Arch. Math. 91 (2008), 44–48

0003/889X/010044-5, *published online* 2008-06-25
DOI 10.1007/s00013-008-2637-5

Archiv der Mathematik

Short proofs of the universality of certain diagonal quadratic forms

Jesse I. Deutsch

Abstract. In a paper of Kim, Chan, and Rhagavan, the universal ternary classical quadratic forms over quadratic fields of positive discriminant were discovered. Here a proof of the universality of some of these quadratic forms is given using a technique of Liouville. Another quadratic form over the field of discriminant 8 is shown universal by a different elementary approach.

Mathematics Subject Classification (2000). Primary 11E25, 11D57, 11P05.

Keywords. Quadratic form, quadratic field, universality.

1. Introduction. The work of Kim, Chan, and Rhagavan on ternary quadratic forms over real quadratic number fields listed all the universal classical forms. Classical forms are those with even coefficients on the cross product terms. A form is universal if it represents all totally positive algebraic integers in the corresponding field. They showed that the relevant number fields could only be $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{2})$, and $\mathbb{Q}(\sqrt{3})$. The proof involved the use of lattice theory and p-adic numbers. See Kim et al. [9].

In previous work, the author was able to demonstrate the universality of sums of squares for the algebraic integers in the field $\mathbb{Q}(\sqrt{5})$ and near-universality for $\mathbb{Q}(\sqrt{2})$. These proofs used alternate techniques (see Deutsch [4, 5]). It is therefore natural to consider other approaches to the results of Kim et al. [9].

In Dickson [7, p. 227] a result of Liouville is mentioned where the near-universality of a quaternary quadratic form over the ring $\mathbb{Z}$ is proved. The technique used depends upon the famous result of Gauss on the representations of the sum of three squares over $\mathbb{Z}$. An obvious analogue of Liouville's method would be to use Maass's Theorem on the universality of the sum of three squares for $\mathbb{Q}(\sqrt{5})$. In the early 1960's, H. Cohn gave a proof of this and other results on sums of squares over quadratic fields of low positive discriminant. See Cohn [1, 2, 3] for details.

Adapting this technique of Liouville, we can prove the universality of the quadratic forms $x^2 + y^2 + 2\,z^2$ and $x^2 + y^2 + \dfrac{5+\sqrt{5}}{2}z^2$ over the algebraic integers in $\mathbb{Q}(\sqrt{5})$. In addition, a quaternary quadratic form over $\mathbb{Q}(\sqrt{2})$ is shown to be universal for the integers of that field. This latter form could be considered an analogue of $x^2 + 2\,y^2 + 2\,z^2 + 4\,w^2$, which is universal over $\mathbb{Z}$.

2. Liouville's method and result. The above mentioned result of Liouville is the following.

Theorem 2.1. *The quadratic form* $x^2+y^2+5\,z^2+5\,w^2$ *represents all integers over the ring* $\mathbb{Z}$ *except for* 3.

This form satisfies a multiplication rule derived from an appropriate quaternion ring (see Deutsch [6]). Since it represents 2, it is only necessary to show that it represents each odd integer besides 3. Fleshing out the comments in Dickson [7], provides the demonstration below.

Proof. For integers n congruent to 1, 5 or 7 (mod 8) it follows that $5\,n$ is not congruent to 7 modulo 8. Hence by Gauss's Theorem on representations by sums of three squares, we find there exist integers, x, y and z such that $5\,n = x^2+y^2+z^2$. Thus $x^2+y^2+z^2 \equiv 0 \pmod 5$. It follows that at least one of x, y or z is congruent to 0 modulo 5. With no loss of generality, let this be z. Then $x^2 + y^2$ is divisible by 5. A Lemma of Euler states that the if sum of two integer squares is divisible by a prime that is the sum of two squares, then the quotient is the sum of two squares (see Deutsch [4]). Hence $x^2 + y^2 = 5(x_1^2 + y_1^2)$. We conclude that in this case $n = x_1^2 + y_1^2 + 5\,z^2$.

In the other case where $n \equiv 3 \pmod 8$, consider $n - 20$. Since $5\,(n-20) \not\equiv 7 \pmod 8$, it follows that $5\,(n-20)$ is the sum of three integer squares for all $n > 20$. By the same argument as above we find $n - 20 = x^2 + y^2 + 5\,z^2$ or equivalently $n = x^2 + y^2 + 5\,z^2 + 5 \cdot 2^2$.

The only remaining cases are 3, 11 and 19. It is easy to see that only 11 and 19 are represented by the form in question. □

3. A ternary form over $\mathbb{Q}(\sqrt{5})$. Returning to $\mathbb{Q}(\sqrt{5})$, we start with the simpler case. First set $\tau = \tau_5 = (1+\sqrt{5})/2$. In particular τ_5 is the fundamental unit of the integers in $\mathbb{Q}(\sqrt{5})$. Also, the algebraic integers in $\mathbb{Q}(\sqrt{5})$ are the $\mathbb{Z}$ module generated by $\{1, \tau_5\}$, denoted $O(\sqrt{5})$.

Theorem 3.1. *The following quadratic form is universal for totally positive algebraic integers in* $O(\sqrt{5})$.

$$x^2 + y^2 + \frac{5+\sqrt{5}}{2}\,z^2. \tag{3.1}$$

Proof. Let η be totally positive, then so is $\sqrt{5}\,\tau\,\eta$. By Maass's Theorem we have a representation

$$\sqrt{5}\,\tau\,\eta \;=\; x^2+y^2+z^2\,. \tag{3.2}$$

We get

$$0 \;\equiv\; x^2+y^2+z^2 \pmod{\sqrt{5}}\,. \tag{3.3}$$

Since there is only one field of order 5, we have by isomorphism, the equation

$$0 \;\equiv\; r^2+s^2+t^2 \pmod{5} \tag{3.4}$$

over $\mathbb{Z}$. Since the only squares modulo 5 are $\{0, \pm 1\}$ this forces one of r, s, or t to be zero modulo 5. Thus one of x, y or z is divisible by $\sqrt{5}$ in the integers of $\mathbb{Q}(\sqrt{5})$. With no loss of generality, let $z=\sqrt{5}\,\tau\,z_1$ where $z_1 \in O(\sqrt{5})$.

$$\sqrt{5}\,\tau\,\eta \;=\; x^2+y^2+(\sqrt{5}\,\tau\,z_1)^2\,. \tag{3.5}$$

So now we have x^2+y^2 divisible by $\sqrt{5}\,\tau$. Since $\sqrt{5}\,\tau \;=\; 1^2+\tau^2$, using Euler's Lemma as in the previous case, we find $x^2+y^2=\sqrt{5}\,\tau\,(x_1^2+y_1^2)$.

We conclude that

$$\eta \;=\; x_1^2+y_1^2+\sqrt{5}\,\tau\,z_1^2\,. \tag{3.6}$$

□

4. Another ternary form over $\mathbb{Q}(\sqrt{5})$. We now proceed to the more complicated case.

Theorem 4.1. *The following quadratic form is universal for algebraic integers in $\mathbb{Q}(\sqrt{5})$.*

$$x^2 \,+\, y^2 \,+\, 2\,z^2. \tag{4.1}$$

Proof. Let η be totally positive and odd. Then $2\,\eta$ is totally positive. Again by Maass's Theorem we have a representation

$$2\,\eta \;=\; x^2+y^2+z^2\,. \tag{4.2}$$

So

$$0 \;\equiv\; x^2+y^2+z^2 \pmod{2}\,. \tag{4.3}$$

Since 2 is prime and the representatives of $O(\sqrt{5})/(2)$ can be chosen $\{0,\,1,\,\tau,\,\overline{\tau}\}$, either one of x, y, or z is zero or they are 1, τ, $\overline{\tau}$ in some order. This is because $\tau^2\equiv\overline{\tau} \pmod{2}$ and vice versa, $\overline{\tau}^2\equiv\tau \pmod{2}$. As in Deutsch [4], we find that if x, y, and z are 1, τ and $\overline{\tau}$ in some order, then the sum of the squares are congruent to 0 modulo 4. This contradicts the oddness of η.

Thus one of x, y, or z is zero modulo 2. By Euler's Lemma with the prime $2=1^2+1^2$ we get a representation

$$\eta \;=\; x_1^2+y_1^2+2\,z_1^2\,. \tag{4.4}$$

Let η be totally positive, and even. Since 2 is prime, we can split this into the case that $2\,||\,\eta$ or that a higher power of 2 divides η. Suppose the first case. Then we have a representation

$$\begin{aligned} \eta/2 &= x^2+y^2+z^2 \\ \eta &= 2\,x^2+2\,y^2+2\,z^2 \qquad (4.5)\\ \eta &= (x+y)^2+(x-y)^2+2\,z^2\,. \end{aligned}$$

For any higher power, $2\,a+b$, of 2 such that $2^{2\,a+b}\,||\,\eta$ we can limit the possibilities to $b=0$ or $b=1$. In either case, we have $\eta/2^{2\,a}$ represented by the form $x^2+y^2+2\,z^2$, and we need only multiply through by $(2^a)^2$ to get a representation of η by this ternary quadratic form. That completes the demonstration. □

5. A quaternary quadratic form over $\mathbb{Q}(\sqrt{2})$. The universality of one of the quaternary forms turns out to have a very short proof.

Theorem 5.1. *The following quadratic form is universal for algebraic integers in* $\mathbb{Q}(\sqrt{2})$.

$$x^2\;+\;(2+\sqrt{2})\,y^2\;+\;(2-\sqrt{2})\,z^2\;+\;2\,w^2 \qquad (5.1)$$

Proof. We start with the known fact that the ternary form $x^2+y^2+(2+\sqrt{2})z^2$ is universal (see Kim et. al. [9]). For any totally positive odd prime ρ, that is, a prime not equal to $\sqrt{2}$ times a unit, we have algebraic integers satisfying

$$x^2+y^2+(2+\sqrt{2})z^2=\rho\,. \qquad (5.2)$$

Since the ring of algebraic integers modulo $\sqrt{2}$ must be the unique ring of two elements, taking the above equation modulo $\sqrt{2}$ and noting the oddness of ρ we have

$$x^2+y^2\;\equiv\;1\pmod{\sqrt{2}} \qquad (5.3)$$

which reduces to

$$x+y\;\equiv\;1\pmod{\sqrt{2}} \qquad (5.4)$$

Thus at least one of x or y must be congruent to zero modulo $\sqrt{2}$. With no loss of generality suppose it is y. Then write $y=y_1\cdot\sqrt{2}$. We have

$$x^2+2\,y_1^2+(2+\sqrt{2})z^2=\rho\,. \qquad (5.5)$$

Thus ρ is represented by the quaternary form in (5.1).

The only even prime is $2+\sqrt{2}$ times a unit, and clearly these are represented by $(2+\sqrt{2})\,y^2$ as the norm of the fundamental unit, $1-\sqrt{2}$, is -1.

Thus the quadratic form in (5.5) can be thought of as universal for the set of all totally positive primes in $\mathbb{Q}(\sqrt{2})$. Since $(2+\sqrt{2})\times(2-\sqrt{2})=2$ we have a norm multiplication law related to the quaternions that lets us conclude the product of any number of totally positive primes is also represented by (5.1). By standard arguments, any totally positive integer in $\mathbb{Q}(\sqrt{2})$ can be factored into a product of totally positive primes, so the universality of (5.1) follows.

A similar, shorter proof can be obtained by using the same technique as above but with the form $x^2 + y^2 + (2+\sqrt{2})\, z^2 + (2-\sqrt{2})\, w^2$. This form must be universal given that it is an extension of the known universal form $x^2 + y^2 + (2 + \sqrt{2})\, z^2$. Universality among the primes, plus a norm multiplication law finishes the proof. □

6. The computation. Supporting computations were done in the Python language on a 2003 era laptop running Linux kernel 2.4.33.3. There were 256 Megabytes of RAM and about 10.8 gigabytes in the two hard drive partitions used. The Python version was 2.5.0. It was compiled using GNU GCC 3.4.6.

References

[1] H. Cohn, Decomposition into Four Integral Squares in the Fields $2^{1/2}$ and $3^{1/2}$. Amer. J. Math. **82**, 301–322 (1960).

[2] H. Cohn, Calculation of Class Numbers by Decomposition into Three Integral Squares in the Fields of $2^{1/2}$ and $3^{1/2}$. Amer. J. Math. **83**, 33–56 (1961).

[3] H. Cohn, Cusp Forms Arising from Hilbert's Modular Functions for the Field of $3^{1/2}$. Amer. J. Math. **84**, 283–305 (1962).

[4] J. I. Deutsch, Geometry of Numbers Proof of Götzky's Four Squares Theorem. J. Number Theory **96**, 417–431 (2002).

[5] J. I. Deutsch, An Alternate Proof of Cohn's Four Squares Theorem. J. Number Theory **104**, 263–278 (2004).

[6] J. I. Deutsch, A Quaternionic Proof of the Universality of Some Quadratic Forms. (to appear in INTEGERS, EJCNT).

[7] L. E. Dickson, History of the Theory of Numbers, vol. III, Chelsea Publishing Co., New York 1952.

[8] W. Duke, Some Old Problems and New Results about Quadratic Forms. Notices of the AMS **44**, 190–196 (1997).

[9] M.-H. Kim, W.-H. Chan, and S. Rhagavan, Ternary Universal Integral Quadratic Forms over Real Quadratic Fields. Japanese J. Math. **22**, 263–273 (1996).

Jesse I. Deutsch, 1621 Yale Place, Rockville, MD 20850, USA
e-mail: deutschj_1729@yahoo.com

Received: 30 October 2007