ACTA ARITHMETICA
136.3 (2009)

Universality of a non-classical integral quadratic form over $\mathbb{Q}(\sqrt{5})$

by

Jesse Ira Deutsch (Rockville, MD)

1. Introduction. Representations of integers by quadratic forms have been of interest since the 17th century. Fermat, Euler and Lagrange worked on representations of such forms as x^2+y^2, x^2+2y^2 and $x^2+y^2+z^2+w^2$ over the rational integers. Gauss discovered those integers expressible by the sum of three squares. In the 19th century further results were obtained on a variety of quadratic forms. This included finding the number of representations of an integer by some of the above-mentioned forms. See Dickson [7, Ch. X] for more background and information.

In the early 20th century, Götzky showed that the sum of four squares represented all totally positive integers in the field of $\mathbb{Q}(\sqrt{5})$. Later Cohn proved that the sum of four squares represented all totally positive integers in $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ with even coefficients on the radical. Using theta functions and modular forms, Götzky and Cohn were able to get the number of such representations. See Götzky [8] and Cohn [2, 3, 4] for details.

We say that a form is *universal* if it represents all totally positive integers in a given number field. Also, we define classical quadratic forms as those that have cross product terms divisible by 2.

Other results during and just before the 20th century included proofs of the universality of the sum of four squares by different methods, for example, quaternion algebras and the Geometry of Numbers. In the 1990's demonstrations of universality of quadratic forms over quadratic number fields were developed using the theory of lattices and p-adic numbers. The situation for classical forms with three variables over real quadratic fields was completely determined (see Kim, Chan and Rhagavan [11]). Very recently, the case of classical forms of four variables over $\mathbb{Q}(\sqrt{5})$ was resolved (see Lee [12]).

2000 *Mathematics Subject Classification*: Primary 11E25, 11D57.
Key words and phrases: quadratic form, universality, quaternions.

DOI: 10.4064/aa136-3-3 © Instytut Matematyczny PAN, 2009

In 2002 the author was able to prove the universality portion of Götzky's result using Geometry of Numbers. The existence of representations for Cohn's result in the ring $\mathbb{Q}(\sqrt{2})$ and another proof for $\mathbb{Q}(\sqrt{5})$ were later developed by the author using both quaternion rings and Geometry of Numbers. In the current paper, these results are extended to an integral quaternary quadratic form over $\mathbb{Q}(\sqrt{5})$. It is believed that the main result of this paper is new, and is the first case of the universality of an integral nonclassical form over a quadratic field. See Deutsch [5, 6] for details on the earlier results.

We follow the notation of Deutsch [6] for quaternions and quadratic fields. A quick review of that notation suffices. Bold Roman font will be used for quaternions, e.g. $\mathbf{q}$ is a typical quaternion. The ring of all quaternions is denoted $\mathbb{H}$. Each element of $\mathbb{H}$ has a conjugate, denoted $\overline{\mathbf{q}}$. There is a quaternionic norm $N(\mathbf{q}) = \mathbf{q} \cdot \overline{\mathbf{q}}$, sometimes called the *reduced norm*.

Lower case Roman letters will be used for real numbers or variables. Lower case Greek letters will correspond to elements of a real quadratic field. The conjugate with respect to the field is denoted by a star, e.g. α^* is the conjugate of α. The field norm is defined as $N(\alpha) = \alpha \cdot \alpha^*$. The context will make clear whether the field norm or the quaternionic norm is being used.

In addition, for a real ring R and quaternions $\mathbf{q}_1, \ldots, \mathbf{q}_4$, the R-module generated by these quaternions is denoted $R[\mathbf{q}_1, \mathbf{q}_2, \mathbf{q}_3, \mathbf{q}_4]$. For example, the Hurwitz quaternions are defined as $H = \mathbb{Z}[\mathbf{1}, \mathbf{i}, \mathbf{j}, (\mathbf{1} + \mathbf{i} + \mathbf{j} + \mathbf{k})/2]$. The last module generator in this list is called $\mathbf{h}$ in honor of Hurwitz. H can be shown to be a norm Euclidean ring. Further details are found in Hurwitz [10], Deutsch [6], Baake and Moody [1].

2. The quadratic form G. We now introduce the quadratic form under consideration. Set $g(x, y) = x^2 + xy + y^2$, and let $G(x, y, z, w) = g(x, y) + g(z, w)$. The universality of G ought to present a smaller problem in some sense to that of the universality of the sum of four squares. The form analogous to g for the sum of four squares is simply the sum of two squares $f(x, y) = x^2 + y^2$. Note that the discriminants of the related nonhomogeneous quadratic forms $x^2 + x + 1$ and $x^2 + 1$ are 3 and 4 respectively. It should be pointed out that in Dickson's chapter on quadratic forms, G is practically the first form to be claimed universal over $\mathbb{Z}$ (see Dickson [7, Ch. X]).

Set $\boldsymbol{\varrho} = (1 + \sqrt{3}\,\mathbf{i})/2$. Then the $\mathbb{Z}$-module generated by 1 and $\boldsymbol{\varrho}$ is the ring of integers of the field $E = \mathbb{Q}(\sqrt{-3})$. It is easy to see that the norm of a typical element of E, namely $x + y\boldsymbol{\varrho}$, is simply $g(x, y)$. Applying the general product identity for norms over the complex numbers, we find that there is

a formula of the type

$$g(x_1, y_1) \cdot g(x_2, y_2) = g(X, Y). \tag{2.1}$$

Note that X and Y must arise from the product of the corresponding elements in the field E. More specifically, we find that

$$(x_1^2 + x_1y_1 + y_1^2) \cdot (x_2^2 + x_2y_2 + y_2^2) = X^2 + XY + Y^2, \tag{2.2}$$

where

$$X = x_1x_2 - y_1y_2, \quad Y = x_1y_2 + x_2y_1 + y_1y_2. \tag{2.3}$$

Also, using the quaternion module $\mathbb{Q}(\sqrt{3}\,\mathbf{i}) \oplus \mathbf{j} \cdot \mathbb{Q}(\sqrt{3}\,\mathbf{i})$ we get a similar result for $g(x, y) + g(z, w)$. More precisely, with $\boldsymbol{\varrho} = (1 + \sqrt{3}\,\mathbf{i})/2$ we are looking at the $\mathbb{Z}$-module generated by $[\mathbf{1}, \boldsymbol{\varrho}, \mathbf{j}, \mathbf{j} \cdot \boldsymbol{\varrho}]$. The norm identity for quaternion products analogous to (2.1), (2.2) and (2.3) becomes

$$\begin{aligned}(x_1^2 + x_1y_1 + y_1^2 + z_1^2 + z_1w_1 + w_1^2) \cdot (x_2^2 + x_2y_2 + y_2^2 + z_2^2 + z_2w_2 + w_2^2)\\ = X^2 + XY + Y^2 + Z^2 + ZW + W^2,\end{aligned} \tag{2.4}$$

where

$$\begin{aligned} X &= x_1x_2 - y_1y_2 - w_1w_2 - w_1z_2 - z_1z_2,\\ Y &= x_1y_2 + x_2y_1 + y_1y_2 + w_1z_2 - w_2z_1,\\ Z &= -y_1z_2 - x_1z_2 - x_2z_1 + w_1y_2 - w_2y_1,\\ W &= y_1z_2 - y_2z_1 - w_1y_2 - w_1x_2 - w_2x_1. \end{aligned} \tag{2.5}$$

These results obviously hold in all commutative rings.

3. Universality of G over $\mathbb{R}$. Recall that the universality of the sum of four squares can be proven by recourse to the Geometry of Numbers (see Grace [9] and Deutsch [5]). Some nontrivial modifications make it possible to prove the universality of G by the same underlying technique.

LEMMA 1. *For any rational prime p, there exist integers a and b such that*

$$a^2 + a + 1 + b^2 \equiv 0 \pmod{p}. \tag{3.1}$$

Proof. For $p = 2$ take $a = 1$ and $b = 1$. For odd primes, the proof is similar to that of the well known demonstration for $a^2 + b^2 + 1 \equiv 0 \pmod{p}$. Generally, we observe that the number of distinct elements of the form $-(b^2 + 1)$ modulo p is $(p + 1)/2$. Note that

$$a^2 + a \equiv a^2 + (p + 1)a \equiv (a + (p + 1)/2)^2 + c \pmod{p} \tag{3.2}$$

for some constant c that depends on p. It follows that the number of different elements of the form $a^2 + a$ modulo p is also $(p + 1)/2$. Thus there must be some overlap of these two sets, so there exist a and b modulo p which satisfy (3.1). ∎

If we consider the basis of the lattice used in the proof of the classical Four Squares Theorem via Geometry of Numbers as a matrix, we find that it is

$$M = \begin{pmatrix} 1 & 0 & a & b \\ 0 & 1 & -b & a \\ 0 & 0 & p & 0 \\ 0 & 0 & 0 & p \end{pmatrix}. \tag{3.3}$$

Setting (x, z, y, w) equal to the matrix product $(m, r, n, s) \times M$ where m, n, r, s are rational integers, we find

$$\left.\begin{aligned} x &\equiv m \\ y &\equiv m \cdot a - b \cdot r \\ z &\equiv r \\ w &\equiv m \cdot b + a \cdot r \end{aligned}\right\} \pmod{p}. \tag{3.4}$$

Now it is left to compute $G = g(x, y) + g(z, w)$. Modulo p this becomes

$$\begin{aligned} x^2 + xy + y^2 + z^2 + zw + w^2 &\equiv m^2 + m^2a^2 - 2abmr + r^2b^2 + m(ma - br) \\ &\quad + r^2 + m^2b^2 + 2abmr + r^2a^2 + r(mb + ar) \\ &\equiv m^2(1 + a^2 + a + b^2) + r^2(b^2 + 1 + a^2 + a) \equiv 0. \end{aligned} \tag{3.5}$$

It is obvious that $\det(M) = p^2$.

LEMMA 2. *The ellipsoidal object in $\mathbb{R}^4$ defined by $G(x, y, z, w) < r^2$ is centrally symmetric and convex. Its volume is $\frac{2}{3}\pi^2 r^4$.*

Proof. Central symmetry is obvious. Since G is the norm of a quaternion, it is always greater than or equal to zero. To show convexity we consider a point (x_0, y_0, z_0, w_0) and a parametrized line segment in Euclidean four-space contained in the ellipsoidal object. Then the line is defined by the equations

$$x = x_0 + tm_1, \quad y = y_0 + tm_2, \quad z = z_0 + tm_3, \quad w = w_0 + tm_4. \tag{3.6}$$

Here, $m_1, \ldots, m_4$ are constants, t is a real parameter. With no loss of generality we may choose the m's so that $t = 1$ corresponds to the endpoint of the line segment. Clearly, $t = 0$ represents the beginning of the line segment. Taking the second derivative with respect to t of $h(t) = G(x, y, z, w)$ we find

$$h''(t) = 2(m_1^2 + m_1m_2 + m_2^2 + m_3^2 + m_3m_4 + m_4^2). \tag{3.7}$$

As the expression in parentheses is the norm of a quaternion, it is always greater than or equal to zero. Hence $h(t)$ is a convex function of t, so the maximum value of h on the line occurs at $t = 0$ or $t = 1$. Since both the

values are less than or equal to r by hypothesis, the entire line segment resides in the object of the lemma.

To find the volume of the region $G \leq r^2$ we note that

$$G(x,y,z,w) = \left(x + \frac{1}{2}\,y\right)^2 + \frac{3}{4}\,y^2 + \left(z + \frac{1}{2}\,w\right)^2 + \frac{3}{4}\,w^2. \tag{3.8}$$

Making the linear transformation

$$X = x + \frac{1}{2}\,y, \quad Y = \frac{\sqrt{3}}{2}\,y, \quad Z = z + \frac{1}{2}\,w, \quad W = \frac{\sqrt{3}}{2}\,w \tag{3.9}$$

we obtain a sphere of radius r in the X, Y, Z and W coordinates. The absolute value of the determinant of the linear transformation is $3/4$. Let **vol** mean volume, and $B_4(r)$ be the ball of radius r in $\mathbb{R}^4$. Using the inverse linear transformation and a standard result in multivariable calculus, we have

$$\mathbf{vol}(G \leq r^2) = \mathbf{vol}(B_4(r)) \cdot \frac{4}{3} = \frac{4}{3} \cdot \frac{\pi^2 r^4}{2}. \tag{3.10}$$

See Spivak [13, p. 67] for details. ∎

THEOREM 3. *The quadratic form $G(x,y,z,w)$ is universal over $\mathbb{Z}$.*

Proof. We take the lattice in $\mathbb{R}^4$ corresponding to the matrix (3.3). This lattice is the $\mathbb{Z}$-module with basis

$$\{(1,0,a,b), (0,1,-b,a), (0,0,p,0), (0,0,0,p)\}. \tag{3.11}$$

By Minkowski's Theorem from the Geometry of Numbers, the region $G \leq r^2$ will contain a nonzero point of the lattice if

$$\frac{2}{3}\,\pi^2 r^4 \geq 16p^2. \tag{3.12}$$

Thus r need only satisfy $r^2 \geq 1.560p$. Choose $r^2 = 1.6p$. Then a nonzero point of the lattice exists inside $G \leq r^2$. Call it (x,y,z,w). For this point, $G \equiv 0 \pmod{p}$ by equation (3.5). Also, $0 < G(x,y,z,w) \leq 1.6p$, which forces the value of G at the lattice point to equal p.

Since G represents 1, and obeys the multiplicative law of equations (2.4) and (2.5), it follows that the theorem holds. ∎

4. Geometry of Numbers results over quadratic fields. At this juncture it would be advantageous to find an analogue to the statement for sums of squares derived from Geometry of Numbers in Deutsch [6]. Namely, there is always a representation

$$\kappa\varrho = \alpha^2 + \beta^2 + \gamma^2 + \delta^2, \tag{4.1}$$

where ϱ is a prime factor of a rational prime p that splits in the quadratic field K, and α, β, γ, δ, κ are algebraic integers in K, and there is a bound on $|N(\kappa)|$ which depends only on the discriminant of K.

Such an argument is readily constructed. However, we first need to compute the volume of a particular region in $\mathbb{R}^8$. We let $\mathcal{D}(r)$ be the subset of $\mathbb{R}^8$ defined by

$$G(x_1, x_2, x_3, x_4) + G(x_5, x_6, x_7, x_8) \le r^2. \tag{4.2}$$

LEMMA 4. *The region $\mathcal{D}(r)$ is centrally symmetric and convex. It has volume $\frac{2}{27}\pi^4 r^8$.*

Proof. As before, central symmetry is obvious. Using the linear transformation of (3.9) twice, once for the variables x_1, x_2, x_3, x_4, and then again for the variables x_5, x_6, x_7, x_8, we obtain a ball of radius r in 8-dimensional real space. The matrix of transformation has determinant that is the square of the determinant for the 4-dimensional case. Thus we find that

$$\mathbf{vol}(\mathcal{D}(r)) = \mathbf{vol}(B_8(r)) \cdot \frac{16}{9} = \frac{16}{9} \cdot \frac{\pi^4 r^8}{4!}. \tag{4.3}$$

Convexity follows easily from that of G. Take two points $(x_1, \dots, x_8)$ and $(y_1, \dots, y_8)$ in $\mathcal{D}(r)$. Then we have

$$\begin{aligned} &G\left(\frac{x_1+y_1}{2}, \dots, \frac{x_4+y_4}{2}\right) + G\left(\frac{x_5+y_5}{2}, \dots, \frac{x_8+y_8}{2}\right) \\ &\le \frac{1}{2}\{G(x_1, \dots, x_4) + G(y_1, \dots, y_4) + G(x_5, \dots, x_8) + G(y_5, \dots, y_8)\} \\ &\le \frac{1}{2}\{r^2 + r^2\} = r^2. \ \blacksquare \end{aligned} \tag{4.4}$$

We let O be the ring of integers in the real quadratic field K of discriminant d. Let p be a rational prime which splits in O into two prime factors $p = \varrho\varrho^*$. Then the following holds.

LEMMA 5. *With K, O, d and ϱ as above, there exist κ, α, β, γ and δ in O for which $\kappa\varrho = G(\alpha, \beta, \gamma, \delta)$ and $|N(\kappa)| \le 1.49d$.*

Proof. We model the demonstration on the argument in Deutsch [6]. By Lemma 1 there exist rational integers a and b for which $a^2 + b^2 + b + 1 \equiv 0 \pmod{p}$. This implies that $a^2 + b^2 + b + 1 \equiv 0 \pmod{\varrho}$ and also modulo ϱ^*. We may pick $\varepsilon \in O$ such that $O = \mathbb{Z}[1, \varepsilon]$.

The convex region of $\mathbb{R}^8$ is slightly modified from Deutsch [6], though the same lattice may be used. For the convex region we use $\mathcal{D}(r)$. The matrix associated with the lattice used in Deutsch [6] is

$$\begin{pmatrix} 1 & 1 & 0 & 0 & a & a & b & b \\ \varepsilon & \varepsilon^* & 0 & 0 & a\varepsilon & a\varepsilon^* & b\varepsilon & b\varepsilon^* \\ 0 & 0 & 1 & 1 & b & b & -a & -a \\ 0 & 0 & \varepsilon & \varepsilon^* & b\varepsilon & b\varepsilon^* & -a\varepsilon & -a\varepsilon^* \\ 0 & 0 & 0 & 0 & \varrho & \varrho^* & 0 & 0 \\ 0 & 0 & 0 & 0 & \varepsilon\varrho & \varepsilon^*\varrho^* & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \varrho & \varrho^* \\ 0 & 0 & 0 & 0 & 0 & 0 & \varepsilon\varrho & \varepsilon^*\varrho^* \end{pmatrix}. \tag{4.5}$$

We take the $\mathbb{Z}$-lattice in $\mathbb{R}^8$ having as basis the columns of the above matrix. As noted in Deutsch [5, 6] the lattice can be written

$$(\alpha, \alpha^*, \beta, \beta^*, a\alpha + b\beta + \mu\varrho, a\alpha^* + b\beta^* + \mu^*\varrho^*, \\ b\alpha - a\beta + \nu\varrho, b\alpha^* - a\beta^* + \nu^*\varrho^*) \tag{4.6}$$

where α, β, μ and ν run through all of $O(\sqrt{5})$. Setting this equal to

$$(x_1, x_5, x_3, x_7, x_4, x_8, x_2, x_6) \tag{4.7}$$

we observe that

$$\left.\begin{aligned} x_1 &\equiv \alpha \\ x_2 &\equiv b\cdot\alpha - a\cdot\beta \\ x_3 &\equiv \beta \\ x_4 &\equiv a\cdot\alpha + b\cdot\beta \end{aligned}\right\} \pmod{\varrho}, \qquad \left.\begin{aligned} x_5 &\equiv \alpha^* \\ x_6 &\equiv b\cdot\alpha^* - a\cdot\beta^* \\ x_7 &\equiv \beta^* \\ x_8 &\equiv a\cdot\alpha^* + b\cdot\beta^* \end{aligned}\right\} \pmod{\varrho}. \tag{4.8}$$

Computer algebra shows that

$$G(x_1, x_2, x_3, x_4) \equiv (\alpha^2 + \beta^2)\cdot(1 + a^2 + b + b^2) \equiv 0 \pmod{\varrho}. \tag{4.9}$$

Similarly, $G(x_5, x_6, x_7, x_8) \equiv 0 \pmod{\varrho^*}$. From Deutsch [6], the size of the lattice is $|(\varepsilon - \varepsilon^*)^4\varrho^2(\varrho^*)^2|$ or d^2p^2 where d is the discriminant of the field.

To apply Geometry of Numbers, we need to find r such that the volume of $\mathcal{D}(r)$ is greater than $2^8d^2p^2$. Thus

$$\frac{2}{27}\pi^4 r^8 \;\geq\; 2^8\cdot d^2\cdot p^2 \;\Leftrightarrow\; r^8 \;\geq\; \frac{27\cdot 2^8}{2\pi^4}\, d^2p^2, \tag{4.10}$$

which yields $r^2 \geq \sqrt{dp}\cdot 2.44058\ldots$. Thus there exist algebraic integers, not all zero, for which

$$G(\alpha, \beta, \gamma, \delta) = \kappa\varrho, \qquad G(\alpha^*, \beta^*, \gamma^*, \delta^*) = \kappa^*\varrho^* \tag{4.11}$$

with

$$\kappa\varrho + \kappa^*\varrho^* \leq 2.4406\sqrt{dp}. \tag{4.12}$$

Applying the Theorem of Arithmetic Means and Geometric Means we find

$$\begin{aligned} 2\sqrt{\kappa\varrho\kappa^*\varrho^*} &\le \kappa\varrho + \kappa^*\varrho^* \le 2.4406\sqrt{dp}, \\ \sqrt{\kappa\varrho\kappa^*\varrho^*} &\le 1.2203\sqrt{dp}, \\ |\kappa\kappa^*| &\le 1.48914d. \end{aligned} \tag{4.13}$$

This proves the lemma. ∎

Corollary 6. *Under the conditions of the previous lemma, in the case of* $O(\sqrt{5})$ *we have the bound* $|\kappa\kappa^*| \le 7.45$.

By the argumentation in Deutsch [5] after equation (4.15), we conclude the following.

Corollary 7. *Under the conditions of Lemma* 5, *in the case of* $O(\sqrt{5})$ *it is only necessary to consider the possibilities* $|\kappa\kappa^*| \in \{1, 4, 5\}$.

5. The ring of icosians $\mathbb{I}$ and certain of its subrings. We review the definition and some properties of the quaternionic ring of icosians. Set $\tau = (1+\sqrt{5})/2$. Then $[1, \tau]$ is an $O(\sqrt{5})$-basis for the algebraic integers in the field $\mathbb{Q}(\sqrt{5})$. Also, τ is the fundamental unit for this ring of integers. In the notation of Vignéras [14], the ring of icosians $\mathbb{I}$ is the $O(\sqrt{5})$-module with generators

$$\begin{aligned} \mathbf{e}_1 &= \frac{1}{2}(\mathbf{1} + \tau^{-1}\mathbf{i} + \tau\mathbf{j}), \quad & \mathbf{e}_2 &= \frac{1}{2}(\tau^{-1}\mathbf{i} + \mathbf{j} + \tau\mathbf{k}), \\ \mathbf{e}_3 &= \frac{1}{2}(\tau\mathbf{i} + \tau^{-1}\mathbf{j} + \mathbf{k}), \quad & \mathbf{e}_4 &= \frac{1}{2}(\mathbf{i} + \tau\mathbf{j} + \tau^{-1}\mathbf{k}). \end{aligned} \tag{5.1}$$

It is noted that the number of units of norm one in $\mathbb{I}$ amounts to 120 (see Baake and Moody [1] and Vignéras [14]). We define $\mathbb{I}_0 = O(\sqrt{5})[\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}]$ and quote the following results.

Lemma 8 (Deutsch [6, Lemma 15]). *For all* $\mathbf{q} \in \mathbb{I}$ *there exist quaternion units* $\mathbf{u}_1, \mathbf{u}_2 \in \mathbb{I}$ *of norm* 1 *such that* $\mathbf{u}_1\mathbf{q}\mathbf{u}_2$ *has* $O(\sqrt{5})$*-integer coefficients, i.e.* $\mathbf{u}_1\mathbf{q}\mathbf{u}_2 \in \mathbb{I}_0$.

Lemma 9 (Deutsch [6, Lemma 16]). *Suppose* ϱ *is a prime of the ring* $O(\sqrt{5})$. *Then there exists a unit* λ *of* $O(\sqrt{5})$ *and a quaternion* $\mathbf{q}$ *of* $\mathbb{I}$ *such that* $N(\mathbf{q}) = \lambda\varrho$.

In addition, a second subring of $\mathbb{I}$ plays an important role. We want the norm of a member of this subring to equal the quadratic form $G(x, y, z, w)$ when the coefficients of the quaternion in a specified basis are x, y, z and w. This subring can be developed as follows.

Recall that the quaternion $\mathbf{h}$ is defined as $(\mathbf{1}+\mathbf{i}+\mathbf{j}+\mathbf{k})/2$. We note that for any real x and y, $N(x+y\mathbf{h}) = g(x, y) = x^2 + xy + y^2$. This is related the fact that $\mathbf{h}^2 - \mathbf{h} + 1 = 0$. Therefore there is a canonical embedding of the

algebraic integers of $\mathbb{Q}(\sqrt{-3})$ into the Hurwitz quaternions. Also, $\mathbf{h} \in \mathbb{I}$, as computer algebra shows that

$$\mathbf{h} = \mathbf{e}_1 + (\tau - 1)\mathbf{e}_2 + (\tau - 1)\mathbf{e}_3 - \mathbf{e}_4. \tag{5.2}$$

Since the norm of a quaternion is the length of the corresponding vector in $\mathbb{R}^4$, we wish to find two quaternions of length one orthogonal to the subspace spanned by $\mathbf{1}$ and $\mathbf{h}$. We may write one such vector as $\mathbf{r} = a\mathbf{i} + b\mathbf{j} + c\mathbf{k}$. It would be convenient for the second vector to be equal to $\mathbf{rh}$. From the expression for $\mathbf{r}$ we have an equation for orthogonality via the dot product in $\mathbb{R}^4$, namely $a + b + c = 0$. Set $a = -b - c$ and substitute into the norm 1 property. We find that $2b^2 + 2bc + 2c^2 = 1$. Solving for c in terms of b we have

$$c = \frac{-b \pm \sqrt{2 - 3b^2}}{2}. \tag{5.3}$$

Since it is necessary for the coefficients of $\mathbf{r}$ to be in $\mathbb{Q}(\sqrt{5})$ to possibly be an icosian, we choose $b = 1/2$. Taking the negative sign on the radical, we find

$$c = -\frac{1 + \sqrt{5}}{4}, \qquad a = \frac{-1 + \sqrt{5}}{4}. \tag{5.4}$$

Computer algebra yields

$$\mathbf{r} = -\tau\mathbf{e}_2 + \tau\mathbf{e}_4, \qquad \mathbf{rh} = -\tau\mathbf{e}_2 + \tau\mathbf{e}_3, \tag{5.5}$$

and also that for any real x, y, z, w we have

$$N(x\mathbf{1} + y\mathbf{h} + z\mathbf{r} + w\mathbf{rh}) = x^2 + xy + y^2 + z^2 + zw + w^2 = G(x, y, z, w). \tag{5.6}$$

This situation is summarized in the following definition and lemma.

DEFINITION 10. $\mathbb{I}_{\mathbf{h}}$ is the $O(\sqrt{5})$-module with generators $\{\mathbf{1}, \mathbf{h}, \mathbf{r}, \mathbf{rh}\}$.

LEMMA 11. *$\mathbb{I}_{\mathbf{h}}$ is a subring of the icosians $\mathbb{I}$. The norm of a typical element of $\mathbb{I}_{\mathbf{h}}$ is given by equation* (5.6).

Table I. Multiplication table for $\mathbb{I}_{\mathbf{h}}$

	1	**h**	**r**	**rh**
1	**1**	**h**	**r**	**rh**
h	**h**	**−1 + h**	**r − rh**	**r**
r	**r**	**rh**	**−1**	**−h**
rh	**rh**	**−r + rh**	**−1 + h**	**−1**

Proof. The multiplication table for $\mathbb{I}_{\mathbf{h}}$ is shown in Table I. Being closed under addition and multiplication demonstrates the subring property. ∎

6. Elements of norm 2 and $2 + \tau$ in $\mathbb{I}$ and $\mathbb{I}_{\mathbf{h}}$. Consider an arbitrary totally positive prime ϱ in $O(\sqrt{5})$. We wish to find a representation of it

by $G(x,y,z,w)$ with $x,y,z,w \in O(\sqrt{5})$. If ϱ is inert, such a representation follows from the universality of G over $\mathbb{Z}$. If ϱ ramifies, then up to a square unit it equals $\tau\sqrt{5}$. As noted in Deutsch [5], we have $\tau\sqrt{5} = 1^2 + \tau^2$. Thus $\tau\sqrt{5} = G(1,0,\tau,0)$. The only case left is when ϱ is a factor of a rational prime p which splits in $O(\sqrt{5})$.

By Lemma 5 and Corollary 7, there exist κ, α, β, γ and δ in $O(\sqrt{5})$ such that $\kappa\varrho = G(\alpha,\beta,\gamma,\delta)$ and $|\kappa\kappa^*| \in \{1,4,5\}$. Note that $G(\alpha,\beta,\gamma,\delta)$ is the norm of the quaternion $\alpha\mathbf{1}+\beta\mathbf{h}+\gamma\mathbf{r}+\delta\mathbf{rh}$. Thus $G(\alpha,\beta,\gamma,\delta)$ is nonnegative and the same holds for $G(\alpha^*,\beta^*,\gamma^*,\delta^*)$. Thus $\kappa\varrho$ is totally positive. Since ϱ is totally positive it follows that so is κ.

As in Deutsch [5], we find that when $|\kappa\kappa^*| = 4$ or 5 then κ must be 2 times a unit of $O(\sqrt{5})$ in the first case, and $2+\tau$ times a unit in the second case. By moving this unit from κ to ϱ we can take $\kappa = 2$ or $2+\tau$ respectively. Note that the unit must be totally positive as 2 or $2+\tau$ and the original ϱ are totally positive.

LEMMA 12. *$(\mathbf{1}+\mathbf{h})\mathbb{I} \subseteq \mathbb{I}_\mathbf{h}$ and $\mathbb{I}(\mathbf{1}+\mathbf{h}) \subseteq \mathbb{I}_\mathbf{h}$.*

Proof. Computer algebra shows that $(\mathbf{1}+\mathbf{h})\mathbf{e}_n \in \mathbb{I}_\mathbf{h}$ for $n = 1,\dots,4$. For example

$$(\mathbf{1}+\mathbf{h})\mathbf{e}_2 = -\tau\mathbf{1} + \tau\mathbf{h} + \tau^*\mathbf{r}. \tag{6.1}$$

Similar results hold if the factors are taken in the opposite order. ∎

Since the quaternionic norm of $\mathbf{1}+\mathbf{h}$ is 3, for every prime $\varrho \in O(\sqrt{5})$ there is an element of $\mathbb{I}_\mathbf{h}$ with norm 3ϱ. Given an element of $\mathbb{I}_\mathbf{h}$ of norm 2ϱ, it may be reasonable to try to come up with some linear combination that would produce an element of that ring with norm ϱ. The next lemmas proceed down this path.

LEMMA 13. *There are 24 elements of norm 2 in $\mathbb{I}_0$. There are 48 elements of norm $2+\tau$ in $\mathbb{I}_0$.*

Proof. Take a typical element $\mathbf{q}$ in $\mathbb{I}_0$ and consider its norm. Write $\mathbf{q}$ as

$$\mathbf{q} = \alpha\mathbf{1} + \beta\mathbf{i} + \gamma\mathbf{j} + \delta\mathbf{k}. \tag{6.2}$$

Then the norm is just the sum $\alpha^2+\cdots+\delta^2$. Since the coefficients are elements of $O(\sqrt{5})$ we may write $\alpha = a+b\tau$. Thus $\alpha^2 = a^2+b^2+(2ab+b^2)\tau$. Similarly for β, γ and δ. For the case of norm 2, equating the norm of $\mathbf{q}$ with $2+0\tau$ in the ring $O(\sqrt{5})$ we find that

$$\begin{aligned} 2 &= a^2 + b^2 + \text{sum of other squares}, \\ 0 &= 2ab + b^2 + \text{further sum}. \end{aligned} \tag{6.3}$$

Thus $|a|$ and $|b|$ are less than or equal to $\sqrt{2}$. Similar inequalities hold for β, γ and δ. A computer scan, written in C, produces the 24 elements of norm 2. A similar scan yields the 48 elements of norm $2+\tau$. ∎

LEMMA 14. *There are exactly* 600 *elements of norm* 2 *in* $\mathbb{I}$. *There are exactly* 720 *elements of norm* $2+\tau$ *in* $\mathbb{I}$.

Proof. Let $\mathbf{s}$ be an element of $\mathbb{I}$ with norm 2. Then by Lemma 8 there exist quaternion units $\mathbf{u}_1$, $\mathbf{u}_2$ of norm 1 for which $\mathbf{u}_1\mathbf{s}\mathbf{u}_2 \in \mathbb{I}_0$. Since the quaternionic norm of this product is 2, it follows that the product must be one of the 24 elements of norm 2 mentioned in Lemma 13. Thus all elements of norm 2 in $\mathbb{I}$ are of the form $\mathbf{u}_1\mathbf{r}\mathbf{u}_2$ where $\mathbf{r} \in \mathbb{I}_0$ and of norm 2 while $\mathbf{u}_1$, $\mathbf{u}_2$ are units of $\mathbb{I}$ of norm 1.

It is well known that there are exactly 120 elements of norm 1 in $\mathbb{I}$ (see Baake and Moody [1] or Vignéras [14]). The determination of the complete set of elements of norm 2 in $\mathbb{I}$ is thus a finite computation. The way chosen to proceed was to scan the coefficients of all possible products $\mathbf{u}_1\mathbf{r}\mathbf{u}_2$ in the basis for $\mathbb{I}$. After expressing these coefficients in the basis $[1,\tau]$ for $O(\sqrt{5})$, the maximum absolute value of the latter coefficients was computed. This turned out to be 2. Then an ordered scan of all possible linear combinations of the basis of $\mathbb{I}$ with $O(\sqrt{5})$ coefficients less than or equal to 2 was made, yielding the 600 distinct elements of norm 2. The first scan was done using a computer algebra system, while the second scan was done in C.

The same method was used to construct the 720 distinct elements of $\mathbb{I}$ of norm $2+\tau$. The corresponding maximum absolute value for the coefficients was 3. ∎

LEMMA 15. *For each of the* 600 *elements* $\mathbf{q}$ *of norm* 2 *in* $\mathbb{I}$ *there exists a quaternionic unit* $\mathbf{u} \in \mathbb{I}$ *and a number field unit* $\alpha \in O(\sqrt{5})$ *such that*

$$N(\mathbf{v}\mathbf{q} - (\mathbf{1}+\mathbf{h})\mathbf{u}) = \alpha. \tag{6.4}$$

(*Here* $\mathbf{v}$ *equals either* $\mathbf{1}$ *or* $\mathbf{1}+\mathbf{r}$.) *The same holds for the* 720 *elements of norm* $2+\tau$ *in* $\mathbb{I}$.

Proof. A scan using computer algebra demonstrates the existence of $\mathbf{u}$ and $\mathbf{v}$ for each element of $\mathbb{I}$ under consideration. See Table II for examples. ∎

Table II. Linear combinations of elements of $\mathbb{I}$ of norm $2+\tau$ as in equation (6.4)

Quaternion $\mathbf{q}$	Unit $\mathbf{u}$	$\mathbf{v}$	α
⋮	⋮	⋮	⋮
$[\tau-1]\mathbf{e}_1 - 2\tau\mathbf{e}_2 + [\tau+1]\mathbf{e}_3$	$-\mathbf{e}_1 - \tau\mathbf{e}_2 + \mathbf{e}_3 + \mathbf{e}_4$	$\mathbf{1}+\mathbf{r}$	1
$[\tau-1]\mathbf{e}_1 - 2\tau\mathbf{e}_2 + 2\mathbf{e}_3$	$-\mathbf{e}_1 - \tau\mathbf{e}_2 + \mathbf{e}_3 + \tau\mathbf{e}_4$	$\mathbf{1}$	$\tau+1$
$[\tau-1]\mathbf{e}_1 - 2\tau\mathbf{e}_2 + 2\mathbf{e}_3 + \mathbf{e}_4$	$\tau\mathbf{e}_2 - \tau\mathbf{e}_3$	$\mathbf{1}+\mathbf{r}$	$8\tau+5$
$[\tau-1]\mathbf{e}_1 - \tau\mathbf{e}_2 - \tau\mathbf{e}_3 + \tau\mathbf{e}_4$	$-\mathbf{e}_1 - \tau\mathbf{e}_2 + \tau\mathbf{e}_4$	$\mathbf{1}$	1
$[\tau-1]\mathbf{e}_1 - \tau\mathbf{e}_2 - \tau\mathbf{e}_3 + [\tau+1]\mathbf{e}_4$	$\tau\mathbf{e}_2 - \tau\mathbf{e}_4$	$\mathbf{1}+\mathbf{r}$	$8\tau+5$
⋮	⋮	⋮	⋮

7. End of proof. We are now prepared to prove the result on representation by G for $O(\sqrt{5})$.

THEOREM 16. *Let ϱ be a totally positive prime factor of a rational prime p which splits in $O(\sqrt{5})$. Then there exists a quaternion $\mathbf{q} \in \mathbb{I}_{\mathbf{h}}$ such that $N(\mathbf{q}) = \lambda\varrho$ where λ is a unit of $O(\sqrt{5})$.*

Proof. By the discussion before Lemma 12 we know there exists $\mathbf{q} = \alpha\mathbf{1}+\beta\mathbf{h}+\gamma\mathbf{r}+\delta\mathbf{rh}$ such that $\kappa\varrho = N(\mathbf{q}) = G(\alpha,\beta,\gamma,\delta)$ and $|\kappa\kappa^*| \in \{1,4,5\}$. Note $\mathbf{q} \in \mathbb{I}_{\mathbf{h}}$. If $|\kappa\kappa^*| = 1$ we are done. As for the other two cases, again by the discussion before Lemma 12, we may write $2\lambda\varrho$ or $(2+\tau)\lambda\varrho = N(\mathbf{q})$ with λ a totally positive unit of $O(\sqrt{5})$.

Consider the right greatest common divisor of $\mathbf{q}$ and ϱ in the norm Euclidean ring $\mathbb{I}$. Call this quaternion $\mathbf{s}$. Then we have

$$\mathbf{s} = \mathbf{aq} + \mathbf{b}\varrho, \quad N(\mathbf{s}) \,|\, N(\mathbf{q}), \quad N(\mathbf{s}) \,|\, N(\varrho) = \varrho^2. \tag{7.1}$$

From the last two relations we have $N(\mathbf{s}) \,|\, 2\varrho$ (or $(2+\tau)\varrho$) and $N(\mathbf{s}) \,|\, \varrho^2$, so $N(\mathbf{s}) \,|\, \varrho$. We note that ϱ must be relatively prime to 2 and $2+\tau$ as ϱ comes from a splitting prime of $O(\sqrt{5})$. Taking quaternionic conjugates in the first equation, we have

$$\overline{\mathbf{s}} = \overline{\mathbf{q}}\,\overline{\mathbf{a}} + \varrho\overline{\mathbf{b}}. \tag{7.2}$$

By multiplying we find

$$N(\mathbf{s}) = \mathbf{s}\overline{\mathbf{s}} = N(\mathbf{q})N(\mathbf{a}) + \varrho\mathbf{c} \tag{7.3}$$

for some $\mathbf{c} \in \mathbb{I}$. However, $\mathbf{c}$ must be a real number as the rest of the equation is composed of real numbers. It is shown in Deutsch [5] that $\mathbb{R} \cap \mathbb{I}$ is $O(\sqrt{5})$, so $\mathbf{c}$ is in this ring. It follows that $\varrho \,|\, N(\mathbf{s})$. Thus we conclude $N(\mathbf{s}) = \varrho$ up to a totally positive unit.

Since $\mathbf{s}$ is a right divisor of $\mathbf{q}$ we may write $\mathbf{q} = \mathbf{ts}$, $\mathbf{t} \in \mathbb{I}$. This implies that $N(\mathbf{t}) = 2\lambda_1$ or $(2+\tau)\lambda_1$ as the case may be, for λ_1 a totally positive unit. Thus we may write $\lambda_1 = \tau^{2n}$ with $n \in \mathbb{Z}$. This also shows that $N(\mathbf{s}) = \lambda\lambda_1^{-1}\varrho$.

By Lemma 15 there exists $\mathbf{v} \in \mathbb{I}_{\mathbf{h}}$ and a quaternionic unit $\mathbf{u} \in \mathbb{I}$ such that

$$N(\mathbf{v}\tau^{-n}\mathbf{t} - (\mathbf{1}+\mathbf{h})\mathbf{u}) = \alpha \tag{7.4}$$

with α a unit of $O(\sqrt{5})$. As α is the norm of a quaternion, it is totally positive. Set $\mathbf{u} = \tau^{-n}\mathbf{u}_1$. Then $\mathbf{u}_1 \in \mathbb{I}$ and

$$N(\mathbf{v}\tau^{-n}\mathbf{t} - (\mathbf{1}+\mathbf{h})\tau^{-n}\mathbf{u}_1) = \alpha, \quad N(\mathbf{vt} - (\mathbf{1}+\mathbf{h})\mathbf{u}_1) = \tau^{2n}\alpha. \tag{7.5}$$

Thus

$$N(\mathbf{vts} - (\mathbf{1}+\mathbf{h})\mathbf{u}_1\mathbf{s}) = N(\mathbf{vt} - (\mathbf{1}+\mathbf{h})\mathbf{u}_1) \cdot N(\mathbf{s}) \tag{7.6}$$
$$= \tau^{2n}\alpha\lambda\lambda_1^{-1}\varrho = \lambda\alpha\varrho.$$

By Lemma 12, $(\mathbf{1}+\mathbf{h})\mathbf{u}_1\mathbf{s} \in \mathbb{I}_\mathbf{h}$. Also, $\mathbf{q} = \mathbf{ts} \in \mathbb{I}_\mathbf{h}$ and $\mathbf{v} \in \mathbb{I}_\mathbf{h}$. It follows that there is an element of $\mathbb{I}_\mathbf{h}$ with norm ϱ times a unit of $O(\sqrt{5})$. ∎

COROLLARY 17. *Let η be a totally positive integer in $O(\sqrt{5})$. Then there exists a quaternion $\mathbf{q} \in \mathbb{I}_\mathbf{h}$ such that $N(\mathbf{q}) = \eta$.*

Proof. By Deutsch [5, Theorem 10] we may write η as a product of totally positive primes. Each such totally positive prime is a unit times the norm of a quaternion in $\mathbb{I}_\mathbf{h}$. But that unit must be an even power of τ, say τ^{2n}, as it is totally positive. Absorbing τ^n into the quaternion results in a new element of $\mathbb{I}_\mathbf{h}$ whose norm is the totally positive prime factor under consideration.

The corollary now follows from equations (2.4) and (2.5). ∎

THEOREM 18. *The quadratic form $G(x, y, z, w)$ is universal for $O(\sqrt{5})$.*

Proof. This follows from Corollary 17, Lemma 11 and equation (5.6). ∎

8. Other quadratic fields. Computations in other quadratic fields of small norm show that $G(x, y, z, w)$ is not universal. In particular, among fields with odd discriminant, G is not universal for $\mathbb{Q}(\sqrt{13})$ and $\mathbb{Q}(\sqrt{17})$. For those of even discriminant, non-universality holds for $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$. A conjecture may be warranted at this stage.

9. Remarks on the computations. Two computers were used in the computations mentioned above. One was a pc with Pentium dual core P920 cpu and one gigabyte of RAM. The other was a 2003 era laptop with a Pentium 4 chip running at 2.6 gigahertz, and 256 megabytes of RAM. Most of the computations were done on the laptop, but certain large scale verifications were moved to the pc. It turned out that the pc was 20 to 30 per cent faster on the same calculations.

The software used in both cases was LINUX Slackware 11.0, MAXIMA 5.9.0, MAXIMA 5.14.0 and Python 2.5. MAXIMA was built on top of the ANSI version of GNU Common Lisp 2.6.6 or 2.6.7. Python was compiled using GNU GCC 3.4.6. The latter was also used to compile all C programs. The LINUX kernel version was 2.4.33.3.

Acknowledgments. The author would like to thank Harvey Cohn and Mike Rosen for their continued encouragement. The author would also like to express his appreciation to the referee for pointing out the very recent result of Lee [12].

References

[1] M. Baake and R. Moody, *Similarity submodules and root systems in four dimensions*, Canad. J. Math. 51 (1999), 1258–1276.

[2] H. Cohn, *Decomposition into four integral squares in the fields of* $2^{1/2}$ *and* $3^{1/2}$, Amer. J. Math. 82 (1960), 301–322.

[3] —, *Calculation of class numbers by decomposition into three integral squares in the fields of* $2^{1/2}$ *and* $3^{1/2}$, ibid. 83 (1961), 33–56.

[4] —, *Cusp forms arising from Hilbert's modular functions for the field of* $3^{1/2}$, ibid. 84 (1962), 283–305.

[5] J. I. Deutsch, *Geometry of numbers proof of Götzky's four-squares theorem*, J. Number Theory 96 (2002), 417–431.

[6] —, *An alternate proof of Cohn's four squares theorem*, ibid. 104 (2004), 263–278.

[7] L. E. Dickson, *History of the Theory of Numbers*, *Vol. III*, Chelsea, New York, 1966.

[8] F. Götzky, *Über eine zahlentheoretische Anwendung von Modulfunktionen zweier Veränderlicher*, Math. Ann. 100 (1928), 411–437.

[9] J. Grace, *The Four Square Theorem*, J. London Math. Soc. 2 (1927), 3–8.

[10] A. Hurwitz, *Vorlesungen über die Zahlentheorie der Quaternionen*, Julius Springer, Berlin, 1919.

[11] M. H. Kim, W. H. Chan and S. Rhagavan, *Ternary universal integral quadratic forms over real quadratic fields*, Japan. J. Math. 22 (1996), 263–273.

[12] Y. H. Lee, *Universal forms over* $\mathbb{Q}(\sqrt{5})$, Ramanujan J. 16 (2008), 97–104.

[13] M. Spivak, *Calculus on Manifolds*, W. A. Benjamin, New York, 1965.

[14] M.-F. Vignéras, *Arithmétique des Algèbres de Quaternions*, Lecture Notes in Math. 800, Springer, Berlin, 1980.

1621 Yale Place
Rockville, MD 20850, U.S.A.
E-mail: deutschj_1729@yahoo.com

Received on 15.5.2008
and in revised form on 2.9.2008 (5709)