#A50 INTEGERS 12 (2012)

GONII: UNIVERSAL QUATERNARY QUADRATIC FORMS

Pete L. Clark
Department of Mathematics, Boyd Graduate Studies Research Center, University of Georgia, Athens, Georgia
pete@math.uga.edu

Jacob Hicks
Department of Mathematics, Boyd Graduate Studies Research Center, University of Georgia, Athens, Georgia
jhicks@math.uga.edu

Katherine Thompson
Department of Mathematics, Boyd Graduate Studies Research Center, University of Georgia, Athens, Georgia
thompson@math.uga.edu

Nathan Walters
Department of Mathematics, Boyd Graduate Studies Research Center, University of Georgia, Athens, Georgia
nwalters@math.uga.edu

Received: 12/3/11, Accepted: 7/30/12, Published: 9/3/12

Abstract

We continue our study of quadratic forms using Geometry of Numbers methods by considering universal quaternary positive definite integral forms of square discriminant. We give a *small multiple theorem* for such forms and use it to prove universality for all nine universal diagonal forms. The most interesting case is $x^2 + 2y^2 + 5z^2 + 10w^2$, which required computer calculations.

1. Introduction

This is the second in a series of papers exploring Diophantine applications of *geometry of numbers* (henceforth "GoN") and associated elementary combinatorial number theory. Whereas the first paper [11] treats primes represented by positive definite integral binary quadratic forms, this paper concerns the universality of positive definite quaternary integral quadratic forms.

In [15], Hermite applied GoN methods to give a striking new proof that every positive integer is a sum of four squares (Lagrange's Theorem), many years before Minkowski's foundational work in GoN [22]. It is thus remarkable that a systematic study of the application of GoN methods to universality theorems for quadratic forms seems not to have been undertaken until now. The closest precedent in the literature is a late paper of L.J. Mordell [23]. Mordell proves in particular a *small multiple theorem* for certain diagonal quaternary forms of square discriminant. Especially, his results apply to the *multiplicative forms*

$$q_{a,b} = x^2 + ay^2 + bz^2 + abw^2$$

for $a, b \in \mathbb{Z}^+$. We generalize this to all forms of square discriminant (Theorem 7).

Although our methods apply to many nondiagonal forms of square discriminant [12], in the remainder of this paper we concentrate on the diagonal case. Work of Ramanujan [24] and Dickson [7] shows that there are precisely nine universal diagonal positive definite quaternary integral quadratic forms of square discriminant. Here we give GoN proofs of the universality of all nine of these forms.

Of these nine forms, seven are multiplicative,

$$q_{1,1},\ q_{1,2},\ q_{1,3},\ q_{2,2},\ q_{2,3},\ q_{2,4},\ q_{2,5},$$

and the universality of the two remaining forms can be rather easily deduced from these (Theorems 17 and 18). Mordell gives GoN proofs of the universality of $q_{1,1}$, $q_{1,2}$, $q_{1,3}$ and also alludes to Liouville's reduction of $q_{2,3}$ to $q_{1,1}$ (Theorem 15). Similar methods can be applied to show universality of the forms $q_{2,2}$ and $q_{2,4}$ (Theorems 14 and 16), as Mordell likely knew. Because of [11] we possess certain analogous results for representations of primes by binary quadratic forms, and we make use of them in the proofs. In [20], [21], Liouville (briefly!) states how to give elementary (non-GoN) proofs of the universality of these six multiplicative forms.

This leaves $q_{2,5}$. This form stymied Liouville, who says he can only prove that it represents all positive *even* integers [21]. The universality of $q_{2,5}$ was indeed first proven by Ramanujan and Dickson, using (non-elementary) representation theorems for certain ternary subforms. Mordell does not mention that there are seven universal multiplicative forms, and the form $q_{2,5}$ does not appear in [23].

In [16], Hurwitz gave an elementary proof of Lagrange's Theorem using quaternion arithmetic. Recently Deutsch [6] gave Hurwitz-style universality proofs for eight of the nine diagonal universal forms of square discriminant, but not for $q_{2,5}$. This lack of success is somewhat puzzling because the relevant quaternion algebra $\left(\frac{-2,-5}{\mathbb{Q}}\right)$ still carries a Euclidean quaternion order, as was shown by Fitzgerald [9]. Using quaternionic methods Fitzgerald showed $q_{2,5}$ represents $16n$ for all $n \in \mathbb{Z}^+$.

Thus it seems that the literature contains no elementary proof of the universality of $q_{2,5}$.[1] The main result of the present work, Theorem 19, gives an elementary – though computational – proof of the universality of $q_{2,5}$. Moreover, in a key step of the argument we show that if $q_{2,5}$ represents $2n$ then it also represents n. This step does not use GoN methods and thus could be used to complete the elementary universality proofs of Liouville and Fitzgerald.

Most of the universality proofs for the first eight forms make use of well-chosen linear changes of variable. This is one of the oldest tricks of the trade, going back at least to Euler [8, 141: July 26, 1749]. However, in the proofs of the first eight theorems (and in the classical literature) the relevant changes of variable are written down without any systematic justification. (In [23] Mordell exhibits relations between these changes of variable and the multiplicative structure of the forms $q_{a,b}$ via (2), but this is not a complete explanation.) In order to prove the universality of $q_{2,5}$, we needed to devise and implement an algorithm to search for these changes of variable, of which some thousands were required. Our algorithm can be used on the other eight forms as well, and indeed it forms the basis of the universality proofs of the nondiagonal forms explored in [12]. Work is in progress on extending the techniques of this paper to study representations by quadratic forms of square discriminant in an even number of variables over an S-integer ring in a global field.

This work was done in the context of a VIGRE Research Group at the University of Georgia throughout the 2011-2012 academic year, led by the first author and with participation of the other three authors together with Christopher Drupieski (postdoc), Brian Bonsignore, Harrison Chapman, Lauren Huckaba, David Krumm, Allan Lacy Mora, Nham Ngo, Hans Parshall, Alex Rice, James Henry Stankewicz, Lee Troupe (doctoral students) and Jun Zhang (master's student).

Acknowledgement: We are grateful to David B. Leep for educating us on the early history of universal quaternary forms, in particular the results of Liouville.

2. Review of Quadratic Forms

2.1. Quadratic Forms Over a Ring

Let R be a commutative ring, and let $n \in \mathbb{Z}^+$. An *n-ary quadratic form over R* is a homogeneous quadratic polynomial

$$q(v) = q(x_1, \ldots, x_n) = \sum_{1 \le i \le j \le n} a_{ij} x_j x_j \in R[x_1, \ldots, x_n]. \tag{1}$$

[1] Added in July, 2012: we recently learned that David B. Leep has found a different elementary proof of the universality of $q_{2,5}$.

Two quadratic forms $q(v) = q(x_1, \ldots, x_n)$, $q'(v) = q'(x_1, \ldots, x_n)$ over R are *equivalent over* R if there is $A \in \mathrm{GL}_n(R)$ such that $q(Av) = q'(v)$. We write $q \cong q'$.

Let $q(v)$ be an n-ary quadratic form over R, and let $d \in R$. We say that q *R-represents* d if there exists $v \in R^n$ such that $q(v) = d$. We say that q is *isotropic* over R if there exists $v \in R^n$, $v \neq (0, \ldots, 0)$ such that $q(v) = 0$; otherwise q is *anisotropic*. We say q is *universal* over R if q R-represents every element of R.

Base change: Let S be another commutative ring, and let $\varphi : R \to S$ be a ring homomorphism. Given an n-ary quadratic form q over R and such a map φ, we may associate an n-ary quadratic form $q_{/S}$ in the evident way; namely,

$$q_{/S}(x_1, \ldots, x_n) = \sum_{1 \leq i \leq j \leq n} \varphi(a_{ij}) x_j x_j \in S[x_1, \ldots, x_n].$$

Here we will generally have $R = \mathbb{Z}$, and either $\varphi : \mathbb{Z} \to \mathbb{Q}$, $\varphi : \mathbb{Z} \to \mathbb{R}$, or $\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. Base change is useful for showing that q *does not* represent $d \in R$: if q R-represents d, then for all homomorphisms $\varphi : R \to S$, $q_{/S}$ S-represents $\varphi(d)$: indeed, if $q(x_1, \ldots, x_n) = d$, then $q_{/S}(\varphi(x_1), \ldots, \varphi(x_n)) = \varphi(d)$. (For succinctness we will say that q S-represents d.) For instance, let $R = \mathbb{Z}$ and $q = x^2 + y^2$. Then q does not $\mathbb{Z}$-represent any negative intgers. The formal justification of this is that in the ordered field $\mathbb{R}$ any sum of squares is non-negative, so q does not even $\mathbb{R}$-represent any negative integers. Moreover, q does not represent any $n \equiv 3 \pmod 4$: taking the map $\varphi : \mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$, by enumeration of cases one sees that $x^2 + y^2 = 3$ has no solution in $\mathbb{Z}/4\mathbb{Z}$.

Suppose that R is a domain of characteristic different from 2 and with fraction field K. For the n-ary quadratic form $q(v)$ of (1), let $M_q = (m_{ij}) \in M_n(K)$ be the matrix with $m_{ii} = a_{ii}$ for all i and $m_{ij} = \frac{a_{ij}}{2}$ for all $i \neq j$. Then, putting $v = (x_1, \ldots, x_n)^t$, we have

$$q(v) = v^t M_q v. \tag{2}$$

The form q is *classical* if $M_q \in M_n(R)$, or equivalently, $a_{ij} \in 2R$ for all $i \neq j$. Diagonal forms are classical. Two n-ary forms q and q' are equivalent over R iff there exists $A \in \mathrm{GL}_n(R)$ with $M_{q'} = A M_q A^t$. Then $\det M_{q'} = (\det A)^2 \det M_q$, which shows that the class $\operatorname{disc} q$ of $\det M_q$ modulo $(R^\times)^2$ is an invariant of the equivalence class of q, called the *discriminant* of q. When $R = \mathbb{Z}$, $(\mathbb{Z}^\times)^2 = \{1\}$, so $\operatorname{disc} q$ is a well-defined integer. In general we say q is *nondegenerate* if $\operatorname{disc} q \neq 0$.

Let $q_1(x_1, \ldots, x_m)$ be an m-ary quadratic form over R and $q_2(y_1, \ldots, y_n)$ be an n-ary quadratic form over R. We define their *direct sum* $q_1 \oplus q_2$ to be the $(m+n)$-ary form $q(x_1, \ldots, x_m, y_1, \ldots, y_n) = q_1(x_1, \ldots, x_m) + q_2(y_1, \ldots, y_n)$.

2.2. Quadratic Forms Over a Field of Characteristic Different From 2

The theory of quadratic forms simplifies considerably when $R = K$ is a field of characteristic different from 2. The results that we need are literally from Chapter 1 of the theory of quadratic forms over fields (specifically, from [18, Ch. I]).

Fact 1 [18, Cor. I.2.4]. *Every form q over K is K-equivalent to a diagonal form $(a_1, \ldots, a_n) := a_1x_1^2 + \ldots + a_nx_n^2$. In other words, there is $A \in \mathrm{GL}_n(K)$ such that $AM_qA^t = D(a_1, \ldots, a_n)$, where $D(a_1, \ldots, a_n)$ is diagonal with (i, i) entry a_i.*

The binary form $\mathbb{H} = (1, -1)$ plays a distinguished role in the theory.

Fact 2 [18, Thm. 1.3.2].*For a nondegenerate binary form $q(x, y)$ over K, the following are equivalent:*
(i) q is K-equivalent $\mathbb{H}$.
(ii) $\operatorname{disc} q = -1$.
(iii) q is isotropic.

Fact 3 [18, Thm. 1.3.4(2)]. *For a nondegenerate quadratic form q over K, the following are equivalent:*
(i) q is isotropic.
(ii) There exists a quadratic form q' such that $q \cong q' \oplus \mathbb{H}$.

A quadratic form is *hyperbolic* if it is isomorphic to $\bigoplus_{i=1}^{r} \mathbb{H}$ for some $r \in \mathbb{N}$.

2.3. Totally Isotropic Subspaces

We may view an n-ary quadratic form q as a map $q : K^n \to K$. A K-subspace W of K^n is called *totally isotropic* for q if $q|_W \equiv 0$.

Fact 4 [18, Thm. 1.3.4(1)]. *Let $q : K^n \to K$ be a nondegenerate quadratic form, and let $W \subset K^n$ be a totally isotropic subspace of dimension r. Then $q \cong \mathbb{H}^r \oplus q'$.*

Proposition 1. *Let q be a nondegenerate, isotropic quaternary quadratic form over a field K of characteristic different from 2. The following are equivalent:*
(i) q is hyperbolic.
(ii) $\operatorname{disc} q = 1$.
(iii) q admits a two-dimensional totally isotropic subspace.

Proof. (i) $\implies$ (ii): A quaternary hyperbolic form q is equivalent to the diagonal form $(1, -1, 1, -1)$, which has discriminant 1.

(ii) $\implies$ (i): Since q is isotropic, by Fact 3, $q \cong \mathbb{H} \oplus q'$, with q' binary. We have

$$1 = \operatorname{disc} q = (\operatorname{disc} \mathbb{H}) \cdot (\operatorname{disc} q') = -\operatorname{disc} q',$$

so $\operatorname{disc} q' = -1$. By Fact 2, $q' \cong \mathbb{H}$, so $q \cong \mathbb{H} \oplus \mathbb{H}$.

(i) $\implies$ (iii): We may assume $q = \mathbb{H} \oplus \mathbb{H} = (1, -1, 1, -1)$, in which case $W = \langle e_1 - e_2, e_3 - e_4 \rangle$ is a 2-dimensional totally isotropic subspace.

(iii) $\implies$ (i): This follows immediately from Fact 4. □

3. Quaternary Forms of Square Discriminant

3.1. A Multiplicative Identity

Lemma 2. *(Lagrange [19]) Let R be a commutative ring, and let $a, b, x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4$ be elements of R. Then:*

$$(x_1^2 + ax_2^2 + bx_3^2 + abx_4^2)(y_1^2 + ay_2^2 + by_3^2 + aby_4^2) = (x_1y_1 - ax_2y_2 - bx_3y_3 - abx_4y_4)^2$$

$$+a(x_1y_2 + x_2y_1 + bx_3y_4 - bx_4y_3)^2 + b(x_1y_3 - ax_2y_4 + x_3y_1 + ax_4y_2)^2$$

$$+ab(x_1y_4 + x_2y_3 - x_3y_2 + x_4y_1)^2.$$

Proof. The proof is a direct application of Littlewood's Principle: all purely algebraic identities are trivial to prove (though not necessarily trivial to discover). □

Corollary 3. *Let R be any commutative ring, let $a, b \in R$, and let $q_{a,b}$ be the diagonal quadratic form $(1, a, b, ab)$. Then the set of elements of R which are R-represented by $q_{a,b}$ is multiplicatively closed.*

In view of Corollary 3 we call a quadratic form $q_{a,b}$ *multiplicative.*

3.2. An application of geometry of numbers

Lemma 4. *Let p be an odd prime, and let $q(v)$ be an n-ary quadratic form over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. If $n \geq 3$, then q is isotropic.*

Proof. This is a special case of the Chevalley-Warning Theorem [17, Thm. 10.2.1]. For the convenience of the reader, we give a (yet) more elementary proof.

Step 1: We show that any nondegenerate binary quadratic form $q(x, y)$ over $\mathbb{F}_p$ is universal. By Fact 1 above, we may assume q is diagonal, say $q(x, y) = ax^2 + by^2$, with $ab \in \mathbb{F}_p^\times$. Let $d \in \mathbb{F}_p$. We may rewrite the equation $q(x, y) = d$ as

$$x^2 = \frac{d - by^2}{a}.$$

Then as x and y range over all elements of $\mathbb{Z}/p\mathbb{Z}$, both the left and right hand sides take on $\frac{p-1}{2} + 1 = \frac{p+1}{2}$ distinct values. Since $p < \frac{p+1}{2} + \frac{p+1}{2}$, these values sets cannot be disjoint, which leads to a solution (x, y).

Step 2: It is enough to show every ternary form over $\mathbb{F}_p$ is isotropic; since degenerate forms are isotropic, we may assume $q(x,y,z) = ax^2 + by^2 + cz^2$ with $abc \in \mathbb{F}_p^\times$. By Step 1, there are $x_0, y_0 \in \mathbb{F}_p$ such that $q(x_0, y_0) = -c$, and then $q(x_0, y_0, 1) = 0$. $\square$

Theorem 5. *Let $q(v)$ be a nondegenerate quaternary integral quadratic form of square discriminant. For each squarefree positive integer n prime to $2 \operatorname{disc} q$, there is an index n^2 subgroup $\Lambda_n \subset \mathbb{Z}^4$ such that for all $v \in \Lambda_n$, $q(v) \equiv 0 \pmod{n}$.*

Proof. `Step 1.` Let $n = p_1 \cdots p_r$, with $p_1, \ldots, p_r$ distinct odd primes. Suppose that for all $1 \leq i \leq r$ there exists a subgroup Λ_i of $\mathbb{Z}^4$ of index p_i^2 such that for all $v \in \Lambda_i$, $q(v) \equiv 0 \pmod{p_i}$. Then taking $\Lambda_n = \bigcap_{i=1}^r \Lambda_i$, an easy Chinese Remainder Theorem argument gives $[\mathbb{Z}^4 : \Lambda_n] = n^2$ and for all $v \in \Lambda_n$, $q(v) \equiv 0 \pmod{n}$.

`Step 2.` We are reduced to considering the case $n = p$ for $p \nmid 2\operatorname{disc}(q)$ and $a \in \mathbb{Z}^+$. Let $\overline{q}$ be the reduction of q modulo p. Since $p \nmid \operatorname{disc}(q)$, $\operatorname{disc} \overline{q} = 1 \pmod{(\mathbb{F}_p^\times)^2}$: in particular $\overline{q}$ is nondegenerate. By Proposition 1, $\overline{q}$ admits a 2-dimensional totally isotropic subspace $W \subset \mathbb{F}_p^4$. Now reduction modulo p induces an isomorphism of commutative groups $\mathbb{Z}^4/(p\mathbb{Z}^4) \xrightarrow{\sim} \mathbb{F}_p^4$. Taking $\Lambda_p = \varphi^{-1}(W)$ gives an index p^2 subgroup of $\mathbb{Z}^4$ such that for all $v \in \Lambda_p$, $q(v) \equiv 0 \pmod{p}$. $\square$

Theorem 6. *(Korkine-Zolotarev) Let $q(v)$ be a positive definite real quaternary quadratic form, and let $\Lambda \subset \mathbb{Z}^4$ be a finite index subgroup. Then there exists $0 \neq v \in \Lambda$ such that*

$$q(v) \leq (4 \operatorname{disc} q)^{\frac{1}{4}} \sqrt{[\mathbb{Z}^4 : \Lambda]}.$$

Proof. In [3, Section X.3.2] the result is stated with $\Lambda = \mathbb{Z}^4$. Our version follows: if $\Lambda = A\mathbb{Z}^4$, replace $q(v)$ with $q(Av)$, of discriminant $(\det A)^2 \operatorname{disc} q = [\mathbb{Z}^4 : \Lambda]^2 \operatorname{disc} q$. $\square$

For a positive definite real quaternary quadratic form q, put

$$\mathrm{KZ}(q) = (4 \operatorname{disc} q)^{\frac{1}{4}},$$

$$M(q) = \left(\frac{4\sqrt{2}}{\pi}\right) (\operatorname{disc} q)^{\frac{1}{4}} = \left(\frac{4}{\pi}\right) \mathrm{KZ}(q).$$

Theorem 7. *Let $q(x,y,z,w)$ be a positive definite integral quadratic form of square discriminant. Let $n \in \mathbb{Z}^+$ be squarefree and prime to $2 \operatorname{disc} q$. Then there exist $x, y, z, w, k \in \mathbb{Z}$ such that*

$$q(x,y,z,w) = kn$$

and

$$1 \leq k \leq \lfloor (4 \operatorname{disc} q)^{\frac{1}{4}} \rfloor = \lfloor \mathrm{KZ}(q) \rfloor.$$

Proof. Applying Theorem 6 to Λ_n from Theorem 5, we get $v \in \mathbb{Z}^4$ such that

$$q(v) \equiv 0 \pmod{n}$$

and

$$0 < q(v) \le (4 \operatorname{disc} q)^{\frac{1}{4}} \sqrt{[\mathbb{Z}^4 : \Lambda]} = \mathrm{KZ}(q) \cdot n. \tag{3}$$

□

Theorem 6 is classical, but not so easy. One gets a version of Theorem 6 with a slightly worse constant more easily by applying Minkowski's Convex Body Theorem to the ellipsoids $\Omega_R = q(x, y, z, w) \le R^2$: there is a nonzero element $v \in \Lambda$ with

$$q(v) \le \frac{4\sqrt{2}}{\pi} (\operatorname{disc} q)^{\frac{1}{4}} \sqrt{[\mathbb{Z}^4 : \Lambda]}$$

and thus a version of Theorem 7 with (3) replaced by

$$1 \le k \le \left\lfloor \frac{4\sqrt{2}}{\pi} (\operatorname{disc} q)^{\frac{1}{4}} \right\rfloor = \lfloor M(q) \rfloor = \left\lfloor \frac{4}{\pi} \mathrm{KZ}(q) \right\rfloor. \tag{4}$$

In all the cases considered here we can make do with $M(q)$ instead of $\mathrm{KZ}(q)$.

4. Nine Universality Theorems

CONVENTION: For the remainder of this paper, all quadratic forms considered will be positive definite quadratic forms over $\mathbb{Z}$, so we make the convention that "form" means "positive definite quadratic form over $\mathbb{Z}$," a representation of n means a $\mathbb{Z}$-representation of the integer n, and "universal" means "positive universal," i.e., the form q integrally represents every positive integer.

4.1. Some History of Universal Forms

Recall the following theorem, a high water mark of classical number theory.

Theorem 8. *(Lagrange [19]) Every positive integer is the sum of four squares.*

Proof. Apply Corollary 3 with $a = b = 1$: we get the set of integers $\mathbb{Z}$-represented by $q = (1, 1, 1, 1)$ is multiplicatively closed. Since $1 = 1^2 + 0^2 + 0^2 + 0^2$ and $2 = 1^2 + 1^2 + 0^2 + 0^2$ are represented by q, it's enough to show q $\mathbb{Z}$-represents every odd prime p. Apply Theorem 7 with $n = p$: there are $x, y, z, w, k \in \mathbb{Z}$ such that

$$x^2 + y^2 + z^2 + w^2 = kp,$$

with

$$1 \le k \le \lfloor (4 \operatorname{disc} q)^{\frac{1}{4}} \rfloor = \lfloor \sqrt{2} \rfloor = 1.$$

Thus $k = 1$ and every odd prime is a sum of four squares: done! □

Thus Lagrange's Theorem is the assertion that $(1, 1, 1, 1)$ is universal. Which other forms are universal? As we have already mentioned, Liouville proved several further universality theorems [20], [21]. The following result surveys more recent work. (When we enumerate forms, we really mean integral equivalence classes of forms.)

Theorem 9. *a) There is no universal form in fewer than four variables.*
b) For every $n \geq 5$, there are infinitely many universal forms.
c) (Ramanujan-Dickson) There are precisely 54 diagonal *universal quaternary forms.*
d) (Halmos) A diagonal quaternary form is universal iff it represents 1 *through* 15*.*
e) (Conway-Schneeberger, Bhargava) A classical form is universal iff it represents 1 *through* 15*. Moreover there are precisely* 204 *such forms.*
f) (Bhargava-Hanke) A form is universal iff it represents 1 *through* 290*. Moreover there are, up to equivalence, precisely* 6436 *such quaternary forms.*

Proof. a) See e.g. [4, p. 142]. b) Since $q_{1,1}$ is universal, for all $n \geq 4$ and all $d \in \mathbb{Z}^+$ so is $(1, \ldots, 1 \text{ ($n$ times)}, d)$. This exhibits infinitely many pairwise nonisomorphic universal $(n + 1)$-ary forms for all $n \geq 4$. c) See [24] and [7]. d) See [14]. This follows directly from the proof of part c), but P.R. Halmos seems to have been the first to have explicitly noticed this. e) See [5] and [1]. f) See [2]. □

Parts b) through f) of Theorem 9 rely heavily on the theory of *ternary forms* as well as the local theory over $\mathbb{Q}_p$ and $\mathbb{Z}_p$. Thus these proofs are not elementary in our sense, but we hope to apply GoN methods to ternary forms in the near future. Parts b) through e) are still relatively elementary in the sense of not requiring high technology: especially, Bhargava's proof of the "15 Theorem" is a triumph of insight over hard computations or deep theory. In contrast, the proof of the "290 Theorem" uses both lengthy computer calculations and sophisticated modular forms theory.

What about GoN methods? Our GoN proof Theorem 8 is far from the first. Rather Hermite was first [15]. Another GoN proof was given by J.H. Grace [13].

The results of §3 bring GoN methods to bear on all quaternary forms of square discriminant. The work of Bhargava-Hanke shows that there are 112 such universal forms – a sizable number – so it makes sense to concentrate first on diagonal forms. Of the 54 universal diagonal forms, nine have square discriminant:

$$(1, 1, 1, 1),\ (1, 1, 2, 2),\ (1, 1, 3, 3),\ (1, 2, 2, 4),\ (1, 2, 3, 6), (1, 2, 4, 8),\ (1, 2, 5, 10), \quad (5)$$

$$(1, 1, 1, 4),\ (1, 1, 2, 8). \quad (6)$$

Remark. It is an easy exercise to write down a list of 54 forms such that any universal quaternary form is integrally equivalent to *at most one* form in the list. In particular, it is elementary to see that there can be no diagonal universal forms of square discriminant other than the nine listed in (5) and (6).

The seven forms of (5) are multiplicative forms $q_{a,b} = (1, a, b, ab)$ – whereas the two forms of (6) are not, although $(1, 1, 1, 4)$ is closely related to $q_{1,1}$ and $(1, 1, 2, 8)$ is closely related to $q_{1,2}$.

We will show that all of these forms are universal. First observe:

Lemma 10. *A form representing all squarefree positive integers is universal.*

Proof. Every positive integer n may be written uniquely in the form $A^2 b$ with b squarefree. If $q(x_1, \ldots, x_n) = b$, then $q(Ax_1, \ldots, Ax_n) = A^2 b = n$. □

4.2. Binary Subforms

Theorem 11. *a) A prime $p > 2$ is represented by $x^2 + y^2$ iff $p \equiv 1 \pmod 4$.*
b) A prime $p > 2$ is represented by $x^2 + 2y^2$ iff $p \equiv 1, 3 \pmod 8$.
c) A prime $p > 3$ is represented by $x^2 + 3y^2$ iff $p \equiv 1 \pmod 3$.
d) A prime $p > 2$ is represented by $x^2 + 4y^2$ iff $p \equiv 1 \pmod 4$.
e) A prime $p > 5$ is represented by $x^2 + 5y^2$ iff $p \equiv 1, 9 \pmod{20}$.
f) A prime $p > 5$ is represented by $2x^2 + 5y^2$ iff $p \equiv 7, 13, 23, 27 \pmod{40}$.

Proof. These results are part of the classical theory of binary forms; the point is to give completely elementary proofs. For treatment using the Thue-Vinogradov Lemma, see [10]. For treatment using GoN, see [11]. □

4.3. Six Multiplicative Forms

Let $q = q_{a,b}$ be one of the forms of (5). One checks that q represents all primes $p \leq \operatorname{disc} q$. By Lemma 2, to establish universality it suffices to show q represents every $p > \operatorname{disc} q$. By Theorem 7, for any such p there are $x, y, z, w, k \in \mathbb{Z}$ such that

$$q(x, y, z, w) = kp, \ 1 \leq k \leq M(q) = \left\lfloor \frac{4\sqrt{2}}{\pi} (\operatorname{disc} q)^{\frac{1}{4}} \right\rfloor.$$

Theorem 12. *The form $q_{1,2} = x^2 + y^2 + 2z^2 + 2w^2$ is universal.*

Proof. By Theorem 11a), it suffices to show that $q_{1,2}$ represents every prime $p \equiv 3 \pmod 4$; fix such a p. We have $M(q_{1,2}) = 2$, so there are $k, x, y, z, w \in \mathbb{Z}$ with

$$x^2 + y^2 + 2z^2 + 2w^2 = kp, \ k \in \{1, 2\}.$$

If $k = 1$, we're done, so suppose $x^2 + y^2 + 2z^2 + 2w^2 = 2p$. Then $x \equiv y \pmod 2$.
`Case 1.` x and y are both even. So we may take $x = 2X$, $y = 2Y$ to get

$$2X^2 + 2Y^2 + z^2 + w^2 = p.$$

`Case 2.` x and y are both odd. Then

$$p = \frac{1}{2}(x^2+y^2)+z^2+w^2 = \left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 + z^2+w^2 = X^2+Y^2+z^2+w^2.$$

Since $p \equiv 3 \pmod 4$, exactly 3 of X, Y, z, w are odd: without loss of generality suppose z and w are odd. Then

$$p = X^2+Y^2+2\left(\frac{z+w}{2}\right)^2 + 2\left(\frac{z-w}{2}\right)^2 = X^2+Y^2+2Z^2+2W^2. \qquad \square$$

Theorem 13. *The form* $q_{1,3} = x^2+y^2+3z^2+3w^2$ *is universal.*

Proof. Here $M(q_{1,3}) = 3$, so for all $p > 3$, there are $k, x, y, z, w \in \mathbb{Z}$ with

$$x^2+y^2+3z^2+3w^2 = kp, \; k \in \{1,2,3\}.$$

`Case 1.` Suppose $k = 2$. Then $x+y$ and $z+w$ have the same parity.
`Subcase a.` Suppose $x+y$, $z+w$ are both even. Then $\frac{x\pm y}{2}, \frac{z\pm w}{2} \in \mathbb{Z}$, so

$$\left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 + 3\left(\frac{z+w}{2}\right)^2 + 3\left(\frac{z-w}{2}\right)^2 = \frac{2p}{2} = p.$$

`Subcase b.` $x+y$ and $z+w$ are both odd. Without loss of generality x and z are odd and y and w are even, so

$$2p \equiv x^2+y^2+3z^2+3w^2 \equiv 1+3 \equiv 0 \pmod 4,$$

so p is even, contradiction.
`Case 2.` Suppose $k = 3$, i.e., $x^2+y^2+3z^2+3w^2 = 3p$. Then $3 \mid x^2+y^2$, so x and y are both divisible by 3. Substituting $x = 3X$, $y = 3Y$ and simplifying gives

$$z^2+w^2+3X^2+3Y^2 = p. \qquad \square$$

Theorem 14. *The form* $q_{2,2} = x^2+2y^2+2z^2+4w^2$ *is universal.*

Proof. It suffices to show that $q_{2,2}$ represents every prime $p > 2$. Taking $z = w = 0$ and applying Theorem 11b), we see q represents all $p \equiv 1, 3 \pmod 8$; taking $y = z = 0$ and applying Theorem 11d), we see $q_{2,2}$ represents all $p \equiv 1 \pmod 4$, so we may assume $p \equiv 7 \pmod 8$. By Theorem 8, there are $x, y, z, w \in \mathbb{Z}$ such that

$$x^2+y^2+z^2+w^2 = p. \tag{7}$$

Up to order, the only way to write 7 as a sum of three squares in $\mathbb{Z}/8\mathbb{Z}$ is $7 = 1+1+1+4$, so we may assume that in (7) we have y, z odd and w even, and thus

$$x^2+y^2+z^2+w^2 = x^2+2\left(\frac{y-z}{2}\right)^2 + 2\left(\frac{y+z}{2}\right)^2 + 4\left(\frac{w}{2}\right)^2 = p. \qquad \square$$

Theorem 15. *The form* $q_{2,3} = x^2 + 2y^2 + 3z^2 + 6w^2$ *is universal.*

Proof. (Liouville [20]) Let $n \in \mathbb{Z}^+$. By Theorem 8, there are $x, y, z, w \in \mathbb{Z}$ with $n = x^2 + y^2 + z^2 + w^2$. After replacing some of x, y, z, w by their negatives and reordering, we may assume $3 \mid (y + z + w)$; further, two of y, z, w must have the same parity, so after reordering them we may assume $y \equiv z \pmod 2$. Then $Z = \frac{y+z+w}{3}$, $W = \frac{y+z-2w}{2}$, $Y = \frac{y-z}{2}$ are all integers, and, as one readily checks,

$$n = x^2 + y^2 + z^2 + w^2 = x^2 + 2Y^2 + 3Z^2 + 6W^2. \qquad \square$$

Theorem 16. *The form* $q_{2,4} = x^2 + 2y^2 + 4z^2 + 8w^2$ *is universal.*

Proof. It suffices to show that q represents each $p > 2$. By Theorem 11d), every $p \equiv 1 \pmod 4$ is represented by $x^2 + 4z^2$, so we may assume $p \equiv 3 \pmod 4$. By Theorem 14 there are $x, y, z, w \in \mathbb{Z}$ such that

$$p = x^2 + 2y^2 + 2z^2 + 4w^2. \tag{8}$$

If y is even, put $y = 2Y$ to get $p = x^2 + 2z^2 + 4w^2 + 8Y^2$; and similarly if z is even. So suppose y and z are both odd. Also x is odd, so reducing (8) modulo 4 gives

$$p \equiv x^2 + 2y^2 + 2z^2 + 4w^2 \equiv 1 + 2 + 2 \equiv 1 \pmod 4. \qquad \square$$

4.4. Two Non-Multiplicative Forms

Theorem 17. *The form* $q = x^2 + y^2 + z^2 + 4w^2$ *is universal.*

Proof. Let $n \in \mathbb{Z}^+$ be squarefree, so in particular $4 \nmid n$. By Theorem 8 there are $x, y, z, w \in \mathbb{Z}$ such that $n = x^2 + y^2 + z^2 + w^2$. Since $4 \nmid n$, x, y, z, w cannot all be odd. Without loss of generality, $w = 2W$ for $W \in \mathbb{Z}$ and thus

$$n = x^2 + y^2 + z^2 + (2W)^2 = x^2 + y^2 + z^2 + 4W^2. \qquad \square$$

Theorem 18. *The form* $q = x^2 + y^2 + 2z^2 + 8w^2$ *is universal.*

Proof. `Step 1.` We claim q represents every $n \equiv 3 \pmod 4$. By Theorem 12 there are $x, y, z, w \in \mathbb{Z}$ such that

$$n = x^2 + y^2 + 2z^2 + 2w^2. \tag{9}$$

If w is even, we may substitute $w = 2W$ to get $n = x^2 + y^2 + 2z^2 + 8W^2$, and similarly if z is even. Thus we may assume z, w are both odd. Reducing (9) modulo 4 gives $n \equiv x^2 + y^2 \pmod 4$, so $n \not\equiv 3 \pmod 4$.

`Step 2.` Suppose n_1 and n_2 are odd positive integers both represented by q. We claim that n_1n_2 is also represented by q. Indeed, if

$$n_1 = x_1^2 + x_2^2 + 2x_3^2 + 2(2x_4)^2, \; n_2 = y_1^2 + y_2^2 + 2y_3^2 + 2(2y_4)^2,$$

then by Lemma 2 we have

$$n_1n_2 = z_1^2 + z_2^2 + 2z_3^2 + 2(2x_1y_4 + x_2y_3 - x_3y_2 + 2x_4y_1)^2. \tag{10}$$

with $z_1, z_2, z_3 \in \mathbb{Z}$. Equation (10) exhibits n_1n_2 in the form $q(v)$ iff $x_2y_3 - x_3y_2$ is even. Since n_1 is odd, then $x_1^2 + x_2^2$ is odd and thus exactly one of x_1, x_2 is even. By interchanging x_1 and x_2 if necessary, we may assume that x_2 is even. In exactly the same way we may assume that y_2 is even and thus that $x_2y_3 - x_3y_2$ is even.
Step 3: Every odd $n \in \mathbb{Z}^+$ is represented by q. By Step 2 it is enough to show that every odd prime number p is represented by q. If $p \equiv 1 \pmod 4$, then by Theorem 11a) $p = x_1^2 + x_2^2$, whereas if $p \equiv 3 \pmod 4$ then q represents p by Step 1.
Step 4: Suppose $n = 2n' \equiv 2 \pmod 4$. Since n' is odd, by Step 3, there are integers y_1, y_2, y_3, y_4, with $y_2 = 2Y_2$, such that $n' = y_1^2 + y_2^2 + 2y_3^2 + 2(2y_4)^2$. Then

$$\begin{aligned} n = 2 \cdot n' &= (0^2 + 0^2 + 2 \cdot 1^2 + 2(2 \cdot 0)^2)(y_1^2 + y_2^2 + 2y_3^2 + 2(2y_4)^2) \\ &= z_1^2 + z_2^2 + z_3^2 + 2(-y_2)^2 = z_1^2 + z_2^2 + z_3^2 + 8Y_2^2. \end{aligned}$$

□

4.5. The Form $q_{2,5} = (1, 2, 5, 10)$

Theorem 19. *The form $q_{2,5} = x^2 + 2y^2 + 5z^2 + 10w^2$ is universal.*

To prove Theorem 19 we need to clarify and systematize the rather *ad hoc* methods used for the other universality proofs, so we begin by laying out a general strategy.

Let $q(v)$ be an n-ary integral quadratic form, and let $d \in \mathbb{Z}$. We wish to show that q represents d, and say we know that it integrally represents kd for some "small" positive integer k, i.e., there exists $x \in \mathbb{Z}^n$ such that $q(x) = kd$.

Suppose first that we can find $A \in M_n(\mathbb{Z})$ such that we have an identity of quadratic forms $q(Av) = kq(v)$. Then $q(Ax) = kq(x) = k^2d$, and thus

$$q(A\left(\frac{x}{k}\right)) = d.$$

This gives an integral representation of d by q *provided* $Ax \in (k\mathbb{Z})^n$, a condition which depends only the classes of $x_1, \ldots, x_n \pmod k$. Since $q(x) = kd$, we need only consider admissible n-tuples, i.e., $(x_1, \ldots, x_n) \in (\mathbb{Z}/k\mathbb{Z})^n$ such that $q(x_1, \ldots, x_n) \equiv 0 \pmod k$. And we do not need the same matrix A to work for each admissible n-tuple: we only need that for each admissible n-tuple $x \in (\mathbb{Z}/k\mathbb{Z})^n$ there is *some* $A_x \in M_n(\mathbb{Z})$ such that $q(Av) = kq(v)$ and $A_xx \equiv 0 \pmod k$.

However, in most cases this is asking too much.

Lemma 20. *For all $k \in \mathbb{Z}^+$, $\{A \in M_n(\mathbb{Z}) \mid q(Av) = kq(v)\}$ is finite.*

Proof. $M_n(\mathbb{R})$ is an n^2-dimensional Euclidean space in which $M_n(\mathbb{Z})$ sits as a discrete subgroup. Since q is positive definite, the set of $A \in M_n(\mathbb{R})$ with $q(Av) = kq(v)$ for all $v \in \mathbb{R}^n$ is bounded, so its intersection with $M_n(\mathbb{Z})$ is finite.

However, for our applications we want an algorithmic enumeration of $O_q(k)$. This can be achieved by revisiting the above argument more quantitatively.
`Step 1.` Suppose $q = q_0 = x_1^2 + \ldots + x_n^2$, so

$$O_q(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid q(Av) = q(v)\}$$

is the standard real orthogonal group $O_n(\mathbb{R})$. $M_n(\mathbb{R})$ endowed with the *Frobenius norm* $A = (a_{ij}) \mapsto |A| = \sqrt{\sum_{1 \le i,j \le n} a_{ij}^2}$ is a Banach algebra: for all $A, B \in M_n(\mathbb{R})$, $|AB| \le |A||B|$ (this amounts to the Cauchy-Schwarz inequality). Let $q_0 = x_1^2 + \ldots + x_n^2$. Then $O_{q_0}(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid q_0(Av) = q(v)\}$ is the standard orthogonal group $O_n(\mathbb{R})$, and thus for all $A \in O_{q_0}(\mathbb{R})$, $|A| = \sqrt{n}$. All positive definite n-ary forms are $\mathbb{R}$-equivalent, so choose $P \in \mathrm{GL}_n(\mathbb{R})$ such that $q(v) = q_0(Pv)$. Then $O_q(\mathbb{R}) = P^{-1}O_{q_0}(\mathbb{R})P$: if $A \in O_{q_0}(\mathbb{R})$, then $q(P^{-1}APv) = q_0(APv) = q_0(Pv) = q(v)$, and conversely. So for $A \in O_q(\mathbb{R})$,

$$|A| = |P^{-1}PAP^{-1}P| \le |P^{-1}||PAP^{-1}||P| \le \sqrt{n}|P||P^{-1}|.$$

`Step 2.` For $A \in M_n(\mathbb{R})$, $k \in \mathbb{R}^{>0}$, $q(Av) = kq(v)$ iff $q(\frac{A}{\sqrt{k}}v) = q(v) \iff \frac{A}{\sqrt{k}} \in O_q(\mathbb{R})$. Thus if $A \in M_n(\mathbb{R})$ and $q(Av) = kq(v)$,

$$|A| \le \sqrt{kn}|P||P^{-1}|.$$

So we may compute $O_q(k)$ by running through $\{A \in M_n(\mathbb{Z}) \mid |A| \le \sqrt{kn}|P||P^{-1}|\}$ and testing to see whether $q(Av) = kq(v)$ holds. $\square$

Remark. The algorithm given above was chosen because it is (we hope) easily understood by a wide audience. We do not claim any particular efficiency.

However, we may also consider matrices with denominators. For $k, r \in \mathbb{Z}^+$, put

$$O_q(k, r) = \{A \in M_n(\mathbb{Z}) \mid q\left(\frac{A}{r}v\right) = kq(v)\} = \{A \in M_n(\mathbb{Z}) \mid q(Av) = kr^2q(v)\}.$$

By Lemma 20, $O_q(k, r)$, is finite *for each fixed k and r*, but for fixed k the sets $O_q(k, r)$ tend to grow in size with r.[2] This improves our chances of success: we say a tuple $x \in (\mathbb{Z}/kr\mathbb{Z})^n$ is *admissible* if $q(x) \equiv 0 \pmod{k}$. Let $A_q(k, r)$ denote the set of all admissible tuples. We say that $O_q(k, r)$ *covers* $A_q(k, r)$ if for each $x \in A_q(k, r)$, there exists $A_x \in O_q(k, r)$ such that $A_x x \equiv 0 \pmod{kr}$. If for some

[2] One can show that for any multiplicative form q, for all $k \in \mathbb{Z}^+$, $\bigcup_{r=1}^{\infty} O_q(k, r)$ is infinite.

$r \in \mathbb{Z}^+$ we have that $O_q(k,r)$ covers $A_q(k,r)$, then for all $d \in \mathbb{Z}^+$, if there exists $x \in \mathbb{Z}^n$ such that $q(x) = kd$, then $A_x\left(\frac{x}{kr}\right) \in \mathbb{Z}^n$ and $q(A_x\left(\frac{x}{kr}\right)) = d$.

We now turn to the proof of Theorem 19. As usual, we apply Theorem 7: since $\lfloor M(q) \rfloor = 5$, for any prime $p > 5$ there exists $(x,y,z,w) \in \mathbb{Z}^4$ with $x^2 + 2y^2 + 5z^2 + 10w^2 = kp$ with $k \in \{1,2,3,4,5\}$. So to complete the proof, it suffices to find, for each $k \in \{2,3,4,5\}$, a positive integer r such that $O_q(k,r)$ covers $A_q(k,r)$.

Theorem 21. *Let $q = q_{2,5} = x^2 + 2y^2 + 5z^2 + 10w^2$. Then:*
a) The 26768 elements of $O_q(2,8)$ cover all $\#A_q(2,8) = 32768$ admissible tuples, and thus for all $d \in \mathbb{Z}^+$, if q represents $2d$ then it also represents d.
b) For no $r < 8$ does $O_q(2,r)$ cover $A_q(2,r)$.
c) The 83072 elements of $O_q(3,8)$ cover all $\#A_q(3,8) = 135168$ admissible tuples, and thus for all $d \in \mathbb{Z}^+$, if q represents $3d$ then it also represents d.
d) For no $r < 8$ does $O_q(3,r)$ cover $A_q(3,r)$.
e) The 10384 elements of $O_q(4,4)$ cover all $\#A_q(4,4) = 16384$ admissible tuples.
f) For no $r < 4$ does $O_q(4,r)$ cover $A_q(4,r)$.
g) The 16 elements of $O_q(5,1)$ cover all $\#A_q(5,1) = 25$ admissible tuples, and thus for all $d \in \mathbb{Z}^+$, if q represents $5d$ then it also represents d.

Proof. A computer calculation. The C++ code used for this may be found at `http://www.math.uga.edu/~pete/MinimalCode.cpp`. □

This completes the proof of Theorem 19.

Remark. Notice that – without any GoN input – Theorem 21a) yields:

Theorem 22. *For all $d \in \mathbb{Z}^+$, if $q_{2,5}$ represents $2d$, then it also represents d.*

As described in the introduction, Theorem 22 completes a quaternionic proof of the universality of $(1,2,5,10)$ initiated by Deutsch and continued by Fitzgerald.

Remark. The case $k = 5$ is easy enough to be treated by hand. Indeed, if $x^2 + 2y^2 + 5z^2 + 10w^2 = 5p$, then $5 \mid (x^2 + 2y^2)$, so x and y are both divisible by 5. Putting $x = 5X$, $y = 5Y$ and simplifying gives $z^2 + 2w^2 + 5X^2 + 10Y^2 = p$.

References

[1] M. Bhargava, *On the Conway-Schneeberger fifteen theorem*. Quadratic forms and their applications (Dublin, 1999), 27–37, Contemp. Math., 272, Amer. Math. Soc., Providence, RI, 2000.

[2] M. Bhargava and J.P. Hanke, *Universal quadratic forms and the 290-theorem*, preprint.

[3] J.W.S. Cassels, *An introduction to the geometry of numbers*. Corrected reprint of the 1971 edition. Classics in Mathematics. Springer-Verlag, Berlin, 1997.

[4] J. H. Conway, *The sensual (quadratic) form*, Carus Mathematical Monographs 26, MAA, 1997.

[5] J.H. Conway, *Universal quadratic forms and the fifteen theorem.* Quadratic forms and their applications (Dublin, 1999), 23–26, Contemp. Math., 272, Amer. Math. Soc., Providence, RI, 2000.

[6] J.I. Deutsch, *A quaternionic proof of the universality of some quadratic forms.* Integers 8 (2008), no. 2, A3, 23 pp.

[7] L.E. Dickson, *Integers represented by positive ternary quadratic forms.* Bull. Amer. Math. Soc. 33 (1927), 63–70.

[8] L. Euler, *Opera Omnia IV.A-4. The Correspondence Euler - Goldbach* F. Lemmermeyer, M. Mattmüller, eds., Basel 2011.

[9] R.W. Fitzgerald, *Norm Euclidean quaternionic orders.* Integers 11 (2011), A58, 12 pp.

[10] P.L. Clark, *Thue-Vinogradov and integers of the form* $x^2 + Dy^2$, 2011 preprint.

[11] P.L. Clark, J. Hicks, H. Parshall, and K. Thompson, *GoNI: Binary quadratic forms*, submitted.

[12] J. Hicks and K. Thompson, *GoNIII: More universal quaternary forms*, in preparation.

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

[14] P.R. Halmos, *Note on almost-universal forms.* Bull. Amer. Math. Soc. 44 (1938), 141–144.

[15] C. Hermite, *Sur la théorie des formes quadratiques, II.* J. Reine Angew. Math. 47 (1854), 343–368.

[16] A. Hurwitz, *Vorlesungen über die Zahlentheorie der Quaternionen.* Berlin, 1919.

[17] K. Ireland and M. Rosen, *A classical introduction to modern number theory.* Second edition. Graduate Texts in Mathematics, 84. Springer-Verlag, New York, 1990.

[18] T.Y. Lam, *Introduction to quadratic forms over fields.* Graduate Studies in Mathematics, 67. American Mathematical Society, Providence, RI, 2005.

[19] J.L. Lagrange, *Démonstration d'un Théorème D'Arithmétique*, Nouv. Mém. Acad. Roy. Sc. de Berlin, année 1770, Berlin, 1772, 123–133, Oeuvres, 3, 1869, 189–201.

[20] J. Liouville, *Sur Les Deux Formes* $x^2 + y^2 + z^2 + t^2, x^2 + 2y^2 + 3z^2 + 6t^2$. Jour. de Math., (1) 10, (1845), 169–170.

[21] J. Liouville, *Sur La Représentation Des Nombres Par La Forme Quadratique* $x^2 + ay^2 + bz^2 + abt^2$. Jour. de Math., (2) 1, (1856), 230.

[22] H. Minkowski, *Geometrie der Zahlen*, Leipzig and Berlin, 1910.

[23] L.J. Mordell, *The representation of numbers by some quaternary quadratic forms.* Acta Arith. 12 (1966/1967), 47–54.

[24] Ramanujan, *On the expression of a number in the form* $ax^2 + by^2 + cz^2 + du^2$, Proceedings of the Cambridge Philosophical Society 19 (1917), 11–21.