ACTA ARITHMETICA
LXII.2 (1992)

On formal groups obtained from symmetric powers

by

MINATSU YAMAJI (Tokyo)

1. Preliminaries. In [3], Honda proved that for any elliptic curve C over $\mathbb{Q}$, a formal completion $\widehat{C}$ of C is isomorphic over $\mathbb{Z}$ to a formal group whose invariant differential has the same coefficients as the zeta-function of C, and his result was generalized to abelian varieties over $\mathbb{Q}$ with real multiplication by Deninger and Nart in [1]. In this paper, we classify formal groups which are obtained from some L-series associated with symmetric powers.

Let p be a rational prime and let a_p be a rational integer. Let $\mathbb{Q}_p$ and $\mathbb{Z}_p$ denote the field of p-adic numbers and the ring of p-adic integers, respectively. Consider an equation

(a) $$X^2 - a_p X + p^{k-1} = 0\,,$$

where $k \in \mathbb{N}$ and $k \geq 2$. Let α_p, β_p be roots of the equation (a) in $\overline{\mathbb{Q}}_p$. Let $m \in \mathbb{N}$ and consider a local Dirichlet series:

$$L_p^{(m)}(s) = \frac{1}{(1-\alpha_p^m p^{-s})(1-\alpha_p^{m-1}\beta_p p^{-s})\ldots(1-\alpha_p\beta_p^{m-1}p^{-s})(1-\beta_p^m p^{-s})}.$$

Expanding it out, we have

$$L_p^{(m)}(s) = \frac{1}{1 + c_p p^{-s} + p c_{p^2} p^{-2s} + \ldots + p^m c_{p^{m+1}} p^{-(m+1)s}}\,.$$

LEMMA 1. *For any* ν, $1 \leq \nu \leq m+1$, $c_{p^\nu} \in \mathbb{Z}$.

Proof. This can be shown by easy calculations. ■

Now we put together all local Dirichlet series, and define the global Dirichlet series:

$$L^{(m)}(s) = \prod_p L_p^{(m)}(s) = \prod_p (1 + c_p p^{-s} + \ldots + p^m c_{p^{m+1}} p^{-(m+1)s})^{-1}\,,$$

where p runs over all rational primes. Put

$$L^{(m)}(s) = \sum_{n=1}^{\infty} A_n n^{-s}\,.$$

Then $A_n \in \mathbb{Z}$, and $A_{nn'} = A_n A_{n'} = A_{n'} A_n$ if $(n, n') = 1$.

This L-series is very important in number theory and algebraic geometry (cf. [5]). So it is interesting and meaningful to consider formal groups obtained from this L-series. Put

$$f^{(m)}(x) = \sum_{n=1}^{\infty} n^{-1} A_n x^n \quad \text{and} \quad F^{(m)}(x,y) = {f^{(m)}}^{-1}(f^{(m)}(x) + f^{(m)}(y))\,.$$

Then by Theorem 8 in [4], $F^{(m)}(x,y)$ is a formal group over $\mathbb{Z}$. For a rational prime p, let $F^{(m)*}(x,y)$ denote the reduction of $F^{(m)}(x,y)$ modulo p. For $b \in \mathbb{Z}_p$, let $[b]_{F^{(m)}}(x) = {f^{(m)}}^{-1}(bf^{(m)}(x))$. Then $[b]_{F^{(m)}}(x) \in \mathbb{Z}_p[[x]]$ and let $[b]^*_{F^{(m)}}$ denote the reduction of $[b]_{F^{(m)}}$ modulo p (cf. [2]). We use ord_p for the p-adic valuation of $\mathbb{Z}_p$ normalized by $\mathrm{ord}_p(p) = 1$. Then we have the following lemma.

Lemma 2. *Let $(a_p, p) > 1$ and $\nu \in \mathbb{N}$.*

(1) *For $k = 2$, we have*

$$\mathrm{ord}_p(\alpha_p^\nu + \beta_p^\nu) \geq \begin{cases} \nu/2 & \text{if } \nu \text{ is even,} \\ (\nu+1)/2 & \text{if } \nu \text{ is odd.} \end{cases}$$

(2) *For $k > 2$, we have*

$$\mathrm{ord}_p(\alpha_p^\nu + \beta_p^\nu) \geq \nu\,.$$

Proof. This is proved by induction on ν, using the identity

$$\alpha_p^\nu + \beta_p^\nu = (\alpha_p + \beta_p)(\alpha_p^{\nu-1} + \beta_p^{\nu-1}) - \alpha_p\beta_p(\alpha_p^{\nu-2} + \beta_p^{\nu-2})\,. \ \blacksquare$$

2. The case of $(a_p, p) > 1$. Let p be a rational prime, and let $a_p \in \mathbb{Z}$ such that $p \mid a_p$. Let $\alpha_p, \beta_p, L_p^{(m)}(s)$, $f^{(m)}(x)$, $F^{(m)}(x,y)$ and $F^{(m)*}(x,y)$ be as in Section 1. If $m = 1$ and $k = 2$, $f^{(1)}$ is of type $u = p + c_p T + T^2$ by Theorem 8 in [4]. Hence $F^{(1)*}$ has height 2 by Proposition 3.5 in [4]. In fact, it is associated with the elliptic curve which has Hasse invariant 0 (cf. [6]). In other cases, we have the following results.

Proposition 1. *If $m = 1$ and $k \geq 3$, or $m \geq 2$ and $k \geq 2$, then $F^{(m)*}$ has infinite height.*

Proof. We only need to show that for $\nu \ge 1$, $A_{p^\nu} \equiv 0 \pmod{p^\nu}$. We have

$$\begin{aligned} A_{p^\nu} &= \sum_{k_1+k_2+\ldots+k_{m+1}=\nu} (\alpha_p^m)^{k_1}(\alpha_p^{m-1}\beta_p)^{k_2}\ldots(\alpha_p\beta_p^{m-1})^{k_m}(\beta_p^m)^{k_{m+1}} \\ &\equiv \sum_{\substack{i=1 \\ k_1+k_{m+1}=i}}^{\nu} \Big((\alpha_p^m)^{k_1}(\beta_p^m)^{k_{m+1}} \\ &\qquad \times \Big(\sum_{k_2+\ldots+k_m=\nu-i} (\alpha_p^{m-1}\beta_p)^{k_2}\ldots(\alpha_p\beta_p^{m-1})^{k_m}\Big)\Big) \pmod{p^\nu}. \end{aligned}$$

If i is even,

$$\begin{aligned} &\mathrm{ord}_p\Big(\sum_{k_1+k_{m+1}=i} (\alpha_p^m)^{k_1}(\beta_p^m)^{k_{m+1}}\Big) \\ &\quad = \mathrm{ord}_p((\alpha_p^m)^i + (\beta_p^m)^i + (\alpha_p^m)^{i-1}\beta_p^m + \alpha_p^m(\beta_p^m)^{i-1} + \ldots + (\alpha_p^m\beta_p^m)^{i/2}) \\ &\quad \ge \min\{\mathrm{ord}_p((\alpha_p^m)^i + (\beta_p^m)^i), \mathrm{ord}_p((\alpha_p^m)^{i-1}\beta_p^m + \alpha_p^m(\beta_p^m)^{i-1}), \\ &\qquad\qquad \ldots, \mathrm{ord}_p((\alpha_p^m\beta_p^m)^{i/2})\} \\ &\quad \ge i \quad \text{by Lemma 2.} \end{aligned}$$

If i is odd,

$$\begin{aligned} &\mathrm{ord}_p\Big(\sum_{k_1+k_{m+1}=i} (\alpha_p^m)^{k_1}(\beta_p^m)^{k_{m+1}}\Big) \\ &\quad = \mathrm{ord}_p((\alpha_p^m)^i + (\beta_p^m)^i + (\alpha_p^m)^{i-1}\beta_p^m + \alpha_p^m(\beta_p^m)^{i-1} + \ldots \\ &\qquad\qquad + (\alpha_p^m)^{(i-1)/2}(\beta_p^m)^{(i+1)/2} + (\alpha_p^m)^{(i+1)/2}(\beta_p^m)^{(i-1)/2}) \\ &\quad \ge \min\{\mathrm{ord}_p((\alpha_p^m)^i + (\beta_p^m)^i), \mathrm{ord}_p((\alpha_p^m)^{i-1}\beta_p^m + \alpha_p^m(\beta_p^m)^{i-1}), \ldots \\ &\qquad\qquad \ldots, \mathrm{ord}_p((\alpha_p^m)^{(i-1)/2}(\beta_p^m)^{(i+1)/2} + (\alpha_p^m)^{(i+1)/2}(\beta_p^m)^{(i-1)/2})\} \\ &\quad \ge i \quad \text{by Lemma 2.} \end{aligned}$$

On the other hand,

$$\mathrm{ord}_p\Big(\sum_{k_2+\ldots+k_m=\nu-i} (\alpha_p^{m-1}\beta_p)^{k_2}\ldots(\alpha_p\beta_p^{m-1})^{k_m}\Big) \ge \nu - i\,.$$

So we have $\mathrm{ord}_p(A_{p^\nu}) \ge \nu$. Hence $A_{p^\nu} \equiv 0 \pmod{p^\nu}$. ∎

3. The case of $(a_p, p) = 1$. Let a_p be a rational integer such that $p \nmid a_p$. If $m = 1$ and $k = 2$, we know that $F^{(1)*}$ has height 1 by Lemma 6 in [3]. It is associated with the elliptic curve which has Hasse invariant 1 (cf. [6]). If $m = 1$ and $k \ge 3$, then in the same way as in Lemma 6 of [3], we have $\mathrm{ht}(F^{(1)*}) = 1$. More generally, we get the height of $F^{(m)*}$ by direct calculations.

Proposition 2. *$F^{(m)*}$ has always height* 1.

Proof. We have

$$\begin{aligned} A_p &= \alpha_p^m + \alpha_p^{m-1}\beta_p + \ldots + \alpha_p\beta_p^{m-1} + \beta_p^m \\ &\equiv \alpha_p^m + \beta_p^m \pmod p \equiv a_p^m \pmod p \not\equiv 0 \pmod p . \ \blacksquare \end{aligned}$$

Since $(a_p, p) = 1$, by Hensel's lemma, α_p and β_p are elements in $\mathbb{Z}_p$. Let α_p be the unit solution and let β_p be p^{k-1}/α_p.

In general, let R be a commutative ring with identity and let F and G be formal groups over R. A formal power series $\varphi(x) = a_1x + \ldots \in R[[x]]$ is a *homomorphism* of F to G if $\varphi(F(x,y)) = G(\varphi(x), \varphi(y))$ and $a_1 \neq 0$. If a_1 is a unit in R, the inverse power series φ^{-1} is a homomorphism of G to F. In this case, we say that G is *weakly isomorphic* to F, denoted by $F \sim G$. In particular, if $a_1 = 1$, we say that G is *strongly isomorphic* to F, denoted by $F \approx G$.

Proposition 3. *The following assertions hold*:

(1) $\left[\dfrac{p}{\alpha_p^m}\right]^*_{F^{(m)}}(x) = x^p$.

(2) $F^{(m)} \approx F^{(m')}$ *over* $\mathbb{Z}$ *if* $\alpha_p = 1$ *or* $\alpha_p = -1$ *and* $m \equiv m' \pmod 2$. *Otherwise*, $F^{(m)} \not\sim F^{(m')}$ *over* $\mathbb{Z}$.

Proof. (1) Let π be the prime element such that $[\pi]^*_{F^{(m)}}(x) = x^p$. By Corollary 2 of Theorem 8 in [4], we have

$$[p]^*_{F^{(m)}} + \sum_{\nu=1}^{m+1} [c_{p^\nu}]^*_{F^{(m)}} [\pi]^{*\nu}_{F^{(m)}} = 0 \,,$$

that is, $[p + c_p\pi + c_{p^2}\pi^2 + \ldots + c_{p^{m+1}}\pi^{m+1}]^*_{F^{(m)}} = 0$. Since the map $*$ is bijective, $p + c_p\pi + c_{p^2}\pi^2 + \ldots + c_{p^{m+1}}\pi^{m+1} = 0$. Put $g(x) = p + c_px + c_{p^2}x^2 + \ldots + c_{p^{m+1}}x^{m+1}$. Then π is one of the solutions of $g(x)$. Also, p/α_p^m is a solution of $g(x)$. But, since $g(x) \equiv x(c_p + c_{p^2}x + \ldots + c_{p^{m+1}}x^m) \pmod p$ and $c_p \not\equiv 0 \pmod p$, there is only one solution of $g(x)$ which is divisible by p. Hence $\pi = p/\alpha_p^m$.

(2) Since $\mathrm{ht}(F^{(m)*}) = 1$, by Corollary of Theorem 2 in [3], $p/\alpha_p^m = p/\alpha_p^{m'}$, that is, $\alpha_p = 1$ or $\alpha_p = -1$ and $m \equiv m' \pmod 2$ if and only if $F^{(m)}$ and $F^{(m')}$ are strongly isomorphic to each other. By Proposition 3.5 in [4], weak isomorphisms are strong isomorphisms in this case. $\blacksquare$

It would be nicer to give the geometrical interpretation of these formal groups $F^{(m)}(x,y)$, but it seems difficult for the time being.

Acknowledgement. The author would like to express her thanks to Professor K. Katayama for turning her attention to this problem and Professor N. Yui for her useful advice.

References

[1] C. Deninger and E. Nart, *Formal groups and L-series*, Comment. Math. Helv. 65 (1990), 318–333.

[2] A. Fröhlich, *Formal Groups*, Lecture Notes in Math. 74, Springer, 1968.

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

[4] —, *On the theory of commutative formal groups*, J. Math. Soc. Japan 22 (2) (1970), 213–246.

[5] J. P. Serre, *Abelian l-Adic Representations and Elliptic Curves*, W. A. Benjamin, 1968.

[6] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Math. 106, Springer, 1986.

DEPARTMENT OF MATHEMATICS
TSUDA COLLEGE
KODAIRA, TOKYO 187
JAPAN

Received on 8.10.1991
and in revised form on 17.4.1992 (2180)