Class numbers and a generalized Fermat theorem.


Corrigenda: “Class numbers and a generalized Fermat theorem”.


This article is concerned with two somewhat related problems, namely class number divisibility and representation of numbers by certain binary quadratic forms.

Some results of M. Watabe [J. Reine Angew. Math. 301 (1978), 212–215; MR0506086 (80h:12005)] are corrected and generalized in the first part of the article. The first theorem employs the well-known formula for the number of ambiguous classes for a cyclic extension to obtain several nice class number divisibility criteria. For example, if \( p \) and \( q \) are primes with \( p \equiv 1 (\text{mod } q) \) and \( q \geq 5 \) then the \( pq \)th cyclotomic field has class number divisible by \( q^{(q-3)/2} \). Also, the author describes certain cyclic extensions \( K/k \) of \( p \)-power degree such that the conditions \( p \mid h(k), \ p \mid h(K) \) and \( p \mid h(L) \) are all equivalent, where \( L \) is a certain cyclotomic extension of \( K \).

In the second section of the article the author relates representations of integers \( n \) by the binary quadratic form \( f = x^2 - py^2 \) for an odd prime \( p \) or \( f = x^2 + y^2 \) when \( p = 2 \), to the solvability of \( \varphi_{2p}(X) \equiv 0 (\text{mod } n) \), where \( \varphi_{2p}(X) \) is the \( 2p \)th cyclotomic polynomial. The hypothesis that \( \mathbb{Q}(\sqrt{p}) \) has class number 1 is assumed for this result. However, it appears that the theory of genera of binary quadratic forms [Z. I. Borevich and I. R. Shafarevich , Number theory, see p. 240, Theorem 3, Academic Press, New York, 1966; MR0195803 (33 #4001)] can be employed to give better results.

The corrigenda correct a couple of misprints and omissions and the proof of one case of Theorem 2.6. 

Charles J. Parry (1-VAPI)