

GONII: UNIVERSAL QUATERNARY QUADRATIC FORMS

PETE L. CLARK, JACOB HICKS, KATHERINE THOMPSON, AND NATHAN WALTERS

CONTENTS

1. Introduction	1
2. Review of Quadratic Forms	2
2.1. Quadratic forms over a ring	2
2.2. Quadratic forms over a field of characteristic different from 2	3
2.3. Totally isotropic subspaces	4
3. Quaternary Forms of Square Discriminant	4
3.1. A generalized Euler identity	4
3.2. An application of geometry of numbers	5
4. Nine Universality Theorems	7
4.1. Some history of universal forms	7
4.2. Binary subforms	8
4.3. Six multiplicative forms	9
4.4. Two non-multiplicative forms	11
4.5. The form $(1, 2, 5, 10)$	12
References	14

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 [GoN1] treats primes represented by positive definite integral binary quadratic forms, this paper concerns the universality of positive definite quaternary integral quadratic forms.

We use GoN methods to prove a theorem (Theorem 7) on representation of small multiples of a positive integer by a given positive definite quaternary integral quadratic form of square discriminant. Although this result should have somewhat wider application, in this paper we restrict our attention to *diagonal* forms. Work of Ramanujan [Ra17] and Dickson [Di27] shows that there are, up to isomorphism, precisely nine diagonal positive definite quaternary integral quadratic forms of square discriminant which integrally represent all positive integers. Here we succeed in using Theorem 7 to give elementary GoN proofs of the universality of all nine of these forms. In some cases we make use of results from [GoN1].

The complexity of the proofs increases as we go down the list, and two of the forms required computer assistance. For $(1, 2, 3, 6)$ the proof, once found, was quickly converted into a “hand calculation”. For $(1, 2, 5, 10)$ this does not seem feasible: instead we explain how the result can be reduced to a certain calculation

and include a link to the C++ code used to perform the calculation.

Two prior works are sufficiently closely related to the present work to merit discussion and comparison here. A late paper of L.J. Mordell [Mo66] uses GoN methods to prove universality theorems for diagonal quaternary integral quadratic forms. We were not aware of [Mo66] when we began the present work, but finding and reading it was a crucial step forward. Mordell’s paper is somewhat tersely written, and is moreover exemplary rather than comprehensive. Of the nine forms treated here, four are mentioned by Mordell, two of which merit only a one line remark. Especially, Mordell writes “It is well known that the case $a = 2$, $b = 3$ is the same as $a = b = 1$.” We do not doubt him, but this argument was not well known to *us*. We took the hint – eventually – but even so this was one of the hardest forms. The last line of Mordell’s paper is “There is no need to give further instances of the method.” With all due respect to the Master, we must disagree!

The second is a recent paper of J.I. Deutsch [De08], which also gives universality proofs for diagonal positive definite quaternary integral quadratic forms of square discriminant. Whereas we are inspired by the GoN proofs of the four squares theorem due to Hermite, Minkowski and Grace, Deutsch takes inspiration from Hurwitz’s proof of the four squares theorem using quaternion arithmetic, especially Euclidean quaternion orders. He is able to give Hurwitz-style universality proofs for eight of the nine forms, but not $(1, 2, 5, 10)$. Further Hurwitz-style study of $(1, 2, 5, 10)$ occurs in [Fi11]; Fitzgerald shows that $(1, 2, 5, 10)$ represents $16n$ for all $n \in \mathbb{Z}^+$ but laments the absence of a descent argument to go from representations of $2n$ to representations of n . Precisely this descent is a key step in our proof, which may therefore also be viewed as completing work of Deutsch and Fitzgerald.

We acknowledge that quaternionic methods are clearly relevant to the present work, but we hasten to add that the present work is not simply a case of using quaternions and then hiding them in order to arrive at “more elementary” proofs...or at least, we have not yet managed to view it in that way. As pointed out by Fitzgerald, to each of these nine universal quadratic forms the naturally associated quaternion algebra admits a Euclidean order. The norm form of a Euclidean quaternion order is positive universal...but the nine forms in question here are *non-maximal* lattices inside a maximal lattice corresponding to a Euclidean order. All in all, some mysteries remain!

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 participants 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).

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**

\mathbf{R} is a homogeneous quadratic polynomial

$$(1) \quad q(v) = q(x_1, \dots, x_n) = \sum_{1 \leq i \leq j \leq n} a_{ij} x_i x_j \in R[x_1, \dots, x_n].$$

Two quadratic forms $q(v) = q(x_1, \dots, x_n)$, $q'(v) = q'(x_1, \dots, x_n)$ over R are **equivalent over \mathbf{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 **\mathbf{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 $v \in R^n$, $v \neq (0, \dots, 0)$ 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 $\varphi : R \rightarrow S$ 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

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

Here we will generally have $R = \mathbb{Z}$, and either $\varphi : \mathbb{Z} \rightarrow \mathbb{Q}$, $\varphi : \mathbb{Z} \rightarrow \mathbb{R}$, or $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$. Base change is useful for showing that q *does not* represent $d \in R$: if q R -represents d , then for all homomorphisms $\varphi : R \rightarrow S$, $q_{/S}$ S -represents $\varphi(d)$: indeed, if $q(x_1, \dots, x_n) = d$, then $q_{/S}(\varphi(x_1), \dots, \varphi(x_n)) = \varphi(d)$. (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 integers. 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 $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}/4\mathbb{Z}$, 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 $v = (x_1, \dots, x_n)^t$, we have

$$(2) \quad q(v) = v^t M_q v.$$

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 $M_{q'} = A^t M_q A$. Then $\det M_{q'} = (\det A)^2 \det M_q$, which shows that the class $\mathrm{disc} q$ 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 $\mathrm{disc} q$ is a well-defined integer. In general we say q is **nondegenerate** if $\mathrm{disc} q \neq 0$.

Let $q_1(x_1, \dots, x_m)$ be an m -ary quadratic form over R and $q_2(y_1, \dots, y_n)$ 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 $q(x_1, \dots, x_m, y_1, \dots, y_n) = q_1(x_1, \dots, x_m) + q_2(y_1, \dots, y_n)$.¹

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

¹Here it is to be understood that $x_1, \dots, x_m, y_1, \dots, y_n$ are independent indeterminates.

1 of the theory of quadratic forms over fields (specifically, from [L, Ch. I]).

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

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

Fact 2 [L, Thm. 1.3.2]: For a nondegenerate binary form $q(x, y)$ over K , TFAE:

- (i) q is K -equivalent to the hyperbolic plane \mathbb{H} .
- (ii) $\mathrm{disc} q = -1$.
- (iii) q is isotropic.

Fact 3 [L, Thm. 1.3.4(2)]: For a nondegenerate quadratic form q over K , TFAE:

- (i) q is isotropic.
- (ii) There exists a quadratic form q' such that $q \cong q' \oplus \mathbb{H}$.

An n -ary quadratic form is **hyperbolic** if it is isomorphic to a direct sum of $r = \frac{n}{2}$ copies of the hyperbolic plane. (In particular, n must be even.)

2.3. Totally isotropic subspaces.

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

Fact 4 [L, Thm. 1.3.4(1)]: Let $q : K^n \rightarrow K$ 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. TFAE:*

- (i) q is hyperbolic.
- (ii) $\mathrm{disc} q = 1$.
- (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

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

so $\mathrm{disc} q' = -1$. 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. \square

3. QUATERNARY FORMS OF SQUARE DISCRIMINANT

3.1. A generalized Euler identity.

The following is well known: c.f. e.g. [Mo66, p. 48].

Lemma 2. (*Generalized Euler Identity*) *Let R be any 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:*

$$\begin{aligned} (x_1^2 + ax_2^2 + bx_3^2 + abx_4^2)(y_1^2 + ay_2^2 + by_3^2 + aby_4^2) &= (x_1y_1 - ax_2y_2 - bx_3y_3 - abx_4y_4)^2 \\ &\quad + a(x_1y_2 + x_2y_1 + bx_3y_4 - bx_4y_3)^2 + b(x_1y_3 - ax_2y_4 + x_3y_1 + ax_4y_2)^2 \\ &\quad + ab(x_1y_4 + x_2y_3 - x_3y_2 + x_4y_1)^2. \end{aligned}$$

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). \square

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 $q_{a,b}$ is a **multiplicative form**: the set of elements of R which are R -represented by $q_{a,b}$ is multiplicatively closed.*

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-Waring Theorem [IR, 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, \dots, 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 \bar{q} be the reduction of q modulo p . Since $p \nmid \operatorname{disc}(q)$, $\operatorname{disc} \bar{q} = 1 \pmod{(\mathbb{F}_p^\times)^2}$: in particular \bar{q} is nondegenerate. By Proposition 1, \bar{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. See [Ca, § X.3.2] or [S, § XII.1]. Therein the result is stated with $\Lambda = \mathbb{Z}^4$, but our version follows immediately upon making a change of variables: if $\Lambda = A\mathbb{Z}^4$, then 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

$$\begin{aligned} \operatorname{KZ}(q) &= (4 \operatorname{disc} q)^{\frac{1}{4}}, \\ M(q) &= \left(\frac{4\sqrt{2}}{\pi} \right) (\operatorname{disc} q)^{\frac{1}{4}} = \left(\frac{4}{\pi} \right) \operatorname{KZ}(q). \end{aligned}$$

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

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

Proof. Apply Theorem 6 to the index n^2 sublattice Λ_n of Theorem 5. We get a vector $v \in \mathbb{Z}^4$ such that

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

and

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

\square

Remark 3.1: Theorem 5 holds without the assumption that n is squarefree, as can be seen by considering q/\mathbb{Q}_p , observing that it is isotropic (as is any quaternary p -adic form of unit discriminant), and applying Proposition 1. Such an argument is however not in the spirit of the present work, and it turns out that this stronger result is not helpful in the applications considered here. We hope to return to the question of existence of sublattices like Λ_n in more generality in the future.

The Korkine-Zolotarev theorem is definitely part of classical GoN...but it is not an easy result. One gets a version of Theorem 6 with a slightly worse constant much more easily by applying Minkowski's Convex Body Theorem [HW, Thm. 446] to the ellipsoids $\Omega_R = \{q(x, y, z, w) \leq R^2\}$. Since $\operatorname{Vol}(\Omega_R) = \frac{\pi^2 R^4}{2\sqrt{\operatorname{disc} q}}$, by the Convex Body Theorem there is $v \in \Omega_R \cap (\Lambda \setminus \{0\})$ when

$$\frac{\pi^2 R^4}{2\sqrt{\operatorname{disc} q}} = \operatorname{Vol}(\Omega_R) \geq 2^4 \operatorname{Vol}(R^4/\Lambda) = 2^4 [\mathbb{Z}^4 : \Lambda].$$

So there is $v \in \Lambda \setminus \{0\}$ with

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

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

$$(4) \quad 1 \leq k \leq \lfloor \frac{4\sqrt{2}}{\pi}(\text{disc } q)^{\frac{1}{4}} \rfloor = \lfloor M(q) \rfloor = \lfloor \frac{4}{\pi} \text{KZ}(q) \rfloor.$$

In fact we manage to prove all nine universality theorems using the Minkowski bound $M(q)$ in place of the Korkine-Zolotarev bound $\text{KZ}(q)$. It seems though that we got lucky: for the $(1, 2, 2, 4)$ form in particular our original proof used $\lfloor \text{KZ}(q) \rfloor = 2$, and we were not able to extend this argument so as to work with the weaker bound $\lfloor M(q) \rfloor = 3$. Instead we did something different, namely a reduction to $(1, 1, 1, 1)$ and use of representation theorems for binary subforms.

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) *Every positive integer is the sum of four integral 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

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

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

Thus Lagrange’s Theorem is the assertion that $(1, 1, 1, 1)$ is universal. Which other forms are universal? The following result surveys the work done on this problem.

Theorem 9. *a) There is no universal form in fewer than four variables.*
b) For every $n \geq 5$, there are, up to isomorphism, infinitely many universal forms.
c) (Ramanujan-Dickson) There are, up to equivalence, precisely 54 diagonal universal 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, up to equivalence, 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. [Co, p. 142].² b) Since $(1, 1, 1, 1)$ is universal, for all $n \geq 4$ and all $d \in \mathbb{Z}^+$ so is $q_{n,d} = (1, \dots, 1$ (n times), d). Since $\text{disc } q_{n,d} = d$, this exhibits infinitely many universal $(n + 1)$ -ary forms for all $n \geq 4$. c) See [Ra17] and [Di27].

²Unfortunately we do not know a primary source.

d) See [Ha38]. This follows directly from the proof of part c), but P.R. Halmos seems to have been the first to have explicitly noticed this. Halmos goes on to show there are precisely 86 diagonal quaternary forms which represent all but exactly one positive integer (the point being that this exception must be at most 15). It would be interesting to try to approach this result by GoN methods: we leave this for a possible future work. e) See [Co00] and [Bh00]. f) See [BH05]. \square

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 very far from the first. Rather Hermite was first. And indeed Minkowski gave a proof using the Convex Body Theorem. Another GoN proof was given by J.H. Grace [Gr27].

The results of §3 can be used to handle more than just $(1, 1, 1, 1)$: they apply to (especially multiplicative) quaternary forms of square discriminant. The Bhargava-Hanke classification yields 112 universal quaternary forms of square discriminant – a sizable number – so it makes sense to concentrate first on *diagonal forms*. Of the 54 universal diagonal quaternary forms, 9 have square discriminant:

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

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

Note that the seven forms of (5) are multiplicative forms in the sense of Corollary 3 – i.e., are of the form $(1, a, b, ab)$ – and the latter two are not, although $(1, 1, 1, 4)$ is closely related to $(1, 1, 1, 1)$ and $(1, 1, 2, 8)$ is closely related to $(1, 1, 2, 2)$.

We will use the results of §3 to show that all of these forms are universal.

Every positive integer d may be uniquely written in the form D^2e , with e squarefree. It follows that an integral form which represents every squarefree positive integer is universal: if $q(x_1, \dots, x_n) = e$, then $q(Dx_1, \dots, Dx_n) = D^2e = d$.

4.2. Binary subforms.

- Theorem 10.** *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 $p \equiv 1 \pmod{4}$.*

Proof. For treatment of these forms using elementary combinatorial number theory, see [Cl11, Thms. 15, 17, 19, 21]. For treatment using GoN, see [GoN1]. \square

4.3. Six multiplicative forms.

Let q be one of the seven multiplicative forms of (5). One sees immediately that in all cases q represents all primes $p \leq \text{disc } q$. Applying Lemma 2, to obtain the universality of q it suffices to show that q represents every $p > \text{disc } q$. By Theorem 7, for any such prime number p there exist $x, y, z, w, k \in \mathbb{Z}$ such that

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

The general strategy of the proofs is a case-by-case analysis of $1 < k \leq M(q)$. Sometimes though one of the forms $q' = (1, A, B, AB)$ can be “reduced” to an earlier form $q = (1, a, b, ab)$ on the list: when this happens, $q \cong_{\mathbb{Q}} q'$.

Theorem 11. *The form $q(v) = x^2 + y^2 + 2z^2 + 2w^2$ is universal.*

Proof. Here $M(q) = 2$, so for all $p > 2$, there are $k, x, y, z, w \in \mathbb{Z}$ with

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

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

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

□

Theorem 12. *The form $q(v) = x^2 + y^2 + 3z^2 + 3w^2$ is universal.*

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

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

Case 1: Suppose $k = 2$.

Case 1a): Suppose $x + y, z + w$ are both even. Then $\frac{x \pm y}{2}, \frac{z \pm w}{2} \in \mathbb{Z}$, so

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

and we have found a \mathbb{Z} -representation of p .

Case 1b): $x + y$ 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

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

□

Theorem 13. *The form $q(v) = x^2 + 2y^2 + 2z^2 + 4w^2$ is universal.*

Proof. It suffices to show that q represents every prime $p > 2$. Taking $z = w = 0$ and applying Theorem 10b), we see q represents all $p \equiv 1, 3 \pmod{8}$; taking $y = z = 0$ and applying Theorem 10d), we see q 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

$$(7) \quad x^2 + y^2 + z^2 + w^2 = p.$$

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

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

□

Theorem 14. *The form $q(v) = x^2 + 2y^2 + 3z^2 + 6w^2$ is universal.*

Proof. Step 1: First consider the identity

$$x^2 + (y+z+w)^2 + (y-z-w)^2 + (z-2w)^2 = x^2 + 2y^2 + 3z^2 + 6w^2,$$

and the inverse identity

$$x^2 + y^2 + z^2 + w^2 = x^2 + \left(\frac{y+z}{2}\right)^2 + \left(\frac{y-z+w}{3}\right)^2 + \left(\frac{y-z-2w}{6}\right)^2.$$

Let $n \in \mathbb{Z}^+$. By Theorem 8, there are $x, y, z, w \in \mathbb{Z}$ with $n = x^2 + y^2 + z^2 + w^2$, so

$$n = x^2 + \left(\frac{y+z}{2}\right)^2 + \left(\frac{y-z+w}{3}\right)^2 + \left(\frac{y-z-2w}{6}\right)^2.$$

This gives an integral representation of n by q provided all the following congruence conditions are satisfied:

$$\begin{aligned} y+z &\equiv 0 \pmod{2}, \\ y-z+w &\equiv 0 \pmod{3}, \\ y-z-2w &\equiv 0 \pmod{6}. \end{aligned}$$

Step 2: It suffices to show that q \mathbb{Z} -represents all primes $p > 3$. Since by Theorem 10c), $x^2 + 3y^2$ represents all primes $p \equiv 1 \pmod{3}$, we may assume $p \equiv 5 \pmod{6}$.

Step 3: Let $p \equiv 5 \pmod{6}$ be a prime. As above there are $x, y, z, w \in \mathbb{Z}$ such that

$$(8) \quad p = x^2 + y^2 + z^2 + w^2.$$

Now we consider (8) as a congruence modulo 6. The squares modulo 6 are 0, 1, 3, 4. Without loss of generality we may take the congruence classes of x, y, z, w in non-decreasing order, and then there are four ways for $x^2 + y^2 + z^2 + w^2 \equiv 5 \pmod{6}$:

$$0 + 0 + 1 + 4 \equiv 0 + 1 + 1 + 3 \equiv 0 + 3 + 4 + 4 \equiv 1 + 3 + 3 + 4 \equiv 5 \pmod{6}.$$

Case 1: By adjusting the signs on x, y, z, w we may assume $x \equiv y \equiv 0 \pmod{6}$, $z \equiv 1 \pmod{6}$, $w \equiv 2 \pmod{6}$ and write

$$p = y^2 + 2\left(\frac{w+x}{2}\right)^2 + 3\left(\frac{w-x+z}{3}\right)^2 + 6\left(\frac{w-x-2z}{6}\right)^2.$$

Case 2: We may assume $x \equiv 0 \pmod{6}$, $y \equiv z \equiv 1 \pmod{6}$, $w \equiv 3 \pmod{6}$. Then

$$p = x^2 + 2 \left(\frac{y+z}{2} \right)^2 + 3 \left(\frac{y-z+w}{3} \right)^2 + 6 \left(\frac{y-z-2w}{6} \right)^2.$$

Case 3: We may assume $x \equiv 0 \pmod{6}$, $y \equiv 3 \pmod{6}$, $z \equiv w \equiv 4 \pmod{6}$. Then

$$p = x^2 + 2 \left(\frac{z+w}{2} \right)^2 + 3 \left(\frac{z-w+y}{3} \right)^2 + 6 \left(\frac{z-w-2y}{6} \right)^2.$$

Case 4: We may assume $x \equiv 1 \pmod{6}$, $y \equiv z \equiv 3 \pmod{6}$, $w \equiv 4 \pmod{6}$. Then

$$p = z^2 + 2 \left(\frac{y+x}{2} \right)^2 + 3 \left(\frac{y-x+w}{3} \right)^2 + 6 \left(\frac{y-x-2w}{6} \right)^2.$$

□

Theorem 15. *The form $q(v) = x^2 + 2y^2 + 4z^2 + 8w^2$ is universal.*

Proof. It suffices to show that q represents each $p > 2$. By Theorem 10d), every $p \equiv 1 \pmod{4}$ is represented by $x^2 + 4z^2$, so we may assume $p \equiv 3 \pmod{4}$. By Theorem 13 there are $x, y, z, w \in \mathbb{Z}$ such that

$$(9) \quad p = x^2 + 2y^2 + 2z^2 + 4w^2.$$

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 (9) modulo 4 gives

$$p \equiv x^2 + 2y^2 + 2z^2 + 4w^2 \equiv 1 + 2 + 2 \equiv 1 \pmod{4}.$$

□

4.4. Two non-multiplicative forms.

Theorem 16. *The form $q(v) = x^2 + y^2 + z^2 + 4w^2$ 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

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

□

Theorem 17. *The form $q(v) = x^2 + y^2 + 2z^2 + 8w^2$ is universal.*

Proof. Step 1: We claim q represents every $n \equiv 3 \pmod{4}$. By Theorem 11 there are $x, y, z, w \in \mathbb{Z}$ such that

$$(10) \quad n = x^2 + y^2 + 2z^2 + 2w^2.$$

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 (10) 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 $n_1 n_2$ is also represented by q . Indeed, if

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

then by Lemma 2 we have

$$(11) \quad n_1 n_2 = z_1^2 + z_2^2 + 2z_3^2 + 2(2x_1 y_4 + x_2 y_3 - x_3 y_2 + 2x_4 y_1)^2.$$

with $z_1, z_2, z_3 \in \mathbb{Z}$. Equation (11) exhibits $n_1 n_2$ in the form $q(v)$ iff $x_2 y_3 - x_3 y_2$ is even. Now if 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 $x_2 y_3 - x_3 y_2$ 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 10a) $p = x_1^2 + x_2^2$, 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 $(1, 2, 5, 10)$.

Theorem 18. *The form $q(v) = x^2 + 2y^2 + 5z^2 + 10w^2$ is universal.*

To prove Theorem 18 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 $q(x) = kn$.

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 $q(Ax) = kq(x) = k^2q(v) = k^2d$, and thus

$$q\left(A \begin{pmatrix} x \\ k \end{pmatrix}\right) = d.$$

This gives an integral representation of d by q provided $Ax \in (k\mathbb{Z})^n$, a condition which depends only the classes of $x_1, \dots, x_n \pmod{k}$. Since $q(x) = kd$ we need only consider admissible n -tuples, i.e., $(x_1, \dots, x_n) \in (\mathbb{Z}/k\mathbb{Z})^n$ such that $q(x_1, \dots, x_n) \equiv 0 \pmod{k}$. 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 $q(A_x v) = kq(v)$ and $A_x x \equiv 0 \pmod{k}$.

However, in most cases this is asking too much.

Lemma 19. *For all $k \in \mathbb{Z}^+$, $O_q(k) = \{A \in M_n(\mathbb{Z}) \mid q(Av) = kq(v)\}$ 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 $q = q_0 = x_1^2 + \dots + x_n^2$, 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** $A = (a_{ij}) \mapsto |A| = \sqrt{\sum_{1 \leq i, j \leq n} a_{ij}^2}$ is a Banach algebra: for all $A, B \in$

$M_n(\mathbb{R})$, $|AB| \leq |A||B|$.³ Let $q_0 = x_1^2 + \dots + x_n^2$ be the “standard” positive definite n -ary quadratic form. Its orthogonal group $O_{q_0}(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid q_0(Av) = q_0(v)\}$ 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 $P \in \text{GL}_n(\mathbb{R})$ such that $q(v) = q_0(Pv)$. Then $O_q(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid q(Av) = q(v)\} = P^{-1}O_{q_0}(\mathbb{R})P$: indeed, if $A \in O_{q_0}(\mathbb{R})$, then $q(P^{-1}APv) = q_0(APv) = q_0(Pv) = q(v)$, and conversely. Therefore, for any $A \in O_q(\mathbb{R})$, we have

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

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 $q(Av) = kq(v)$,

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

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

Remark 4.1: 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

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

By Lemma 19, $O_q(k, r)$, 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 .⁴ 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 $r \in \mathbb{Z}^+$ 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 $A_x(\frac{x}{kr}) \in \mathbb{Z}^n$ and $q(A_x(\frac{x}{kr})) = d$.

We now turn to the proof of Theorem 18. As usual, we apply Theorem 7: since $[M(q)] = 5$, 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 20. *Let $q = x^2 + 2y^2 + 5z^2 + 10w^2$. 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 all $A(q, 2, r)$ admissible tuples.*
- 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 .*

³Perhaps we are overbilling this: it is nothing else than the Cauchy-Schwarz inequality.

⁴If q is a multiplicative quaternary form, then for all $k \in \mathbb{Z}^+$, $\bigcup_{r=1}^{\infty} O_q(k, r)$ is infinite.

Proof. By computer calculation. The C++ code used for this may be found at <http://www.math.uga.edu/~pete/MinimalCode.cpp>. \square

This completes the proof of Theorem 18.

Remark 4.2: Notice that – without any GoN input – Theorem 20a) yields:

Theorem 21. *For all $d \in \mathbb{Z}^+$, if $q(v) = x^2 + 2y^2 + 5z^2 + 10w^2$ represents $2d$, then it also represents d .*

As described in the introduction, Theorem 21 completes a quaternionic proof of the universality of $(1, 2, 5, 10)$ initiated by Deutsch and continued by Fitzgerald.

Remark 4.3: 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 $z^2 + 2w^2 + 5X^2 + 10Y^2 = p$.

Remark 4.4: Theorem 20a) renders Theorem 20e) logically superfluous: if we can pass from a representation of $2n$ to a representation of n , then of course we can pass from a representation of $4n$ to a representation of n . (Our computer did this unneeded work without complaint...) Parts b), d) and f) of Theorem 20 are included as evidence that this calculation would have been impractical to do by hand.

REFERENCES

- [Bh00] M. Bhargava, *On the Conway-Schneeberger fifteen theorem*. Quadratic forms and their applications (Dublin, 1999), 2737, Contemp. Math., 272, Amer. Math. Soc., Providence, RI, 2000.
- [BH05] M. Bhargava and J.P. Hanke, *Universal quadratic forms and the 290-theorem*, preprint.
- [Ca] J.W.S. Cassels, *An introduction to the geometry of numbers*. Corrected reprint of the 1971 edition. Classics in Mathematics. Springer-Verlag, Berlin, 1997.
- [Cl11] P.L. Clark, *Thue-Vinogradov and integers of the form $x^2 + Dy^2$* , 2011 preprint.
- [Co] J. H. Conway, *The sensual (quadratic) form*, Carus Mathematical Monographs 26, MAA, 1997.
- [Co00] 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.
- [De08] J.I. Deutsch, *A quaternionic proof of the universality of some quadratic forms*. Integers 8 (2008), no. 2, A3, 23 pp.
- [Di27] L.E. Dickson, *Integers represented by positive ternary quadratic forms*. Bull. Amer. Math. Soc. 33 (1927), 63-70.
- [Fi11] R.W. Fitzgerald, *Norm Euclidean quaternionic orders*. Integers 11 (2011), A58, 12 pp.
- [GoN1] P.L. Clark and H. Parshall, *GoNI: Binary quadratic forms*, in preparation.
- [Gr27] J.H. Grace, *The Four Square Theorem*. J. London Math. Soc. 2 (1927), 3-8.
- [Ha38] P.R. Halmos, *Note on almost-universal forms*. Bull. Amer. Math. Soc. 44 (1938), 141-144.
- [HW] G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers*.
- [IR] K. Ireland and M. Rosen, *A classical introduction to modern number theory*. Second edition. Graduate Texts in Mathematics, 84. Springer-Verlag, New York, 1990.
- [L] T.Y. Lam, *Introduction to quadratic forms over fields*. Graduate Studies in Mathematics, 67. American Mathematical Society, Providence, RI, 2005.
- [Mo66] L.J. Mordell, *The representation of numbers by some quaternary quadratic forms*. Acta Arith. 12 (1966/1967), 47-54.
- [Ra17] 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.
- [S] C.L. Siegel, *Lectures on the geometry of numbers*. Springer-Verlag, Berlin, 1989.