Honda, T.
Osaka J. Math.
9 (1972), 447-462

FORMAL GROUPS OBTAINED FROM GENERALIZED HYPERGEOMETRIC FUNCTIONS

TAIRA HONDA

(Received November 10, 1971)

An abelian variety defined over an algebraic number field K naturally yields a formal group of the same dimension over K, whose coefficients are integral at almost all primes of K. Let us see how this is obtained in case of dimension one. Let E be an elliptic curve, namely an abelian variety of dimension one, over K and $\omega(\neq 0)$ be a differential of the first kind on E. If an element x of $K(E)$ is a local parameter at the origin of E, ω has a power series expansion of the form $g_E(x)dx$, where $g_E(x)$ is an algebraic function in $K[[x]]$ with $g_E(0)\neq 0$. By replacing ω by its constant multiple if necessary, we may assume $g_E(0)=1$. Thus we can write $\omega=df_E(x)$ where $f'_E(x)=g_E(x)$ and $f_E(x)=x+\cdots\in K[[x]]$. Let $F_E(x, y)=f_E^{-1}(f_E(x)+f_E(y))$. Then the (commutative) formal group F_E is nothing other than the completion of the group law of E relative to the parameter x. To see it one has only to note that $df_E(x)$ is an invariant differential on the formal group F_E as is easily verified.

Now we ask if one can find non-algebraic formal groups (of dimension one) over K, whose coefficients are integral at almost all primes of K, by some analytic means. In that case we require that formal groups should be constructed globally and finitely. To do this one of the most natural ideas would be to replace an algebraic function $g_E(x)$ by a solution of a suitable algebraic differential equation with coefficients in $K[x]$. Since $g_E(x)$ is a solution of a linear algebraic differential equation of the first order under a suitable choice of x, we should primarily be concerned with linear equations. Moreover equations should be of Fuchsian type in view of a recent work [7] of Katz.

In this paper we study a formal group $F(x, y)$ whose invariant differential is $g(x)dx$ with a generalized hypergeometric function $g(x)$. Let $N\geqq 2$ be a natural number and S a subset of $\{1/N, 2/N, \cdots, (N-1)/N\}$. Put

$$\begin{cases} A_\theta(0) = 1 \\ A_\theta(n) = \theta(\theta+1)\cdots(\theta+n-1)/n! & \text{for } n\geqq 1 \end{cases}$$

and $A(n)=\prod_{\theta\in S} A_\theta(n)$. Let $g(x)=\sum_{n=0}^{\infty}A(n)x^{Nn}$, $f(x)=\int_0^x g(t)dt$ and $F(x, y)=f^{-1}(f(x)$

$+f(y)$). The power series F is a formal group over $\boldsymbol{Q}$. Our first aim is to study when F is integral at a prime p with $p>N$. Put

$$a(n)=\begin{cases}A((n-1)/N) & \text{if } (n-1)/N\in\boldsymbol{Z}\\ 0 & \text{otherwise.}\end{cases}$$

Then $f(x)=\sum_{n=1}^{\infty}\frac{a(n)}{n}x^n$. It turns out that whether F is p-integral or not depends only on the residue class of p mod N, and we get an explicit condition for p-integrality of F (Theorem 1 and Theorem 2). Let d be the smallest positive integer such that $p^d\equiv 1 \pmod N$ and put $q=p^d$. Then $\lim_{\nu\to\infty} a(q^\nu)/a(q^{\nu-1})$ has a limit ξ_p in $\boldsymbol{Z}_p$. Assume that F is p-integral. Then $\operatorname{ord}_p\xi_p\geqq d-1$. If $\operatorname{ord}_p\xi_p\geqq d$, F is of infinite height at p, namely isomorphic to the additive group over $\boldsymbol{Z}_p$. But if $\operatorname{ord}_p\xi_p=d-1$, F is of Lubin-Tate type as a formal group over $\boldsymbol{Z}_p$ and the q-th power endomorphism of its reduction $\tilde{F}$ is the image of q/ξ_p under the natural imbedding of $\boldsymbol{Z}_p$ into End $\tilde{F}$.

Now by examining the condition for p-integrality of F, one can prove that if the set $\{N\theta\,|\,\theta\in S\}$ contains all reduced residues mod N, then F is p-integral for every $p>N$(Theorem 3). For $N=3$, 4, 6, for example, we get formal groups over $Z[1/N]$ which are isomorphic to completions of elliptic curves over $\mathbf{Z}[1/N]$. But in most cases we get formal groups which are not isomorphic to completions of algebraic formal groups over rings of finite type over $\mathbf{Z}$. It would be an interesting problem to ask if our formal group can be simultaneously non-algebraic and of finite height at almost all p.

An important question is left behind: What is the p-adic integer ξ_p? In studying ξ_p we may assume S consists of a single number i/N. For $i=1$ it is not hard to see $\xi=(-1)^{(q-1)/N}$. For $2\leqq i\leqq N-1$ we can prove that ξ_p is one of the eigenvalues of the q-th power endomorphism of the Jacobian variety of the Fermat curve $x^N+y^N=1$ over GF(q), at least for almost all p. Hence ξ_p is some Jacobi sum by Davenport-Hasse [1] (at least for almost all p). We do not give the proof of this fact here, since it needs a detailed study of the completion of the Jacobian of the Fermat curve over $\boldsymbol{Z}_p$. The detailed account on ξ_p will be published elsewhere.

Our method in this paper is essentially elementary. In many cases the proof consists of a series of congruences modulo a power of p. Our basic congruences are those on binomial type numbers, in Lemma 1 of Dwork [2]. Of course the general theory of commutative formal groups is indispensable (cf. Honda [5]). A brief survey of our results in this paper appeared in [6].

1. Congruences on binomial type numbers

First we prove a number of congruences on binomial type numbers. Let p

be a fixed prime number. We shall use "mod p^ν" (resp. "mod$^\times p^\nu$") to denote an additive (resp. a multiplicative) congruence modulo p^ν. Let θ be a positive rational number integral at p. Put for each non-negative integer n

$$C_\theta(n) = \begin{cases} 1 & \text{for } n = 0 \\ \prod_{\nu=0}^{n-1}(\theta+\nu) & \text{for } n>0. \end{cases}$$

We define θ' to be that unique rational number, integral at p, such that $p\theta'-\theta$ is an ordinary integer in $[0, p-1]$, and $\theta^{(\lambda)}$ by induction: $\theta^{(\lambda+1)}=(\theta^{(\lambda)})'$. For each real x put

$$\rho(x) = \begin{cases} 0 & \text{if } x\leq 0 \\ 1 & \text{if } x>0. \end{cases}$$

Our basic lemma in this section is the following one due to Dwork [2].

Lemma 1. *If a, μ, s are non-negative ordinary integers, $0\leqq a<p$, then*

$$\frac{C_\theta(a+\mu p+mp^{s+1})}{C_{\theta'}(\mu+mp^s)} \equiv \frac{C_\theta(mp^{s+1})C_\theta(a+\mu p)}{C_{\theta'}(mp^s)\,C_{\theta'}(\mu)}\left(1+\frac{mp^s}{\theta'+\mu}\right)^{\rho(a+\theta-p\theta')} \quad \mathrm{mod}^\times p^{s+1}. \tag{1.1}$$

Furthermore

$$\frac{C_\theta(mp^{s+1})}{C_{\theta'}(mp^s)} \equiv ((-p)^{p^s}u_s)^m \quad \mathrm{mod}^\times p^{s+1} \tag{1.2}$$

where $u_s=+1$ unless both $p=2$, $s=1$, in which case $u_s=-1$. Finally

$$\mathrm{ord}_p \frac{C_\theta(a+\mu p)}{C_{\theta'}(\mu)} = \mu+(1+\mathrm{ord}_p(\mu+\theta'))\rho(a+\theta-p\theta'). \tag{1.3}$$

Proof. See [2, p. 31].

Let $N\geqq 2$ be a natural number and S a non-empty subset of $\{i/N \mid 1\leqq i\leqq N-1\}$. From now on we assume that the fixed prime number p is (strictly) larger than N. We define $S'=\{\theta' \mid \theta\in S\}$ and $S^{(\lambda)}$ by induction: $S^{(\lambda+1)}=(S^{(\lambda)})'$. Put

$$A(n) = \prod_{\theta\in S}(C_\theta(n)/n!) = \prod_{\theta\in S}(C_\theta(n)/C_1(n)) \qquad \text{for } n\geqq 0$$

and for $n\geqq 1$

$$a(n) = \begin{cases} A((n-1)/N) & \text{if } (n-1)/N\in \boldsymbol{Z} \\ 0 & \text{otherwise.} \end{cases}$$

By replacing S by $S^{(\lambda)}$ we define $A^{(\lambda)}(n)$, $a^{(\lambda)}(n)$ similarly.

Applying Lemma 1 to $A(n)$, we get

Lemma 2. *Let a, μ, s be as in Lemma 1. Then*

$$\frac{A(a+\mu p+mp^{s+1})}{A'(\mu+mp^s)} \equiv \frac{A(a+\mu p)}{A'(\mu)} \prod_{\theta\in S}\left(1+\frac{mp^s}{\theta'+\mu}\right)^{\rho(a+\theta-p\theta')} \bmod^{\times} p^{s+1}. \tag{1.4}$$

Moreover

$$\mathrm{ord}_p A(a+\mu p)/A'(\mu) = \sum_{\theta\in S}(1+\mathrm{ord}_p(\mu+\theta'))\rho(a+\theta-p\theta'). \tag{1.5}$$

Proof. If $\theta=1$, then $\theta'=1$ and $\rho(a+\theta-p\theta')=0$. Furthermore the right side of (1.2) is independent of θ. Hence our lemma follows from Lemma 1 and the definition of $A(n)$.

For a rational number r whose denominator is prime to N we denote by $(r)_N$ the least non-negative integer congruent to r mod N. Let d be the smallest positive integer such that $(p^d)_N=1$ and put $q=p^d$.

Lemma 3. *Let m, l be positive ordinary integers such that $m\equiv l \pmod N$ and $(m, N)=1$. Let α be an ordinary integer in $[0, d-1]$ and put $k=(mp^{\alpha})_N$ and $h=(mp^{\alpha-1})_N$. Then we have for $\nu d+\alpha\geqq 1$*[1]

$$\frac{a(mp^{\nu d+\alpha}-k+1)}{a'(mp^{\nu d+\alpha-1}-h+1)} \equiv \frac{a(lp^{\nu d+\alpha}-k+1)}{a'(lp^{\nu d+\alpha-1}-h+1)}(1+Cp^{\nu d+\alpha-1}) \bmod^{\times} p^{\nu d+\alpha}, \tag{1.6}$$

where C is a rational number integral at p. We may take $C=0$ if $h=1$.

Proof. It suffices to consider the case S consists of a single number $\theta=i/N$. Furthermore we may assume $l=(m)_N$. Put $\theta'=j/N$ and $m=nN+l$ $(1\leqq l\leqq N-1)$. Since

$$(mp^{\nu d+\alpha}-k)/N = np^{\nu d+\alpha}+((lp^{\nu d+\alpha-1}-h)/N)\cdot p+(hp-k)/N$$

and

$$\rho((hp-k)/N+i/N-ip/N) = \rho(h-j),$$

we get by Lemma 2

$$\frac{A((mp^{\nu d+\alpha}-k)/N)}{A'(np^{\nu d+\alpha-1}+(lp^{\nu d+\alpha-1}-h)/N)} \equiv \frac{A((lp^{\nu d+\alpha}-k)/N)}{A'((lp^{\nu d+\alpha-1}-h)/N} \tag{1.7}$$

1) This lemma does not hold for $\nu d+\alpha=1$ since we may not assume $l=(m)_N$ in this case. (The author thanks to the referee for pointing out this fact.) But it always holds if $l=(m)_N$, and this is sufficient to obtain the subsequent lemmas. For example Lemma 4 is true since it is proved for $l=(m)_N$.

$$\times\left(1+\frac{Np^{\nu d+\alpha-1}}{lp^{\nu d+\alpha-1}-h+j}\right)^{\rho(h-j)} \qquad \bmod^{\times} p^{\nu d+\alpha}.$$

Suppose first that $\nu d+\alpha=1$. Because $\alpha=1$ or $d=1$ in this case, $m\equiv h \pmod N$ and hence $l=h$. Therefore $lp^{\nu d+\alpha-1}-h+j=i$ is a p-unit. If $\nu d+\alpha\geqq 1$, then

$$lp^{\nu d+\alpha-1}-h+j\equiv j-h \qquad \bmod p.$$

Since $0\leqq|j-h|<N<p$, $\operatorname{ord}_p(j-h)>0$ if and only if $j=h$, in which case $\rho(h-j)=0$. Summing up, $lp^{\nu d+\alpha-1}-h+j$ is a p-unit unless $\rho(h-j)=0$. Finally $\rho(h-j)=0$ if $h=1$. Now our lemma is proved by rewriting (1.7) into a congruence on the $a(s)$ and $a'(s)$.

Lemma 4. *Let $0\leqq\alpha\leqq d-1$ and $\nu\geqq 1$: let m, l be positive ordinary integers such that*

$$mp^{\alpha}\equiv lp^{\alpha}\equiv 1 \qquad (\bmod N).$$

Then

$$\frac{a(mp^{\nu d+\alpha})}{a(mp^{(\nu-1)d+\alpha})}\equiv\frac{a(lp^{\nu d+\alpha})}{a(lp^{(\nu-1)d+\alpha})} \qquad \bmod^{\times} p^{(\nu-1)d+\alpha+1}. \tag{1.8}$$

Proof. Put $k_\beta=(mp^{\alpha-\beta})_N$. It follows from Lemma 3

$$\begin{aligned}\frac{a^{(\beta)}(mp^{\nu d+\alpha-\beta}-k_\beta+1)}{a^{(\beta+1)}(mp^{\nu d+\alpha-\beta-1}-k_{\beta+1}+1)}&\equiv\frac{a^{(\beta)}(lp^{\nu d+\alpha-\beta}-k_\beta+1)}{a^{(\beta+1)}(lp^{\nu d+\alpha-\beta-1}-k_{\beta+1}+1)}\\ &\times(1+C_\beta p^{\nu d+\alpha-\beta-1}) \qquad \bmod^{\times} p^{\nu d+\alpha-\beta}\end{aligned} \tag{1.9}$$

for $0\leqq\beta\leqq d-1$, where the C_β are p-integral. Since $k_d=(mp^{\alpha-d})_N=1$, we may assume $C_{d-1}=0$. Then our lemma immediately follows from d congruences (1.9) noting $a^{(d)}(n)=a(n)$.

Put $\alpha=0$, $m=q$ and $l=1$ in (1.8). Then we get

$$\frac{a(q^{\nu+1})}{a(q^{\nu})}\equiv\frac{a(q^{\nu})}{a(q^{\nu-1})} \qquad \bmod^{\times} pq^{\nu-1}. \tag{1.10}$$

Therefore $a(q^{\nu})/a(q^{\nu-1})$ has a limit in $\mathbf{Z}_p$ as $\nu\to\infty$. We denote it by ξ_p.

From now on we shall write ord n instead of $\operatorname{ord}_p n$ for the sake of simplicity.

Lemma 5. *Let m, α and ν be as in Lemma 4. Then*

$$\operatorname{ord} a(mp^{\nu d+\alpha}) = \nu \operatorname{ord} a(q)+\operatorname{ord} a(mp^{\alpha}). \tag{1.11}$$

In particular

$$\text{ord } a(q^\nu) = \nu \text{ ord } a(q). \tag{1.12}$$

Proof. From Lemma 4 follows

$$\frac{a(mp^{\nu d+\alpha})}{a(mp^{(\nu-1)d+\alpha})} \equiv \frac{a(q^{\nu+1})}{a(q^\nu)} \qquad \bmod^\times p^{(\nu-1)d+\alpha+1}$$

and

$$\begin{aligned}\frac{a(q^\nu)}{a(q^{\nu-1})} \equiv \cdots \equiv \frac{a(q)}{a(1)} \qquad & \bmod^\times p \\ = a(q).\end{aligned}$$

Our lemma is an immediate consequence of these congruences.

Lemma 6. *Let m, α be as in Lemma 4. Put $m_\alpha = (p^{-\alpha})_N$. Then*

$$\text{ord } a(mp^{\nu d+\alpha}) \geqq \text{ord } a(m_\alpha p^{\nu d+\alpha}) \qquad \textit{for } \nu \geqq 0. \tag{1.13}$$

Proof. In view of Lemma 5 we may assume $\nu = 0$. By Lemma 3 we get by working $\bmod^\times p$

$$\begin{aligned}\frac{a(mp^\alpha)}{a(m_\alpha p^\alpha)} &\equiv \frac{a'(mp^{\alpha-1} - m_1 + 1)}{a'(m_\alpha p^{\alpha-1} - m_1 + 1)} \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ &\equiv \frac{a^{(\alpha)}(m - m_\alpha + 1)}{a^{(\alpha)}(m_\alpha - m_\alpha + 1)}(1+C) = a^{(\alpha)}(m - m_\alpha + 1)(1+C),\end{aligned}$$

which proves our lemma.

Lemma 7. *Assume $d \geqq 2$. Then*

$$\text{ord } \frac{a(m_\alpha p^{\alpha-\lambda} - m_\lambda + 1)}{a'(m_\alpha p^{\alpha-\lambda-1} - m_{\lambda+1} + 1)} = \sum_{\theta \in S} \rho(m_{\lambda+1} - N\theta') \tag{1.14}$$

for $1 \leqq \alpha \leqq d-1$ and $0 \leqq \lambda \leqq \alpha - 1$.

Proof. Since

$$(m_\alpha p^{\alpha-\lambda} - m_\lambda)/N = (m_\alpha p^{\alpha-\lambda-1} - m_{\lambda+1})p/N + (m_{\lambda+1}p - m_\lambda)/N,$$

Lemma 2 shows

$$\begin{aligned}&\text{ord } \frac{a(m_\alpha p^{\alpha-\lambda} - m_\lambda + 1)}{a'(m_\alpha p^{\alpha-\lambda-1} - m_{\lambda+1} + 1)} = \text{ord } \frac{A((m_\alpha p^{\alpha-\lambda} - m_\lambda)/N)}{A'((m_\alpha p^{\alpha-\lambda-1} - m_{\lambda+1})/N)} \\ &= \sum_{\theta \in S} \{1 + \text{ord}((m_\alpha p^{\alpha-\lambda-1} - m_{\lambda+1})/N + \theta'\} \rho((m_{\lambda+1}p - m_\lambda)/N + \theta - p\theta').\end{aligned}$$

Because

$$(m_{\lambda+1}p-m_\lambda)/N+\theta-p\theta'>0$$

is equivalent to

$$m_{\lambda+1}-N\theta'>0,$$

it suffices to prove that $m_{\lambda+1}>N\theta'$ implies ord $(\mu+\theta')=0$ where $\mu=(m_\alpha p^{\alpha-\lambda-1}-m_{\lambda+1})/N$. Let $\theta=i/N$ and $\theta'=j/N$. For $\lambda=\alpha-1$ we have

$$\text{ord}\,(\mu+\theta') = \text{ord}\,(m_\alpha-m_\alpha+j) = \text{ord}\,j = 0.$$

But for $\lambda>\alpha-1$ we have

$$\text{ord}\,(\mu+\theta') = \text{ord}\,(-m_{\lambda+1}+i) = 0,$$

as $0<m_{\lambda+1}-j<N<p$. This completes our proof.

2. Construction of formal groups from generalized hypergeometric functions

We use the same notations as in **1**. Define

$$g(x) = \sum_{n=0}^{\infty} A(n)x^{Nn}. \tag{2.1}$$

This is a generalized hypergeometric function satisfying the linear algebraic differential equation

$$(x^N \prod_{\theta\in S}(\delta+N\theta)-\delta^{|S|})y = 0, \tag{2.2}$$

and is the unique solution up to constant, holomorphic at the origin, where $\delta=x(d/dx)$ and $|S|$ means the cardinal of the set S. It is well known that the equation (2.2) is of Fuchsian type, namely all its singular points are regular. Now define

$$f(x) = \int_0^x g(t)dt = \sum_{n=1}^{\infty} a(n)x^n/n \tag{2.3}$$

$$F(x, y) = f^{-1}(f(x)+f(y)).$$

Then $F(x, y)$ is considered a formal group over $\mathbf{Q}$ with the canonical invariant differential $g(x)dx$ (cf. [4]). It is well known that the coefficients of $g(x)$ are integral at each prime not dividing N. But, at what prime is F integral?

Theorem 1. *All coefficients of F are p-integral for $p>N$, if and only if*

$$\text{ord}\,a(m_\alpha p^\alpha)\geqq\alpha \qquad \textit{for } 0\leqq\alpha\leqq d-1. \tag{2.4}$$

Assume (2.4) *holds. Then* ord $a(q)\geqq d-1$. *If* ord $a(q)\geqq d$, *F is isomorphic to the*

additive group over $\mathbf{Z}_p$. *If* ord $a(q)=d-1$, *F is of Lubin-Tate type as formal group over* $\mathbf{Z}_p$ (cf. [8]). *F is of height d and attached to the prime element q/ξ_p of* $\mathbf{Z}_p$.

Proof. We use the terminology and results of our previous paper [5]. First assume F is p-integral. Then, regarded as power series in $\mathbf{Q}_p[[x]]$, $f(x)$ is killed by some special element $u=p+\sum_{\nu=1}^{\infty} c_\nu T^\nu$ of $\boldsymbol{Z}_p[[T]]$:

$$pf(x)+\sum_{\nu=1}^{\infty} c_\nu f(x^{p^\nu}) \equiv 0 \mod p. \tag{2.5}$$

We will show that we may assume $c_1=\cdots=c_{d-1}=0$ (if $d\geqq 2$) by replacing u by another special element, (left) associate to it if necessary. Suppose $c_1=\cdots=c_{i-1}=0$ and $c_i\neq 0$ for some $i\leqq d-1$. Comparing the coefficients of x^{p^i} on the both sides of (2.5), we see ord $c_i>0$. Therefore the i-th degree coefficient of u is killed by multiplying u by $(1-c_i/p)T^i$. This proves our claim by induction. Putting $c_1=\cdots=c_{d-1}=0$ in (2.5), we see for $0\leqq\alpha\leqq d-1$

$$pa(m_\alpha p^\alpha)/(m_\alpha p^\alpha) \equiv 0 \mod p,$$

namely

$$\text{ord } a(m_\alpha p^\alpha) \geqq \alpha.$$

Conversely, assume that (2.4) is satisfied. It follows from Lemma 6

$$\text{ord } a(q)\geqq \text{ord } a(m_{d-1}p^{d-1})\geqq d-1.$$

First we consider the case ord $a(q)\geqq d$. Then, by Lemma 5 and Lemma 6,

$$\begin{aligned}\text{ord } a(mp^{\nu d+\alpha}) &\geqq \text{ord } a(m_\alpha p^{\nu d+\alpha})\\ &= \nu \text{ ord } a(q)+\text{ord } a(m_\alpha p^\alpha)\\ &\geqq \nu d+\alpha\end{aligned}$$

for $p\nmid m$, $0\leqq\alpha\leqq d-1$ and $\nu\geqq 0$. Therefore all coefficients of $f(x)$ are already p-integral and F is isomorphic to the additive group $x+y$ in this case.

Now, suppose ord $a(q)=d-1$. Then ord $\xi_p=d-1$ by (1.10) and $\pi_p=q/\xi_p$ is a prime element of $\mathbf{Z}_p$. We will prove

$$\pi_p f(x) \equiv f(x^q) \mod p, \tag{2.6}$$

namely that f is killed by the special element π_p-T^d. Write an arbitrary positive integer, congruent to 1 mod N, in the form $mp^{\nu d+\alpha}$ where $p\nmid m$, $mp^\alpha\equiv 1$ (mod N), $\nu\geqq 0$ and $0\leqq\alpha\leqq d-1$. The coefficients of x^{mp^α} on the both sides of (2.6) are certainly congruent mod p, because

$$\pi_P\, a(m_\alpha p^\alpha)/(m_\alpha p^\alpha) \equiv 0 \qquad \mod p$$

by (2.4) and a fortiori

$$\pi_p\, a(mp^\alpha)/(mp^\alpha) \equiv 0 \qquad \mod p$$

by Lemma 6. We must still prove

$$\pi_p \frac{a(mp^{(\nu+1)d+\alpha})}{mp^{(\nu+1)d+\alpha}} \equiv \frac{a(mp^{\nu d+\alpha})}{mp^{\nu d+\alpha}} \qquad \mod p,$$

which is equivalent to

$$a(mp^\alpha q^{\nu+1}) \equiv \xi_p\, a(mp^\alpha q^\nu) \qquad \mod p^\alpha q^{\nu+1}. \tag{2.7}$$

Now we get by Lemma 4

$$\frac{a(mp^\alpha q^{\nu+1})}{a(mp^\alpha q^\nu)} \equiv \frac{a(q^{\nu+2})}{a(q^{\nu+1})} \equiv \xi_p \qquad \mod^\times p^{\alpha+1} q^\nu,$$

namely

$$a(mp^\alpha q^{\nu+1}) \equiv \xi_p\, a(mp^\alpha q^\nu) \qquad \mod^\times p^{\alpha+1} q^\nu. \tag{2.8}$$

Since ord $a(mp^\alpha q^{\nu+1}) \geqq (\nu+1)$ ord $a(q)+$ord $a(m_\alpha p^\alpha)$

$$\geqq (\nu+1)(d-1)+\alpha$$

by Lemma 5 and Lemma 6, (2.8) implies

$$a(mp^\alpha q^{\nu+1}) \equiv \xi_p\, a(mp^\alpha q^\nu) \qquad \mod p^\mu \tag{2.9}$$

where $\mu = \nu d+\alpha+1+(\nu+1)(d-1)+\alpha$. But

$$\mu - \{(\nu+1)d+\alpha\} = \nu(d-1)+\alpha \geqq 0.$$

Therefore the desired congruence (2.7) follows from (2.9). This completes the proof of (2.6), from which follow the other assertions of our theorem (cf. [5, § 5.3]).

We now study conditions for p-integrality of F more in detail.

Theorem 2. *If $d \geqq 2$ and $0 \leqq \alpha \leqq d-1$, then*

$$\text{ord } a(m_\alpha p^\alpha) = \sum_{\theta \in S} \sum_{\lambda=1}^{\alpha} \rho(m_\lambda - N\theta^{(\lambda)}). \tag{2.10}$$

Proof. It follows from Lemma 7

$$\text{ord } \frac{a^{(\lambda)}(m_\alpha p^{\alpha-\lambda} - m_\lambda + 1)}{a^{(\lambda+1)}(m_\alpha p^{\alpha-\lambda-1} - m_{\lambda+1} + 1)} = \sum_{\theta \in S} \rho(m_{\lambda+1} - N\theta^{(\lambda+1)}) \tag{2.11}$$

for $0 \leqq \lambda \leqq \alpha - 1$. Our theorem is an easy consequence of (2.11).

Consequently, given the set S and the residue class of p mod N, we can easily determine whether F is p-integral or not. It is clear that, if F is p-integral and $S \subset S_1 \subset \{1/N, \cdots, (N-1)/N\}$, the group F_1 obtained from S_1 is also p-integral.

As an application of Theorem 2 we have:

Theorem 3. *If the set* $\{N\theta \mid \theta \in S\}$ *contains all reduced residues* mod N, F *is* p*-integral for every* $p > N$.

Proof. By Theorem 1 F is p-integral if $d=1$, i.e., $p \equiv 1 \pmod{N}$. Assume $d \geqq 2$. Then, for each λ, $1 \leqq \lambda \leqq d-1$, at least one of $\theta^{(\lambda)}$ is equal to $1/N$ if the assumption of our theorem is satisfied. Moreover $m_\lambda > 1$ for $1 \leqq \lambda \leqq d-1$. Consequently

$$\sum_{\theta \in S} \rho(m_\lambda - N\theta^{(\lambda)}) \geqq 1 \qquad \text{for } 1 \leqq \lambda \leqq d-1.$$

Our theorem follows from this, Theorem 1 and Theorem 2.

3. Examples and remarks

In this section we first study ξ_p for $S = \{1/N\}$. To do that we consider any prime number p with $p \nmid N$. Fix such a prime p and let q, d be as before. Given a map $s \mapsto b(s)$ of $\mathbf{Z}$ into $\mathbf{Z}_p - \{0\}$, we denote by $\prod_{s=m}^{n}{}' b(s)$ the product of all the $b(s)$ such that $m \leqq s \leqq n$ and $q \nmid b(s)$. Furthermore, denote by $n?$ the product $\prod_{s=1}^{n}{}'s$. We see easily

$$n! = q^m \cdot m! \cdot n? \tag{3.1}$$

where $m = [n/q]$. Put $n_\nu = (q^\nu - 1)/N$ for $\nu \geqq 0$.

Lemma 8. *Put* $\theta = i/N$ *for* $1 \leqq i \leqq N$. *Then*

$$C_\theta(n_\nu)/C_\theta(n_{\nu-1}) = q^{n_{\nu-1}} \prod_{s=0}^{n_\nu - 1}{}' (\theta + s).$$

Proof. We defined

$$C_\theta(n_\nu) = \prod_{s=0}^{n_\nu - 1} (\theta + s).$$

If $q \mid \theta + s$, $(i + Ns)/q$ is an integer congruent to i mod N. Therefore $i/N + s = q(i/N + t)$ with $t \in \boldsymbol{Z}$. As $0 \leqq s \leqq n_\nu - 1$, we have

$$-i(q-1)/(Nq) \leqq t \leqq (q^{\nu}-1-N-i(q-1))/(Nq). \tag{3.2}$$

Now since

$$-1 < i(q-1)/(Nq) < 0,$$
$$(q^{\nu}-1-N-i(q-1))/(Nq) = n_{\nu-1} - ((i-1)(q-1)+N)/(Nq)$$

and

$$1-((i-1)(q-1)+N)/(Nq) = (N+1-i)(q-1)/(Nq) > 0,$$

the range of t is $[0, n_{\nu-1}-1]$. This completes our proof.

Theorem 4. *For $S=\{1/N\}$ and $p \nmid N$ we have*

$$\lim_{\nu\to\infty} a(q^{\nu})/a(q^{\nu-1}) = \begin{cases} (-1)^{(q-1)/N} & \text{if } p \neq 2 \\ 1 & \text{if } p = 2. \end{cases} \tag{3.3}$$

Proof. If p is odd, then for $\nu \geqq 1$

$$n_{\nu} - n_{\nu-1} \equiv (q-1)/N \mod 2.$$

But if $p=2$, $n_{\nu}-n_{\nu-1}$ is even for $\nu \geqq 2$. Hence it suffices to prove for $\nu \geqq 1$

$$n_{\nu}!/n_{\nu-1}! \equiv (-1)^{n_{\nu}-n_{\nu-1}} C_{\theta}(n_{\nu})/C_{\theta}(n_{\nu-1}) \mod^{\times} pq^{\nu-1} \tag{3.4}$$

with $\theta = 1/N$. By Lemma 8, (3.4) is equivalent to

$$n_{\nu}? \equiv (-1)^{n_{\nu}-n_{\nu-1}} \prod_{s=0}^{n_{\nu}-1}{}' (\theta+s) \mod^{\times} pq^{\nu-1}. \tag{3.5}$$

Now

$$n_{\nu}? = \prod_{s=1}^{n_{\nu}}{}' s = \prod_{s=0}^{n_{\nu}-1}{}' (n_{\nu}-s)$$

and for $q \nmid n_{\nu}-s$ we get

$$\begin{aligned} n_{\nu}-s &= (q^{\nu}-1)/N - s \\ &\equiv -(\theta+s) \mod^{\times} pq^{\nu-1}. \end{aligned}$$

This proves (3.5) and completes our proof.

Returning to cases of general S, we will look into formal groups F for smaller values of N.

$N=2$. Only $S=\{1/2\}$ is possible. We see

$$g(x) = (1-x^2)^{-1/2}, f(x) = \sin^{-1}x.$$

The group F is nothing other than the expansion of the addition formula of sin x into power series. Since $\xi_p=(-1/p)$ for $p\neq 2$, F is isomorphic, over $\boldsymbol{Z}[1/2]$, to the formal group obtained from the Dirichlet L-function $\sum_{n=1}^{\infty}(-4/n)n^{-s}$(Honda [4]). Hence F is isomorphic to a group of multiplicative type over $\mathbf{Z}[1/2]$. (This fact is also verified by a simple transformation of the differential $g(x)dx$.)

$N=3$. By Theorem 3 and Theorem 4 the group F is integral at each $p>3$ if and only if $S=\{2/3\}$ or $S=\{1/3,\ 2/3\}$. Moreover formal groups obtained from these two sets are isomorphic over $\mathbf{Z}[1/6]$ by our theorems and the general theory [5], because $(-1)^{(q-1)/3}=1$ for $p>3$. Take $S=\{2/3\}$. Then $g(x)dx=(1-x^3)^{-2/3}dx$ is a differential of the first kind on the elliptic curve $x^3+y^3=1$ and x is a local papameter at each zero of x. Hence F is an algebraic formal group. As π_p is an eigenvalue of the q-th power endomorphism of the reduction mod p of this curve, so is $\xi_p=q/\pi_p$. The explicit value of ξ_p is well known (Davenport-Hasse [1]). The reduction of F mod p is of height 1 (resp. 2) if $p\equiv 1$ (resp. -1) mod 3.

$N=4$. The group F is integral at each $p>4$ if and only if S contains 2/4 or 3/4, as is seen from Theorem 1 and Theorem 2. For $S=\{2/4\}$, $g(x)dx=(1-x^4)^{-1/2}dx$ is a differential of the first kind on the elliptic curve $C_1: x^4+y^2=1$ and x is a local parameter at each zero of x. Hence F is an algebraic group and the explicit value of ξ_p is well known ([1]). Next, take $S=\{3/4\}$. The differential $g(x)dx=(1-x^4)^{-3/4}dx$ is of the first kind on the curve $x^4+y^4=1$. Put $X=y/x$ and $Y=x^{-2}$. Then $(X,\ Y)$ defines the curve $C_2: Y^2=X^4+1$. Since

$$-2x^{-3}dx = dY,\ x^3dx = -y^3dy,$$
$$YdY = 2X^3dX,$$

one has

$$g(x)dx = y^{-3}dx = -(1/2)(x/y)^3dY = -dY/(2X^3)$$
$$= (-1/2)(dX/Y).$$

Working on the curve C_2, we can take x as a local parameter at the pole of Y. (Although x is not in the function field of C_2, it can be used to get a formal model of C_2 over $\mathbf{Z}[1/2]$.) Thus F is a formal model of an algebraic group (over a ring of finite type over $\mathbf{Z}$) in this case, too. The values of ξ_p differ by a class character from those obtained from $S=\{2/4\}$. In either case the reduction of F mod p is of height 1 (resp. 2) if $p\equiv 1$ (resp. -1) mod 4. The structure of F for other S can easily be determined from what we have said.

$N=6$. By Theorem 1 and Theorem 2 it is easily verified that F is integral at each $p>6$ if and only if S contains at least one of $\{i/6\,|\,2\leqq i\leqq 5\}$. We will show that for each $S=\{i/N\}$ $(2\leqq i\leqq 5)$ F is a formal model, over $\mathbf{Z}[1/6]$, of an

elliptic curve with invariant 0 and defined over $\mathbf{Q}$. This fact might be proved by suitable transformations of the differentials $g(x)dx$, but we will do it mainly by proving a number of congruences.

For $S=\{i/6\}$ we write $a_i(n)$ for $a(n)$ and $\xi_{i,p}$ for ξ_p. From Lemma 8 it follows for $p>6$, $\nu\geqq 1$

$$\begin{aligned} a_3(q^\nu)/a_3(q^{\nu-1}) &= C_\theta(n_\nu)/C_\theta(n_{\nu-1})\cdot n_{\nu-1}!/n_\nu! \\ &= (n_\nu?)^{-1}\prod_{s=0}^{n_\nu-1}{}'(3/6+s) \\ &= (n_\nu?)^{-1}\prod_{s=0}^{n_\nu-1}{}'(1/2+n_\nu-s-1). \end{aligned}$$

Here, if $q\nmid 1/2+n_\nu-s-1$, then

$$\begin{aligned} 1/2+n_\nu-s-1 &\equiv 1/2-1/6-s-1 \qquad \bmod^{\times} pq^{\nu-1} \\ &\equiv -(s+2/3). \end{aligned}$$

Consequently we get

$$a_3(q^\nu)/a_3(q^{\nu-1}) \equiv (-1)^{n_\nu-n_{\nu-1}}\, a_4(q^\nu)/a_4(q^{\nu-1}) \qquad \bmod^{\times} pq^{\nu-1}, \tag{3.6}$$

where $n_\nu-n_{\nu-1}$ may be replaced by$(q-1)/6$ or $(q-1)/2$. By the same argument we obtain

$$a_2(q^\nu)/a_2(q^{\nu-1}) \equiv (-1)^{(q-1)/2}\, a_5(q^\nu)/a_5(q^{\nu-1}) \qquad \bmod^{\times} pq^{\nu-1}, \tag{3.7}$$

noting

$$2/6-1/6-1 = -5/6.$$

Since (3.6) and (3.7) implies

$$\xi_{3,p} = (-1)^{(q-1)/2}\xi_{4,p}, \qquad \xi_{2,p} = (-1)^{(q-1)/2}\xi_{5,p}, \tag{3.8}$$

we have only to study $\xi_{3,p}$ and $\xi_{5,p}$.

On $\xi_{3,p}$. Let C_3 be the elliptic curve defined by $Y^2=X^3-1$. We can take x with $X=x^{-2}$ as a local parameter at infinity to get a formal model of C_3 over $\mathbf{Z}[1/6]$. Then $g(x)dx=(1-x^6)^{-1/2}dx$ is the x-expansion of a differential of the first kind on C_3 and F is a formal model of C_3 over $\mathbf{Z}[1/6]$.

On $\xi_{5,p}$. By Theorem 4 it suffices to consider ξ_p for $S=\{1/6, 5/6\}$. For this S an easy computation shows

$$a(q^\nu) = \frac{(6n_\nu)!}{2^{4n_\nu}3^{3n_\nu}n_\nu!(2n_\nu)!(3n_\nu)!}. \tag{3.9}$$

Consider the elliptic curve C_4 defined by $Y^2=X^3+4$. Taking a local parameter

t with $X=t^{-2}$ at the infinity of C_4, a formal model G of C_4 over $\mathbf{Z}[1/6]$ is obtained from the differential $(1+4t^6)^{-1/2}dt$. Write

$$(1+4t^6)^{-1/2}dt = \sum_{n=1}^{\infty} b(n)t^{n-1}dt.$$

We will show that F is isomorphic to G over $\mathbf{Z}[1/6]$. (Our results in **1** and **2** can be applied also to $p=5$. More generally they are applicable to $p=N-1$ if it is a prime. In fact, if $p=N-1$, $0\leqq|j-h|\leqq N-2<p$ in the proof of Lemma 3 and $0<m_{\lambda+1}-j\leqq N-2<p$ in that of Lemma 7.) Since both F and G are of Lubin-Tate type at $p\neq 2,3$, we have only to prove that the reductions of both formal groups mod p have the same q-th power endomorphism as p-adic integer (cf. [5]). By Theorem 1 this will follow from the congruence

$$a(q^\nu)/a(q^{\nu-1}) \equiv b(q^\nu)/b(q^{\nu-1}) \qquad \mathrm{mod}^{\times} pq^{\nu-1}. \tag{3.10}$$

Since

$$b(q^\nu) = (-1)^{n_\nu}(2n_\nu)!/(n_\nu!)^2$$

as is easily verified, (3.10) is reduced to

$$\begin{aligned}(-2^4\cdot 3^3)^{n_\nu-n_{\nu-1}}\{(2n_\nu)?\}^2(3n_\nu)? \\ \equiv n_\nu?(6n_\nu)? \qquad \mathrm{mod}^{\times} pq^{\nu-1}\end{aligned} \tag{3.11}$$

by Lemma 8. Furthermore, because

$$\begin{aligned}(6n_\nu)? &= (3n_\nu)?\prod_{s=0}^{3n_\nu-1}{}' (6n_\nu-s) \\ &\equiv (3n_\nu)?\prod_{s=0}^{3n_\nu-1}{}' (-1-s) \qquad \mathrm{mod}^{\times} pq^{\nu-1} \\ &= (-1)^{n_\nu-n_{\nu-1}}\{(3n_\nu)?\}^2,\end{aligned}$$

the congruence (3.11) is equivalent to

$$(2^4\cdot 3^3)^{n_\nu-n_{\nu-1}}\{(2n_\nu)?\}^2 \equiv n_\nu?(3n_\nu)? \qquad \mathrm{mod}^{\times} pq^{\nu-1}. \tag{3.12}$$

Here we will show

$$3^{3(n_\nu-n_{\nu-1})} \equiv (-1)^{n_\nu-n_{\nu-1}} \qquad \mathrm{mod}^{\times} pq^{\nu-1}. \tag{3.13}$$

For $d=1$, i.e. $q=p$ this follows from

$$\begin{aligned}(-3)^{3(n_\nu-n_{\nu-1})} &\equiv \left(\frac{-3}{p}\right) \qquad \mathrm{mod}\ q^\nu \\ &= 1.\end{aligned}$$

But for $d=2$, i,e. $q=p^2$ we have

$$3(n_\nu - n_{\nu-1}) = (q^\nu - q^{\nu-1})/2 = p^{2\nu-2}(p^2-1)/2$$
$$\equiv 0 \qquad \mod p^{2\nu-2}(p-1).$$

Therefore for any a with $p \nmid a$ it holds

$$a^{3(n_\nu - n_{\nu-1})} \equiv 1 \qquad \mod p^{2\nu-1}(= pq^{\nu-1}).$$

This proves (3.13), by which (3.12) is reduced to

$$2^{2(n_\nu - n_{\nu-1})} n_\nu ?\ (3n_\nu)? \tag{3.14}$$
$$\equiv (-1)^{n_\nu - n_{\nu-1}}\{(2n_\nu)^2\}?\ \qquad \mod^{\times} pq^{\nu-1}.$$

Now we have

$$(-2)^{n_\nu - n_{\nu-1}}(3n_\nu)? = (-2)^{n_\nu - n_{\nu-1}}(2n_\nu)? \prod_{s=2n_\nu+1}^{3n_\nu}{}' s \tag{3.15}$$
$$\equiv (2n_\nu)? \prod_{s=2n_\nu+1}^{3n_\nu}{}' (q^\nu - 2s) \qquad \mod^{\times} pq^{\nu-1}.$$

As s runs through $[2n_\nu+1, 3n_\nu]$, $q^\nu - 2s$ runs through all odd integers in $[1, (q^\nu - 4)/3]$. Consequently

$$\prod_{s=2n_\nu+1}^{3n_\nu}{}' (q^\nu - 2s) = 2^{-(n_\nu - n_{\nu-1})}(2n_\lambda)?/n_\lambda ?. \tag{3.16}$$

Now (3.14) is an immediate consequence of (3.15) and (3.16). Thus (3.10) is proved and the structure of F is determined.

The structure of F for other S can be determined from the above results by Theorem 1 and Theorem 2.

In all the above cases $N=2,3,4,6$ we can verify that F is simultaneously integral and of finite height at almost all primes, only if F is a formal model of an algebraic group over a ring of finite type over $\mathbf{Z}$.

What happens for $N=5$ or $N \geqq 7$? We have $\phi(N) \geqq 4$ for these N. I have verified for $N=5$ and $7 \leqq N \leqq 12$ that F is not integral at infinitely many p, if S consists of a single element. The same fact would probably hold for $N \geqq 13$. If so, S should have at least two elements other than $1/N$ for $\phi(N) \geqq 4$, in order that F is integral at almost all p. But in that case F is of infinite height at p with $p \equiv -1 \pmod N$, because

$$\operatorname{ord} a(m_1 p) = \operatorname{ord} a((N-1)p)$$
$$= \sum_{\theta \in S} \rho(N-1-N\theta') \geqq 2 = d$$

by Theorem 2. Thus we have arrived at the following conjecture:

(C) *Let F be a formal group constructed in* **2**. *If F is integral and of finite height at almost all p, F is a formal model of some algebraic group over a ring of*

finite type over **Z**.

More generally let K be a finite algebraic number field and $h'(x)=1+\cdots\in K[[x]]$ a solution of an algebraic differential equation with coefficients in $K[x]$. Let $H(x, y)$ be the formal group over K, with the canonical invariant differential $h'(x)\,dx$. Is H a formal model, over a ring of finite type over **Z**, of an algebraic group over K, if H is integral and of finite height at almost all primes of K ? This question extends to higher dimensional cases in an appropriate way by replacing the notion of "a group of finite height" by "a p-divisible group" (cf. Tate [9]). If our question has an affirmative answer, it will yield an interesting characterization of algebraic functions. But if there were counter-examples, they would certainly be of great interest. We could define their zeta functions with Euler products and these zeta functions would be quite new beings (cf. [5, p. 245]).

OSAKA UNIVERSITY

References

[1] H. Davenport and H. Hasse: *Die Nullstellen der Kongruenzzetafunktionen im gewissen zyklischen Fällen,* J. Reine Angew. Math. **172** (1935), 151–182.

[2] B. Dwork: *p-adic cycles,* Inst. Hautes Études Sci. Publ. Math. **37** (1969), 28–115.

[3] H. Hasse: *Zetafunktion und L-Funktionen zu einem arithmetischen Funktionenkörper vom Fermatschen Typus,* Abh. Deutsch. Akad. Wiss. Berlin Kl. Math.-Natur., 1955, 1–70.

[4] T. Honda: *Formal groups and zeta-functions,* Osaka J. Math. **5** (1968), 199–213.

[5] T. Honda: *On the theory of commutative formal groups,* J. Math. Soc. Japan **22** (1970), 213–246.

[6] T. Honda: *Differential equations and formal groups,* The Japan-U.S. Seminar on Modern Methods in Number Theory, Tokyo, 1971.

[7] N.M. Katz: *Nilpotent connections and the monodromy theorem: Applications of a result of Turrittin,* Inst. Hautes Études Sci. Publ. Math. **39** (1970), 175–232.

[8] J. Lubin and J. Tate: *Formal complex multiplication in local fields,* Ann. of Math. **81** (1965), 380–387.

[9] J. Tate: *p-divisible groups,* Proceedings of a Conference on Local Fields, Driebergen, 1966, 157–183.