AN ELEMENTARY PROOF OF A THEOREM ABOUT THE REPRESENTATION OF PRIMES BY QUADRATIC FORMS

W. E. BRIGGS

1. Introduction. The theorem that *every properly primitive binary quadratic form is capable of representing infinitely many prime numbers* was first proved completely by H. Weber **(5)**. The purpose of this paper is to give an elementary proof of the case where the form is $ax^2 + 2bxy + cy^2$, with $a > 0$, $(a, 2b, c) = 1$, and $D = b^2 - ac$ not a square. The cases where the form is $ax^2 + bxy + cy^2$ with b odd, and the case where the form is $ax^2 + 2bxy + cy^2$ with D a square, can be settled very simply once the first case is taken care of, and this is done in a page and a half in the Weber paper. The proof follows the methods used by Atle Selberg in his elementary proof of Dirichlet's theorem about primes in an arithmetic progression **(3)**.

2. Representation of numbers by quadratic forms. Some basic facts concerning the representation of numbers by binary quadratic forms are now given. The h classes of properly primitive quadratic forms of determinant D can be taken as $\theta_1, \theta_2, \ldots \theta_h$, and in the case of negative determinants only the classes which contain positive definite forms are considered. These classes considered as elements form an Abelian group of order h under Gauss's law of composition.

A positive number m, relatively prime to $2D$, is primitively representable by forms of determinant D, if and only if D is a quadratic residue of m, and to each root n of the congruence $x^2 \equiv D \pmod{m}$ correspond one or more representations of m by each form of the class to which $mx^2+2nxy+[(n^2-D)/m]y^2$ belongs. If p is a prime which does not divide $2D$ and of which D is a quadratic residue, then to each of the two roots of $x^2 \equiv D \pmod{p}$ correspond one or more representations of p by the forms of one or two classes. These two classes are conjugate and can be indicated as θ and θ^{-1}. If the classes are identical, then θ is called ambiguous. The number of representations of such an m by each form of the class to which $mx^2 + 2nxy + [(n^2 - D)/m]y^2$ belongs is equal to the number of integral solutions of $t^2 - Du^2 = 1$. In order that this number not be infinite when $D > 0$, it is required that the x and y in $ax^2 + 2bxy + cy^2$ satisfy the conditions

$$(2.1) \qquad y \geqslant 0,\ x > \frac{T - bU}{aU}\, y = \nu y, \qquad D > 0,$$

Received April 6, 1953; in revised form January 5, 1954. This paper is a portion of a thesis prepared under the direction of Professor B. W. Jones and submitted for a Ph.D. degree at the University of Colorado.

https://doi.org/10.4153/CJM-1954-034-0 Published online by Cambridge University Press

where T, U is the fundamental solution of the Pell equation. In this way there are now w representations of m by each form of the class where

$$\begin{aligned} w &= 1, && D > 0, \\ w &= 4, && D = -1, \\ w &= 2, && D < -1. \end{aligned} \tag{2.2}$$

Defining

$$S_\psi(x) = \sum_{\substack{p \leqslant x \\ p = \psi}} \frac{\log p}{p} \quad \text{and} \quad Q_\psi(x) = \frac{S_\psi(x)}{\log x}, \tag{2.3}$$

where the summation is extended over primes represented by $\psi = ax^2 + 2bxy + cy^2$, the proof will be completed by showing that $Q_\psi(x)$ is greater than a positive constant for $x > x_0$ for any ψ.

3. Several preliminary lemmas.

LEMMA 1. *The number of lattice points $N(T)$, subject to restriction* (2.1) *if $D > 0$, within $ax^2 + 2bxy + cy^2 = T$ which make the form prime to $2D$ is*

$$N(T) = \frac{\phi(|2D|)}{|2D|} \beta T + O(\sqrt{T})$$

where

$$\beta = \frac{\pi}{\sqrt{-D}}, \qquad D < 0,$$

$$\beta = \frac{1}{2\sqrt{D}} \log (T + U\sqrt{D}), \qquad D > 0.$$

Proof. Each $|2D|$ by $|2D|$ square built up over the plane from the origin contains $|2D|\phi(2D)$ lattice points which make the form prime to $|2D|$ **(1,** pp. 235-6**)**. Let the number of these squares lying entirely within the appropriate area be $N'(T)$. Then $|4D^2N'(T) - \text{Area}|$ is less than the area of the squares which are cut by the perimeter, which is of the order of the length of the perimeter. The perimeter is $O(\sqrt{T})$ and the area is βT, and the result follows.

LEMMA 2. *For any D not a square*

$$\sum_{\substack{p \leqslant x \\ (D|p)=1 \\ (p, 2D)=1}} \frac{\log p}{p} = \tfrac{1}{2} \log x + O(1).$$

This was proved by Selberg in his elementary proof of the prime-number theorem for arithmetic progressions **(4)**.

LEMMA 3.

$$\sum_{\substack{p \leqslant x \\ (p, 2D)=1}}{}' \frac{\log p}{p} = w \log x + O(1).$$

https://doi.org/10.4153/CJM-1954-034-0 Published online by Cambridge University Press

Here $\sum'$ means a summation over all representations, subject to restriction (2.1) if $D > 0$, by a representative system of one form from each properly primitive class of determinant D, and where w has the meaning (2.2).

Proof. This follows from Lemma 2 since each prime p with $(p, 2D) = 1$ and $(D|p) = 1$ has $2w$ representations in all by the classes θ_p and θ_p^{-1}. If θ_p is an ambiguous class, then there are $2w$ representations by the single class $\theta_p = \theta_p^{-1}$.

LEMMA 4.

$$\sum_{\substack{p \leqslant x \\ (p,2D)=1 \\ (D|p)=1}} \frac{\log^{r+1} p}{p} = \frac{1}{2}\frac{\log^{r+1} x}{r+1} + O(\log^r x).$$

Proof. This follows from Lemma 2 by partial summation.

LEMMA 5.

$$\sum_{\substack{p \leqslant x \\ (p,2D)=1}}{}' \frac{\log^{r+1} p}{p} = w\frac{\log^{r+1} x}{r+1} + O(\log^r x).$$

Proof. This follows from Lemma 4 and the proof of Lemma 3.

4. Proof of the theorem. Next consider

$$\sum_{\substack{n \leqslant x \\ n = \psi \\ (n,2D)=1}} \omega_n,$$

where $\omega_n = \omega_{n,x} = \sum_{d|n} \lambda_d$, $\lambda_d = \lambda_{d,x} = \mu(d) \log^2 \frac{x}{d}$, ψ is a properly primitive form of determinant D, and $n = \psi$ means n is represented by ψ and that each representation is counted with the usual restriction (2.1). But

$$\omega_n = \begin{cases} \log^2 x & n = 1, \\ \log p \log (x^2/p), & n = p^\alpha, \quad \alpha \geqslant 1, \\ 2 \log p \log q, & n = p^\alpha q^\beta, \alpha\beta \geqslant 1, \\ 0 & \text{for all other } n, \end{cases}$$

where p and q denote prime numbers.

Therefore, where p and q do not divide $2D$,

$$\sum_{\substack{n \leqslant x \\ n=\psi \\ (n,2D)=1}} \omega_n = \sum_{\substack{p^\alpha \leqslant x \\ p^\alpha = \psi}} \log p \log (x^2/p) + \sum_{\substack{p^\alpha q^\beta \leqslant x \\ p^\alpha q^\beta = \psi \\ \alpha\beta \geqslant 1}} \log p \log q + O(\log^2 x)$$

$$= \sum_{\substack{p \leqslant x \\ p = \psi}} (2 \log x \log p - \log^2 p) + \sum_{\substack{p^\alpha \leqslant x \\ p^\alpha = \psi \\ \alpha > 1}} \log p \log (x^2/p)$$

$$+ \sum_{\substack{pq \leqslant x \\ pq = \psi}} \log p \log q + \sum_{\substack{p^\alpha q^\beta \leqslant x \\ p^\alpha q^\beta = \psi \\ \alpha\beta > 1}} \log p \log q + O(\log^2 x).$$

From this follows, using the arguments of Selberg **(3)** with appropriate changes in the indices of summation, that

$$(4.1)\qquad \sum_{\substack{n\leqslant x\\ n=\psi\\ (n,2D)=1}} \omega_n = \sum_{\substack{p\leqslant x\\ p=\psi\\ (p,2D)=1}} \log^2 p + \sum_{\substack{pq\leqslant x\\ pq=\psi\\ (pq,2D)=1}} \log p \log q + O(x).$$

On the other hand,

$$\sum_{\substack{n\leqslant x\\ n=\psi\\ (n,2D)=1}} \omega_n = \sum_{\substack{d\leqslant x\\ (d,2D)=1}} \lambda_d \sum_{\substack{d\mid n\\ n\leqslant x\\ n=\psi\\ (n,2D)=1}} 1.$$

The second sum on the right is the number of multiples of d which are relatively prime to $2D$, less than or equal to x, and represented by ψ. This is RS where R is the number of representations of d by the forms of determinant D, and S is the number of numbers relatively prime to $2D$ and less than or equal to x/d which are represented by $\theta_d^{-1}\psi$ if θ_d represents d. From **(2**, p. 144**)**

$$R = w\sum_{\delta\mid d} (D|\delta)$$

and from Lemma 1,

$$S = \frac{\phi(|2D|)}{|2D|}\,\beta\frac{x}{d} + O(\sqrt{x/d}),$$

since β does not depend on any particular class but only on D. Therefore

$$RS = \left\{w\sum_{\delta\mid d}(D|\delta)\right\}\left\{\beta'\frac{x}{d} + O(\sqrt{x/d})\right\},\quad \beta' = \frac{\phi(|2D|)}{|2D|}\,\beta,$$

and

$$\sum_{\substack{n\leqslant x\\ n=\psi\\ (n,2D)=1}} \omega_n = w\beta' x \sum_{\substack{d\leqslant x\\ (d,2D)=1}} \frac{\lambda_d}{d}\sum_{\delta\mid d}(D|\delta) + \sqrt{x}\; O\Bigg(\sum_{\substack{d\leqslant x\\ (d,2D)=1}} \frac{|\lambda_d|}{\sqrt{d}}\sum_{\delta\mid d}(D|\delta)\Bigg).$$

Next the error term is estimated. Let

$$E = \sum_{\substack{d\leqslant x\\ (d,2D)=1}} \frac{|\lambda_d|}{\sqrt{d}}\, R_d,$$

where R_d is the number of representations of d by classes of forms of determinant D. By Lemma 1, $N(T)$ is independent of the class and since R_d is $N(d) - N(d-1)$ summed over the h classes, it follows that

$$|E| \leqslant h\sum_{t=2}^{x} \frac{N(t) - N(t-1)}{\sqrt{t}} \log^2\frac{x}{t} + O(\log^2 x).$$

A simple calculation shows that $E = O(\sqrt{x})$, and therefore

$$(4.2)\qquad \sum_{\substack{n\leqslant x\\ n=\psi\\ (n,2D)=1}} \omega_n = w\beta' x \sum_{\substack{d\leqslant x\\ (d,2D)=1}} \frac{\lambda_d}{d}\sum_{\delta\mid d}(D|\delta) + O(x),$$

https://doi.org/10.4153/CJM-1954-034-0 Published online by Cambridge University Press

where β' and w depend only on D, so that (4.2) holds for a ψ in any properly primitive class.

Comparing (4.1) and (4.2) and summing over the h properly primitive classes, there results

(4.3)

$$\sum_{\substack{p \leqslant x \\ p = \psi \\ (p, 2D)=1}} \log^2 p + \sum_{\substack{pq \leqslant x \\ pq = \psi \\ (pq, 2D)=1}} \log p \log q = \frac{1}{h}\left\{ \sum_{\substack{p \leqslant x \\ (p,2D)=1}}' \log^2 p + \sum_{\substack{pq \leqslant x \\ (pq,2D)=1}}' \log p \log q \right\} + O(x).$$

By partial summation one gets

$$\sum_{\substack{p \leqslant x \\ p = \psi \\ (p, 2D)=1}} \frac{\log^2 p}{p} + \sum_{\substack{pq \leqslant x \\ pq = \psi \\ (pq, 2D)=1}} \frac{\log p \log q}{pq} = \frac{1}{h}\left\{ \sum_{\substack{p \leqslant x \\ (p,2D)=1}}' \frac{\log^2 p}{p} + \sum_{\substack{pq \leqslant x \\ (pq,2D)=1}}' \frac{\log p \log q}{pq} \right\} + O(\log x).$$

Since each pq in the summation on the right above appears $4w$ times, it follows that

$$\sum_{\substack{pq \leqslant x \\ (pq,2D)=1}}' \frac{\log p \log q}{pq} = 4w \sum_{\substack{p \leqslant x \\ (p,2D)=1 \\ (D|p)=1}} \frac{\log p}{p} \sum_{\substack{q \leqslant x/p \\ (q,2D)=1 \\ (D|q)=1}} \frac{\log q}{q}.$$

This is easily evaluated by using Lemmas 2 and 4 giving $w/2 \log^2 x + O(\log x)$. Therefore from this and Lemma 5,

$$\sum_{\substack{p \leqslant x \\ p = \psi \\ (p, 2D)=1}} \frac{\log^2 p}{p} + \sum_{\substack{pq \leqslant x \\ pq = \psi \\ (pq, 2D)=1}} \frac{\log p \log q}{pq} = \frac{w}{h} \log^2 x + O(\log x). \tag{4.4}$$

By partial summation from (4.3) results

$$\sum_{\substack{p \leqslant x \\ p = \psi \\ (p, 2D)=1}} \frac{\log^3 p}{p} + \sum_{\substack{pq \leqslant x \\ pq = \psi \\ (pq, 2D)=1}} \frac{\log p \log q}{pq} \log pq$$

$$= \frac{1}{h}\left\{ \sum_{\substack{p \leqslant x \\ (p,2D)=1}}' \frac{\log^3 p}{p} + \sum_{\substack{pq \leqslant x \\ (pq,2D)=1}}' \frac{\log p \log q}{pq} \log pq \right\} + O(\log^2 x).$$

$$\sum_{\substack{pq \leqslant x \\ (pq,2D)=1}}' \frac{\log p \log q}{pq} \log pq = \sum_{\substack{pq \leqslant x \\ (pq,2D)=1}}' \frac{\log^2 p \log q}{pq} + \sum_{\substack{pq \leqslant x \\ (pq,2D)=1}}' \frac{\log p \log^2 q}{pq}.$$

But each of the two symmetric terms on the right above can be written as

$$4w \sum_{\substack{p \leqslant x \\ (p,2D)=1 \\ (D|p)=1}} \frac{\log^2 p}{p} \sum_{\substack{q \leqslant x/p \\ (q,2D)=1 \\ (D|q)=1}} \frac{\log q}{q},$$

and by Lemma 4 this equals $\frac{1}{6}w \log^3 x + O(\log^2 x)$. Using this and Lemma 5 results in

https://doi.org/10.4153/CJM-1954-034-0 Published online by Cambridge University Press

$$(4.5)\qquad \sum_{\substack{p\leqslant x\\ p=\psi\\ (p,2D)=1}} \frac{\log^3 p}{p} + \sum_{\substack{pq\leqslant x\\ pq=\psi\\ (pq,2D)=1}} \frac{\log p \log q}{pq}\log pq = \frac{2w}{3h}\log^3 x + O(\log^2 x).$$

Next,

$$\sum_{\substack{pq\leqslant x\\ pq=\psi\\ (pq,2D)=1}} \frac{\log p \log^2 q}{pq} = \sum_{\substack{p\leqslant x\\ (p,2D)=1\\ (D|p)=1}} \frac{\log p}{p}\left\{\sum_{\substack{q\leqslant x/p\\ q=\bar{\psi}_p\\ (q,2D)=1}} \frac{\log^2 q}{q} + \sum_{\substack{q\leqslant x/p\\ q=\bar{\psi}_p^{-1}\\ (q,2D)=1}} \frac{\log^2 q}{q}\right\},$$

where p is represented by ψ_p and ψ_p^{-1} and $\psi_p\bar{\psi}_p = \psi_p^{-1}\bar{\psi}_p^{-1} = \psi$. The above expression is equal to

$$\sum_{\substack{p\leqslant x\\ (p,2D)=1\\ (D|p)=1}} \frac{\log p}{p}\left\{\frac{2w}{h}\log^2\frac{x}{p} - \sum_{\substack{qr\leqslant x/p\\ qr=\bar{\psi}_p\\ qr=\bar{\psi}_p^{-1}\\ (qr,2D)=1}} \frac{\log q \log r}{qr} + O(\log x)\right\}$$

by (4.4) (which holds for a ψ from any class), and where r denotes a prime number. Expanding and simplifying by Lemma 4 gives the last expression equal to

$$\frac{w}{3h}\log^3 x - \sum_{\substack{pqr\leqslant x\\ pqr=\psi\\ (pqr,2D)=1}} \frac{\log p \log q \log r}{pqr} + O(\log^2 x).$$

Therefore from (4.5),

$$(4.6)\qquad \sum_{\substack{p\leqslant x\\ p=\psi\\ (p,2D)=1}} \frac{\log^3 p}{p} = 2\sum_{\substack{pqr\leqslant x\\ pqr=\psi\\ (pqr,2D)=1}} \frac{\log p \log q \log r}{pqr} + O(\log^2 x).$$

From (4.4), we have

$$(4.7)\qquad \sum_{\substack{p\leqslant x\\ p=\psi\\ (p,2D)=1}} \frac{\log^2 p}{p} \leqslant \frac{w}{h}\log^2 x + O(\log x),$$

which yields by partial summation

$$(4.8)\qquad \sum_{\substack{p\leqslant x\\ p=\psi\\ (p,2D)=1}} \frac{\log p}{p} \leqslant \frac{2w}{h}\log x + O(\log\log x).$$

Next,

$$\sum_{\substack{pq\leqslant x\\ pq=\psi\\ (pq,2D)=1}} \frac{\log p \log q}{pq} \leqslant \sum_{p\leqslant x^{1/3}}\sum_{\substack{q\leqslant x^{1/3}\\ pq=\psi\\ (pq,2D)=1}} \frac{\log p \log q}{pq} + 2\sum_{\substack{x^{1/3}<p\leqslant x\\ (p,2D)=1\\ (D|p)=1}} \frac{\log p}{p}\sum_{\substack{q\leqslant x/p\\ q=\bar{\psi}_p\\ q=\bar{\psi}_p^{-1}\\ (q,2D)=1}} \frac{\log q}{q}$$

Applying (4.8) and Lemma 4, we find

$$\sum_{\substack{pq\leqslant x\\ pq=\psi\\ (pq,2D)=1}} \frac{\log p \log q}{pq} \leqslant \sum_{p\leqslant x^{1/3}}\sum_{\substack{q\leqslant x^{1/3}\\ pq=\psi\\ (pq,2D)=1}} \frac{\log p \log q}{pq} + \frac{8w}{9h}\log^2 x + O(\log x \log\log x).$$

https://doi.org/10.4153/CJM-1954-034-0 Published online by Cambridge University Press

Therefore from (4.4),

$$\sum_{\substack{p\leqslant x\\ p=\psi\\ (p,2D)=1}} \frac{\log^2 p}{p} \geqslant \frac{w}{9h}\log^2 x - \sum_{p\leqslant x^{1/3}}\sum_{\substack{q\leqslant x^{1/3}\\ pq=\psi\\ (pq,2D)=1}} \frac{\log p \log q}{pq} + O(\log x \log\log x);$$

that is, for $x > x_0$,

$$\log x \sum_{\substack{p\leqslant x\\ p=\psi\\ (p,2D)=1}} \frac{\log p}{p} > \frac{w}{10h}\log^2 x - \sum_{\substack{p,q\leqslant x^{1/3}\\ p=\psi_p\\ q=\psi_q\\ (p,2D)=1\\ (q,2D)=1}} \frac{\log p}{p}\,\frac{\log q}{q},$$

where the latter sum is taken over primes p and q with $\psi_p\psi_q = \psi$. Recalling (2.3), this can be written as

$$\log x\, S_\psi(x) > \frac{w}{10h}\log^2 x - \sum_{\theta\theta'=\psi} S_\theta(x^{\frac{1}{3}})\, S_{\theta'}(x^{\frac{1}{3}}),$$

where the sum is taken over all pairs of classes θ, θ' such that ψ belongs to the class $\theta\theta'$.

Division of both sides by $\log^2 x = 9\log^2 x^{\frac{1}{3}}$ yields

$$Q_\psi(x) > \frac{w}{10h} - \frac{1}{9}\sum_{\theta\theta'=\psi} Q_\theta(x^{\frac{1}{3}})\, Q_{\theta'}(x^{\frac{1}{3}}), \qquad x > x_0. \tag{4.9}$$

By (4.6)

$$\log^3 x\, Q_\psi(x) \geqslant 2\sum_{\substack{pqr\leqslant x^{1/3}\\ pqr=\psi\\ (pqr,2D)=1}} \frac{\log p\log q\log r}{pqr} + O(\log^2 x),$$

$$Q_\psi(x) \geqslant \frac{2}{27}\sum_{\theta\theta'\theta''=\psi}\left\{\frac{1}{\log x^{1/3}}\sum_{\substack{p\leqslant x^{1/3}\\ p=\theta\\ (p,2D)=1}}\frac{\log p}{p}\right\}\left\{\frac{1}{\log x^{1/3}}\sum_{\substack{q\leqslant x^{1/3}\\ q=\theta'\\ (q,2D)=1}}\frac{\log q}{q}\right\}$$
$$\times\left\{\frac{1}{\log x^{1/3}}\sum_{\substack{r\leqslant x^{1/3}\\ r=\theta''\\ (r,2D)=1}}\frac{\log r}{r}\right\} + O\left(\frac{1}{\log x}\right)$$

or

$$Q_\psi(x) \geqslant \frac{2}{27}\sum_{\theta\theta'\theta''=\psi} Q_\theta(x^{\frac{1}{3}})\, Q_{\theta'}(x^{\frac{1}{3}})\, Q_{\theta''}(x^{\frac{1}{3}}) + O\left(\frac{1}{\log x}\right). \tag{4.10}$$

Then (4.8) gives

$$Q_\psi(x) \leqslant \frac{2w}{h} + O\left(\frac{\log\log x}{\log x}\right). \tag{4.11}$$

At this point the characters of classes of forms of determinant D are introduced where the character χ of a class θ, $\chi(\theta)$, is obtained as an Abelian group character from the group which the classes form under composition. In general they are divided into three categories: The principal character χ_0, with $\chi_0(\theta) = 1$ for all θ, real non-principal characters, with $\chi(\theta) = \pm 1$ for all θ

and which exist if and only if h is even since each character is an h-th root of unity, and the non-real characters. These characters are needed only when $h(D)$ is even.

LEMMA 6. *If h is even and χ is any real non-principal character, then*

$$\sum_{\substack{p \leqslant x \\ \chi(\theta_p)=1 \\ (p,2D)=1}} \frac{\log p}{p} = \frac{1}{4}\log x + O(1).$$

Here the summation is extended over all primes which are representable by forms of classes of determinant D and for which classes $\chi(\theta) = 1$.

Proof. By considering all possible products of Gauss's generic characters, one gets that for any real non-principal character, there exists a factor D_1 of D such that $\chi(\theta) = (D_1|m)$, where m is any number prime to 2D which is representable by forms of the class θ (**5**, pp. 311-312). Therefore $\chi(\theta_p) = (D_1|p)$ and since if p is represented by a form of determinant D, $(D|p) = 1$, the sum takes the form

$$\sum_{\substack{p \leqslant x \\ (p,2D)=1 \\ (\frac{D}{p})=(\frac{D_1}{p})=1}} \frac{\log p}{p} = W.$$

However,

$$W = \tfrac{1}{2}\left\{ \sum_{\substack{p \leqslant x \\ (DD_1|p)=1}} \frac{\log p}{p} - \sum_{\substack{p \leqslant x \\ (D_1|p)=-1}} \frac{\log p}{p} + \sum_{\substack{p \leqslant x \\ (D|p)=1}} \frac{\log p}{p} \right\}$$

since each desired prime appears twice in the sums of the right member. Since by Lemma 2

$$\sum_{\substack{p \leqslant x \\ (D_1|p)=-1}} \frac{\log p}{p} = \sum_{p \leqslant x} \frac{\log p}{p} - \sum_{\substack{p \leqslant x \\ (D_1|p)=1}} \frac{\log p}{p} = \tfrac{1}{2}\log x + O(1),$$

it follows, again by Lemma 2, that

$$W = \tfrac{1}{2}(\tfrac{1}{2} - \tfrac{1}{2} + \tfrac{1}{2})\log x + O(1) = \tfrac{1}{4}\log x + O(1).$$

LEMMA 7. *Suppose $h(D)$ is even and there is a set of different classes of properly primitive forms of determinant D, $\theta_1, \theta_2, \ldots, \theta_k$, and that $k \geqslant \frac{1}{2}h$, and that for each real character χ for forms of determinant D, there is a θ in the set with $\chi(\theta) = 1$. Let ψ be a properly primitive form of determinant D, and suppose that there is a θ and a θ', not necessarily different, belonging to the set, such that ψ belongs to the class $\theta\theta'$. Then there is a triple of classes belonging to the set, θ, θ', θ'', such that $\theta\,\theta'\,\theta'' = \psi$ under composition.*

Proof. The proof follows from the proof of Selberg's lemma (**3**, Lemma 2) by replacing primitive residue classes by properly primitive classes of quadratic forms.

LEMMA 8. *If $h(D)$ is odd, and there is a set of different classes of properly primitive forms of determinant D, $\theta_1, \theta_2, \ldots, \theta_k$, with $k > h/2$, and if a θ and a θ', not necessarily different, such that $\theta\theta' = \psi$, belong to this set, then there exists a triple of classes belonging to the set, $\theta, \theta', \theta''$, such that $\theta\,\theta'\,\theta'' = \psi$.*

The proof is the same as the proof of the preceding lemma for $k > \frac{1}{2}h$.

Now it can be shown that

$$Q_\psi(x) > \frac{1}{(130)^4 h^6}, \qquad x > x_0.$$

Assume that for some large x

$$Q_\psi(x) < \frac{1}{130h}. \tag{4.12}$$

By Lemma 3,

$$\sum_\theta Q_\theta(x^{\frac{1}{3}}) = \frac{w}{\log x^{1/3}}\,[\log x^{\frac{1}{3}} + O(1)] = w + O\left(\frac{1}{\log x}\right).$$

But

$$Q_\theta(x^{\frac{1}{3}}) \leqslant \frac{2w}{h} + O\left(\frac{\log\log x}{\log x}\right)$$

for all θ by (4.11).

Therefore there are at least the greatest integer in $(h+1)/2$ classes θ with

$$Q_\theta(x^{\frac{1}{3}}) > \frac{1}{130h^2}, \qquad x > x_0.$$

From (4.9),

$$Q_\psi(x) > \frac{1}{10h} - \frac{1}{9}\sum_{\theta\theta'=\psi} Q_\theta(x^{\frac{1}{3}})\,Q_{\theta'}(x^{\frac{1}{3}}), \qquad x > x_0,$$

and (4.12),

$$Q_\psi(x) < \frac{1}{130h}.$$

Therefore

$$\sum_{\theta\theta'=\psi} Q_\theta(x^{\frac{1}{3}})\,Q_{\theta'}(x^{\frac{1}{3}}) > 9\left(\frac{1}{10h} - \frac{1}{130h}\right) > \frac{1}{15h}.$$

Therefore there exists at least one pair of classes θ, θ' with $\theta\theta' = \psi$ such that

$$Q_\theta(x^{\frac{1}{3}})\,Q_{\theta'}(x^{\frac{1}{3}}) > \frac{1}{15h^2}$$

or

$$Q_\theta(x^{\frac{1}{3}}) > \frac{1}{Q_{\theta'}(x^{1/3})\,15h^2} > \frac{1}{\left(\frac{2w}{h} + \epsilon\right)15h^2} \qquad \text{by (4.11)}$$

$$= \frac{1}{30wh + 15h^2\epsilon} > \frac{1}{130h^2}, \qquad x > x_0,$$

and likewise

$$Q_{\theta'}(x^{\frac{1}{3}}) > \frac{1}{130h^2}, \qquad x > x_0.$$

5. Completion of proof for $h(D)$ even. By Lemma 6

$$\sum_{\substack{p \leqslant x \\ p=\theta_p \\ \chi(\theta_p)=1}} \frac{\log p}{p} = \frac{w}{2} \log x + O(1) > \frac{1}{9} \log x, \qquad x > x_0,$$

or

$$\sum_{\substack{\theta \\ \chi(\theta)=1}} \sum_{\substack{p \leqslant x \\ p=\theta}} \frac{\log p}{p} > \frac{1}{9} \log x, \qquad x > x_0,$$

or

$$\sum_{\substack{\theta \\ \chi(\theta)=1}} \frac{1}{\log x^{1/3}} \sum_{\substack{p \leqslant x^{1/3} \\ p=\theta}} \frac{\log p}{p} = \sum_{\substack{\theta \\ \chi(\theta)=1}} Q_\theta(x^{\frac{1}{3}}) > \frac{1}{9}, \qquad x > x_0.$$

Therefore there exists at least one θ with

$$Q_\theta(x^{\frac{1}{3}}) > \frac{1}{9h} > \frac{1}{130h^2}$$

and with $\chi(\theta) = 1$ for each real non-principal character χ.

Thus there is a set of different classes $\theta_1, \theta_2, \ldots \theta_k$, with $k \geqslant h/2$, such that for $i = 1, 2, \ldots k$,

$$Q_{\theta_i}(x^{\frac{1}{3}}) > \frac{1}{130h^2}$$

and such that for each real character χ there is a θ_i with $\chi(\theta_i) = 1$, and finally such that there exist classes θ, θ', with $\theta\theta' = \psi$. Therefore by Lemma 7, there exist classes $\theta, \theta', \theta''$, belonging to the set with $\theta\theta'\theta'' = \psi$. Then by (4.10)

$$Q_\psi(x) \geqslant \frac{2}{27} Q_\theta(x^{\frac{1}{3}})\, Q_{\theta'}(x^{\frac{1}{3}})\, Q_{\theta''}(x^{\frac{1}{3}}) - O\left(\frac{1}{\log x}\right) > \frac{1}{(130)^4 h^6}$$

for $x > x_0$, which completes the proof for $h(D)$ even.

6. Completion of proof for $h(D)$ odd. Again there is a set of different classes $\theta_1, \theta_2, \ldots \theta_k$, with $k > h/2$ such that for $i = 1, 2, \ldots k$,

$$Q_{\theta_i}(x^{\frac{1}{3}}) > \frac{1}{130h^2}$$

and such that there exist classes θ, θ' in the set with $\theta\theta' = \psi$. Therefore by Lemma 8 there exists a triple of classes $\theta, \theta', \theta''$, belonging to the set with $\theta\theta'\theta'' = \psi$. Then again by (4.10)

$$Q_\psi(x) \geqslant \frac{2}{27} Q_\theta(x^{\frac{1}{3}})\, Q_{\theta'}(x^{\frac{1}{3}})\, Q_{\theta''}(x^{\frac{1}{3}}) - O\left(\frac{1}{\log x}\right) > \frac{1}{(130)^4 h^6}$$

for $x > x_0$ which completes the proof of the theorem.

References

1. P. G. L. Dirichlet, *Vorlesungen über Zahlentheorie* (Brauschweig, 1879).

2. E. Landau, *Vorlesungen über Zahlentheorie*, vol. 1 (New York, 1950).

3. A. Selberg, *An elementary proof of Dirichlet's theorem about primes in an arithmetic progression*, Annals of Math., *50* (1949), 297–304.

4. ———, *An elementary proof of the prime-number theorem for arithmetic progressions*, Can. J. Math., *2* (1950), 66–78.

5. H. Weber, *Beweis des Satzes, dass jede eigentlich primitive quadratische Form unendlich viele Primzahlen darzustellen fähig ist*, Math. Annalen, *20* (1882), 301-329.

University of Colorado

https://doi.org/10.4153/CJM-1954-034-0 Published online by Cambridge University Press