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.

elliptic curve $E : y^2 = 4x^3 - g_2(z)x - g_3(z)$ over $\mathbf{C}$ is defined by

$$J(z) = 12^3 \frac{g_2^3(z)}{\Delta(z)},$$

where $\Delta(z) = g_2^3(z) - 27g_3^2(z) \neq 0$ is the discriminant of E.

Let $\Gamma = SL_2(\mathbf{Z})$, $\Gamma_n = \{\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mid a, b, c, d \in \mathbf{Z}, (a, b, c, d) = 1, \det \alpha = n\}$. Let Γ and Γ_n operate on the upper half plane $\mathcal{H} = \{z = x + iy \in \mathbf{C} \mid y > 0\}$ in the usual way.

We have

$$\Gamma_n = \bigcup_{i=1}^{\psi(n)} \Gamma\alpha_i,$$

where $\psi(n) = n \prod_{p|n}(1 + (1/p))$ and

$$\{\alpha_i\} = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid ad = n, (a, d, b) = 1, 0 \leq b < d \right\}.$$

For $n > 1$, consider the polynomial

$$\Phi_n(X) = \prod_{i=1}^{\psi(n)} (X - J \circ \alpha_i) = \sum_{m=0}^{\psi(n)} s_m X^{\psi(n)-m},$$

with an indeterminate X, where $J \circ \alpha_i = J(\alpha_i(z))$. It is known that $s_m \in \mathbf{Z}[J]$. For details, see [**3**], [**6**]. Thus $\Phi_n(X)$ is a polynomial in two independent variables X and J over $\mathbf{Z}$, i.e.,

$$\Phi_n(X) = \Phi_n(X, J) = \prod_{i=1}^{\psi(n)} (X - J \circ \alpha_i) \in \mathbf{Z}[J, X].$$

The polynomial $\Phi_n(X, J)$ is called the modular polynomial of degree n. The equation $\Phi_n(X, J) = 0$ is called the modular equation of degree n. Here are some well known results:

Theorem 1. *Let $\Phi_n(X, J)$ be the modular polynomial of order n.*

(1) *The polynomial $\Phi_n(X, J)$ is irreducible over $\mathbf{C}(J)$ and has degree $\psi(n) = n \prod_{p|n}(1 + (1/p))$.*

(2) *We have* $\Phi_n(X,J) = \Phi_n(J,X)$.

For the proof, see [**6**].

By Theorem 1 we can write

$$\Phi_n(X,J) = X^{\psi(n)} + J^{\psi(n)} + \sum_{0\le j\le i\le \psi(n)-1} C_{ij}(X^iJ^j + X^jJ^i),$$

where $C_{ij} \in \mathbf{Z}$, $F_{i,j} = X^iJ^j + X^jJ^i$, $j \le i$. So to determine $\Phi_n(X,J)$ explicitly is to determine C_{ij} explicitly.

For $n = p$ prime, the coefficient C_{ij} may be obtained by studying the q-expansion of $j(z)$. For n composite, $\Phi_n(X,J)$ is reduced to the prime cases by the following theorem.

Theorem 2 [**3**], [**9**]. *Let $n > 1$ be an integer, and set $\psi(n) = n\prod_{p|n}(1 + (1/p))$.*

(i) *If $n = n_1n_2$, $(n_1,n_2) = 1$, then*

$$\Phi_n(X,J) = \prod_{i=1}^{\psi(n_2)} \Phi_{n_1}(X,\xi_i)$$

where $X = \xi_i$ are the roots of $\Phi_{n_2}(X,J) = 0$.

(ii) *If $n = p^e$ where p is prime and $e > 1$, then*

$$\Phi_n(X,J) = \begin{cases} (\prod_{i=1}^{\psi(p^{(e-1)})} \Phi_p(X,\xi_i))/[\Phi_{p^{e-2}}(X,J)]^p & e > 2, \\ (\prod_{i=1}^{p+1} \Phi_p(X,\xi_i))/(X-J)^{p+1} & e = 2, \end{cases}$$

where $X = \xi_i$ are the roots of $\Phi_{p^{e-1}}(X,J) = 0$.

For the proof, see Weber [**9**].

Theorem 2 implies an algorithm for computing $\Phi_{p^2}(X,J)$. However, in this work we will find $\Phi_{p^2}(X,J)$ using q-expansion at two cusps.

3. Cusps and expansions. In this section we will give some known facts concerning the cusps of $\Gamma_0(p^e)$ and the expansions of $X = J(p^ez)$ and $J = J(z)$ at those cusps.

Let $\Gamma_0(p^e) = \{\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma = \mathrm{SL}\,(2, \mathbf{Z}) \mid c \equiv 0 \pmod{p^e}\}$. We have

Lemma 1. *A complete set of coset representations $\{\alpha_j\}$ for $\Gamma_0(p^e)$ in Γ is*

$$\begin{aligned} &\{I\} \cup \{ST^k \mid k = 0, 1, \ldots, p^e - 1\} \\ &\qquad \cup \{ST^{kp}S \mid k = 1, 2, \ldots, p^{e-1} - 1\}, \end{aligned}$$

where

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \textit{and} \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Lemma 2. *The cusps of $\Gamma_0(p^e)$ are*

$$\{\infty; 0\} \cup \left\{ -\frac{1}{kp} \mid k = 1, \ldots, p-1 \ \textit{or}\ k = k'p,\ k' = 1, 2, \ldots, p^{e-2} - 1 \right\}.$$

Let x be a cusp of $\Gamma_0(p^e)$. Let $\alpha \in \mathrm{SL}\,(2, \mathbf{Z})$, $\alpha(x) = \infty$. Define $\Gamma_x = \{\gamma \in \Gamma_0(p^e) \mid \gamma(x) = x\}$. Then $\alpha\Gamma_x\alpha^{-1}(\infty) = \infty$. Thus, $\alpha\Gamma_x\alpha^{-1}(\infty)$ is a subgroup of $\langle \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \rangle = \Gamma_\infty$. If $\alpha\Gamma_x\alpha^{-1}(\infty)$ is generated by $\left(\begin{smallmatrix} 1 & n \\ & 1 \end{smallmatrix}\right)$, $n > 0$, n is called the width of the cusp x. For any modular function f of $\Gamma_0(p^e)$, we define the Fourier expansion of f at a cusp x to be the Fourier expansion of $f(\alpha^{-1}(z))$ at $i\infty$ with respect to $e^{(2\pi i z/n)}$. We have

Lemma 3. *Width of cusp $-(1/kp)$, $k = p^r k'$ is* $\max\{1, p^{e-2-2r}\}$ *where* $\gcd\,(k', p) = 1$.

We omit the proofs of Lemmas 1, 2 and 3. All can be easily checked.

The following is the well-known q-expansion of $J(z)$.

$$J(z) = q^{-1} + 744 + 196884q + 21493760q^2 + \cdots = \sum_{n=-1}^{\infty} a_n q^n, \tag{1}$$

where $q = e^{2\pi iz}$. It is easily checked that $X = J(p^e z)$ is a modular function of $\Gamma_0(p^e)$. And we have

Lemma 4. *The expansion of $X = J(p^e z)$ at the cusp $-(1/p^{r+1})$, $r \leq [e/2] - 1$ is*

$$\zeta_{p^{e-r-1}} e^{-2\pi iz/p^{e-2(r+1)}} + 744 + \cdots = \zeta_{p^{e-r-1}} q_r^{-1} + 744 + \cdots , \tag{2}$$

where $q_r = e^{2\pi iz/p^{e-2-2r}}$, $\zeta_{p^{e-r-1}}$ is the primitive root of 1.

Proof. Choosing $\alpha = ST^{-p^{r+1}}S$, we have

$$\begin{aligned} X \circ \alpha^{-1}(z) &= J\left[\begin{pmatrix} p^e & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ p^{r+1} & -1 \end{pmatrix} (z)\right] \\ &= J\left[\begin{pmatrix} p^{e-r-1} & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} -p^{r+1} & 1 \\ 0 & -p^{e-r-1} \end{pmatrix} (z)\right] \\ &= J\left[\begin{pmatrix} -p^{r+1} & 1 \\ 0 & -p^{e-r-1} \end{pmatrix} (z)\right] \\ &= J\left(\frac{p^{r+1}z - 1}{p^{e-r-1}}\right) \\ &= e^{-2\pi i(p^{r+1}z - 1/p^{e-(r+1)})} + 744 + \cdots \\ &= \zeta_{p^{e-r-1}} q_r^{-1} + 744 + \cdots . \end{aligned}$$

Notice that, by Lemma 3, width at cusp $-(1/p^{r+1})$ is $p^{e-2(r+1)}$.

4. The case $n = p^2$. To simplify the situation, we will only demonstrate our algorithm for the case $n = p^2$. In this case, we will only make use of the Fourier expansion at the two cusps $i\infty$, $-(1/p)$.

At $i\infty$, $X(z)$ has a q-expansion as follows:

$$\begin{aligned} X(z) = J(p^2 z) &= e^{-2\pi ip^2 z} + 744 + 196884 e^{2\pi ip^2 z} + \cdots \\ &= q^{-p^2} + 744 + 196884 q^{p^2} + \cdots , \end{aligned} \tag{3}$$

where $q = e^{2\pi iz}$. At $-(1/p)$, the expansion of $X(z)$ is given by Lemma 4. The expansion of $J(z)$ at $-(1/p)$ is the same as the expansion of $J(z)$ at $i\infty$.

Putting (1), (2) and (3) together, we have the table:

cusp	$i\infty$	$-1/p$
width	1	1
order of pole of X	p^2	1
leading coefficient of X	1	ζ_p
order of pole of J	1	1
leading coefficient of J	1	1
order of pole of $F_{i,j}$	$ip^2 + j$	$i + j$
leading coefficient of $F_{i,j} (i > j)$	1	$\zeta_p^j + \zeta_p^i$
leading coefficient of $F_{i,i}$	2	$2\zeta_p^i$.

The following two lemmas are key to the algorithm. We will give a detailed proof of Lemma 5. Lemma 6 may be proven similarly.

Lemma 5. *Let N be an integer, $N \geq 2p^2 + p - 2$. If $\{C_{ij} \mid i + j \geq N+1$ or $i = p^2+p-1$ and $j \geq p^2-1\}$ is known, then $\{C_{ij} \mid i+j = N\}$ can be determined by comparing the expansions at cusp $-1/p$.*

Proof. As $\Phi_{p^2}(X, J) = 0$, coefficients of q-expansion of $\Phi_{p^2}(X, J)$ at cusp $-1/p$ equal 0. Considering the term q^{-N}, we have

$$\begin{aligned} 0 = & \sum_{i+j=N} C_{ij}(\zeta_p^i + \zeta_p^j) \\ & + \text{coefficient of the term } q^{-N} \text{ in} \\ & \left(X^{\psi(n)} + J^{\psi(n)} + \sum_{i+j \geq N+1} C_{ij} F_{i,j}\right). \end{aligned} \tag{4}$$

The second term on the righthand side of (4) is known. Write $\{(i, j) \mid i \geq j, i + j = N\}$ as

$$\big\{(p^2 + p - 1 - k, N - (p^2 + p - 1) + k) \mid k = 0, 1, \cdots, \\ [(p^2 + p - 1) - (N/2)]\big\}.$$

For $k=0$, $C_{p^2+p-1,N-(p^2+p-1)}$ is known. For unknown C_{ij}, let

$$\begin{aligned} A &= \left\{p^2+p-1-k \mid k=1,2,\cdots,\left[(p^2+p-1)-\frac{N}{2}\right]\right\} \\ &= \left\{i \mid p^2+p-2 \geq i \geq -\left[-\frac{N}{2}\right]\right\} \end{aligned}$$

be the set of the index i,

$$\begin{aligned} B &= \left\{N-(p^2+p-1)+k \mid k=1,2,\cdots,\left[(p^2+p-1)-\frac{N}{2}\right]\right\} \\ &= \left\{j \mid N+\left[-\frac{N}{2}\right] \geq j \geq N-(p^2+p-1)+1\right\} \end{aligned}$$

be the set of the index j.

We have $\min(A) \geq \max(B)$ and

$$\max(A)-\min(B) = (p^2+p-1-1)-(N-(p^2+p-1)+1) \leq p-2,$$

as $N \geq 2p^2+p-2$.

Further, we have $A \cap B = \Phi$ when N is odd, and $A \cap B = \{N/2\}$ when N is even. Thus $\{\zeta_p^m \mid m \in A \cup B\}$ is a linearly independent set over $\mathbf{Q}$; it can be extended to a basis of $\mathbf{Q}(\zeta_p)$ over $\mathbf{Q}$.

After writing the right side of (4) in terms of this basis, C_{ij} may be solved by comparing scalars, in $\mathbf{Q}$, of $\{\zeta_p^i \mid i \in A\}$. Note that, when N is even, and $i=j=(N/2)$, $C_{ij}(\zeta_p^i+\zeta_p^j) = 2C_{ii}\zeta_p^i$. The scalars of $\{\zeta_p^j \mid j \in B, j \neq (N/2)\}$ may be used to verify the calculation.

Lemma 6. *Let N be an integer $2p^2+p-2 \geq N \geq 2p^2-1$. If $\{C_{ij} \mid i+j \geq N+1$ or $i+j=N$ and $j \leq p^2-1\}$ is known, then $\{C_{ij} \mid i+j=N\}$ can all be determined by comparing the expansion at cusp $-1/p$.*

Proof. We will still use equation (4) and write $\{(i,j) \mid i \geq j, i+j=N\}$ as

$$\big\{(p^2+p-1-k, N-(p^2+p-1)+k) \mid k=0,1,\cdots, \\ [(p^2+p-1)-(N/2)]\big\}.$$

For those $k \le (2p^2+p-2)-N$, $j = N-(p^2+p-1)+k \le p^2-1$, and $C_{p^2+p-1-k,N-(p^2+p-1)+k}$ is known. For unknown C_{ij}, let

$$\begin{aligned} A &= \left\{ p^2+p-1-k \mid (2p^2+p-2)-N+1 \le k \le \left[p^2+p-1-\frac{N}{2} \right] \right\} \\ &= \left\{ i \mid N-p^2 \ge i \ge -\left[-\frac{N}{2} \right] \right\} \end{aligned}$$

be the set of the index i,

$$\begin{aligned} B &= \left\{ N-(p^2+p-1)+k \mid (2p^2+p-2)-N+1 \le k \le \left[p^2+p-1-\frac{N}{2} \right] \right\} \\ &= \left\{ j \mid N+\left[-\frac{N}{2} \right] \ge j \ge p^2 \right\} \end{aligned}$$

be the set of index j.

We have $\min(A) \ge \max(B)$ and

$$\max(A)-\min(B) = (N-p^2)-p^2 \le p-2,$$

as $N \le 2p^2+p-2$.

The rest of the proof is similar to that of Lemma 5.

Note that $N < 2p^2-1$ implies $j \le p^2-1$.

Theorem 3. *The modular equation $\Phi_{p^2}(X,J)=0$ can be determined explicitly by studying q-expansion at cusps $i\infty$ and $-1/p$ of $\Gamma_0(p^2)$.*

Proof. We will outline the steps to proceed and the cusps involved in each step.

(i) $\{C_{ij}\}$, where $i = p^2+p-1$, $j \ge p-1$.

We consider the q-expansion at $i\infty$ because $\mathrm{ord}_{i\infty} F_{ij}$ are among the largest and differ from each other.

(ii) $\{C_{ij}\}$, where $i+j \ge 2p^2+p-2$.

As $\mathrm{ord}_{i\infty} F_{p^2+p-1,p-2} = \mathrm{ord}_{i\infty} F_{p^2+p-2,p^2+p-2}$, the q-expansion at $i\infty$ is not useful. We consider the q-expansion at $-1/p$ using Lemma 5.

(iii) $\{C_{ij}\}$, where $i = p^2+p-1$, $p-2 \ge j \ge 0$.

Now $\{C_{p^2+p-2,j+p^2}\}$ is known. We can proceed using the cusp $i\infty$.

(iv) Now repeat the following steps for $k = 1, 2, \dots, p-1$:

(a) $\{C_{ij}\}$, where $i = p^2 + p - 1 - k$, $j \leq p - 1 - k$. We use the q-expansion at $i\infty$.

(b) $\{C_{ij}\}$, where $i + j = 2p^2 + p - 2 - k$. We use the q-expansion at $-1/p$ and Lemma 6.

(c) $\{C_{ij}\}$, where $i = p^2 + p - 1 - k$, $0 \leq j \leq p - 2 - k$. We use the q-expansion at $i\infty$. This step is not there when $k = p - 1$.

(v) Now, for $\{C_{ij}\}$ with $0 \leq j \leq i \leq p^2 - 1$, we use the q-expansion at $i\infty$ as $\mathrm{ord}_{i\infty} F_{ij}$ all differ from each other.

5. An example. As mentioned in the introduction, $\Phi_4(X, J)$ has already been obtained by the algorithm of Theorem 2. We will compute $\Phi_9(X, J)$ which is of degree $\psi(9) = 12$ using Mathematica.

1. Using cusp $i\infty$, we have

$C_{11\ 11} = 0,$

$C_{11\ 10} = 0,$

$C_{11\ 9} = -1,$

$C_{11\ 8} = 6696,$

$C_{11\ 7} = -18155340,$

$C_{11\ 6} = 25558882848,$

$C_{11\ 5} = -19911358807902,$

$C_{11\ 4} = 8462621974879728,$

$C_{11\ 3} = -1807128632206069128,$

$C_{11\ 2} = 160958016085240175040.$

2. Using cusp $-1/3$, we have

$C_{10\ 10} = -1/2,$

$C_{10\ 9} = 15624.$

3. Using cusp $i\infty$ again, we have

$C_{11\ 1} = -3894864835363363281932,$

$C_{11\ 0} = 5567288717204029440000,$

$C_{10\ 8} = 28587961990122552,$

$C_{10\ 7} = 1029690595459616365730 88,$

$C_{10\ 6} = 116453208984017958681441584 04,$

$C_{10\ 5} = 1862048317782426516269385402765 60,$

$C_{10\ 4} = 680444811295518681180723971143182528,$

$C_{10\ 3} = 6554247305012036269515997976469117859 20,$

$C_{10\ 2} = 1557054176340129070242665015899136894464 66,$

$C_{10\ 1} = 638123189914701743031446707008730202112 0000.$

4. Using cusp $-1/3$, we have

$C_{9\ 9} = 14293980977975892.$

5. From now on, we only need to use $i\infty$.

$C_{10\ 0} = 103315678869024976287708798983570718720 00000,$

$C_{9\ 8} = 2058743107606285214213 76,$

$C_{9\ 7} = -16909630643312139881974226219181 0,$

$C_{9\ 6} = 1097815847178520649575574301039075207792,$

$C_{9\ 5} = -452102708759835815999184660653014461675230688,$

$C_{9\ 4} = 299389800957296742788373819083889098866668351168 00,$

$C_{9\ 3} = -52778283631612341869117096244707842911950881335795 2220,$

$C_{9\ 2} = 327326681021262948059545296305369431846439352393498624 0000,$

$C_{9\ 1} = -7900333936192849023918427261965278932265209355223171072000000,$

$C_{9\ 0} = 63909801475312950154933446165028703540750368581982617600000000000.$

We omit the rest. A detailed version is available upon request.

Finally, let us point out that, for $n = p^e$, $e \geq 3$, we need to use q-expansions of X and J at the cusps $\{i\infty, -(1/p), \ldots, -(1/p^{[e/2]})\}$, and the algorithm becomes much more complex.

Acknowledgment. The authors thank the referee for the valuable comments.

REFERENCES

1. S. Bae, *On the modular equation for Drinfeld modules of rank* 2, J. Number Theory **42** (1992), 123–133.

2. H. Cohn, *Introduction to the construction of class fields*, Cambridge University Press, Cambridge, 1985.

3. D. Cox, *Primes of the form* $X^2 + nY^2$, John Wiley & Sons, New York, 1989.

4. O. Herrmann, *Über die Berechnung der Fourierkoeffizienten der Funktion* $j(\tau)$, J. Reine Angew. Math. **274/275** (1975), 187–195.

5. E. Kaltofen and N. Yui, *On the modular equation of order* 11, in Proceedings Third MACSYMA User's Conference, General Electric, 1984, 472–485.

6. S. Lang, *Elliptic functions*, New York, 1973.

7. A. Schweizer, *On Drinfeld modular polynomial* $\Phi_T(X,Y)$, J. Number Theory **52** (1995), 53–68.

8. G. Shimura, *Introduction to arithmetic theory of automorphic functions*, Tokyo, 1971.

9. H. Weber, *Lehrbuch der Algebra*, Vol. III, 2nd ed., Braunschweig (1908), reprint by Chelsea, New York, 1961.

10. N. Yui, *Explicit form of modular equation*, J. Reine Angew. Math. **299–300** (1978), 185–200.

Department of Mathematics, Florida International University, University Park, Miami, Florida 33199
E-mail address: duttagus@fiu.edu

New York Life Insurance Company, 51 Madison Avenue, New York, NY 10010
E-mail address: xiaoties@hotmail.com