простых чисел p, q и целых $u>0$, $v>0$, для которых $p^u-q^v=2$, причем $\max(u,v)\ll 1$. Из теории диофантовых уравнений следует тогда, что хотя бы одно из чисел u, v равно 1, и мы найдем, что существует бесконечное число простых чисел вида q^w+2 или q^w-2, где q — простое, а w ограничено.

Цитированная литература

[1] Ю. В. Линник, *О выражении L-рядов через ζ-функцию*, Докл. АН СССР 57 (1947), стр. 435–437.
[2] Е. К. Титчмарш, *Теория дзета-функции Римана*, Москва 1953.

Поступило 11. 10. 1973 (472)

ACTA ARITHMETICA
XXVII (1975)

On shifted primes

by

E. Fogels (Riga)

In memory of Yu. V. Linnik

1. Introduction. Using the extended Riemann hypothesis in 1930 Titchmarsh [15] proved an asymptotic estimate for the sum of the number of divisors $d(p-c_1)$ extended over the shifted primes $p-c_1$ (c_1 an integer constant $\neq 0$). In 1957 Hooley [10] proved an analogous formula (also on the extended Riemann hypothesis) with $d(p-c_1)$ replaced by $r(p-c_1)$, the number of representations of $p-c_1$ as a sum of two squares (which is also the number of integers having the norm $p-c_1$ in the field generated by $\sqrt{-1}$). About 1960 Linnik (see [13]) showed that these results of Titchmarsh and Hooley can be proved without any hypotheses but using his rather complicated method of dispersions. In 1965 Bombieri ([1], Theorem 4) proved a mean value theorem for the function

$$\max_{1\leqslant y\leqslant x}\max_{(k,l)=1}\Big|\sum_{y\geqslant n\equiv l(\mathrm{mod}\,k)}\Lambda(n)-y/\varphi(k)\Big|$$

where $\Lambda(n)=\log p$ if $n=p^k$ (p prime, $k=1,2,\ldots$), $\Lambda(n)=0$ otherwise and $\varphi(k)$ is the number of reduced classes mod k. This theorem has been used since by many authors as a powerful substitute for the extended Riemann hypothesis. We shall mention here merely Elliott and Halberstam [6] who showed that some small changes in Hooley's paper would make his proofs unconditional. In the present paper we shall prove a generalization of this result for a set of primes p^* which are norms of ideals of a fixed class $\mathfrak{K}_1$ in a quadratic field K_1 (of discriminant Δ_1) on the condition that the shifted primes p^*-c_1 are norms of integer ideals $\mathfrak{a}$ belonging to another class $\mathfrak{K}$ (possibly $\mathfrak{K}=\mathfrak{K}_1$) in the same or another quadratic field K with the discriminant Δ. For the sum

$$(1)\qquad \pi(x;\mathfrak{K})=\pi(x;\mathfrak{K},\mathfrak{K}_1,c_1)=\sum_{\substack{\mathfrak{a}\in\mathfrak{K},(N\mathfrak{a},\Delta)=1\\ p^*-c_1=N\mathfrak{a}\leqslant x}}1$$

we shall prove the asymptotic formula

$$\pi(x; \mathfrak{K}) = c_2 x/\log x + O\big(x(\log x)^{-1-\delta_1}\big) \quad (x\to\infty) \tag{2}$$

where δ_1 stands for a positive constant depending merely on the number of ideal classes in K (see (50), (46), (44)) and apart from an exceptional case $c_2 = c_2(c_1, \Delta_1, \Delta)$ is positive (see the Theorem and (50), (35), (20), (19), (74)).

The principal aim in writing this paper is a possibly simple application of a mean value theorem of Bombieri's type (see (13), (14)). For this reason we have introduced in (1) the restriction $(N\mathfrak{a}, \Delta) = 1$ which could be removed using in (8) one more summation (cf. [3], pp. 150–151).

Let g denote the number of genera of classes $\mathfrak{K}$ in K and let $\lambda = \varphi(\Delta)/2g$ (1). There are λ natural numbers $c_0 < |\Delta|$ with

$$(c_0, \Delta) = 1 \tag{3}$$

such that the idealnorms $N\mathfrak{a}$ with $(N\mathfrak{a}, \Delta) = 1$ and $\mathfrak{a}$ belonging to the genera $\mathfrak{G} \supset \mathfrak{K}$ are the positive numbers $\equiv c_0 (\mathrm{mod}\ \Delta)$ (see [3], pp. 150–151). In proving (2) we shall use the following restriction: For at least one of the numbers c_0 there is an integer ideal $\mathfrak{a}_1 \in \mathfrak{K}_1$ such that

$$(N\mathfrak{a}_1, \Delta) = 1, \quad N\mathfrak{a}_1 \equiv c_0 + c_1 (\mathrm{mod}\ \Delta). \tag{4}$$

We shall prove the following

THEOREM. *On the condition* (4) *we have in* (2) $c_2 > 0$ *with exception of the case* $\Delta_1 \equiv 12 (\mathrm{mod}\ 16)$, $\Delta \equiv 5 (\mathrm{mod}\ 8)$ *and* $-c_1$ *an odd number congruent* mod 4 *to an idealnorm of the class* $\mathfrak{K}_1$. *In this exceptional case* $c_2 = 0$.

The theorem remains true also in the case of $\Delta_1 = 1$ when K_1 is the field of rational numbers and p^* runs through all primes, generally denoted by p (2). We take for granted that $\Delta \neq 1$ (whence $|\Delta| \geqslant 3$), since the case with K the field of rationals is of no interest.

The condition (4) by which a restriction on the choice of c_1 is imposed, is not superfluous. If for example $\Delta = \Delta_1 = -3$, then merely the primes $p^* = 3$ and $p^* \equiv 1 (\mathrm{mod}\ 3)$ are representable by the form u^2+uv+v^2 (representing norms in K and K_1); diminished by $c_1 = -1$ they give 4 and numbers $\equiv 2 (\mathrm{mod}\ 3)$. The latter being not representable by the form, in the present case the equation $p^* - c_1 = N\mathfrak{a}$ ($\mathfrak{a} \in \mathfrak{K}$, $N\mathfrak{a} \leqslant x$) has no more than a single solution, whence (2) cannot hold with $c_2 > 0$.

---

(1) For $\Delta < 0$ by $\varphi(\Delta)$, mod Δ, ... we mean $\varphi(|\Delta|)$ and mod $|\Delta|$, respectively.

(2) In the case of $\Delta_1 = 1$ the proof is simpler and can be based on Bombieri's theorem [1]; and if we drop in (1) the restriction $(N\mathfrak{a}, \Delta) = 1$, then the condition (4) gets superfluous.

In the expression (1) any shifted prime $p^* - c_1$ reappears as many times as there are ideals $\mathfrak{a} \in \mathfrak{K}$ with $N\mathfrak{a} = p^* - c_1$. The number of ideals $\mathfrak{a}$ in K with $N\mathfrak{a} = a$ being

$$\sum_{d|a} \left(\frac{\Delta}{d}\right) \tag{5}$$

(cf. [12], Satz 882) from (2) we deduce (provided $c_2 > 0$) that for any constant $\varepsilon > 0$ and $x > x_0(\varepsilon)$ there are $> x^{1-\varepsilon}$ shifted primes $p^* - c_1$ in the sequence of all different idealnorms $N\mathfrak{a} \leqslant x$ with $\mathfrak{a} \in \mathfrak{K}$. By Iwaniec [11] the order of magnitude for the number of shifted primes $p - c_1$ in the sequence of all different idealnorms $N\mathfrak{a} \leqslant x$, $\mathfrak{a} \in \mathfrak{K}$, is $x(\log x)^{-3/2}$. His method seems applicable in proving a similar result also for the shifted primes $p^* - c_1$.

The chief weapon of proof in the present paper is a mean value theorem of Bombieri's type, but for primes p^* which are idealnorms of class $\mathfrak{K}_1$ (see [9]). The method is in outline the same as in the papers of Elliott–Halberstam [6], Hooley [10] and Bredihin–Linnik [3], except that we deal with the conjugate problem. The transition from $\pi(x; \mathfrak{G})$ (see (6)) to $\pi(x; \mathfrak{K})$ in § 8 is then by the method of Bredihin–Linnik [3], first used in proving an asymptotic formula for the number of representations of a large number n as the sum of a prime p and a number representable by a given binary quadratic form. In a similar paper [4] by the same authors and Čudakov the same problem is considered but for a set of primes p^* representable by some other binary quadratic form, both discriminants supposed negative.

2. The function $\pi(x; \mathfrak{G})$**.** Instead of (2) we shall prove first an analogous result for a simpler function

$$\pi(x; \mathfrak{G}) = \sum_{\substack{\mathfrak{a}\in\mathfrak{G}, (N\mathfrak{a}, \Delta)=1 \\ p^*-c_1=N\mathfrak{a}\leqslant x}} 1 \tag{6}$$

where $\mathfrak{G}$ is the genera containing the given class $\mathfrak{K}$. Choosing a fixed c_0 satisfying (3) and (4) we introduce the function

$$g(x, c_0) = \sum_{x\geqslant p^*-c_1=lm\equiv c_0 (\mathrm{mod}\ \Delta)} \left(\frac{\Delta}{l}\right). \tag{7}$$

The Kronecker symbol (Δ/l) being a character mod $|\Delta|$ ([12], I, p. 83) instead of it throughout this paper we shall write $\chi(l)$. Considering that all ideals $\mathfrak{a}$ with the same norm $a = N\mathfrak{a}$ are in the same genera (see [2], p. 320), we have by (5), (6), (7)

$$\pi(x; \mathfrak{G}) = \sum_{c_0} g(x, c_0). \tag{8}$$

Comparing (8), (35) and (48) one can see that for any fixed value of c_0 not satisfying (4) the contribution of the shifted primes in (2) is of no importance (³). Therefore the sum in (8) is merely over numbers c_0 satisfying (4).

By c denoting some constant $\geqslant 3$ (which will be specified in § 3) we split the sum (7) into parts

$$g(x, c_0) = \Sigma_A + \Sigma_B + \Sigma_C \tag{9}$$

corresponding to the values of

$$l \leqslant x^{1/2}(\log x)^{-c}, \quad x^{1/2}(\log x)^{-c} < l < x^{1/2}(\log x)^{c}, \quad l \geqslant x^{1/2}(\log x)^{c}, \tag{10}$$

respectively.

3. An estimate for the sum Σ_A. For any natural number q let $\varphi_1(q)$ denote the number of reduced classes $a \pmod q$ such that there are integer ideals $\mathfrak{a}_1 \in \mathfrak{K}_1$ with $N\mathfrak{a}_1 \equiv a \pmod q$; any such a throughout this paper will be called *admissible* mod q. We shall use the following properties:

$$\varphi_1(q) = \varphi(q) \quad \text{if} \quad (q, \Delta_1) = 1; \tag{11}$$

$$\varphi_1(q_1 q_2) = \varphi_1(q_1) \cdot \varphi_1(q_2) \quad \text{if} \quad (q_1, q_2) = 1. \tag{12}$$

For a proof see the Appendix, Lemma 3.

Let a be admissible mod q and $\pi^*(x; q, a)$ stand for the number of primes $p^* \equiv a \pmod q$, $p^* \leqslant x$. By h_1 denoting the number of the ideal classes in the field K_1 and writing

$$E(y, q) = \max_{a \pmod q} |\pi^*(y; q, a) - (\mathrm{Li}\, y)/h_1\varphi_1(q)| \tag{13}$$

we have (see [9])

$$\sum_{q \leqslant x^{1/2}(\log x)^{-B}} \max_{y \leqslant x} E(y, q) \ll x(\log x)^{-A} \quad (x \geqslant 3) \tag{14}$$

for any constant $A > 0$ and appropriate $B = B(A) > 0$. We shall use (14) with $A = 2$. Now we fix the constant c in (10) to be $= \max\{3, B(2)+1\}$.

To estimate Σ_A by means of (14) we have first to show that the primes p^* satisfying the condition

$$p^* - c_1 \equiv lm \equiv c_0 \pmod \Delta \tag{15}$$

(see (7)) are admissible mod $l\Delta$, provided that $(l, c_1) = 1$ and $(l, \Delta) = 1$. We may take for granted that $(l, \Delta) = 1$, since otherwise in (7) $\chi(l) = 0$. We replace (15) by the system of congruences

$$\begin{cases} p^* \equiv c_1 \pmod l, \\ p^* \equiv c_1 + c_0 \pmod \Delta. \end{cases} \tag{16}$$

Since by (4) $c_1 + c_0$ is admissible mod Δ, there are primes p^* satisfying the second congruence (16) (see [9], § 3). Provided that c_1 is admissible mod l (no other values of l will be used) the system (16) is compatible (since $(l, \Delta) = 1$), its solution being

$$p^* \equiv c_3 \pmod{l\Delta} \tag{17}$$

for appropriate c_3, admissible mod $l\Delta$ (see the proof of (12)).

Now by (7), (9), (10), (15), (17)

$$\Sigma_A = \sum_{\substack{l \leqslant x^{1/2}(\log x)^{-c},\, c_1 \text{adm.} \bmod l \\ p^* \equiv c_3 \pmod{l\Delta}}} \chi(l)$$

whence by (13), (14)

$$\Big| \Sigma_A - \sum_{l \leqslant x^{1/2}(\log x)^{-c},\, c_1 \text{adm.} \bmod l} \frac{\chi(l)\,\mathrm{Li}(x + c_1)}{h_1 \varphi_1(l\Delta)} \Big| \leqslant \sum_{l \leqslant x^{1/2}(\log x)^{-c}} E(x + c_1, l\Delta) \ll \frac{x + c_1}{\log^2 x}$$

and thus by (12)

$$\Sigma_A = \frac{\mathrm{Li}(x + c_1)}{h_1 \varphi_1(\Delta)} \sum_{l \leqslant x^{1/2}(\log x)^{-c},\, c_1 \text{adm.} \bmod l} \frac{\chi(l)}{\varphi_1(l)} + O\Big(\frac{x}{\log^2 x}\Big). \tag{18}$$

By a generalization of Hooley [10], Lemma 3, for a nonprincipal character $\chi \bmod \Delta$ we have

$$\sum_{\substack{l' \leqslant y \\ (l', m) = 1}} \frac{\chi(l')}{\varphi(l')} = C_\chi E(m) + O\Big(\frac{\log 2y}{y} d(m)\Big)$$

(for any $y > 1$ and any natural number m) where

$$C_\chi = L(1, \chi) \prod_p \Big(1 + \frac{\chi(p)}{p(p-1)}\Big), \quad E(m) = \prod_{p \mid m} \frac{(p-1)(p - \chi(p))}{p^2 - p + \chi(p)}, \tag{19}$$

$L(s, \chi)$ being the Dirichlet L-function. Hence

$$\sum_{\substack{l' \leqslant y \\ (l', c_1\Delta_1) = 1}} \frac{\chi(l')}{\varphi(l')} = c_4 + O\Big(\frac{\log 2y}{y}\Big), \quad c_4 = C_\chi \cdot E(c_1\Delta_1) > 0, \tag{20}$$

by (19).

(³) Let us suppose that corresponding to the fixed c_0 (satisfying (3)) there is at least one shifted prime $p^* - c_1 > |\Delta| + |c_1|$ in the sequence of idealnorms $N\mathfrak{a}$ with $\mathfrak{a} \in \mathfrak{K}$, $(N\mathfrak{a}, \Delta) = 1$. Then there is a prime ideal $\mathfrak{p}_1 \in \mathfrak{K}_1$ such that $N\mathfrak{p}_1 = p^* > |\Delta|$, whence $(N\mathfrak{p}_1, \Delta) = 1$ and we have $p^* - c_1 = N\mathfrak{a} \equiv c_0 \pmod \Delta$. Hence $N\mathfrak{p}_1 \equiv c_1 + c_0 \pmod \Delta$, which is (4) with $\mathfrak{a}_1 = \mathfrak{p}_1$.

Let us write the variable l of (18) in the form of

$$l = ql', \quad (l', c_1\Delta_1) = 1, \tag{21}$$

where q is either 1 or a natural number divisible merely by primes dividing Δ_1. Then $(q, l') = 1$, whence by (21), (12), (11)

$$\varphi_1(l) = \varphi_1(q)\cdot\varphi(l')$$

and writing

$$y = x^{1/2}(\log x)^{-c} \tag{22}$$

we have

$$\sum_{\substack{l\leqslant y\\ c_1\text{adm.}\bmod l}} \frac{\chi(l)}{\varphi_1(l)} = \sum_{\substack{1\leqslant q\leqslant y\\ c_1\text{adm.}\bmod q}} \frac{\chi(q)}{\varphi_1(q)} \sum_{\substack{l'\leqslant y/q,\, c_1\text{adm.}\bmod l'\\ (l', c_1\Delta_1)=1}} \frac{\chi(l')}{\varphi(l')}. \tag{23}$$

Since $l = q\cdot l'$, $(q, l') = 1$, in order that c_1 should be admissible mod l, it is necessary and sufficient that (i) c_1 admissible mod l' and (ii) c_1 admissible mod q (see the proof of (12)). The condition (i) holds by (11) for any l' with $(l', \Delta_1 c_1) = 1$. The investigation of numbers q satisfying (ii) will be postponed to the Appendix, Lemmas 4–7.

By (20), (23), (22) and Appendix, Lemma 8

$$\sum_{\substack{l\leqslant y\\ c_1\text{adm.}\bmod l}} \frac{\chi(l)}{\varphi_1(l)} = \sum_{\substack{1\leqslant q\leqslant y\\ c_1\text{adm.}\bmod q}} \frac{\chi(q)}{\varphi_1(q)}\left\{c_4 + O\left(\frac{\log 2y}{y/q}\right)\right\}$$

$$= c_4 \sum_{\substack{1\leqslant q\leqslant y\\ c_1\text{adm.}\bmod q}} \frac{\chi(q)}{\varphi_1(q)} + O\left(\frac{\log y}{y}\sum_{1\leqslant q\leqslant y}\frac{q}{\varphi_1(q)}\right)$$

$$= c_4\left\{\sum_{\substack{1\leqslant q<\infty\\ c_1\text{adm.}\bmod q}} \frac{\chi(q)}{\varphi_1(q)} - \sum_{\substack{q>y\\ c_1\text{adm.}\bmod q}} \frac{\chi(q)}{\varphi_1(q)}\right\} + O\left(\frac{\log^{b+2} y}{y}\right)$$

$$= c_4 c_7 + O\left(\frac{\log^{b+c+2} x}{x^{1/2}}\right),$$

since the number of numbers $q \leqslant x$ $(x > 8)$ is $\ll (\log x)^b$, where b stands for the number of different primes dividing Δ_1, and since $q/\varphi_1(q) \ll \log q$ ([14], p. 24, Satz 5.1). Hence by (18)

$$\Sigma_A = c_5 x/\log x + O(x/\log^2 x), \tag{24}$$

where the constant

$$c_5 = c_4 c_7/h_1\varphi_1(\Delta) \tag{25}$$

(see (20), (74)) is generally > 0 with exception of the case when $-c_1$ is an odd number $\equiv N\mathfrak{a}_1 \pmod 4$ for appropriate $\mathfrak{a}_1 \in \mathfrak{K}_1$, and $\Delta_1 \equiv 12 \pmod{16}$, $\Delta \equiv 5 \pmod 8$ (see Appendix, Lemma 8).

4. The sum Σ_C. In accordance with (7), (9), (10)

$$\Sigma_C = \sum_{\substack{l\geqslant x^{1/2}(\log x)^c\\ x\geqslant lm = p^*-c_1\equiv c_0 \pmod\Delta}} \chi(l) = \sum_{\substack{m\leqslant x^{1/2}(\log x)^{-c}\\ c_1\text{adm.}\bmod m}} \sum_{\substack{x^{1/2}(\log x)^c\leqslant l\leqslant x/m\\ p^*-c_1=lm\equiv c_0\pmod\Delta}} \chi(l). \tag{26}$$

For any fixed m satisfying the condition under the first sum on the right in (26) we consider separately the set of numbers $l = l'$ with $\chi(l') = 1$ and the set $l = l''$ with $\chi(l'') = -1$. The first set contains one half of the reduced classes mod Δ and the second set the other half. Let the corresponding classes be represented by $l_1', \ldots, l_\nu'$ and $l_1'', \ldots, l_\nu''$ $(\nu = \varphi(\Delta)/2)$, respectively. The primes p^* with $p^*-c_1 = lm$ corresponding to l_j' are

$$p^* = c_1 + m(l_j' + t\Delta) \equiv c_1 + ml_j' \pmod{m\Delta}$$

(t integer). We shall first prove that for any $j = 1, 2, \ldots, \varphi(\Delta)/2$ the system of congruences

$$p^* \equiv c_1 + ml_j' \pmod{m\Delta}, \quad p^* \equiv c_1 + c_0 \pmod\Delta, \quad ml_j' \equiv c_0 \pmod\Delta \tag{27}$$

is compatible and has the solution

$$p^* \equiv a_j' \pmod{m\Delta} \tag{28}$$

with $a_j' = c_1 + ml_j'$, admissible mod $m\Delta$.

Since $lm \equiv c_0 \pmod\Delta$ and $(c_0, \Delta) = 1$ (see (3)), it follows that $(m, \Delta) = 1$. Therefore the first congruence (27) (which will be denoted by (27_1) etc.) can be replaced by two congruences of modulus m and Δ, respectively; the latter congruence may be dropped, being a consequence of (27_2). The remaining system

$$p^* \equiv c_1 + ml_j' \pmod m, \quad p^* \equiv c_1 + c_0 \pmod\Delta, \quad ml_j' \equiv c_0 \pmod\Delta$$

can be replaced by

$$\begin{cases} p^* \equiv c_1 + ml_j' \pmod m, \\ p^* \equiv c_1 + ml_j' \pmod\Delta. \end{cases} \tag{29}$$

Since $(m, \Delta) = 1$, it remains to prove that taken separately the congruences (29_1) and (29_2) can be satisfied. (29_1) being the same as $p^* \equiv c_1 \pmod m$ can be satisfied, since c_1 is admissible mod m (see (26)). Since $ml_j' \equiv c_0 \pmod\Delta$, the congruence (29_2) is the same as $p^* \equiv c_1 + c_0 \pmod\Delta$. It can be satisfied, since by (4) $c_1 + c_0$ is admissible mod Δ. This completes the proof of (28).

In the same way one can prove that the analogous system of congruences (27) with l_j' replaced by l_j'' is compatible and has a solution $p^* \equiv a_j''$ (mod $m\Delta$) with an admissible a_j'' mod $m\Delta$.

Now by (26) and (28)

$$\Sigma_C = \sum_{\substack{m \leqslant x^{1/2}(\log x)^{-c}\\ c_1 \mathrm{adm.\,mod}\, m}} \sum_{1\leqslant j \leqslant \varphi(\Delta)/2} \Big\{ \sum_{\substack{p^* \equiv a_j'(\mathrm{mod}\, m\Delta)\\ y'_{mj} \leqslant p^* \leqslant x+c_1}} 1 - \sum_{\substack{p^* \equiv a_j''(\mathrm{mod}\, m\Delta)\\ y''_{mj} \leqslant p^* \leqslant x+c_1}} 1 \Big\},$$

$$y'_{mj} = c_1 + ml'_{j0}, \quad y''_{mj} = c_1 + ml''_{j0},$$

where l'_{j0} is the minimal $l \equiv l_j' \pmod{\Delta}$ satisfying $l \geqslant x^{1/2}(\log x)^c = x_0$, say (analogous definition for l''_{j0}). From both terms of the difference in Σ_C subtracting $\{\mathrm{Li}(x+c_1) - \mathrm{Li}\, mx_0\}/h_1\varphi_1(m\Delta)$, using (14) (with $\Delta = 2$) and considering that

$$y''_{mj} - y'_{mj} = m(l''_{j0} - l'_{j0}) \leqslant m, \qquad \sum_{m \leqslant x^{1/2}(\log x)^{-c}} m \leqslant x(\log x)^{-2c},$$

we obtain

(30)
$$\Sigma_C \leqslant \sum_{m \leqslant x^{1/2}(\log x)^{-c}} \{E(x+c_1, m\Delta) + E(mx_0, m\Delta)\} + x(\log x)^{-2c} \leqslant x(\log x)^{-2}.$$

5. The sum Σ_B. In this section the estimation of the sum

$$\Sigma_B = \sum_{\substack{x \geqslant p^* - c_1 = lm \equiv c_0 (\mathrm{mod}\, \Delta)\\ x^{1/2}(\log x)^{-c} < l < x^{1/2}(\log x)^c}} \chi(l)$$

of (9) will be reduced to that of two other sums Σ_E and Σ_D defined by (32). Writing

(31) $$D(m) = \sum_{\substack{l \mid m\\ x^{1/2}(\log x)^{-c} < l < x^{1/2}(\log x)^c}} 1, \quad F(m) = \sum_{\substack{l \mid m\\ x^{1/2}(\log x)^{-c} < l < x^{1/2}(\log x)^c}} \chi(l)$$

we have

$$\Sigma_B = \sum_{\substack{x \geqslant p^* - c_1 \equiv c_0 (\mathrm{mod}\, \Delta)\\ D(p^* - c_1) > 0}} F(p^* - c_1),$$

whence by the inequality of Cauchy–Schwarz

(32)
$$\Sigma_B \leqslant \Big(\sum_{\substack{x \geqslant p^* - c_1 \equiv c_0 (\mathrm{mod}\, \Delta)\\ D(p^* - c_1) > 0}} 1 \Big)^{1/2} \Big(\sum_{x \geqslant p^* - c_1 \equiv c_0 (\mathrm{mod}\, \Delta)} F^2(p^* - c_1) \Big)^{1/2} = (\Sigma_D)^{1/2} (\Sigma_E)^{1/2},$$

say. By the method of Hooley in §§ 6 and 7 we shall prove that

(33) $$\Sigma_E \leqslant x(\log\log x)^7/\log x,$$

(34) $$\Sigma_D \leqslant x(\log x)^{-1.01}$$

whence by (32)

$$\Sigma_B \leqslant x(\log x)^{-1.003}.$$

Hence by (8), (9), (24), (25), (30)

(35) $$\pi(x; \mathfrak{G}) = c_8 x/\log x + O(x(\log x)^{-1.003}),$$

where

$$c_8 = \sum_{c_0} c_4 c_7 / h_1 \varphi_1(\Delta)$$

is generally > 0 with exception of the case mentioned in the theorem.

6. A proof of (34). In order to prove (34) we start with

$$\Sigma_D \leqslant \sum_{\substack{p^* - c_1 \leqslant x\\ D(p^* - c_1) > 0}} 1$$

(cf. (32)) and go on as in [10], p. 104, except that now (L), (M), (P) denote conditions

$$x^{1/2}(\log x)^{-c} < l < x^{1/2}(\log x)^c,$$
$$x^{1/2}(\log x)^{-c-2} < m < x^{1/2}(\log x)^c,$$
$$p^* - c_1 = lm \leqslant x,$$

respectively, and in [10], Lemma 7, the sum is over the interval $y^{1/2}(\log x)^{-c-2} < m < y^{1/2}(\log x)^c$. For a proof of [10], Lemma 5, see [14], p. 50, Satz 4.6.

7. A proof of (33). We start the proof of (33) by introducing the number

(36) $$x_1 = x^{1/(\log\log x)^2}$$

and writing

$$t^{(1)} = \prod_{p \mid t,\, p \leqslant x_1} p^a$$

for any t with the canonical representation $t = \prod_{p \mid t} p^a$. Further we introduce a non-negative arithmetical function $f(n) = f_x(n)$ such that $f(p) = 1$ for any prime p (see [10], p. 96). By (32), (31)

$$\Sigma_E = \sum_{x \geqslant p^* - c_1 \equiv c_0 (\mathrm{mod}\, \Delta)} F^2(p^* - c_1) \leqslant \sum_{\substack{n \leqslant x + c_1\\ n \equiv c_1 + c_0 (\mathrm{mod}\, \Delta)}} F^2(n - c_1) f(n)$$
$$= \sum_{\substack{x \geqslant l_1' m_1 = l_2' m_2 = n - c_1 \equiv c_0 (\mathrm{mod}\, \Delta)\\ x^{1/2}(\log x)^{-c} < l_1', l_2' < x^{1/2}(\log x)^c}} \chi(l_1') \chi(l_2') f(n).$$

For fixed l_1', l_2' the number $n-c_1$ is divisible by the least common multiple $[l_1', l_2']$. Writing $(l_1', l_2') = d$, $l_1' = dl_1$, $l_2' = dl_2$ we have $(l_1, l_2) = 1$ and $[l_1', l_2'] = dl_1l_2$. We can take for granted that $(dl_1l_2, \Delta) = 1$ (since otherwise $\chi(l_1')\chi(l_2') = 0$) in which case the system of congruences $\{n \equiv c_1 (\mathrm{mod}\ dl_1l_2),\ n \equiv c_1+c_0 (\mathrm{mod}\ \Delta)\}$ is satisfied by a single class $c_6 (\mathrm{mod}\ dl_1l_2\Delta)$. Using the conditions

$$(L_i)\ \frac{x^{1/2}}{d(\log x)^c} < l_i < \frac{x^{1/2}(\log x)^c}{d};\quad (H)\ (l_1, l_2) = 1;\quad (K)\ (\Delta dl_1l_2, c_6^{(1)}) = 1$$

we can write

$$(37)\quad \Sigma_E \ll \sum_{\substack{l_1l_2dm = n-c_1 \equiv c_0 (\mathrm{mod}\ \Delta)\\ (L_1)(L_2)(H)}} \chi(d^2l_1l_2)f(n) = \sum_{d \geqslant x^{1/8}} + \sum_{d < x^{1/8}} = \Sigma_1 + \Sigma_2,$$

say. Since in Σ_2 we have $l_1l_2d < x(\log x)^{2c}/d$, by [10], Lemma 4,

$$(38)\quad \Sigma_1 = \sum_{(L_1)(L_2)(H)} \chi(d^2l_1l_2) \sum_{\substack{n \leqslant x+c_1\\ n \equiv c_1 (\mathrm{mod}\ dl_1l_2)\\ n \equiv c_1+c_0 (\mathrm{mod}\ \Delta)}} f(n) \ll (x+c_1)B_x\{\Sigma_3+\Sigma_4\} + x/\log^2 x,$$

where

$$(39)\quad B_x \ll (\log\log x)^2/\log x,$$

$$\Sigma_3 = \sum_{\substack{(L_1)(L_2)(H)(K)\\ x^{1/8} \leqslant d \leqslant x^{1/2}(\log x)^{-c}}} \frac{\chi(d^2l_1l_2)}{\varphi(\Delta dl_1l_2)},\qquad \Sigma_4 = \sum_{\substack{(L_1)(L_2)(H)(K)\\ x^{1/2}(\log x)^{-c} < d < x^{1/2}(\log x)^c}} \frac{\chi(d^2l_1l_2)}{\varphi(\Delta dl_1l_2)}.$$

Using [10], Lemma 8, and a generalization of [10], Lemma 9 (with the interval of summation $u/d < l < u(\log x)^c/d$) one can prove that $\Sigma_3 \ll \ll (\log\log x)^5$, whence by (38), (39) (since evidently $\Sigma_4 \ll (\log\log x)^4$)

$$(40)\quad \Sigma_1 \ll x(\log\log x)^7/\log x.$$

By (37)

$$\Sigma_2 = \sum_{\substack{l_1l_2dm = n-c_1 \equiv c_0 (\mathrm{mod}\ \Delta)\\ (L_1)(L_2)(H), d < x^{1/8}}} \chi(d^2l_1l_2)f(n).$$

Considering that ([12], Satz 35)

$$\sum_{\substack{rt = l_1\\ st = l_2}} \mu(t) = \begin{cases} 1 & \text{if}\quad (l_1, l_2) = 1,\\ 0 & \text{otherwise}\end{cases}$$

we can write

$$(41)\quad \Sigma_2 = \sum_{x \geqslant rst^2dm = n-c_1 \equiv c_0 (\mathrm{mod}\ \Delta)} \mu(t)\chi(t^2d^2rs)f(n) = \sum_{t < x^{1/8}} + \sum_{\geqslant x^{1/8}} = \Sigma_5 + \Sigma_6,$$

say. Since in Σ_5

$$rt^2dm \leqslant \frac{x}{s} < \frac{x}{x^{1/2}(\log x)^{-c}d^{-1}t^{-1}} = x^{1/2}(\log x)^c dt < x^{3/4}(\log x)^c,$$

using the conditions

$$(R)\ \left\{\frac{x^{1/2}}{dt(\log x)^c} < r < \frac{x^{1/2}(\log x)^c}{dt}\right\},$$

$$(S)\ \left\{\frac{x^{1/2}}{dt(\log x)^c} < s < \frac{x^{1/2}(\log x)^c}{dt}\right\},\qquad (DT)\ \{d < x^{1/8}, t < x^{1/8}\}$$

we have

$$(42)\quad \Sigma_5 = \sum_{rt^2dm < x^{3/4}(\log x)^c} \mu(t)\chi(t^2d^2r) \sum_{x \geqslant n-c_1 = rst^2dm \equiv c_0 (\mathrm{mod}\ \Delta)} \chi(s)f(n)$$
$$\ll \sum_{\substack{rt^2dm < x^{3/4}(\log x)^c\\ (R)(DT)}} \Bigg| \sum_{\substack{n-c_1 = rt^2dms \equiv c_0 (\mathrm{mod}\ \Delta)\\ (S), y_1 < n < y_2}} \chi(s)f(n)\Bigg|,$$

where $1 \ll y_1$, $y_2 = x+c_1$. We split the inner sum into parts corresponding to pairs of classes $s', s'' (\mathrm{mod}\ \Delta)$ with $\chi(s') = 1$, $\chi(s'') = -1$, and for each class separately we shall use [10], Lemma 4, the corresponding numbers ν being

$$(43)\quad \begin{aligned} \nu &\equiv a_1 = c_1 + rt^2dms' (\mathrm{mod}\ rt^2dm\Delta),\\ \nu &\equiv a_2 = c_1 + rt^2dms'' (\mathrm{mod}\ rt^2dm\Delta).\end{aligned}$$

Yet we have first to prove that if one of the numbers

$$\delta_1 = \left(c_1 + rt^2dms', (rt^2dm\Delta)^{(1)}\right),\qquad \delta_2 = \left(c_1 + rt^2dms'', (rt^2dm\Delta)^{(1)}\right)$$

is > 1, so is the other.

Let p_1 be a prime $\leqslant x_1$ (see (36)) such that $p_1 | c_1 + rt^2dms'$ and $p_1 | rt^2dm\Delta$. Then either (i) $p_1 | rt^2dm$ or (ii) $p_1 | \Delta$ (or both). In the first case $p_1 | c_1$ and thus $\delta_1 > 1$ implies $\delta_2 > 1$ and *vice versa*. In the second case consider that (see (42)) $rt^2dms \equiv c_0 (\mathrm{mod}\ \Delta)$, whence $c_1 + rt^2dms' \equiv c_1 + +c_0 (\mathrm{mod}\ \Delta)$. Since $p_1 | \Delta$ and $p_1 | c_1 + rt^2dms'$, it follows that $p_1 | c_1 + c_0$ and $p_1 | \Delta$, a contradiction to (4).

Now by [10], Lemma 4, the part of the last sum on the right in (42) for any of the pairs of numbers (43) is

$$\frac{y_2-y_1}{\varphi(rt^2dm\Delta)}B_x - \frac{y_2-y_1}{\varphi(rt^2dm\Delta)}B_x + O\left(\frac{x}{rt^2dm|\Delta|\log^5 x}\right) \ll \frac{x}{rt^2dm(\log x)^5},$$

whence by (42)

$$\Sigma_5 \ll \frac{x}{(\log x)^5} \sum_{r,d,m,t^2} \frac{1}{rdmt^2} \ll \frac{x}{\log^2 x}.$$

Σ_6 satisfies the same estimate (see [10], (62)) and so does Σ_2, by (41). Hence (33) follows from (40), (37).

8. Proof of the theorem. We shall use (35) with $c_8 > 0$, the exceptional case $c_8 = 0$ being excluded. In what follows let

$$K_0 = [\varepsilon_0 \log\log x],$$

where ε_0 stands for the least positive solution of the equation

(44) $$1/h - 2\varepsilon\log 2 - \varepsilon + \varepsilon\log\varepsilon = 0,$$

h being the number of the classes $\mathfrak{K}_i$ of the field K. We split the sum (6) into parts

(45) $$\pi(x; \mathfrak{G}) = \Sigma_H + \Sigma_F,$$

where each $\mathfrak{a}$ of Σ_H is a product of at least K_0 prime ideals $\mathfrak{p} \in \mathfrak{K}_i$ (for every $i = 1, 2, \ldots, h$; $\mathfrak{p}^2 \nmid \mathfrak{a}$) and Σ_F is the remaining part.

Let F_i $(1 \leqslant i \leqslant h)$ denote the set of natural numbers m having less than K_0 prime divisors $p_i | m$ such that $\chi(p_i) = 1$, $p_i = \mathfrak{p}_i\mathfrak{p}_i'$, $\mathfrak{p}_i \in \mathfrak{K}_i$. Write

$$A(m) = \sum_{\substack{\mathfrak{a} \\ N\mathfrak{a} = m}} 1, \quad \Sigma_{F_i} = \sum_{\substack{m = p^* - c_1 \leqslant x \\ m \in F_i}} A(m).$$

Then

$$\Sigma_F \leqslant h \cdot \max_{1 \leqslant i \leqslant h} \Sigma_{F_i}.$$

Arguing as in Bredihin–Linnik [3], pp. 154–157 (with $p^* - c_1 = m$ instead of $p + m = n$ and x instead of n) we can prove that

(46) $$\Sigma_F \ll \frac{x(\log\log x)^4 (\log x)^{\varepsilon_0 \log 2e - \varepsilon_0\log\varepsilon_0}}{(\log x)^{1+1/h}} = \frac{x(\log\log x)^4}{(\log x)^{1+\varepsilon_0\log 2}} \leqslant \frac{x}{(\log x)^{1+\delta_0}}$$

for any $\delta_0 < \varepsilon_0 \log 2$. Hence by (45)

(47) $$\pi(x; \mathfrak{G}) = \Sigma_H + O\big(x(\log x)^{-1-\delta_0}\big).$$

Let $F_{\mathfrak{K}}(m)$ be the number of solutions of the equation

(48) $$N\mathfrak{a} = m \quad (m \leqslant x)$$

with the restriction $\mathfrak{a} \in \mathfrak{K}$ $(\mathfrak{K} \in \mathfrak{G})$ and let $F_{\mathfrak{G}}(m)$ denote the number of solutions of (48) when $\mathfrak{a}$ runs through all the classes $\mathfrak{K} \in \mathfrak{G}$ (t_0 in number).

Writing $m \in H$ if $m = N\mathfrak{a}$ with $\mathfrak{a}$ satisfying the restriction imposed on Σ_H, we have by [3], Lemma 5, for $m \in H$

(49) $$F_{\mathfrak{K}}(m) = t_0^{-1} F_{\mathfrak{G}}(m)\{1 + O(\log^{-\delta} x)\}, \quad \delta = \varepsilon_0 \log 2.$$

Summing (49) over the numbers $m = p^* - c_1 \in H$, $m \leqslant x$ we get

$$\Sigma_H = t_0 \sum_{x \geqslant m = p^* - c_1 \in H} F_{\mathfrak{K}}(m)\{1 + O(\log^{-\delta} x)\},$$

whence by (47), (35)

$$t_0 \sum_{x \geqslant m = p^* - c_1 \in H} F_{\mathfrak{K}}(m) = c_8 \frac{x}{\log x} + O\left(\frac{x}{(\log x)^{1+\delta_0}}\right) + O\left(\frac{x}{(\log x)^{1.003}}\right).$$

Now using (46) we get

$$\sum_{p^* - c_1 \leqslant x} F_{\mathfrak{K}}(p^* - c_1) = c_2 x/\log x + O\big(x(\log x)^{-1-\delta_1}\big),$$

where

(50) $$c_2 = c_8/t_0, \quad \delta_1 = \min(\delta_0, 3\cdot 10^{-3}).$$

This completes the proof of the theorem.

Appendix

9. In this section we shall prove some properties of the function $\varphi_1(q)$ denoting the number of normresidues $a \bmod q$ with $(a, q) = 1$ for a given class $\mathfrak{K}_1$ of ideals in the quadratic field K' of discriminant d. Instead of the class of ideals we shall deal with a quadratic form and solve the question in a more general setting.

Given a primitive binary quadratic form $F(u, v) = Au^2 + Buv + Cv^2$ (or a class $\mathfrak{C}$ of forms with $F \in \mathfrak{C}$), we call a rational integer n *admissible* mod q if $(n, q) = 1$ and if there are rational integers u, v such that $F(u, v) \equiv n \pmod q$. In what follows we denote the number of admissible numbers (in a set of residues mod q) by $\varphi_1(q) = \varphi_1(q, \mathfrak{C})$. If in particular the form F represents the norms in question (cf. [7], § 3), we get the desired results.

LEMMA 1. *Let $F(u, v) = Au^2 + Buv + Cv^2$ be a primitive form and let q be any natural integer. Then F represents some integer n such that $(n, q) = 1$.*

For the proof see e.g. [5], Satz 66.

LEMMA 2. *Suppose that $q = q_1 q_2$, $(q_1, q_2) = 1$ and n is admissible* mod q_1 *and admissible* mod q_2. *Then n is admissible* mod q *and conversely.*

Proof. By the premises of the lemma we have $(n, q_1) = 1$, $(n, q_2) = 1$ and $F(u_1, v_1) \equiv n \pmod{q_1}$, $F(u_2, v_2) \equiv n \pmod{q_2}$ for appropriate integers u_1, v_1, u_2, v_2. Hence $(n, q_1q_2) = 1$ and for all u, v satisfying

$$\begin{cases} u \equiv u_1 \pmod{q_1}, \\ u \equiv u_2 \pmod{q_2}; \end{cases} \quad \begin{cases} v \equiv v_1 \pmod{q_1}, \\ v \equiv v_2 \pmod{q_2} \end{cases}$$

we have $F(u, v) \equiv n \pmod{q_1q_2}$. If on the contrary $F(u_0, v_0) \equiv n \pmod{q}$, $(n, q) = 1$, $q = q_1q_2$, then evidently $F(u_0, v_0) \equiv n \pmod{q_1}$, $F(u_0, v_0) \equiv n \pmod{q_2}$, $(n, q_1) = 1$, $(n, q_2) = 1$, whence the lemma.

LEMMA 3. *Suppose that $F(u, v) = Au^2+Buv+Cv^2$ is a primitive form of discriminant $D = B^2-4AC$. Let (for any integer $q \geqslant 1$) $\varphi(q)$ be the number of reduced classes* mod q *and $\varphi_1(q)$ denote the number of reduced classes $a \pmod{q}$ such that $F(u, v) \equiv a \pmod{q}$ has a solution. Then*

$$\varphi_1(q_1q_2) = \varphi_1(q_1)\varphi_1(q_2) \quad \textit{if} \quad (q_1, q_2) = 1; \tag{51}$$

$$\varphi_1(q) = \varphi(q) \quad \textit{if} \quad (D, q) = 1; \tag{52}$$

$$\varphi_1(1) = \varphi_1(2) = 1; \tag{53}$$

$$\varphi_1(p^k) = \tfrac{1}{2}\varphi(p^k) \quad \textit{for } k \geqslant 1 \textit{ and any odd prime } p \textit{ dividing } D; \tag{54}$$

$$\varphi_1(4) = \begin{cases} 1 & \textit{if} \quad D \equiv 12 \pmod{16}, \\ 2 & \textit{if} \quad D \equiv 8 \pmod{16}; \end{cases} \tag{55}$$

$$\varphi_1(2^k) = 2^{k-2} \quad \textit{if } k \geqslant 3 \textit{ and } D \textit{ is an even fundamental discriminant } (D = d). \tag{56}$$

From Lemma 3 follows the inequality $\varphi_1(q) \gg \varphi(q)$ which was used in [9] without a proper reference.

Proof. Let a_i and b_j run through the sets of all incongruent and admissible numbers mod q_1 and mod q_2, respectively. Solving all systems of congruences

$$\begin{cases} r \equiv a_i \pmod{q_1}, & 1 \leqslant i \leqslant \varphi_1(q_1), \\ r \equiv b_j \pmod{q_2}, & 1 \leqslant j \leqslant \varphi_1(q_2) \end{cases} \tag{57}$$

(compatible, since $(q_1, q_2) = 1$) we get a set of $\varphi_1(q_1)\varphi_1(q_2)$ numbers r:

$$r_1, r_2, \ldots, r_N; \quad N = \varphi_1(q_1)\varphi_1(q_2). \tag{58}$$

By Lemma 2 all the numbers (57) are admissible mod q_1q_2. And evidently any two of them are incongruent mod q_1q_2.

If a_0 is any admissible number mod q_1q_2, then a_0 is also admissible mod q_1 and admissible mod q_2, whence for appropriate i_0, j_0 $(1 \leqslant i_0 \leqslant \varphi_1(q_1)$, $1 \leqslant j_0 \leqslant \varphi_1(q_2))$ $a_0 \equiv a_{i_0} \pmod{q_1}$ and $a_0 \equiv b_{j_0} \pmod{q_2}$. Hence a_0 is congruent mod q_1q_2 to some of the numbers (58), whence (51) follows.

For a proof of (52) see [8], § 23.

By the definition of $\varphi_1(q)$ we have $1 \leqslant \varphi_1(q) \leqslant \varphi(q)$, whence (53) follows (since $\varphi(1) = \varphi(2) = 1$).

10. In proving (54) we may suppose that $p \nmid A$ (otherwise use Lemma 1 and replace F by appropriate equivalent form). From

$$4AF(u, v) = (2Au+Bv)^2-Dv^2, \qquad D = B^2-4AC \tag{59}$$

we deduce that $4AF(u, v) \equiv (2Au+Bv)^2 \pmod{p}$. Hence we see that the admissible numbers mod p are quadratic residues, if A is quadratic residue, and otherwise they are all quadratic nonresidues.

Supposing A a quadratic residue mod p let us prove that for any of the $\frac{1}{2}(p-1)$ quadratic residues $l \pmod{p}$ there are integers u, v such that

$$F(u, v) \equiv l \pmod{p}. \tag{60}$$

A and l being quadratic residues we can find an integer n such that

$$4Al \equiv n^2 \pmod{p}. \tag{61}$$

Now let u, v be a pair of integers satisfying $2Au+Bv \equiv n \pmod{p}$ (one can take for example $v = 0$, $u \equiv n/2A \pmod{p}$). Then by (61) and (59)

$$\left.\begin{aligned} 4Al &\equiv (2Au+Bv)^2 \\ 4AF(u, v) &\equiv (2Au+Bv)^2 \end{aligned}\right\} \pmod{p},$$

whence (60) follows.

By the same argument one can prove that in the case of a quadratic nonresidue A for any of the $\frac{1}{2}(p-1)$ quadratic nonresidues l there are integers u, v satisfying (60). This proves (54) for $k = 1$.

Let us suppose that (54) holds for some fixed $k \geqslant 1$ and a is admissible mod p^{k+1}. Then a is also admissible mod p^k whence $a \equiv l_0 \pmod{p^k}$, where l_0 stands for one of the $\varphi_1(p^k)$ admissible numbers mod p^k. It remains to prove that for any l_0 all the numbers l_0+yp^k (with y runing through the set of all residues mod p) are admissible mod p^{k+1}. From this it would follow that $\varphi_1(p^{k+1}) = p\cdot\varphi_1(p^k) = p\cdot\frac{1}{2}\varphi(p^k) = \frac{1}{2}\varphi(p^{k+1})$ and the truth of (54) would be established for the exponent $k+1$.

By the definition of l_0 there are integers u_0, v_0 such that

$$F(u_0, v_0) \equiv l_0 \pmod{p^k} \tag{62}$$

which is the same thing as

$$F(u_0, v_0) = l_0+p^ky_0. \tag{63}$$

Let us write $u = u_0+p^kt$, where t stands for a variable integer. By the Taylor expansion

$$F(u, v_0) = F(u_0, v_0)+p^ktb+cp^{2k}, \tag{64}$$

where b and c are integers,

$$b = \left(\frac{\partial F}{\partial u}\right)_{u=u_0,\, v=v_0} = 2Au_0+Bv_0.$$

Since $p\nmid l_0$, from (62) and (59) (where $p\nmid 4A, p\mid D$) we deduce that $b\not\equiv 0 \pmod p$. Hence, if t runs through the set of all residues mod p, so does bt. Now by (63) and (64)

$$F(u_0+p^k t, v_0) \equiv l_0+p^k(y_0+bt) \pmod{p^{k+1}}$$

and the desired result follows.

11. In order to prove (55) consider that by (59)

(65) $$A\cdot F(u,v) = (Au+\tfrac{1}{2}Bv)^2-D_1v^2,$$

where

$$D_1 = D/4 \equiv 2 \text{ or } 3 \pmod 4,$$

$2\mid B$, and we may suppose that $2\nmid A$. In (65) we shall use merely such values of u and v for which the right hand side U (say) is an odd number (since even U do not furnish admissible numbers mod 2^k). Supposing v odd we have

$$\pmod 4 \quad U \equiv \begin{cases}1\\3\end{cases} \text{if} \quad (Au+\tfrac{1}{2}Bv)^2 \equiv \begin{matrix}0\\1\end{matrix} \quad \text{and} \quad D_1 \equiv \begin{matrix}3\\2\end{matrix}.$$

If v is even, then $U\equiv A^2u^2\equiv 1 \pmod 4$. This proves (55).

Passing to the computation of $\varphi_1(8)$ let us write

(66) $$U = E^2-D_1v^2, \quad \text{where} \quad E = Au+\tfrac{1}{2}Bv,\ D_1 = D/4.$$

Suppose first v odd and thus $v^2\equiv 1 \pmod 8$. We have

(67) $$D_1 \equiv 2,\ 6 \text{ or } 3,\ 7 \pmod 8.$$

In the first two cases (67) we have in (66) an odd U merely for $E^2\equiv 1 \pmod 8$; in the remaining cases U is odd for $E^2\equiv 4$ or $0 \pmod 8$. The corresponding values of U are

$$\pmod 8 \quad U \equiv 7,\ 3,\ \begin{cases}1,\ 5 & \text{if} \quad E^2\equiv 4,\\ 5,\ 1 & \text{if} \quad E^2\equiv 0.\end{cases}$$

Now suppose v even and thus $v^2\equiv 4$ or $0 \pmod 8$. Then we have an odd U in (66) merely for an odd $E^2\equiv 1 \pmod 8$. The values of U corresponding to the numbers (67) are as follows:

$$\pmod 8 \quad U \equiv \begin{cases}1,\ 1,\ 1,\ 1 & \text{if} \quad v^2\equiv 0,\\ 1,\ 1,\ 5,\ 5 & \text{if} \quad v^2\equiv 4.\end{cases}$$

This proves that $\varphi_1(8) = 2$.

In order to compute $\varphi_1(2^k)$ for $k\geqslant 4$ consider that an admissible number mod 2^k is also admissible mod 2^{k-1} and from any of the two congruences

$$U\equiv n \pmod{2^k} \quad \text{and} \quad U\equiv n+2^{k-1} \pmod{2^k}$$

it follows $U\equiv n \pmod{2^{k-1}}$. Therefore

(68) $$\varphi_1(2^k)\leqslant 2\cdot\varphi_1(2^{k-1}).$$

Let us suppose that for some fixed $k\geqslant 4$

(69) $$\varphi_1(2^{k-1}) = 2^{k-3}.$$

Then by (68) $\varphi_1(2^k)\leqslant 2^{k-2}$ whence (56) would follow if we could find a set of 2^{k-2} numbers U, incongruent and admissible mod 2^k.

The numbers $a\equiv 1 \pmod 4$ of the reduced system of residues mod 2^k are representable as the powers 5^b, $b = 1, 2, \ldots, 2^{k-2}$ and the remaining numbers $\equiv 3 \pmod 4$ are representable as -5^b ([12], I, Satz 126). These representations being unique there are 2^{k-3} odd quadratic residues mod 2^k, viz. the numbers $\equiv 5^b$ with $b = 2, 4, \ldots, 2^{k-2}$. In another arrangement they are the numbers

(70) $$q\equiv 1 \pmod 8.$$

Using in (66) $v = 0$ we get these 2^{k-3} numbers (70) as values of U. It remains to prove that there are at least as many incongruent (mod 2^k) other values of U.

If $D_1\equiv 2 \pmod 4$, then using in (65) $v^2 = 1$ we get 2^{k-3} odd values of $U\equiv q-D_1 \pmod{2^k}$. Not being congruent neither among themselves nor to any of the numbers (70) (since otherwise would follow $0\equiv -D_1 \pmod 8$) they furnish the set of numbers U we need.

If $D_1\equiv 3 \pmod 4$, then using $v^2 = 4$ we get 2^{k-3} numbers $U\equiv q-4D_1 \pmod{2^k}$ and argue as before.

By this we have proved (56). From the proof follows that if $k\geqslant 4$ and n runs through a set of all admissible numbers mod 2^{k-1}, then so does $n+2^{k-1}$. Any admissible number mod 2^k is either in the first or in the second set (since the set theoretical sum of both sets contain 2^{k-2} numbers, incongruent mod 2^k).

12. LEMMA 4. *Suppose that p is an odd prime, $F(u,v) = Au^2+Buv+Cv^2$ is a primitive form with the discriminant $D = B^2-4AC$, and the integer c_1 is admissible* mod p *with respect to F. Then for any $k = 1, 2, \ldots$ there are integers u, v such that $F(u,v)-c_1$ is divisible by p^k.*

Proof. Being admissible mod p the integer c_1 is not divisible by p. Hence if $p\nmid D$, then the result follows from [8], § 23 with $q = p^k$. If $p\mid D$, then arguing as in the proof of (54) we prove that c_1 is also admissible mod p^k, $k = 2, 3, \ldots$

If c_1 and the discriminant D of $F(u,v)$ are odd numbers, then by [8], § 23 with $q = 2^k$ for any $k = 1, 2, \ldots$ there are integers u, v such that $2^k | F(u,v) - c_1$. This may not be true for an even D.

LEMMA 5. *Let $F(u,v) = Au^2 + Buv + Cv^2$ (A odd) be a primitive form with the discriminant $D = 4D_1$, $D_1 \equiv 2 \pmod 4$. Let further c_1 be an odd number and $k \geqslant 3$. Then for the existence of integers u, v with $2^k | F(u,v) - c_1$ we have the necessary and sufficient condition*

$$(71) \qquad \pmod 8 \; Ac_1 \equiv \begin{cases} 1,\ 7, & \textit{if} \quad D_1 \equiv 2, \\ 1,\ 3, & \textit{if} \quad D_1 \equiv 6. \end{cases}$$

Proof. Since by (56) $\varphi_1(2^k) = \varphi(2^k)/2$, the congruence

$$(72) \qquad F(u,v) \equiv c_1 \pmod{2^k}$$

has a solution merely for one half of the odd numbers constituting the reduced system of residues mod 2^k. Since (72) is equivalent to

$$E^2 - D_1 v^2 \equiv Ac_1 \pmod{2^k}, \qquad E = Au + \tfrac{1}{2}Bv$$

(see (65)), from § 11 (the proof of $\varphi_1(8) = 2$) the lemma follows for $k = 3$.

Suppose $Ac_1 \equiv a \pmod{2^4}$ (where a runs through $\varphi_1(2^4) = 4$ incongruent numbers) is the necessary and sufficient condition for the existence of u, v such that $2^4 | F(u,v) - c_1$. Comparing with the condition for $k = 3$ we deduce (cf. the remark at the end of § 11) that

$$a \equiv \begin{cases} 1,\ 7; \quad 1+2^3,\ 7+2^3 \pmod{2^4}, & \text{if} \quad D_1 \equiv 2 \pmod 8, \\ 1,\ 3; \quad 1+2^3,\ 3+2^3 \pmod{2^4}, & \text{if} \quad D_1 \equiv 6 \pmod 8. \end{cases}$$

This proves (71) for $k = 4$. Proceeding in the same manner we prove the lemma for any $k > 4$.

LEMMA 6. *Let $F(u,v) = Au^2 + Buv + Cv^2$ (A odd) be a primitive form with the discriminant $D = 4D_1$, $D_1 \equiv 3 \pmod 4$. Let further c_1 be an odd number and $k \geqslant 2$. Then $Ac_1 \equiv 1 \pmod 4$ is the necessary and sufficient condition for the existence of integers u, v such that $2^k | F(u,v) - c_1$.*

The proof is similar to that of the previous lemma. If $k = 2$, from $E^2 - D_1 v^2 \equiv Ac_1 \pmod 4$ we get $Ac_1 \equiv 1 \pmod 4$ (cf. the proof of (55)), whence for $k = 3$ we get (cf. the proof of $\varphi_1(8) = 2$) $Ac_1 \equiv 1, 1+4 \pmod 8$, etc.

LEMMA 7. *Let $F(u,v) = Au^2 + Buv + Cv^2$ (A odd) be a primitive form with the discriminant $D = 4D_1$, $D_1 \equiv 3 \pmod 4$ and let $Ac_1 \equiv 3 \pmod 4$. Then there are integers u, v such that $2 | F(u,v) - c_1$.*

(By Lemma 6 there are no integers u, v with $4 | F(u,v) - c_1$.)

Proof. By (55) we have $\varphi_1(4) = 1 = \frac{1}{2}\varphi(4)$. If $F(u,v) - c_1$ is divisible by 2 but not by 4, then

$$(73) \qquad F(u,v) \equiv c_1 + 2 \pmod 4,$$

whence $c_1 + 2$ is admissible mod 4. (73) being equivalent to $E^2 - D_1 v^2 \equiv A(c_1+2) \pmod 4$, which is the same thing as $E^2 + v^2 \equiv Ac_1 + 2 \pmod 4$, we deduce that $Ac_1 \equiv 3 \pmod 4$. If this condition is satisfied we can get values of v, E (or u, v) satisfying the previous congruence and also (73).

13. In this section let $c_1, \Delta_1, \Delta, \mathfrak{K}_1$ and $\varphi_1(q)$ have the meaning as explained in §§ 1, 3.

LEMMA 8. *Let $\chi(n)$ be the Kronecker symbol (Δ/n) and let q run through all natural numbers including 1 such that any $q > 1$ is divisible merely by primes dividing Δ_1 and c_1 is admissible mod q with respect to $F(u,v)$, representing idealnorms of the class $\mathfrak{K}_1$. Writing*

$$(74) \qquad \sum_{\substack{1 \leqslant q < \infty \\ c_1 \text{ adm. mod } q}} \frac{\chi(q)}{\varphi_1(q)} = c_7$$

we have $c_7 > 0$ apart from the exceptional case when $-c_1$ is an odd number $\equiv N\mathfrak{a}_1 \pmod 4$ for appropriate $\mathfrak{a}_1 \in \mathfrak{K}_1$ and $\Delta_1 \equiv 12 \pmod{16}$, $\Delta \equiv 5 \pmod 8$, in which case $c_7 = 0$.

Proof. Let us consider that if c_1 is admissible mod q, then c_1 is also admissible mod q_1 for any q_1 dividing q. Using Lemma 4 (with $F(u,v)$ representing idealnorms of the class $\mathfrak{K}_1$) we deduce that q is divisible by any power of any odd prime p_1 dividing Δ_1, provided c_1 admissible mod p_1. In the case of an even Δ_1 the same is true for the powers 2^k if c_1 satisfies the restrictions stated in Lemmas 5 and 6 where $k \geqslant 3$ or $k \geqslant 2$, respectively; simultaneously it is true also for lower powers of 2 (see the beginning of this proof). In the case of Lemma 7 there are even numbers q, but no q divisible by 4. Therefore using (51) we can represent (74) as the product

$$(75) \qquad \sum_{\substack{1 \leqslant q < \infty \\ c_1 \text{ adm. mod } q}} \frac{\chi(q)}{\varphi_1(q)} = f_2 \cdot \prod_{\substack{p_1 > 2 \\ p_1 | \Delta_1, p_1 \nmid c_1 \\ c_1 \text{ adm. mod } p_1}} \left\{1 + \frac{\chi(p_1)}{\varphi_1(p_1)} + \frac{\chi(p_1^2)}{\varphi_1(p_1^2)} + \ldots\right\},$$

where

$$(76) \qquad f_2 = \begin{cases} 1, \quad \text{if} \quad 2 \nmid \Delta_1, \\ 1 + \chi(2), \quad \text{if} \quad Ac_1 \equiv 3 \pmod 4,\ \Delta_1 \equiv 12 \pmod{16}, \\ 1 + \chi(2) + \chi(4) + \chi(8)/2 + \chi(16)/4 + \ldots, \\ \qquad\qquad \text{if} \quad Ac_1 \equiv 1 \pmod 4,\ \Delta_1 \equiv 12 \pmod{16}, \\ 1 + \chi(2) + \chi(4)/2 + \chi(8)/2 + \chi(16)/4 + \ldots, \quad \text{if} \quad Ac_1 \equiv 1, 7 \pmod 8, \\ \qquad \Delta_1 \equiv 8 \pmod{32} \ \text{or if} \ Ac_1 \equiv 1, 3 \pmod 8,\ \Delta_1 \equiv 24 \pmod{32}. \end{cases}$$

From (74), (75), (76) it follows that generally $c_7 > 0$, except merely the case with $\chi(2) = -1$ (whence $\Delta \equiv 5 \pmod 8$; see [12], I, p. 51), $\Delta_1 \equiv 12 \pmod{16}$ and $\Delta c_1 \equiv 3 \pmod 4$, in which case $f_2 = 0$ and simultaneously $c_7 = 0$. In this exceptional case $\varphi_1(4) = 1$, by (55). Therefore we have either $\Delta \equiv 1 \pmod 4$ (whence $c_1 \equiv 3$, $-c_1 \equiv \Delta$) or $\Delta \equiv 3 \pmod 4$ (whence $c_1 \equiv 1$, $-c_1 \equiv \Delta$). In both cases $-c_1$ is an odd number congruent mod 4 to a norm of some ideal of the class $\mathfrak{K}_1$. This completes the proof of the lemma.

References

[1] E. Bombieri, *On the large sieve*, Mathematika 12 (1965), pp. 201–225.
[2] З. И. Боревич, И. Р. Шафаревич, *Теория чисел*, Москва 1964.
[3] Б. М. Бредихин, Ю. В. Линник, *Асимптотика и эргодические свойства решений обобщенного уравнения Гарди-Литтлвуда*, Мат. Сб. 71 (113), № 2 (1966), pp. 145–161.
[4] B. M. Bredihin, N. G. Čudakov, Ju. V. Linnik, *Über binäre additive Probleme gemischter Art*, Abhandlungen aus Zahlentheorie und Analysis (zum Erinnerung an Edmund Landau), Berlin u. New York 1968, pp. 23–37.
[5] L. E. Dickson und E. Bodewig, *Einführung in die Zahlentheorie*, Leipzig u. Berlin 1931.
[6] P. D. T. A. Elliott and H. Halberstam, *Some applications of Bombieri's theorem*, Mathematika 13 (1966), pp. 196–203.
[7] E. Fogels, *On the distribution of prime ideals*, Acta Arith. 7 (1962), pp. 255–269.
[8] — *On the abstract theory of primes III*, Acta Arith. 11 (1966), pp. 293–331.
[9] — *A mean value theorem of Bombieri's type*, Acta Arith. 21 (1972), pp. 137–151.
[10] C. Hooley, *On the representation of a number as the sum of two squares and a prime*, Acta Math. 97 (1957), pp. 189–210.
[11] H. Iwaniec, *Primes of the type $\varphi(x, y) + \Delta$ where φ is a quadratic form*, Acta Arith. 21 (1972), pp. 203–234.
[12] E. Landau, *Vorlesungen über Zahlentheorie I, III*, Leipzig 1927.
[13] Ю. В. Линник, *Дисперсионный метод в бинарных аддитивных задачах*, Ленинград 1961.
[14] K. Prachar, *Primzahlverteilung*, Berlin 1957.
[15] E. C. Titchmarsh, *A divisor problem*, Rend. Circ. Mat. Palermo 54 (1930), pp. 414–429.

Received on 12. 10. 1973 (473)

ACTA ARITHMETICA
XXVII (1975)

The exceptional set in Goldbach's problem

by

H. L. Montgomery (Ann Arbor, Mich.) and R. C. Vaughan (London)

*Dedicated with deepest respect
to the memory of
Academician Yu. V. Linnik*

1. Introduction. Goldbach stated, in a letter to Euler (c. 1742), that every even integer exceeding 2 can be written as a sum of two primes. If we let $E(X)$ denote the number of even numbers not exceeding X which cannot be written as a sum of two primes, then Goldbach's conjecture can be formulated as the assertion that $E(X) = 1$ for $X \geqslant 2$. Goldbach's problem remains unsettled, but Vinogradov's fundamental work ([20], [21]) on three primes inspired others [1], [4], [17] to show that $E(X) = o(X)$, so that almost all even numbers can be expressed as a sum of two primes. Recently Vaughan [18] sharpened the earlier results by showing that

$$E(X) < X\exp(-c\log^{1/2} X).$$

We improve on this by establishing the following theorem.

THEOREM 1. *There is a positive (effectively computable) constant δ such that for all large X*

$$E(X) < X^{1-\delta}.$$

Hardy and Littlewood [6] introduced the approach by which one shows that most even integers are sums of two primes; they showed that if the Generalized Riemann Hypothesis (GRH) is true then one may take $\delta = \frac{1}{2} - \varepsilon$ in the above. We avoid the GRH by appealing to a recent result of Gallagher [5] which reflects considerable knowledge of the distribution of the zeros of L-functions. To indicate the depth of Gallagher's result (our Lemma 4.3), we note that one may easily derive from it the celebrated theorem of Linnik ([9], [10]) concerning the least prime in an arithmetic progression. A recent form of the Linnik–Rényi large sieve, Turán's method, and the Deuring–Heilbronn phenomenon all play essential roles in Gallagher's proof.