Furman University
Electronic Journal of Undergraduate Mathematics
Volume **14, 1 − 4, 2009**

INTEGERS OF THE FORM $a^2 \pm b^2$

ROBERT ZEMAN

Abstract. This paper explores which integers can be expressed in the form $a^2 \pm 2b^2$ by using rings of the form $\mathbb{Z}[\sqrt{d}]$, particularly when $d = 2$ and $d = -2$.

1. Introduction and preliminaries

It has been proven that an integer n can be expressed as the sum of two squares if and only if each prime $p \equiv 3 \pmod 4$ that divides n occurs to an even power in the prime factorization of n [1, Theorem 13.3]. The goal of this work is to describe which integers can be expressed in the forms $a^2 + 2b^2$ and $a^2 - 2b^2$.

We will assume familiarity with elementary notions from divisor theory in integral domains such as can be found in [2]. In particular, for a square-free integer d, we shall make frequent use of the norm function on $\mathbb{Z}[\sqrt{d}]$: for $x = s + t\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, we set $N(x) = s^2 - dt^2$. We collect for ease of reference some of the results we shall need. Proofs of our first two results can be found in [2].

Lemma 1. *Let d be a square-free integer., and let $a, b \in \mathbb{Z}[\sqrt{d}]$. Then:*

(i) *a is a unit of $\mathbb{Z}[\sqrt{d}]$ if and only if $N(a) = \pm 1$.*
(ii) *$N(a) = 0$ if and only if $a = 0$.*
(iii) *The norm function is multiplicative; that is, $N(ab) = N(a)N(b)$.*

Lemma 2. *If d is a square-free integer, $a \in \mathbb{Z}[\sqrt{d}]$, and $N(a) = p$, where p is prime, then a is irreducible in $\mathbb{Z}[\sqrt{d}]$.*

Lemma 3. *Let p be an odd prime. If p can be expressed in the form $a^2 + 2b^2$, then $p \equiv 1$ or $3 \pmod 8$, and if p can be expressed in the form $a^2 - 2b^2$, then $p \equiv 1$ or $7 \pmod 8$.*

Proof. One can easily see that $a^2, b^2 \equiv 0, 1,$ or $4 \pmod 8$. Thus $2b^2 \equiv 0$ or $2 \pmod 8$, and so $a^2 + 2b^2 \equiv 0, 1, 2, 3, 4$ or $6 \pmod 8$ and $a^2 - 2b^2 \equiv 0, 1, 2, 4, 6$ or $7 \pmod 8$. Therefore, given an odd prime $p = a^2 + 2b^2$, then $p \equiv 1$ or $3 \pmod 8$ and given an odd prime $p = a^2 - 2b^2$, then $p \equiv 1$ or $7 \pmod 8$. □

Lemma 4. *Let p be an odd prime. Then 2 is a quadratic residue of p when $p \equiv 1$ or $7 \pmod 8$, and -2 is a quadratic residue of p when $p \equiv 1$ or $3 \pmod 8$.*

Proof. See [1]. □

Received by the editors April 10, 2009.
2000 *Mathematics Subject Classification.* 13A99.
Key words and phrases. prime, irreducible, unique factorization domain.
The author would like to thank his sponsor, Professor Evan Houston of UNC Charlotte.

2. Characterization of integers of the form $a^2 \pm 2b^2$

We now specialize $\mathbb{Z}[\sqrt{d}]$ to the cases $d = \pm 2$.

Theorem 5. *If $a \in \mathbb{Z}[\sqrt{-2}]$ and $N(a) = p^2$, p prime, with $p \equiv 5$ or $7 \pmod 8$, then a is irreducible in $\mathbb{Z}[\sqrt{-2}]$. If $a \in \mathbb{Z}[\sqrt{2}]$ and $N(a) = p^2$, p prime, with $p \equiv 3$ or $5 \pmod 8$, then a is irreducible in $\mathbb{Z}[\sqrt{2}]$.*

Proof. Let $a \in \mathbb{Z}[\sqrt{d}]$ with $d = \pm 2$, and assume that $N(a) = p^2$ with p prime. Suppose that $a = bc$, with $b, c \in \mathbb{Z}[\sqrt{d}]$. In order to prove that a is irreducible, we wish to show that $N(b) = 1$ or $N(c) = 1$. If this is false, then $N(b) = N(c) = \pm p$. If $d = -2$ and $p \equiv 5$ or $7 \pmod 8$, then $p = N(b) = s^2 + 2b^2$ for $s, t \in \mathbb{Z}$, a contradiction to Lemma 3. A similar contradiction is obtained in the case $d = 2$ and $p \equiv 3$ or $5 \pmod 8$. $\square$

Lemma 6. *$\mathbb{Z}[\sqrt{-2}]$ and $\mathbb{Z}[\sqrt{2}]$ are unique factorization domains.*

Proof. A proof that $\mathbb{Z}[\sqrt{-2}]$ is a unique factorization can be found in [2]. We present a unified proof for both cases.

Let $a = x + y\sqrt{\pm 2}$ and $b = s + t\sqrt{\pm 2} \neq 0$. Then $|N(a)| = |x^2 \mp 2y^2|$ and $|N(ab)| = |x^2 \mp 2y^2||s^2 \mp 2t^2|$. Since $|s^2 \mp 2t^2| \geq 1$, $|x^2 \mp 2y^2| \leq |x^2 \mp 2y^2||s^2 \mp 2t^2|$. Hence $|N(a)| \leq |N(ab)|$.

Now,

$$\frac{a}{b} = \frac{x + y\sqrt{\pm 2}}{s + t\sqrt{\pm 2}} = \frac{(x + y\sqrt{\pm 2})(s - t\sqrt{\pm 2})}{s^2 \mp 2t^2} = \frac{xs \mp 2yt}{s^2 \mp 2t^2} + \frac{(ys - xt)\sqrt{\pm 2}}{s^2 \mp 2t^2}.$$

Let $c = (xy \mp 2yt)/(s^2 \mp 2t^2)$ and $d = (ys - xt)/(x^2 \mp 2t^2)$. Then $c, d \in \mathbb{Q}$ and there are integers m, n such that $|c - m| \leq 1/2$ and $|d - n| \leq 1/2$. Therefore, $a = b(c + d\sqrt{\pm 2}) = b((c - m + m) + (d - n + n)\sqrt{\pm 2} = b(m + n\sqrt{\pm 2}) + b((c - m) + (d - n)\sqrt{\pm 2})$. Then $a = bq + r$, where $q = m + n\sqrt{\pm 2}$ and $r = b((c - m) + (d - n)\sqrt{\pm 2}$. Since $r = a - bq$, and $a, b, q \in \mathbb{Z}[\sqrt{\pm 2}]$, then $r \in \mathbb{Z}[\sqrt{\pm 2}]$. Also, $|N(r)| = |N(b)||N(c - m) + (d - n)\sqrt{\pm 2}| \leq |N(b)||(1/2)^2 \mp 2(1/2)^2| \leq |N(b)|$. That is, $a = bq + r$ with $0 \leq |N(r)| < |N(b)|$.

Therefore, $\mathbb{Z}[\sqrt{-2}]$ and $\mathbb{Z}[\sqrt{2}]$ are Euclidean domains and hence are unique factorization domains. $\square$

Theorem 7. *Let p be an odd prime. If $p \equiv 1$ or $3 \pmod 8$, then p is not irreducible in $\mathbb{Z}[\sqrt{-2}]$, and if $p \equiv 1$ or $7 \pmod 8$, then p is not irreducible in $\mathbb{Z}[\sqrt{2}]$.*

Proof. Given $p \equiv 1$ or $3 \pmod 8$, then -2 is a quadratic residue of p by Lemma 4. Therefore, there exists some $x \in \mathbb{Z}$ such that $p|(x^2 + 2)$. In $\mathbb{Z}[\sqrt{-2}]$, $x^2 + 2 = (x + \sqrt{-2})(x - \sqrt{-2})$. Therefore, $p|(x + \sqrt{-2})(x - \sqrt{-2})$. If p were irreducible, then $p|x + \sqrt{-2}$ or $p|x - \sqrt{-2}$ because $\mathbb{Z}[\sqrt{-2}]$ is a unique factorization domain. This produces an equation $x \pm \sqrt{-2} = p(a + b\sqrt{-2})$ from which it follows that $pb = \pm 1$. This is impossible. Therefore, p is not irreducible in $\mathbb{Z}[\sqrt{-2}]$.

Given $p \equiv 1$ or $7 \pmod 8$, then 2 is a quadratic residue of p by Lemma 4. Therefore, there exists some $x \in \mathbb{Z}$ such that $p|(x^2 - 2)$. Since $x^2 - 2 = (x + \sqrt{2})(x = \sqrt{2})$, irreducibility of p would imply that $p|x + \sqrt{2}$ or $p|x - \sqrt{2}$, because $\mathbb{Z}[\sqrt{2}]$ is a unique factorization domain. This produces an equation $x \pm \sqrt{2} = p(a + b\sqrt{2})$, from which it follows that $pb = \pm 1$. Again, this is impossible, and p is not irreducible in $\mathbb{Z}[\sqrt{2}]$. $\square$

Theorem 8. *Let p be an odd prime. If $p \equiv 1$ or $3 \pmod 8$, then p can be written in the form $a^2 + 2b^2$, and if $p \equiv 1$ or $7 \pmod 8$, then p can be written in the form $a^2 - 2b^2$.*

Proof. Given $p \equiv 1$ or $3 \pmod 8$, then p is not irreducible in $\mathbb{Z}[\sqrt{-2}]$, and given $p \equiv 1$ or $7 \pmod 8$, then p is not irreducible in $\mathbb{Z}[\sqrt{2}]$ by Theorem 7. Then $p = (a + b\sqrt{\mp 2})(c + d\sqrt{\mp 2})$, where neither term on the right is a unit. Then $p^2 = (a^2 \pm 2b^2)(c^2 \pm 2d^2)$. Therefore, $p = a^2 \pm 2b^2 = c^2 \pm 2d^2$ (because $a^2 \pm 2b^2$ and $c^2 \pm 2d^2$ are not units). The desired conclusion follows easily. □

Lemma 9. *The product of two numbers of the form $a^2 \pm 2b^2$ is itself of the form $a^2 \pm 2b^2$.*

Proof. We have

$$\begin{aligned}(a^2 \pm 2b^2)(c^2 \pm 2d^2) &= (a + b\sqrt{\mp 2})(a - b\sqrt{\mp 2})(c + d\sqrt{\mp 2})(c - d\sqrt{\mp 2}) \\ &= (a + b\sqrt{\mp 2})(c + d\sqrt{\mp 2})(a - b\sqrt{\mp 2})(c - d\sqrt{\mp 2}) \\ &= ((ac \mp 2bd) + (ad + bc)\sqrt{\mp 2})((ac \mp 2bd) - (ad + bc)\sqrt{\mp 2}) \\ &= (ac \mp 2bd)^2 \pm 2(ad + bc)^2\end{aligned}$$

. □

We are now ready to state and prove the main result of this work.

Theorem 10. *Let $n = N^2 m$, where m is square-free. Then n can be written in the form $a^2 + 2b^2$ if and only if m contains no prime factor p such that $p \equiv 5$ or $7 \pmod 8$, and n can be written in the form $a^2 - 2b^2$ if and only if m contains no prime factor p such that $p \equiv 3$ or $5 \pmod 8$.*

Proof. Suppose that we have $n = N^2 m = a^2 \pm 2b^2$. Let $d = \gcd(a, b)$, and write $a = dr$, $b = ds$, so that $n = N^2 m = d^2(r^2 \pm 2s^2)$. Then $d^2 | N^2 m$, and, given that m is square-free, we have that $d^2 | N^2$. Hence we can write $(N^2/d^2)m = r^2 \pm 2s^2 = t$ for some integer t. Let p be a prime factor of t. Then $r^2 \pm 2s^2 \equiv 0 \pmod m$. Now, since r and s are relatively prime, at least one must be relatively prime to p. If s is not relatively prime to p, then $r^2 = t \mp 2s^2$, and, if $p|s$, then $p|r$, a contradiction. Hence it must be that p is relatively prime to s. Thus there exists some s' such that $ss' \equiv 1 \pmod p$. Multiplying the equation $r^2 \pm 2s^2 \equiv 0 \pmod p$ then yields $(rs')^2 \pm 2 \equiv 0 \pmod p$, or $(rs')^2 \equiv \mp 2 \pmod p$. Thus ∓ 2 is a quadratic residue of p. Recall that -2 is a quadratic residue of p if and only if $p \equiv 1$ or $3 \pmod 8$, and 2 is a quadratic residue of p if and only if $p \equiv 1$ or $7 \pmod 8$ by Lemma 4. Thus if n is of the form $a^2 + 2b^2$, then each prime factor of (t and hence) m satisfies the condition $p \equiv 1$ or $3 \pmod 8$, and if n is of the form $a^2 - 2b^2$, then each prime factor p of m satisfies the condition $p \equiv 1$ or $7 \pmod 8$.

For the converse, the condition on m and Theorem 8 guarantee that each odd prime factor of m can be written in the appropriate form. Of course, $2 = 0^2 + 2 \cdot 1^2 = 2^2 - 2 \cdot 1^2$. Thus each prime factor of m can be written in the appropriate form, and the result follows from Lemma 9. □

Theorem 10 is our desired result. It shows that a number n can be written in the form $a^2 + 2b^2$ (respectively, $a^2 - 2b^2$) if and only if each prime $p \equiv 5$ of $7 \pmod 8$ (respectively, $p \equiv 3$ or $5 \pmod 8$)) that divides n occurs to an even power in the prime factorization of n.

References

[1] Burton, David, *Elementary number theory* (sixth edition), McGraw-Hill, Boston, 2007.
[2] Hungerford, Thomas, *Abstract algebra, an introduction* (2nd edition), Thomson Learning, Inc., 1997.

Department of Mathematics and Statistics, University of North Carolina at Charlotte, Charlotte, NC 28223 U.S.A.
E-mail address: rmzeman.uncc.edu

Sponsor: Evan Houston, Professor of Mathematics, UNC Charlotte
E-mail address: eghousto@uncc.edu