ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 31, Number 1, Spring 2001

ON EXPLICIT FORMULAS FOR THE MODULAR EQUATION

SHAMITA DUTTA GUPTA AND XIAOTIE SHE

ABSTRACT. An algorithm is given to determine explicitly the modular equation $\Phi_n(X,J)=0$ of degree n, $n=p^2$. $\Phi_9(X,J)$ is used as an example.

1. Introduction. Let $J(z)$ be the modular invariant of an elliptic curve. The modular equation $\Phi_n(X,J)=0$ of degree n is the algebraic relation between $X=J(nz)$ and $J(z)$. This equation is one of the key concepts in algebraic number theory [**2**], [**3**], [**6**], [**8**] closely related to class field theory, theory of elliptic curves, theory of complex multiplication, etc. In recent years it has been generalized to other settings, such as Drinfeld module [**1**].

The explicit form of modular equation $\Phi_n(X,J)$ for small primes 2, 3, 5, 7, 11 can be found in literature [**4**], [**5**]. Through private communication, it is known to authors that for $n=4$ and primes up to 31, the explicit forms for the modular equations have been obtained recently. For any prime p, Yui [**10**] gave an algorithm to determine $\Phi_p(X,J)$ by using the q-expansion of the j-invariant. In the case of the Drinfeld modular polynomial $\Phi_T(X,Y)$, Schweizer used another approach [**7**].

In this work we extend Yui's method to compute the $\Phi_n(X,J)$ for $n=p^2$. As the q-expansion of the j-invariant is insufficient in this case, we introduce another expansion at the second cusp, other than $i\infty$. As an example, $\Phi_9(X,J)$ is given. Traditionally, $\Phi_{p^e}(X,J)$ is reduced to $\Phi_p(X,J)$ using Theorem 2. The authors believe that the algorithm offered here, when compared to Theorem 2, is simpler and more applicable.

2. The modular equation. The modular function $J(z)$ of the

Received by the editors on August 25, 1999, and in revised form on November 8, 1999.