INTEGRAL 4 BY 4 SKEW CIRCULANTS*

WILLIAM C. WATERHOUSE
The Pennsylvania State University, University Park, PA 16802

(Submitted June 1986)

1. INTRODUCTION

A 4 by 4 skew circulant matrix is a matrix of the form

$$\begin{bmatrix} a & b & c & d \\ -d & a & b & c \\ -c & -d & a & b \\ -b & -c & -d & a \end{bmatrix}$$

and the determinant of such a matrix is called a "skew circulant." A pleasant article by I. J. Good [2] devoted to skew circulants contains, in particular, a study of the values such a determinant could take for integer entries a, b, c, and d. The numerical evidence led him to two conjectures:

Conjecture I. An odd prime p occurs as a value if and only if $p \equiv 1 \pmod 8$.

Conjecture II. A positive integer in general occurs as a value if and only if it is a power of 2 times a square times primes $\equiv 1 \pmod 8$.

In this note I shall prove that both conjectures are correct. This is not altogether a new result, for (as Good later pointed out in [3]) there is work on the topic going back to Jacobi; as we shall note at the end of the paper, much more general results have been obtained using advanced methods of algebraic number theory. But it is possible to prove the two conjectures by elementary means, using hardly anything beyond the material available (for instance) in Hardy and Wright [4].

2. REFORMULATION IN TERMS OF ROOTS OF UNITY

Following Good's paper, we begin by reformulating the question in terms of roots of unity. The point is that the particular matrix J with $a = c = d = 0$ and $b = 1$ generates the skew circulant matrices, in the sense that an arbitrary

*Work supported in part by the National Science Foundation, Grant No. DMS-8400649.

one can be expressed as

$$aI + bJ + cJ^2 + dJ^3 \text{ (with } J^4 = -I\text{).}$$

Thus, if $j = \exp(\pi i/4) = (1 + i)/\sqrt{2}$ is a primitive 8th root of unity, then the map sending J to j induces an isomorphism (bijection preserving both sums and products) from the family of integral skew circulant matrices to the subring A of the complex numbers consisting of integral combinations of powers of j. The same would be true if we sent J to any one of the other primitive 8th roots of unity, which are j^3, j^5, and $j^7 = j^{-1}$. When we deal with elements of A, we call these other values (obtained by replacing j by an appropriate power) the "conjugates" of the original element. Straightforward computation shows that the determinant is simply then the product of the element and its three conjugates, which in rings like this is usually called the "norm." Thus, our question is concerned with possible norms of elements. Worked out as a polynomial in a, b, c, and d, the norm $N(a + bj + cj^2 + dj^3)$ can be written as

$$(a^2 - c^2 + 2bd)^2 + (b^2 - d^2 - 2ac)^2, \text{ or as}$$
$$(a^2 + b^2 + c^2 + d^2)^2 - 2(ad - ab - bc - ac)^2, \text{ or as}$$
$$(a^2 - b^2 + c^2 - d^2)^2 + 2(ad + ab - bc + cd)^2.$$

In particular, of course, the first expression shows that the norm is positive for nonzero elements of A. Furthermore, these three factorizations (arising originally from different ways of grouping the conjugates in the product into pairs) reflect three subrings that will play a role in our analysis:

$$A_1 = \text{combinations of 1 and } j^2 = i,$$
$$A_2 = \text{combinations of 1 and } \sqrt{2} = j + j^7, \text{ and}$$
$$A_3 = \text{combinations of 1 and } i\sqrt{2} = j + j^3.$$

Note, at once, that a conjugate of a product of elements is the corresponding product of conjugates and, hence, the norm of a product is the product of the norms. Also note that $a = b = 1$, $c = d = 0$ gives $N = 2$. Hence, 2 and all its powers occur as norms; and if an odd number q occurs as a norm, so does every product $2^r q$. Thus, our main concern is with possible odd norms.

3. BASIC FACTS ABOUT FACTORIZATION IN A

The basic idea that we need was already suggested by the expression of the norm as a product: it is factorization. The facts involved are available in several texts, such as [4], and I shall state some of them here without proof.

The most important [4, p. 230] is that *unique factorization holds* for our ring A. That is, every element that is not a unit can be written as a product of primes, and this product is unique except for multiplication by units. Here a unit is an element of A that has an inverse in A, and a prime is an element that cannot be factored except by allowing one of the factors to be a unit.

Now, if an element x is a unit, then we have $xy = 1$ for some y in A. It follows that $N(x)N(y) = N(1) = 1$ and, hence, $N(x) = \pm 1$. But the first of the formulas for the norm above shows that norms are nonnegative; thus, any unit in A has norm 1. Conversely, whenever $N(x) = 1$, the product of x by its other conjugates is 1, and, of course, this shows that x has an inverse in A. Thus, we have the following lemma.

Lemma 1: An element of A is a unit if and only if its norm is 1.

The units of A have, in fact, been known at least since the time of Kronecker [5] and are listed in Good's paper [3]: they are powers of j times $(1+\sqrt{2})^r$ for integral r.

Furthermore, since every (nonunit) element in A is a product of prime elements, every norm except 0 and 1 will be a product of norms of prime elements.

Lemma 2: An integer larger than 1 occurs as a norm from A if and only if it is a product of integers that occur as norms of prime elements in A.

We already know that $2 = N(1 + j)$ occurs as a norm. Incidentally, this shows that $1 + j$ is a prime in A; for, if we have a factorization $1 + j = yz$, then

$$2 = N(1 + j) = N(y)N(z),$$

and, hence, either $N(y) = 1$ or $N(z) = 1$. Observe now that every prime element π in A divides an ordinary integer, namely $N(\pi)$. But we can write this positive integer as the product of its ordinary integer prime factors. Since π is prime in A and divides this product, unique factorization shows that π must divide one of the factors. Therefore, we have the following lemma.

Lemma 3: Every prime of A divides some ordinary prime integer.

Thus, we can determine the possible norms if only we can determine enough about how ordinary integer primes factor in A.

4. PROOF OF THE CONJECTURES

The next information we need [4, pp. 212-13] is that the rings A_1, A_2, and A_3 also have unique factorization (though, of course, the elements that are "prime" in them may factor when we allow the larger range of possible factors available in A). Furthermore, we know in detail just how the different odd integer primes p factor in these quadratic fields. (The integer 2 factors as a unit times a square of a prime in each of them, but we do not need that information.) The factorizations of p are essentially equivalent to information on the representability of the prime p by suitable quadratic forms; thus, for instance [4, p. 219], we can factor p nontrivially in A_1 iff it can be written as $(a + bi)(a - bi)$, which happens iff we can express p as $a^2 + b^2$. It is well known that this is possible iff p is congruent to 1 mod 4. Similar statements are true in the other two A_i: either p remains a prime in A_i or it factors into two primes, and the different behaviors depend only on p mod 8. (The result for A_2 is worked out in [4, p. 221], where it is remarked that A_3 can be treated similarly.) In A_2, the primes congruent to 1 or 7 mod 8 can be factored into two prime factors, while those congruent to 3 or 5 remain prime; and in A_3, those congruent to 1 or 3 mod 8 can be factored, while the others remain prime.

Now, first of all, this tells us at once that all squares of odd primes are norms from A. For, if (for instance) we have p congruent to 5 mod 8, then p factors at least as $(a + bi)(a - bi)$. We then have

$$p^4 = N(p) = N(a + bi)N(a - bi).$$

Furthermore, $a + bi$ and $a - bi$ are conjugates. Thus, they both must have the same norm, namely p^2. A simple congruence argument given by Good [2, pp. 55-56] shows that p cannot itself be a norm, and an argument like that after Lemma 2 shows then that $a \pm bi$ here are prime elements in A. Similarly, if p is congruent to 7 mod 8, then it factors as $(a + b\sqrt{2})(a - b\sqrt{2})$, and the factors have norm = p^2 and are prime in A; while, if p is congruent to 3 mod 8, then it factors as $(a + bi\sqrt{2})(a - bi\sqrt{2})$, and again the factors have norm = p^2 and are prime in A.

Of course, the primes p congruent to 1 mod 8 are the ones that deserve special attention. We know that such a p factors into two factors in each of the rings A , and hence, as before, p^2 occurs as a norm. But the existence of these different factorizations should lead us to suspect that we have not actually found the prime factors of p in A, and that is exactly what is true. We can, e.g., write p as $(a + bi)(a - bi)$; we can also write p as $(c + d\sqrt{2})(c - d\sqrt{2})$. If (say) $c + d\sqrt{2}$ is prime in A, then its conjugate $c - d\sqrt{2}$ is also prime, since the conjugations are isomorphisms. By unique factorization, the two nonunit factors $a \pm bi$ must be units times $c \pm d\sqrt{2}$. But since we know the units in A, this gives

$$a \pm bi = j^k(1 + \sqrt{2})^r(c \pm d\sqrt{2}).$$

Thus, $a \pm bi$ would have to be j^k times a real number. Such an equality can occur only when $a = 0$ or $b = 0$ or $a = \pm b$, all of which are impossible when $a^2 + b^2 = p$. Thus, the element $c + d\sqrt{2}$ (of norm p^2) must have nontrivial factors, and they can only have norm p. Hence, we have proved both conjectures.

5. A SUBSIDIARY CONJECTURE

There is one other conjecture made in Good's paper [2], but it is closer to familiar results and we can dispose of it quickly; it is worth noting, however, that unique factorization is again the main idea. We already know that there exists a solution of the equation $p = a^2 - 2b^2$ when p is congruent to 1 or 7 mod 8, and the problem is then to determine all solutions. But one solution corresponds to a factorization $p = (a + b\sqrt{2})(a - b\sqrt{2})$ in A_2, and, hence, unique factorization shows that all other solutions must differ by units; and since we know the units (solutions of Pell's equation!), any other solution α, β must satisfy $\alpha + \beta\sqrt{2} = \pm(1 + \sqrt{2})^r(a \pm b\sqrt{2})$. By proper choice of signs for α and β, we can assume that $\alpha + \beta\sqrt{2} = (1 + \sqrt{2})^r(a + b\sqrt{2})$. To get the product to come out equal to p rather than $-p$, we must have r even, or, in other terms,

$$\alpha + \beta\sqrt{2} = (3 + 2\sqrt{2})^s(a + b\sqrt{2}).$$

Thus, the solutions are exactly those given by the recurrences in [2, p. 57].

6. GENERALIZATIONS

We have shown that in the ring A generated by 8th roots of units, an odd prime p occurs as a norm iff p is congruent to 1 mod 8; along the way, we were reminded also that an odd prime p occurs as a norm from the ring A_1 generated by 4th roots of unity iff p is congruent to 1 mod 4. The general fact is that essentially the same result holds in general, *but* the statement has to be modified because unique factorization usually fails to be true in the rings generated by higher roots of unity. This was the famous discovery of Kummer that set modern algebraic number theory on its way (cf. Edwards [1]). He introduced certain objects called "ideal prime factors" and he could prove that there was a unique factorization into them. Furthermore, when we take the ring generated over the integers by the nth roots of unity, an odd prime p (relatively prime to n) will be a norm of one of these "ideal" factors iff it is congruent to 1 mod n. But these ideal primes correspond to actual single elements of the ring only when we have unique factorization, which holds in only finitely many cases (which are all known; see [6] or [7, Chap. 11]). In particular, it holds for $n = 16$ and for $n = 32$, but not for any higher powers of 2.

REFERENCES

1. H. M. Edwards. *Fermat's Last Theorem.* New York: Springer, 1977.
2. I. J. Good. "Skew Circulants and the Theory of Numbers." *The Fibonacci Quarterly 24*, no. 1 (1986):47-60.
3. I. J. Good. "Skew Circulants and the Theory of Numbers: An Addendum." *The Fibonacci Quarterly 24*, no. 2 (1986):176-177.
4. G. H. Hardy & E. M. Wright. *An Introduction to the Theory of Numbers.* 4th ed. Oxford: Oxford University Press, 1960.
5. L. Kronecker. "Über komplexe Einheiten." *J. reine angew. Math. 53* (1857): 176-181 = *Werke* I:109-118. New York: Chelsea, 1968.
6. J. Masley & H. Montgomery. "Cyclotomic Fields with Unique Factorization." *J. reine angew. Math. 286/287* (1976):248-256.
7. L. C. Washington. *Introduction to Cyclotomic Fields.* New York: Springer-Verlag, 1982.

◆◇◆◇◆