ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 27, Number 1 Winter 1997

EISENSTEIN AND THE JACOBIAN VARIETIES OF FERMAT CURVES

ALLAN ADLER

ABSTRACT. In this paper we present evidence that Eisenstein knew something about the Jacobian varieties of Fermat curves, including the curve of degree 7. More precisely, the evidence suggests that Eisenstein had some way of knowing that certain differentials on these Fermat curves are reducible to elliptic differentials without explicitly reducing them. Our argument depends on a close examination of Gauss' first memoir [**39**] on biquadratic residues and of three related papers [**12, 13, 14**] of Eisenstein. In particular, we include a certain amount of expository material that may be of independent interest to many readers. We do not insist that the hypothesis presented here is necessarily true. We also point to evidence against it and to interesting directions for further study of Eisenstein's work.

0. Introduction. The discovery that every prime of the form $4n+1$ is the sum of two squares is due to Fermat[1] [**34**], [**35**][2], [**36**][3] along with results for representing the numbers in the form a^2+2b^2 and a^2+3b^2. Proofs of these results were published by Euler [**27, 28**]. In Gauss' Disquisitiones [**38**, Section 182, pp. 159–163], the results are proved again as simple consequences of his theory of binary quadratic forms. A striking refinement of the results for primes of the form $4n+1$ appears in Gauss' paper [**39**]. It is that refinement, rarely included in courses on number theory, which concerns us here.

To state Gauss' result, let $p = 4n+1$ be a prime number. Then Gauss' theorem says that p can be written in the form a^2+b^2 where a and b are integers and where $2a$ is congruent modulo p to the binomial coefficient $\binom{2n}{n}$. Since the absolute value of a is necessarily less than

AMS *Subject Classification Numbers* (1980). 01A55, 10A03, 10A10, 10A15, 10B35, 10D25, 12C20, 14H40, 14H45, 14K07, 14K22, 32A05, 33A25.

Key words and phrases. Abelian function, binomial coefficient, CM type, complex multiplication, diagonal hypersurface, Eisenstein sum, elliptic curve, elliptic function, Fermat curve, Gauss sum, Jacobi sum, Klein curve, Kronecker congruence relation, Lemniscatic function, permutation twist.

Received by the editors on July 29, 1992, and in revised form on September 15, 1995.