we shall call (7), is stated in §3. Results of this type were known to Hecke [4], and Rademacher [12] and others have improved the error term.

Notation. We list here the symbols and terms we will be using.

S denotes the interior and boundary of a contour which is piecewise C^1.

$xS = \{xz\colon z \in S\}$.

$\pi(xS)$ is the number of prime Gaussian integers in xS, where the associates $p, -p, ip, -ip$ are counted as distinct.

$$\mathrm{Li}(xS) = \frac{2}{\pi}\int_{xS\cap\{|z|>2\}} \frac{d\,\mathrm{area}}{\log|z|}.$$

$N(z) = z\bar{z}$. Note that if a is a Gaussian integer, $N(a)$ equals the number of distinct congruence classes mod a.

An admissible set B of Gaussian integers b_i, $1 \leqslant i \leqslant k$, is a set which satisfies the following condition:

(3) For every Gaussian prime p there exists some congruence class a mod p such that $b_i \not\equiv a \bmod p$ for any i, $1 \leqslant i \leqslant k$.

Remark. On the basis of Hypothesis H, if B is admissible then there are infinitely many Gaussian y for which $y+b_i$, $1 \leqslant i \leqslant k$, are all Gaussian primes. The reason is that from B we may construct rational integer polynomials which satisfy the conditions of Hypothesis H. Without loss of generality we may assume that no b_i is real. The polynomials $(n+b_i)(n+\bar{b}_i)$ over the rational integers then satisfy the conditions of H. Thus, there exist infinitely many n for which $(n+b_i)(n+\bar{b}_i)$, $1 \leqslant i \leqslant k$ are all rational primes. For these n, for $1 \leqslant i \leqslant k$, $n+b_i$ is a Gaussian prime.

Denote by $\varrho^*(S)$ the largest N for which there exists an admissible subset of S with N elements.

Remark. In our notation, (1) now reads: $\overline{\lim}_{|y|\to\infty} \pi(xS+y) > \pi(xS)$ for all sufficiently large x. On Hypothesis H, $\varrho^*(xS) = \overline{\lim}_{|y|\to\infty} \pi(xS+y)$. Accordingly, we drop the Hypothesis, and restate (1) in a form which depends on no conjecture. If S is not logarithmically centered then:

(1′) For all sufficiently large x, $\varrho^*(xS) > \pi(xS)$.

1. The Gaussian integers. Our goal is

THEOREM 1′. *If S is a finite, simply connected region in the complex plane with piecewise C^1 boundary, and if S is not logarithmically centered, then there exists $c > 0$ for which as $x \to \infty$,*

$$\varrho^*(xS) - \pi(xS) > \frac{cx^2}{(\log x)^2}.$$

Proof. Several ingredients go into the proof; they are laid out here for the reader to inspect.

(4) If a is a logarithmic center for S and β is not, then as $x \to \infty$,

$$\mathrm{Li}\big(x(S-a)\big) - \mathrm{Li}\big(x(S-\beta)\big) \sim \frac{cx^2}{(\log x)^2} \quad \text{for some } c > 0;$$

c depends on a, β, and S, but not x (cf. (2) above and §3 below).

(5) A Chinese Remainder Theorem holds for quadratic number fields. If $P_1, P_2, \ldots, P_k$ are distinct prime ideals, $Q = \prod_1^k P_i$, and $a_i \bmod P_i$, $1 \leqslant i \leqslant k$ are congruence classes, then there exists a unique $a \bmod Q$ such that $b \equiv a \bmod Q$ if and only if $b \equiv a_i \bmod P_i$ for all i, $1 \leqslant i \leqslant k$.

(6) A Mertens' Theorem holds:

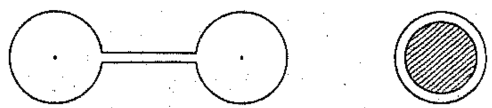
$$\prod_{N(P)<x}\left(1-\frac{1}{N(P)}\right) = (e^{-\gamma}/h\lambda\log x)\left(1+O\left(\frac{1}{\log x}\right)\right),$$

where $h\lambda > 0$ is the residue of the field's Dedekind zeta function at 1.

(The proof is similar to the classical one involving the Riemann zeta function (cf. [3]), and the modifications needed for the Dedekind zeta function can be found in [9].)

2. The logarithmic center. We have defined a logarithmic center of S as an a which minimizes $f(\beta) = \int_S \log|z-\beta|\,d\,\mathrm{area}$. Since the question of existence and uniqueness of logarithmic centers belongs more to potential theory than to number theory, we shall not give an exhaustive treatment. Rather we give examples which illustrate the main possibilities, and establish a few basic facts about $f(\beta)$. The most important of these is that there exists at least one logarithmic center.

EXAMPLE 1. Let S be a dumbell-shaped region. Then there are two logarithmic centers, one in each "weight".



EXAMPLE 2. Let S be the annulus $\{z\colon 1 \leqslant |z| \leqslant 2\}$. Then any a such that $|a| \leqslant 1$ is a logarithmic center for S.

EXAMPLE 3. Let S be a disk. Then S has a unique logarithmic center a; a is also the geometric center of S. The same applies to an ellipse, a rectangle, or a regular polygon (cf. Proposition 3).

PROPOSITION 1. *At least one logarithmic center exists.*

Proof. f is continuous and as $|\beta| \to \infty$, $f(\beta) \to +\infty$.

PROPOSITION 2. *$f(\beta)$ is harmonic in S^c, and for $\beta \in S^0$,*

$$\frac{\partial^2 f}{\partial x^2}(\beta) + \frac{\partial^2 f}{\partial y^2}(\beta) = 2\pi.$$

Proof (Sketch). Let ∂S be the oriented boundary of S. Then

$$\frac{\partial f}{\partial x}(\beta) + i\frac{\partial f}{\partial y}(\beta) = i\int_{\partial S} \log|z-\beta|\,dz.$$

Call this integral $g(\beta)$. Then

$$\frac{\partial g}{\partial x}(\beta) - i\frac{\partial g}{\partial y}(\beta) = -i\int_{\partial S}\frac{dz}{z-\beta} = -i\;[0 \text{ if } \beta \notin S,\ 2\pi i \text{ if } \beta \in S^0],$$

which proves the proposition.

PROPOSITION 3. *If S is convex and has an axis L of mirror symmetry, S has a unique logarithmic center a, and a is on L.*

The proof will be published elsewhere (cf. [5]). Here we note the easy results: Under the assumptions of Proposition 3, all logarithmic centers lie on L. Hence, if there are two lines of mirror symmetry, then their intersection forms the only possible logarithmic center. This applies e.g. to the cases in Example 3 above.

PROPOSITION 4. *If there are two concentric disks S_1 and S_2 such that $S_1 \subseteq S \subseteq S_2$, and the radius of S_2 is $11/10$ that of S_1, then S has a unique logarithmic center.*

The proof, which is similar to that of Proposition 3, will appear in [5].

CONJECTURE. *If S is convex then S has a unique logarithmic center.*

Remark. The author does not know whether the conjecture holds even for convex regions with central symmetry.

3. The prime number theorem. The following result is implicit in the work of Hecke [4] and Rademacher [12]; it has been adapted to fit our needs.

(7) THEOREM. *Let S be a region with piecewise C^1 boundary. Then*

$$\pi(xS) = \mathrm{Li}(xS) + O(x^2 e^{-c\sqrt{\log x}}) \quad \text{for some } c > 0.$$

Remark. Hecke [4] obtained $\pi(xS) \approx \mathrm{Area}(xS)/\log x$. For circular sectors K in imaginary quadratic number fields, Kubilius [8] gives $\pi(xK) = \mathrm{Li}(xK) + O(x^2 e^{-c\sqrt{\log x}})$, and for hyperbolic sectors K in real quadratic number fields, Rademacher [12] gives the same type of estimate.

By partitioning xS into several thin wedges and balancing various error terms, the result follows for a general region S. The error term is larger; where for the circular sectors $e^{-c\sqrt{\log x}}$ held, in our case $e^{-\frac{c}{2+\varepsilon}\sqrt{\log x}}$ is obtained.

An immediate consequence of the prime number theorem above is the

LEMMA 1. *If a is a logarithmic center of S and zero is not, then there exists $c > 0$ such that $\pi\big(x(S-a)\big) - \pi(xS) > cx^2/(\log x)^2$ for all sufficiently large x.*

Proof. We consider $\pi\big(x(S-\beta)\big)$ as a function of β and x (where $x \to \infty$ and β varies over a bounded region containing a and zero). From (7)

$$\pi\big(x(S-\beta)\big) = \frac{2}{\pi}\int_{xS\cap\{|z|>2\}} \frac{d\,\mathrm{area}(z)}{\log|z-\beta x|} + o\left(\frac{x^2}{(\log x)^2}\right)$$
$$= \frac{2}{\pi}x^2 \int_{S\cap\{|z|>2/x\}} \frac{d\,\mathrm{area}(z)}{\log|xz-x\beta|} + o\left(\frac{x^2}{(\log x)^2}\right).$$

Expanding

$$\frac{1}{\log|xz-x\beta|} = \frac{1}{\log x} - \frac{\log|z-\beta|}{(\log x)^2} + o\big((\log x)^{-3}\big)$$

and integrating, we have

$$\pi\big(x(S-\beta)\big)$$
$$= \frac{2}{\pi}\mathrm{Area}(S)\frac{x^2}{\log x} - \frac{2}{\pi}\frac{x^2}{(\log x)^2}\int_{S\cap\{|z|>2/x\}} \log|z-\beta|\,d\,\mathrm{area}(z) + o\left(\frac{x^2}{(\log x)^2}\right),$$

and the lemma is proved.

4. Proof of the main result. The proof procedes via a lemma to roughly the opposite effect as our theorem. Consider $C_x = \{a\colon N(a) \leqslant x\}$. Let $T(x)$ be the least integer for which C_x can be covered, using only prime ideals P_i with $N(P_i) < T(x)$, and only one congruence class $a_i \bmod P_i$ (so that for any $a \in C_x$, $a \equiv a_i \bmod P_i$ for some P_i with $N(P_i) < T(x)$).

LEMMA 2. *We have $T(x) = o(x)$.*

Notation. Let $\pi_G(x)$ be the number of Gaussian prime ideals with $N(P) \leqslant x$.

Proof of Lemma 2. Fix a large positive M. For all P_i such that $N(P_i) \leqslant M$ or $\exp(M) \leqslant N(P_i) \leqslant x/M$, put $a_i = 0$. Call the set of points in C_x not yet covered the *residual set* R. (R will act as a marker, and shrink as sieving proceeds.

R is composed of:

(a) prime Gaussian integers p such that $x/M < N(P) \leqslant x$, where P denotes the prime ideal (p), and

(b) Gaussian integers all of whose prime factors p lie in the range $M < N(P) < \exp(M)$.

As x increases, (b) becomes negligible compared to (a). Next use the prime ideals $M < N(P) < \exp(M)$ in order of increasing norm (say). At each successive prime ideal P_i, delete from R that congruence class $a_i \bmod P_i$ which contains the maximal number of remaining points in R. For each prime ideal P_i used, the chosen class a_i contains $\geqslant \frac{1}{N(P_i)}$th of the remaining points, since every point of R is in one of the $N(P_i)$ classes mod P_i. This procedure reduces the size of R by a factor of at least

$$\prod_{M<N(P)<\exp(M)} \left(1-\frac{1}{N(P)}\right),$$

which for large x is $\leqslant 2\log M/M$ by our Mertens' theorem. Finally, cover the (at most) $\frac{2\log M}{M}\pi_G(x)$ remaining points one at a time, using the next (at most) $\frac{2\log M}{M}\pi_G(x)$ prime ideals. Fewer than $2\left[\pi_G\left(\frac{x}{M}\right) + \frac{2\log M}{M}\pi_G(x)\right]$ prime ideals have been used, so

$$\pi[T(x)] = \frac{\log M}{M} O\left(\pi_G(x)\right) \quad \text{and} \quad T(x) = \frac{\log M}{M} O(x).$$

Releasing $M \to \infty$, $T(x) = o(x)$, and Lemma 2 is proved.

We now construct an admissible subset of $x(S-a)$. Fix $\varepsilon > 0$. Then from $x(S-a)$ remove any number which has a prime ideal factor P with $N(P) \leqslant \varepsilon x^2/\log x$, or which is a unit. The remaining set $y_\varepsilon(x)$ will for large x consist of prime Gaussian integers.

Lemma 3. *For all sufficiently large x, $y_\varepsilon(x)$ is admissible.*

Proof. $(S-a)$ is contained in some disk D about zero. Let Q be an arbitrary prime ideal, generated by q. We must show that there exists some congruence class $a \bmod Q$ such that $y_\varepsilon(x) \cap \{b\colon b \equiv a \bmod Q\} = \emptyset$.

If $N(Q) \leqslant \varepsilon x^2/\log x$, then $0 \bmod Q$ works. There exists A such that if $N(Q) > Ax^2/\log x$, there are more classes mod Q than points in $y_\varepsilon(x)$, so again some congruence class is disjoint from $y_\varepsilon(x)$. Accordingly, we consider the non-trivial case, when

$$\frac{\varepsilon x^2}{\log x} < N(Q) < \frac{Ax^2}{\log x}.$$

Each congruence class $a \bmod Q$ intersects the disk xD in a lattice J. Now there exists $c_2 > 0$ such that for all x, for all non-trivial Q, and all a such that $N(a) < N(Q)$, the disk of radius $c_2 x$ about a contains J. The points b inside this larger disk for which $b \equiv a \bmod Q$ are all $a+n$ where n is any element of Q with $N(n) \leqslant c_2 x^2$. This set, though, is exactly the image under a translation (by a) and a multiplication (by q) of

$$\{n\colon N(n) \leqslant c_2 x^2/N(Q)\}.$$

Since $N(Q) > \varepsilon x^2/\log x$,

$$c_2 x^2/N(Q) < \frac{c_2^2}{\varepsilon}\log x.$$

We apply our sieving lemma to the slowly growing disk of algebraic radius $\frac{c_2^2}{\varepsilon}\log x$ to find some combination of $(a_i \bmod P_i)$'s which covers, and then use the Chinese Remainder Theorem to convert this into a proof that the $a \bmod Q$ we seek exists. By Lemma 2, for sufficiently large x,

$$T\left(\frac{c_2^2}{\varepsilon}\log x\right) = o(\log x).$$

It is therefore possible to choose $a_1 \bmod P_1,\ a_2 \bmod P_2, \ldots, a_k \bmod P_k$ such that for each P_i, $1 \leqslant i \leqslant k$, $N(P_i) = o(\log x)$ and such that for any n with $N(n) \leqslant \frac{c_2^2}{\varepsilon}\log x$ there is an $i \leqslant k$ for which $n \equiv a_i \bmod P_i$.

Remark. This is the decisive step in the proof! A covering with *small primes* for the image of a congruence class mod Q is obtained. The close relation via the Chinese Remainder Theorem between image and object is now used. We are nearly done.

Since $N(P_k) = o(\log x)$, $\prod_{i=1}^{k} N(P_i) < x$ by a form of the prime number theorem. In turn, $x = o(\varepsilon x^2/\log x) < N(Q)$. By our Chinese Remainder Theorem, there exists some a_0, $N(a_0) < \prod_{i=1}^{k} N(P_i) < N(Q)$, such that $a_0 + a_i q \equiv 0 \bmod P_i$ $(1 \leqslant i \leqslant k)$, and we calculate that if $N(n) \leqslant \frac{c_2^2}{\varepsilon}\log x$, $n \equiv a_i \bmod P_i$ (some i) so $nq \equiv a_i q \bmod P_i$ and $a_0 + nq \equiv 0 \bmod P_i$.

Hence P_i divides a_0+nq. But since $N(P_i)<\log x$, 0 mod P_i has already been sieved from $y_\varepsilon(x)$. Therefore $a_0+nq\notin y_\varepsilon(x)$ for any n, as required. $y_\varepsilon(x)$ is admissible, and Lemma 3 is proved.

We finish by combining Lemmas 1 and 3 to get (1′), the main result. From the construction of $y_\varepsilon(x)$, it is clear that for ε small enough, the loss of an amount asymptotic to

$$\frac{2\varepsilon x^2}{(\log x)^2}\lesssim \pi\left\{n:\ N(n)<\frac{\varepsilon x^2}{\log x}\right\}$$

from the set of *all* prime points in $x(S-a)$ is not sufficient to counter the excess (cf. Lemma 1)

$$\pi\big(x(S-a)\big)-\pi(xS)>\frac{c_1x^2}{(\log x)^2}.$$

Thus $\varrho^*(xS)>\pi(xS)$; the difference is eventually greater than some constant multiple of $x^2/(\log x)^2$. Q.E.D.

5. Modifications needed for other quadratic number fields. A given quadratic number field $\mathcal{F}$ may be embedded in the xy plane by mapping $a\in\mathcal{F}$ to $\left(\frac{a+\bar a}{2},\frac{a-\bar a}{2}\right)$. Thus the x axis is the rational axis, the y axis the algebraic axis. If $\mathcal{F}$ is an imaginary quadratic field, our embedding in the xy plane is just the natural one associated with the complex field. If $\mathcal{F}$ is a real quadratic number field, the number $r_1+r_2\sqrt{n}$ (r_i rational) is mapped to $(r_1, r_2\sqrt{n})$. Here the xy plane is sectioned by two intersecting lines of norm zero; $x=y$ and $x=-y$. The curves of constant norm K are the hyperbolae $x^2-y^2=K$.

In the real case, the argument of a, $\operatorname{arc}a$, is defined to be $\log|a/\bar a|$. (This is consistent with the geometric definition for imaginary fields.) When $a=(a,b)$ and $a>b>0$, an equivalent expression for $\operatorname{arc}a$ is $\operatorname{arc}a=4A$, where A is the area enclosed by the x axis, the curve $x^2-y^2=1$, and the straight line between 0 and a. We note that $\sinh A=b$, $\cosh A=a$.

Hecke [4] has shown that this embedding of $\mathcal{F}$ may be extended to represent non-principal ideals of $\mathcal{F}$ by specific points in the xy plane. This extension has two basic properties: (i) the multiplicative group of the set of points obtained is isomorphic to the group of fractional ideals of $\mathcal{F}$; (ii) for each ideal class C of $\mathcal{F}$, the points corresponding to integral ideals in C form a two dimensional lattice which faithfully reflects the structure of C as an $\mathcal{F}$-module. Thus we may talk of congruence classes, admissibility, etc. (When C is the class of principal ideals, we recover the original embedding of $\mathcal{F}$ itself.) The points representing prime ideals we call prime points. For S a region in the xy plane satisfying the restrictions of Theorem 1, and C any ideal class, $\varrho_C^*(S)$ has the expected meaning:

DEFINITION. $\varrho_C^*(S)$ = the maximum number of elements belonging to any admissible set $A\subseteq S\cap$(the image of C under Hecke's embedding).

For the real quadratic case,

DEFINITION. A *logarithmic center a of S* is an a for which

$$\int_{S-a}\log N(z)\,d\,\text{area}$$

is minimal.

With the above definitions in mind, one may prove a prime number theorem similar to that of §3 for the number of prime points in xS which represent ideals of a given ideal class (cf. [4], [12]).

One can now state and prove an extended version of Theorem 1′; the proof for the most part follows that of Theorem 1′.

THEOREM 1″. *If S is a bounded, simply connected region in the xy plane with piecewise C^1 boundary, and if S is not logarithmically centered, then for each ideal class C there exists $c>0$ for which as $x\to\infty$,*

$$\varrho_C^*(xS)-\pi_C(xS)>\frac{cx^2}{(\log x)^2}.$$

Remark. The new complexities introduce unfavorable constant factors into a "little o" argument, and so the basic line of reasoning is unaffected. The technique gets messier.

We now say how the proof of Theorem 1′ must be modified for Theorem 1″. For real quadratic fields, Lemma 2 must be restated as Lemma 2′ below. For fields of class number larger than one, the proof of Lemma 3 and the final argument make use of Hecke's embedding.

Lemmas 2, 3 and the final argument must also be modified to adjust to the new geometry and to the larger class number.

For the case of real quadratic number fields, in place of Lemma 2 we have the following

LEMMA 2′. *Consider $C_x'=\{a$: a is embedded in the xy plane as (a_1,a_2) and $a_1^2+a_2^2\leqslant x\}$. Then $T(x)$ defined as in Lemma 2, is $o(x)$.*

Remark. The number of prime points in C_x', counting associates as distinct, is on the order of $x/\log x$. This follows from the general case of the prime number theorem for contours. Other than this, the proof of Lemma 2′ is the same as that of Lemma 2.

The statement of Lemma 3 for the general case is unchanged, but the proof uses Hecke's extension of the embedding

$$a\to(a_1,a_2)=\left(\frac{a+\bar a}{2},\frac{a-\bar a}{2}\right)$$

and uses Lemma 2′ for the real quadratic case. To prove Lemma 3:

For any ideal I, let us denote by $\bar{I}$ a point where I is embedded. ($\bar{I}$ is unique up to unit multiples.) Let us denote by $m(I)$ an ideal in the same ideal class as I which has minimal norm. Since the class number of $\mathscr{F}$ is finite, $\sup_I m(I)$ is finite. Let N denote the set of $\mathscr{F}$ integers.

As before, let Q be a non-trivial prime ideal. Unfortunately Q may not have a generator q. In place of q we use $\bar{q}$, defined by $\bar{q} = u\overline{Q}/\overline{m(Q)}$, where u is that unit which minimizes the Euclidean norm of $\bar{q}$. To control the position of generators a for congruence classes mod Q, we note that there exists $c_2' > 0$ such that for any ideal I of $\mathscr{F}$, $\{a\colon a_1^2+a_2^2 < c_2' N(I)\}$ contains an element of each congruence class mod I.

As before, there exists $c_2 > 0$ such that for all x, for all non-trivial Q, and all a such that $a_1^2+a_2^2 < c_2' N(Q)$, the disk of radius $c_2 x$ about a contains J. The points b inside this larger disk for which $b \equiv a \bmod Q$ are all $a+n$ where n is any element of Q for which $n_1^2+n_2^2 \leqslant c_2^2 x^2$. This set, though, is *contained in* (instead of, as previously, equal to) the image under translation by a and multiplication by $\bar{q}$ of $\{n\colon n_1^2+n_2^2 \leqslant c_{\mathscr{F}} x^2/N(Q)\}$ (where $c_{\mathscr{F}} > c_2^2$ by a factor depending on $\mathscr{F}$). This is because $Q \subseteq \bar{q}N$, since if $a \in Q$, $[a] = QT$ for some ideal T, so $a = \overline{Q}\overline{T}\cdot u$ (u a unit) and $a = \bar{q}\big(\overline{m(Q)}\overline{T}u\big)$. But $\overline{m(Q)}\overline{T}u \in N$.

Now since $N(Q) > \varepsilon x^2/\log x$,

$$\frac{c_{\mathscr{F}} x^2}{N(Q)} < \frac{c_{\mathscr{F}}}{\varepsilon}\log x .$$

The rest of the proof follows the lines of the earlier Lemma 3. At the end Lemma 2′ covers $\{n\colon n_1^2+n_2^2 \leqslant cx^2/N(Q)\}$, which then via CRT provides the required empty congruence class in $y_s(x) \bmod Q$.

Finally, at the point where the CRT is used to go back, we choose a_0 from $\{n\colon n_1^2+n_2^2 \leqslant c_2' \prod_{i=1}^{k} N(P_i)\}$.

6. Further questions. Upper bounds for $\varrho^*(xS)$ may be derived from generalizations of large sieve results (cf. [7], [14], [17]). If $\mathscr{F}$ is a field of class number greater than one, and if C_1 and C_2 are distinct ideal classes of $\mathscr{F}$, what can one say about $\varrho^*_{C_1}(xS)$ compared to $\varrho^*_{C_2}(xS)$? If A is an admissible subset of C_1, then there exists an additive group isomorphism of C_1 onto C_2 which maps A to an admissible subset of C_2, but the mapping depends on A, and hence is not very helpful.

If $\mathscr{F}$ is a real quadratic number field, the function

$$f(\beta) = \int_S \log N(z-\beta)\, d\,\mathrm{area}(z)$$

has a minimum, but the geometric arguments of §2 fail, and the question of when S has a unique logarithmic center remains completely open.

Finally, we note the Conjecture of §2, about uniqueness of the logarithmic center for convex regions in the complex plane. If true, it would be a very nice result in its own right, as well as a useful number theoretic tool. If false, any counterexample would certainly be noteworthy.

References

[1] P. Erdös, *On the difference of consecutive primes*, Quarterly J. Math. (Oxford) 6 (1935), pp. 124–128.

[2] A. O. Gelfond and Yu. V. Linnik, *Elementary Methods in Analytic Number Theory* (translation), Chicago 1965.

[3] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford 1938.

[4] E. Hecke, *Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen II*, Math. Zeitschr. 6 (1920), pp. 11–51.

[5] D. Hensley, *On the logarithmic center of a planar region*, to appear in Proc. Amer. Math. Soc.

[6] — and I. Richards, *Primes in intervals*, Acta Arith. 25 (1974), pp. 375–391.

[7] M. Huxley, *The large sieve inequality for algebraic number fields*, Mathematika 15 (1968), pp. 178–187.

[8] I. P. Kubilius, *The distribution of prime numbers of the Gaussian field in sectors and contours* (in Russian), Leningr. Gos. Univ. Uch. Zap., Ser. Mat. Nauk, 19 (1950), pp. 40–52.

[9] E. Landau, *Einführung in die elementare und analytische Theorie der algebraischen Zahlen und der Ideale*, Leipzig 1927.

[10] H. Montgomery, *Topics in Multiplicative Number Theory*, New York 1971.

[11] H. Rademacher, *Zur additiven Primzahltheorie algebraischer Zahlkörper III*, Math. Zeitschr. 27 (1927).

[12] — *Primzahlen reell-quadratischen Zahlkörper in Winkelräumen*, Math. Ann. 111 (1935), pp. 209–228.

[13] R. A. Rankin, *The difference between consecutive prime numbers*, J. London Math. Soc. 13 (1938), pp. 242–247.

[14] W. Schaal, *On the large sieve method in algebraic number fields*, J. Number Theory 2 (1970), pp. 249–270.

[15] A. Schinzel et W. Sierpiński, *Sur certaines hypothèses concernant les nombres premiers*, Acta Arith. 4 (1958), pp. 185–208.

[16] E. Westzynthius, *Über die Verteilung der Zahlen, die zu den n ersten Primzahlen teilerfremd sind*, Comm. Phys. Math. Helsingfors (5) 25 (1931), pp. 1–37.

[17] R. Wilson, *The large sieve in algebraic number fields*, Mathematika 16 (1969), pp. 189–204.

UNIVERSITY OF MINNESOTA
Minneapolis, Minnesota

Received on 30. 11. 1973 (498)