Formal groups and some arithmetic properties of elliptic curves

Noriko Yui

1. Introduction.

Let E be an elliptic curve, i.e, an abelian variety of dimension 1, defined over a field K. E has a plane cubic model given by a Weierstrass equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.1}$$

where $a_i \in K$ for all i and x, y are affine coordinates.

Let $\mathfrak{D}_1$ denote the K-vector space of all differential 1-forms of the first kind on E. $\mathfrak{D}_1$ has dimension 1 over K and its canonical basis is given by

$$\omega_0 = \frac{dx}{2y+a_1x+a_3}. \tag{1.2}$$

We call ω_0 the canonical invariant differential on E.

Let $u = -\frac{x}{y}$ be a local parameter of E near the point at infinity $(0,1,0)$ of E. Put $w = -\frac{1}{y}$. Then we can express the Weierstrass equation for E in (u,w)-coordinate as

$$w = u^3 + a_1uw + a_2u^2w + a_3w^2 + a_4uw^2 + a_6w^3. \tag{1.3}$$

Substitute w recursively in the right hand side of (1.3). We obtain the formal power series expansion for E in u. In the same fashion, ω_0 can be expressed as a formal power series in u as

$$\begin{aligned}\omega_0 &= du\{1 + a_1u + (a_1^2+a_2)u^2 + (a_1^3+2a_1a_2+2a_3)u^3 \\ &\quad + (a_1^4+3a_1^2a_2+6a_1a_3+a_2^2+2a_4)u^4 + \cdots\} \\ &= \sum_{n=1}^{\infty} a(n)u^{n-1}du\end{aligned} \tag{1.4}$$

where $a(1) = 1$ and $a(n) \in \mathbb{Z}[a_1,a_2,a_3,a_4,a_6]$ for all n.

When the characteristic of K is different from 2 or 3, E

can be defined by the equation of the form

(1.1') $$y^2 = x^3 + ax + b$$

where $a, b \in K$ and the cubic $x^3 + ax + b$ has distinct roots. In this case, the canonical invariant differential ω_0 on E is given by

(1.2') $$\omega_0 = \frac{dx}{2y}.$$

E is defined in (u,w)-plane by the equation

(1.3') $$w = u^3 + auw + bw^3,$$

and ω_0 has the formal power series expansion in u as follows.

(1.4') $$\omega_0 = \frac{dx}{2y} = \frac{dx/du}{2y}du = (-\frac{1}{2} + \frac{u}{2w}\frac{dw}{du})$$
$$= du\{1 + 2au^4 + 3bu^6 + 6a^2u^8 + 20abu^{10} + \cdots\}$$
$$= \sum_{n=1}^{\infty} a(n)u^{n-1}du. \quad \text{(See Yui [15].)}$$

The objects of our discussion in this talk are the coefficients $a(n)$ of the canonical invariant differential ω_0 on E. These coefficients provide us with subtle arithmetic information on elliptic curves, e.g, the Hasse invariant, the liftability of the Frobenius morphism, the Atkin and Swinnerton-Dyer congruences and so on. In the present lecture, we shall review the papers [15]-[16].

The theory of (commutative 1-dimensional) formal groups is extensively used as a tool in the investigation of arithmetic properties of elliptic curves. So here is the appropriate place and time to recall the definitions and some basic properties of (commutative 1-dimensional) formal groups, which we need in the succeeding discussions. For a thorough discussion of (commutative 1-dimensional) formal groups, see Fröhlich [5].

Let R be a commutative ring with the identity 1. We denote by $R[[x_1,\ldots,x_n]]$ the ring of formal power series in the variables $x_1,\ldots,x_n$. For f and g in $R[[x_1,\ldots,x_n]]$, we write $f \equiv g \pmod{\deg r}$ if $f - g$ contains no monomials of total degree less than r.

(1.5) Definition. A (commutative 1-dimensional) formal group over R is a formal power series $\Phi(x,y)$ over R in two variables x, y satisfying the following axioms:

(1) $\Phi(x,y) \equiv x + y \pmod{\deg 2}$,

(2) $\Phi(\Phi(x,y),z) = \Phi(x,\Phi(y,z))$,

(3) $\Phi(x,y) = \Phi(y,x)$.

(In this paper, we discuss only commutative 1-dimensional formal groups, so we simply use the terminology formal groups to mean those commutative 1-dimensional ones.)

If Φ and Ψ are formal groups over R, an R-homomorphism of Φ to Ψ is a formal power series $\lambda(x) \in R[[x]]$ without constant term satisfying $\lambda(\Phi(x,y)) = \Psi(\lambda(x), \lambda(y))$. Such a λ is called an R-isomorphism if $\lambda(x) \equiv x \pmod{\deg 2}$. If there is an R-isomorphism of Φ to Ψ, Φ and Ψ are said to be isomorphic over R, or simply R-isomorphic. The set $\mathrm{Hom}_R(\Phi,\Psi)$ of all R-homomorphisms of Φ to Ψ forms an abelian group under the addition $(\lambda_1+\lambda_2)(x) = \Psi(\lambda_1(x), \lambda_2(x))$ for $\lambda_1, \lambda_2 \in \mathrm{Hom}_R(\Phi,\Psi)$. In particular, $\mathrm{End}_R(\Phi) = \mathrm{Hom}_R(\Phi,\Phi)$ is a ring. We denote by $[n]_\Phi \in \mathrm{End}_R(\Phi)$ the image of $n \in \mathbb{Z}$ under the natural embedding $\mathbb{Z} \to \mathrm{End}_R(\Phi)$. In characteristic $p > 0$, $[p]_\Phi$ has the form

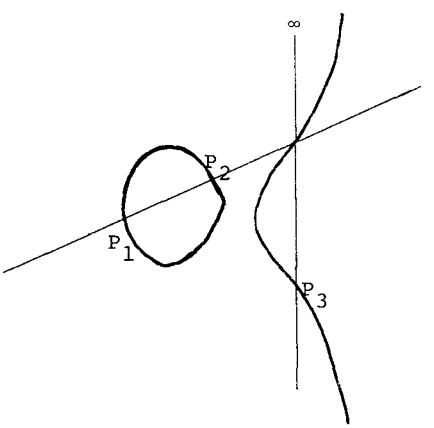
$$[p]_\Phi(x) = c_1 x^{p^h} + c_2 x^{p^{2h}} + \cdots .$$

(See Lazard [10] and Lubin [11].)

If $c_1 \neq 0$, the height of Φ is defined to be the integer h in this expression. If $[p]_\Phi = 0$, Φ is said to have infinite height. We denote by h or $\mathrm{ht}(\Phi)$ the height of Φ.

2. Formal groups of elliptic curves.

Let E be an elliptic curve over a field K defined by the Weierstrass equation (1.1). Let $E(K)$ be the set of all K-rational points on E and of the point at infinity $(0,1,0)$. It is a well known result that $E(K)$ forms an abelian group under the group law :



$P_1 + P_2 =: P_3$

with the point at infinity as its identity (zero). As we get formal power series expansions for E and ω_0 in the local parameter u, we can expand the group law of E into a formal power series in u. Let $P_i = (u_i, w_i)$, $i = 1,2,3$ be K-rational points on E such that $P_3 = P_1 + P_2$. Then we have

$$\begin{aligned} u_3 &= \Gamma(u_1,u_2) \\ &= u_1 + u_2 - a_1u_1u_2 - a_2(u_1^2u_2+u_1u_2^2) - 2a_3(u_1^3u_2+u_1u_2^3) \\ &\quad + (a_1a_2-3a_3)u_1^2u_2^2 + \cdots \in \mathbb{Z}[a_1,a_2,a_3,a_4,a_6][[u_1,u_2]]. \end{aligned}$$

This Γ is the formal group (law on one parameter) of E. (See Tate [14].)

If the characteristic of K is different from 2 or 3, E can be defined by an equation of the form (1.1') and the formal group Γ of E is explicitly given by the formal power series as

$$\begin{aligned} \Gamma(u_1,u_2) &= u_1 + u_2 - 2au_1u_2 - 4a(u_1^3u_2^2+u_1^2u_2^3) \\ &\quad - 16b(u_1^3u_2^4+u_1^4u_2^3) - 9b(u_1^5u_2^2+u_1^2u_2^5) + \cdots \\ &\quad \in \mathbb{Z}[a,b][[u_1,u_2]]. \quad \text{(See Yui [15].)} \end{aligned}$$

Let $m > 1$ be a rational integer. Then the rational map "multiplication by m" : $x \to mx$ (x a generic point) of E into itself is an isogeny of degree m^2 (see Cassels [3] or Lang [9]) and the endomorphism $[m]_\Gamma$:multiplication by m on Γ, is given recursively by

$$[1]_\Gamma(x) = x, \quad [m]_\Gamma(x) = \Gamma(x,[m-1]_\Gamma(x)).$$

(2.1) Proposition. (Honda [7].) Let E be an elliptic curve over a field K and $\omega_0 = \sum_{n=1}^{\infty} a(n)u^{n-1}du$ the canonical invariant differential on E. Put $f(u) = \sum_{n=1}^{\infty} \frac{a(n)}{n}u^n$ and define $\Gamma(u,v)$ by $\Gamma(u,v) = f^{-1}(f(u)+f(v))$. Then Γ is the formal group of E and $[p]_\Gamma(u) = f^{-1}(pf(u))$. (In this case, $f(u)$ is called the logarithm of Γ.) ∎

3. Elliptic curves and formal groups over fields of finite characteristic.

Let K be a field of characteristic $p > 0$ and let $\bar{K}$ be the algebraic closure of K. Let E, u, ω_0 and Γ be as above. We know that $p : E \to E$ is an isogeny of degree p^2 and $[p]_\Gamma : \Gamma \to \Gamma$ has the form

$$[p]_\Gamma(u) = c_1 u^{p^h} + c_2 u^{p^{2h}} + \cdots \quad \text{with} \quad c_1 \neq 0. \tag{3.1}$$

(3.2) Theorem. The formal group Γ of E has height $h = 1$ or 2. Moreover, we have the following assertions.

(1) $h = 1 \iff E$ has p points of order p in $\bar{K}$.

(2) $h = 2 \iff E$ has no points of order p in $\bar{K}$.

Proof. We know that the isogeny $p : E \to E$, which has degree p^2, is not separable (as $p = \text{char.}(K)$). p^h in the expression (3.1) gives the inseparable degree of this isogeny. So p^h must divide p^2 and hence we get $h = 1$ or 2. For the second assertions, let ${}_pE(\bar{K})$ denote the group of rational points on E of order p defined over $\bar{K}$. Then we know that the order of ${}_pE(\bar{K})$ is equal to the separable degree of the isogeny $p : E \to E$. Hence the order of ${}_pE(\bar{K})$ is given by p^{2-h}, from which the assertions (1) and (2) follow immediately. QED

(3.3) Proposition. Let $\omega_0 = \sum_{n=1}^{\infty} a(n) u^{n-1} du$ be the canonical invariant differential on E. Then we have

(1) $a(p) \neq 0$ in $K \iff h = 1 \overset{\text{defn}}{\iff} E$ is ordinary.

(2) $a(p) = 0$ in $K \iff h = 2 \overset{\text{defn}}{\iff} E$ is supersingular.

Proof. By Proposition (2.1), we know that $[p]_\Gamma(u) = f^{-1}(pf(u))$ with $f(u) = \sum_{n=1}^{\infty} \frac{a(n)}{n} u^n$. On the other hand, we also have the expression (3.1). So by comparing the coefficients of u^p of both equations, we get

$$a(p) = c_1 \quad \text{in} \quad K.$$

Hence the assertions (1) and (2) follow. QED

Now we consider the differential 1-forms on E. We denote by $K(E) = K(x,y)$ the function field of E over K and by $\Omega^1(K(E))$

the K-vector space of all differential 1-forms on E over k. Then every element ω of $\Omega^1(K(E))$ can be expressed uniquely in the form

$$\omega = d\phi + \eta^p x^{p-1}\,dx, \qquad \phi,\ \eta \in K(E) \tag{3.4}$$

(once the p-variable x is fixed).

(3.5) Definition. (Cf. Cartier [1].) The Cartier operator

$$C : \Omega^1(K(E)) \longrightarrow \Omega^1(K(E))$$

is defined for ω of (3.4) by letting

$$C(\omega) = \eta\,dx.$$

C is well defined independently of the choice of p-variable x. C is a p^{-1}-linear operator, that is,

$$C(\phi^p\,\omega_1 + \psi^p\,\omega_2) = \phi C(\omega_1) + \psi C(\omega_2)$$

for $\phi,\ \psi \in K(E)$ and $\omega_1,\ \omega_2 \in \Omega^1(K(E))$.
For an arbitrary $\phi \in K(E)$, we have

$$C(\phi^{n-1}\,d\phi) = \begin{cases} d\phi & \text{if } n = p, \\ 0 & \text{if } (n,p) = 1. \end{cases}$$

$\omega \in \Omega^1(K(E))$ is said to be logarithmic $\iff C(\omega) = \omega \iff \omega = \dfrac{d\phi}{\phi}$ with some $\phi \in K(E)$. $\omega \in \Omega^1(K(E))$ is said to be exact $\iff C(\omega) = 0 \iff \omega = d\phi$ with some $\phi \in K(E)$.

Now we apply the Cartier operator C to the canonical invariant differential ω_0 on the elliptic curve E of the form (1.1). The result is the following

(3.6) Theorem. The image of ω_0 under the Cartier operator C is given by

$$C(\omega_0) = A^{1/p}\,\omega_0$$

where C is represented by the element $A^{1/p}$ in K and A is explicitly given by the following value :

$$A = \begin{cases} a_1 & \text{if } p = 2, \\ a_1^2 + a_2 & \text{if } p = 3, \\ \displaystyle\sum_{2i+3j=\frac{p-1}{2}} \frac{(\frac{p-1}{2})!}{i!j!(\frac{p-1}{2}-i-j)!} a^i b^j 4^{\frac{p-1}{2}-i-j} & \text{if } p \geq 5 \end{cases}$$

where $a = \dfrac{-(a_1^2+4a_2)^2}{12} + 4a_4 + 2a_1a_3$

and $b = \dfrac{(a_1^2+4a_2)^3}{216} - \dfrac{(a_1^2+4a_2)(a_1a_3+2a_4)}{6} + a_3^2 + 4a_6$.

Proof. To apply the Cartier operator ζ on ω_0, we put ω_0 into the following form .

$$\omega_0 = \frac{dx}{2y+a_1x+a_3} = \frac{1}{(2y+a_1x+a_3)^p}(2y+a_1x+a_3)^{p-1}dx.$$

Then it suffices to compute the coefficient A of x^{p-1} in $(2y+a_1x+a_3)^{p-1}$, because all other terms give exact differentials. We have immediately that $A = a_1$ for $p = 2$, $a_1^2+a_2$ for $p = 3$. For $p \geq 5$, we replace x and y by

$$X = x + \frac{a_1^2+4a_2}{12}, \quad Y = 2y+a_1x+a_3.$$

Then E can be defined by the equation of the form

$$Y^2 = 4X^3 + aX + b$$

where a and b are as in the statement of the theorem. Then the coefficient A of $x^{p-1}(= X^{p-1})$ in $Y^{p-1} = (4X^3+aX+b)^{\frac{p-1}{2}}$ is given by the Deuring formula as above. (Cf. Deuring [4].) QED

(3.7) Definition. The value A obtained in Theorem (3.6) is called the Hasse invariant of E.

(3.8) Theorem. Let A be the Hasse invariant of E. Put $H = \{ \alpha \in K \mid A\alpha^p = 0 \}$ and $G = \{ \alpha \in K \mid A\alpha^p = \alpha \}$. Then H is a K-vector space and G generates a K-vector space $< G >$. Moreover, we have the following assertions:

(1) $\mathfrak{D}_1 \simeq H\omega_0 \iff A = 0 \iff$ every $\omega \in \mathfrak{D}_1$ is exact.

(2) $\mathfrak{D}_1 \simeq <G>\omega_0 \iff A \neq 0 \iff$ every $\omega \in \mathfrak{D}_1$ is logarithmic.

Proof. The first assertions are clear. To prove the second assertions, we recall that $\mathfrak{D}_1$ is a K-vector space of dimension 1 with the canonical basis ω_0. So every element $\omega \in \mathfrak{D}_1$ can be written as $\omega = \alpha\omega_0$ with $\alpha \in K$. Now $H\omega_0$ and $<G>\omega_0$ are K-vector subspaces of $\mathfrak{D}_1$, so it follows that they are either $\{0\}$ or $\mathfrak{D}_1$ itself. Hence we get what we claimed. QED

4. Elliptic curves and formal groups over $\mathfrak{p}$-adic integer rings.

In this section, let us assume that K is a field complete with respect to a rank-one valuation v (additively written) which is the extension of the p-adic valuation ord_p of $\mathbb{Q}_p$ normalized so that $v(p) = 1$. Let R be the ring of intgers in K with maximal ideal $\mathfrak{p}$ and with the residue field k of characteristic $p > 0$.

Let E be an elliptic curve defined over K. Then there exists the Weierstrass minimal model of the form (1.1) for E with $a_i \in R$ for every i and with the discriminant of minimal order. So we can define $E^* = :E \bmod \mathfrak{p}$ by the equation obtained from (1.1) by replacing a_i by $a_i^* = :a_i \bmod \mathfrak{p}$ for every i. If E^* is also an elliptic curve over k, we say that E has <u>good reduction at</u> $\mathfrak{p}$. If E^* no longer defines an elliptic curve over k, E is said to have <u>bad reduction at</u> $\mathfrak{p}$. $\omega_0^* = \sum_{n=1}^{\infty} a(n)^* u^{n-1} du$ where $a(n)^* = :a(n) \bmod \mathfrak{p}$ is the canonical invariant differential on the elliptic curve E^* over k. Let Γ be the formal group of E. We denote by Γ^* the formal group of E^*, which is defined by $\Gamma^* = :\Gamma \bmod \mathfrak{p}$ over k. If E has good reduction at $\mathfrak{p}$, Γ^* has height $h = 1$ or 2 by (3.2). If E has bad reduction at $\mathfrak{p}$, i.e, E^* has a singularity, we have the following possibilities. If the singularity is a cusp, the group law of E^* is given by a usual addition of point coordinates. Hence $\Gamma^*(u,v) = u + v$, the additive (formal) group, and $h = \infty$. If the singularity is an ordinary double point with tangent rational over k (resp. with tangent not defined over k), the group law of E^* is given by multiplication of point coordinates. So $\Gamma^*(u,v) = u + v - uv$ (resp. $u + v + uv$, the multiplicative (formal) group). Hence in both cases, $h = 1$ because

$$[p]_{\Gamma^*}(u) = (1 \mp u)^p - 1 \equiv \mp u^p \pmod{\mathfrak{p}}.$$

(4.1) Proposition. With E, Γ, u and $\omega_0 = \sum_{n=1}^{\infty} a(n)u^{n-1}du$ as above, let

$$[p]_\Gamma(u) = pug_0(u) + \sum_{i=1}^{h-1} b(p^i)u^{p^i}g_i(u) + b(p^h)u^{p^h}g_h(u)$$

where $v(b(p^i)) > 0$ for each $1 \le i \le h-1$, $v(b(p^h)) = 0$ and $g_0(u)$, $g_i(u)$, $1 \le i \le h-1$ are units in $R[[u]]$ and $g_h(u) \in R[[u]]$, be the endomorphism multiplication by p on Γ. Assume that E has good reduction at $\mathfrak{p}$. Let $\omega_0^* = \sum_{n=1}^{\infty} a(n)^* u^{n-1}du$ be the canonical invariant differential on $E^* = E \bmod \mathfrak{p}$ and let $A^* = :A \bmod \mathfrak{p}$ be the Hasse invariant of E^*, where A is the value given in Theorem (3.6) with $a_i \in R$ for all i. Then we have the congruence:

$$a(p) \equiv b(p) \equiv A \pmod{\mathfrak{p}}.$$

Proof. We know that

$$[p]_\Gamma(u) = f^{-1}(pf(u)) \in R[[u]] \quad \text{with} \quad f(u) = \sum_{n=1}^{\infty} \frac{a(n)}{n}u^n.$$

So by looking at the coefficients of u^p of this equation in characteristic $p > 0$, i.e, in $k = R/\mathfrak{p}$, we get the congruence

$$a(p) \equiv b(p) \pmod{\mathfrak{p}}.$$

To show the second congruence, we apply the Cartier operator ζ to ω_0^*. We get

$$\zeta(\omega_0^*) = A^{*1/p}\omega_0^* = A^{*1/p}\,du + \cdots .$$

On the other hand, we also have the equation

$$\zeta(\omega_0^*) = \zeta\Big(\sum_{n=1}^{\infty} a(n)^* u^{n-1}du\Big) = \sum_{n=1}^{\infty} a(np)^{*1/p}\, u^{n-1}\,du$$

$$= a(p)^{*1/p}\,du + \cdots .$$

Hence we get the required congrence

$$A \equiv a(p) \pmod{\mathfrak{p}}. \qquad \text{QED}$$

Denote by $\bar{K}$ the algebraic closure of K, by $\bar{R}$ the integral closure of R in $\bar{K}$ and by $\bar{\mathfrak{p}}$ the maximal ideal of $\bar{R}$. The unique extension to $\bar{K}$ of the valuation v will be also denoted by v.

Let Γ be the formal group of E defined over R. Then $\bar{\mathfrak{p}}$ forms an abelian group $\Gamma(\bar{R})$ under Γ by defining the operation as follows: $\alpha \underset{\Gamma}{*} \beta = \Gamma(\alpha,\beta)$ for $\alpha, \beta \in \bar{\mathfrak{p}}$. The elements of $\Gamma(\bar{R})$ of finite order form a torsion subgroup. In particular, $\mathrm{Ker}\,[p]_\Gamma$ is a p-torsion subgroup of $\Gamma(\bar{R})$ (as one sees easily that

$$[p]_\Gamma(\alpha \underset{\Gamma}{*} \beta) = \Gamma([p]_\Gamma(\alpha),[p]_\Gamma(\beta)) = 0 \quad \text{for any } \alpha, \beta \in \mathrm{Ker}\,[p]_\Gamma).$$

For any positive real number $r \in \mathbb{R}^+$, we define (after Lubin [12]),

$$\Gamma(\bar{R})_r = \{ \alpha \in \Gamma(\bar{R}) \mid \nu(\alpha) \geq r \}.$$

Then $\Gamma(\bar{R})_r$ is a subgroup of $\Gamma(\bar{R})$.

(4.2) Definition. (See Lubin [12].) A subgroup S of $\Gamma(\bar{R})$ is called a congruence torsion subgroup of Γ, if there is a positive real number $r \in \mathbb{R}^+$ for which

$$S = \left\{ \alpha \in \Gamma(\bar{R})_r \;;\; \begin{array}{l} \text{there is } n \in \mathbb{N} \text{ such that} \\ \alpha \in \mathrm{Ker}\,[p^n]_\Gamma \end{array} \right\}.$$

A canonical subgroup $\mathrm{can}(\Gamma)$ of Γ is a congruence torsion subgroup of order p in $\mathrm{Ker}\,[p]_\Gamma$.

A natural question one can ask is "When does Γ have a canonical subgroup $\mathrm{can}(\Gamma)$?"

(4.3) Theorem. (Cf. Lubin [12].) With E, Γ, Γ^* and $[p]_\Gamma(u)$ as above, we assume that E has good reduction at $\mathfrak{p}$. Then we have the following assertions.

(1) If $h = 1$, then a canonical subgroup $\mathrm{can}(\Gamma)$ of Γ always exists and it is explicitly given by

$$\mathrm{can}(\Gamma) = \{ 0 \} \cup \{ \alpha \in \Gamma(\bar{R})_{\frac{1}{p-1}} \;\Big|\; \nu(\alpha) = \frac{1}{p-1} \}.$$

(2) If $h = 2$, then a canonical subgroup $\mathrm{can}(\Gamma)$ of Γ exists if and only if $\nu(b(p)) < \frac{p}{p+1}$. When $\mathrm{can}(\Gamma)$ exists, it is explicitly given by

$$\mathrm{can}(\Gamma) = \{0\} \cup \{\, \alpha \in \Gamma(\bar{R})_{\frac{1-\nu(b(p))}{p-1}} \mid \nu(\alpha) = \frac{1-\nu(b(p))}{p-1} \text{ with } \nu(b(p)) < \frac{p}{p+1} \,\}.$$

Proof. First we note that $[p]_\Gamma(u) = 0$ has p^h distinct roots in $\bar{\mathfrak{p}}$. (In fact, by differentiating the equation

$$[p]_\Gamma(\Gamma(u,v)) = \Gamma([p]_\Gamma(u),[p]_\Gamma(v))$$

with respect to v, we get

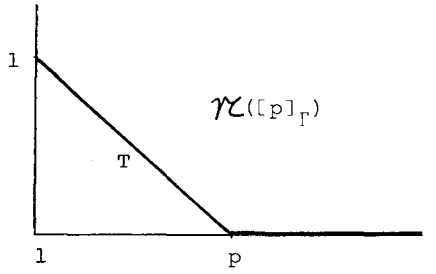
$$[p]'_\Gamma(\Gamma(u,v))\cdot\Gamma_2(u,v) = \Gamma_2([p]_\Gamma(u),[p]_\Gamma(v))\cdot[p]'_\Gamma(v).$$

Let $\alpha \in \bar{\mathfrak{p}}$ be a root of $[p]_\Gamma(u) = 0$. Put $u = \alpha$ and $v = 0$ in the above equation. Then we get

$$[p]'_\Gamma(\alpha)\cdot\Gamma_2(\alpha,0) = \Gamma_2(0,0)\cdot[p]'_\Gamma(0) = [p]'_\Gamma(0) \neq 0$$

and hence we have $[p]'_\Gamma(\alpha) \neq 0$.)

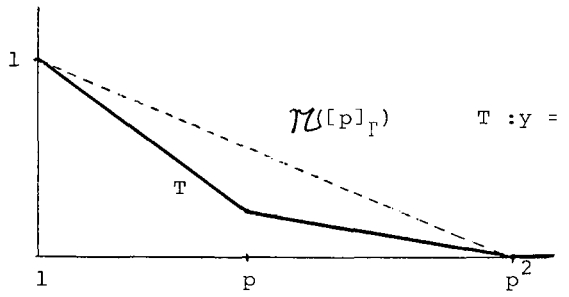
(1) If $h = 1$, then $\nu(b(p)) = 0$ and Ker $[p]_\Gamma$ has order p. Hence by Definition (4.2), $\mathrm{can}(\Gamma) = \mathrm{Ker}\ [p]_\Gamma$. Now look at the Newton polygon $\mathcal{N}([p]_\Gamma)$ of $[p]_\Gamma(u)$. It has the shape as



$$T : y = -\frac{1}{p-1}x + \frac{p}{p-1}$$

Hence every element of $\mathrm{can}(\Gamma)$ has order $\nu(\alpha) = \frac{1}{p-1}$ and we can take $r = \frac{1}{p-1}$.

(2) If $h = 2$, then Ker $[p]_\Gamma$ has order p^2 and the Newton polygon $\mathcal{N}([p]_\Gamma)$ of $[p]_\Gamma(u)$ has the shape as below with slope of T in the interval $\left(-\frac{1}{p-1}, -\frac{1}{p^2-1} \right]$.



Now suppose that a canonical subgroup can(Γ) of Γ exists. Then $[p]_\Gamma(u)$ must have the factor $g(u)$ of degree p. This means that the Newton polygon $\mathcal{N}([p]_\Gamma)$ must have a vertex at $(p, \nu(b(p)))$. This is possible only if $\nu(b(p)) < \frac{p}{p+1}$. Conversely, if this inequality holds true, then the segment T of the Newton polygon $\mathcal{N}([p]_\Gamma)$ gives rise $p-1$ roots of $[p]_\Gamma(u) = 0$ with order $\frac{1-\nu(b(p))}{p-1}$. These $p-1$ roots together with 0 form a canonical subgroup can(Γ) with $r = \frac{1-\nu(b(p))}{p-1}$. QED

(4.4) Theorem. With E, Γ, u, E*, A, $\omega_0 = \sum_{n=1}^{\infty} a(n)u^{n-1}du$ and $[p]_\Gamma(u) = pug_0(u) + b(p)u^p g_1(u) + \cdots$ as above, suppose that $h = 2$. Then the following conditions are equivalent.

(i) Γ possesses a canonical subgroup can(Γ).

(ii) $0 < \nu(b(p)) < \frac{p}{p+1}$.

(iii) $0 < \nu(a(p)) < \frac{p}{p+1}$.

(iv) $0 < \nu(A) < \frac{p}{p+1}$.

Proof. We have only to show the equivalences (ii) $\Leftrightarrow$ (iii) $\Leftrightarrow$ (iv). Let $f(u) = \sum_{n=1}^{\infty} \frac{a(n)}{n}u^n$ be the logarithm of Γ. An examination of the coefficients of the u^p-term of the equation $[p]_\Gamma(u) = f^{-1}(pf(u))$ gives the following identity:

$$a(p) = b(p)g_1(0) + p\cdot(\text{some element in } R).$$

Compare the ν-order of both sides. Then we obtain (by noting that $g_1(u)$ is a unit in $R[[u]]$),

$$\nu(b(p)) = \nu(a(p))$$

and hence the equivalence (ii) $\Leftrightarrow$ (iii).
To show the equivalence (iii)$\Leftrightarrow$(iv), note that Γ is a standard generic formal group over R (i.e, $[p]_\Gamma(u)$ necessarily has the form of Proposition (4.1), see also Lubin [12] for the definition). So p generates the maximal ideal $\mathfrak{p}$ of R, and by Proposition (4.1), we have

$$A = a(p) + p\cdot(\text{some element in } R).$$

Hence A and $a(p)$ have the same ν-order, from which the equivalence (iii)$\Leftrightarrow$(iv) follows immediately. QED

(4.6) Examples. (1) Suppose that the residue characteristic $p = 2$. Let E be dfined by the equation

$$y^2 + xy = x^3 + a_2x + a_6 \quad \text{with} \quad \nu(a_6) = 0.$$

Then E^* is ordinary (since $\nu(a_1) = \nu(1) = 0$) and hence Γ always has a canonical subgroup $\mathrm{can}(\Gamma)$.

If E is given by the equation

$$y^2 + a_3y = x^3 + a_4x + a_6 \quad \text{with} \quad \nu(a_3) = 0,$$

then E^* is supersingular and Γ does not have a canonical subgroup (because $\nu(a_1) = \nu(0) = \infty$).

If E is given by the equation

$$y^2 + a_1xy + a_3y = x^3 \quad \text{with} \quad \nu(a_3) = 0\ ,$$

then E^* is ordinary $\Leftrightarrow$ $\nu(a_1) = 0$, respectively E^* is supersingular and Γ has a canonical subgroup $\mathrm{can}(\Gamma)$ $\Leftrightarrow$ $0 < \nu(a_1) < 2/3$.

(2) Suppose that the residue characteristic $p = 3$.

If E is given by the equation

$$y^2 = x^3 + a_2x^2 + a_6 \quad \text{with} \quad \nu(a_6) = 0,$$

then E^* is ordinary $\Leftrightarrow$ $\nu(a_2) = 0$, respectively E^* is supersingular and Γ has a canonical subgroup $\mathrm{can}(\Gamma)$ $\Leftrightarrow$ $0 < \nu(a_2) < 3/4$.

If E is given by the equation

$$y^2 = x^3 + a_4x + a_6 \quad \text{with} \quad \nu(a_4) = 0,$$

then E^* is supersingular and Γ does not possess a canonical subgroup $\mathrm{can}(\Gamma)$ (because $\nu(A) = \nu(0) = \infty$).

(3) Suppose that the residue characteristic $p \geq 5$.
Let E be given by the equation

$$y^2 = x^3 + a_4x + a_6 \quad \text{with} \quad \nu(a_6) = 0.$$

Then some results are summarized in the following table.

p	i	j	E* and Γ
5	1	0	E* ordinary $\Leftrightarrow \nu(a_4) = 0$ E* supersingular & $\exists$ can(Γ) $\Leftrightarrow 0 < \nu(a_4) < \frac{5}{6}$
7	0	3	E* ordinary
11	1	1	E* ordinary
13	3	0	E* ordinary $\Leftrightarrow \nu(a_4) = 0$ E* supersingular & $\exists$ can(Γ) $\Leftrightarrow 0 < \nu(a_4) < \frac{13}{42}$
	0	2	E* ordinary
17	4	0	E* ordinary $\Leftrightarrow \nu(a_4) = 0$ E* supersingular & $\exists$ can(Γ) $\Leftrightarrow 0 < \nu(a_4) < \frac{17}{72}$
	1	2	E* ordinary
19	3	1	E* ordinary
	0	3	E* ordinary

We see tnat the condition $p \equiv 3 \pmod 4$ is sufficient for E* to be ordinary (because there always exists an integer $j > 0$ satisfying $2i + 3j = 2n + 1$, $n \in \mathbb{N}$). If $p \equiv 1 \pmod 4$, then there is the possibility that E* becomes supersingular (since there always exists an integer $i > 0$ satisfying $2i + 3j = 2n$, $n \in \mathbb{N}$).

(4.7) Theorem. (Cf. Lubin [12].) With E and Γ as above, assume that E has good reduction at $\mathfrak{P}$. Let F be the Frobenius morphism of E* and Γ^* induced by the p-th power map $x \to x^p$ of k. Suppose that Γ has a canonical subgroup can(Γ), then the Frobenius morphism F can be lifted back to cahracteristic 0, i.e, to R[[u]].

Proof. Put

$$\tilde{F}(x) = \prod_{\alpha \in \mathrm{can}(\Gamma)} (x - \alpha).$$

Then $\tilde{F}(x)$ is a monic polynomial over R of degree p and moreover by the construction,

$$\tilde{F}(x) \equiv x^p \pmod{\wp}.$$

Here we claim that $\tilde{F}(x)$ is indeed the lifting of the Frobenius morphism F to $R[[u]]$. For this, we observe that $\tilde{F}(\Gamma(u,v))$ is the ideal $(\tilde{F}(u),\tilde{F}(v))$ which is the set of all formal power series $\Phi(u,v) \in R[[u,v]]$ satisfying $\Phi(\alpha,\beta) = 0$ for any $\alpha, \beta \in \mathrm{can}(\Gamma)$. (For any $\alpha, \beta \in \mathrm{can}(\Gamma)$, $\Gamma(\alpha,\beta) = \alpha \underset{\Gamma}{*} \beta \in \mathrm{can}(\Gamma)$. This implies that $\tilde{F}(\Gamma(u,v)) \in (\tilde{F}(u),\tilde{F}(v))$. The other implication is clear.) We have the following commutative diagram:

$$\begin{array}{ccc} \Gamma(u,v) & \xrightarrow{\tilde{F}} & \tilde{F}(\Gamma(u,v)) \\ \Big\downarrow \bmod \wp & & \Big\downarrow \bmod \wp \\ \Gamma^*(u,v) & \xrightarrow{F} & \Gamma^{*(p)}(u^p,v^p) \end{array}$$

where $\Gamma^{*(p)}(u^p,v^p)$ is the formal power series in u^p, v^p with coefficients of the p-th power of those of Γ^*.
Hence $\tilde{F}(x)$ is in fact the lifting back of the Frobenius morphism F to characteristic 0, i.e, to $R[[u]]$. QED

5. Elliptic curves and formal groups over $\mathbb{Q}$.

Let E be an elliptic curve over $\mathbb{Q}$. Then there exists an (essentially unique) global Weierstrass minimal equation for E of the form (1.1) with $a_i \in \mathbb{Z}$ for every i and with the discriminant as small as possible. So $E^* = E \bmod p$ is defined over $\mathbb{F}_p$ for any rational prime p. As before, let $u = -\frac{x}{y}$ be a local parameter of E at the point at infinity of E and let

$$\omega_0 = \frac{dx}{2y+a_1x+a_3} = \sum_{n=1}^{\infty} a(n)u^{n-1}du, \quad a(1) = 1$$

be the canonical invariant differential on E. Then $a(n) \in \mathbb{Z}$ for all n.

The following two theorems (5.1) and (5.2) are very classical and well known, but we include them here for the sake of completeness.

(5.1) Theorem. (Cf. Tate [14].) Let E be an elliptic curve over $\mathbb{Q}$ given by the global Weierstrass minimal equation. For a rational prime p, let $E^* = E \bmod p$. Let N_p denote the number of rational points on E^* defined over $\mathbb{F}_p$. Put $f_p = p+1-N_p$. If E has good reduction at p, then $f_p = \mathrm{Tr}(\pi_{E^*/\mathbb{F}_p})$ (the trace of the Frobenius endomorphism $\pi_{E^*/\mathbb{F}_p}$ of E^* relative to $\mathbb{F}_p$ in its ℓ-adic representation) and it satisfies the Riemann hypothesis $|f_p| \leq 2\sqrt{p}$. If E^* has a node with tangent defined over $\mathbb{F}_p$ (resp. not defined over $\mathbb{F}_p$), then $f_p = +1$ (resp. -1). If E^* has a cusp, then $f_p = 0$. ∎

(5.2) Theorem. (Cf. Olson [13].) Let E be an elliptic curve over $\mathbb{Q}$ defined by the equation of the form (1.1') with $a, b \in \mathbb{Z}$. Let p be a rational prime $\neq 2,3$. Assume that E has good reduction at p. Let $\omega_0 = \sum_{n=1}^{\infty} a(n)u^{n-1}du$, $a(1) = 1$ and $a(n) \in \mathbb{Z}$ for all n be the canonical invariant differential on E given by (1.4'). Then

$$a(p) \equiv -\sum_{x \in CSR(p)} \left(\frac{x^3+ax+b}{p}\right) \pmod{p}$$

where CSR(p) stands for the complete system of residues mod p and $\left(\frac{\cdot}{p}\right)$ denotes the Legendre symbol.

In particular, if E is given by the equation $y^2 = x^3 + ax$ (resp. $y^2 = x^3 + b$), then

$$a(p) \equiv \left(\frac{\frac{p-1}{2}}{\frac{p-1}{4}}\right) a^{\frac{p-1}{4}} \pmod{p} \quad \left(\text{resp.} \left(\frac{\frac{p-1}{2}}{\frac{p-1}{6}}\right) b^{\frac{p-1}{6}} \pmod{p}\right). \text{ ∎}$$

Now we are about to state one of the main theorems of this paper.

(5.3) Theorem. Let E be an elliptic curve over $\mathbb{Q}$ given by the global Weierstrass minimal equation (1.1) with $a_i \in \mathbb{Z}$ for all i and let $\omega_0 = \sum_{n=1}^{\infty} a(n)u^{n-1}du$ be the canonical invariant differential on E given by (1.4). Assume that E has good reduction at a

rational prime p and put $E^* \equiv E \bmod p$. Then we have the following assertions.

(1) $a(p) \equiv \mathrm{Tr}(\pi_{E^*/\mathbb{F}_p}) \pmod p$

where $\pi_{E^*/\mathbb{F}_p}$ is the Frobenius endomorphism of E^* relative to $\mathbb{F}_p$ and $\mathrm{Tr}(\pi_{E^*/\mathbb{F}_p})$ is the trace of $\pi_{E^*/\mathbb{F}_p}$ in its ℓ-adic representation.

(2) $a(np) \equiv a(n)a(p) \pmod p$ for $(n,p) = 1$.

(3) $a(np) - \mathrm{Tr}(\pi_{E^*/\mathbb{F}_p})a(n) + pa(n/p) \equiv 0 \pmod{p^\alpha}$

for $n \equiv 0 \pmod{p^{\alpha-1}}$, $\alpha \geq 1$.

Historical remark on Theorem (5.3). The congruence relation (2) was discovered by Atkin and Swinnerton-Dyer, but their proof was never published. At the same time they conjectured the higher congruence (3). Cartier announced a proof of (3) in [1]. A complete proof of Theorem (5.3) was given by the author in [15].

In the rest of this paper, we shall survey the proofs of the congruences in Theorem (5.3). Our proof is based on deep study of formal groups associated to formal Dirichlet series with Euler products. So first of all, we shall look into the formal groups associated to certain formal Dirichlet series over integral domains of characteristic 0.

Let R be an integral domain of characteristic 0 with the field K of quotients. Let Φ be a formal group defined over R. Then over a $\mathbb{Q}$-algebra K, Φ is isomorphic to the additive (formal) group $G_a(x,y) = x + y$ and there exists a unique formal power series $\phi \in \mathrm{Hom}_K(\Phi, G_a)$, i.e, the logarithm of Φ, such that

$$\Phi(x,y) = \phi^{-1}(\phi(x) + \phi(y)).$$

We can write

$$\phi(x) = \sum_{n=1}^{\infty} \frac{\alpha(n)}{n} x^n, \qquad \alpha(n) \in R \quad \text{for all} \quad n.$$

Associated to the logarithm ϕ of Φ, we put

$$\omega = d\,\phi(x) = \phi'(x)dx = \sum_{n=1}^{\infty} \alpha(n) x^{n-1} dx.$$

This ω is called the invariant differential of Φ. We now define a formal Dirichlet series $D_\Phi(s)$ associated to Φ by letting

$$D_\Phi(s) = \sum_{n=1}^{\infty} \alpha(n) n^{-s}.$$

Then Honda [7] has shown that the following assertion holds ture.

(5.4) Proposition. Over a $\mathbb{Q}$-algebra K, we have the following correspondences :

$$\Phi \longleftrightarrow \phi \longleftrightarrow \omega \longleftrightarrow D_\Phi(s)$$

that is, if one of Φ, ϕ, ω and $D_\Phi(s)$ is given, then the rest are uniquely determined from the given one. ∎

Proposition (5.4) asserts, among other things, that a formal Dirichlet series over R yields a formal group over K. However, in most of the cases, formal groups obtained by this construction are not defined over R. So a basic number theoretic problem left to be settled is formulated as follows : What kinds of formal Dirichlet series over R give rise to formal groups defined over R?

For the sake of applications and simplicity, we confine our discussion to formal Dirichlet series with Euler products defined over $\mathbb{Z}$ or rather $\mathbb{Z}_p$ for all rational prime p. Progress in this direction has been made by Honda [6] and Hill [7].

(5.5) Theorem. Let

$$D(s) = (1 - b_1 p^{-s} - \cdots - b_i p^{-is} - \cdots - b_n p^{-ns})^{-1} \sum_{m=1}^{\infty} u_m m^{-s}$$

be a formal Dirichlet series with b_i, $u_m \in \mathbb{Z}_p$, $u_1 = 1$ and $u_m \in m\mathbb{Z}_p$ for every m. If $\mathrm{ord}_p(b_n) = n-1$ and $\mathrm{ord}_p(b_i) \geq i-1$ for $1 \leq i \leq n-1$, then the formal group Φ_D associated to D(s) by the construction of Proposition (5.4) is defined over $\mathbb{Z}_p$. Moreover the characteristic polynomial of $\Phi_D^* = :\Phi_D \bmod p$, which is Eisenstein over $\mathbb{Z}_p$ of degree h = height of Φ_D^*, divides the polynomial

$$S(x) = -\frac{p^n}{b_n} g(x/p) \quad \text{where} \quad g(x) = 1 - b_1 x - \cdots - b_n x^n. \ ∎$$

(Theorem (5.5) needs some comments. Let $\bar{k}$ be an algebraically closed field of characteristic $p > 0$ and let Φ be a formal group

over $\bar{k}$ of height $h < \infty$. Then the structure theorem of Dieudonné and Lubin asserts that $\mathrm{End}_{\bar{k}}(\Phi)$ is the maximal order in the central division algebra of rank h^2 over $\mathbb{Q}_p$ with invariant $1/h$ (see Honda [7], Theorem 1). Thus it follows that if k is an arbitrary field of characteritic $p > 0$, $\mathrm{End}_k(\Phi)$ is an order in a division algebra of rank dividing h^2 over $\mathbb{Q}_p$ (Lubin [11]) and, moreover, any $\lambda \in \mathrm{End}_k(\Phi)$ sits in a commutative field extension of $\mathbb{Q}_p$ of degree h and it is integral over $\mathbb{Z}_p$ and hence it satisfies a monic irreducible polynomial of degree dividing h over $\mathbb{Z}_p$: <u>the characteristic polynomial of</u> λ. If Φ is defined over a finite field with q elements, we mean by <u>the characteristic polynomial of</u> Φ , that of the Frobenius endomorphism x^q of Φ. If $k = \mathbb{F}_p$, the characteristic polynomial of Φ is an Eisenstein polynomial of degree h over $\mathbb{Z}_p$ (Cartier [1], Hill [6]).)

<u>(5.6) Observation.</u> <u>With</u> $D(s)$ <u>and</u> Φ_D <u>as in Theorem (5.5), put</u>

$$D(s) = \sum_{n=1}^{\infty} \alpha(n) n^{-s} \quad \underline{\text{with}} \quad \alpha(n) \in \mathbb{Z}_p \quad \underline{\text{for all}} \quad n.$$

<u>Then the coefficients</u> $\alpha(n)$ <u>satisfy the following equivalent conditions.</u>

(i) $\alpha(m) \equiv b_1 \alpha(m/p) + b_2 \alpha(m/p^2) + \cdots + b_n \alpha(m/p^n) \pmod{m}$

<u>where</u> $\alpha(r) = 0$ <u>if</u> $r \notin \mathbb{Z}$.

(ii) <u>Let</u> $\phi(x) = \sum_{n=1}^{\infty} \frac{\alpha(n)}{n} x^n$ <u>be the logarithm of</u> Φ_D.

<u>Put</u> $\Theta(x) = \phi(x) - \sum_{i=1}^{n} \frac{b_i}{p^i} \phi(x^{p^i})$. <u>Then</u> $\Theta(x) \in \mathbb{Z}_p[[x]]$.

Proof. (i) follows immediately from the definition of the coefficients $\alpha(n)$ and from the hypothesis on $D(s)$. To show the equivalence (i) $\Longleftrightarrow$ (ii), look at the coefficients of the term $x^{p^\ell m}$ with $(p,m) = 1$ of $\Theta(x)$. It is given by

$$\frac{a(p^\ell m)}{p^\ell m} - \sum_{i=1}^{n} \frac{b_i}{p^i} \frac{a(p^{\ell-i} m)}{p^{\ell-i} m} = \frac{1}{p^\ell m} \left\{ a(p^\ell m) - \sum_{i=1}^{n} b_i a(p^{\ell-i} m) \right\}.$$

Hence this is in $\mathbb{Z}_p$ if and only if the condition (i) holds true.

QED

(5.7) Lemma. Let $D_1(\mathbb{Z}_p)$ be the set of all formal power series over $\mathbb{Z}_p$ of the form $\sum_{m=1}^{\infty} u_m m^{-s}$ with $u_1 = 1$ and $u_m \in m\mathbb{Z}_p$ for all m. (We call such a formal Dirichlet series a "1-Dirichlet series".) Then $D_1(\mathbb{Z}_p)$ forms a ring.

Proof. It is easy to see that formal Dirichlet series over any ring R form a ring $D(R)$ and $R \to D(R)$ is a functor. In particular, if R is a field of characteristic 0, then for any $r \in \mathbb{Z}$, the formal substitution $s \to s+r$ defines an automorphism of $D(R)$ as follows.

$$\sum_{m=1}^{\infty} u_m m^{-s} \longrightarrow \sum_{m=1}^{\infty} u_m m^{-s-r} = \sum_{m=1}^{\infty} (u_m/m^r) m^{-s}.$$

We see that

$$D_1(\mathbb{Z}_p) = \{ \sum_{m=1}^{\infty} u_m m^{-s} \mid u_1 = 1,\ u_m \in m\mathbb{Z}_p \}$$

$$= \{ D(s) \in D(\mathbb{Z}_p) \mid D(s+1) \in D(\mathbb{Z}_p) \}$$

is the inverse image of $D(\mathbb{Z}_p)$ under the automorphism of $D(\mathbb{Q}_p)$ induced by the formal substitution $s \to s+1$. Hence it is a ring.

QED

(5.8) Theorem. Let $\Phi = \Phi_D$ be the formal group over $\mathbb{Z}_p$ constructed in Theorem (5.5) and let $\Phi^* =: \Phi \bmod p$ be the formal group defined over $\mathbb{F}_p$. Let $P(x) \in \mathbb{Z}_p[x]$ be the characteristic polynomial of Φ^*. Then the formal Dirichlet series $D_\Phi(s)$ ($= D(s)$ in Theorem (5.5)) associated to Φ has the "canonical factorization"

$$D_\Phi(s) = P(0)P(p^{1-s})^{-1}U(s) \quad \text{with} \quad U(s) \in D_1(\mathbb{Z}_p).$$

Proof. Let $S(x)$ be as in Theorem (5.5), i.e,

$$S(x) = -\frac{p^n}{b_n} g(x/p)$$

$$= x^n + (\frac{b_{n-1}}{b_n} p)x^{n-1} + \cdots + (\frac{b_i}{b_n} p^{n-i})x^i + \cdots - (\frac{1}{b_n} p^n)$$

$$= \sum_{i=0}^{n} c_i x^i.$$

Then

$$\mathrm{ord}_p(c_0) = \mathrm{ord}_p(-\frac{p^n}{b_n}) = 1,$$

$$\mathrm{ord}_p(c_i) = \mathrm{ord}_p(\frac{p^n}{b_n}\cdot\frac{b_i}{p^i}) \geq n-(n-1)+i-1-i \geq 0.$$

As the characteristic polynomial $P(x)$ of Φ_D^* is an Eisenstein factor of $S(x)$ of degree h = height of Φ_D^* (so $1 \leq h \leq n$), we can factor $S(x)$ into the product:

$$S(x) = P(x)\,Q(x).$$

Now we have

$$g(x) = -\frac{b_n}{p^n}\,P(px)\,Q(px) = \bar{P}(px)\bar{Q}(px)$$

where

$$\bar{P}(x) = :P(x)/P(0), \quad \bar{Q}(x) = :(-\frac{b_n}{p^n})\,P(0)Q(x).$$

So we can write

$$D(s) = g(p^{-s})^{-1}\sum_{m=1}^{\infty} u_m m^{-s} = \bar{P}(p^{1-s})^{-1}\,\bar{Q}(p^{1-s})^{-1}\sum_{m=1}^{\infty} u_m m^{-s}$$

$$= P(0)P(p^{1-s})^{-1}\,\bar{Q}(p^{1-s})^{-1}\sum_{m=1}^{\infty} u_m m^{-s}.$$

It remains to show that $\bar{Q}(p^{1-s})^{-1}\sum_{m=1}^{\infty} u_m m^{-s} \in D_1(\mathbb{Z}_p)$. Note that $\bar{Q}(x)$ has the constant term 1. So it follows immediately that $\bar{Q}(x)^{-1} \in \mathbb{Z}_p[[x]]$ and $\bar{Q}(p^{-s})^{-1} \in D(\mathbb{Z}_p)$. Hence $\bar{Q}(p^{1-s})^{-1} \in D_1(\mathbb{Z}_p)$. Thus we complete the proof by Lemma (5.7). QED

Hill [6] has shown that formal groups over $\mathbb{Z}_p$ are isomorphic over $\mathbb{Z}_p$ if and only if their reductions over $\mathbb{F}_p$ have the same characteristic polynomial. Here we shall investigate what happens to the formal Dirichlet series of formal groups over $\mathbb{Z}_p$, furnished with the canonical factorization, under $\mathbb{Z}_p$-isomorphisms of formal groups.

(5.9) Theorem (The isotypic theorem of formal Dirichlet series). With Φ, $D_{\Phi}(s)$ and $P(x)$ as in Theorem (5.8), let Ψ be a formal group over $\mathbb{Z}_p$ isomorphic over $\mathbb{Z}_p$ to Φ. Then the formal Dirichlet series $D_{\Psi}(s)$ associated to Ψ has the same type of factorization as $D_{\Phi}(s)$, that is,

$$D_{\Psi}(s) = P(0)P(p^{1-s})^{-1}\,\tilde{U}(s) \quad \text{with} \quad \tilde{U}(s) \in D_1(\mathbb{Z}_p).$$

Proof. Put $\Phi^* = \Phi \bmod p$ and $\Psi^* = \Psi \bmod p$. Let $P(x) = \sum_{i=0}^{h} c_i x^i$, $c_h = 1$, $c_i \equiv 0 \pmod p$ for $i \le i \le h-1$, $c_0 \not\equiv 0 \pmod{p^2}$ be the characteristic polynomial of Φ^* and Ψ^*. Then by the hypothesis, $D_{\Phi}(s)$ has the form:

$$D_{\Phi}(s) = \left[1+(\frac{c_1}{c_0}p)p^{-s} + \cdots + (\frac{c_i}{c_0}p^i)p^{-is} + \cdots + (\frac{1}{c_0}p^h)p^{-hs}\right]^{-1}U(s)$$
$$= \sum_{n=1}^{\infty} \alpha(n)n^{-s}, \quad \text{with} \quad U(s) \in D_1(\mathbb{Z}_p).$$

Let $\phi(x) = \sum_{n=1}^{\infty} \frac{\alpha(n)}{n} x^n$ be the logarithm of Φ. Then by applying the same argument as Observation (5.6), we get

$$\phi(x) + \sum_{i=1}^{h-1} (\frac{c_i}{c_0})\phi(x^{p^i}) + (\frac{1}{c_0})\phi(x^{p^h}) \in \mathbb{Z}_p[[x]].$$

Now let $\lambda(x) \in \mathbb{Z}_p[[x]]$ be a $\mathbb{Z}_p$-isomorphism of Φ to Ψ. Then it is easy to see that $\lambda(\phi(x)) = :\psi(x)$ is the logarithm of Ψ, i.e, $\Psi(x,y) = \psi^{-1}(\psi(x)+\psi(y))$. Here we claim that the following relation (*) holds true.

$$(*) \qquad \psi(x) + \sum_{i=1}^{h-1} (\frac{c_i}{c_0})\psi(x^{p^i}) + (\frac{1}{c_0})\psi(x^{p^h}) \in \mathbb{Z}_p[[x]].$$

For this, first of all, note that we have the congruence

$$\Psi \sum_{i=0}^{h} [c_i]_{\Psi}(x^{p^i}) \equiv 0 \pmod{p\,\mathbb{Z}_p[[x]]}$$

where the sum is taken with respect to Ψ. (This is because $\sum_{i=0}^{h} c_i x^i$ is the characteristic polynomial of Ψ^*.) Then we get

$$\psi(\Psi(\sum_{i=0}^{h} [c_i]_\Psi(x^{p^i}))) \equiv 0 \pmod{p\mathbb{Z}_p[[x]]}.$$

But by the fact that ψ is the logarithm of Ψ, this congruence is read as

$$\sum_{i=0}^{h} \psi([c_i]_\Psi(x^{p^i})) \equiv 0 \pmod{p\mathbb{Z}_p[[x]]}$$

where the sum is the ordinary one.
Thus we obtain, by noting that $[c_i]_\Psi \in \mathrm{End}_{\mathbb{Z}_p}(\Psi)$,

$$\sum_{i=0}^{h} c_i \psi(x^{p^i}) \equiv 0 \pmod{p\mathbb{Z}_p[[x]]}.$$

As c_0 is a p-adic prime, by dividing the above congruence by c_0, we get the required relation (*).

Now put $\psi(x) = \sum_{n=1}^{\infty} \frac{\beta(n)}{n} x^n$ and $D_\Psi(s) = \sum_{n=1}^{\infty} \beta(n) n^{-s}$. Then an examination of the coefficients of x^n-term in the relation (*) gives

$$\beta(n) + \sum_{i=1}^{h-1} (\frac{c_i}{c_0} p^i)\ \beta(n/p^i) + (\frac{1}{c_0} p^h)\beta(n/p^h) \in n\mathbb{Z}_p.$$

Therefore $D_\Psi(s)$ has the factorization as

$$D_\Psi(s) = P(0)P(p^{1-s})^{-1}\ \tilde{U}(s) \quad \text{with} \quad \tilde{U}(s) \in D_1(\mathbb{Z}_p).$$

QED

Now we shall discuss formal groups of L-series of elliptic curves (cf. Tate [14]). Let E be an elliptic curve defined over $\mathbb{F}_p$. Then the L-series L(E:s) of E is defined by

$$L(E:s) = (1 - \mathrm{Tr}(\pi_{E/\mathbb{F}_p})p^{-s} + p^{1-2s})^{-1}.$$

One can define the L-series even if E is not an elliptic curve, but a curve of the form (1.1) with a singularity. If E has an ordinary double point with tangent rational (resp. not rational) over $\mathbf{F}_p$, then

$$L(E:s) = (1-p^{-s})^{-1} \quad (\text{resp. } (1+p^{-s})^{-1}).$$

If E has a cusp, then

$$L(E:s) = 1.$$

If E is an elliptic curve over $\mathbb{Q}$ defined by the global Weierstrass minimal equation, we define the local L-series $L_p(E:s)$ of E at each rational prime p by $L(E^*:s)$ with $E^* = E \bmod p$. The global L-series $L(E:s)$ of E is then given by putting together all local $L_p(E:s)$.

$$L(E:s) = 1 \cdot \prod_{p|\Delta} (1 \pm p^{-s})^{-1} \prod_{p \nmid \Delta} (1 - \mathrm{Tr}(\pi_{E^*/\mathbb{F}_p}) p^{-s} + p^{1-2s})^{-1}$$

where Δ = discriminant of E.
Observe that when E has good reduction at p, $L_p(E:s)$ satisfies the conditions of Theorem (5.5). Moreover, we have

(5.10) Theorem. (Honda [7, 8].) *Let E be an elliptic curve over $\mathbb{Q}$ given by the global Weierstrass minimal equation (1.1). For each rational prime p, let $L_p(E:s)$ be the local L-series of E at p. Then the formal group Φ_p associated to $L_p(E:s)$ is defined over $\mathbb{Z}_p$ and moreover, it is $\mathbb{Z}_p$-isomorphic to the formal group (law) Γ of E. If p is a ratioanl prime such that E^* has a node with tangent rational over $\mathbb{F}_p$ (resp. tangent not defined over $\mathbb{F}_p$), then Φ_p is isomorphic over $\mathbb{Z}_p$ to the formal group $x + y - xy$ (resp. $x + y + xy$ the multiplicative (formal) group). If p is a rational prime such that E^* has a cusp, then Φ_p is isomorphic over $\mathbb{Z}_p$ to the additive (formal) group $x + y$.* ∎

(5.11) Proof of Theorem (5.3).

Step 1. Let p be a rational prime at which E has good reduction. Let Φ_p be the formal group over $\mathbb{Z}_p$ associated to the local L-series

$$L_p(E:s) = (1 - \mathrm{Tr}(\pi_{E^*/\mathbb{F}_p}) p^{-s} + p^{1-2s})^{-1}.$$

Put $\Phi_p^* = \Phi_p \bmod p$. Then by Theorem (5.5), the characteristic polynomial $P_{\Phi_p}(x)$ of Φ_p^* divides the polynomial $x^2 - \mathrm{Tr}(\pi_{E^*/\mathbb{F}_p})x + p$. Suppose that $h = \mathrm{ht}(\Phi_p^*) = 1$, then $P_{\Phi_p}(x)$ must be an Eisenstein factor of the polynomial $x^2 - \mathrm{Tr}(\pi_{E^*/\mathbb{F}_p})x + p$. The existence of such a factor is assured by the Riemann hypothesis. We put $P_{\Phi_p}(x) = x + \xi$ with a p-adic prime ξ. Then

$$x^2 - \mathrm{Tr}(\pi_{E/\mathbb{F}_p})x + p = P_{\Phi_p}(x)(x + p/\xi) \quad \text{in } \mathbb{Z}_p[x].$$

Suppose now that $h = ht(\Phi_p^*) = 2$. Then if $p \geq 5$, $P_{\Phi_p}(x) = x^2 + p$. (Because $P_{\Phi_p}(x)$ is Eisenstein over $\mathbb{Z}_p$ of degree 2 and it must divide the polynomial $x^2 - Tr(\pi_{E^*/\mathbb{F}_p})x + p$. So $Tr(\pi_{E^*/\mathbb{F}_p}) \equiv 0 \pmod{p} \iff Tr(\pi_{E^*/\mathbb{F}_p}) = 0$ or p. But by the Riemann hypothesis, $Tr(\pi_{E^*/\mathbb{F}_p}) = 0$ only can occur.) If $p = 2$ or 3, we have $P_{\Phi_p}(x) = x^2 \pm px + p$ or $x^2 + p$ as we can have $Tr(\pi_{E^*/\mathbb{F}_p}) = \pm p$ or 0.

Step 2. Apply Theorem (5.8) to $L_p(E:s)$. We can put $L_p(E:s)$ into the canonical form. If $h = ht(\Phi_p^*) = 1$,

$$L_p(E:s) = (1 + \frac{p}{\xi}p^{-s})^{-1} \sum_{m=1}^{\infty} u_m m^{-s} \quad \text{with} \quad u_m = \begin{cases} (-\xi)^{\nu} & \text{if } m = p^{\nu}, \\ 0 & \text{otherwise.} \end{cases}$$

If $h = ht(\Phi_p^*) = 2$,

$$L_p(E:s) = (1 + p^{1-2s})^{-1} \quad \text{or} \quad (1 \pm p.p^{-s} + p^{1-2s})^{-1}.$$

Step 3. Now we consider the formal group (law) Γ of E. The formal Dirichlet series $D_\Gamma(s)$ associated to Γ is given by

$$D_\Gamma(s) = \sum_{n=1}^{\infty} a(n)n^{-s}$$

where $a(n)$ are the coefficients of the canonical invariant differential ω_0 on E given by (1.4). Since Γ is isomorphic over $\mathbb{Z}_p$ to Φ_p, we can apply Theorem (5.9) to $D_\Gamma(s)$ and we get the factorization :

$$D_\Gamma(s) = \begin{cases} (1 + \frac{p}{\xi}p^{-s})^{-1} U_\Gamma(s) & \text{with } U_\Gamma(s) \in D_1(\mathbb{Z}_p) \text{ if } h = 1, \\ (1 + p^{1-2s})^{-1} U_\Gamma(s) & \text{with } U_\Gamma(s) \in D_1(\mathbf{Z}_p) \\ \quad \text{or} & \\ (1 \pm p \cdot p^{-s} + p^{1-2s})^{-1} U_\Gamma(s) & \text{with } U_\Gamma(s) \in D_1(\mathbf{Z}_p) \text{ if } h = 2. \end{cases}$$

Step 4. If $h = 1$, the canonical factorization of $D_\Gamma(s)$ gives the following congruences :

$$a(np) + \frac{p}{\xi}a(n) \equiv 0 \pmod{np\,\mathbb{Z}_p},$$

$$a(n) + \frac{p}{\xi}a(n/p) \equiv 0 \pmod{n\,\mathbb{Z}_p}.$$

Multiplying the p-adic prime ξ to the second congruence and adding it to the first one, we get

$$a(np) + (\xi + \frac{p}{\xi})a(n) + pa(n/p) \equiv 0 \pmod{np\,\mathbb{Z}_p}.$$

Since we have the equality

$$\xi + \frac{p}{\xi} = \mathrm{Tr}(\pi_{E^*/\mathbb{F}_p}),$$

we finally obtain the congruence (*) :

$$(*) \qquad a(np) - \mathrm{Tr}(\pi_{E^*/\mathbb{F}_p})a(n) + pa(n/p) \equiv 0 \pmod{np\,\mathbb{Z}_p}.$$

If $h = 2$, we have immediately from the canonical factorization of $D_\Gamma(s)$, the congruence (*) :

$$(*) \qquad \begin{aligned} &a(np) + pa(n/p) \equiv 0 \pmod{np\,\mathbb{Z}_p}, \\ &\text{or} \\ &a(np) \pm pa(n/p) + pa(n/p) \equiv 0 \pmod{np\,\mathbb{Z}_p}. \end{aligned}$$

In particular, the Atkin and Swinnerton-Dyer congruence (3) follows immediately from (*) if we take $n \equiv 0 \pmod{p^{\alpha-1}}$, $\alpha \geq 1$.

Step 5. Now let $\lambda(x) = \sum_{i=1}^{\infty} r_i x^i \in \mathbb{Z}_p[[x]]$, $r_1 = 1$ be the isomorphism of Φ_p to Γ over $\mathbb{Z}_p$. The logarithm $\phi_p(x)$ of Φ_p is the formal power series (refer the construction)

$$\phi_p(x) = x - \frac{\xi + p/\xi}{p}x^p + \cdots \in \mathbb{Q}_p[[x]],$$

and the logarithm of Γ is given by

$$(**) \qquad \sum_{n=1}^{\infty} \frac{a(n)}{n} x^n = \lambda(\phi_p(x)).$$

So by comparing the coefficients of x^p-term of (**) modulo p, we get the congruence (1) :

$$a(p) = -(\xi + p/\xi) + pr_p \equiv \mathrm{Tr}(\pi_{E^*/\mathbb{F}_p}) \pmod{p}.$$

Step 6. Take n so that $(n,p) = 1$. Then the congruence (*) is read

$$a(np) \equiv \mathrm{Tr}(\pi_{E^*/\mathbb{F}_p})a(n) \pmod{p\mathbb{Z}_p} \quad \text{if } h = 1,$$

$$a(np) \equiv 0 \pmod{p\mathbb{Z}_p} \quad \text{if } h = 2.$$

This congruence, together with the congruence (1) then gives the congruence (2) :

$$a(np) \equiv a(n)a(p) \pmod{p} \quad \text{for } (n,p) = 1.$$

This concludes the proof of Theorem (5.3).

6. Appendix : Elliptic curves and formal groups over algebraic number fields.

After I had finished writing this paper, Professor I. Barsotti of University of Padova, Italy kindly communicated to me that the Atkin and Swinnerton-Dyer congruence (3) of Theorem (5.3) holds true for slightly more general rings than $\mathbb{Z}$.

(6.1) Theorem. Let R be a Dedekind ring of characteristic 0 in which a rational prime p decomposes as $p = \mathfrak{p}\mathfrak{p}'$, $(\mathfrak{p}, \mathfrak{p}') = 1$. Let $k = R/\mathfrak{p}$ denote the finite field with $q = p^e$ elements. Let E be an elliptic curve over R defined by the equation (1.1) with $a_i \in R$ for every i, and with good reduction at $\mathfrak{p}$. Put $E^* = E \bmod \mathfrak{p}$. Let $u = -\frac{x}{y}$ be a local parameter of E at the point at infinity $(0,1,0)$ and let

$$\omega_0 = \sum_{n=1}^{\infty} a(n)u^{n-1}du, \quad a(1) = 1 \text{ and } a(n) \in R \text{ for all } n$$

be the canonical invariant differential on E given by (1.4). Then the coefficients $a(n)$ satisfy the generalized Atkin and Swinnerton-Dyer congruence :

$$a(nq) - \mathrm{Tr}(\pi_{E^*/k})a(n) + qa(n/q) \equiv 0 \pmod{p^r\mathfrak{p}}$$

for $n \equiv 0 \pmod{p^r}$ with $r \geq e$.
If $r < e$, the above congruence holds true with $a(n/q) = 0$.
(Here $\mathrm{Tr}(\pi_{E^*/k})$ denotes the trace of the Frobenius endomorphism $\pi_{E^*/k}$ of E^* relative to k in its ℓ-adic representation.)

Proof. Let F be the Frobenius morphism and $V = p/F$ the Verschiebung morphism of E^*. Then $\pi_{E^*/k} = F^e$ and $\pi'_{E^*/k} = :V^e$ are endomorphisms of E^* with $\pi_{E^*/k}\,\pi'_{E^*/k} = p^e = q$ and they are conjugates of each other over $\mathbb{Q}$. So we have

$$\mathrm{Tr}(\pi_{E^*/k}) = \pi_{E^*/k} + \pi'_{E^*/k}\,.$$

Now let $f(u) = \sum_{n=1}^{\infty} \frac{a(n)}{n} u^n$ be the logarithm of the formal group Γ of E, i.e, $f'(u)du = \omega_0$. Then we have the identity (A*) :

$$\text{(A*)} \qquad \mathrm{Tr}(\pi_{E^*/k}) f(u) = \pi_{E^*/k} f(u) + \pi'_{E^*/k} f(u)\,.$$

By examining the actions of the Frobenius and Verschiebung morphisms on $f(u)$ modulo $\mathfrak{p}$, we find

$$F\,f(u) \equiv \sum_{p|n} \frac{p a(n/p)^{(p)}}{n} u^n \pmod{\mathfrak{p} R[[u]]},$$

$$V\,f(u) \equiv \sum_{n=1}^{\infty} \frac{a(np)^{(1/p)}}{n} u^n \pmod{\mathfrak{p} R[[u]]}.$$

Hence we obtain

$$\text{(A**)} \qquad \pi_{E^*/k} f(u) \equiv \sum_{q|n} \frac{q a(n/q)}{n} u^n \pmod{\mathfrak{p} R[[u]]},$$

$$\text{(A***)} \qquad \pi'_{E^*/k} f(u) \equiv \sum_{n=1}^{\infty} \frac{a(nq)}{n} u^n \pmod{\mathfrak{p} R[[u]]}.$$

Thus, if $n \equiv 0 \pmod{p^r}$ with $r \geq e$, we obtain by putting together the above relations (A*), (A**) and (A***), the following :

$$a(nq) + q a(n/q) \equiv \mathrm{Tr}(\pi_{E^*/k}) a(n) \pmod{p^r \mathfrak{p}}.$$

If $n \equiv 0 \pmod{p^r}$ with $r < e$, this congruence is read with $a(n/q) = 0$ and hence we get

$$a(nq) \equiv \mathrm{Tr}(\pi_{E^*/k}) a(n) \pmod{p^r \mathfrak{p}}.$$

QED

Acknowledgement. I would like to express my heartfelt thanks to Professor I. Barsotti for his kind advice and to Professor K. Lønsted for encouragement.

References.

[1] Cartier,P., Une nouvelle opération sur les formes différentielles, C.R.Acad. Sci. Paris 244 (1957) 429-428.

[2] Cartier,P., Groupes formels, fonctions automorphes et fonctions zeta des courbes elliptiques, Actes Congrès intern. Math. Nice (1970) T2. 291-299.

[3] Cassels, J.W.S., Diophantine equations with special reference to elliptic curves, survey article, J. London Math. Soc. 41 (1962), 193-291.

[4] Deuring,M., Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Math. Sem. Hamburg 41 (1941), 197-272.

[5] Fröhlich,A., Formal Groups, Springer Lecture Notes in Mathematics No. 74 (1968).

[6] Hill,W., Formal groups and zeta functions of elliptic curves, Inventiones Math. 12 (1971), 337-345.

[7] Honda,T., Formal groups and zeta fucntions, Osaka J. Math. 5 (1968), 199-213.

[8] Honda,T., On the theory of commutative formal groups, J. Math. Soc. Japan 22 (1970), 213-246.

[9] Lang,S., Elliptic Fucntions, Addison-Wesley (1973), New York.

[10] Lazard,M., Sur les groupes de Lie formels à un paramètre, Bull. Soc. Math. France (1955), 251-274.

[11] Lubin,J., One-parameter formal Lie groups over $\mathfrak{p}$-adic integer rings, Ann. of Math. 80 (1964), 464-484.

[12] Lubin,J., Canonical subgroups of formal groups, Københavns Universitets Matematiske Institut Preprint Series No. 8 (1975).

[13] Olson,L., Hasse invariant and anomalous primes for elliptic curves with complex multiplication, J. Number Theory 8, No. 4 (1976), 397-414.

[14] Tate,J., The arithmetic of elliptic curves, Inventiones Math. 23 (1974), 179-206.

[15] Yui,N., Formal groups and p-adic properties of elliptic curves, (1974) Preprint.

[16] Yui,N., Elliptic curves and canonical subgroups of formal groups, (1977), to appear in J.reine u. angewandte Math. (Crelles Jour.).

Noriko Yui
Matematisk Institut
Københavns Universitet
Universitetsparken 5
2100 København Ø
Danmark

(Current address :
Department of Mathematics
University of Ottawa
Ottawa, Ontario
Canada, K1N 6N5)