QUATERNIONS AND SUMS OF THREE SQUARES.*

By GORDON PALL.

1. U. V. Linnik [1] has given essentially the following result:

THEOREM 1. *Let p be an odd prime. Denote by $r(m)$ the number of pure and proper quaternions $x = i_1x_1 + i_2x_2 + i_3x_3$ of norm m, where m is a positive integer such that*

$$m \neq 4k \text{ or } 8k+7, \text{ and } (-m \mid p) = 1. \tag{1}$$

Let x_0 be a solution of the congruence $x_0^2 \equiv -m \pmod{p}$. For each x consider the right-divisor (unique up to a left unit factor) of $x_0 + x$:

$$x_0 + x = zt, \; z \text{ and } t \text{ integral quaternions}, \; Nt = p. \tag{2}$$

Then, if m is sufficiently large, every quaternion t of norm p occurs among the $r(m)$ equations (2).

Linnik's proof is rather ingenious, but contains a serious error, in that on p. 377 he states that "the number of representations of a given binary quadratic form of determinant D as a sum of three squares does not exceed $c_\epsilon D^\epsilon$," and "this can be proved by methods similar to those of Gauss." This statement is false for forms of the type $kh^2(l\xi^2 + 2m\xi\eta + n\eta^2)$ if h is large (see our (41)); and Linnik applies [2] it for forms in which kh^2 may be as large as $\Delta^{1/2}$, $\Delta = ln - m^2$. Direct application, in his article, of the true result introduces a large factor which would seem to vitiate his proof.

In this article we shall revise his proof (which covers nineteen pages, and contains duplications, misprints, and superfluous details), and apply recent results [3] of our own to complete his demonstration of Theorem 1.

To facilitate comparison with Linnik's Russian paper we add the following remarks. His result, tantamount to Theorem 1, is stated on page 365. He does not formulate it as a separate theorem, but remarks that its proof is the

* Received June 4, 1941.

[1] "On the representation of large numbers by positive ternary quadratic forms," *Bull. of the Acad. of Sci. of the USSR, math. ser.*, vol. 4 (1940), pp. 363-402 (Russian).

[2] *Ibid.*, pp. 377 and 382.

[3] References will be made to Pall I and II: I. "On the arithmetic of quaternions," *Transactions of the American Mathematical Society*, vol. 47 (1940), pp. 487-500; II. "On the rational automorphs of $x_1^2 + x_2^2 + x_3^2$," *Annals of Mathematics*, vol. 41 (1940), pp. 754-766.

chief difficulty. The proposition which he applies our Theorem 1 to prove, and which is correct in view of our work, is as follows:

Let f be a positive ternary form with the invariants $\Omega = p$, $\Delta = 1$, where p is an odd prime. Let $(-f \mid p) = 1$. Then every large integer m prime to p and consistent with the generic conditions of f, is represented by f at least $c_1 h(-m)/(\log\log m \cdot \log\log\log m)$ times.

On pages 390-401 he somewhat sketchily extends this result (with m prime to 2Ω) to forms f of invariants $(\Omega, 1)$, where Ω is odd and contains at least one odd prime factor p such that $(-f \mid p) = 1$. His proof involves generalized quaternions, and contains the same errors as in the earlier case. The correction of these errors may be more difficult.

2. Notations. The letters $a, \cdots, e, t, \cdots, z$, and K, L denote integral quaternions of the type $a = a_0 + i_1 a_1 + i_2 a_2 + i_3 a_3$ with rational integers a_i; and $i_a^2 = -1$, etc. Latin letters $f, \cdots, s$, and letters with subscripts (except the quaternion units i_a) denote rational integers. The letters $\kappa_1, \kappa_2, \cdots$ denote positive constants independent of m, and depending at most on p and ϵ. Here ϵ is any given positive number.

We call a *pure*, or a *vector*, if $a_0 = 0$; *proper* if $(a_0, a_1, a_2, a_3) = 1$, *proper* (mod k) if $(a_0, a_1, a_2, a_3, k) = 1$. The norm Σa_i^2 of a is written Na; the real part a_0, $\mathcal{R}(a)$. Every a has eight left-associates $\pm a$, $\pm i_a a$; we may speak of these as "one quaternion" instead of eight.

3. By adjusting unit factors we can confine t in (2) to $p+1$ non-left-associate quaternions of norm p. Let us assume, for the sake of contradiction, that *one of these values t is missing among all $r(m)$ equations* (2). Then $\bar{t}$ (or its associate) is also missing. For (2) implies

$$x_0 + y = z\bar{t}, \qquad y = -txt^{-1}, \tag{3}$$

where y is evidently pure, integral, and of norm m; also, y is proper, since a prime dividing y would divide m $(= Ny)$ and px $(= -\bar{t}yt)$.

Our assumption implies further that if $x_0^2 + m \equiv 0 \pmod{p^s}$, and we consider divisors v of norm p^s,

$$x_0 + x = uv, \qquad Nv = p^s, \tag{4}$$

and factor v as $\theta t' t'' \cdots t^{(s)}$ ($\theta = \pm 1$ or $\pm i_a$), then neither t nor $\bar{t}$ occurs among these factors of norm p. For, from

$$x_0 + x = atb, \qquad Nb = p^r, \qquad r \geqq 0, \tag{5}$$

follows $x_0 + bxb^{-1} = bat$, where bxb^{-1} is another x.

Linnik has the happy idea of choosing s variable with m:

$$m^{\frac{1}{2}+\tau} \leqq p^s < pm^{\frac{1}{2}+\tau}, \tag{6}$$

where τ is the fixed fraction (between 0 and 1/5)

$$\tau = -\tfrac{1}{2}\log(1-p^{-1})/\log p. \tag{7}$$

Hence $p^{-2\tau} = 1 - 1/p$, and we have

$$p(p-1)^{s-1} < 2p^s(1-1/p)^s = 2(p^s)^{1-2\tau} < \kappa_1 m^{\frac{1}{2}-2\tau^2}. \tag{8}$$

Hence the number n of distinct divisors v which can occur in the $r(m)$ equations (4) cannot exceed $8\kappa_1 m^{\frac{1}{2}-2\tau^2}$. For, t' cannot be t (by our assumption), and t'' can be neither t nor $\bar{t}$ nor $\bar{t}'$, at least two of these being non-left-associate, and so on; (if $\bar{t}'$ and t'' were associates, v would be improper). We may observe that, s being variable, $p(p-1)^{s-1}$ is not of the same order of size as the full number $p^s + p^{s-1}$ of proper quaternions of norm p; this is the crucial point in Linnik's method.

Let these n distinct v's occur, respectively, for $a_1, a_2, \cdots, a_n$ distinct vectors x. Accordingly,

$$a_1 + \cdots + a_n = 8r(m), \qquad n < 8\kappa_1 m^{\frac{1}{2}-2\tau^2}. \tag{9}$$

We shall use the result of C. L. Siegel [4] that

$$\kappa_2 m^{\frac{1}{2}-\epsilon} < r(m) < \kappa_3 m^{\frac{1}{2}+\epsilon}. \tag{10}$$

Hence $a_1^2 + \cdots + a_n^2 \geqq (a_1 + \cdots + a_n)^2/n \geqq \kappa_4 m^{1-2\epsilon}/m^{\frac{1}{2}-2\tau^2}$, or

$$a_1^2 + \cdots + a_n^2 \geqq \kappa_4 m^{\frac{1}{2}+2\tau^2-2\epsilon}. \tag{11}$$

We shall ultimately prove that (without any assumption)

$$a_1^2 + \cdots + a_n^2 < \kappa_5 m^{\frac{1}{2}+\epsilon} \tag{12}$$

and shall thus obtain the desired contradiction.

We observe, as in connection with (3), that $\bar{v}$ occurs exactly as often as v. Let us call (x, y) a *conjugate pair* if x and y are proper vectors of norm m, and any right-divisors of norm p^s of $x_0 + x$ and of $x_0 + y$ are conjugates. The number of conjugate pairs is $a_1^2 + \cdots + a_n^2$.

4. Pairs (x, y) associated with binary quadratic forms. We formulate a result from a recent article [5] (Linnik uses a similar result due to Venkov).[6] Let $m > 1$, and let $[x]$ denote a set of four proper vectors

---

[4] "Über die Classenzahl quadratischer Zahlkörper," *Acta Arithmetica*, vol. 1 (1935), pp. 83-86.

[5] Pall I, pp. 495-497. The writer did not then know of Venkov's result.

[6] B. Venkov, "On the arithmetic of quaternions," *Bull. Acad. Sci. USSR*, VI series, vol. 16 (1922), pp. 205-246 (Russian).

$$(13)\qquad \begin{matrix} x = i_1x_1 + i_2x_2 + i_3x_3, & -i_1xi_1 = i_1x_1 - i_2x_2 - i_3x_3, \\ -i_2xi_2 = -i_1x_1 + i_2x_2 - i_3x_3, & -i_3xi_3 = -i_1x_1 - i_2x_2 + i_3x_3, \end{matrix}$$

of norm m. With every class of properly primitive binary quadratic forms ϕ of determinant m is associated a process, expressed by (15) and (16), whereby every $[x]$ is carried into a unique $[y]$, and no two distinct $[x]$'s go into the same $[y]$. For a fixed $[x]$, as ϕ ranges over the p. p. classes of determinant m, $[y]$ ranges over all proper y's of norm m such that

$$(14)\qquad \begin{matrix} y \equiv x \pmod 2, & \text{if } m \equiv 1 \text{ or } 2 \pmod 4, \\ [y] \not\equiv [-x] \pmod 4, & \text{if } m \equiv 3 \pmod 8. \end{matrix}$$

That is, y runs over $\frac{1}{8}$ or $\frac{1}{2}$ of all proper vectors of norm m.

If $\phi = [k, 2h, l]$, $h^2 + m = kl$, the process is defined by

$$(15)\qquad h + x = KL, \qquad h + y = LK,$$

$$(16)\qquad y = LxL^{-1} = K^{-1}xK,$$

where K and L are respectively of norms k and l.

5. Conditions for conjugate pairs associated with ϕ. Besides (15)-(16) if (x, y) is a conjugate pair associated with ϕ,

$$(17)\qquad x_0 + x = uv, \qquad x_0 + y = u^*\bar{v},$$

$$(18)\qquad x_0^2 + m = qp^s, \qquad Nu = q = Nu^*,$$

$$(19)\qquad Lx = yL, \qquad \bar{K}x = y\bar{K}.$$

If we replace x_0 by p^s, q becomes $q + 2x_0 + p^s$. We thus secure

$$(20)\qquad (q, p) = 1.$$

We can take ϕ to be reduced, and hence

$$(21)\qquad 2\,|\,h\,| \leqq k \leqq l, \qquad kl \leqq 4m/3, \qquad k^2 \leqq 4m/3.$$

LEMMA 1. *Let $m > m_1(p)$. For any conjugate pair associated with ϕ,*

$$(22)\qquad vK \text{ is pure, and } p^s \mid \mathfrak{R}(v\bar{L}).$$

For, $L(x_0 + x) = (x_0 + y)L$, or $Luv = u^*\bar{v}L$. Since $(q, p) = 1$, $\bar{v}L$ has the same right-divisors of norm p^s as $u^*\bar{v}L$.[7] We can set

$$(23)\qquad \bar{v}L = wv, \qquad \bar{v}\bar{K} = w'v.$$

[7] Pall I, p. 488, Lemma 2.

Hence v is a right-divisor of the quaternion $z = \bar{v}L$, and of $\bar{z}$, and of $z + \bar{z} = 2z_0$. Hence $2z_0 = ev$, $p^s \mid 2z_0\bar{v}$ where $\bar{v}$ is proper, $p^s \mid z_0$:

$$p^s \mid \mathcal{R}(\bar{v}L), \qquad p^s \mid \mathcal{R}(\bar{v}\bar{K}). \tag{24}$$

Trivially, $\mathcal{R}(\bar{v}\bar{K}) = \mathcal{R}(vK) = \mathcal{R}(Kv) = \mathcal{R}(\bar{K}\bar{v})$. By (21_3) and (6),

$$|\mathcal{R}(vK)| \leqq (Nv \cdot NK)^{\frac{1}{2}} = (p^s k)^{\frac{1}{2}} < k_6 m^{\frac{1}{2}+\frac{1}{2}\tau}. \tag{25}$$

Since $p^s \geqq m^{\frac{1}{2}+\tau}$, (22_1) follows. For $v\bar{L}$ we have similarly

$$|\mathcal{R}(v\bar{L})| < p^{\frac{1}{2}} m^{\frac{1}{4}+\frac{1}{2}\tau} l^{\frac{1}{2}};$$

and would have $\mathcal{R}(v\bar{L}) = 0$ if $l < 2m^{\frac{1}{2}+\tau-\eta}$ with $\eta > 0$. Hence:

LEMMA 2. *If for $\eta = \tau^2$, or for any fixed $\eta > 0$, we have*

$$k \geqq m^{\frac{1}{2}-\tau+\eta}, \tag{26}$$

then $v\bar{L}$ is pure for $m > m_2(p, \eta)$.

Since v and K are proper,[7a] we can set

$$\begin{aligned} &v = v't, \quad K = \bar{t}K', \quad Nt = p^\sigma, \quad 0 \leqq \sigma \leqq s, \quad Nv' = p^{s-\sigma}, \\ &NK' = k' = k/p^\sigma, \text{ while } v'K' \text{ is proper and pure.} \end{aligned} \tag{27}$$

The number of distinct values σ cannot exceed $\kappa_7 \log m < \kappa_8 m^\epsilon$.

From (15)-(19) we obtain

$$\begin{aligned} &x_0 + x = uv't, \quad x_0 + y = u^*\bar{t}\bar{v}', \quad h + x = \bar{t}K'L, \\ &h + y = L\bar{t}K', \quad \bar{K}'tx = y\bar{K}'t. \end{aligned} \tag{28}$$

Hence $x' = txt^{-1}$ is a proper vector of norm m, and

$$x_0 + x' = tuv', \qquad K'y = x'K', \qquad h + x' = K'L\bar{t}. \tag{29}$$

Now $v'K' = -ed$, where $e = \bar{K}'$, $d = \bar{v}'$. Hence we have

$$-etued = etuv'K' = e(x_0 + x')K' = k'(x_0 + y), \text{ or} \tag{30}$$

$$k' \mid etued. \tag{31}$$

Since ed is proper, the greatest common left-divisor of K' and d is 1, and we can solve $K'z + dw = 1$ in integral z and w. Hence

$$k' \mid etuedw = etue(1 - K'z), \qquad k' \mid etue, \qquad \text{or}$$

$$\bar{K}'tu = z'K', \qquad z' \text{ integral}. \tag{32}$$

[7a] Pall I, p. 491, Theorem 5.

Since K' is proper, it follows as in (23) that $k' \mid \mathfrak{R}(etu)$, or

$$\bar{K}'tu = fk' + i_1b_1 + i_2b_2 + i_3b_3 = fk' + b, \tag{33}$$

where f, b_1, b_2, b_3 are rational integers. We also set

$$v'K' = i_1a_1 + i_2a_2 + i_3a_3 = a. \tag{34}$$

By (30) the real part of $(fk' + b)a = etuv'K'$ is $k'x_0$. Hence by forming the norm of $\bar{a}\xi + (fk' + b)\eta$ in two ways we obtain

$$\begin{aligned} k'(p^{s-\sigma}\xi^2 + 2x_0\xi\eta + p^\sigma q\eta^2) - (fk')^2\eta^2 \\ = (a_1\xi - b_1\eta)^2 + (a_2\xi - b_2\eta)^2 + (a_3\xi - b_3\eta)^2. \end{aligned} \tag{35}$$

Thus every conjugate pair associated with ϕ leads for some σ to a representation of $k'\psi$ as a sum of three squares, where

$$\psi = [p^{s-\sigma},\ 2x_0,\ p^\sigma q - f^2k']. \tag{36}$$

However, only those representations in which

(37) a is proper, and a, b have the same right-divisors of norm k',

need be considered in connection with conjugate pairs. We have

(38) the determinant of ψ is equal to $m - p^{s-\sigma}f^2k'$,

and since this cannot be negative, (6) shows that

$$|f| \leqq m^{\frac{1}{4}-\frac{1}{2}\tau}p^\sigma/k^{\frac{1}{2}}. \tag{39}$$

Conversely, no particular complex of values f, a, b can arise for a given σ from more than 64 conjugate pairs. For v' (and therefore K') has at most eight values as a divisor of norm $p^{s-\sigma}$ of a; tu is given by (33), and as $Nt = p^\sigma$ is prime to Nu, t has at most eight values; x' and y are determined by (29), and $x = t^{-1}x't$.

6. Forms ϕ with large minima. We prove

LEMMA 3. *Let $m > m_2$. Let the minima k, k' of ϕ and ϕ' satisfy (26), and let (x, y) and (x, y') be conjugate pairs associated respectively with ϕ and ϕ'. Then $y = y'$.*

For by Lemmas 1 and 2 we can write (temporary notation)

$$\begin{aligned} Kv = a = i_1a_1 + i_2a_2 + i_3a_3, \qquad \bar{v}L = b = i_1b_1 + i_2b_2 + i_3b_3, \\ K'v = c = i_1c_1 + i_2c_2 + i_3c_3, \qquad \bar{v}L' = d = i_1d_1 + i_2d_2 + i_3d_3. \end{aligned}$$

The vector parts of ab and cd are equal:

$$Kv \cdot \bar{v}L = p^s(h + x), \qquad K'v \cdot \bar{v}L' = p^s(h' + x).$$

Hence, the first equality being determinant for determinant,

$$\begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{vmatrix} = \begin{vmatrix} c_1 & c_2 & c_3 \\ d_1 & d_2 & d_3 \end{vmatrix}, \text{ or } \begin{vmatrix} a_1 & b_1 & d_1 \\ a_2 & b_2 & d_2 \\ a_3 & b_3 & d_3 \end{vmatrix} = 0.$$

Since $ab = p^s(h + x)$ is not real, a and b are not proportional. Hence there are real numbers λ and μ such that $d = \lambda a + \mu b$, $\bar{v}L' = \lambda Kv + \mu\bar{v}L = -\lambda\bar{v}\bar{K} + \mu\bar{v}L$, or $L' = -\lambda\bar{K} + \mu L$. By (19), $L'x = yL'$, $y = L'xL'^{-1} = y'$.

COROLLARY 1. *The number of conjugate pairs associated with all forms whose minima k satisfy* (26) *is, for large m, at most $r(m) < \kappa_3 m^{\frac{3}{4}+\epsilon}$.*

7. The number of representations of a binary quadratic form as a sum of three squares. Let N be the number of solutions of

$$g(l\xi^2 + 2m\xi\eta + n\eta^2) = \sum_{i=1}^{3} (a_i\xi + b_i\eta)^2 \tag{40}$$

in integers a_i, b_i. Here $\psi = [l, 2m, n]$ may be assumed to be positive, and properly or improperly primitive, $\Delta = ln - m^2$, and $g > 0$. There is a general formula of C. L. Siegel [8] for questions of this sort, by which it is necessary only to calculate explicitly the number of solutions of certain systems of congruences. This was done for (40) (among other examples) by Hel Braun [9] in the case $g^2\Delta$ odd, and our results agree with hers for that case. The general result for (40) is as follows:

$$N = 24 \prod_p \chi(p), \text{ where} \tag{41}$$

$$\chi(p) = \tfrac{1}{2}[1 + (-\sigma \mid E)(-\tau\alpha \mid k\psi)] \text{ if } p = 2,$$
$$= (1 + \zeta^\delta\eta^\gamma)(p^{[(\gamma+1)/2]} - 1)/(p - 1)$$
$$+ (2 - \sigma)(1 + \zeta + \zeta^2 + \cdots + \zeta^\delta)p^{\gamma/2} \text{ if } p > 2.$$

Here the product is taken over all primes p; and for any p,

$$g = p^\gamma k, \quad \Delta = p^\delta E, \quad \gamma, \delta \geqq 0, \quad p \nmid kE, \quad \sigma = \tfrac{1}{2}(3 - (-1)^\gamma),$$
$$\tau = \tfrac{1}{2}(3 - (-1)^\delta); \ \alpha = (-1 \mid E) \text{ if } p = 2; \ \zeta = (-k\psi \mid p) \text{ and}$$
$$\eta = ((-)^{\delta+1}E \mid p) \text{ if } p > 2.$$

---

[8] "Über die analytische Theorie der Quadratischen Formen," *Annals of Mathematics*, vol. 36 (1935), pp. 527-606.

[9] "Über die Zerlegung quadratischer Formen in Quadrate," *Jour. für Math.*, vol. 178 (1937), pp. 34-64 (p. 62).

In the Legendre symbols ψ is to be replaced by any number represented by ψ and prime to p. Note that $\chi(p) = 1$ if $p \nmid 2g\Delta$.

In particular, if g is quadratfrei, so that γ is 0 or 1 for every p, $\chi(p) \leqq 1 + \delta$ if $\gamma = 0$, $\chi(p) \leqq 2$ if $\gamma = 1$, and $N/24$ does not exceed the number of divisors of $g\Delta$, which is $O(g\Delta)^{\epsilon}$.[10]

If we consider only the representations in which $(a_1, a_2, a_3, b_1, b_2, b_3) = 1$, N is not materially reduced; for $\chi(p)$ is replaced by

$$(1 + \zeta^{\delta}\eta^{\gamma})p^{[(\gamma-1)/2]} + (2 - \sigma)(1 + \zeta + \cdots + \zeta^{\delta})(p - 1)p^{\frac{1}{2}\gamma-1} \text{ when } \gamma \geqq 2.$$

8. Returning to (35) we write $k' = k''h^2$, where h^2 is the largest square in k', $h > 0$. Since $v'K'$ is proper and pure, $k' \not\equiv 0 \pmod 4$.

LEMMA 4. *Every representation* (35) *satisfying* (37) *is of the form*

$$a = zc\bar{z}, \qquad b = zd\bar{z}, \tag{42}$$

where z is a proper quaternion of norm h, and c and d satisfy

$$k''(p^{s-\sigma}\xi^2 + 2x_0\xi\eta + (p^{\sigma}q - f^2k')\eta^2) = \sum_{i=1}^{s}(c_i\xi - d_i\eta)^2. \tag{43}$$

By (37), $b\bar{a} \equiv 0 \pmod{k''h^2}$. Let z be the left-divisor of norm h (unique up to a right-unit factor) of the proper vector $a = zw = -\bar{w}\bar{z}$. Since $b\bar{a} \equiv 0 \pmod h$, Theorem 5′ of a recent article [11] shows that $b = zw'$. Then $ww' \equiv 0 \pmod h$, w is proper, and $h \mid Nw$. The right-divisor of w must be $\bar{z}$, and we have (42). By (42) and (35), $Nc = (Na)/h^2 = k''p^{s-\sigma}$, $Nd = (Nb)/h^2 = (k'qp^{\sigma} - (fk')^2)/h^2 = k''(qp^{\sigma} - f^2k')$, $-\Sigma c_id_i = \mathfrak{R}(cd) = \mathfrak{R}(zc\bar{z}zd\bar{z})/h^2 = \mathfrak{R}(ab)/h^2 = x_0k'/h^2 = x_0k''$.

Since d may be improper we write $k'' = k_1k_2$, $d = k_1d'$, where d' is proper (mod k_2). We note that if $k'' \equiv 2 \pmod 4$, then $2 \mid \mathfrak{R}(cd)$, $4 \mid N(cd)$, hence $2 \mid cd$. We shall prove that (43) implies

$$dc = k''x_0 + k''y', \ y' \text{ pure and integral.} \tag{44}$$

For we have $k'' \mid Nc$, $k'' \mid Nd$, $k'' \mid \Sigma c_id_i$. Hence k_2 divides each of Nc, Nd', and $\Sigma c_id'_i$, where c and d' are proper. By Corollary 10,[12] k_2 divides the vector part of $d'c$; hence k'' divides the vector part of dc. By (43),

$$Ny' = m - p^{s-\sigma}f^2k''h^2. \tag{45}$$

---

[10] For example see Hardy and Wright, *Theory of Numbers*, Clarendon Press (1938), p. 259.

[11] Pall I, p. 492.

[12] Pall I, p. 493.

The condition $b\bar{a} \equiv 0 \pmod{k''h^2}$ requires that we find the number of proper quaternions z of norm h such that $zdc\bar{z} \equiv 0 \pmod{k''h}$, that is, by (44), such that $zy'\bar{z} \equiv 0 \pmod{h}$. Write $y' = h_1 y''$, $h = h_1 h_2$, where y'' is proper (mod h_2). We have to solve

$$zy''\bar{z} \equiv 0 \pmod{h_2}, \quad Nz = h, \quad z \text{ proper.} \tag{46}$$

By (45) we see that $h_1^2 \mid m$ and that $Ny'' \equiv m/h_1^2 \pmod{h_2}$.

9. On the congruence (46). We recently proved [13]

LEMMA 5. *Let x be a proper vector of norm n, h be odd and positive. The proper quaternions t of norm h such that $tx\bar{t} \equiv 0 \pmod{h}$ are the same as the right-divisors of norm h of $x_0 + x$, where x_0 ranges over the solutions $x_0 \pmod{h}$ of $x_0^2 \equiv -n \pmod{h}$.*

Let π be an odd prime. Varying our notations somewhat, we denote by t_r in this section *any* proper quaternion of norm π^r. In Lemmas 6 and 7, x is pure, and proper (mod π). We have first

LEMMA 6. *If $\pi \mid Nx$ and $t_r x \bar{t}_r \equiv 0 \pmod{\pi}$, where $r \geqq 1$, then the right-divisor of norm π of t_r is the right-divisor of norm π of x.*

For we can write $t_r = t_k t_1 t_q$, where $r = k + 1 + q$, $t_q x \bar{t}_q \not\equiv 0$, $t_1 t_q x \bar{t}_q \bar{t}_1 \equiv 0 \pmod{\pi}$. By Lemma 5, t_1 is the right-divisor of $t_q x \bar{t}_q$ of norm π. This contradicts the properness of $\bar{t}_q \bar{t}_1$ unless $q = 0$.

Let ν_s be the number of solutions $x_0 \pmod{\pi^s}$ of $x_0^2 \equiv -n \pmod{\pi^s}$, where $n = Nx$. The ν_s non-left-associate solutions t_s of

$$t_s x \bar{t}_s \equiv 0 \pmod{\pi^s} \tag{47}$$

will be denoted specifically by u_s. We have

LEMMA 7. *Let $r \geqq s \geqq 0$, $r > 0$. The general solution t_r of*

$$t_r x \bar{t}_r \equiv 0 \pmod{\pi^s} \tag{48}$$

is given by $t_{r-s} u_s$ with t_{r-s} restricted only by the properness of $t_{r-s} u_s$. Hence the number of non-left-associate t_r satisfying (48) is $\pi^{r-s}\nu_s$ if $s > 0$, $\pi^{r-1} + \pi^r$ if $s = 0$.

The case $s = 0$ is trivial. Proceeding by induction assume the lemma to be true with $s - k$ ($1 \leqq k \leqq s$) in place of s. We can factor any t_r as $t_{r-s} t_s$. If (48) holds, either i) $t_s x \bar{t}_s \equiv 0 \pmod{\pi^s}$ and t_{r-s} can be taken arbitrary,

[13] Pall II, p. 763, Corollary 6.

which is what we wish to prove, or ii) $v = (t_s x \bar{t}_s)/\pi^{s-k}$ is integral, and proper (mod π) for some k, $1 \leqq k \leqq s$. By assumption, in case ii), $t_s = t_k u_{s-k}$, whence $v = t_k w \bar{t}_k$, w integral. Now $t_{r-s} v \bar{t}_{r-s} \equiv 0 \pmod{\pi^k}$, hence mod π), and by Lemma 6, the right-divisor of norm π of t_{r-s} is equal to that of v, hence to that of $\bar{t}_k$. This implies that t_r is improper, so that case ii) is impossible.

COROLLARY 2. *Let π^q $(q \geqq 0)$ be the highest power of π dividing y'. The number of quaternions t_r such that $t_r y' \bar{t}_r \equiv 0 \pmod{\pi^r}$ is*

$$\pi^{r-1}(\pi+1) \text{ if } q \geqq r \geqq 1, \quad \pi^q \nu \text{ if } q < r, \tag{49}$$

where ν is the number of solutions α of $\alpha^2 \equiv -N(y'/\pi^q) \pmod{\pi^{r-q}}$.

COROLLARY 3. *If y' is replaced by $\lambda a y' \bar{a}$ where $(\lambda N a, \pi) = 1$, the number of quaternions t_r in Corollary 2 is unchanged.*

Write $h = \pi_\mu^{r_\mu} \cdots \pi_2^{r_2} \pi_1^{r_1}$ in powers of distinct odd primes. Every proper z of norm h can be factored (uniquely up to left unit factors) as $z_\mu \cdots z_2 z_1$, with z_i of norm $\pi_i^{r_i}$. The congruence (46) becomes

$$z_\mu \cdots z_2 z_1 y' \bar{z}_1 \bar{z}_2 \cdots \bar{z}_\mu \equiv 0 \pmod{\pi_1^{r_1} \cdots \pi_\mu^{r_\mu}},$$

and reduces to the sequence of congruences

$$z_1 y' \bar{z}_1 \equiv 0 \pmod{\pi_1^{r_1}}, \; z_2 (z_1 y' \bar{z}_1) \bar{z}_2 \equiv 0 \pmod{\pi_2^{r_2}}, \cdots;$$

and the numbers of solutions are, by Corollary 3, respectively the same as those of $z_i y' \bar{z}_i \equiv 0 \pmod{\pi_i^{r_i}}$, $(i = 1, 2, \cdots, \mu)$.

COROLLARY 4. *The number of solutions of (46) does not exceed $2^{\nu(h_1)} h_1 \xi$, where ξ is the number of solutions α of*

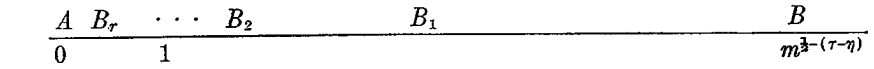
$$\alpha^2 \equiv -m/h_1^2 \pmod{h_2}. \tag{50}$$

Here $\nu(n)$ denotes the number of distinct prime factors of n, and we recall that $2^{\nu(n)} \leqq d(n) = O(n^\epsilon)$, where $d(n)$ is the number of divisors of n.

As for ξ, we have $\xi \leqq 2^{\nu(h_3)} h_3^{1/2}$, where $h_3 = (h_2, m/h_1^2)$. Hence the number of solutions of (46) does not exceed

$$(d(h))^2 \cdot (h_1^2 h_3)^{1/2} \leqq (d(h))^2 \rho^{1/2}, \text{ where } \rho = (m, k') = (m, k). \tag{51}$$

10. We count the conjugate pairs. Linnik classifies the values k not satisfying (26) into r intervals $B_i B_{i-1}$ where $r < \kappa_9 \log m < \kappa_{10} m^\epsilon$, as follows:



Here $AB_1 = m^{\frac{1}{2}-\nu_1} = \frac{1}{2}m^{\frac{1}{2}-(\tau-\eta)}$, $AB_2 = m^{\frac{1}{2}-\nu_2} = \frac{1}{2}m^{\frac{1}{2}-\nu_1}, \cdots, AB_r = m^{\frac{1}{2}-\nu_r} = \frac{1}{2}m^{\frac{1}{2}-\nu_{r-1}}$, $\frac{1}{2} \leqq m^{\frac{1}{2}-\nu_r} = AB_r < 1$, $\tau - \eta < \nu_1 < \nu_2 < \cdots < \nu_r$.

Suppose then that we have

$$\frac{1}{2}m^{\frac{1}{2}-\nu} < k \leqq m^{\frac{1}{2}-\nu} \left(\leqq m^{\frac{1}{2}-(\tau-\eta)}\right). \tag{52}$$

Linnik states incorrectly that the number of reduced forms of determinant m with a given minimum k ($< m^{\frac{1}{2}}$) does not exceed $\kappa_{11}\, m^{\epsilon}$. The following example shows that this is false: $m = 2 \cdot 3^{4n}$, $k = 3^{2n}$, and the $2 \cdot 3^{n-1}$ forms $[3^{2n}, \pm 2 \cdot 3^n j, j^2 + 2 \cdot 3^{2n}]$ with $|j| \leqq 3^n/2$, $3 \nmid j$. The true result is that the number of such forms is equal to the number of solutions of $\alpha^2 \equiv -m \pmod{k}$, hence does not exceed $2^{\nu(k)}(k, m)^{\frac{1}{2}}$.

The number of sets of forms with k in (52) having a fixed value for $\rho = (k, m)$ is $d(m) < \kappa_{12}\, m^{\epsilon}$; and for a given σ (where $\rho^{\sigma} \mid k$), the number of values k with given ρ does not exceed $m^{\frac{1}{2}-\nu}/\rho p^{\sigma}$. The number of values of f is bounded in (39), where we can replace k by $\frac{1}{2}m^{\frac{1}{2}-\nu}$. Lastly, the number of values a, b does not exceed the number of values c, d satisfying (43) (which is $\leqq 24 d(g_1) < \kappa_{13}\, m^{\epsilon}$, $g_1 = k''(m - p^{s-\sigma}f^2k')$) multiplied by the number of solutions z of (46), which we bounded in (51). Putting these together we see that the number of conjugate pairs associated with all forms not satisfying (26) does not exceed

$$\kappa_{14}\, \frac{m^{\frac{1}{2}-\nu}}{p^{\sigma}\rho}\, \rho^{\frac{1}{2}}\rho^{\frac{1}{2}}\, \frac{p^{\sigma} m^{\frac{1}{4}-\frac{1}{2}\tau}}{m^{\frac{1}{4}-\frac{1}{2}\nu}}\, (m^{\epsilon})^{\tau} = \kappa_{14}\, m^{\frac{1}{2}-\frac{1}{2}\nu-\frac{1}{2}\tau+7\epsilon}$$

for the least value of ν, which is $\tau - \eta$, hence $< \kappa_{15}\, m^{\frac{1}{2}-\tau+\frac{1}{2}\eta+\epsilon}$.

Comparing this with the result of § 6, we have (12).

McGill University,
Montreal.