involve
a journal of mathematics

Quadratic forms representing all primes

Justin DeBenedetto

msp

2014 vol. 7, no. 5

msp

INVOLVE 7:5 (2014)
dx.doi.org/10.2140/involve.2014.7.619

Quadratic forms representing all primes

Justin DeBenedetto

(Communicated by Kenneth S. Berenhaut)

Building on the method used by Bhargava to prove "the fifteen theorem", we show that every integer-valued positive definite quadratic form which represents all prime numbers must also represent 205. We further this result by proving that 205 is the smallest nontrivial composite number which must be represented by all such quadratic forms.

1. Introduction and statement of results

The study of quadratic forms in various fashions dates back to the third century works of Diophantus. Diophantus worked with ways to rewrite sums of squares and found that $(a^2+b^2)(c^2+d^2) = (ac \pm bd)^2 + (ad \mp bc)^2$ and that numbers of the form $4n-1$ are not able to be represented as a sum of two squares. It was not until 1625 that Albert Girard (Fermat came to the same result a few years later) wrote that a number is the sum of two squares if and only if when divided by its largest square factor, the result is a product of primes of the form $4n+1$ or twice the product of such primes [Dickson 1920].

Further exploration into representation of numbers by squares led to Lagrange proving in 1770 that every natural number is the sum of four integer squares, $n = a^2+b^2+c^2+d^2$. Ramanujan [1917] furthered this result by conjecturing[1] that there are exactly 55 sets of values for a, b, c, d such that $ax^2+by^2+cz^2+du^2$ represents all positive integers.

Willerding [1948] used an extension of Ramanujan's work to prove the following:

Theorem 1. *There are exactly* 178 *classes of universal positive definite integer matrix quaternary quadratic forms.*

Here positive definite indicates that the quadratic form represents only nonnegative integers, and only represents 0 when every variable is equal to 0. A universal quadratic form represents every number in its range, thus a universal

MSC2010: primary 11E25; secondary 11E20.

Keywords: quadratic forms, number theory, prime number.

[1] Originally it was stated that there are 55 sets of values, but one was later removed when Dickson proved that exactly one of Ramanujan's forms failed to represent all positive integers.

positive definite quadratic form represents all positive integers. Integer matrix means that the coefficients on all cross terms are even.

Bhargava [2000] showed that there are actually 204 universal quaternary forms and enumerated those forms. In the same paper, Bhargava gave a proof of a theorem stated in 1993 by Conway and Schneeberger known as "the fifteen theorem".

Theorem 2. *If a positive definite quadratic form having an integer matrix represents every positive integer up to* 15 *then it represents every positive integer.*

Building on the methods used by Bhargava, we look specifically at integer-valued positive definite quadratic forms representing all prime numbers. Our goal is to determine if there are composite numbers which are represented by every such quadratic form, and if so to find the smallest such composite. Our result is a proof that there are nontrivial composites which are represented by all quadratic forms representing every prime number.

We restrict the composite numbers we are considering to composites which are not a square times a prime. This is due to the fact that all primes are represented by prime universal quadratic forms, and if n is represented then nx^2 is also represented. For this reason, we consider a square times a prime to be a trivial composite number, and search for nontrivial composite numbers which are represented by these quadratic forms.

Theorem 3. *Every integer-valued positive definite quadratic form*, Q, *representing all prime numbers*, *must represent* 205. *Furthermore*, *if n is a composite number less than* 205 *and n is represented by all quadratic forms which represent all prime numbers*, *then n must be a square times a prime.*

Remark. An analogous statement may be made for integer matrix positive definite quadratic forms. The same process is used, but the calculations are simpler and 66 is the smallest non-trivial composite which must be represented in that case.

2. Definitions

First, we define lattices as they pertain to quadratic forms throughout this paper. The set of all integers is denoted $\mathbb{Z}$. An n-dimensional *lattice* L is a subset $L \subseteq \mathbb{R}^n$, together with an inner product that gives a way of measuring distances and angles. Here are the properties that it must satisfy:

(i) The set L must span $\mathbb{R}^n$.

(ii) The set L must have the form $L = \left\{\sum_{i=1}^{n} a_i \vec{v}_i : a_i \in \mathbb{Z}\right\}$.

(iii) The inner product $\langle \vec{v}, \vec{w} \rangle$ is a function from $L \times L \to \mathbb{R}$.

(iv) For any $\vec{v} \in L$, $\langle \vec{v}, \vec{v} \rangle \geq 0$ with $\langle \vec{v}, \vec{v} \rangle = 0$ if and only if $\vec{v} = 0$.

(v) For any $\vec{v}, \vec{w}, \vec{x} \in L$, we have $\langle \vec{v}, \vec{w} \rangle = \langle \vec{w}, \vec{v} \rangle$ and $\langle \vec{v} + \vec{w}, \vec{x} \rangle = \langle \vec{v}, \vec{x} \rangle + \langle \vec{w}, \vec{x} \rangle$.

Note that property (iv) enforces positive definiteness.

Given a lattice L, the function

$$Q(a_1, \dots, a_n) = \left\langle \sum_{i=1}^{n} a_i \vec{v}_i, \sum_{i=1}^{n} a_i \vec{v}_i \right\rangle$$

is a *quadratic form*. Moreover, every quadratic form arises in this way.

A quadratic form is called *integer-valued* if

$$Q(x_1, x_2, \dots, x_n) = \sum_{i=1}^{n} \sum_{j=i}^{n} a_{ij} x_i x_j, \quad a_{ij} \in \mathbb{Z}.$$

Furthermore, an integer-valued quadratic form is called *integer matrix* if a_{ij} is even for all $i \neq j$.

The *Gram matrix* of a quadratic form, Q, is the matrix A such that we can write $Q = x^t A x$. The Gram matrix of an integer-valued quadratic form has entries has integer diagonal entries and half integer off diagonal entries. Similarly, the Gram matrix of an integer matrix quadratic form has integer entries.

Next, we set forth some definitions which are based upon the definitions used in [Bhargava 2000]. We first define the *prime truant* of a quadratic form to be the smallest prime not represented by the quadratic form. We also define a *prime escalation* of a lattice to be a lattice generated by the original lattice and a vector with norm equal to the prime truant of the original lattice. The dimension of a prime escalation is either equal to the dimension of the original lattice or greater by 1. A *prime escalator lattice* is a lattice which is generated by any number of prime escalations of the zero-dimensional lattice. Similarly, a quadratic form is considered to be *prime universal* if it represents all prime numbers.

Two quadratic forms, Q_1 and Q_2, are considered *equivalent* if there is an integral invertible change of variables which sends Q_1 to Q_2.

If Q is a positive definite quadratic form, let $r_Q(n)$ be the number of representations of n by Q. The *theta series* of Q is the power series

$$\Theta_Q(q) = \sum_{n=0}^{\infty} r_Q(n) q^n.$$

3. Prime escalations

We begin by giving an overview of prime escalations. Escalating the zero-dimensional lattice gives us $[2]$ which leads to the form $2x^2$. This represents 2 but not 3, so our two-dimensional prime escalator lattices are

$$\begin{bmatrix} 2 & x \\ x & 3 \end{bmatrix},$$

with $x^2 \leq 6$ by the Cauchy–Schwarz inequality. Since we are looking for integer-valued quadratic forms, we allow x to be of the form $x = y/2$, $y \in \mathbb{Z}$. Thus we have the lattices with matrices

$$\begin{bmatrix} 2 & \pm\frac{1}{2} \\ \pm\frac{1}{2} & 3 \end{bmatrix}, \quad \begin{bmatrix} 2 & \pm 1 \\ \pm 1 & 3 \end{bmatrix}, \quad \begin{bmatrix} 2 & \pm\frac{3}{2} \\ \pm\frac{3}{2} & 3 \end{bmatrix}, \quad \begin{bmatrix} 2 & \pm 2 \\ \pm 2 & 3 \end{bmatrix}, \quad \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix},$$

corresponding to the quadratic forms

$$2x^2 \pm xy + 3y^2, \quad 2x^2 \pm 2xy + 3y^2, \quad 2x^2 \pm 3xy + 3y^2$$
$$2x^2 \pm 4xy + 3y^2, \quad 2x^2 + 3y^2.$$

The form $2x^2 + 3xy + 3y^2$ is equivalent to $2x^2 + xy + 2y^2$, and $2x^2 + 4xy + 3y^2$ is equivalent to $x^2 + 2y^2$. For binary quadratic forms, we may ignore the sign of the cross term since sending x to $-x$ makes the forms equivalent.

To automate this process we ran this through a math program called Magma. The Magma script began with the zero-dimensional lattice and followed the prime escalation process as above. When checking for prime truants, each form was checked for unrepresented primes beginning with 2 and checking each prime until one was unrepresented. Since prime escalator lattices of dimension two are not prime universal, every lattice was escalated at least three times. Some of these lattices were escalated a fourth time if they failed to represent a prime below 1000.

We define two sets, A and B, as follows. If a third escalation prime escalator lattice, L, represents every prime below 1000, then let $L \in A$. If the third escalation prime escalator lattice fails to represent a prime below 1000, then let a prime escalation of L be M, and let $M \in B$.

Theorem 4. *Every prime universal lattice contains a prime escalator lattice from A or B.*

Proof. Suppose L is a prime universal lattice and $L_0 \subseteq L_1 \subseteq L_2 \subseteq L_3 \subseteq \cdots \subseteq L$ is an ascending chain of escalator lattices, with L_0 zero-dimensional and L_i being a prime escalation of L_{i-1} for each i. Since every prime escalator lattice of dimension 0, 1, or 2 increases in dimension when escalated, L_3 is a 3-dimensional escalator lattice. If L_3 has a prime truant below 1000, then its escalation $L_4 \in B$. If not, then $L_3 \in A$. Thus L contains a prime escalator sublattice from A or from B. □

Forms in the set A may not be prime universal, but Theorem 5 allows us to make use of these forms.

4. Composite representation methods

Since we are searching for composite numbers which are represented by every prime universal quadratic form, we take advantage of Lagrange's four-square theorem mentioned above to form the following theorem.

Theorem 5. *Suppose $Q(\vec{y})$ is a positive definite integer-valued quadratic form and there exists a composite number m such that $Q(\vec{y})$ does not represent m. If $Q(\vec{y})$ represents every prime $p < m$, then the quadratic form*

$$R(\vec{y}, a, b, c, d, x_0, \ldots, x_{m-1}) Q(\vec{y}) + (m+1)(a^2+b^2+c^2+d^2) + \sum_{i=0}^{m-1}(m+1+i)x_i^2$$

is prime universal and does not represent m.

Proof. This result is due to the fact that $\sum_{i=0}^{m-1}(m+1+i)x_i^2$ represents every number between $m+1$ and $2m$, and $(m+1)(a^2+b^2+c^2+d^2)$ represents every multiple of $(m+1)$. Thus together these represent every number greater than m. The resultant quadratic form, R, does not represent m due to the fact that Q and each of the two added components are all positive definite. Since the two added components do not represent any numbers less than m and Q does not represent any negative numbers, there is no way to represent m. Finally, since we have shown that our new quadratic form represents every number greater than m and Q represents every prime less than m, R must represent all prime numbers and thus is prime universal. □

With these tools in hand we are now ready to handle the proof of our main result.

Proof of Theorem 3. In this way, if we are able to find a quadratic form which represents all primes less than a composite, but does not represent that composite number, we can construct a prime universal quadratic form which fails to represent that composite. Table 1 provides a list of quadratic forms that show that every composite number less than 205 which is not a square times a prime does not have to be represented by a prime universal quadratic form.

Next, we look at which composites are represented by prime universal quadratic forms. After each prime escalation run using Magma, we checked which composites were represented by every prime escalator lattice. In order to do this, we generated the theta series of each lattice and checked the coefficients of the composite power terms. We began this process after two prime escalations, since the zero-dimensional and one-dimensional prime escalator lattices do not represent any composites which are not a square times a prime. By comparing the represented composites for the five two-dimensional prime escalator lattices corresponding to binary quadratic forms, we find that 818 is represented by all of them. As such, we reduced our theta series to only look at which composites below 818 were represented for subsequent prime escalations. We repeated this process for the third and fourth prime escalations of the zero-dimensional lattice.

This process showed that 818 is represented by all second prime escalations, 453 is represented by all third escalations, and 205 is represented by every lattice in sets A and B.

Quadratic form	Integers not represented
$x^2+xy+2y^2+3z^2$	6, 15, 24, 33, 42, 51, 54, 60, 69, 78, 85, 87, 96, 105, 114, 123, 132, 135, 141, 150, 159, 168, 177, 186, 195, 204
$2x^2-2xz+3y^2+yz+3z^2$	1, 4, 16, 22, 38, 64, 70, 86, 88, 102, 118, 134, 152, 166, 182, 198
$2x^2-2xz+3y^2+3yz+3z^2$	26, 104
$2x^2-xz+3y^2+4z^2$	9, 81
$2x^2-xz+3y^2+3yz+4z^2$	34, 111
$2x^2+3y^2+yz+5z^2$	10, 40, 58, 74, 90, 106, 122, 136, 138, 154, 160, 170, 202
$2x^2+3y^2+3yz+5z^2$	36, 119, 144, 187
$2x^2-2xz+3y^2-yz+5z^2$	46, 178, 184
$x^2+xz+y^2+2z^2$	21, 35, 84, 91, 133, 140, 189
$2x^2+xy-xz+3y^2-yz+3z^2$	25, 30, 65, 110, 115, 155, 165, 185, 190
$x^2+xz+y^2+3z^2$	66, 77, 143
$2x^2+2xy-2xz+3y^2+yz+5z^2$	14, 56, 62, 94, 120, 126, 142, 158, 174
$2x^2+2xy+3y^2+yz+5z^2$	39, 156
$x^2+xy+xz+2y^2+3z^2+19w^2$	57
$2x^2-2xz-xw+3y^2-3yw+3z^2-2zw+14w^2$	49
$2x^2-2xz+3y^2-3yw+3z^2+15w^2$	121
$2x^2-2xz+3y^2+2yz+3z^2+13w^2$	169
$2x^2-xz+3y^2-2yz+3z^2+61w^2$	183
$2x^2-xy+2y^2-yz+3z^2+43w^2$	129
$2x^2+xz-xw+3y^2+3yz-3yw+6z^2-4zw+7w^2$	55
$2x^2+xz+2xw+3y^2+3yz+6z^2+2zw+9w^2$	95
$2x^2-2xz+2xw+3y^2-3yw+7z^2-5zw+11^2$	130
$2x^2-2xz-2xw+3y^2+2yz-3yw+7z^2-zw+9w^2$	82
$2x^2-xz+3y^2-yz+5z^2+23z^2$	161
$2x^2+2xy-xz-xw+3y^2-yw+5z^2+66w^2$	194
$2x^2+2xy-xz-xw+3y^2+2yz-3yw+5z^2+zw+26w^2$	93
$2x^2-xy+xw+2y^2-yz-yw+5z^2+70w^2$	146
$2x^2-xy+xz+2y^2-2yz+5z^2+67w^2$	201
$2x^2-xy-xw+2y^2+2yw+7z^2+8w^2$	196
$2x^2-xy+xz+xw+2y^2+yz+yw+7z^2+4zw+11z^2$	100
$x^2-xz+2y^2-yz+4z^2+29w^2$	145, 203

Table 1. The quadratic forms on the left do not represent the numbers on the right, but represent every prime less than each of those numbers. By Theorem 5, there exists a prime universal quadratic form which represents all primes and does not represent each number listed.

By Theorem 4, every prime universal lattice will contain a prime escalator lattice from sets A or B and thus will represent 205. □

5. Conclusions

There are many questions that remain regarding properties of universal quadratic forms, and specifically prime universal quadratic forms.

Question. *If we let S be a set of positive integers, T be the set of all positive definite quadratic forms that represent every number in S, and U be the set of numbers represented by everything in T, when does $T = U$ and when is U bigger than T?*

We have answered this question in the case of S being the set of all primes, and found that U is bigger than T since $205 \in U$.

Other questions regarding quadratic forms which have been answered for integers remain open when applied specifically to prime numbers. A similar examination could apply to the "290 theorem" (see [Bhargava and Hanke 2011]).

Theorem 6 (290 theorem). *If a positive definite quadratic form with integer coefficients represents the twenty-nine integers* 1, 2, 3, 5, 6, 7, 10, 13, 14, 15, 17, 19, 21, 22, 23, 26, 29, 30, 31, 34, 35, 37, 42, 58, 93, 110, 145, 203, *and* 290, *then it represents all positive integers.*

Question. *What is the smallest set of prime numbers such that all positive definite integer-valued quadratic forms which represent every prime in the set must be prime universal*? (Bhargava has answered this question in the case of positive definite integer matrices.)

Acknowledgements

We used Magma [Bosma et al. 1997] for our escalation computations. I would like to thank Jeremy Rouse for all of his guidance on this project. I would also like to thank the anonymous referee for editing and providing feedback.

References

[Bhargava 2000] M. Bhargava, "On the Conway–Schneeberger fifteen theorem", pp. 27–37 in *Quadratic forms and their applications* (Dublin, 1999), edited by E. Bayer-Fluckiger et al., Contemp. Math. **272**, Amer. Math. Soc., Providence, RI, 2000. MR 2001m:11050

[Bhargava and Hanke 2011] M. Bhargava and J. Hanke, "Universal quadratic forms and the 290-theorem", preprint, 2011; see http://wordpress.jonhanke.com/wp-content/uploads/2011/09/290-Theorem-preprint.pdf.

[Bosma et al. 1997] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system, I: The user language", *J. Symbolic Comput.* **24**:3-4 (1997), 235–265. MR 1484478

[Dickson 1920] L. E. Dickson, *History of the theory of numbers, II: Diophantine numbers*, Carnegie Institution of Washington, 1920.

[Ramanujan 1917] S. Ramanujan, "On the expression of a number in the form $ax^2+by^2+cz^2+du^2$", *Proc. Cambridge Phil. Soc.* **19** (1917), 11–21. Reprinted as pp. 169–177 in *Collected Papers of Srinivasa Ramanujan*, edited by G. H. Hardy et al., Cambridge Univ. Press; reissued Chelsea, New York, 1962. JFM 46.0240.01

[Willerding 1948] M. F. Willerding, "Determination of all classes of positive quaternary quadratic forms which represent all (positive) integers", *Bull. Amer. Math. Soc.* **54** (1948), 334–337. MR 9,571e

Received: 2013-05-03 Revised: 2013-10-01 Accepted: 2013-12-22

debejd0@wfu.edu *Department of Mathematics, Wake Forest University, 127 Manchester Hall, Box 7388, Winston-Salem, NC 27109, United States*

involve

msp.org/involve

See inside back cover or msp.org/involve for submission instructions. The subscription price for 2014 is US $120/year for the electronic version, and $165/year (+$35, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to MSP.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840, is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

involve

2014 vol. 7 no. 5