

THE FORMS $x + 32y^2$ AND $x + 64y^2$

IRVING KAPLANSKY

(Communicated by Lance W. Small)

Throughout this note p is a prime of the form $8n + 1$. One knows that p is represented by both $x^2 + 8y^2$ and $x^2 + 16y^2$. What about the next two powers of 2? Apparently the following result does not appear in the literature.

Theorem. *A prime of the form $16n + 9$ is represented by exactly one of $x^2 + 32y^2$ and $x^2 + 64y^2$. A prime of the form $16n + 1$ is represented either by both or by neither.*

Although this is a simple elementary statement I do not have a direct proof. Instead I shall show that it is a quick corollary of two significant theorems.

(1) The first theorem states that 2 is a 4th power mod p if and only if p is represented by $x^2 + 64y^2$. This is due to Gauss [5, p. 530]. Dirichlet gave an elegant proof [3].

(2) The second theorem states that -4 is an 8th power mod p if and only if p is represented by $x^2 + 32y^2$. This worthy companion to Gauss' theorem is due to Barrucand and Cohn [2].

Although it is peripheral to this paper I mention that there is a third theorem of this kind: -2 is an 8th power mod p if and only if p is represented by $x^2 + 256y^2$. This is due to Aigner [1, Satz 108 on page 195]. I searched for a fourth such result and came up empty-handed. There are, however, theorems concerning the 2^r power behavior of $2 \bmod p$; three references are [4], [6], and [7].

We proceed to the proof of the theorem. We shall work in the integers mod p , speaking of equality rather than congruence. The multiplicative group is cyclic of order $p - 1$, a multiple of 8. Note that p is of the form $16n + 1$ if and only if -1 is an 8th power. Also, if an element has square equal to 1 it is a 4th power, and if it has 4th power equal to 1 it is a square. Now 2 is a square, say $2 = a^2$. Also -4 is a 4th power (if t is a square root of -1 , then $-4 = (t + 1)^4$). Say $-4 = b^4$. If b is a square, then -4 is an 8th power. Conversely if -4 is an 8th power, say c^8 , then $b^4 = c^8$, $(b/c^2)^4 = 1$, b/c^2 is a square, b is a square. Similarly, 2 is a 4th power if and only if a is a square. Next we note $-1 = -4/4 = b^4/a^4 = (ab/a^2)^4/a^8$. If ab is a square, then -1 is an 8th power. If -1 is an 8th power, say d^8 , then $(ab/d^2)^4 = 1$, ab/d^2 is a square, ab is a square. Thus -1 is an 8th power if and only if ab is a square and this holds if and only if a and b are both squares or both nonsquares. The theorem is proved.

Received by the editors April 30, 2002 and, in revised form, August 15, 2002.
2000 *Mathematics Subject Classification.* Primary 11E16.

©2003 American Mathematical Society

REFERENCES

- [1] A. Aigner, *Zahlentheorie*, de Gruyter, 1975. MR **56**:2901
- [2] P. Barrucand and H. Cohn, *Note on primes of type $x^2 + 32y^2$, class number and residuacity*, J. Reine Angew. Math. **238** (1969), 67–70. MR **40**:2641
- [3] G. Lejeune Dirichlet, *Über den biquadratischen Character der Zahl “Zwei”*, in Werke vol. II, Chelsea reprint, 1969, pp. 257–258. MR **40**:2514
- [4] R. J. Evans, *The 2^r -th character of 2*, J. Reine Angew. Math. **315** (1980), 174–189. MR **81f**:10006
- [5] C. F. Gauss, *Theorie der biquadratischen Reste*, I, in Arithmetische Untersuchungen, Chelsea reprint, 1969, pp. 511–533. (This translation by H. Maser of the Disquisitiones also contains several of Gauss’ papers.)
- [6] H. Hasse, *Der 2^n -te Potenzcharacter der 2^n -ten Einheitswurzeln*, Rend. Circ. Mat. Palermo **7** (1958), 185–244. MR **21**:4143
- [7] A. L. Whiteman, *The sixteenth power residue character of 2*, Canad. J. Math. **6** (1954), 364–373. MR **16**:14a

MATHEMATICAL SCIENCES RESEARCH INSTITUTE, BERKELEY, CALIFORNIA 94720
E-mail address: kap@msri.org