Without essential restriction, let $p > 5$. Then

$$(5p)^{10}(\tfrac{4}{5}p^{-1/2})^{(p-1)^2} < 1.$$

Further, by (7), where now $n = p-1$, $m = p$, $A = C_q^p$, we have the estimates

$$x < y < \exp\exp\big(2^p(p-1)^{10(p-1)}\big)^{(p-1)^2} < \exp\exp(2p^{10})^{p^3}.$$

By virtue of estimates given by the author [4] it follows that

$$x > p^{3p-4}, \quad y > \tfrac{1}{2}p^{3p-1},$$

since $p\,|\,y(y+1)$. Recalling that Fermat's conjecture has been proved for $p < 25000$, the magnitude of each of these bounds is fairly large. However, the differences between the above upper bound and these lower bounds are enormous.

References

[1] A. Baker, *Bounds for the solutions of the hyperelliptic equation*, Proc. Camb. Phil. Soc. 65 (1969), pp. 439–444.

[2] C. J. Everett, *Fermat's conjecture, Roth's theorem, Pythagorean triangles, and Pell's equation*, Duke Math. J. 40 (1973), pp. 801–804.

[3] K. Inkeri, *Untersuchungen über die Fermatsche Vermutung*, Ann. Acad. Sci. Fenn. Ser. AI, No. 33 (1946), pp. 1–60.

[4] — *Abschätzungen für eventuelle Lösungen der Gleichung im Fermatschen Problem*, Ann. Univ. Turku, Ser. A, tom. XVI, (1953), pp. 1–9.

[5] K. Inkeri and S. Hyyrö, *Über die Anzahl der Lösungen einiger diophantischer Gleichungen*, Ann. Univ. Turku, Ser. AI, No. 78 (1964), pp. 1–10.

[6] E. Landau, *Vorlesungen über Zahlentheorie*, 3. Bd., Hirzel, Leipzig 1927.

[7] W. J. LeVeque, *Topics in Number Theory*, vol. II, Addison-Wesley, Reading, Massachusetts, 1961.

[8] — *On the equation $y^m = f(x)$*, Acta Arith. 9 (1964), pp. 209–219.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF TURKU
Turku, Finland

Received on 12. 7. 1974 (599)

ACTA ARITHMETICA
XXIX (1976)

On the representation of a number in the form $x^2+y^2+p^2+q^2$ where p, q are odd primes

by

G. Greaves (Cardiff)

1. Introduction. This paper shows that every sufficiently large natural number N that satisfies the necessary condition of incongruence, modulo 8, to 0, 1 or 5 is representable in the form stated in the title. The interest of this result lies partially in the fact that (so far as the author is aware) there is no immediate prospect of any solution of the corresponding "Waring–Goldbach" problem in which the numbers x, y would also be restricted to prime values.

The proof depends on a combination of the mean value theorem of Barban [1] (as re-discovered shortly afterwards by Davenport and Halberstam [3]) with the $\frac{1}{2}$-residue sieve method developed by Rosser (unpublished). An account of this method appears in Iwaniec's paper [7]. Barban's theorem is used in the way described in the author's paper [5] to estimate, with sufficient accuracy for our purposes, the number of pairs of primes p, q that satisfy

$$p^2+q^2 \equiv N \bmod l, \quad p \leqslant Z,\ q \leqslant Z$$

for a modulus l not exceeding $Z/\log^C Z$. Such an estimate is the essential starting point for applications of the sieve method to binary problems involving primes. In this paper the $\frac{1}{2}$-residue sieve method is used in obtaining a positive lower estimate of how often $N-p^2-q^2$ is free of prime factors $\varpi \equiv 3 \bmod 4$, and hence is of the form x^2+y^2.

It is, perhaps, worthy of comment that the $\frac{1}{2}$-residue sieve is sufficiently powerful to establish the existence of numbers that are sums of two squares and lie in a suitable sequence, whereas the 1-residue sieve has not yet been successfully used to establish the existence of primes in any sequence at all.

Iwaniec used his results in his treatment of the number of primes p not exceeding Z that are representable in the form x^2+y^2+A (where, indeed, x^2+y^2 was replaced by an arbitrary quadratic form, positive if definite) but the method applies also to the "conjugate" problem of representing a large number N as

$$N = x^2+y^2+p. \tag{1.1}$$

The tool from prime number theory relevant here is Bombieri's theorem, and one would obtain a lower estimate $\gg N/\log^{3/2}N$ for the number of primes p for which such a representation is possible. On the other hand Bombieri's theorem was also used by Elliott and Halberstam [4] to remove the dependence on a Riemann hypothesis of Hooley's estimate [6] for the total number of representations of N in the form (1.1). It appears, however, that an attempt to adapt Hooley's method to the problem considered in this paper is likely to involve serious difficulties. Accordingly we use the sieve-theoretic method to establish the following result.

THEOREM. *Suppose $N \not\equiv 0, 1, 5 \bmod 8$. Let $S(N)$ be the number of pairs of primes p, q such that*

$$1 < p \leqslant \sqrt{N/2}, \quad 1 < q \leqslant \sqrt{N/2}$$

and $N-p^2-q^2$ is representable as x^2+y^2. Then there is an inequality of the type

$$S(N) > A\frac{N}{\log^{5/2}N}\left\{1+O\left(\frac{\log\log N}{(\log N)^{1/10}}\right)\right\},$$

where $A > 0$ is as described in (6.1) below.

Every sufficiently large such N is representable as $x^2+y^2+p^2+q^2$.

The proof assigns an explicit numerical value to the constant A, but not to the constant implied by the O-symbol. This is because Barban's result rests on Siegel's theorem. Thus it is not possible to deduce how large N must be to guarantee representability.

A very brief outline of the details of our treatment may perhaps be helpful. We restrict p, q to lie within certain residue classes, mod 288, whose choice will ensure that the number $N-p^2-q^2$ considered are of the form $2^g(4n+1)$. Let E be the number of these $N-p^2-q^2$ that are not divisible by any prime $\tilde{\omega}$ for which $\tilde{\omega} < z$ and $\tilde{\omega} \equiv 3 \bmod 4$. Here $z = N^{1/(2v)}$ is to be specified but will satisfy (1.2) below. The $\frac{1}{2}$-residue sieve is then used to give a positive lower bound for E. The method does not permit the choice $z = \sqrt{N}$ that we might wish; when $z > N^{1/3}$, however, the numbers $N-p^2-q^2$ counted by E are either sums of two squares or are of the alternative form mq_1q_2 where

(i) $\tilde{\omega}|m$ implies $\tilde{\omega} \not\equiv 3 \bmod 4$ and $\tilde{\omega} \leqslant z$,

(ii) q_1, q_2 are prime, $z < q_1 \leqslant q_2$ and $q_i \equiv 3 \bmod 4$.

The number E' of these unwanted survivors of the first sifting process is bounded above (in Lemma 10) by the well known methods of Selberg (Brun's would suffice, as the value of the constant C in Lemma 10 is not important). To achieve this, estimates for exponential sums "along a circle" are deduced from well known results on the Kloosterman sum. With an appropriate z the desired result $E' < E$ is achieved with a comfortable margin to spare: the result of our theorem follows from the inequality

$$S(N) \geqslant E-E'.$$

For convenience in exposition, the parameter z will satisfy

$$z > N^{5/12}, \tag{1.2}$$

as the methods used become ineffective as z approaches $N^{1/3}$. Thus

$$N^{5/12} < q_1 \leqslant q_2 \tag{1.3}$$

and accordingly

$$m < N^{1/6}. \tag{1.4}$$

It will not be necessary for the reader to have these restrictions constantly in mind.

Multiplicative functions τ, ϱ, σ are defined when their relevance to the problem becomes clear; γ on the other hand denotes a variable multiplicative function having different meanings at various points of the account. Constants implied by the O and $\ll$ symbols are "absolute": that is to say they may depend at most on the residue of $N \bmod 8$. Other notations are explained as they are introduced.

2. Results from sieve theory. In a popular notation, the symbol $\mathscr{A}$ denotes a set of integers with a property

$$\sum_{\substack{a\in\mathscr{A}\\ a\equiv 0 \bmod l}} 1 = \frac{X\gamma(l)}{l}+E(X, l), \tag{2.1}$$

where for each $\delta > 0$ there is a β such that

$$\sum_{l\leqslant X^{\alpha}/\log^{\beta}X} \mu^2(l)|E(X, l)| \leqslant \frac{X}{(\log X)^{\delta}}, \tag{A1}$$

and the multiplicative function γ satisfies, for some $A_i > 0$,

$$0 \leqslant \gamma(\tilde{\omega}) \leqslant \left(1-\frac{1}{A_1}\right)\tilde{\omega} \quad \text{if} \quad \tilde{\omega} \in \mathscr{P}, \tag{A2}$$

$$-L < \sum_{\substack{\tilde{\omega}\in\mathscr{P}\\ \tilde{\omega}<z}} \gamma(\tilde{\omega})\frac{\log\tilde{\omega}}{\tilde{\omega}} - k\log z < A_2, \tag{A3}$$

$\mathscr{P}$ being a set of "sifting" primes. The constant k is the "dimension" of the sieve under consideration. Here the constants a, A_i are "absolute" but L may depend on $X = X(\mathscr{A})$.

The $\frac{1}{2}$-residue sieve. $k = \frac{1}{2}$. The results we need are obtained by the method described, in a somewhat restricted context, in Iwaniec's paper [7]. There is however no additional difficulty in principle in obtaining the following.

Lemma 1. *Denote by $\Pi(\mathscr{A}, \mathscr{P}_z)$ the number of members of $\mathscr{A}$ divisible by no prime $\tilde{\omega}$ such that $\tilde{\omega} < z$, $\tilde{\omega} \in \mathscr{P}$. Suppose* (A1), (A2), (A3) *are satisfied with $k = \frac{1}{2}$. Then there is a $f(u) > 0$ when $u > 1$ for which*

$$\Pi(\mathscr{A}, \mathscr{P}_z) > X\Big\{\prod_{\substack{\tilde{\omega}\in\mathscr{P}\\ \tilde{\omega}<z}}\Big(1-\frac{\gamma(\tilde{\omega})}{\tilde{\omega}}\Big)\Big\}\Big[f\Big(a\frac{\log X}{\log z}\Big)+O\Big\{\frac{L}{(\log X)^{1/10}}\Big\}\Big].$$

There is a corresponding upper bound in which f is replaced by F: here the functions f, F, continuous in $(0, \infty)$, satisfy

$$F(u) = \frac{2C}{\sqrt{u}}, \qquad f(u) = 0 \quad \text{if} \quad 0 \leqslant u \leqslant 1,$$

$$\frac{d}{du}\{\sqrt{u}f(u)\} = \frac{1}{2\sqrt{u}}F(u-1) \quad \text{if} \quad u > 1,$$

$$\frac{d}{du}\{\sqrt{u}F(u)\} = \frac{1}{2\sqrt{u}}f(u-1) \quad \text{if} \quad u > 1,$$

where $C = \sqrt{e^{\gamma_0}/\pi}$, γ_0 being Euler's constant. In particular

$$\sqrt{u}f(u) = C\int_1^u \frac{dt}{\sqrt{t^2-t}} \quad \text{if} \quad 1 \leqslant u \leqslant 2. \tag{2.2}$$

In our application the set $\mathscr{P}_z$ of sifting primes $\tilde{\omega}$ is

$$\mathscr{P}_z = \{\tilde{\omega}\colon\ \tilde{\omega} < z,\ \tilde{\omega} \equiv 3 \bmod 4\}. \tag{2.3}$$

In this case Lemma 1 gives the more convenient Lemma 2 below, as follows. The well known elementary results

$$\prod_{\tilde{\omega}<z}\Big(1-\frac{1}{\tilde{\omega}}\Big) = \frac{e^{-\gamma_0}}{\log z}+O\Big(\frac{1}{\log^2 z}\Big),$$

$$\prod_{\tilde{\omega}<z}\Big(1-\frac{\chi(\tilde{\omega})}{\tilde{\omega}}\Big) = \frac{4}{\pi}+O\Big(\frac{1}{\log z}\Big),$$

where χ is the non-principal character, mod 4, give

$$\frac{1}{2}\prod_{\substack{\tilde{\omega}<z\\ \tilde{\omega}\equiv 3 \bmod 4}}\frac{1-1/\tilde{\omega}}{1+1/\tilde{\omega}} = \frac{\pi}{4e^{\gamma_0}\log z}+O\Big(\frac{1}{\log^2 z}\Big).$$

Consequently the product featuring in Lemma 1 satisfies

$$C\prod_{\tilde{\omega}\in\mathscr{P}_z}\Big(1-\frac{\gamma(\tilde{\omega})}{\tilde{\omega}}\Big) = \frac{D}{\sqrt{\log z}}\prod_{\tilde{\omega}\equiv 3 \bmod 4}\Big\{\frac{1-\gamma(\tilde{\omega})/\tilde{\omega}}{1-1/\tilde{\omega}}\Big\}+O\Big(\frac{1}{\log^{3/2} z}\Big),$$

where

$$D = \frac{1}{\sqrt{2}}\prod_{\tilde{\omega}\equiv 3 \bmod 4}\Big(1-\frac{1}{\tilde{\omega}^2}\Big)^{1/2} > 0, \tag{2.4}$$

the required estimates for the contributions from primes $\tilde{\omega} > z$ following from (A3).

In the light of these remarks the case of Lemma 1 that we actually use is as follows.

Lemma 2. *Under the hypotheses of Lemma* 1 *we have*

$$\Pi(\mathscr{A}, \mathscr{P}_z) > \frac{X}{\sqrt{\log X^a}}D\Big\{\prod_{\tilde{\omega}\equiv 3 \bmod 4}\frac{1-\gamma(\tilde{\omega})/\tilde{\omega}}{1-1/\tilde{\omega}}\Big\}\Big\{\int_1^u\frac{dt}{\sqrt{t^2-t}}+O\Big(\frac{L}{(\log X)^{1/10}}\Big)\Big\}$$

when $z = X^{a/u}$ *with* $1 \leqslant u \leqslant 2$.

There is a similar upper bound in which the integral is replaced by 2. This upper bound is thus best possible in the sense that it yields the same main term as features in Landau's result [9] (or see [10], for example)

$$\sum_{\substack{m\leqslant M\\ \tilde{\omega}|m \Rightarrow \tilde{\omega}\not\equiv 3 \bmod 4}} 1 = 2D\frac{M}{\sqrt{\log M}}+O\Big(\frac{M}{\log^{3/4} M}\Big).$$

A partial summation on this yields the weaker result

$$\sum_{\substack{m\leqslant M\\ \tilde{\omega}|m \Rightarrow \tilde{\omega}\not\equiv 3 \bmod 4}} \frac{1}{m} = 4D\sqrt{\log M}+O(\log^{1/4} M).$$

We use this in the proof of the following lemma.

Lemma 3. *Suppose that for some $\delta > 0$ a multiplicative function γ satisfies*

$$\sum_{\substack{\tilde{\omega}\leqslant z;\ \mu\geqslant 0\\ \tilde{\omega}\in\mathscr{P}}}\frac{|\gamma(\tilde{\omega}^{\mu+1})-\gamma(\tilde{\omega}^{\mu})|}{\tilde{\omega}^{\mu(1-\delta)}} = O(1),$$

where $\mathscr{P}$ is the set of primes $\tilde{\omega} \not\equiv 3 \bmod 4$. Then

$$\sum_{\substack{m\leqslant z\\ \tilde{\omega}|m \Rightarrow \tilde{\omega}\in\mathscr{P}}}\frac{\gamma(m)}{m} = 4D\sqrt{\log z}\prod_{\tilde{\omega}}\Big\{\Big(1-\frac{1}{\tilde{\omega}}\Big)\sum_{\mu\geqslant 0}\frac{\gamma(\tilde{\omega}^{\mu})}{\tilde{\omega}^{\mu}}\Big\}+O(\log^{1/4} z),$$

where the infinite product is convergent.

Proof. In this proof the symbols l, m, n denote products of primes in $\mathscr{P}$. Set

$$\Gamma(n) = \sum_{lm=n} \mu(l)\gamma(m),$$

so that

$$\gamma(n) = \sum_{l|n} \Gamma(l).$$

The hypotheses of the lemma are needlessly strong (but comfortably satisfied in our application) to show

$$\sum_{n>z} \frac{|\Gamma(n)|}{n} = O\left(\frac{1}{\log z}\right). \tag{2.5}$$

Thus

$$\sum_{n\leqslant z} \frac{\gamma(n)}{n} = \sum_{l\leqslant z} \frac{\Gamma(l)}{l} \sum_{m\leqslant z/l} \frac{1}{m}$$
$$= 4D \sum_{l\leqslant z} \frac{\Gamma(l)}{l} \{\log^{1/2}(z/l) + O(\log^{1/4}(z/l))\},$$

and the result follows by partial summation. The infinite product is that for $\sum \Gamma(n)/n$, convergent because of (2.5).

The next lemma is the case $k = 3$ of Selberg's well known upper bound.

Lemma 4. *If* (A1) *and the left sides of* (A2), (A3) *hold with* $k = 3$ *then*

$$\Pi(\mathscr{A}, \mathscr{P}_z) < XF_3\left(\alpha\frac{\log X}{\log z}\right)\left\{\prod_{\substack{\tilde\omega\in\mathscr{P}\\ \tilde\omega<z}} \left(1 - \frac{\gamma(\tilde\omega)}{\tilde\omega}\right)\right\}\left\{1 + O\left(\frac{L}{\log z}\right)\right\},$$

where $F_3(u) = 3!e^{3\gamma_0}/u^3$ *if* $0 < u \leqslant 2$. *Thus*

$$\Pi(\mathscr{A}, \mathscr{P}_z) < \frac{2^3 3! X}{\alpha^3 \log^3 X}\left\{\prod_{\tilde\omega} \frac{1-\gamma(\tilde\omega)/\tilde\omega}{(1-1/\tilde\omega)^3}\right\}\left\{1 + O\left(\frac{L}{\log X}\right)\right\},$$

where the infinite product is convergent.

3. The applications of the sieve method: preliminaries. The applications of the sieve method made in this paper are to sets

$$\mathscr{A} = \left\{\frac{N-p^2-q^2}{K} : p, q \text{ prime};\ 3 \leqslant p, q \leqslant Z,\ \langle p, q\rangle \in \mathscr{R}_K\right\}; \tag{3.1}$$

$$\mathscr{A}_n = \left\{\frac{rs(N-r^2-s^2)}{Kn} : r^2+s^2 \equiv N \bmod Kn;\ \langle r, s\rangle \in \mathscr{R}_K;\right.$$
$$\left. (rs, Kn) = 1;\ 1 \leqslant r, s \leqslant Z\right\}. \tag{3.2}$$

Here

$$Z = \sqrt{N/2} \tag{3.3}$$

and K is an absolute constant, being a certain divisor of 72 whose identity depends only on the residue of $N \bmod 72$. The set $\mathscr{R}_K$ that is to contain the ordered pairs $\langle p, q\rangle$, $\langle r, s\rangle$ is a corresponding collection of residue classes to a similarly constant modulus that has the same distinct prime factors 2, 3 as has K. The choice of $\mathscr{R}_K$ will ensure that the members of $\mathscr{A}$ are integers. Deferring until later the consideration of most of those properties of $\mathscr{A}$ and $\mathscr{A}_n$ that depend on the choice of $\mathscr{R}_K$, we establish in this section the properties (A3) with appropriate values of α.

Case I. The set $\mathscr{A}$. Let u, v cover the $Kl\psi(K, l)$ solutions of

$$1 \leqslant u, v \leqslant K;\quad (uv, Kl) = 1;\quad u^2+v^2 \equiv N \bmod Kl,\quad \langle u, v\rangle \in \mathscr{R}_K. \tag{3.4}$$

Express ψ as

$$\psi(K, l) = \psi(K, 1)\varrho(l), \tag{3.5}$$

so that ϱ is a multiplicative function.

To estimate the sum (A1) a purely formal application of the Prime Number Theorem would give

$$\sum_{a\equiv 0 \bmod l} 1 = \sum_{u,v}\Big(\sum_{\substack{p\leqslant Z\\ p\equiv u \bmod Kl}} 1\Big)\Big(\sum_{\substack{q\leqslant Z\\ q\equiv v \bmod Kl}} 1\Big)$$
$$= \frac{\mathrm{li}^2 Z}{\varphi^2(Kl)} K\psi(K, 1) l\varrho(l) + \eta(Z, K, l) = X\frac{\gamma(l)}{l} + E(X, l),$$

say. Here φ is Euler's function,

$$X = \frac{K\psi(K, 1)}{\varphi^2(K)} \mathrm{li}^2 Z = B\,\mathrm{li}^2 Z, \tag{3.6}$$

and $\gamma(l) = \tau(l)$, where (for future reference) we define

$$\tau(l) = l\varrho(l)\varphi^2(K)/\varphi^2(Kl). \tag{3.7}$$

Thus the function γ is multiplicative. The choice of $\mathscr{R}_K$ will ensure

$$\psi(K, 1) > 0. \tag{3.8}$$

If $\tilde\omega > 3$ (so that $\tilde\omega$ does not divide K or the modulus of any $\mathscr{R}_K$) then $\tilde\omega\varrho(\tilde\omega^\nu)$ is just the number of solutions $\langle u, v\rangle$ of

$$u^2+v^2 \equiv N \bmod \tilde\omega^\nu,\quad (uv, \tilde\omega) = 1.$$

Note before proceeding that in this case

$$\varrho(\tilde\omega^\nu) = \varrho(\tilde\omega)\quad \text{if}\quad \nu \geqslant 1. \tag{3.9}$$

This is easily verified by induction on ν: for each solution u, v of

$$u^2+v^2 \equiv N \bmod \tilde{\omega}^\nu, \qquad (uv, \tilde{\omega}) = 1$$

the corresponding solutions $u', v' \bmod \tilde{\omega}^{\nu+1}$ satisfy

$$u' = u+\tilde{\omega}^\nu x, \qquad v' = v+\tilde{\omega}^\nu y,$$

where

$$\frac{u^2+v^2-N}{\tilde{\omega}^\nu}+2(xu+yv) \equiv 0 \bmod \tilde{\omega},$$

which has $\tilde{\omega}$ roots x, y because $(2uv, \tilde{\omega}) = 1$.

Note also that

$$(3.10) \qquad \varrho(\tilde{\omega}) = 1+O(1/\tilde{\omega}) \quad \text{if} \quad \tilde{\omega} \nmid N$$

because of the old result of Jacobsthal [8]

$$\sum_{v \bmod \tilde{\omega}} \left(\frac{N-v^2}{\tilde{\omega}}\right) = O(1)$$

on a sum of Legendre symbols. Also, from (3.4),

$$\varrho(\tilde{\omega}) \neq 0 \Rightarrow \varrho(\tilde{\omega}) \geqslant 1 \quad \text{when} \quad \tilde{\omega}|N.$$

Hence

$$(3.11) \qquad \varrho(n) \neq 0 \Rightarrow \varrho(n) \geqslant 1.$$

Observe also from (3.9) and (3.10)

$$(3.12) \qquad \varrho(\tilde{\omega}^\nu) = 1+O(1/\tilde{\omega}) \quad \text{if} \quad \nu \geqslant 1,\ \tilde{\omega} > 3,\ \tilde{\omega} \nmid N.$$

Returning to the "error term" E observe

$$|E(X, l)| \leqslant K\eta_1(Z, l),$$

where η_1 is as discussed in the author's paper [5]. Since the polynomial $f(r, s) = N-r^2-s^2$ satisfies the relevant hypotheses (being irreducible over the integers, having no fixed prime divisor and being not independent of either r or s) we may use the result

$$\sum_{l \leqslant Y/\log^\beta Y} \mu^2(l)|\eta_1(X, l)| \leqslant \frac{\mathrm{li}^2 Y}{(\log Y)^\delta},$$

which was deduced in [5] (for the special case $\delta = 2$, but the method is sufficient here) from Barban's Mean Value Theorem ([1], [3]) for the square of the error term in the prime number theorem for arithmetic progressions. Appropriate choice of Y establishes (A1) with

$$(3.13) \qquad \alpha = \tfrac{1}{2}.$$

Case II. The sets $\mathscr{A}_n$. It is necessary for our purposes to establish the properties (A1), (A2), (A3) for certain $n > Z$. This rules out any completely elementary approach. We quote results on the Kloosterman sum due to Weil, although earlier estimates due to Davenport [2] would also be more than sufficient for our purposes.

Let u, v cover the $Knl\xi(K, n, l)$ solutions of

$$(3.14) \qquad 1 \leqslant u, v \leqslant Knl;\ (uv, Kn) = 1;\ \langle u, v\rangle \epsilon \mathscr{R}_K;$$
$$u^2+v^2-N \equiv 0 \bmod Kn;\ uv(u^2+v^2-N) \equiv 0 \bmod Kln.$$

Express ξ as

$$(3.15) \qquad \xi(K, n, l) = \xi(K, 1, 1)\varrho(n)\sigma(n, l),$$

where $\sigma(n, 1) = 1$, so that ϱ is multiplicative. So too is σ in the sense

$$(3.16) \qquad \sigma(n, l) = \prod_{\tilde{\omega}^\nu \| n, \tilde{\omega}^\lambda \| l} \sigma(\tilde{\omega}^\nu, \tilde{\omega}^\lambda).$$

Observe that ϱ is as has already appeared in (3.5), and that

$$(3.17) \qquad \xi(K, 1, 1) = \psi(K, 1),$$

where ψ was also defined in (3.5).

Note that if $\varrho(n) = 0$ then $\mathscr{A}_n$ would be empty and the desired result (Lemma 9 below) would follow trivially. Consequently we need only consider the case when

$$(3.18) \qquad \varrho(n) \neq 0.$$

Hence, by (3.11),

$$(3.19) \qquad \varrho(n) \geqslant 1.$$

To estimate the sum (2.1) commence by noting

$$\sum_{\substack{a \epsilon \mathscr{A}_n \\ a \equiv 0 \bmod l}} 1 = \sum_{u,v} \Bigl(\sum_{r \equiv u \bmod Knl} 1\Bigr)\Bigl(\sum_{s \equiv v \bmod Knl} 1\Bigr),$$

where u, v cover the solutions of (3.14). Thus

$$(3.20) \qquad \sum_{\substack{a \epsilon \mathscr{A}_n \\ a \equiv 0 \bmod l}} 1 = \frac{1}{(Knl)^2} \sum_{1 \leqslant r,s \leqslant Z} \sum_{g,h \bmod Knl} \sum_{u,v} e\left(\frac{g(u-r)+h(v-s)}{Knl}\right)$$
$$= \frac{Z^2\xi(K, n, l)}{Knl}+O\left(\frac{Z\xi(K, n, l)}{Knl}\right)+$$
$$+\frac{1}{(Knl)^2} \sum_{\substack{g,h \bmod Knl \\ \langle g,h\rangle \neq \langle 0,0\rangle}} \sum_{1 \leqslant r,s \leqslant Z} e\left(\frac{-gr-hs}{Knl}\right) \sum_{u,v} e\left(\frac{gu+hv}{Knl}\right)$$
$$= X_n \frac{\sigma(n, l)}{l}\left\{1+O\left(\frac{1}{Z}\right)\right\}+E_n(X_n, l),$$

say, where

$$X_n = Z^2\xi(K,1,1)\varrho(n)/Kn \tag{3.21}$$

with ϱ, ξ, σ as in (3.15), and $e(x) = \exp(2\pi i x)$. Thus (3.17) shows that, in the notation of (3.6),

$$X_n = Z^2 B\left(\frac{\varphi(K)}{K}\right)^2 \frac{\varrho(n)}{n}. \tag{3.22}$$

We estimate the sum

$$S(g, h;\ K, n, l) = \sum_{u,v} e\left(\frac{gu+hv}{Knl}\right) \tag{3.23}$$

that features in (3.20) via its multiplicative property

$$S(g, h;\ K, n, l) = \prod_{\tilde\omega^{\varkappa}\|K,\, \tilde\omega^{\nu}\|n,\, \tilde\omega^{\lambda}\|l} S(g, h;\ \tilde\omega^{\varkappa}, \tilde\omega^{\nu}, \tilde\omega^{\lambda}). \tag{3.24}$$

Lemma 5. *Let*

$$\delta_{\tilde\omega}(k) = \begin{cases} 1 & \textit{if}\quad \tilde\omega|k, \\ 0 & \textit{if not}. \end{cases}$$

Then

(i) $S(g, h;\ 1, 1, \tilde\omega) \ll \tilde\omega\delta_{\tilde\omega}(g)\delta_{\tilde\omega}(h) + \sqrt{\tilde\omega}$ *if* $\tilde\omega \nmid 2N$,

(ii) $S(g, h;\ 1, 1, \tilde\omega) \ll \tilde\omega\delta_{\tilde\omega}(g)\delta_{\tilde\omega}(h) + (g^2+h^2, \tilde\omega)$ *if* $\tilde\omega|N$, $\tilde\omega \neq 2$,

(iii) $S(g, h;\ \tilde\omega^{\varkappa}, \tilde\omega^{\nu}, \tilde\omega^{\lambda}) \ll \tilde\omega^{\varkappa+\lambda+1}\xi(\tilde\omega^{\varkappa}, \tilde\omega^{\lambda}, \tilde\omega^{\nu})$.

Proof. (i) The non-trivial case is when $\tilde\omega \nmid gh$. Observe

$$S(g, h;\ 1, 1, \tilde\omega) = \sum_{\substack{u,v \\ uv(u^2+v^2-N)\equiv 0 \bmod \tilde\omega}} e\left(\frac{gu+hv}{\tilde\omega}\right)$$

$$= \sum_{u\equiv 0} + \sum_{v\equiv 0} + \sum_{u^2+v^2-N\equiv 0} + O(1).$$

Using well known properties of Gauss and Kloosterman sums we have

$$\sum_{u^2+v^2-N\equiv 0} = \frac{1}{\tilde\omega}\sum_{u,v,w} e_{\tilde\omega}\{w(u^2+v^2-N)+gu+hv\}$$

$$= \frac{1}{\tilde\omega}\sum_{w} e_{\tilde\omega}(-Nw) \sum_{u} e_{\tilde\omega}(wu^2+gu) \sum_{v} e_{\tilde\omega}(wv^2+hv)$$

$$= \frac{1}{\tilde\omega}\sum_{1\leqslant u,v\leqslant\tilde\omega} e_{\tilde\omega}(gu+hv) + \frac{1}{\tilde\omega}\sum_{w=1}^{\tilde\omega-1} e_{\tilde\omega}\{-Nw + a\overline{w}(g^2+h^2)\} \times$$

$$\times\Big[\sum_{x \bmod \tilde\omega} e_{\tilde\omega}(x^2)\Big]^2 \ll \sqrt{\tilde\omega}$$

when $\tilde\omega \nmid 2N$ and g, h are not both $0 \bmod \tilde\omega$. Here $x\overline{x} \equiv 1 \bmod \tilde\omega$ and $a = \overline{4} - \overline{2}$.

(ii) This follows by an argument differing from that for (i) only at the last step.

(iii) This is the "trivial" estimate that follows from $e(x) = O(1)$.

The next lemma uses the structure of n as $n = mq_1$, where q_1 is a "large" prime.

Lemma 6. *Suppose $g^2+h^2 \neq 0$. Define $A = 2mN(g,h)(g^2+h^2)$, where the* h.c.f. (g, h) *satisfies $(0, h) = h$, $(g, 0) = g$. Set $l = l_1 l_2$ where $\tilde\omega|l_1 \Rightarrow \tilde\omega|A$ and $(l_2, A) = 1$. Then if $L < q_1$, q_1 is prime and $\varepsilon > 0$ we have*

(i) $$\Sigma_1 = \sum_{l\leqslant L} \frac{\mu^2(l)}{l} |S(g, h; K, mq_1, l)| \ll KmL^{1/2}(AL)^{\varepsilon},$$

(ii) $$\Sigma_2 = \sum_{l\leqslant L} \mu^2(l)|S(g, h;\ K, mq_1, l)| \ll KmL^{3/2}(AL)^{\varepsilon}.$$

The implied constants may depend on ε.

Remark. In the application of this lemma, it will be crucial that the bounds obtained do not depend on q_1.

Proof. The given conditions imply $\tilde\omega \neq q_1$ when $\tilde\omega|l$ and $l \leqslant L$. Consequently use of Lemma 5 (the "trivial" part (iii) when $\tilde\omega|A$) gives

$$\Sigma_1 \ll \sum_{\substack{l_1 l_2 \leqslant L \\ \mu^2(l_1 l_2)=1}} Km\,\xi(K, m, l_1)\frac{d^{\omega(l_2)}}{\sqrt{l_2}},$$

where d is a constant implied in Lemma 5 by the use of the $\ll$ symbol. Thus

$$\Sigma_1 \ll \sum_{l_1|A} Km\xi(K, m, l_1) \sum_{\substack{l_2\leqslant L \\ \mu^2(l_2)=1}} d^{\omega(l_2)}/\sqrt{l_2} \ll KmL^{1/2}(AL)^{\varepsilon}$$

because $\xi(\tilde\omega^{\varkappa}, \tilde\omega^{\lambda}, \tilde\omega) = O(1)$. This proves part (i) of the lemma; part (ii) follows because $\Sigma_2 \leqslant L\Sigma_1$.

Lemma 7. *Let $E(X_n, l)$ be as defined in* (3.20). *Suppose $n = mq_1$ as in Lemma* 6, *where (as in the introduction) m and the prime q_1 satisfy*

$$m < Z^{1/3}, \quad Z^{5/6} < q_1, \tag{3.25}$$

and $N = 2Z^2$ as in (3.3). *Then the property* (A1) *holds for the set $\mathscr{A}_n$ with $\alpha = 1/3$.*

Proof. Use the inequality

$$\sum_{1\leqslant r<Z} e\left(\frac{gr}{Knl}\right) \ll \min\left\{Z, \frac{Kln}{|g|}\right\},$$

valid when $|g| \leqslant \frac{1}{2}Knl$. This shows

$$E(X_n, l) \ll \sum_{0<|g|,|h|\leqslant\frac{1}{2}Knl} \frac{1}{|gh|}|S(g, h;\ K, n, l)| + \\ + \frac{Z}{Knl} \sum_{0<|g|\leqslant\frac{1}{2}Knl} \frac{1}{|g|}|S(g, 0;\ k, n, l)| + \sum_{|g|=0}.$$

The hypotheses of the lemma give

$$L \leqslant X_n^{1/3} \tag{3.26}$$

while a trivial estimation of the number of solutions of (3.14) shows

$$Kn\xi(K, 1, 1)\varrho(n) \leqslant (Kn)^2,$$

so that (3.21) gives $X_n \leqslant Z^2$. Thus (3.26) and (3.25) give

$$L \leqslant Z^{2/3} \leqslant q_1.$$

Accordingly Lemma 6 applies and shows

$$\sum_{l\leqslant L} \mu^2(l)|E(X_n, l)| \\ \ll \sum_{0<|g|,|h|\leqslant\frac{1}{2}Knl} \frac{1}{|gh|} \sum_{l\leqslant L} \mu^2(l)|S(g, h;\ K, n, l)| + \\ + \frac{Z}{Kn} \sum_{0<|g|<\frac{1}{2}Knl} \frac{1}{|g|} \sum_{l\leqslant L} \frac{\mu^2(l)}{l}|S(g, 0; K, n, l)| + \\ + \sum_{h} \sum_{l\leqslant L, g=0} \\ \ll KmL^{3/2}N^{\varepsilon}(1+Z/Kn) \ll N^{\varepsilon}L^{3/2}(m+Z/q_1).$$

By (3.21), (3.11), (3.25) we have

$$X_n \gg Z^2/mq_1 \gg Z^{5/6} \quad \text{and} \quad Z/q_1+m \ll Z^{1/3} \ll X_n^{2/5}.$$

Also by (3.3) $N^{\varepsilon} \ll Z^{2\varepsilon} \ll X_n^{12\varepsilon/5}$. Thus by (3.26)

$$\sum_{l\leqslant L} \mu^2(l)|E(X_n, l)| \ll X^{9/10+12\varepsilon/5},$$

and the result of the lemma follows.

The reader will observe that the value 1/3 of α could, after some effort, be replaced by some relatively complicated function of m and q_1.

4. The application of the $\frac{1}{2}$-residue sieve. The set $\mathscr{A}$ to be sifted is of the type

$$\mathscr{A} = \Big\{a = \frac{N-p^2-q^2}{2^g 3^h}: p, q \text{ odd primes; } p, q \leqslant \sqrt{N/2}; \\ N-p^2-q^2 \equiv 2^{\varphi} \bmod 2^G;\ N-p^2-q^2 \equiv 0 \bmod 3^h\Big\}. \tag{4.1}$$

Thus in (3.1) we have taken $K = 2^g 3^h$ and $\mathscr{R}_K$ a certain set of residue classes modulo $2^G 3^H$. The choice made below of g, φ, G, H will ensure (*inter alia*)

(i) all members a of $\mathscr{A}$ satisfy

$$a \equiv 1 \bmod 4; \tag{4.2}$$

(ii) the parameter X appearing in (3.6) satisfies

$$X \to \infty \quad \text{as} \quad N \to \infty; \tag{4.3}$$

(iii) the function τ appearing in (3.7) satisfies

$$\tau(\tilde{\omega}) < \tilde{\omega} \quad \text{for all primes } \tilde{\omega} \tag{4.4}$$

and

$$\tau(2^{\mu}) = 0 \quad \text{for all exponents } \mu \geqslant 1. \tag{4.5}$$

To achieve this, specify

$$\begin{array}{lll} g = \varphi = G = 0 & \text{if} & N \equiv 3 \bmod 4, \\ g = 1,\ \varphi = G = 0 & \text{if} & N \equiv 4 \bmod 8, \\ g = \varphi = 2,\ G = 4 & \text{if} & N \equiv 6 \bmod 8, \\ g = \varphi = 3,\ G = 5 & \text{if} & N \equiv 2 \bmod 8 \end{array}$$

and

$$h = \begin{cases} 0 & \text{if} \quad N \equiv 2 \bmod 3, \\ 2 & \text{if} \quad N \equiv 2 \bmod 3. \end{cases}$$

Thus we have considered all five residue classes, mod 8, that, in the enunciation of our theorem, may contain N, and the implicit condition $N-p^2-q^2 \equiv 0 \bmod 2^g$ is a consequence of the others.

Condition (i) is now immediate from the fact $p^2 \equiv q^2 \equiv 1 \bmod 8$ and that h is even. Condition (ii) follows since our choices ensure that the associated congruences (3.4) do in fact have solutions when $l = 1$; thus in the notation of (3.6) we have

$$B > 0. \tag{4.6}$$

On the other hand (3.4) now has no solutions when $l = 2$ (this is a corollary of (i)); thus

$$\tau(2^\mu) = \varrho(2^\mu) = 0, \tag{4.7}$$

where ϱ is as in (3.7). Lastly, to show $\tau(\tilde{\omega}) < \tilde{\omega}$ we have to establish that in the congruences (3.4) with $l = \tilde{\omega}$ it is not the case that the condition

$$\tilde{\omega} | \{(u^2+v^2-N)/K\} \tag{4.8}$$

follows from the others. If $\tilde{\omega} > 3$ (so $\tilde{\omega} \nmid K$) this relation would imply $\tilde{\omega} | (u^2+v^2-N)$ whenever $(uv, \tilde{\omega}) = 1$, hence $\tilde{\omega} | (u_1^2-u_2^2)$ whenever $(u_1 u_2, \tilde{\omega}) = 1$, so $\tilde{\omega}$ would divide one of $5^2-1^2 = 24$ and $7^2-1^2 = 48$, a contradiction. If $\tilde{\omega} = 3$ then the identity $u^2+v^2-N \equiv 2-N \bmod 3$ shows $\tau(3) = 0$ if $N \not\equiv 2 \bmod 3$, while if $N \equiv 2 \bmod 3$ then (4.8) would require $9 | (u^2+v^2-N)$ whenever $(uv, 3) = 1$, hence $9 | (4^2-1^2)$, also a contradiction.

Property (A1), with $a = \frac{1}{2}$, was established in Section 3. To establish (A2), (A3) observe that (3.10) implies

$$\tau(\tilde{\omega}) = 1 + O(\tilde{\omega}^{-1}) \quad \text{if} \quad \tilde{\omega} \nmid N. \tag{4.9}$$

Also $\tau(\tilde{\omega}) = 0$ if $\tilde{\omega} | N$ and $\tilde{\omega} \equiv 3 \bmod 4$. With (iii) above this establishes (A2), (A3), with $\mathscr{P}$ as stated in (2.3), $a = \frac{1}{2}$ and $L = O(\log\log X)$ because

$$\sum_{\tilde{\omega}|N} \frac{\log\tilde{\omega}}{\tilde{\omega}} \leqslant \sum_{\tilde{\omega} \leqslant \log N} \frac{\log\tilde{\omega}}{\tilde{\omega}} + \frac{1}{\log N} \sum_{\tilde{\omega}|N} \log\tilde{\omega} = O(\log\log N). \tag{4.10}$$

From Lemma 2 we accordingly have

LEMMA 8. *Let $\mathscr{A}$ be as in* (4.1), *and suppose $z = X^{a/u}$ with $a = \frac{1}{2}$, $1 < u < 2$ and $X = B\,\mathrm{li}^2(\sqrt{N/2})$ as in* (3.6). *Let $\Pi(\mathscr{A}, \mathscr{P}_z)$ be the number of pairs of odd primes $p, q \leqslant \sqrt{N/2}$ such that the corresponding member $a = (N-p^2-q^2)/K$ of $\mathscr{A}$ is divisible by no prime $\tilde{\omega}$ with $\tilde{\omega} \equiv 3 \bmod 4$, $\tilde{\omega} < z$. Then*

$$\Pi(\mathscr{A}, \mathscr{P}_z) > \frac{X}{\sqrt{\log X^a}} D\Pi_0 \left\{ \int_1^u \frac{dt}{\sqrt{t^2-t}} + O\left(\frac{\log\log X}{(\log X)^{1/10}}\right)\right\},$$

where

$$\Pi_0 = \prod_{\tilde{\omega} \equiv 3 \bmod 4} \frac{1-\tau(\tilde{\omega})/\tilde{\omega}}{1-1/\tilde{\omega}} \tag{4.11}$$

with τ as in (3.7).

It is important to observe that because of (4.4) and property (A3) established above the infinite product defining Π_0 converges, and that

$$\Pi_0 > 0. \tag{4.12}$$

In practice it is slightly more convenient to express this result in terms of N, and to set $z = N^{a/v}$. Since $X = B\,\mathrm{li}^2(\sqrt{N/2})$ from (3.3), (3.6), so that $\log X = \log N + O(\log\log N)$, we obtain under the conditions of Lemma 8 that

$$\Pi(\mathscr{A}, \mathscr{P}_z) > \frac{DB\Pi_0}{\sqrt{2}} \frac{N}{(\log N)^{5/2}} \left\{ \int_1^v \frac{dt}{\sqrt{t^2-t}} + O\left(\frac{\log\log N}{(\log N)^{1/10}}\right)\right\}. \tag{4.13}$$

Observe that in the notation of the introduction

$$\Pi(\mathscr{A}, \mathscr{P}_z) = E. \tag{4.14}$$

5. The application of the upper bound sieve. The sets $\mathscr{A}_n$ to be sifted are

$$\mathscr{A}_n = \left\{\frac{rs(N-r^2-s^2)}{2^g 3^h n} :\ 1 \leqslant r, s \leqslant \sqrt{N/2};\ N-r^2-s^2 \equiv 2^g \bmod 2^G;\right.$$
$$\left. N-r^2-s^2 \equiv 0 \bmod 3^h n;\ (rs, 6n) = 1\right\}, \tag{5.1}$$

where $n = mq_1$ as in Lemmas 6 and 7. These sets are as in (3.2), where the choices of Z, $\mathscr{R}_K$ are as already made in previous sections. Thus from Lemma 7 the property (A1) holds for $\mathscr{A}_n$ with $a = 1/3$ and $X = X_n$, $\gamma(\tilde{\omega}) = \sigma(\tilde{\omega}^\nu, \tilde{\omega})$ as given in (3.20). Recall from (3.16) that ν is defined by $\tilde{\omega}^\nu \| n$ and that we may suppose as in (3.18) that

$$\varrho(n) \neq 0, \tag{5.2}$$

as the result of Lemma 9 below holds trivially if $\varrho(n) = 0$ because the set $\mathscr{A}_n$ is then empty.

Comparison of the congruences in (3.4) and (3.14) shows

$$\sigma(1, \tilde{\omega}) = 2 - \frac{1}{\tilde{\omega}} + \varrho(\tilde{\omega}) \quad \text{if} \quad \tilde{\omega} > 3, \tag{5.3}$$

$$\sigma(\tilde{\omega}^\nu, \tilde{\omega})\, \varrho(\tilde{\omega}^\nu) = \varrho(\tilde{\omega}^{\nu+1}) \quad \text{if} \quad \tilde{\omega} > 3 \text{ and } \nu > 0 \tag{5.4}$$

because $\tilde{\omega} \nmid K$ when $\tilde{\omega} > 3$. Because of (3.12) and (5.2) this implies

$$\gamma(\tilde{\omega}) = 3 + O(\tilde{\omega}^{-1}) \quad \text{if} \quad \tilde{\omega} \nmid mNq_1,$$
$$\gamma(\tilde{\omega}) \geqslant 0 \quad \text{for all } \tilde{\omega}.$$

Note also

$$\sigma(1, 2) = 0 \tag{5.5}$$

because the choice of $\mathscr{R}_K$ in (4.1) satisfies (4.2).

Returning to γ we infer

$$\sum_{\tilde{\omega} < z} \frac{\gamma(\tilde{\omega})\log\tilde{\omega}}{\tilde{\omega}} \geqslant 3\log z + O\left(1 + \sum_{\tilde{\omega}|mN} \frac{\log\tilde{\omega}}{\tilde{\omega}}\right) \geqslant 3\log z + O(\log\log N)$$

by the argument used at (4.10) and the fact that $mq_1 \leqslant N$ from (1.4).

These remarks establish the conditions of Lemma 4 for the set $\mathscr{A}_n$. The corresponding conclusion gives the following result.

LEMMA 9. *Suppose q_1 is prime and $q_1 > N^{5/12}$. Let $P(m, q_1)$ denote the number of pairs of primes p, q such that the corresponding member a of the set $\mathscr{A}$ defined in* (4.1) *is of the form $a = mq_1q_2$ where $q_2 > q_1$ and q_2 is prime. Then*

$$P(m, q_1) < 2^6 3^4 B \frac{\varrho(mq_1)}{mq_1} \left(\frac{\varphi(K)}{K}\right)^2 \frac{N}{\log^3 N} \left\{\prod \frac{1-\sigma(\tilde{\omega}^\nu, \tilde{\omega})/\tilde{\omega}}{(1-1/\tilde{\omega})^3}\right\} \times$$
$$\times \left\{1 + O\left(\frac{\log\log N}{\log N}\right)\right\},$$

where the infinite product is convergent.

Arising from the result of Lemma 9 it will be necessary to estimate

$$\Sigma(y) = \sum_{m \leqslant y} \frac{\varrho(m)}{m} \prod_{\tilde{\omega}^\mu \| m} \frac{1-\sigma(\tilde{\omega}^\mu, \tilde{\omega})/\tilde{\omega}}{(1-1/\tilde{\omega})^3}$$

where the summation is over m divisible by no prime $\tilde{\omega} \equiv 3 \bmod 4$. First note an important property of the function σ: from (5.3) and (3.7) we have for primes $\tilde{\omega} > 3$ (for which $\tilde{\omega} \nmid K$)

$$(5.6) \qquad 1 - \frac{\sigma(1, \tilde{\omega})}{\tilde{\omega}} = \left(1 - \frac{1}{\tilde{\omega}}\right)^2 - \frac{\varrho(\tilde{\omega})}{\tilde{\omega}} = \left(1 - \frac{1}{\tilde{\omega}}\right)^2 \left(1 - \frac{\tau(\tilde{\omega})}{\tilde{\omega}}\right),$$

with τ as in (3.7). Thus $\sigma(1, \tilde{\omega}) < \tilde{\omega}$ because of (4.4), and (4.9) gives

$$(5.7) \qquad \left(1 - \sigma(1, \tilde{\omega})/\tilde{\omega}\right)^{-1} = O(1).$$

Returning to $\Sigma(y)$ observe

$$\Sigma(y) = \prod_{\tilde{\omega} \not\equiv 3 \bmod 4} \frac{1-\sigma(1, \tilde{\omega})/\tilde{\omega}}{(1-1/\tilde{\omega})^3} \sum_{m \leqslant y} \frac{\gamma(m)}{m}$$

where now the multiplicative function γ is given by

$$\gamma(\tilde{\omega}^\mu) = \frac{\varrho(\tilde{\omega}^\mu) - \varrho(\tilde{\omega}^{\mu+1})/\tilde{\omega}}{1 - \sigma(1, \tilde{\omega})/\tilde{\omega}}.$$

Thus because of (3.12) and (5.7) the conditions of Lemma 3 are satisfied and we infer

$$\sum_{m \leqslant y} \frac{\gamma(m)}{m} = gD\sqrt{\log y} + O(\log^{1/4} y),$$

where

$$g = 4 \prod_{\tilde{\omega} \not\equiv 3 \bmod 4} \left\{\left(1 - \frac{1}{\tilde{\omega}}\right) \sum_{\mu \geqslant 0} \frac{\varrho(\tilde{\omega}^\mu)}{\tilde{\omega}^\mu} \frac{1-\sigma(\tilde{\omega}^\mu, \tilde{\omega})/\tilde{\omega}}{1-\sigma(1, \tilde{\omega})/\tilde{\omega}}\right\}.$$

Consequently

$$(5.8) \qquad \Sigma(y) = HD\sqrt{\log y} + O(\log^{1/4} y)$$

where

$$H = 4 \prod_{\tilde{\omega} \not\equiv 3 \bmod 4} \left\{\frac{1}{(1-1/\tilde{\omega})^2} \sum_{\mu \geqslant 0} \frac{\varrho(\tilde{\omega}^\mu)}{\tilde{\omega}^\mu} \left(1 - \sigma(\tilde{\omega}^\mu, \tilde{\omega})/\tilde{\omega}\right)\right\}.$$

Because of (3.12), (5.3) and (5.4) the contribution to H from odd primes $\tilde{\omega}$ is

$$\frac{1}{(1-1/\tilde{\omega})^2} \left\{\left(1 - \frac{\sigma(1, \tilde{\omega})}{\tilde{\omega}}\right) + \frac{\varrho(\tilde{\omega})}{\tilde{\omega}}\right\} = 1.$$

Thus (5.5) and (4.7) show

$$(5.9) \qquad H = 2^4.$$

Lemma 9 and this estimate for $\Sigma(y)$ now yield the following result.

LEMMA 10. *Let $\mathscr{A}$ be as in* (4.1), *and suppose $N^{5/12} < z < N^{1/2}$. Let E' be the number of a in $\mathscr{A}$ that are of the form q_1q_2m, where*

(i) *$\tilde{\omega} | m$ implies $\tilde{\omega} \not\equiv 3 \bmod 4$ and $\tilde{\omega} \leqslant z$,*

(ii) *q_1, q_2 are primes, $z < q_1 \leqslant q_2$, and $q_i \equiv 3 \bmod 4$. Then*

$$E' < CD\Pi_0 \frac{N}{\log^3 N} \log^{1/2}(N/z^2) \log\left(\frac{\log N}{2\log z}\right) \left\{1 + O\left(\frac{\log\log N}{\log N}\right)\right\},$$

where D, Π_0 are as in Lemma 8 and $C = 2^{10} 3^4 B\left(\varphi(K)/K\right)^2$.

Proof. With $P(m, q_1)$ as in Lemma 9 we have

$$E' \leqslant \sum_{m \leqslant N/z^2} \sum_{z < q_1 < \sqrt{N}} P(m, q_1)$$
$$= 2^6 3^4 \left(\frac{\varphi(K)}{K}\right)^2 B \frac{N}{\log^3 N} \Sigma(N/z^2) \sum_{z < q_1 < \sqrt{N}} \frac{\varrho(q_1)}{q_1} \left\{1 + O\left(\frac{\log\log N}{\log N}\right)\right\}.$$

But $\varrho(q_1) = O(1)$ (by (3.10), or trivially if $q_1 | N$ because $q_1 \equiv 3 \bmod 4$). The result now follows by (5.8), (5.9).

6. Conclusion. It merely remains to observe that in the notation of the Introduction we have firstly, by (4.13), (4.14),

$$E > \frac{1}{\sqrt{2}} DB\Pi_0 \frac{N}{(\log N)^{5/2}} \left\{\int_1^v \frac{dt}{\sqrt{t^2 - t}} + O\left(\frac{\log\log N}{(\log N)^{1/10}}\right)\right\},$$

secondly (Lemma 10)

$$E' < DC\Pi_0 \frac{N}{(\log N)^{5/2}} (\log v) \sqrt{\left(1-\frac{1}{v}\right)} \left\{1+O\left(\frac{\log\log N}{(\log N)^{1/10}}\right)\right\}.$$

Here v is defined by the relation $z = N^{1/(2v)}$ as in (4.13). Choose v in the range $1 \leqslant v < 6/5$ permitted in Lemma 10 so as to maximise

$$g(v) = \int_1^v \frac{dt}{\sqrt{t^2-t}} - \frac{C\sqrt{2}}{B} (\log v) \sqrt{\left(1-\frac{1}{v}\right)};$$

this maximum value G is positive because for $v > 1$

$$g(v) = 2\sqrt{v-1} + O\left((v-1)^{3/2}\right).$$

This gives the theorem stated in the Introduction, with

$$A = DBG\Pi_0/\sqrt{2}. \tag{6.1}$$

Here B is as in (4.13) and D is given by (2.4). The product Π_0 was defined in (4.11). Because of (4.12) we have $A > 0$ as required.

It is possible to replace the constant A of our theorem by a larger number, for example by following up the consequences of the remark made at the end of Section 3.

References

[1] M. B. Barban, *Analogues of the divisor problem of Titchmarsh*, Vestnik Leningrad. Univ. Ser. Mat. Meh. Astronom. 18 (1963), pp. 5–33.

[2] H. Davenport, *On certain exponential sums*, J. Reine Angew. Math. 169 (1933), pp. 391–424.

[3] H. Davenport and H. Halberstam, *Primes in arithmetic progressions*, Michigan Math. J. 13 (1966), pp. 485–489.

[4] P. D. T. A. Elliott and H. Halberstam, *Some applications of Bombieri's theorem*, Mathematika 13 (1967), pp. 196–203.

[5] G. Greaves, *An application of a theorem of Barban, Davenport and Halberstam*, Bull. London Math. Soc. 6 (1974), pp. 1–9.

[6] C. Hooley, *On the representation of a number as the sum of two squares and a prime*, Acta Math. 97 (1957), pp. 189–210.

[7] H. Iwaniec, *Primes of the type $\varphi(x, y)+A$ where φ is a quadratic form*, Acta Arith. 21 (1972), pp. 203–234.

[8] E. Jacobsthal, *Anwendungen einer Formal aus der Theorie der Quadratischen Reste*, Dissertation, Berlin 1906.

[9] E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen*, Teubner, Leipzig 1909, or Chelsea, New York 1953.

[10] W. J. LeVeque, *Topics in Number Theory*, Vol. 2, Addison-Wesley, London 1956.

Received on 29. 7. 1974 (604)

ACTA ARITHMETICA
XXIX (1976)

Lower bounds for discriminants of number fields

by

A. M. Odlyzko (Cambridge, Mass.)

1. Introduction. Let K be an algebraic number field of degree $n = n_K$, with r_1 real conjugate fields and $2r_2$ complex conjugate fields, and let $D = D_K$ be the absolute value of the discriminant of K. In 1882 Kronecker [6] conjectured that

$$D > 1 \quad \text{for} \quad n > 1. \tag{1.1}$$

This very important result was first proved in 1891 by Minkowski [10] as one of the earliest applications of geometry of numbers. Subsequently, by refining his methods, Minkowski [11] showed that in fact

$$D^{1/n} \geqslant \left(\frac{\pi}{4}\right)^{2r_2/n} n^2(n!)^{-2/n} = (e^2)^{r_1/n}\left(\frac{\pi e^2}{4}\right)^{2r_2/n} + o(1) \tag{1.2}$$

$$= (7.389\ldots)^{r_1/n}\ (5.803\ldots)^{2r_2/n} + o(1)$$

as $n \to \infty$, which is the estimate usually presented in books [8], [13]. Due to the efforts of many mathematicians, today there exists an extensive literature devoted to lower bounds for discriminants (for complete references, see [13], pp. 80–81 and [16]). Of those papers which do not use geometry of numbers methods, most prove only (1.1). Of the few which obtain lower bounds for D which are exponential in n, the best until very recently was Siegel's estimate [18], which states that for K totally real (i.e., $r_1 = n$, $r_2 = 0$),

$$D^{1/n} \geqslant 7.402\ldots + o(1)$$

as $n \to \infty$, which is slightly better than (1.2). Considerably better estimates have obtained through geometry of numbers. The best published bound for totally real K is due to Rogers [16], who showed that in this case

$$D^{1/n} \geqslant \frac{16e^3}{\pi^2} + o(1) = 32.561\ldots + o(1)$$