SKEW CIRCULANTS AND THE THEORY OF NUMBERS: AN ADDENDUM

I. J. GOOD
Virginia Polytechnic Institute and State University,
Blacksburg, VA 24061
(February 3, 1986)

While correcting the proofs of my article "Skew Circulants and the Theory of Numbers," my interest in the topic was revived, and I have now tracked down some relevant work by the great Jacobi. On pages 277 and 278 of his paper "Uber die complexen Primzahlen, welche in der Theorie der Reste 5^{ten}, 8^{ten} und 12^{ten} Potenzen zu Betrachten sind" (1839), which is in Volume VI of his collected papers, he shows that any prime of the form $8n + 1$ can be factorized as $\phi(\alpha)\phi(\alpha^3)\phi(\alpha^5)\phi(\alpha^7)$, where $\alpha = \exp(2\pi i/8)$ and $\phi(\alpha)$ is of the form $y' + y''\alpha^2 + z'\alpha + z''\alpha^3$, and this is equivalent to my first conjecture although Jacobi does not mention skew circulants. His proof depends on Gauss's theory of "biquadratic residues" and on work by Lagrange (presumably Lagrange's *Oeuvres* III, pp. 693-795). Jacobi's proof is too succinct for me to understand, and I think he may have been slightly careless. For example, he says (in free translation): "One can prove that any number $a + ib$ that divides a number of the form $y^2 - iz^2$ is again of this form itself, and the proof is exactly like that of the analogous fact that any whole number that divides a number of the form $y^2 + z^2$ is itself a sum of two squares. (Without some gloss, this last statement is false; for example, 7 divides $49^2 + 196^2$. No doubt y and z are supposed to be mutually prime.) If his paper had been written by a much less eminent mathematician, I might have suspected that his claims were based in part on numerical evidence and not on complete proofs.

The basic idea in Jacobi's proof is to note that much of ordinary number theory can be generalized to the Gaussian integers $a + ib$.

Jacobi states that a similar method can be used to prove that every prime of the form $12n + 1$ can be expressed as a product of four factors each related to a twelfth root of unity. (Also in the forms $a^2 + b^2$, $c^2 + 3d^2$, and $e^2 - 3f^2$.) This result cannot lead to an expression of $12n + 1$ as a skew circulant of order other than 2 because, for example, 13 and 37 are primes of the form $12n + 1$ but not of the form $8m + 1$. Jacobi mentions further that a prime of the form $5n + 1$ can always be written in the form $a^2 - 5b^2$. The smallest prime that is of all three forms $5\ell + 1$, $8m + 1$, and $12n + 1$ is 241 and is, therefore, presumably the smallest number that can be expressed in all six of the ways:

$$a^2 + b^2,\ c^2 + 2d^2,\ e^2 + 3f^2,\ g^2 - 2h^2,\ k^2 - 3\ell^2, \text{ and } p^2 - 5q^2.$$

Indeed,

$$\begin{aligned} 241 &= 4^2 + 15^2 \\ &= 13^2 + 2\times 6^2 \\ &= 7^2 + 3\times 8^2 \\ &= 21^2 - 2\times 10^2 \\ &= 17^2 - 3\times 4^2 \\ &= 31^2 - 5\times 12^2. \end{aligned}$$

SKEW CIRCULANTS AND THE THEORY OF NUMBERS: AN ADDENDUM

Any prime of the form $120n + 1$ will, of course, have the six representations. Presumably (i) the expressions with positive signs are unique, and (ii) those with negative signs have an infinity of representations.

The main point of this addendum is, of course, that the first conjecture in my paper is equivalent to a result seemingly proved by Jacobi in 1839, although he did not express the result in terms of skew circulants.

I expect that anyone familiar with both Gauss's and Lagrange's work would be able to prove my second conjecture which specified all the integers expressible as skew circulants of order 4. Unfortunately, during the next several months, my other commitments will prevent me from achieving the requisite familiarity, fascinating though this study would undoubtedly be.

♦◇♦◇♦