The sum of the numbers in this array is $\varrho\sigma\binom{g+1}{2}$. Hence if $a(n; f_{1,1}, \ldots, f_{\varrho,\sigma})$ denotes the number of unrestricted ϱ row, σ plane partitions of n with at most $f_{i,j}$ non-zero parts on the i, jth row. Hence

$$b(n; g, \ldots, g) = \sum_{f_{i,j}\leqslant g} a\left(n-\varrho\sigma\binom{g+1}{2}; f_{1,1}, \ldots, f_{\varrho,\sigma}\right).$$

Multiply both sides by $x^{n-\varrho\sigma\binom{g+1}{2}}$ and sum over n. We obtain

$$B(x; g, \ldots, g) = x^{\varrho\sigma\binom{g+1}{2}} \sum_{f_{i,j}\leqslant g} \sum_{n=0}^{\infty} a(n; f_{1,1}, \ldots, f_{\varrho,\sigma}) x^n$$
$$= x^{\varrho\sigma\binom{g+1}{2}} \sum_{f_{i,j}\leqslant g} A(x; f_{1,1}, \ldots, f_{\varrho,\sigma})$$

where we may replace $n-\varrho\sigma\binom{g+1}{2}$ by n as the summation index in the right since the terms vanish for $n < \varrho\sigma\binom{g+1}{2}$. If we let $g\to\infty$ and note that

$$A_{\varrho,\sigma}(x) = \sum_{f_{i,j}} A(x; f_{1,1}, \ldots, f_{\varrho,\sigma})$$

we can obtain an expression for $A_{\varrho,\sigma}(x)$. Further we can see that since

$$A(x) = \lim_{\substack{\varrho\to\infty\\ \sigma\to\infty}} A_{\varrho,\sigma}(x),$$

a solution to the recursion of the theorem will enable us also to obtain a solution to the unrestricted case. At present only a numerical solution is available.

References

[1] A. O. L. Atkin, P. Bratley, I. G. Macdonald and J. K. S. MacKay, *Some computations for m-dimensional partitions*, Proc. Camb. Phil. Soc. 63 (1967), p. 1057.

[2] B. Gordon and L. Houten, *Notes on plane partitions I*, J. of Comb. Thy. 4 (1) (1968).

[3] P. A. MacMahon, *Combinatory Analysis, II*, Cambridge 1916.

WASHINGTON STATE UNIVERSITY

Reçu par la Rédaction le 23. 1. 1968

ACTA ARITHMETICA
XV (1968)

A note on the representability of binary quadratic forms with Gaussian integer coefficients as sums of squares of two linear forms

by

JOHN HARDY (Athens, Ga.)

1. Notations. Let G denote the ring of Gaussian integers. Small Greek letters will denote elements of G, except for the unit i, and small Latin letters will denote ordinary integers in Z. If a is in G, the norm of a will be denoted by $N(a)$.

DEFINITION. a in G is called *odd* if $N(a)$ is odd. a in G is called *even* if $N(a)$ is even.

With each integer $a+bi$ in G, there are associated three other integers, namely $-a-bi$, $-b+ai$, $b-ai$.

DEFINITION. The number $x+yi$ of the four associated odd integers $a+bi$, $-a-bi$, $-b+ai$, $b-ai$ is called *primary* if

$$x\equiv 1\ (4), \quad y\equiv 0\ (4)$$

or

$$x\equiv 3\ (4), \quad y\equiv 2\ (4).$$

In any group of four associated odd integers, exactly one is primary.

DEFINITION. If a in G is even, we distinguish between the associates of a by taking as *primary* that one which can be written as $(1+i)^k\beta$ where β is an odd, primary integer.

DEFINITION. Let a, β, δ be Gaussian integers. δ will be called the *greatest common divisor* of a and β if

1) δ is a common divisor of a and β,
2) if γ in G is a common divisor of a and β, then $\gamma\,|\,\delta$,
3) δ is primary.

We shall write $\delta = (a, \beta)$.

2. The following result may be found in [2].

THEOREM. *If a is an odd Gaussian integer of the form $a+2bi$, then a can be expressed as a sum of two squares of integers in G. If a is even,* *then a can be expressed as a sum of two squares if and only if $(1+i) \nmid a$ or $(1+i)^3 \nmid a$.*

The next result is well-known.

LEMMA 1. (Gauss Criterion.) *Let $[a, \beta, \gamma]$ and $[a', \beta', \gamma']$ be two binary quadratic forms with coefficients in G such that $\beta'^2 - 4a'\gamma' = (\beta^2 - 4a\gamma)\varepsilon^2$ for some ε in G and $\beta' = \beta\varepsilon + 2\nu$ for some ν in G. Then there exists a transformation of determinant ε with coefficients in G which carries $[a, \beta, \gamma]$ into $[a', \beta', \gamma']$ if and only if there exist elements τ_1, τ_3 in G which satisfy*

$$a\tau_1^2 + \beta\tau_1\tau_3 + \gamma\tau_3^2 = a',$$

$$\varepsilon a\tau_1 + \tfrac{1}{2}(\varepsilon\beta + \beta')\tau_3 \quad \text{and} \quad \tfrac{1}{2}(\varepsilon\beta - \beta')\tau_1 + \varepsilon\gamma\tau_3$$

are divisible by a'.

LEMMA 2. *Let π and $\varkappa$ be two non-zero Gaussian integers which are each sums of two squares. Then $\pi\varkappa$ is a sum of two squares, say $\pi\varkappa = \xi^2 + \eta^2$. Then, there exist a_1 and a_2 in G such that*

$$\pi = a_1^2 + a_2^2, \qquad \pi^2\varkappa = (\xi a_1 + \eta a_2)^2 + (\xi a_2 - \eta a_1)^2,$$

and

$$\pi \mid (\xi a_1 + \eta a_2) \quad \text{and} \quad \pi \mid (\xi a_2 - \eta a_1).$$

Proof. Clearly, $\pi\varkappa$ is a sum of two squares. There exist $\beta_1, \beta_2, \varkappa_1, \varkappa_2$ in G such that

$$\xi = \beta_1\varkappa_1 + \beta_2\varkappa_2, \qquad \eta = \beta_1\varkappa_2 - \beta_2\varkappa_1$$

where $\pi = \beta_1^2 + \beta_2^2$ and $\varkappa = \varkappa_1^2 + \varkappa_2^2$. Taking $a_1 = \beta_1$ and $a_2 = -\beta_2$,

$$\pi^2\varkappa = (\xi\beta_1 - \eta\beta_2)^2 + (\eta\beta_1 + \xi\beta_2)^2 = (\beta_1^2\varkappa_1 + \beta_2^2\varkappa_2)^2 + (\beta_1^2\varkappa_2 + \beta_2^2\varkappa_2)^2.$$

THEOREM 1. *Let $f = ax^2 + 2\eta xy + \beta y^2$ be a binary quadratic form with coefficients in G and $a\beta \neq 0$. Necessary and sufficient conditions that f be expressible as a sum of squares of two linear forms with coefficients in G*

$$f = (a_1x + \beta_1y)^2 + (a_2x + \beta_2y)^2$$

are that $\Delta = a\beta - \eta^2$ be a perfect square and that a, β, and $\delta = (a, 2\eta, \beta)$ be sums of two squares of elements in G.

Proof. Suppose $f = ax^2 + 2\eta xy + \beta y^2 = (a_1x + \beta_1y)^2 + (a_2x + \beta_2y)^2$ for some $a_1, a_2, \beta_1, \beta_2$ in G. Now $a = a_1^2 + a_2^2$, $\beta = \beta_1^2 + \beta_2^2$ and $\eta = a_1\beta_1 + a_2\beta_2$. Then $\Delta = a\beta - \eta^2 = (a_2\beta_1 - a_1\beta_2)^2$. If a or β is odd, then $\delta = (a, 2\eta, \beta)$ is odd and δ can be expressed as a sum of two squares. Suppose a and β are both even. Clearly $(1+i) \nmid \delta$. Assume $(1+i)^3 \| \delta$. Then $(1+i)^3 \| 2\eta$ and $(1+i) \| \eta$ which is impossible. Therefore, δ can be expressed as a sum of two squares.

Now assume $\Delta = a\beta - \eta^2$ is a square, say Δ_0^2, and δ, a, and β are each sums of two squares. Without loss of generality, we can assume $\delta = 1$. By Lemma 2, there exist a_1, a_2 in G such that

$$a^2\beta = (\Delta_0a_1 + \eta a_2)^2 + (\Delta_0a_2 - \eta a_1)^2, \qquad a = a_1^2 + a_2^2,$$
$$a \mid (\Delta_0a_1 + \eta a_2), \quad \text{and} \quad a \mid (\Delta_0a_2 - \eta a_1).$$

By Lemma 1, there exist β_1, β_2 in G such that the transformation whose matrix is $\begin{bmatrix} a_1 & \beta_1 \\ a_2 & \beta_2 \end{bmatrix}$ carries $[1, 0, 1]$ into $[a, 2\eta, \beta]$. Hence, f can be expressed as a sum of squares of two linear forms with coefficients in G.

We might note here that $f = ax^2 + 2\eta xy + \beta y^2$ may be a sum of squares of two linear forms without (a, η, β) being a sum of two squares of Gaussian integers. For example,

$$4ix^2 + 2(-6+2i)xy + (-4+8i)y^2$$
$$= \{(1+i)x + 2iy\}^2 + \{(1+i)x + (-2+2i)y\}^2$$

but

$$(4i, -6+2i, -4+8i) = (1+i)^3 = -2+2i$$

which is not a sum of two squares.

THEOREM 2. *Let $f = ax^2 + 2\eta xy + \beta y^2$ be a binary quadratic form with coefficients in G such that $\beta = 0$, $a \neq 0$. Necessary and sufficient conditions that f be expressible as a sum of squares of two linear forms with coefficients in G are that $\delta = (a, 2\eta)$, a are each sums of two squares and η is divisible by $a_1 + ia_2$ or $a_1 - ia_2$ where $a = a_1^2 + a_2^2$ for some a_1, a_2 in G.*

Proof. Assume f can be expressed as a sum of squares of two linear forms, say

$$f = (a_1x + \beta_1y)^2 + (a_2x + \beta_2y)^2$$

with $a_1, a_2, \beta_1, \beta_2$ in G. Then $a = a_1^2 + a_2^2$, $0 = \beta = \beta_1^2 + \beta_2^2$, $\eta = a_1\beta_1 + a_2\beta_2$. Since $\beta_1 = \pm i\beta_2$, $\eta = (a_1 - ia_2)\beta_1$ or $\eta = (a_1 + ia_2)\beta_1$. An argument similar to that in Theorem 1 shows $\delta = (a, 2\eta)$ is a sum of two squares.

Now, suppose a, δ are each sums of two squares and η is divisible by $a_1 + ia_2$ where $a = a_1^2 + a_2^2$. Now $a\beta - \eta^2 = -\eta^2 = (\eta i)^2$. Since η is divisible by $a_1 + ia_2$, $a \mid (\eta a_1 i + \eta a_2)$ and $a \mid (-\eta a_1 + \eta i a_2)$. Thus, by Lemma 1, there exists a transformation of determinant ηi which carries $[1, 0, 1]$ into $[a, 2\eta, 0]$. Hence, f can be expressed as a sum of squares of two linear forms with coefficients in G. If η is divisible by $a_1 - ia_2$, there is a transformation of determinant $-\eta i$ which carries $[1, 0, 1]$ into $[a, 2\eta, 0]$.

THEOREM 3. *Let $f = ax^2 + 2\eta xy + \beta y^2$ be a binary quadratic form with coefficients in G such that $a, \beta = 0$. A necessary and sufficient condition* *that f be a sum of squares of two linear forms with coefficients in G is that η be divisible by 2.*

Proof. The theorem is trivial if $\eta = 0$. Assume $\eta \neq 0$ and f can be expressed as a sum of squares of two linear forms, say

$$f = (a_1x+\beta_1y)^2+(a_2x+\beta_2y)^2$$

with $a_1, a_2, \beta_1, \beta_2$ in G. Now $0 = a = a_1^2+a_2^2$, $0 = \beta = \beta_1^2+\beta_2^2$, and $\eta = a_1\beta_1+a_2\beta_2$. If $a_1 = ia_2$, $\beta_1 = i\beta_2$ or if $a_1 = -ia_2$, $\beta_1 = -i\beta_2$, then $\eta = 0$. If $a_1 = -ia_2$ or $\beta_1 = -i\beta_2$, say $\beta_1 = -i\beta_2$, then $\eta = 2a_2\beta_2$.

Now, assume that $\eta \neq 0$ is divisible by 2. If we put $\eta = 2a_1\beta_1$ for some a_1, β_1 in G, f can be expressed as

$$(a_1x+\beta_1y)^2+(ia_1x-i\beta_1y)^2.$$

We note here that if η is divisible by 2 ($a = \beta = 0$), then 2η is a sum of squares of two Gaussian integers.

3. In this section we attempt to determine the number of ways a binary quadratic form with coefficients in G can be represented as a sum of squares of two linear forms. The procedure followed here is essentially the same as that in [4].

Let $f = ax^2+2\eta xy+\beta y^2$ be a binary quadratic form with $a\beta \neq 0$ which can be expressed as a sum of squares of two linear forms, namely

$$f = (a_1x+\beta_1y)^2+(a_2x+\beta_2y)^2. \tag{1}$$

We can express this using matrix notation as

$$T'T = B \quad \text{where} \quad B = \begin{bmatrix} a & \eta \\ \eta & \beta \end{bmatrix}, \quad T = \begin{bmatrix} a_1 & \beta_1 \\ a_2 & \beta_2 \end{bmatrix}. \tag{2}$$

The determinant of the matrix B must be a square, say $|B| = \mu^2$.

In case $\mu = 0$, f is a perfect square,

$$f = \delta_1(a'x+\beta'y)^2, \quad (a', \beta') = 1.$$

Each of $a_1x+\beta_1y$ must be proportional to $a'x+\beta'y$. If $a_1x+\beta_1y = \varepsilon_1(a'x+\beta'y)$ and $a_2x+\beta_2y = \varepsilon_2(a'x+\beta'y)$, then $\delta_1 = \varepsilon_1^2+\varepsilon_2^2$. If $\delta_1 = (a, 2\eta, \beta)$, and $|B| = 0$, the number of solutions of (1) is equal to $r_2(\delta_1)$, the number of representations of δ_1 as a sum of squares of two Gaussian integers.

If $|B| = \mu^2 \neq 0$, $|T| = \mu$ or $-\mu$. The number of solutions with $|T| = -\mu$ is equal to the number with $|T| = \mu$. Suppose $\mu = (1+i)^k\mu'$ where μ' is an odd integer of the form $2a+bi$. The form $f' = [-a, 2i\eta, \beta]$ can also be expressed as a sum of squares of two linear forms. In fact, the number of representations of f' as a sum of two squares is the same as f. The determinant of f' is $-a\beta+\eta^2 = -\mu^2 = (\mu i)^2$ and

$\mu i = (1+i)^k(-b+2ai)$. Thus, we shall assume that if μ^2 is the determinant of f, then $\mu = (1+i)^k\mu'$, where μ' is an odd integer of the form $a+2bi$.

A matrix with entries from G of the type

$$H = \begin{bmatrix} \mu_1 & \lambda \\ 0 & \mu_2 \end{bmatrix}, \quad 0 \leqslant N(\lambda) < N(\mu_2), \quad \mu_1\mu_2 = \mu, \tag{3}$$

$\mu_1 = (1+i)^u\mu_1'$, $\mu_2 = (1+i)^v\mu_2'$ where μ_1' and μ_2' are odd integers of the form $a+2bi$, will be called an *Hermite-matrix* of determinant μ.

Two matrices S and T with entries from G are called *left-equivalent* if there exists a unimodular matrix V (i.e., a matrix with entries from G of determinant $+1$) such that $S = UT$.

LEMMA 3. *An integral matrix (of order 2) with determinant $\mu = (1+i)^k\mu'$, where μ' is an odd integer of the form $a+2bi$, is left-equivalent to one and only one Hermite-matrix of determinant μ.*

LEMMA 4. *Write $\mu = \pi_1^{r_1}\pi_2^{r_2}\ldots\pi_s^{r_s}$ as a product of powers of distinct primes π_i, $i = 1, \ldots, s$, where the odd primes are of the form $a+2bi$. If T is a given matrix of determinant μ, then, for each i, there exists a unique Hermite-matrix right-divisor of T of determinant π_i.*

LEMMA 5. *Any given system $H_1, \ldots, H_s$ of Hermite-matrices of respective determinants $\pi_1^{r_1}, \ldots, \pi_s^{r_s}$ determine as right-divisors a unique Hermite-matrix H of determinant μ, and hence are the right-divisors of an integral matrix T of determinant μ which is determined up to a left unimodular factor.*

The method of proof for the three preceeding lemmas is the same for the corresponding ones in [4].

Given a matrix B such that $B = T'T$ for some T, we wish to count the number of such matrices T. It is sufficient to construct the matrices $H'^{-1}BH^{-1}$ with H ranging over all the Hermite-matrices of determinant μ such that $H'^{-1}BH^{-1}$ is equivalent to the identity matrix. In view of the preceeding lemmas, we need only apply the matrices H_i whose determinant is a power of a prime. $H'^{-1}BH^{-1}$ is integral and of determinant prime to μ, if and only if for each of the divisors H_i of determinant $\pi_i^{r_i}$, $H_i'^{-1}BH_i^{-1}$ is integral and of determinant prime to π_i.

In applying these conditions for a given prime π, we can replace B by any equivalent matrix. Before proceeding, we state the following two lemmas.

LEMMA 6. *For any odd prime π and integer t (> 0), if $\delta_1 = (a, 2\eta, \beta)$, f is equivalent to a form with the residue*

$$\pi^u(a'x^2+\pi^v\beta y^2) \pmod{\pi^t} \tag{4}$$

where $\pi^u \| \delta_1$, $(a'\beta', \pi) = 1$.

LEMMA 7. *For the prime $1+i$, f is equivalent to a form with residue*

$$(1+i)^u\left(a'x^2+(1+i)^v\beta'y^2\right) \pmod{(1+i)^t}$$

where $(1+i)^u \| \delta_1$, a' *and* β' *are odd, or*

$$(1+i)^u(jx^2+xy+jy^2) \pmod{(1+i)^t}$$

where $j = 0$ *or* 1.

The proofs of the above are similar to those for forms with coefficients in Z.

The second possibility in Lemma 7 is excluded here since it cannot be transformed into a sum of two squares. Since $|B|$ is a square, v is even, $(a'\beta'|\pi) = 1$ if π is odd, and $a' \equiv \beta' \pmod{(1+i)^5}$ if $\pi = 1+i$.

We apply to f, assumed to have the residue (4), the inverse of transformation (3) with $\mu_1 = \pi^r$, $\mu_2 = \pi^s$, $0 \leqslant N(\lambda) < N(\pi^s)$ and obtain a form congruent to a sufficiently high power of π to

$$f_1 = a_1x^2+2\eta_1xy+\beta_1y^2,$$

where

$$a_1 = \pi^{u-2r}a', \quad \eta_1 = -\pi^{u-2r-s}\lambda a', \quad \beta_1 = a'\lambda\pi^{u-2r-2s}+\beta'\pi^{u+v-2s}.$$

We wish to count the number of systems r, s, and λ for which $a_1\beta_1-\eta_1^2$ is prime to π and f_1 is integral and transformable into x^2+y^2.

If $\lambda = 0$, then $\eta_1 = 0$, and a_1 and β_1 must be integers prime to π. This means that $u = 2r$ and $u+v = 2s$. Clearly, $[a_1, 0, \beta_1]$ can be transformed into $[1, 0, 1]$. Since v is even, the number of systems r, s, and λ in this case is $\frac{1}{2}\left(1+(-1)^u\right)$.

We now consider $0 < N(\lambda) < N(\pi^s)$. Set $\lambda = \pi^e\mu$, with μ prime to π and $e = 0, 1, \ldots, s-1$.

If $u = 2r$, $\eta_1 = \pi^{e-s}\mu a'$ is not an integer. Hence, $u > 2r$ and η_1 must be prime to π in order that $a_1\beta_1-\eta_1^2$ shall be prime to π. Hence,

$$u+e = 2r+s, \quad \beta_1 = (a'\mu^2+\pi^{2r+v-2e}\beta')/\pi^{s-e};$$

hence, $e = r+\frac{1}{2}v$. Also, $a_1\beta_1-\eta_1^2$ is a square mod π for π an odd prime and $\pi = 1+i$. Using Lemmas 1 and 2, we can show that $[a_1, 2\eta_1, \beta_1]$ can be transformed into $[1, 0, 1]$.

Let π be an odd prime. Then $a'\mu^2+\beta \equiv 0 \pmod{\pi^{s-e}}$ has two solutions $\mu \pmod{\pi^{s-e}}$, and hence $\lambda = \pi^e\mu$ has two values $\bmod\, \pi^s$. Now r can be given any of the values $0, 1, \ldots, [\frac{1}{2}(u-1)]$; and for each value of r, s is uniquely determined by $e = r+\frac{1}{2}v$, $2r+(s-e) = u$. The number of systems r, s, λ is thus $2[\frac{1}{2}(u+1)]$. Including the case $\lambda = 0$, the number of systems is

$$\tfrac{1}{2}\left(1+(-1)^u\right)+2[\tfrac{1}{2}(u+1)] = u+1.$$

Now consider $\pi = 1+i$. Since x^2+y^2 cannot represent primitively an odd multiple of $(1+i)^k$ for $k \leqslant 4$, the same must be true of f_1. Therefore, $u-2r \geqslant 5$ and $s-e \geqslant 5$ Also, $a'\mu^2+\beta \equiv 0 \pmod{(1+i)^{s-e}}$ has two solutions $\mu \pmod{(1+i)^{s-e}}$ and $\lambda = (1+i)^e\mu$ has two values $\bmod\,(1+i)^e$. Again, r can be given any of the values $0, 1, \ldots, [\frac{1}{2}(u-5)]$; and for each value of r, s is uniquely determined by $e = r+\frac{1}{2}v$, $2r+(s-e) = u$. The number of systems r, s, λ is thus $2[\frac{1}{2}(u-3)]$. Including the case $\lambda = 0$, the number of systems is

$$\tfrac{1}{2}\left(1+(-1)^u\right)+2[\tfrac{1}{2}(u-3)] = u-3.$$

A glance at Theorem 2 in [4] shows that if π is an odd prime (of the form $a+2bi$), the number of representations of π^u as a sum of two squares is $4(1+u)$. Also, the number of representations of $(1+i)^u$ as a sum of two squares is $4\varepsilon_u$ where $\varepsilon_0 = 1$ and $\varepsilon_u = |u-3|$ if $u \geqslant 2$.

We may now summarize the preceeding results in the following theorem.

THEOREM 4. *Let $f = ax^2+2\eta xy+\beta y^2$ be a binary quadratic form with coefficients in G and $a\beta \neq 0$ which can be expressed as a sum of squares of two linear forms with coefficients in G. Also, let $f = \delta_1 f_1$ where f_1 is primitive and of square determinant μ^2. If $\mu^2 \neq 0$, the number of representations of f as a sum of squares of two linear forms is $2r_2(\delta_1)$; if $\mu^2 = 0$, the number is $r_2(\delta_1)$. Here, $r_2(\delta_1)$ denotes the number of representations of δ_1 as a sum of squares of two Gaussian integers.*

We finish the section by proving two theorems which correspond to Theorems 2 and 3.

THEOREM 5. *Let $f = ax^2+2\eta xy+\beta y^2$ be a binary quadratic form with coefficients in G such that $a \neq 0$, $\beta = 0$ which is expressible as a sum of squares of two linear forms. Also, let $f = \delta_1 f_1$ where f is primitive and of square determinant μ^2. If $\mu^2 \neq 0$, the number of representations of f as a sum of squares of two linear forms is $2r_2(\delta_1)$; if $\mu^2 = 0$, the number is $r_2(\delta_1)$.*

Proof. If $\mu^2 = 0$, then $\eta = 0$ and $\delta_1 = a$. In this case, $f = ax^2$ and the number of representations of f as a sum of two squares is clearly $r_2(a)$ or $r_2(\delta_1)$.

If $\mu^2 \neq 0$, then $\eta \neq 0$. For each a_1, a_2 in G such that $a = a_1^2+a_2^2$ and η is divisible by a_1+ia_2 or a_1-ia_2, we have $\eta = (a_1+ia_2)\beta_1$ or $(a_1-ia_2)\beta_1$. Thus, β_1 is determined as is β_2 such that $0 = \beta_1^2+\beta_2^2$. The number of representations of f as a sum of two squares is twice the number of representations of a as $a_1^2+a_2^2$ such that η is divisible by a_1+ia_2 or a_1-ia_2. This is just the number of representations of δ_1 as a sum of two squares.

THEOREM 6. *Let $f = ax^2+2\eta xy+\beta y^2$ be a binary quadratic form with coefficients in G such that $a = \beta = 0$ which can be expressed as a sum* *of squares of two linear forms. The number of representations of f as a sum of two squares is $r_2(2\eta)$.*

Proof. If $\eta = 0$, $r_2(2\eta) = r_2(0)$ is infinite as is the number of representations of f as a sum of two squares. Suppose $\eta \neq 0$. From Theorem 3 we see that η must be even, and with every factorization $\eta = 2\alpha_1\beta_1$ there is associated a representation of f as a sum of squares of two linear forms. We have only to count the number of factors α_1, β_1. We may write $2\eta = i^r(1+i)^s\pi_1^{k_1}\pi_2^{k_2}\ldots\pi_n^{k_n}$ where the π_i are odd primary primes, $r = 0, 1, 2$, or 3, and $s \geqslant 4$. The number of factors of $2\eta/4$ is then $4(s-3)(k_1+1)\ldots(k_n+1)$ which is just $r_2(2\eta)$.

References

[1] G. L. Dirichlet, *Recherches sur les formes quadratiques à coefficients et à indéterminées complexes*, Journ. Math. 24 (1842), pp. 291-371.

[2] Ivan Niven, *Integers of quadratic fields as sums of squares*, Trans. Amer. Math. Soc. 48 (1940), pp. 405-417.

[3] — *A note on the number theory of quaternions*, Duke Math. Journ. 13 (1946), pp. 397-400.

[4] Gordon Pall, *Sums of two squares in a quadratic field*, Duke Math. Journ. 18 (1951), pp. 399-409.

[5] — *Representation by quadratic forms*, Canad. Journ. Math. 1 (1949), pp. 344-364.

[6] L. W. Reid, *The Elements of the Theory of Algebraic Numbers*, New York 1910.

THE UNIVERSITY OF GEORGIA
Athens, Georgia

Reçu par la Rédaction le 23. 1. 1968

ACTA ARITHMETICA
XV (1968)

On a problem of P. Erdös and S. Stein

by

P. Erdös and E. Szemerédi (Budapest)

The system of congruences

$$a_i(\operatorname{mod} n_i), \quad n_1 < \ldots < n_k \tag{1}$$

is called a *covering system* if every integer satisfies at least one of the congruences (1). An old conjecture of P. Erdös states that for every integer c there is a covering system with $n_1 = c$. Selfridge and others settled this question for $c \leqslant 8$. The general case is still unsettled and seems difficult.

A system (1) is called *disjoint* if every integer satisfies at most one of the congruences (1). It is trivial that in a disjoint system we must have

$$(n_i, n_j) > 1 \quad \text{and} \quad \sum_{i=1}^{k} 1/n_i \leqslant 1.$$

It is known that a disjoint system can never be covering [2] and that for a disjoint system we have [3]

$$\sum_{i=1}^{k} \frac{1}{n_i} \leqslant 1 - \frac{1}{2^k}. \tag{2}$$

(2) is easily seen to be best possible.

Denote by $f(x)$ the largest value of k for which there exists a disjoint system (1) satisfying $n_k \leqslant x$. P. Erdös and S. Stein conjectured that $f(x) = o(x)$.

The main purpose of this paper will be to prove this conjecture. In fact, we prove the following

THEOREM 1. *For every $\varepsilon > 0$ if $x > x_0(\varepsilon)$ we have* ($c_1, c_2, \ldots$ denote suitable positive constants)

$$\frac{x}{\exp\left((\log x)^{1/2+\varepsilon}\right)} < f(x) < \frac{x}{(\log x)^{c_1}}. \tag{3}$$