(Accepted and Corrected Version : June 5, 2012)

Generalized Bernoulli-Hurwitz Numbers and The Universal Bernoulli Numbers

Yoshihiro Ônishi

Abstract

The three fundamental properties of the Bernoulli numbers, namely, the theorem of von Staudt-Clausen, von Staudt's second theorem, and Kummer's original congruence, are generalized to new numbers that we call generalized Bernoulli-Hurwitz numbers. These are coefficients of power series expansion of a higher genus algebraic function with respect to suitable variable. Our generalization strongly contrasts with the previous works. Indeed, the order of the power of the modulus prime in our Kummer-type congruences is exactly the same as in trigonometric function case, namely, Kummer's own congruence for the original Bernoulli numbers, and as in elliptic function case, namely, H. Lang's extension to the Hurwitz numbers. However, in the other past results on higher genus algebraic functions, the modulus was at most half of these classical cases. This contrast is clarified by investigating the analog of the three properties above for the universal Bernoulli numbers.

Introduction

In order to recall material on the Bernoulli and Hurwitz numbers, and to explain our new numbers, we consider a curve $\mathscr{C}$ of genus $g \geqq 0$ defined by

$$y^2 = x^{2g+1} - 1, \quad \text{or} \quad y^2 = x^{2g+1} - x. \tag{0.1}$$

Here we assume $\mathscr{C}$ is proper by adding in a natural way a point ∞ at infinity. The integral

$$u = \int_{\infty}^{(x,y)} \frac{x^{g-1}dx}{2y} \tag{0.2}$$

2000 *Mathematics Subject Classification.* Primary 11B68; Secondary 11R58,14L05.

Key words and phrases. Bernoulli numbers, Abelian functions, formal groups.

Partly supported by the Grant-in-Aid for Scientific Research (C), Japan Society for the Promotion of Science. (No.16540002, No.19540002, and No.22540006)

takes finite values for all $(x, y) \in \mathscr{C}$ and has a zero of order 1 at ∞. By regarding (0.2) as an equation in u and x, we consider a function $x \mapsto u$ on a neighbourhood of ∞. If $g = 1$, namely if $\mathscr{C}$ is an *elliptic curve*, the inverse function $u \mapsto x$ extends to the whole of the complex plane and is just the elliptic function $\wp(u)$ of Weierstrass.

If $g \geqq 2$, the inverse function above does not extend globally, so we should consider inverse functions of a *system of summations*

$$(u_1, u_2, \cdots, u_g) = \sum_{j=1}^{g} \int_{\infty}^{(x_j, y_j)} \Big(\frac{dx}{2y}, \frac{xdx}{2y}, \cdots, \frac{x^{g-1}dx}{2y}\Big) \tag{0.3}$$

of g integrals to g points (x_1, y_1), (x_2, y_2), $\cdots$, (x_g, y_g) of a natural base of holomorphic 1-forms. This is the classical theory of Abelian functions ever since Jacobi.

Now we back to (0.2) for $g = 0$ for the curve in the first part of (0.1). The function $u \mapsto x$ is just $1/\sin^2(u)$, and its Laurent coefficients are the Bernoulli numbers B_{2n}:

$$\frac{1}{\sin^2(u)} = \frac{-1}{u^2} + \sum_{n=1}^{\infty} (-1)^n \frac{2^{2n} B_{2n}}{2n} \frac{u^{2n-2}}{(2n-2)!}. \tag{0.4}$$

Moreover if $g = 1$ and $\mathscr{C}$ is defined by $y^2 = x^3 - x$, the Hurwitz numbers E_{4n}, important analogs of the Bernoulli numbers, are defined as Laurent coefficients of $x(u) = \wp(u)$:

$$\wp(u) = \frac{1}{u^2} + \sum_{n=1}^{\infty} \frac{2^{4n} E_{4n}}{4n} \frac{u^{4n-2}}{(4n-2)!}. \tag{0.5}$$

It seems extremely difficult, at least to the author, to find a generalization of these numbers for the case $g \geqq 2$ in the case of (0.3) involving several variables.

However, the Laurent development of the inverse function $u \mapsto x$ near $u = 0$ for several cases of $g \geqq 2$ has a surprising property of the coefficients, namely, a higher genus analog of some of the famous properties of the Bernoulli numbers ([Clau], [vS1], [vS2], [Ku]) and for Hurwitz numbers ([Hu1], [Hu2], [L]). They are formulated as our main theorems 6.1, 6.3, 7.1, and 7.5.

Here we explain the situation and results more explicitly. We suppose $g \geqq 1$. We recall that the values $\boldsymbol{u} = (u_1, u_2, \cdots, u_g)$ of (0.3) for variable g points (x_1, y_1), (x_2, y_2), $\cdots$, (x_g, y_g) on $\mathscr{C}$ and for all g paths of integrals from ∞ to (x_j, y_j) fill the whole g-dimensional linear space over the complex numbers $\mathbf{C}$. We denote the space by $\mathbf{C}^g$. The periods of (0.3), namely, the values of $\boldsymbol{u} = (u_1, u_2, \cdots, u_g)$ for all closed g paths give a lattice, say Λ, in $\mathbf{C}^g$. Then $\mathbf{C}^g/\Lambda$ is Jacobian variety of $\mathscr{C}$. We denote by ι the canonical embedding $(x, y) \mapsto \boldsymbol{u}$ of $\mathscr{C}$ into $\mathbf{C}^g/\Lambda$ defined by

$$\boldsymbol{u} = \int_{\infty}^{(x,y)} \Big(\frac{dx}{2y}, \frac{xdx}{2y}, \cdots, \frac{x^{g-1}dx}{2y}\Big) \tag{0.6}$$

modulo Λ. Our situation is summarized as follows:

$$\begin{array}{ccc} \kappa^{-1}\iota(\mathscr{C}) & \twoheadrightarrow & \mathscr{C} \\ \downarrow & & \downarrow \iota \\ \mathbf{C}^g & \xrightarrow{\kappa} & \mathbf{C}^g/\Lambda \end{array}$$

where κ is the map given by modulo Λ. The object $\kappa^{-1}\iota(\mathscr{C})$ is a *universal Abelian covering* of $\mathscr{C}$ and is denoted by $\widetilde{\mathscr{C}}$ in this paper. If $g = 1$, then the vertical map of the left hand side is an epimorphism.

If $\boldsymbol{u}$ varies along $\widetilde{\mathscr{C}}$, $\boldsymbol{u}$ determines uniquely a point (x, y) on $\mathscr{C}$ by (0.6). We denote the coordinates by

$$x(\boldsymbol{u}) \quad \text{and} \quad y(\boldsymbol{u}).$$

We can take the g-th coordinate u_g as a local parameter on $\widetilde{\mathscr{C}}$ near the point $\mathbf{0} = (0, 0, \cdots, 0)$ as explained in Section 4.2. So we have Laurent development of $x(\boldsymbol{u})$ and $y(\boldsymbol{u})$ by u_g. Their Laurent coefficients, which we call *generalized Bernoulli-Hurwitz numbers*, surprisingly resemble the classical Bernoulli and Hurwitz numbers, especially, they satisfy quite natural generalizations of von Staudt-Clausen's theorem([vS1] and [Clau]), von Staudt's second theorem([Ku]), and Kummer's original congruence([vS2]).

The properties discussed above of the generalized Bernoulli-Hurwitz numbers were known from computer calculations at the beginning of this work. Then the author arrived the *universal Bernoulli numbers* after thinking about proofs concerning the generalized Bernoulli-Hurwitz numbers.

Although there exist many researches generalizing those properties, for example, [Ca4], [Ka2], [RS], [Sn1], [Sn2], [Sn3], [Sn4], [Sn5], [Sn6], [V], and etcetera, it should be noticed that, in those works generalizing Kummer's congruence, the order of the power of respecting prime p are *less than the half* of the modulus of Kummer's original congruence. To the best knowledge of the author, Carlitz is the first who tried to find a generalization of the Hurwitz numbers to hyperelliptic functions, as is seen by his papers [Ca1] and [Ca4]. He did not consider our functions $x(\boldsymbol{u})$ and $y(\boldsymbol{u})$ and incompletely succeeded. Contrasting with this, our generalization of Kummer's original-type congruence for the generalized Bernoulli-Hurwitz numbers in this paper is a congruence modulo the *same power* of the respecting prime with the case of $g = 0$ ([Ku]) that is the classical congruence of Kummer himself for the Bernoulli numbers, and with the case of $g = 1$ ([L]) that is the Kummer-type congruence given by H. Lang for Hurwitz numbers.

The most remarkable thing is that the order of power of the modulus in our Kummer congruence (Theorem 3.1) for the universal Bernoulli numbers, which is best possible as is explained in 3.2(2), is *also less than half* of the order in the cases of the classical Bernoulli numbers and our generalized Bernoulli-Huriwitz numbers.

As the classical Bernoulli numbers are associated with the formal group law such that its formal logarithm is $t \mapsto \log(1 + t)$, the universal Bernoulli numbers are associated to

the *universal formal group law* that is a commutative formal group law of one variable and given over a ring known as the Lazard ring (see §1.5 of [Ha]). These numbers are used in stable homotopy theory rather than number theory (see §31.1 of [Ha]).

The generalized Bernoulli-Hurwitz numbers are associated with certain commutative formal group laws of one variable, as explained in Section 13.1. Similarly, the numbers which Carlitz et al. studied also are associated with commutative formal group laws. Since any commutative formal group law of one variable is obtained from the universal formal group law by specializing it, because of universality, any properties of the universal Bernoulli numbers are inherited not only by the generalized Bernoulli-Hurwitz numbers but also by Carlitz's generalizations, etc.

After all, the Kummer congruence for the universal Bernoulli numbers can not be used to prove such a congruence for the generalized Bernoulli-Hurwitz numbers, because the best possible order of power of the former is less than the half of the expected order of the later.

The result in the Section 2, namely, Clarke's theorem, which is the nice generalization and unification of the von Staudt-Clausen theorem and von Staudt's 2nd theorem, is used in the proof of such theorems for the generalized Bernoulli-Hurwitz numbers. On the other hand, the Kummer congruence for the universal Bernoulli numbers is proved in Section 3 and it is not used later. So, if the reader is interested only in the generalized Bernoulli-Hurwitz numbers, he/she could skip the whole of the Section 3.

Since writing the proof in the most general setting is so complicated, we prove the properties of the generalized Bernoulli-Hurwitz numbers only for the hyperelliptic curve of genus two defined by

$$y^2 = x^5 - 1.$$

The endomorphism ring of the Jacobian of this curve contains the 10th roots of unity. Then, for instance, a type of our numbers denoted by C_{10n} is defined by

$$x(\boldsymbol{u}) = \frac{1}{{u_2}^2} + \sum_{n=0}^{\infty} \frac{C_{10n}}{10n} \frac{{u_2}^{10n-2}}{(10n-2)!}. \tag{0.7}$$

Our results also hold for non-hyperelliptic curves of type described in the Section 14.1 (*curves of cyclotomic type*). The author think that it is not so difficult for the reader to give the proof of the properties of the numbers for such general curves. On the other hand our method gives a new proof of the three properties for Bernoulli numbers, and for Hurwitz numbers.

The author expect similar numbers might be obtained from more general curve such that the formal completion of its Jacobian variety over suitable local ring has a 1 dimensional factor of formal groups.

The proof of the von Staudt-Clause type theorem of ours strongly depends on nice paper by L.Carlitz [Ca1]. For the case $g \geqq 2$, it seems to difficult to use the classical

algebraic addition formula and multiplication formulae to prove the theorems. In his paper above Carlitz gave an interesting proof avoiding the addition and multiplication formulae of elliptic functions. Roughly speaking, his method is technical extension of Lagrange inversion theorem(see [WW], pp.131-133)[1]. However the divisor (in the sense of algebraic geometry) of n-th power of a given function is just the n-multiplication of the divisor of the function. We should think that the proof of Carlitz's and our proofs use multiplication formulae on Jacobian varieties[2].

Acknowledgements: This research was inspired by a suggestion of Masao Koike during my visit to Kyushu University and by unique book [AIK]. Proposition 3.4(2), Theorems 7.1 and 7.5 had been problematical conjectures at early stages of this work, until they were proved for me by Seidai Yasuda. I regret that Yasuda turned down an invitation to coauthor this paper, but I would like to express my sincere thanks for his important contribution to this work. Dr. Naruo Kanou gave me a nice program running on `pari/GP`, which consists of only a few lines (then we shall call it a *script*) but is so fast to get results. His script was so helpful to check numerically the results though out this work, and is quoted in Section 16.1 with his permission. A. Adelberg read carefully the Section 3 and gave important comments. Discussions with S. Matsutani and Takayuki Oda were very helpful. Hiroshi Suzuki at Nagoya University show me certain Lemma (see Lemma 18.3.2 in [O]) which is not mentioned in this paper but was helpful for the author to understand Proposition 13.13. I would like to express my deep gratitude to all these colleagues.

Contents

[1]This was pointed out by Takayuki Oda.
[2]This was pointed out by Shigeki Matsutani.

Convention and notations

(1) For a rational number α, we denote by $\lfloor \alpha \rfloor$ the largest integer which does not exceed α, and by $\lceil \alpha \rceil$ the smallest integer not smaller than α.

(2) We use the notation

$$(z)_n = z(z-1)\cdots(z-n+1)$$

for an integer $n = 0$. Here the range of z is determined by each context. The binomial coefficient is written by this as

$$\binom{z}{n} = \frac{(z)_n}{n!}.$$

(3) Generalizing the factorial symbol, we denote by $n!!$ the product

$$n(n-2)(n-4)\cdots$$

of the sequence with step -2 from n to 1 or 2. Similarly $n!!!$ means the product of the sequence of positive integers from n with step -3. Moreover, for instance, we denote $n!!!!! = n!^{(5)}$. For example, $12!^{(5)} = 12 \cdot 7 \cdot 2$.

(4) If p is a prime and the p-part of given rational number r is p^e, then we write $e = \mathrm{ord}_p r$. If τ is a polynomial (possibly in several variables) with rational coefficients, then we denote by $\mathrm{ord}_p \tau$ the least number of $\mathrm{ord}_p r$ for all the coefficients r of τ.

(5) For a prime number p and an integer a, we denote by $a|_p$ the remainder of the p-part of a, namely $a|_p = a/p^{\mathrm{ord}_p a}$.

(6) If $F(z)$ is a formal power series with respect to z, we denote by $[z^n]F(z)$ its coefficient of z^n. We use also $[\frac{z^n}{n!}]F(z) := n![z^n]F(z)$ or $[\frac{z}{n}]F(z) := n[z^n]F(z)$.

(7) For a formal power series $\varphi(z)$ with respect to z (permitting negative-power terms), we call $[\frac{z^n}{n!}]\varphi(z)$ $(n \geqq 0)$ the *Hurwitz coefficient* for $\varphi(z)$ of z^n. We say $[\frac{z}{n}]\varphi(z)$ is its *Carlitz coefficient*.

(8) Let R be a commutative ring. We denoted by $R\langle\langle v \rangle\rangle$ the ring of the formal power series with respect to z consisting of only terms of non-negative order such that all the corresponding Hurwitz coefficients belong to R.

(9) In an expression of a power series with respect to z, the symbol $(d^\circ(z) \geqq m)$ stands for its part of the terms of degree at least m. When m is obvious, we simply denote them as usual by $+\cdots$.

1 Preliminaries from Combinatorics

1.1 Fundamentals on factorial operation

The following properties on the factorial operation are frequently used in this paper. Let n and k be non-negative integers, and let p be a prime number. If $n = kp + a$ with $0 \leqq a < p$, then

$$\mathrm{ord}_p(n!) = \mathrm{ord}_p((kp)!) = \mathrm{ord}_p(k!) + k. \tag{1.1}$$

We denote by $S_p(n)$ the sum of the digits with respect to the base p expression of n. Then

$$\mathrm{ord}_p(n!) = \frac{n - S_p(n)}{p-1}. \tag{1.2}$$

1.2 Lagrange inversion formula

For a power series $F(z)$ of z, we denote by $[z^n]F(z)$ the coefficient of z^n. The following formula is called the Lagrange inversion formula.

PROPOSITION 1.3. *Let $\varphi(u) = u + \cdots$ be a power series of u having only terms of positive degree such that its coefficient of degree one term is* 1. *Let $\psi(t) = \varphi^{-1}(t)$ be its formal inverse series, namely, the power series with respect to t such that $\varphi(\psi(t)) = t$. Then*

$$[u^n]\Big(\frac{u}{\varphi(u)}\Big)^{\ell} = \frac{\ell}{\ell - n}[t^n]\Big(\frac{\psi(t)}{t}\Big)^{\ell - n}.$$

A proof of this is found in [Co], pp.148-153, for instance. See also [WW], pp.128-133 (Lagrange-Bürmann theorem).

1.3 Fundamentals on binomial coefficients

The following Lemma is used in 10.1.

LEMMA 1.4. *Let $n \geqq 0$, $q > 0$, r be three integers. Then*

$$\frac{(qn - r)!^{(q)}}{(qn)!^{(q)}} \in \mathbf{Z}\left[\frac{1}{q}\right].$$

PROOF. The number in the statement is the coefficient $[u^{n+1}]\big(-(1-u)^{r/q}\big)$. Let $t = q\{(1-u)^{1/q} - 1\}$, so that $u = 1 - (1 + \frac{1}{q}t)^q$. By applying the Lagrange inversion formula (1.3) for $\ell = -1$, we have

$$[u^n]\left(\frac{q\{(1-u)^{1/q} - 1\}}{u}\right) = [u^n]\left(\frac{u}{q\{(1-u)^{1/q} - 1\}}\right)^{-1} = [t^n]\left(\frac{1 - (1 + \frac{1}{q}t)^q}{t}\right)^{-1-n}.$$

Since the right hand side belongs to $\mathbf{Z}[\frac{1}{q}]$, the left hand side does also. Hence $[u^n]\big((1-u)^{1/q}\big) \in \mathbf{Z}[\frac{1}{q}]$. So that $[u^n]\big((1-u)^{r/q}\big) \in \mathbf{Z}[\frac{1}{q}]$ for all n. □

Here, we give another another proof of this.

LEMMA 1.5. *Let p be a prime number, $n \geqq 0$ be an integer, and $z \in \mathbf{Z}_{(p)}$. Then*

$$\binom{z}{n} \in \mathbf{Z}_{(p)}.$$

PROOF. For a given integer $n \geqq 0$, the function $z \mapsto n$ is a continuous map from $\mathbf{Z}_p$ to $\mathbf{Q}_p$. Since $\mathbf{Z}$ is dense in $\mathbf{Z}_p$ and $\binom{z}{n} \in \mathbf{Z}$ for $z \in \mathbf{Z}$, the statement follows. □

Although 1.5 is weaker than 1.4, 1.4 implies 1.4 by varying p because of the equality

$$\binom{\frac{r}{q}-1}{n} = \frac{r-q}{q} \cdot \frac{r-2q}{q} \cdot \cdots \cdot \frac{r-nq}{q} \Big/ n! = (-1)^n \frac{(qn-r)!^{(q)}}{(qn)!^{(q)}}. \tag{1.6}$$

2 Clarke's theorem

2.1 Definition of the universal Bernoulli numbers

Let f_1, f_2, $\cdots$ be infinitely many indeterminates. We consider the power series

$$u = u(t) = t + \sum_{n=1}^{\infty} f_n \frac{t^{n+1}}{n+1}, \tag{2.1}$$

and its formal inverse series

$$t = t(u) = u - f_1 \frac{u^2}{2!} + (3{f_1}^2 - 2f_2)\frac{u^3}{3!} + \cdots, \tag{2.2}$$

namely, the series such that $u(t(u)) = u$. Then we define $\hat{B}_n \in \mathbf{Q}[f_1, f_2, \cdots]$ by

$$\frac{u}{t(u)} = \sum_{n=0}^{\infty} \hat{B}_n \frac{u^n}{n!} \tag{2.3}$$

and call them *the universal Bernoulli numbers* (of order 1). If we specialize as $f_n = (-1)^n$, then $u(t) = \log(1+t)$ and $t(u) = e^u - 1$. Then $\hat{B}_n$ is specialized to the classical Bernoulli number B_n.

2.2 An expansion of the universal Bernoulli numbers

For a finite sequence $U = (U_1, U_2, \cdots)$ of non-negative integers, we denote $w(U) = \sum_j jU_j$, and call it the *weight* of U. The number $d(U) = \sum_j U_j$ is called the *degree* of U. We can regard U as a partition of $w(U)$. For simplicity, we write

$$U! = U_1!U_2! \cdots, \quad \binom{d}{U} = \frac{d!}{U!}. \tag{2.4}$$

Using the notations $\Lambda^U = 2^{U_1}3^{U_2}4^{U_3}\cdots$ and $f^U = {f_1}^{U_1}{f_2}^{U_2}{f_3}^{U_3}\cdots$, we define

$$\gamma_U = \Lambda^U U!. \tag{2.5}$$

If we set $h(t) = (u(t)/t) - 1$, then

$$\left(\frac{u(t)}{t}\right)^s = \big(1+h(t)\big)^s = \sum_{d=0}^{\infty}\binom{s}{d}h^d(t), \quad h^d(t) = \sum_{d(U)=d}\binom{d}{U}\frac{f^U}{\Lambda^U}\,t^{w(U)}. \tag{2.6}$$

Hence, by writing

$$\tau_U = (-1)^{d(U)-1}\frac{(w(U)+d(U)-2)!}{\gamma_U} \tag{2.7}$$

and using 1.3 for $\ell = 1$, we have the following expression for $\hat{B}_n$.

PROPOSITION 2.8. *We have*

$$\frac{\hat{B}_n}{n} = \sum_{w(U)=n}\tau_U f^U.$$

2.3 Clarke's theorem

Now, we describe Clarke's theorem on the universal Bernoulli numbers. For a prime number p and an integer a, we denote by $a|_p$ the remainder of the p-part of a, namely $a|_p = a/p^{\mathrm{ord}_p a}$.

PROPOSITION 2.9. *One has*

$$\hat{B}_1 = \frac{1}{2}f_1,$$

$$\frac{\hat{B}_2}{2} = -\frac{1}{4}{f_1}^2 + \frac{1}{3}f_2,$$

$$\frac{\hat{B}_n}{n} \equiv \begin{cases} \displaystyle\sum_{\substack{n=a(p-1)\\ p:\text{prime}}}\frac{{a|_p}^{-1} \bmod p^{1+\mathrm{ord}_p a}}{p^{1+\mathrm{ord}_p a}}\ {f_{p-1}}^a & (\text{ if } n\equiv 0 \mod 4\ ) \\ \dfrac{{f_1}^{n-6}{f_3}^2}{2} - \dfrac{n{f_1}^n}{8} + \displaystyle\sum_{\substack{n=a(p-1)\\ p:\text{odd prime}}}\frac{{a|_p}^{-1} \bmod p^{1+\mathrm{ord}_p a}}{p^{1+\mathrm{ord}_p a}}\ {f_{p-1}}^a & \\ & (\text{ if } n\neq 2 \text{ and } n\equiv 2 \mod 4\ ) \\ \dfrac{{f_1}^n + {f_1}^{n-3}f_3}{2} & (\text{ if } n\neq 1 \text{ and } n\equiv 1,\,3 \mod 4\ ) \end{cases}$$

mod *"the set of weight n polynomials in $\mathbf{Z}[f_1, f_2, \cdots]$"*.

The proof is refered to [Clar], which is done by a quite involved use of 2.8.

REMARK 2.10. (1) Of coarse, we have a congruence on $\hat{B}_n$ itself. For example, if $n \equiv 0 \mod 4$, this proposition shows that

$$\hat{B}_n \equiv -\sum_{\substack{p:\text{prime} \\ p-1|n}} \frac{{f_{p-1}}^{n/(p-1)}}{p} \mod \mathbf{Z}[f_1, f_2, \cdots]. \tag{2.11}$$

Indeed, for a prime p, if $n = a(p-1)$ and $\mathrm{ord}_p a = \nu$, then

$$\frac{n \cdot \left(a|_p{}^{-1} \mod p^{1+\nu}\right)}{p^{1+\nu}} \equiv 1 - \frac{1}{p} \equiv -\frac{1}{p} \mod \mathbf{Z}.$$

Hence we have (2.11). If we suppose additional condition $p-1 \not| n$, then we see easily

$$\hat{B}_n/n \in \mathbf{Z}_{(p)}[f_1, f_2, \cdots]. \tag{2.12}$$

The property (2.11) is an analog of the von Staudt-Clausen theorem for the classical Bernoulli numbers, and (2.12) is an analog of the von Staudt second theorem. Clarke's theorem is a beautiful unification of the analogs of these two theorems.
(2) Although the modulus is whole the ring $\mathbf{Z}[f_1, f_2, \cdots]$ in [Clar], we obviously see that it may be replaced as above because of 2.8.

3 Universal Kummer-type congruences

3.1 Main theorem

The universal Bernoulli numbers satisfy the congruence relation of Kummer's original type modulo $p^{\lfloor a/2 \rfloor}$.

THEOREM 3.1. *Let p be a prime, a and n be positive integers. Assume that $n > a$ and $n \not\equiv 0 \mod (p-1)$. Then*

$$\sum_{r=0}^{a} \binom{a}{r} (-f_{p-1})^{a-r} \frac{\hat{B}_{n+r(p-1)}}{n+r(p-1)} \equiv 0 \mod p^{\lfloor a/2 \rfloor} \mathbf{Z}_{(p)}[f_1, f_2, \cdots].$$

REMARK 3.2. (1) If $a = 1$ and $n > a = 1$ with $n \not\equiv 0, 1 \mod (p-1)$, then the congruence above holds modulo p. This fact appeared in [Ad1], Theorem 3.2 for the first time. A shorter proof and an extension to the case when $n \equiv 1 \mod (p-1)$ are given in [Ad2], Theorem 1.
(2) For an odd prime $p \geqq 7$, let us consider U such that $U_1 = p$, $U_{2p-1} = (p-3)/2$, and the other entries are $U_j = 0$. Then $w(U) = p + (p-5)(2p-1)/2 \equiv -1 \mod (p-1)$. For this U, we can easily show that

$$\mathrm{ord}_p(\tau_U) = (p-5)/2 (= \lfloor (p-4)/2 \rfloor).$$

Note that we have $n > a$ for $a = p-4$ and $n = w(U)$. Looking at (3.13) below, we understand that the estimate 3.1 is best possible.
(3) In the example above for $p = 5$, we have $\mathrm{ord}_5(\tau_U) = 0$. Then $n = w(U) = 5 \equiv 1 \bmod (5-1)$ and this is one of the excluded case in [Ad1], Theorem 3.2. Keeping this case in mind and slightly modifying the proof of 3.11 below, we can show that the congruence in 3.1 holds modulo p for $a = 1$ provided the additional condition $n \not\equiv 1 \bmod (p-1)$.

In 3.5, we give a new proof of the following congruence of Adelberg ([Ad3], (i) of the Theorem) directly from 3.1 and the Remark 3.2(1).

COROLLARY 3.3. (Adelberg's congruence) *If $n \not\equiv 0,\ 1 \bmod (p-1)$ and $n > a$, then*

$$f_{p-1}{}^{p^{a-1}} \cdot \frac{\hat{B}_n}{n} \equiv \frac{\hat{B}_{n+p^{a-1}(p-1)}}{n+p^{a-1}(p-1)} \mod p^a \mathbf{Z}_{(p)}[f_1, f_2, \cdots].$$

Theorem 3.1 gives more complicated but similar congruence to Corollary 3.3 if $n \equiv 1 \bmod (p-1)$. This is (ii) of the Theorem in [Ad3].

3.2 The first tool for the proof

We need two Propositions for the proof of 3.1. The following is the first one.

PROPOSITION 3.4. *Let p be a prime, and a, n be non-negative integers. Let*

$$M = \begin{cases} \mathrm{ord}_p(n!) & (\ \textit{if } n \geqq ap\ ), \\ a - \lfloor n/p \rfloor + \mathrm{ord}_p(n!) - \lfloor (a - \lfloor n/p \rfloor)/p \rfloor & (\ \textit{if } n < ap\ ). \end{cases}$$

Then we have the following congruences.
(1) *If q is a non-negative integer, then*

$$\sum_{r=0}^{a} \frac{((r+q)p+n)!}{(r+q)!p^{r+q}} \binom{a}{r} \equiv 0 \mod p^M;$$

(2) *If r_0 is an integer such that $0 < r_0 \leqq a$ and $n \geqq r_0 p$ is an integer, then*

$$\sum_{r=r_0}^{a} \frac{((r-r_0)p+n)!}{(r-r_0)!p^{r-r_0}} \binom{a}{r} \equiv 0 \mod p^M.$$

We define, for two real numbers $\alpha > 0$ and β,

$$\mathbf{Z}_p\langle\langle v \rangle\rangle^{(\alpha),\beta} = \left\{ \varphi \in \mathbf{Q}_p[[v]] \;\middle|\; \left(\tfrac{d}{dv}\right)^{pa} \varphi \in p^{\lceil \alpha(a+\beta) \rceil} \mathbf{Z}_p\langle\langle v \rangle\rangle \text{ for all } a \geqq 0 \right\}. \tag{3.5}$$

REMARK 3.6. (1) The reader may find it easier to understand the proof by regarding $\mathbf{Z}_p\langle\langle v \rangle\rangle^{(\alpha),\beta}$ as "$p^{\alpha\beta}\mathbf{Z}_p\langle\langle p^{\alpha/p} v \rangle\rangle$".
(2) We only use the case of $\alpha = 1 - \frac{1}{p}$ for the proof of 3.4

LEMMA 3.7. (1) $\mathbf{Z}_p\langle\langle v\rangle\rangle^{(\alpha),\beta}$ *is a* $\mathbf{Z}_p$*-submodule in* $\mathbf{Q}_p[[v]]$.
(2) $\mathbf{Z}_p\langle\langle v\rangle\rangle^{(\alpha),\beta} \subset p^{\lceil\alpha\beta\rceil}\mathbf{Z}_p\langle\langle v\rangle\rangle$, *Especially, if* $\beta \geqq 0$ *then* $\mathbf{Z}_p\langle\langle v\rangle\rangle^{(\alpha),\beta} \subset \mathbf{Z}_p\langle\langle v\rangle\rangle$.
(3) *For* $f(v) = \sum_{n=0}^{\infty} a_n v^n \in \mathbf{Q}_p[[v]]$, $f(v) \in \mathbf{Z}_p\langle\langle v\rangle\rangle^{(\alpha),\beta}$ *if and only if* $\sum_{n=0}^{m} a_n v^n \in \mathbf{Z}_p\langle\langle v\rangle\rangle^{(\alpha),\beta}$ *for all* $m \geqq 0$.
(4) *If* $\alpha_1 \geqq \alpha_2 > 0$ *then* $\mathbf{Z}_p\langle\langle v\rangle\rangle^{(\alpha_1),\beta} \subset \mathbf{Z}_p\langle\langle v\rangle\rangle^{(\alpha_2),\beta}$.
(5) *If* $\beta_1 \geqq \beta_2$ *then* $\mathbf{Z}_p\langle\langle v\rangle\rangle^{(\alpha),\beta_1} \subset \mathbf{Z}_p\langle\langle v\rangle\rangle^{(\alpha),\beta_2}$.
(6) *If* $n \in \mathbf{Z}$ (*possibly negative*) *then* $p^n\mathbf{Z}_p\langle\langle v\rangle\rangle^{(\alpha),\beta} \subset \mathbf{Z}_p\langle\langle v\rangle\rangle^{(\alpha),\beta+\frac{n}{\alpha}}$.
(7) *If* $\varphi \in \mathbf{Z}_p\langle\langle v\rangle\rangle^{(\alpha),\beta}$ *then* $\frac{d}{dv}\varphi \in \mathbf{Z}_p\langle\langle v\rangle\rangle^{(\alpha),\beta}$.
(8) *If* $\varphi \in \mathbf{Z}_p\langle\langle v\rangle\rangle^{(\alpha),\beta}$ *then* $\left(\frac{d}{dv}\right)^p\varphi \in \mathbf{Z}_p\langle\langle v\rangle\rangle^{(\alpha),\beta+1}$.
(9) *Let* $m \geqq 0$ *and* $b \in \mathbf{Q}_p$. $bv^m/m! \in \mathbf{Z}_p\langle\langle v\rangle\rangle^{(\alpha),\beta}$ *if and only if* $\mathrm{ord}_p(b) \geqq \alpha\left(\lfloor\frac{m}{p}\rfloor + \beta\right)$.

PROOF. (1) For $\varphi_1, \varphi_2 \in \mathbf{Z}_p\langle\langle v\rangle\rangle^{(\alpha),\beta}$, obviously $\varphi_1+\varphi_2 \in \mathbf{Z}_p\langle\langle v\rangle\rangle^{(\alpha),\beta}$. For $\varphi\mathbf{Z}_p\langle\langle v\rangle\rangle^{(\alpha),\beta}$ and $a \in \mathbf{Z}_p$, obviously $a\varphi \in \mathbf{Z}_p\langle\langle v\rangle\rangle^{(\alpha),\beta}$.
(2) If $\varphi \in \mathbf{Z}_p\langle\langle v\rangle\rangle^{(\alpha),\beta}$, then $\left(\frac{d}{dv}\right)^{pa}\varphi \in p^{\lceil\alpha(a+\beta)\rceil}\mathbf{Z}_p\langle\langle v\rangle\rangle$ by the definition. If we set $a = 0$, then we obtain just the statement.
(3) For the $f(v) \in \mathbf{Q}_p[[v]]$, write down the definition of $\mathbf{Z}_p\langle\langle v\rangle\rangle^{(\alpha),\beta}$. Then we see that $f(v) \in \mathbf{Z}_p\langle\langle v\rangle\rangle^{(\alpha),\beta}$ if and only if $a_n v^n \in \mathbf{Z}_p\langle\langle v\rangle\rangle^{(\alpha),\beta}$ for all $n \geqq 0$.
(4) This follows from the inequality $\lceil\alpha_1(a+\beta)\rceil \geqq \lceil\alpha_2(a+\beta)\rceil$ for all $a \geqq 0$.
(5) It suffice from (the proof of) (3) to show that $a_n v^n \in \mathbf{Z}_p\langle\langle v\rangle\rangle^{(\alpha),\beta_1}$ implies $a_n v^n \in \mathbf{Z}_p\langle\langle v\rangle\rangle^{(\alpha),\beta_2}$. This is obvious from the definition of $\mathbf{Z}_p\langle\langle v\rangle\rangle^{(\alpha),\beta}$.
(6) This follow from $\lceil\alpha(a+\beta+\frac{n}{\alpha})\rceil = \lceil\alpha(a+\beta)\rceil + n$.
(7) If $\left(\frac{d}{dv}\right)^{pa} a_n v^n \in p^{\lceil\alpha(a+\beta)\rceil}\mathbf{Z}_p\langle\langle v\rangle\rangle$, then $\left(\frac{d}{dv}\right)^{pa} n a_n v^{n-1} \in p^{\lceil\alpha(a+\beta)\rceil}\mathbf{Z}_p\langle\langle v\rangle\rangle$. Thus the statement follows from (the proof of) (3).
(8) Suppose $\varphi \in \mathbf{Z}_p\langle\langle v\rangle\rangle^{(\alpha),\beta}$. Then $\left(\frac{d}{dv}\right)^{pa}\varphi \in p^{\lceil\alpha(a+\beta)\rceil}\mathbf{Z}_p\langle\langle v\rangle\rangle$ by the definition. By replacing a by $a+1$, we have

$$\left(\tfrac{d}{dv}\right)^{pa}\left(\tfrac{d}{dv}\right)^{p}\varphi = \left(\tfrac{d}{dv}\right)^{p(a+1)}\varphi \in p^{\lceil\alpha((a+1)+\beta)\rceil}\mathbf{Z}_p\langle\langle v\rangle\rangle = p^{\lceil\alpha(a+(\beta+1))\rceil}\mathbf{Z}_p\langle\langle v\rangle\rangle,$$

and the statement.
(9) For $\varphi = bv^m/m!$, the property

$$\left(\tfrac{d}{dv}\right)^{pa}\varphi \in p^{\lceil\alpha(a+\beta)\rceil}\mathbf{Z}_p\langle\langle v\rangle\rangle \quad \text{for all } a \geqq 0$$

is equivalent to

$$\left(\tfrac{d}{dv}\right)^{pa}\varphi \in p^{\lceil\alpha(a+\beta)\rceil}\mathbf{Z}_p\langle\langle v\rangle\rangle \quad \text{for all } \lfloor\tfrac{m}{p}\rfloor \geqq a \geqq 0$$

(because of $(d/dv)^{(m+1)}v^m = 0$), and is also equivalent to

$$bv^{m-pa}/(m-pa)! \in p^{\lceil\alpha(a+\beta)\rceil}\mathbf{Z}_p v^{m-pa}/(m-pa)! \quad \text{for all } \lfloor\tfrac{m}{p}\rfloor \geqq a \geqq 0.$$

Since the last one is equivalent to

$$b \in p^{\lceil\alpha(a+\beta)\rceil}\mathbf{Z}_p \quad \text{for all } \lfloor\tfrac{m}{p}\rfloor \geqq a \geqq 0,$$

we have the statement immediately. □

COROLLARY 3.8. *If* $0 < \alpha \leqq 1$, $\varphi \in \mathbf{Z}_p\langle\langle v\rangle\rangle^{(\alpha),\beta}$ *then*

$$\Big(\Big(\frac{d}{dv}-1\Big)^p+1\Big)\varphi \in \mathbf{Z}_p\langle\langle v\rangle\rangle^{(\alpha),\beta+1}.$$

PROOF. For our purpose it suffices only to prove the case $p \neq 2$. The Leibniz rule shows

$$\Big(\Big(\frac{d}{dv}-1\Big)^p+1\Big)\varphi = \Big(\frac{d}{dv}\Big)^p\varphi + \sum_{j=1}^{p-1}(-1)^j\binom{p}{j}\Big(\frac{d}{dv}\Big)^j\varphi.$$

This belongs to $\mathbf{Z}_p\langle\langle v\rangle\rangle^{(\alpha),\beta+1} + p\mathbf{Z}_p\langle\langle v\rangle\rangle^{(\alpha),\beta}$ Therefore the statement follows from 3.7 (6), (5) and the assumption for α. □

LEMMA 3.9. *Let* $0 < \alpha \leqq 1$.
(1) $\mathbf{Z}_p[[v]] \subset \mathbf{Z}_p\langle\langle v\rangle\rangle^{(\alpha),0}$.
(2) *If* $\varphi_1 \in \mathbf{Z}_p\langle\langle v\rangle\rangle^{(\alpha),\beta_1}$ *and* $\varphi_2 \in \mathbf{Z}_p\langle\langle v\rangle\rangle^{(\alpha),\beta_2}$, *then* $\varphi_1\varphi_2 \in \mathbf{Z}_p\langle\langle v\rangle\rangle^{(\alpha),\beta_1+\beta_2}$.
Particularly, if $0 < \alpha \leqq 1$, *then* $\mathbf{Z}_p\langle\langle v\rangle\rangle^{(\alpha),0}$ *is a sub* $\mathbf{Z}_p$*-algebra in* $\mathbf{Z}_p\langle\langle v\rangle\rangle$, *and* $\mathbf{Z}_p\langle\langle v\rangle\rangle^{(\alpha),\beta}$ *is a* $\mathbf{Z}_p\langle\langle v\rangle\rangle^{(\alpha),0}$*-module.*

PROOF. (1) Suppose $\varphi \in \mathbf{Z}_p[[v]]$. Since $\frac{1}{(pa)!}\big(\frac{d}{dv}\big)^{pa}\varphi \in \mathbf{Z}_p[[v]] \subset \mathbf{Z}_p\langle\langle v\rangle\rangle$ for arbitrary $a \geqq 0$, we have

$$\Big(\frac{d}{dv}\Big)^{pa}\varphi \in (pa)!\mathbf{Z}_p\langle\langle v\rangle\rangle = p^a a!\mathbf{Z}_p\langle\langle v\rangle\rangle \subset p^a\mathbf{Z}_p\langle\langle v\rangle\rangle.$$

Because $\alpha \leqq 1$, this is contained in $p^{\lceil \alpha a\rceil}\mathbf{Z}_p\langle\langle v\rangle\rangle$. Hence $\varphi \in \mathbf{Z}_p\langle\langle v\rangle\rangle^{(\alpha),0}$.
(2) By the Leibniz rule, we see

$$\begin{aligned}\Big(\frac{d}{dv}\Big)^{pa}(\varphi\psi) &= \sum_{j=0}^{pa}\binom{pa}{j}\Big(\Big(\frac{d}{dv}\Big)^j\varphi\Big)\Big(\Big(\frac{d}{dv}\Big)^{pa-j}\psi\Big)\\ &= \sum_{j=0}^{a}\binom{pa}{pj}\Big(\Big(\frac{d}{dx}\Big)^{pj}\varphi\Big)\Big(\Big(\frac{d}{dv}\Big)^{pa-pj}\psi\Big)\\ &\quad + \sum_{0\leqq j\leqq pa,\, p\not| j}\binom{pa}{j}\Big(\Big(\frac{d}{dv}\Big)^j\varphi\Big)\Big(\Big(\frac{d}{dv}\Big)^{pa-j}\psi\Big).\end{aligned}$$

If $p \not| j$ then $p\big|\binom{pa}{j}$. The definition (3.5) and 3.7 (7) imply

$$\begin{aligned}\Big(\frac{d}{dv}\Big)^{pa}(\varphi\psi) &\in \sum_{j=0}^{a} p^{\lceil\alpha(j+\beta_1)\rceil}p^{\lceil\alpha(a-j+\beta_2)\rceil}\mathbf{Z}_p\langle\langle v\rangle\rangle\\ &\quad + \sum_{0\leqq j\leqq pa,\ p\not| j} pp^{\lceil\alpha(\lfloor\frac{j}{p}\rfloor+\beta_1)\rceil}p^{\lceil\alpha(\lfloor\frac{pa-j}{p}\rfloor+\beta_2)\rceil}\mathbf{Z}_p\langle\langle v\rangle\rangle\\ &\subset p^{\lceil\alpha(a+\beta_1+\beta_2)\rceil}\mathbf{Z}_p\langle\langle v\rangle\rangle + pp^{\lceil\alpha(a-1+\beta_1+\beta_2)\rceil}\mathbf{Z}_p\langle\langle v\rangle\rangle.\end{aligned}$$

By $\alpha \leqq 1$, this is contained in $p^{\lceil\alpha(a+\beta_1+\beta_2)\rceil}\mathbf{Z}_p\langle\langle v\rangle\rangle$, and we have shown that

$$\varphi\psi \in \mathbf{Z}_p\langle\langle v\rangle\rangle^{(\alpha),\beta_1+\beta_2}$$

as desired. □

LEMMA 3.10. *We have*

$$\exp\Big(v+\frac{v^p}{p}\Big)\in \mathbf{Z}_p\langle\langle v\rangle\rangle^{(1-\frac{1}{p}),0}.$$

PROOF. Thanks to 3.9 (2) and (3), it suffices to show
(1) $\exp\big(\sum_{n=0}^{\infty}\frac{v^{p^n}}{p^n}\big)\in \mathbf{Z}_p[[v]]$.
(2) $\exp\big(-\frac{v^{p^n}}{p^n}\big)\in \mathbf{Z}_p\langle\langle v\rangle\rangle^{(1-\frac{1}{p}),0}$ for all $n\geqq 2$.
Since the property (1) is well-known and proved in [Ho], p.238, 5.4 and [R], p.388, Theorem, we show only (2). To do so, by 3.7 (3), it suffices to show
(2)′ $\frac{1}{m!}\big(\frac{v^{p^n}}{p^n}\big)^m\in \mathbf{Z}_p\langle\langle v\rangle\rangle^{(1-\frac{1}{p}),0}$ for all $n\geqq 2$ and $m\geqq 0$.
This (2)′ is equivalent to
(2)″ $\mathrm{ord}_p\big(\frac{(p^nm)!}{m!p^{mn}}\big)\geqq(1-\frac{1}{p})p^{n-1}m$ for all $n\geqq 2$ and $m\geqq 0$,
because of 3.7(9). As

$$\mathrm{ord}_p\Big(\frac{(p^nm)!}{m!}\Big)=\sum_{j=0}^{n-1}p^jm\geqq p^{n-1}m+m,$$

to show (2)″ it suffices to check

$$p^{n-1}m+m-mn\geqq\big(1-\tfrac{1}{p}\big)p^{n-1}m,$$

namely, $m(p^{n-2}-n+1)\geqq 0$. This is easily checked. □

PROOF. (of 3.4) Let $n\geqq 0$ and $m=-\lceil\frac{n}{p}\rceil$. By 3.7(9), we see

$$\frac{v^n}{n!}\in \mathbf{Z}_p\langle\langle v\rangle\rangle^{(1-\frac{1}{p}),m}\cap\mathbf{Z}_p\langle\langle v\rangle\rangle.$$

By 3.10 and 3.9(2) we have $\frac{v^n}{n!}\exp\big(v+\frac{v^p}{p}\big)\in \mathbf{Z}_p\langle\langle v\rangle\rangle^{(1-\frac{1}{p}),m}\cap\mathbf{Z}_p\langle\langle v\rangle\rangle$; and by 3.8 we have

$$\Big(\Big(\frac{d}{dv}-1\Big)^p+1\Big)^a\Big(\frac{v^n}{n!}\exp\Big(v+\frac{v^p}{p}\Big)\Big)\in \mathbf{Z}_p\langle\langle v\rangle\rangle^{(1-\frac{1}{p}),m+a}\cap\mathbf{Z}_p\langle\langle v\rangle\rangle$$

for all $a\geqq 0$. This is contained in $p^{\lceil(1-\frac{1}{p})(m+a)\rceil}\mathbf{Z}_p\langle\langle v\rangle\rangle\cap\mathbf{Z}_p\langle\langle v\rangle\rangle$ by the property 3.7(2). Since

$$\begin{aligned}\Big(\Big(\frac{d}{dv}-1\Big)^p+1\Big)^a&\Big(\frac{v^n}{n!}\exp\Big(v+\frac{v^p}{p}\Big)\Big)\\&=\exp(v)\Big(\Big(\frac{d}{dv}\Big)^p+1\Big)^a\Big(\frac{v^n}{n!}\exp\Big(\frac{v^p}{p}\Big)\Big),\end{aligned}$$

and $\exp(v)$ is a unit in $\mathbf{Z}_p\langle\langle v\rangle\rangle$, we see

$$\Big(\Big(\frac{d}{dv}\Big)^p+1\Big)^a\Big(\frac{v^n}{n!}\exp\Big(\frac{v^p}{p}\Big)\Big)\in p^{\lceil(1-\frac{1}{p})(m+a)\rceil}\mathbf{Z}_p\langle\langle v\rangle\rangle\cap\mathbf{Z}_p\langle\langle v\rangle\rangle.$$

Substituting $m=-\lfloor\frac{n}{p}\rfloor$, we have finally

$$\Big(\Big(\frac{d}{dv}\Big)^p+1\Big)^a\Big(\frac{v^n}{n!}\exp\Big(\frac{v^p}{p}\Big)\Big)\in\begin{cases}\mathbf{Z}_p\langle\langle v\rangle\rangle & (\text{ if } pa<n\ ),\\ p^{a-\lfloor\frac{n}{p}\rfloor-\lfloor(a-\lfloor\frac{n}{p}\rfloor)/p\rfloor}\mathbf{Z}_p\langle\langle v\rangle\rangle & (\text{ if } pa\geqq n\ ).\end{cases}$$

Looking at the coefficients of $v^{n+qp}/(n+qp)!$ or $v^{n-r_0p}/(n-r_0p)!$ of the above after multiplying it by $n!$, we get the desired congruences. □

3.3 The second tool for the proof

We show the second Proposition that is used in the proof of 3.1.

PROPOSITION 3.11. *Let p be an odd prime and U is a partition with $U_{p-1} = 0$, $d(U) \neq 0$. Then τ_U defined by (2.2.4) satisfies*

$$\mathrm{ord}_p(\tau_U) \geqq \left\lfloor \frac{w(U) + d(U) - 2}{2p} \right\rfloor.$$

REMARK 3.12. As we mentioned in 3.2(2), we have $\mathrm{ord}_p(\tau_U) = (p-5)/2$ for any prime $p \geqq 5$ and any partition U such that $U_1 = p$, $U_{2p-1} = (p-5)/2$, with the others $U_j = 0$. For this U, since $w(U) = p + \frac{(2p-1)(p-5)}{2}$, $d(U) = p + \frac{p-5}{2}$, and $\lfloor (w(U) + d(U) - 2)/(2p) \rfloor = \left\lfloor (p^2 - 3p - 2)/(2p) \right\rfloor = \lfloor \frac{p-5}{2} + \frac{p-1}{p} \rfloor = (p-5)/2$, the estimate above is best possible.

PROOF. As $d(U) \neq 0$, we have $w(U) + d(U) - 2 > 0$. We show the estimate under the condition $U_{2p-1} \neq 0$ as follows:

$$\begin{aligned}
&\mathrm{ord}_p(\tau_U) = \mathrm{ord}_p((n+d-2)!) - \mathrm{ord}_p(\gamma_U) \\
&= \mathrm{ord}_p\Big(\Big(-2 + \sum_{j \neq p-1} (j+1)U_j \Big)! \Big) - \sum_{(\epsilon,k) \neq (1,1)} k U_{\epsilon p^k - 1} - \sum_{j \neq p-1} \mathrm{ord}_p(U_j!) \\
&\qquad (\text{ In the bellow } \epsilon \text{ runs through the positive integers coprime to } p. \ ) \\
&\geqq \mathrm{ord}_p\Big(\Big(-2 + \sum_{j \neq p-1,\ 2p-1} jU_j + 2pU_{2p-1} \Big)! \Big) - \sum_{(\epsilon,k) \neq (1,1)} k U_{\epsilon p^k - 1} - \mathrm{ord}_p(U_{2p-1}!) \\
&= \mathrm{ord}_p\Big(\Big(-2 + \sum_{p \not| j+1} jU_j + \sum_{(\epsilon,k) \neq (1,1),\ (2,1)} (\epsilon p^k - 1) U_{\epsilon p^k - 1} + 2pU_{2p-1} \Big)! \Big) \\
&\qquad - \sum_{(\epsilon,k) \neq (1,1)} k U_{\epsilon p^k - 1} - \mathrm{ord}_p(U_{2p-1}!) \\
&\geqq \sum_{\nu=1}^{\infty} \left\lfloor \frac{1}{p^\nu} \Big(-2 + \sum_{p \not| j+1} jU_j + \sum_{(\epsilon,k) \neq (1,1),\ (2,1)} (\epsilon p^k - 1) U_{\epsilon p^k - 1} + 2pU_{2p-1} \Big) \right\rfloor \\
&\qquad - \sum_{(\epsilon,k) \neq (1,1)} k U_{\epsilon p^k - 1} - \mathrm{ord}_p(U_{2p-1}!) \qquad (\text{ because } \mathrm{ord}_p(N!) = \sum_{\nu=1}^{\infty} \lfloor \tfrac{N}{p^\nu} \rfloor \ ) \\
&= \left\lfloor \frac{1}{p} \Big(-2 + \sum_{p \not| j+1} jU_j + \sum_{(\epsilon,k) \neq (1,1),\ (2,1)} (\epsilon p^k - 1) U_{\epsilon p^k - 1} + 2pU_{2p-1} \Big) \right\rfloor \\
&\qquad + \sum_{\nu=2}^{\infty} \left\lfloor \frac{1}{p^\nu} \Big(-2 + \sum_{p \not| j+1} jU_j + \sum_{(\epsilon,k) \neq (1,1),\ (2,1)} (\epsilon p^k - 1) U_{\epsilon p^k - 1} + 2pU_{2p-1} \Big) \right\rfloor \\
&\qquad - \sum_{(\epsilon,k) \neq (1,1)} k U_{\epsilon p^k - 1} - \mathrm{ord}_p(U_{2p-1}!) \\
&\geqq \left\lfloor \frac{1}{p} \Big(-2 + \sum_{p \not| j+1} jU_j + \sum_{(\epsilon,k) \neq (1,1),\ (2,1)} (\epsilon p^k - 1) U_{\epsilon p^k - 1} + 2pU_{2p-1} \Big) \right\rfloor
\end{aligned}$$

$$
\begin{aligned}
&\quad + \sum_{\nu=2}^{\infty} \left\lfloor \frac{-2+2pU_{2p-1}}{p^{\nu}} \right\rfloor - \sum_{(\epsilon,k)\neq(1,1)} kU_{\epsilon p^k-1} - \mathrm{ord}_p(U_{2p-1}!) \\
&= \left\lfloor \frac{1}{p}\Big(-2 + \sum_{p\not| j+1} jU_j + \sum_{(\epsilon,k)\neq(1,1),\ (2,1)} (\epsilon p^k-1)U_{\epsilon p^k-1} + 2pU_{2p-1} \Big) \right\rfloor \\
&\quad - \sum_{(\epsilon,k)\neq(1,1)} kU_{\epsilon p^k-1} + \sum_{\nu=2}^{\infty} \left\lfloor \frac{-2+2pU_{2p-1}}{p^{\nu}} \right\rfloor - \mathrm{ord}_p(U_{2p-1}!) \\
&= \left\lfloor \frac{1}{p}\Big(-2 + \sum_{p\not| j+1} jU_j + \sum_{(\epsilon,k)\neq(1,1),\ (2,1)} (\epsilon p^k-kp-1)U_{\epsilon p^k-1} + 2pU_{2p-1} \Big) \right\rfloor \\
&\quad - U_{2p-1} + \sum_{\nu=2}^{\infty} \left\lfloor \frac{-2+2pU_{2p-1}}{p^{\nu}} \right\rfloor - \mathrm{ord}_p(U_{2p-1}!) \\
&= \left\lfloor \frac{1}{p}\Big(-2 + \sum_{p\not| j+1} jU_j + \sum_{(\epsilon,k)\neq(1,1),\ (2,1)} (\epsilon p^k-kp-1)U_{\epsilon p^k-1} + 2pU_{2p-1} \Big) \right\rfloor \\
&\quad - U_{2p-1} + \mathrm{ord}_p((-2+2pU_{2p-1})!) - \left\lfloor \frac{-2+2pU_{2p-1}}{p} \right\rfloor - \mathrm{ord}_p(U_{2p-1}!).
\end{aligned}
$$

Here we can replace the first term $-\frac{2}{p}$ by $-\frac{1}{p}$, because if in the first bracket $\lfloor\ \rfloor$ the sum of the other terms is an integer then both of $-\frac{2}{p}$ and $-\frac{1}{p}$ contribute as -1, and if the sum is not an integer its fractional part is larger than or equals to $\frac{1}{p}$. Moreover, since $j \leqq (j+1)/2$ about the term jU_j in the second term sum, and $\epsilon p^k - kp - 1 > \epsilon p^k/2$ if $(\epsilon, k) \neq (1,1)$, $(2,1)$ for the third term sum, we see, by using 1.1, that

$$
\begin{aligned}
&\geqq \left\lfloor \frac{1}{2p}\Big(-2 + \sum_{p\not| j+1} (j+1)U_j + \sum_{(\epsilon,k)\neq(1,1),\ (2,1)} \epsilon p^k U_{\epsilon p^k-1} + 2pU_{2p-1} \Big) + U_{2p-1} \right\rfloor \\
&\quad - U_{2p-1} + \mathrm{ord}_p((-2+2pU_{2p-1})!) - \left\lfloor \frac{-2+2pU_{2p-1}}{p} \right\rfloor - \mathrm{ord}_p(U_{2p-1}!) \\
&= \left\lfloor \frac{-2+w(U)+d(U)}{2p} \right\rfloor + \mathrm{ord}_p\big((2U_{2p-1})!\big) + 2U_{2p-1} - \mathrm{ord}_p(2pU_{2p-1}) \\
&\quad - \left\lfloor \frac{-2+2pU_{2p-1}}{p} \right\rfloor - \mathrm{ord}_p(U_{2p-1}!) \\
&= \left\lfloor \frac{-2+w(U)+d(U)}{2p} \right\rfloor + \mathrm{ord}_p\big((2U_{2p-1})!\big) + 2U_{2p-1} - \mathrm{ord}_p(2U_{2p-1}) - 1 \\
&\quad - (-1+2U_{2p-1}) - \mathrm{ord}_p(U_{2p-1}!) \\
&\geqq \left\lfloor \frac{-2+w(U)+d(U)}{2p} \right\rfloor + \mathrm{ord}_p\left(\frac{(2U_{2p-1}-1)!}{U_{2p-1}!} \right).
\end{aligned}
$$

Hence, our proof has been completed for the case $U_{2p-1} \neq 0$. If $U_{2p-1} = 0$, by substituting this at the beginning of this calculation, we can more easily prove the desired estimate. $\square$

3.4 Proof of Kummer-type congruence relations

Let us finalize the proof of 3.1. By 2.8, $(-1)^a$ times the left hand side of the congruence in 3.1 is rewitten as

$$\sum_{r=0}^{a}\binom{a}{r}(-f)^r {f_{p-1}}^{a-r}\sum_{w(U)=n+r(p-1)}\tau_U f^U, \tag{3.13}$$

where τ_U is defined by (2.7). By picking up ${f_{p-1}}^r$ or ${f_{p-1}}^{r-r_0}$ from f^U, we know that (3.13) is equal to

$$\begin{aligned}\sum_{r=0}^{a}\binom{a}{r}(-1)^r {f_{p-1}}^{a-r}\Bigg\{&\sum_{w(U)=n}\tau_{U[r]}f^U{f_{p-1}}^r\\ &+\sum_{r_0=1}^{r}\Bigg(\sum_{\substack{w(U)=n+r_0(p-1)\\ U_{p-1}=0}}\tau_{U[r-r_0]}f^U{f_{p-1}}^{r-r_0}\Bigg)\Bigg\},\end{aligned} \tag{3.14}$$

where $U[r]$ means to increase r the $(p-1)$-st entry of U. After exchanging the sums about r and about U, by writing down $\tau_{U[r]}$ and $\tau_{U[r-r_0]}$, we see that (3.14) is equal to

$$\begin{aligned}&\sum_{w(U)=n}\frac{f^U{f_{p-1}}^a}{\gamma_{U|_{p-1}}}\sum_{r=0}^{a}\binom{a}{r}(-1)^{d(U[r])+r-1}\frac{\{w(U[r])+d(U[r])-2\}!}{p^{r+U_{p-1}}(r+U_{p-1})!}\\ &+\sum_{r_0=1}^{a}\sum_{\substack{w(U)=n+r_0(p-1)\\ U_{p-1}=0}}\frac{f^U{f_{p-1}}^{a-r_0}}{\gamma_U}\Bigg\{\sum_{r=r_0}^{a}\binom{a}{r}(-1)^{d(U[r-r_0])+r-1}\\ &\qquad\cdot\frac{\{w(U[r-r_0])+d(U[r-r_0])-2\}!}{p^{r-r_0}(r-r_0)!}\Bigg\}.\end{aligned} \tag{3.15}$$

Here $U|_{p-1}$ means the one which is obtained by replacing the $(p-1)$-st entry of U by 0, so that $\gamma_{U|_{p-1}}$ in the former sum means the one which is obtained by omitting the $(p-1)$-st part $p^{U_{p-1}}U_{p-1}!$ of γ_U. Note that, for each r,

$$\begin{aligned}\gamma_{U[r]|_{p-1}}&=\gamma_{U|_{p-1}},\\ \gamma_{U[r]|_{p-1}}p^{r+U_{p-1}}(r+U_{p-1})!&=\gamma_{U[r]},\end{aligned} \tag{3.16}$$

and that, in the later sum,

$$\gamma_U=\left(2^{U_1}\cdots(p-1)^{U_{p-2}}(p+1)^{U_p}\cdots\right)\cdot(U_1!\cdots U_{p-2}!U_p!\cdots) \tag{3.17}$$

does not contain $(p-1)$-st part. We denote the first and second sum of (3.15) by $\sum_1$ and $\sum_2$, respectively, and denote

$$=\sum\nolimits_1+\sum\nolimits_2=\sum_{w(U)=n}S_1(U)\quad+\sum_{r_0=1}^{a}\sum_{\substack{w(U)=n+r_0(p-1)\\ U_{p-1}=0}}S_2(U). \tag{3.18}$$

Then for $S_1(U)$ of U with $n = w(U)$, we have

$$\begin{aligned} w(U[r]) + d(U[r]) - 2 &= n + (p-1)r + d(U) + r - 2 \\ &= n + pr + d - 2 \\ &= (r + U_{p-1})p + n - pU_{p-1} + d(U) - 2. \end{aligned} \tag{3.19}$$

Here we note that

$$\begin{aligned} n - pU_{p-1} + d(U) - 2 &= \big(n - (p-1)U_{p-1}\big) + (d(U) - U_{p-1}) - 2 \\ &= w(U|_{p-1}) + d(U|_{p-1}) - 2. \end{aligned} \tag{3.20}$$

For $S_2(U)$ of U with $w(U) = n + r_0(p-1)$, we see

$$\begin{aligned} &w(U[r-r_0]) + d(U[r-r_0]) - 2 \\ &\quad = n + r_0(p-1) + (p-1)(r-r_0) + d(U) + (r-r_0) - 2 \\ &\quad = (r-r_0)p + n + r_0 p + d(U) - r_0 - 2. \end{aligned} \tag{3.21}$$

We divide $\sum_1$ (resp. $\sum_2$) into two parts according to $n - pU_{p-1} + d(U) - 2$ in (3.20) (resp. $n + r_0 p + d(U) - r_0 - 2$ in (3.21)) is $\geqq ap$ or $< ap$, and denote the sum as $\sum_1' + \sum_1''$ (resp. $\sum_2' + \sum_2''$). Here we pay attention in (3.20) that $n - pU_{p-1} + d(U) - 2 > 0$ because of $n \not\equiv 0 \bmod (p-1)$.

(a) For the sum $\sum_1'$, since $n - pU_{p-1} + d(U) - 2 \geqq ap$, we have

$$\begin{aligned} \mathrm{ord}_p(S_1(U)) &\geqq -\mathrm{ord}_p(\gamma_{U|_{p-1}}) + \mathrm{ord}_p((n - pU_{p-1} + d - 2)!) \\ &\geqq \left\lfloor \frac{n - pU_{p-1} + d(U) - 2}{2p} \right\rfloor \\ &\geqq \left\lfloor \frac{ap}{2p} \right\rfloor \\ &= \left\lfloor \frac{a}{2} \right\rfloor \end{aligned} \tag{3.22}$$

by 3.4(1) and 3.11.

(b) For the sum $\sum_1''$, we let $N = n - pU_{p-1} + d(U) - 2$ and $N = pb + e$ $(0 \leqq e < p)$. Then we see $b < a$ because $0 < n - pU_{p-1} + d(U) - 2 < ap$. Therefore, by 3.11, we have

$$\begin{aligned} &\mathrm{ord}_p(N!) - \mathrm{ord}_p(\gamma_{U|_{p-1}}) \\ &\quad = \mathrm{ord}_p((w(U|_{p-1}) + d(U|_{p-1}) - 2)!) - \mathrm{ord}_p(\gamma_{U|_{p-1}}) \\ &\quad = \mathrm{ord}_p(\tau_{U|_{p-1}}) \\ &\quad \geqq \lfloor N/(2p) \rfloor. \end{aligned} \tag{3.23}$$

This and 3.4(1) give

$$
\begin{aligned}
\mathrm{ord}_p(S_1(U)) &\geqq a - \left\lfloor \frac{N}{p} \right\rfloor + \mathrm{ord}_p(N!) - \left\lfloor \frac{a - \lfloor N/p \rfloor}{p} \right\rfloor - \mathrm{ord}_p(\gamma_{U|_{p-1}}) \\
&= \left\lfloor \frac{N}{2p} \right\rfloor + a - \left\lfloor \frac{N}{p} \right\rfloor - \left\lfloor \frac{a - \lfloor N/p \rfloor}{p} \right\rfloor \\
&\geqq \left\lfloor \frac{b}{2} \right\rfloor + a - b - \left\lfloor \frac{a-b}{p} \right\rfloor \\
&> \left(\frac{b}{2} - 1\right) - b + a - \frac{a-b}{p} \\
&= -1 + \frac{a}{2} - \frac{(a-b)(p-2)}{2p} \\
&= -1 + \frac{a}{2}.
\end{aligned} \tag{3.24}
$$

As the initial side is an integer, it must be $\geqq \lfloor a/2 \rfloor$. Hence $\mathrm{ord}_p(\sum_1) \geqq \lfloor a/2 \rfloor$. We can prove $\mathrm{ord}_p(\sum_2) \geqq \lfloor a/2 \rfloor$ by using 3.4(2) instead of 3.4(1). About such the proof, we should keep in mind that, for the case $n + r_0 p + d(U) - r_0 - 2 < ap$ in (3.21), in order to use 3.4(2), it must be $n + r_0 p + d(U) - r_0 - 2 \geqq r_0 p$. However, since $d(U) \geqq 1$, this condition is satisfied if $n + r_0 p + 1 - r_0 - 2 \geqq r_0 p$, namely, $n - r_0 - 1 \geqq 0$. The latest condition is valid for all $r_0 = 1, \cdots, a$ because of our assumption $n > a$.

Remark 3.25. If we replace the condition $a < n$ in 3.1 by $a = n$, the Kummer-type congruence relation for the generalized Bernoulli-Hurwitz numbers described later holds only modulo p^{n-1}. We can see by numerical computation that the modulus of such congruence is best possible. This means that the condition $a < n$ in 3.1 is essential because the generalized Bernoulli-Hurwitz numbers are given by a specialization of the universal Bernoulli numbers.

3.5 The Kummer-Adelberg congruence relation

We prove the congruence relation 3.3 of Adelberg by using 3.1 and 3.2(1).

Proof. (of 3.3) We note that if $p = 3$, the condition $n \neq 0, 1 \bmod (p-1)$ is always false and the statement of 3.3 is vacuous. So that, we may suppose $p \geqq 5$. We prove the congruence relation by induction on a. As we already mentioned the case $a = 1$ in 3.2(1), we assume $a > 1$. By taking p^{a-1} as a in 3.1, we see

$$
\sum_{r=0}^{p^{a-1}} (-1)^r \binom{p^{a-1}}{r} {f_{p-1}}^{p^{a-1}-r} \frac{\hat{B}_{n+r(p-1)}}{n + r(p-1)} \equiv 0 \mod p^{\lfloor p^{a-1}/2 \rfloor}. \tag{3.26}
$$

Here, we have $\lfloor p^{a-1}/2 \rfloor > a$ since $a \geqq 2$ and $p \geqq 5$. If $r \neq 0$ and $r \neq p^{a-1}$, then

$$
\begin{aligned}
\mathrm{ord}_p \binom{p^{a-1}}{r} &= \frac{S_p(p^{a-1} - r) + S_p(r) - S_p(p^{a-1})}{p-1} \\
&= \frac{S_p(p^{a-1} - r) + S_p(r) - 1}{p-1}
\end{aligned} \tag{3.27}
$$

by (1.2). We denote $\nu = \mathrm{ord}_p r$. Let

$$p^{a-1} - r = d_{a-2}p^{a-2} + d_{a-3}p^{a-3} + \cdots + d_1 p + d_0 \qquad (0 \leqq d_j \leqq p-1),$$
$$r = h_{a-2}p^{a-2} + h_{a-3}p^{a-3} + \cdots + h_1 p + h_0 \qquad (0 \leqq h_j \leqq p-1)$$

be their p-base digit expressions. Then, obviously,

$$d_j + h_j = \begin{cases} p-1, & (a-2 \geqq j \geqq \nu+1), \\ p, & (j = \nu), \\ 0, & (\nu - 1 \geqq j \geqq 0). \end{cases} \tag{3.28}$$

Namely, $S_p(p^{a-1} - r) + S_p(r) = (p-1)(a-2-\nu) + p$. Thus $\mathrm{ord}_p\binom{p^{a-1}}{r} = a - 1 - \nu$. Keeping in mind that p is an odd number, and consider the sum

$$\begin{aligned} D_r = (-1)^r \binom{p^{a-1}}{r} {f_{p-1}}^{p^{a-1}-r} \frac{\hat{B}_{n+r(p-1)}}{n + r(p-1)} \\ + (-1)^{p^{a-1}-r} \binom{p^{a-1}}{p^{a-1}-r} {f_{p-1}}^{r} \frac{\hat{B}_{n+(p^{a-1}-r)(p-1)}}{n + (p^{a-1}-r)(p-1)} \end{aligned} \tag{3.29}$$

for $0 < r \leqq (p^{a-1}-1)/2$. Summing up consideration above, we see that D_r is divisible by p^a by using the assumption of induction on $\nu = \mathrm{ord}_p r = \mathrm{ord}_p(p^{a-1} - r)(< a)$. Since

$${f_{p-1}}^{p^{a-1}} \cdot \frac{\hat{B}_n}{n} - \frac{\hat{B}_{n+p^{a-1}(p-1)}}{n + p^{a-1}(p-1)}$$

is difference of the left hand side of (3.26) and

$$\sum_{r=1}^{p^{a-1}-1} D_r.$$

Hence 3.3. □

4 Hyperelliptic functions

4.1 Fundamentals on hyperelliptic functions

We consider a hyperellptic curve $\mathscr{C}$ of genus g that is defined by $y^2 = f(x)$, where

$$f(x) = \lambda_0 x^{2g+1} + \lambda_1 x^{2g} + \cdots + \lambda_{2g+1}$$

is a polynomial of x over $\mathscr{C}$, and $f(x) = 0$ has no multiple roots. We set $\lambda_0 = 1$ for our convenience. The curve $\mathscr{C}$ is regarded as a non-singular algebraic curve with unique point ∞ at infinity. As is well-known, the set of

$$\frac{x^{j-1}dx}{2y} \quad (j = 1, \ldots, g) \tag{4.1}$$

forms a basis of the differential forms of the first kind on $\mathscr{C}$. Let $[\omega'\ \omega'']$ be the period matrix defined by taking a suitable set of generators of the fundamental group of $\mathscr{C}$, and let

$$\Lambda := \omega'^t\Big[\mathbf{Z}\ \ \mathbf{Z}\ \ \cdots\ \ \mathbf{Z}\Big] + \omega''^t\Big[\mathbf{Z}\ \ \mathbf{Z}\ \ \cdots\ \ \mathbf{Z}\Big]\ (\subset \mathbf{C}^g)$$

be the lattice in $\mathbf{C}^g$ with respect to the differentials (4.1). We denote by J the jacobian variety of $\mathscr{C}$, and by $\mathrm{Sym}^g(\mathscr{C})$ the symmetric product of g copies of $\mathscr{C}$. Then we have a birational map

$$\mathrm{Sym}^g(\mathscr{C}) \to \mathrm{Pic}^\circ(\mathscr{C}) = J$$
$$(P_1, \ldots, P_g) \mapsto \text{the class of } P_1 + \cdots + P_g - g\cdot\infty.$$

We identify J as analytic manifolds with $\mathbf{C}^g/\Lambda$. We denote the natural map $\mathbf{C}^g \mapsto \mathbf{C}^g/\Lambda = J$ by κ. The map

$$\iota : Q \mapsto Q - \infty$$

is an embedding of $\mathscr{C}$ into J. The pull-back $\kappa^{-1}\iota(\mathscr{C})$ of ι with respect to κ is a *universal Abelian covering* of the curve $\mathscr{C}$. The birational map above sends the each element $(P_1, \cdots, P_g) \in \mathrm{Sym}^g(\mathscr{C})$ to the point $\boldsymbol{u} \mod \Lambda \in \mathbf{C}^g/\Lambda$, where

$$\boldsymbol{u} = (u_1, \ldots, u_g) = \left(\int_\infty^{P_1} + \cdots + \int_\infty^{P_g}\right)(\omega_1,\ \ldots,\ \omega_g). \tag{4.2}$$

The following notational convention is important.
Convention : In this paper, we denote u_g simply by u.

4.2 The hyperelliptic functions and their variable

In this paper, for each point $\boldsymbol{u} \in \kappa^{-1}\iota(\mathscr{C})$, we denote by

$$(x(\boldsymbol{u}),\ y(\boldsymbol{u}))$$

the coordinate (x, y) of $\mathscr{C}$ such that $\kappa(\boldsymbol{u}) = \iota\,(x(\boldsymbol{u}),\ y(\boldsymbol{u}))$. We call a rational expression in terms of $x(\boldsymbol{u})$ and $y(\boldsymbol{u})$ hyperelliptic function, and is regarded also as a function on $\kappa^{-1}\iota(\mathscr{C})$. We confirm the following fundamental fact.

Lemma 4.3. *The lowest degree terms of the Laurent developments of $x(\boldsymbol{u})$ and $y(\boldsymbol{u})$ at $\boldsymbol{u} = (0, \cdots, 0)$ with respect to $u = u_g$ is given by*

$$x(\boldsymbol{u}) = \frac{1}{u^2} + (d^\circ(u) \geqq 0), \quad y(\boldsymbol{u}) = -\frac{1}{u^{2g+1}} + (d^\circ(u) \geqq -2g+1).$$

Proof. We take $t = \dfrac{1}{\sqrt{x}}$ as a local parameter at ∞. Here we consider the brunch such that $t > 0$ for $x > 0$. We suppose that $u \in \kappa^{-1}\iota(\mathscr{C})$ is sufficiently near to $(0, 0, \ldots, 0)$,

and that the three kinds of coordinates t, $\boldsymbol{u}=(u_1,\dots,u_g)$, (x,y) correspond to the same point of $\mathscr{C}$. Then

$$u=u_g=\int_\infty^{(x,y)}\frac{x^{g-1}dx}{2y}=\int_\infty^{(x,y)}\frac{x^{-3/2}dx}{2\sqrt{1+\lambda_1\frac{1}{x}+\cdots+\lambda_{2g+1}\frac{1}{x^{2g+1}}}}$$
$$=\int_0^t\frac{t^3\cdot\left(-\frac{2}{t^3}\right)dt}{2+(d^\circ\geqq 1)}=-t+(d^\circ(t)\geqq 2).$$

Thus $x(\boldsymbol{u})=\frac{1}{u^2}+(d^\circ(u)\geqq -1)$. The similar fact is shown for $y(\boldsymbol{u})$. By the definition, we see $x(-\boldsymbol{u})=x(\boldsymbol{u})$, $y(-\boldsymbol{u})=-y(\boldsymbol{u})$ The proof have been completed. □

The following properties are shown by the similar argument and omit their proofs.

LEMMA 4.4. *Let $\boldsymbol{u}=(u_1,u_2,\dots,u_g)$ be a variable on $\kappa^{-1}\iota(\mathscr{C})$. Then*

$$u_1=\tfrac{1}{2g-1}{u_g}^{2g-1}+(d^\circ(u_g)\geqq 2g),$$
$$u_2=\tfrac{1}{2g-3}{u_g}^{2g-3}+(d^\circ(u_g)\geqq 2g-2),$$
$$\cdots\cdots\cdots$$
$$u_{g-1}=\tfrac{1}{3}{u_g}^{3}+(d^\circ(u_g)\geqq 4).$$

These facts suggest that *it is natural to take $u=u_g$ as the variable for the hyperelliptic functions in a vicinity of the point $\boldsymbol{u}=(0,\cdots,0)$.*

5 Differential equations

5.1 General setting

For the hyperelliptic curve $y(\boldsymbol{u})^2=f\big(x(\boldsymbol{u})\big)$ (f is a separable polynomial of degree $2g+1$), the definition of $u=u_g$ gives

$$\frac{du}{dx}(\boldsymbol{u})=\frac{x^{g-1}}{2y}(\boldsymbol{u}). \tag{5.1}$$

After squaring this, substituting the defining equation above of $\mathscr{C}$ into it, we have $\left(\frac{du}{dx}\right)^2=\frac{x^{2g-2}}{4f}$. Namely,

$$x(\boldsymbol{u})^{2g-2}x'(\boldsymbol{u})^2=4f\big(x(\boldsymbol{u})\big)\quad(\ '\text{ means }\tfrac{d}{du}\ ). \tag{5.2}$$

This (5.2) is just the analogy of $\wp'(u)^2=4\wp(u)^3-g_2\wp(u)-g_3$ in our theory[3]. Now we define the numbers C_n by the Laurent development of $x(\boldsymbol{u})$ with respect to u:

$$x(\boldsymbol{u})=\frac{1}{u^2}+\frac{c_{-1}}{u}+\sum_{n=2}^{\infty}\frac{C_n}{n}\frac{u^{n-2}}{(n-2)!} \tag{5.3}$$

[3]Carlitz studied in [Ca4] about the solution of the differential equation $\left(\frac{dx}{du}(u)\right)^2=$ "a degree six polynomial of $x(u)$" ($u\in\mathbf{C}$) instead of $\wp'(u)^2=4\wp(u)^3-g_2\wp(u)-g_3$.

These C_n are analogy of Bernoulli and Hurwitz numbers. Though the definition of Bernoulli and Hurwitz numbers are based on the determination of their 2-parts, such the property is a problem in the future for our theory. Of course, the recursion relation for C_n is obtained from (5.1.2). For the function $y(\boldsymbol{u})$, we define also the numbers D_n by its Laurent expansion at $u = 0$ of $y(\boldsymbol{u})$ with respect to u:

$$y(\boldsymbol{u}) = \frac{-1}{u^{2g+1}} + \frac{d_{-2g}}{u^{2g}} + \cdots + \frac{d_{-1}}{u} + \sum_{n=2g+1}^{\infty} \frac{D_n}{n} \frac{u^{n-2g-1}}{(n-2g-1)!}. \tag{5.4}$$

Since the differential equation for $y(\boldsymbol{u})$ is given by $du = x^{g-1}dx/2y$, we also have the recursion relation for D_n. We shall call C_ns and D_ns it generalized Bernoulli-Hurwitz numbers.

5.2 The case of $y(\boldsymbol{u})^2 = x(\boldsymbol{u})^{2g+1} - 1$

In this case (5.2) is

$$x(\boldsymbol{u})^{2g-2}x'(\boldsymbol{u})^2 = 4x^{2g+1}(\boldsymbol{u}) - 4 \qquad (\ ' \text{ means } \tfrac{d}{du}\ ). \tag{5.5}$$

This is a generalization of $\wp'(u)^2 = 4\wp(u)^3 - 1$. Here, we describe automorphisms of this curve $\mathscr{C} : y^2 = x^{2g+1} - 1$ and its Jacobian variety J. Let $\zeta = e^{2\pi\sqrt{-1}/(2g+1)}$, Then $\mathscr{C}$ has automorphisms

$$\pm\lceil\zeta^j\rceil : \mathscr{C} \to \mathscr{C}, \quad (x, y) \mapsto (\zeta^j x, \pm y) \quad (j = 0, \cdots, 2g)$$

They induce automorphisms of $\mathrm{Pic}^\circ(\mathscr{C})$ by

$$\pm\lceil\zeta^j\rceil : P_1 + \cdots + P_g - g\infty \mapsto (\pm\lceil\zeta^j\rceil)P_1 + \cdots + (\pm\lceil\zeta^j\rceil)P_g - g\infty$$

where P_1, $\cdots$, $P_g \in \mathscr{C}$; and also give automorphisms of J. From (4.1) and (4.2), we see

$$-\lceil\zeta\rceil(u_1, u_2, \cdots, u_g) = (-\zeta u_1, -\zeta^2 u_2, \cdots, -\zeta^g u_g).$$

Namely,

$$x(-\lceil\zeta\rceil\boldsymbol{u}) = \zeta x(\boldsymbol{u}), \quad y(-\lceil\zeta\rceil\boldsymbol{u}) = -y(\boldsymbol{u}) \tag{5.6}$$

Therefore, if n is not divisible by $2(2g + 1)$, then $C_n = D_n = 0$.

5.3 The case of $y(\boldsymbol{u})^2 = x(\boldsymbol{u})^{2g+1} - x(\boldsymbol{u})$

In this case, (5.2) is

$$x(\boldsymbol{u})^{2g-2}x'(\boldsymbol{u})^2 = 4x^{2g+1}(\boldsymbol{u}) - 4x(\boldsymbol{u}) \qquad (\ ' \text{ means } \tfrac{d}{du}\ ). \tag{5.7}$$

This is a generalization of $\wp'(u)^2 = 4\wp(u)^3 - 4\wp(u)$. We describe automorphisms of this curve $\mathscr{C} : y^2 = x^{2g+1} - x$ and its Jacobian J. Let $\zeta = e^{2\pi\sqrt{-1}/(2g)}$. Then $\mathscr{C}$ has sutomorphisms

$$\lceil\zeta^j\rceil : \mathscr{C} \to \mathscr{C}, \quad (x, y) \mapsto (\zeta^{2j}x, \zeta^j y) \quad (j = 0, \cdots, 2g).$$

They induce automorphisms of $\mathrm{Pic}^\circ(\mathscr{C})$ by

$$\pm\lceil\zeta^j\rceil : P_1 + \cdots + P_g - g\infty \mapsto (\pm\lceil\zeta^j\rceil)P_1 + \cdots + (\pm\lceil\zeta^j\rceil)P_g - g\infty$$

where P_1, $\cdots$, $P_g \in \mathscr{C}$; and also give automorphisms of J. From (4.1) and (4.2), we see

$$\lceil\zeta\rceil(u_1, u_2, \cdots, u_g) = (\zeta u_1, \zeta^3 u_2, \cdots, \zeta^{2g-1}u_g).$$

Namely,

$$x(\lceil\zeta\rceil\boldsymbol{u}) = \zeta^2 x(\boldsymbol{u}), \quad y(\lceil\zeta\rceil\boldsymbol{u}) = \zeta y(\boldsymbol{u}). \tag{5.8}$$

Therefore, if n is coprime to $4g$, then $C_n = D_n = 0$.

6 von Staudt theorems in algebraic functions

6.1 The case of $y(\boldsymbol{u})^2 = x(\boldsymbol{u})^{2g+1} - 1$

In this case Clarke type theorems for $C_{(4g+2)n}$ and $D_{(4g+2)n}$ are stated as follows:

THEOREM 6.1. *For each numbers $C_{(4g+2)n}$ and $D_{(4g+2)n}$ defined in* (5.3) *and* (5.4)*, respectively, for the curve $y^2 = x^{2g+1} - 1$, we have*

$$\frac{C_{(4g+2)n}}{(4g+2)n} \equiv -\sum_{\substack{p\equiv 1 \bmod (2g+1)\\ (4g+2)n = a(p-1)}} \frac{a|_p{}^{-1} \bmod p^{1+\mathrm{ord}_p a}}{p^{1+\mathrm{ord}_p a}} A_p{}^a \mod \mathbf{Z},$$

$$\frac{D_{(4g+2)n}}{(4g+2)n} \equiv -\sum_{\substack{p\equiv 1 \bmod (2g+1)\\ (4g+2)n = a(p-1)}} \frac{((2g)!a)|_p{}^{-1} \bmod p^{1+\mathrm{ord}_p a}}{p^{1+\mathrm{ord}_p a}} A_p{}^a \mod \mathbf{Z},$$

where $A_p = (-1)^{(p-1)/(4g+2)} \cdot \binom{(p-1)/2}{(p-1)/(4g+2)}$.

Obviously, these results show the following extensions of von Staudt-Clausen theorem and von Staudt second theorem for $C_{(4g+2)n}$ and $D_{(4g+2)n}$.

COROLLARY 6.2. (1) *For each numbers $C_{(4g+2)n}$ and $D_{(4g+2)n}$, there are rational integers $G_{(4g+2)n}$ and $H_{(4g+2)n}$ such that*

$$C_{(4g+2)n} = \sum_{\substack{p\equiv 1 \bmod (2g+1)\\ p-1 | (4g+2)n}} \frac{A_p{}^{(4g+2)n/(p-1)}}{p} + G_{(4g+2)n},$$

$$D_{(4g+2)n} = \sum_{\substack{p\equiv 1 \mod (2g+1)\\ p-1|(4g+2)n}} \frac{((2g)!^{-1} \bmod p)\ {A_p}^{(4g+2)n/(p-1)}}{p} \ + \ H_{(4g+2)n},$$

where A_p is the same one defined in 6.1.
(2) *If $(p-1) \not| (4g+2)n$, then $C_{(4g+2)n}/((4g+2)n)$ and $D_{(4g+2)n}/((4g+2)n)$ belong to $\mathbf{Z}_p$.*

PROOF. Let $p \equiv 1 \bmod (2g+1)$, $(4g+2)m = a(p-1)$, and $\mathrm{ord}_p a = \nu$. Then

$$\frac{(4g+2)m \cdot \left(a|_p{}^{-1} \bmod p^{1+\nu}\right)}{p^{1+\nu}} \equiv 1 - \frac{1}{p} \equiv -\frac{1}{p} \mod \mathbf{Z}.$$

This yields the results. □

6.2 The case of $y(\boldsymbol{u})^2 = x(\boldsymbol{u})^{2g+1} - x(\boldsymbol{u})$

In this case, Clarke type theorem for C_{4gn} and D_{4gn} are stated as follows:

THEOREM 6.3. *For each numbers C_{4gn} and D_{4gn} defined in* (5.3) *and* (5.4)*, respectively, for the curve $y^2 = x^{2g+1} - x$, we have*

$$\frac{C_{4gn}}{4gn} \equiv -\sum_{\substack{p\equiv 1 \mod 4g\\ 4gn=a(p-1)}} \frac{a|_p{}^{-1} \bmod p^{1+\mathrm{ord}_p a}}{p^{1+\mathrm{ord}_p a}} {A_p}^a \mod \mathbf{Z},$$

$$\frac{D_{4gn}}{4gn} \equiv -\sum_{\substack{p\equiv 1 \mod 4g\\ 4gn=a(p-1)}} \frac{((2g)!a)|_p{}^{-1} \bmod p^{1+\mathrm{ord}_p a}}{p^{1+\mathrm{ord}_p a}} {A_p}^a \mod \mathbf{Z},$$

where $A_p = (-1)^{(p-1)/(4g)} \cdot \binom{(p-1)/2}{(p-1)/(4g)}$.

These results also show the following extensions of von Staudt-Clausen theorem and von Staudt second theorem for C_{4gn} and D_{4gn}.

COROLLARY 6.4. (1) *For each numbers C_{4gn} and D_{4gn}, there are integers G_{4gn} and H_{4gn} such that*

$$C_{4gn} = \sum_{\substack{p\equiv 1 \mod 4g\\ p-1|4gn}} \frac{{A_p}^{4gn/(p-1)}}{p} \ + \ G_{4gn},$$

$$D_{4gn} = \sum_{\substack{p\equiv 1 \mod 4g\\ p-1|4gn}} \frac{((2g)!^{-1} \bmod p)\ {A_p}^{4gn/(p-1)}}{p} \ + \ H_{4gn},$$

where A_p is the same one defined in 6.3.
(2) *If $(p-1) \not| 4gn$, then $C_{4gn}/(4gn)$ and $D_{4gn}/(4gn)$ belong to $\mathbf{Z}_p$.*

PROOF. Similar to 6.2. □

6.3 A remark on A_p

Let p be a prime number such that $p \equiv 1 \bmod (2g+1)$ or $p \equiv 1 \bmod 4g$ according to that $\mathscr{C}$ is defined by $y^2 = x^{2g+1} - 1$ or $y^2 = x^{2g+1} - x$.

We take the set of (4.1), namely

$$\Big(\frac{1}{2y},\ \frac{x}{2y},\ \cdots,\ \frac{x^{g-1}}{2y}\Big)$$

as the basis of the differential forms of the first kind on $\mathscr{C}$ mod p. Then the Hasse-Witt matrix ($g \times g$ matrix) with respect to this basis is a diagonal matrix ([Yu], p.381), and its (g,g)-entry is just the number A_p. Katz pointed out in the case of Hurwitz numbers that A_p is equal to the Hasse invariant (the unique entry of the Hasse-Witt matrix!) [Ka1], p.2. Our results are quite natural extension of that fact.

7 Kummer congruences in algebraic functions

7.1 The case of $y(\boldsymbol{u})^2 = x(\boldsymbol{u})^{2g+1} - 1$

In this case, Kummer's original type congruence relations for $C_{(4g+2)n}$ and $D_{(4g+2)n}$ are stated as follows:

THEOREM 7.1. *Let $C_{(4g+2)n}$ and $D_{(4g+2)n}$ be the numbers defined in* (5.3) *and* (5.4)*, respectively, for the curve $y^2 = x^{2g+1} - 1$. For a prime $p \equiv 1 \bmod (2g+1)$ and positive integers a and n such that $(4g+2)n - 2 \geqq a$, if $(p-1) \not| (4g+2)n$, then we have*

$$\sum_{r=0}^{a} \binom{a}{r} (-A_p)^{a-r} \cdot \frac{C_{(4g+2)n+r(p-1)}}{(4g+2)n + r(p-1)} \equiv 0 \mod p^a \mathbf{Z}_{(p)}, \tag{7.2}$$

$$\sum_{r=0}^{a} \binom{a}{r} (-A_p)^{a-r} \cdot \frac{D_{(4g+2)n+r(p-1)}}{(4g+2)n + r(p-1)} \equiv 0 \mod p^a \mathbf{Z}_{(p)}, \tag{7.3}$$

where

$$A_p = (-1)^{(p-1)/(4g+2)} \cdot \binom{(p-1)/2}{(p-1)/(4g+2)}.$$

These congruence relations are just the same form as in Kummer's original paper [Ku] and in the case of Hurwitz numbers [L], p.193, (26).

REMARK 7.4. (1) Under the facts (10.1), (10.2), and (10.3) proved later, we understand that 7.1 is satisfied modulo $p^{\lfloor a/2 \rfloor}$.
(2) If we replace the condition $(4g+2)n-2 \geqq a$ in 7.1 by $(4g+2)n-2 < a$ the congruence relation seems to stand up modulo p^{n-1} and this modulus is best possible.

7.2 The case of $y(\boldsymbol{u})^2 = x(\boldsymbol{u})^{2g+1} - x(\boldsymbol{u})$

In this case, the Kummer's original type congruence relations for C_{4gn} and D_{4gn} are stated as follows:

THEOREM 7.5. *Let C_{4gn} and D_{4gn} be the numbers defined in* (5.3) *and* (5.4)*, respectively, for the curve $y^2 = x^{2g+1} - x$. For a prime $p \equiv 1 \bmod 4g$ and positive integers a and n satisfying $4gn - 2 = a$, if $(p-1) \not| 4gn$, then we have*

$$\sum_{r=0}^{a} \binom{a}{r} (-A_p)^{a-r} \cdot \frac{C_{4gn+r(p-1)}}{4gn + r(p-1)} \equiv 0 \mod p^a \mathbf{Z}_{(p)},$$
$$\sum_{r=0}^{a} \binom{a}{r} (-A_p)^{a-r} \cdot \frac{D_{4gn+r(p-1)}}{4gn + r(p-1)} \equiv 0 \mod p^a \mathbf{Z}_{(p)},$$

where

$$A_p = (-1)^{(p-1)/(4g)} \cdot \binom{(p-1)/2}{(p-1)/(4g)}.$$

These relations are also the same form as in the original [Ku] for the Bernoulli numbers and [L], p.193, (23) for the Hurwitz numbers.

REMARK 7.6. By the easily shown simple facts (11.1), (11.2), (11.3) proved later, we see that 7.5 is satisfied modulo $p^{\lfloor a/2 \rfloor}$.

8 Hurwitz-integral series

8.1 Definition and basic properties

We describe here the notion of Hurwitz integrality and its properties. In this subsection the letter R always means a subring of the field $\mathbf{Q}_p$ of the p-adic numbers for a fixed prime p. In our practice, R will be $\mathbf{Z}[\frac{1}{q}]$ with non-zero integer q, the localization $\mathbf{Z}_{(p)}$ of the integer ring $\mathbf{Z}$ at p, or its p-adic completion $\mathbf{Z}_p$.

DEFINITION 8.1. Let z be an indeterminate or a variable. Let

$$h(z) = \sum_{n=0}^{\infty} h_n \frac{z^n}{n!} \quad (\ h_n \in \mathbf{Q}_p\ )$$

be a power series with respect to z. If all the coefficients h_n belong to R, then we say $h(z)$ is of Hurwitz integral over R. The ring consists of the Hurwitz-integral series over R with respect to z is denoted by $R\langle\langle z \rangle\rangle$.

The ring $R\langle\langle z \rangle\rangle$ is an integral domain, and is closed under the operations d/dz and $\int_0^z \cdot\, dz$. A series $h(z) \in R\langle\langle z \rangle\rangle$ is a unit in $R\langle\langle z \rangle\rangle$ if and only if its constant term is a unit in R. Moreover the following properties are easily shown (see [Hu2], Section 1).

PROPOSITION 8.2. *Let*

$$h(z) = \sum_{n=0}^{\infty} h_n \frac{z^n}{n!} \quad (\ h_n \in \mathbf{Q}_p \ ).$$

(1) *If the first n coefficients $h_0, \cdots, h_{n-1}$ belong to R, and there is a polynomial F of n variables over R such that there exists a relation*

$$h^{(n)}(z) = F(h(z), h'(z), \cdots, h^{(n-1)}(z))$$

on derivatives of $h(z)$, then $h(z) \in R\langle\langle z \rangle\rangle$.
(2) *If $h(z) \in R\langle\langle z \rangle\rangle$, $h_0 = 0$, and $h_1 = 1$, then the formal inverse series*

$$z = h^{-1}(w) = w + \cdots$$

of $w = h(z)$ also belongs to $R\langle\langle z \rangle\rangle$.
(3) *If $h(z) \in R\langle\langle z \rangle\rangle$, $h_0 = 0$, and $h_1 = 1$, then for any positive integer m,*

$$\frac{h(z)^m}{m!}$$

also belongs to $R\langle\langle z \rangle\rangle$.

8.2 Hurwitz-integrality of $x(\boldsymbol{u})^{1/2}$

Here, we check the following fact.

PROPOSITION 8.3. *On the curve $y^2 = x^{2g+1} - 1$ or $y^2 = x^{2g+1} - x$, we have*

$$t := -1/x(\boldsymbol{u})^{1/2} \ \ (= u + \cdots) \in \mathbf{Z}\langle\langle u \rangle\rangle.$$

PROOF. For simplicity, we restrict the argument within only the curve $y^2 = x^5 - 1$. We denote simply $t' = dt/du$, $t'' = d^2t/du^2$, $\cdots$. By (5.5), we see

$$(t')^2 = 1 - t^{10}. \tag{8.4}$$

After differentiating this by u, dividing by $2t'$, we have

$$t'' = -5t^9. \tag{8.5}$$

Since $t(0) = t'(0) = 0$, 8.2(1) yields that

$$1/x^{1/2}(\boldsymbol{u}) = -u + 5 \cdot 9! \ \frac{u^{11}}{11!} + \cdots \in \mathbf{Z}\langle\langle u \rangle\rangle \tag{8.6}$$

for the curve $y^2 = x^5 - 1$. □

8.3 Hurwitz-integrality of $1/y^{1/5}(\boldsymbol{u})$

We show the following fact.

PROPOSITION 8.7. *On the curve $y^2 = x^{2g+1} - 1$ or $y^2 = x^{2g+1} - x$, we have*

$$s := -1/y(\boldsymbol{u})^{1/(2g+1)} (= u + \cdots) \ \in \ \mathbf{Z}\langle\langle u \rangle\rangle.$$

PROOF. We restrict again the argument within only the curve $y^2 = x^5 - 1$. By (5.1), we see that

$$du = \frac{xdx}{2y} = \frac{x\frac{dx}{dy}dy}{2y} = \frac{xdy}{2y\frac{dy}{dx}} = \frac{xdy}{5x^4} = \frac{dy}{5x^3} = \frac{dy}{5(y^2+1)^{3/5}}, \tag{8.8}$$

and

$$\frac{dy}{du} = 5(y^2+1)^{3/5}. \tag{8.9}$$

Writing simply $s' = ds/du$, $s'' = d^2s/du^2$, $\cdots$, we have $dy/du = -5s^{-6}ds/du$. Hence

$$s' = -(1+s^{10})^{3/5}. \tag{8.10}$$

This formula gives the following equation by induction: For each integer $n \geqq 1$, the n-th derivative of s is written as a finite sum of the form

$$s^{(n)} = \sum_j (1+s^{10})^{L_{nj}/5} P_{nj}(s, s', s'', \cdots, s^{(n-1)}), \tag{8.11}$$

where each P_{nj} means a polynomial of n variables over $\mathbf{Z}$, and L_{nj} is an integer. Summing up this and $s(0) = 0$, we see that $s'(0)$, $s''(0)$, $s^{(3)}(0)$, $\cdots$ are all integers. Therefore we conclude that

$$1/y(\boldsymbol{u})^{1/5} = -u - 48 \cdot 9! \ \frac{u^{11}}{11!} + \cdots \in \mathbf{Z}\langle\langle u \rangle\rangle \tag{8.12}$$

for the curve $y^2 = x^5 - 1$. □

9 Outline of the proof

We sketch the proofs of 6.1 and 7.1 (also of 6.3 and 7.5) by taking the case of the curve $y^2 = x^5 - 1$ as an example. Recall our convention that, for a given power series $\varphi(z)$ with respect to z, each coefficient $\left[\frac{z^n}{n!}\right]\varphi(z)$ ($n \geqq 0$) is called a *Hurwitz coefficient* of it. In the following, any Hurwitz coefficients are those of developments with respect to u.

9.1 The von Staudt theorems in algebraic functions

The proof of Theorem 6.1 is divided into the following three steps:

1. *To prove the Clarke type theorem for the Hurwitz coefficients C_n/n of $x(\boldsymbol{u})$ over $\mathbf{Z}[\frac{1}{2}]$.*
2. *To prove the Clarke type theorem for the Hurwitz coefficients D_n/n of $y(\boldsymbol{u})$ over $\mathbf{Z}[\frac{1}{5}]$.*
3. *To make a connection of the results above. By using simple formulae concerning $D = d/du$ among the functions $x(\boldsymbol{u})$, $x^2(\boldsymbol{u})$, $y(\boldsymbol{u})$, we can connect the Hurwitz coefficients of these functions, and show both results in Steps* **1** *and* **2** *are valid over $\mathbf{Z} = \mathbf{Z}[\frac{1}{2}] \cap \mathbf{Z}[\frac{1}{5}]$.*

More detailed outline is as follows.

Step 1: We prove the Clarke style theorem (10.7) for the Hurwitz coefficients $C^{(1)}_{10m}/(10m)$ of $x^{1/2}(\boldsymbol{u})$ over $\mathbf{Z}[\frac{1}{2}]$. In the next stage, we show relations between the Hurwitz coefficients of $x(\boldsymbol{u})$ and $x^{1/2}(\boldsymbol{u})$, $x^{3/2}(\boldsymbol{u})$ and $x(\boldsymbol{u})$, and $x^2(\boldsymbol{u})$ and $x^{3/2}(\boldsymbol{u})$. These are (10.11) for $k = 1, 2, 3$. These relations yield the Clarke style theorems for these Hurwitz coefficients over $\mathbf{Z}[\frac{1}{2}]$ by using the integrality property (10.3) of the Carlitz coefficients (see the Convention) of the formal inverse series u with respect to $t = x^{-1/2}(\boldsymbol{u})$.

The Clarke style theorem above for the Hurwitz coefficients of $x^2(\boldsymbol{u}) = \left(x^{1/2}(\boldsymbol{u})\right)^4$ (namely, (10.15)) is important in Step 3.

Step 2: In 11.1, we prove the Clarke style theorem (11.7) for the Hurwitz numbers $D^{(1)}_{10m}/(10m)_4$ of $y^{1/5}(\boldsymbol{u})$ by using the integrality (11.3) of the Carlitz coefficients of the formal inverse series u with respect to $s = y^{-1/5}(\boldsymbol{u})$. On the other hand, we show that the relation (11.11) for $k = 1, 2, 3, 4$, namely, the relations between the Hurwitz coefficients of $y^{(k+1)/5}(\boldsymbol{u})$ and those of $y^{k/5}(\boldsymbol{u})$, for $k = 1, 2, 3, 4$. They are (11.11).

Summing up these, we can connect the Hurwitz coefficients $D_{10m}/(10m)$ of $y(\boldsymbol{u}) = \left(y^{1/5}(\boldsymbol{u})\right)^5$ to $D^{(1)}_{10m}/(10m)$ (see (11.12) and (11.13)). Therefore we have the relation (11.14) for $D_{10m}/(10m)$ over $\mathbf{Z}[\frac{1}{5}]$, and finish the Step 2.

Step 3: Let $D = d/du$. We can show by using

$$(Dx^2)(\boldsymbol{u}) = 4y(\boldsymbol{u})$$

that D_{10m} and $C^{(4)}_{10m}$ are essentially the same numbers. Since $D_{10m}/(10m) \in \mathbf{Z}_{(2)}$, the denominator of $C^{(4)}_{10m}/(10m)_4$ contains neither a power of 2 nor of 5. Hence, we have the relation (12.4) for $D_{10m}/(10m)$ over $\mathbf{Z}$, namely the second formula in 6.1. Finally, the formula

$$D^2x(\boldsymbol{u}) = 6x^2(\boldsymbol{u}) + \frac{4}{x^3(\boldsymbol{u})}$$

with $D = d/du = (2y/x)d/dx$, and the Hurwitz-integrality (8.6) of $1/x^3(\boldsymbol{u})$ connect $C^{(4)}_{10m}/(10m)_4$ with $C_{10m}/(10m)$. So that we have the desired theorem for $C_{10m}/(10m)$ which is a specialization of Clarke's theorem 2.9.

There is also a congruence in [Ad1], Theorem 3.4 connecting various order universal Bernoulli numbers, the universal case of Hurwitz coefficients of various powers of $1/t(u)$ with respect to u. While the author believe it would closely relate to our method, he could not use it.

9.2 The Kummer congruences in algebraic functions

Let $p \equiv 1 \bmod 5$ be a fixed prime number. Although we describe only about C_{10m}, the theorem for D_{10m} is proved similarly. The outline of the proof is as follows.

Step 1: We show that the formal inverse series $u(t) \in \mathbf{Z}_p\langle\langle t\rangle\rangle$ of $u \mapsto t = x(\boldsymbol{u})^{-1/2}$ satisfies the Honda's criterion that is Lemma 13.10. This fact implies the formal group law F whose formal logarithm is $u(t)$, namely

$$F(t_1, t_2) := u^{-1}(u(t_1) + u(t_2))$$

is defined over $\mathbf{Z}_p$ (see 13.1).

Step 2: By using Hochshild's formula and Honda's property (13.10), we see that

$$\Big(\big(\tfrac{d}{du}\big)^p - A_p \tfrac{d}{du}\Big) t(u) \in p\mathbf{Z}_p[[t(u)]] \tag{9.1}$$

for $t = t(u) = x(\boldsymbol{u})^{-1/2} \in \mathbf{Z}_p\langle\langle u\rangle\rangle$, in 13.2.

Step 3: Let $\xi \in \mathbf{Z}_p$ be a primitive $(p-1)$-st root of 1. The multiplication by ξ

$$F_\xi(t) := u^{-1}\big(\xi u(t)\big) = \xi + \cdots .$$

determined from F belongs to $\xi t + t^2\mathbf{Z}_p[[t]]$ by the results in the Step 1. Now we use the notation $x\langle u\rangle = x(\boldsymbol{u}) \in \frac{1}{u^2} + \mathbf{Q}_p[[u]]$ in order to avoid confusion. Thanks to existence of such $F_\xi(t)$, we can easily show that

$$x\langle u(t)\rangle - \xi^2 x\langle \xi u(t)\rangle \in \mathbf{Z}_p[[t]]. \tag{9.2}$$

Adding (9.1) to (9.2), we have, for any integer $a > 0$, that

$$\Big(\big(\tfrac{d}{du}\big)^p - A_p \tfrac{d}{du}\Big)^a \big(x\langle u(t)\rangle - \xi^2 x\langle \xi u(t)\rangle\big) \in p^a\mathbf{Z}_p[[t]] \subset p^a\mathbf{Z}_p\langle\langle u\rangle\rangle. \tag{9.3}$$

The coefficient of $u^{10n-a-2}/(10n-a-2)!$ is just the left hand side of the first formula in 7.1, and the poof has been completed.

We mention here that Kummer type congruence relations for $C^{(\nu)}_{10m}$ and $D^{(\nu)}_{10m}$ without division by $10m$ are proved in 14.1.

10 The Clarke theorem on $x(\boldsymbol{u})$ over $\mathbf{Z}[\frac{1}{2}]$

We deal with only the curve $y^2 = x^5 - 1$ in this Chapter.

10.1 The Clarke theorem on $x(\boldsymbol{u})^{1/2}$

Let us consider the formal inverse series of $u \mapsto \sqrt{x(\boldsymbol{u})}$, namely, the power series u with respect to

$$t = \frac{-1}{x^{1/2}(\boldsymbol{u})}.$$

That is

$$\begin{aligned} u &= \int_{\infty}^{x} \frac{xdx}{2y} \\ &= \int_{0}^{-t} \frac{\frac{1}{t^2} \cdot \left(-\frac{2dt}{t^3}\right)}{2\sqrt{\frac{1}{t^{10}} - 1}} \\ &= -\int_{0}^{-t} \frac{1}{\sqrt{1-t^{10}}} dt \\ &= -\int_{0}^{-t} \left(1 + \sum_{m=1}^{\infty} (-1)^m \binom{-\frac{1}{2}}{m} t^{10m}\right) dt \\ &= t + \sum_{m=1}^{\infty} (-1)^m \binom{-\frac{1}{2}}{m} \frac{t^{10m+1}}{10m+1}. \end{aligned}$$

For convenience of reference, we write again this;

$$u = t + \sum_{m=1}^{\infty} (-1)^m \binom{-\frac{1}{2}}{m} \frac{t^{10m+1}}{10m+1}. \tag{10.1}$$

We denote the Carlitz coefficients by

$$f_{10m} = (-1)^m \binom{-\frac{1}{2}}{m}. \tag{10.2}$$

This notation corresponds to that in the definition of the universal Bernoulli numbers. By 1.4 and (1.6), we see that

$$f_{10m} \in \mathbf{Z}[\tfrac{1}{2}]. \tag{10.3}$$

The other coefficients f_n are 0. Then the divided universal Bernoulli number $\hat{B}_{10m}/(10m)$ is specialized to $C^{(1)}_{10m}/(10m)$, and the expression of 2.8 yields that

$$\frac{C^{(1)}_{10m}}{10m} \ \in \ 3!\mathbf{Z}[\tfrac{1}{2}] \tag{10.4}$$

as follows. To prove this, we apply 3.11 for $p = 2$ and $p = 3$. Since $f_{2-1} = 0$ and $f_{3-1} = 0$ in this case, we may consider only the partitions U such that $U_{2-1} = U_{3-1} = 0$. Here, as

$$w(U) = 10m \geqq 10, \quad d(U) \geqq 1$$

we see

$$\mathrm{ord}_2(\tau_U) \geqq \lfloor \tfrac{10+1-2}{4} \rfloor = 2, \quad \mathrm{ord}_3(\tau_U) \geqq \lfloor \tfrac{10+1-2}{6} \rfloor = 1.$$

Hence, in the expression of 2.8 for $C^{(1)}_{10m}/(10m)$, all its coefficients are divisible by 3!. Adding this to (10.3), we conclude (10.4).

If $p = 10m+1$ is a prime number, then the coefficient f_{p-1} of $t^{10m+1}/(10m+1)$ modulo p coincides with $(2,2)$-entry of the Hasse-Witt matrix with respect to our canonical base of the differential of the first kind on the curve $\mathscr{C}$ of reduction modulo p, namely,

$$f_{p-1} = (-1)^{(p-1)/10}\binom{-\frac{1}{2}}{\frac{p-1}{10}} \equiv A_p \mod p. \tag{10.5}$$

For this, see 18.1.

Under the consideration above, we apply Clarke's theorem 2.9 for the function $u \mapsto x(\boldsymbol{u})^{1/2}$. Let

$$\frac{1}{t} = \sum_{m=0}^{\infty} \frac{C^{(1)}_{10m}}{10m} \frac{{u_2}^{10m-1}}{(10m-1)!} \tag{10.6}$$

Proposition 2.9 and (10.4) deduce that

$$\frac{1}{3!}\frac{C^{(1)}_{10m}}{10m} \in \sum_{\substack{p\equiv 1 \mod 5 \\ 10m=a(p-1)}} \frac{(3!a)|_p{}^{-1} \mod p^{1+\mathrm{ord}_p a}}{p^{1+\mathrm{ord}_p a}} {A_p}^a + \mathbf{Z}[\tfrac{1}{2}]. \tag{10.7}$$

10.2 Congruence between $x(\boldsymbol{u})^{k/2}$ and $x(\boldsymbol{u})^{(k+1)/2}$

Throughout this Section, we assume $k = 1$, 2, or 3. For the curve $y^2 = x^5 - 1$ and

$$t = \frac{-1}{x(\boldsymbol{u})^{1/2}} \quad (= u + \cdots),$$

we let

$$\frac{1}{t^j} = x(\boldsymbol{u}) = \frac{1}{u^j} + \sum_{m=1}^{\infty} \frac{C^{(j)}_{10m}}{(10m)_j} \frac{u^{10m-j}}{(10m-j)!} \quad (C^{(j)}_0 = 1) \tag{10.8}$$

for $j = 1$, 2, 3, and 4. Then

$$\begin{aligned} \int_0^u \left(\frac{1}{t^{k+1}} - \frac{1}{u^{k+1}}\right) du &= \int_0^u \left(\sum_{m=1}^{\infty} \frac{C^{(k+1)}_{10m}}{(10m)_{k+1}} \frac{u^{10m-(k+1)}}{(10m-k)!}\right) du \\ &= \sum_{m=1}^{\infty} \frac{C^{(k+1)}_{10m}}{(10m)_{k+1}} \frac{u^{10m-k}}{(10m-k)!}. \end{aligned} \tag{10.9}$$

On the other hand, after differentiating (10.1) with respect to u, dividing by t^{k+1}, we have

$$\frac{1}{t^{k+1}} = \frac{1}{t^{k+1}}\frac{dt}{du} + \sum_{m=1}^{\infty} (-1)^m \binom{-\frac{1}{2}}{m} t^{10m-(k+1)} \frac{dt}{du}. \tag{10.10}$$

Therefore,

$$\int_0^u \left(\frac{1}{t^{k+1}} - \frac{1}{u^{k+1}}\right) du_2 = \left(-\frac{1}{k}\frac{1}{t^k} + \sum_{m=1}^{\infty}(-1)^m \binom{-\frac{1}{2}}{m} \frac{t^{10m-k}}{10m-k}\right) + \frac{1}{k}\frac{1}{u^k}.$$

By equating this with (10.9) and by using (10.6), we see that

$$\sum_{m=1}^{\infty} \frac{C_{10m}^{(k+1)}}{(10m)_{k+1}} \frac{u^{10m-k}}{(10m-k)!}$$
$$= \left(-\sum_{m=0}^{\infty} \frac{C_{10m}^{(k)}}{(10m)_k} \frac{u^{10m-k}}{(10m-k)!} + \sum_{m=1}^{\infty}(-1)^m \binom{-\frac{1}{2}}{m} \frac{t^{10m-k}}{10m-k}\right) + \frac{1}{k}\frac{1}{u^k}.$$

Since $C_0^{(k)} = 1$, we can remove the terms of negative degree, and we have

$$\sum_{m=1}^{\infty} \frac{C_{10m}^{(k)}}{(10m)_k} \frac{u^{10m-k}}{(10m-k)!} + \sum_{m=1}^{\infty} \frac{C_{10m}^{(k+1)}}{(10m)_{k+1}} \frac{u^{10m-k}}{(10m-k)!}$$
$$= \sum_{m=1}^{\infty}(-1)^m \binom{-\frac{1}{2}}{m} \frac{t^{10m-k}}{10m-k}.$$

The right hand side of this belongs to $\mathbf{Z}[\frac{1}{2}]\langle\langle u\rangle\rangle$ because of 1.4, 8.2(3), and (8.6). Adding this to (10.3), we see that

$$\frac{C_{10m}^{(k)}}{(10m)_k} + k\frac{C_{10m}^{(k+1)}}{(10m)_{k+1}} \in (10\cdot 1-(k+1))!\mathbf{Z}[\tfrac{1}{2}] \subset 3!\mathbf{Z}[\tfrac{1}{2}]. \tag{10.11}$$

At this stage, as $C_{10m}/(10m) = C_{10m}^{(2)}/(10m)_2$ by the definition, we have

$$\frac{C_{10m}}{10m} \in -\frac{C_{10m}^{(1)}}{10m} + 3!\mathbf{Z}[\tfrac{1}{2}] \tag{10.12}$$

from (10.11) for $k = 1$.

We remark that we can conclude the Clarke theorem for C_{10m} over $\mathbf{Z}[\frac{1}{2}]$ by (10.12) above and (10.7). We need, however, in order to prove the Clarke theorem over $\mathbf{Z}$ to take a rather long way mentioned in 9.1.

10.3 The Clarke theorem on $x(\boldsymbol{u})^2$ over $\mathbf{Z}[\frac{1}{2}]$

We summarize the results which obtained in this Section. The results (10.11) for $k = 1$, 2, 3 show that

$$\frac{C_{10m}^{(1)}}{10m} + 3!\frac{C_{10m}^{(4)}}{(10m)_4} \in\ 3!\mathbf{Z}[\tfrac{1}{2}]. \tag{10.13}$$

So that

$$\frac{1}{3!}\frac{C_{10m}^{(1)}}{10m} + \frac{C_{10m}^{(4)}}{(10m)_4} \in \mathbf{Z}[\tfrac{1}{2}]. \tag{10.14}$$

This and 10.7 yield that

$$\frac{C^{(4)}_{10m}}{(10m)_4} \in -\sum_{\substack{p\equiv 1 \bmod 5\\ 10m=a(p-1)}} \frac{((3!a)|_p{}^{-1} \bmod p^{1+\mathrm{ord}_p a}}{p^{1+\mathrm{ord}_p a}} {A_p}^a + \mathbf{Z}[\tfrac{1}{2}]. \tag{10.15}$$

Especially, we see that

$$\frac{C^{(4)}_{10m}}{(10m)_4} \in \mathbf{Z}_{(5)}. \tag{10.16}$$

11 The Clarke theorem on $y(\boldsymbol{u})$ over $\mathbf{Z}[\frac{1}{5}]$

We deal with only the curve $y^2 = x^5 - 1$ in this section too.

11.1 The Clarke theorem on $y^{1/5}(\boldsymbol{u})$

Being parallel to the Chapter 10, we consider the formal inverse series of $u \mapsto y(\boldsymbol{u})^{1/5}$. Let

$$y(\boldsymbol{u}) = -1/s^5.$$

Then

$$\begin{aligned}
u &= \int_\infty^x \frac{xdx}{2y} = \int_\infty^y \frac{x}{2y}\frac{dx}{dy}dy = \int_\infty^y \frac{x}{5x^4}dy = \int_\infty^y \frac{1}{5x^3}dy \\
&= \int_\infty^y \frac{1}{5(y^2+1)^{3/5}}dy = \int_0^s \frac{\frac{5ds}{s^6}}{5(\frac{1}{s^{10}}+1)^{3/5}} \\
&= \int_0^s \frac{1}{(1+s^{10})^{3/5}}ds \\
&= \int_0^s \left(1 - \frac{1}{1!}\frac{3}{5}s^{10} + \frac{1}{2!}\frac{3}{5}\frac{8}{5}s^{20} - \frac{1}{3!}\frac{3}{5}\frac{8}{5}\frac{13}{5}s^{30} + \cdots\right)ds \\
&= \int_0^s \left(1 + \sum_{m=1}^\infty \binom{-\frac{3}{5}}{m} s^{10m}\right)ds \\
&= s + \sum_{m=1}^\infty \binom{-\frac{3}{5}}{m}\frac{s^{10m+1}}{10m+1}.
\end{aligned}$$

For convenience of quotation, we rewrite this:

$$u = s + \sum_{m=1}^\infty \binom{-\frac{3}{5}}{m}\frac{s^{10m+1}}{10m+1}. \tag{11.1}$$

We denote each the Carlitz coefficient of this by

$$f_{10m} = \binom{-\frac{3}{5}}{m}. \tag{11.2}$$

By 1.4 and (1.6), we see that

$$f_{10m} \in \mathbf{Z}[\tfrac{1}{5}]. \tag{11.3}$$

The other coefficients f_n are 0. Here we are regarding each the coefficient as a specialization of f_j of the Subsection 2.1. Then the divided universal Bernoulli number $\hat{B}_{10m}/(10m)$ is specialized to $D^{(1)}_{10m}/(10m)$. We claim that

$$\frac{D^{(1)}_{10m}}{10m} \ \in \ 4!\mathbf{Z}[\tfrac{1}{5}]. \tag{11.4}$$

To prove this, we apply 3.11 for $p = 2$ and $p = 3$. In this case, as $f_{2-1} = 0$ and $f_{3-1} = 0$, we may consider only the partitions U such that $U_{2-1} = U_{3-1} = 0$. If $m = 1$, then $D^{(1)}_{10}/10 = (3/5)(9!/11) = 2^7 3^5 7/11$ is divisible by 4!. If $m \geqq 2$, then because of

$$w(U) = 10m \geqq 20, \quad d(U) \geqq 1$$

we have

$$\mathrm{ord}_2(\tau_U) \geqq \lfloor \tfrac{20+1-2}{4} \rfloor = 4, \quad \mathrm{ord}_3(\tau_U) \geqq \lfloor \tfrac{20+1-2}{6} \rfloor = 3.$$

Hence, thanks to the expression in 2.8, all the coefficients $D^{(1)}_{10m}/(10m)$ are divisible by 4!. This and (11.3) yield (11.4).

If $p = 10m + 1$ is a prime number, then the coefficient f_{p-1} coincides with $(2, 2)$-entry of the Hasse-Witt matrix with respect to the natural basis of the differential forms of the first kind on C of reduction modulo p:

$$f_{p-1} = -\binom{-\frac{3}{5}}{\frac{p-1}{10}} \equiv A_p \mod p. \tag{11.5}$$

See also 18.1.

Under the consideration above, by applying Clarke's theorem 2.9 to the Laurent development of the function $u \mapsto -y(\boldsymbol{u})^{1/5}$ at $u = 0$, namely to

$$\frac{1}{s} = \sum_{m=0}^{\infty} D^{(1)}_{10m} \frac{u^{10m-1}}{(10m)!}, \tag{11.6}$$

we have

$$\frac{1}{4!}\frac{D^{(1)}_{10m}}{10m} \in \ -\sum_{\substack{p \equiv 1 \mod 5 \\ 10m = a(p-1)}} \frac{(4!a)|_p{}^{-1} \mod p^{1+\mathrm{ord}_p a}}{p^{1+\mathrm{ord}_p a}} {A_p}^a + \mathbf{Z}[\tfrac{1}{5}]. \tag{11.7}$$

11.2 Congruence between $y(\boldsymbol{u})^{k/5}$ and $y(\boldsymbol{u})^{(k+1)/5}$

Throughout this Section, we assume $k = 1$, 2, 3, or 4. We prove here a congruence relation between the Hurwitz coefficients of $y^{(k+1)/5}(\boldsymbol{u})$ and of $y(\boldsymbol{u})^{k/5}$ for $y^2 = x^5 - 1$.

$$s = \frac{-1}{y(\boldsymbol{u})^{1/5}} \ \ (= u + \cdots),$$

we let

$$\frac{1}{s^j} = y(\boldsymbol{u})^{j/5} = \frac{1}{u^j} + \sum_{m=1}^{\infty} \frac{D_{10m}^{(j)}}{(10m)_j} \frac{u^{10m-j}}{(10m-j)!} \qquad (D_0^{(2)} = 1) \tag{11.8}$$

for $j = 1$, 2, 3, 4, and 5. Then

$$\begin{aligned} &\int_0^u \Big(\frac{1}{s^{k+1}} - \frac{1}{u^{k+1}}\Big) du \\ &\quad = \int_0^u \left(\sum_{m=1}^{\infty} \frac{D_{10m}^{(k+1)}}{(10m)_{k+1}} \frac{u^{10m-(k+1)}}{(10m-(k+1))!} \right) du \\ &\quad = \sum_{m=1}^{\infty} \frac{D_{10m}^{(k+1)}}{(10m)_{k+1}} \frac{u^{10m-k}}{(10m-k)!}. \end{aligned} \tag{11.9}$$

On the other hand, after differentiating (11.1) with respect to u, dividing by s^{k+1}, we have

$$\frac{1}{s^{k+1}} = \frac{1}{s^{k+1}} \frac{ds}{du} + \sum_{m=1}^{\infty} \binom{-\frac{3}{5}}{m} s^{10m-(k+1)} \frac{ds}{du}. \tag{11.10}$$

Therefore,

$$\int_0^u \left(\frac{1}{s^{k+1}} - \frac{1}{u^{k+1}} \right) du = \left(-\frac{1}{k} \frac{1}{s^k} + \sum_{m=1}^{\infty} \binom{-\frac{3}{5}}{m} \frac{s^{10m-k}}{10m-k} \right) + \frac{1}{k} \frac{1}{u^k}.$$

By equating this with (11.9), and by using (11.6), we see that

$$\begin{aligned} &\sum_{m=1}^{\infty} \frac{D_{10m}^{(k+1)}}{(10m)_{k+1}} \frac{u^{10m-k}}{(10m-k)!} \\ &\qquad = \left(-\sum_{m=0}^{\infty} \frac{D_{10m}^{(k)}}{(10m)_k} \frac{u^{10m-k}}{(10m-k)!} + \sum_{m=1}^{\infty} \binom{-\frac{3}{5}}{m} \frac{s^{10m-k}}{10m-k} \right) + \frac{1}{k} \frac{1}{u^k}. \end{aligned}$$

Since $D_0^{(1)} = 1$, we can remove the terms of negative degree, and we have

$$\sum_{m=1}^{\infty} \frac{D_{10m}^{(k)}}{(10m)_k} \frac{u^{10m-k}}{(10m-k)!} + \sum_{m=1}^{\infty} \frac{D_{10m}^{(k+1)}}{(10m)_{k+1}} \frac{u^{10m-k}}{(10m-k)!} = \sum_{m=1}^{\infty} \binom{-\frac{3}{5}}{m} \frac{s^{10m-k}}{10m-k}.$$

The right hand side belongs to $\mathbf{Z}[\frac{1}{5}]\langle\langle u \rangle\rangle$ because of 8.2(3) and (8.12). Adding this with (11.3), we conclude that

$$\frac{D_{10m}^{(k)}}{(10m)_k} + \frac{D_{10m}^{(k+1)}}{(10m)_{k+1}} \in (10 \cdot 1 - 2)! \mathbf{Z}[\tfrac{1}{5}] \subset 4! \mathbf{Z}[\tfrac{1}{5}]. \tag{11.11}$$

11.3 The Clarke theorem on $y(\boldsymbol{u})$ over $\mathbf{Z}[\frac{1}{5}]$

The results we have obtained (11.11) for $k = 1, 2, 3, 4$ are

$$\begin{aligned}
\frac{D^{(4)}_{10m}}{(10m)_4} + 4\frac{D^{(5)}_{10m}}{(10m)_5} &\in 4!\mathbf{Z}[\tfrac{1}{5}],\\
\frac{D^{(3)}_{10m}}{(10m)_3} + 3\frac{D^{(4)}_{10m}}{(10m)_4} &\in 4!\mathbf{Z}[\tfrac{1}{5}],\\
\frac{D^{(2)}_{10m}}{(10m)_2} + 2\frac{D^{(3)}_{10m}}{(10m)_3} &\in 4!\mathbf{Z}[\tfrac{1}{5}],\\
\frac{D^{(1)}_{10m}}{10m} + \frac{D^{(2)}_{10m}}{(10m)_2} &\in 4!\mathbf{Z}[\tfrac{1}{5}].
\end{aligned}$$

Summing up these results, we have

$$\frac{D^{(1)}_{10m}}{10m} - 4!\frac{D^{(5)}_{10m}}{(10m)_5} \in 4!\mathbf{Z}[\tfrac{1}{5}]. \tag{11.12}$$

Hence

$$\frac{1}{4!}\frac{D^{(1)}_{10m}}{10m} - \frac{D^{(5)}_{10m}}{(10m)_5} \in \mathbf{Z}[\tfrac{1}{5}].$$

Since $y(\boldsymbol{u}) = -1/s(\boldsymbol{u})^5$ we see

$$\frac{D_{10m}}{10m} = \frac{D^{(5)}_{10m}}{(10m)_5}. \tag{11.13}$$

This and 11.7 show that the aimed result of this section, that is

$$\frac{D_{10m}}{(10m)} \in -\sum_{\substack{p\equiv 1 \mod 5\\ 10m=a(p-1)}} \frac{(4!a|_p)^{-1} \mod p^{1+\mathrm{ord}_p a}}{p^{1+\mathrm{ord}_p a}} {A_p}^a + \mathbf{Z}[\tfrac{1}{5}]. \tag{11.14}$$

12 The Clarke theorem on $x(\boldsymbol{u})$ and $y(\boldsymbol{u})$ over Z

We still deal with only the curve $y^2 = x^5 - 1$ in this section.

12.1 Congruence between $y(\boldsymbol{u})$ and $x^2(\boldsymbol{u})$

Let

$$x^2(\boldsymbol{u}) = \frac{1}{t^4} = \sum_{m=0}^{\infty} \frac{C^{(4)}_{10m}}{(10m)_4}\frac{u^{10m-4}}{(10m-4)!}. \tag{12.1}$$

If $D = d/du = (2y/x)d/dx$, then

$$D(x^2) = 2xDx = 2x\tfrac{2y}{x} = 4y. \tag{12.2}$$

Hence

$$\frac{C^{(4)}_{10m}}{(10m)_4} = 4\frac{D_{10m}}{10m}. \tag{12.3}$$

Therefore, (10.15) and (11.14) show that the denominator of $C^{(4)}_{10m}/(10m)_4$ does not contain any power of 2, and that $C^{(4)}_{10m}/(10m)_4$ has the property that

$$\frac{C^{(4)}_{10m}}{(10m)_4} \in -\sum_{\substack{p\equiv 1 \mod 5\\ 10m=a(p-1)}} \frac{(3!a)|_p{}^{-1} \mod p^{1+\mathrm{ord}_p a}}{p^{1+\mathrm{ord}_p a}} {A_p}^a + \mathbf{Z}. \tag{12.4}$$

Furthermore, since $\frac{1}{4}\frac{C^{(4)}_{10m}}{(10m)_4} = \frac{D_{10m}}{10m}$ by (12.3), we see that

$$\frac{D_{10m}}{10m} \in \mathbf{Z}\Big[\frac{1}{5},\ \frac{1}{p}\ ;\ p\equiv 1 \bmod 5,\ p-1|10m\Big] \subset \mathbf{Z}_{(2)},$$

and that the denominator of $D_{10m}/(10m)$ does not contain any power of 2. Thus the numerator of $C^{(4)}_{10m}/(10m)_4$ is divisible by 4. This consideration and (11.14) give rise to

$$\frac{D_{10m}}{10m} \in -\sum_{\substack{p\equiv 1 \mod 5\\ 10m=a(p-1)}} \frac{(4!a)|_p{}^{-1} \mod p^{1+\mathrm{ord}_p a}}{p^{1+\mathrm{ord}_p a}} {A_p}^a + \mathbf{Z}. \tag{12.5}$$

This is the second formula in 6.1.

12.2 From $x^2(\boldsymbol{u})$ to $x(\boldsymbol{u})$

Finally, we use

$$D^2x = D\frac{2y}{x} = 6x^2 + \frac{4}{x^3} \quad (\ D = \tfrac{d}{du} = \tfrac{2y}{x}\tfrac{d}{dx}\ ). \tag{12.6}$$

Operating D to the differential equation (5.5), we have

$$D^2\Big(\frac{1}{x}\Big) = 3\frac{1}{x}\Big(D\frac{1}{x}\Big)^2 - 10. \tag{12.7}$$

Therefore $1/x(\boldsymbol{u}) \in \mathbf{Z}\langle\langle u\rangle\rangle$ by 8.2(1), and also $1/x^3 \in \mathbf{Z}\langle\langle u\rangle\rangle$. These facts were proved also by 8.3 and 8.2(3). Thus, we see that

$$\frac{C_{10m}}{10m} = 6\cdot\frac{C^{(4)}_{10m}}{(10m)_4} + \text{“an integer”}. \tag{12.8}$$

Because of (12.4), we conclude that

$$\begin{aligned}\frac{C_{10m}}{10m} &= 3!\frac{C^{(4)}_{10m}}{(10m)_4} + \text{“an integer”}\\ &= G_{10m} - \sum_{\substack{p\equiv 1 \mod 5\\ 10m=a(p-1)}} \frac{a|_p{}^{-1} \mod p^{1+\mathrm{ord}_p a}}{p^{1+\mathrm{ord}_p a}} {A_p}^a\end{aligned} \tag{12.9}$$

with a suitable $G_{10m} \in \mathbf{Z}$. This is the desired first formula in 6.1.

13 Proof of the Kummer-type congruences

13.1 Honda's theorem and formal groups.

Now we start to prove 7.1 (and 7.5). We show that there exists formal group over $\mathbf{Z}$ such that its formal logarithm is (10.1) (or (11.1)).

PROPOSITION 13.1. *Suppose p be a fixed prime number. Let t be an indeterminate and let $u(t) \in \mathbf{Q}_p[[t]]$. If there exists $\beta \in \mathbf{Z}_p$ such that*

$$pu(t) - \beta u(t^p) \in p\mathbf{Z}_p[[t]] \tag{13.2}$$

then the formal group law F given by

$$F(t_1, t_2) := u^{-1}(u(t_1) + u(t_2)) \tag{13.3}$$

is defined over $\mathbf{Z}_p$ (i.e. $\in \mathbf{Z}_p[[t_1, t_2]]$). Here $u^{-1}(t) \in \mathbf{Q}_p[[t]]$ means the unique power series such that $u^{-1}(u(t)) = t$. In particular, if $\alpha \in \mathbf{Z}_p$, then we have

$$F(\alpha t) = u^{-1}(\alpha u(t)) \in \alpha t + t^2\mathbf{Z}_p[[t]]. \tag{13.4}$$

This is obtained by applying Honda's theorem [Ho], p.223, Theorem 2 as $n = 1$, $q = p$, $P = 1$, $u = p - \beta T$, $f = u(t)$. We can apply this theorem to $t \mapsto u = u_g$ of (10.1) and $s \mapsto u$ of (11.1). To do so, we introduce the p-adic Γ-function

$$\Gamma_p : \mathbf{Z}_p \to \mathbf{Z}_p^{\times}. \tag{13.5}$$

This function satisfies, for any positive integer n, that

$$\Gamma_p(n) = (-1)^n \prod_{\substack{1 \leqq j < n \\ p \nmid j}} j. \tag{13.6}$$

The most important properties are that

$$\Gamma_p(z+1) = \begin{cases} -z\Gamma_p(z) & (z \notin p\mathbf{Z}_p) \\ -\Gamma_p(z) & (z \in p\mathbf{Z}_p) \end{cases} \tag{13.7}$$

and that, for any positive integer ν,

$$z \equiv w \mod p^{\nu}\mathbf{Z}_p \text{ implies } \Gamma_p(z) \equiv \Gamma_p(w) \mod p^{\nu}\mathbf{Z}_p. \tag{13.8}$$

For the details, see [Mo] or [R].

Denoting by $u(t)$ the power series development of

$$u(= u_g) = \int_{\infty}^{(x,y)} \frac{x^{g-1}dx}{2y}$$

with respect to $t = -x^{-\frac{1}{2}}$ we claim that

LEMMA 13.9. *For the curve $y^2 = x^{2g+1} - 1$ (resp. $y^2 = x^{2g+1} - x$) and a prime $p \equiv 1 \mod 2g+1$ (resp. $p \equiv 1 \mod 4g$),*

$$\beta_p = -(-1)^{(p-1)/(4g+2)} \frac{\Gamma_p(\frac{1}{2})}{\Gamma_p(\frac{4g+1}{4g+2})\Gamma_p(\frac{2g+2}{4g+2})} \quad (\in \mathbf{Z}_p{}^\times).$$

$$\left(\textit{resp.} \quad \beta_p = -(-1)^{(p-1)/(4g)} \frac{\Gamma_p(\frac{1}{2})}{\Gamma_p(\frac{4g-1}{4g})\Gamma_p(\frac{2g+1}{4g})} \quad (\in \mathbf{Z}_p{}^\times).\right)$$

Then the series satisfies

$$pu(t) - \beta_p u(t^p) \in p\mathbf{Z}_p[[t]]. \tag{13.10}$$

This property is satisfied by the power series development $s = -y^{-\frac{1}{2g+1}}$ with respect to u also.

PROOF. For simplicity, we prove the statement only for the curve $y^2 = x^5 - 1$ ($g = 2$). Let $f_{10n}/(10n+1) = [t^{10n+1}]u(t)$. Then, as is stated in (10.2), $f_{10n} = (-1)^n\binom{-\frac{1}{2}}{n}$. It suffice for us to prove that, if $p(10m+1) = 10n+1$, then

$$p\frac{f_{10n}}{10n+1} - \beta_p \frac{f_{10m}}{10m+1} \in p\mathbf{Z}_p.$$

We notice that $\lfloor \frac{n}{p} \rfloor = \lfloor m + \frac{1}{10} - \frac{1}{10p} \rfloor = m$. This and

$$p(2\lfloor \tfrac{n}{p} \rfloor - 1) \leqq 2n - 1 \leqq p\big(2(\lfloor \tfrac{n}{p} \rfloor + 1) - 1\big)$$

show that the largest odd integer divisible by p not exceed $2n-1$ is $p(2m-1)$. Hence

$$\begin{aligned}
&p\frac{f_{10n}}{10n+1} - \beta_p \frac{f_{10m}}{10m+1} \\
&= p(-1)^n \binom{-\frac{1}{2}}{n} \frac{1}{10n+1} - \beta_p \cdot (-1)^m \binom{-\frac{1}{2}}{m} \frac{1}{10m+1} \\
&= \frac{1}{10m+1}\left\{ (-1)^{pm+\frac{p-1}{10}} \frac{\prod_{j=1}^n \left(-\frac{2j-1}{2}\right)}{n!} - \beta_p \cdot (-1)^m \frac{\prod_{j=1}^m \left(-\frac{2j-1}{2}\right)}{m!} \right\} \\
&= \frac{(-1)^{m+\frac{p-1}{10}}}{10m+1}\left\{ \frac{\prod_{j=1,p\not| 2j-1}^n \left(-\frac{2j-1}{2}\right) \prod_{k=1}^m \left(-\frac{p(2k-1)}{2}\right)}{\left(\prod_{j=1,p\not| j}^n j\right)\left(\prod_{k=1}^m pk\right)} \right. \\
&\qquad\qquad \left. - (-1)^{\frac{p-1}{10}} \beta_p \frac{\prod_{j=1}^m \left(-\frac{2j-1}{2}\right)}{m!} \right\}.
\end{aligned}$$

By using (13.7) repeatedly, we have

$$\begin{aligned}
&= \frac{(-1)^{m+\frac{p-1}{10}}}{10m+1}\left\{ \frac{(-1)^n \Gamma_p(-\frac{1}{2}+1)}{\Gamma_p(-\frac{2n-1}{2})} \frac{p^m \prod_{k=1}^m \left(-\frac{2k-1}{2}\right)}{(-1)^{n+1}\Gamma_p(n+1)\, p^m m!} - (-1)^{\frac{p-1}{10}} \beta_p \frac{\prod_{j=1}^m \left(-\frac{2j-1}{2}\right)}{m!} \right\} \\
&= \frac{(-1)^{m+\frac{p-1}{10}}}{10m+1}\left\{ - \frac{\Gamma_p(\frac{1}{2})}{\Gamma_p(n+1)\Gamma_p(-n+\frac{1}{2})} \frac{\prod_{k=1}^m \left(-\frac{2k-1}{2}\right)}{m!} \right.
\end{aligned}$$

$$+\frac{\Gamma_p(\frac{1}{2})}{\Gamma_p(\frac{9}{10})\Gamma_p(\frac{6}{10})}\frac{\prod_{j=1}^{m}\left(-\frac{2j-1}{2}\right)}{m!}\Bigg\}$$

$$=\frac{(-1)^{m+\frac{p-1}{10}}}{10m+1}\binom{-\frac{1}{2}}{m}\Bigg\{-\frac{\Gamma_p(\frac{1}{2})}{\Gamma_p(\frac{1}{10}p(10m+1)+\frac{9}{10})\Gamma_p(-\frac{1}{10}p(10m+1)+\frac{6}{10})}$$

$$+\frac{\Gamma_p(\frac{1}{2})}{\Gamma_p(\frac{9}{10})\Gamma_p(\frac{6}{10})}\Bigg\}.$$

Let ν be the integer such that $\mathrm{ord}_p(10m+1)=\nu$. Then (13.7) and (13.8) show

$$\frac{\Gamma_p(\frac{1}{2})}{\Gamma_p(\frac{1}{10}p(10m+1)+\frac{9}{10})\Gamma_p(-\frac{1}{10}p(10m+1)+\frac{6}{10})}$$
$$\equiv\frac{\Gamma_p(\frac{1}{2})}{\Gamma_p(\frac{9}{10})\Gamma_p(\frac{6}{10})}\mod p^{\nu+1}\mathbf{Z}_p.$$

It follows from 1.5 that

$$\binom{-\frac{1}{2}}{m}\in\mathbf{Z}_p.$$

Therefore

$$p\frac{f_{10n}}{10n+1}-\beta_p\frac{f_{10m}}{10m+1}\in p\mathbf{Z}_p.$$

and the proof has completed. □

Remark 13.11. (1) Regarding the map $\iota:\mathscr{C}\to J$ to be defined over $\mathbf{Z}_p$, we denote its formal completion at $\infty\mapsto$ "the origin of J" by $\hat{\iota}:\hat{\mathscr{C}}\to\hat{J}$. Because of the action (5.6) (resp. (5.8)), $\hat{J}$ is decomposed into a product of 1-dimensional formal groups. The composite map $\hat{\pi}\circ\hat{\iota}:\hat{\mathscr{C}}\to G$ of $\hat{\iota}$ with the projection $\pi:\hat{J}\to G$, where G is a certain factor of the product, would be an isomorphism of formal groups.
(2) The height of the formal group F over $\mathbf{Z}_p$ associated to $u(t)$ above is 1, namely, there exists $b\in\mathbf{Z}_p^\times$ such that $u^{-1}(pu(t))\equiv bt^p \mod p\mathbf{Z}_p[[t]]$. This is a consequence from

$$pu(t)=p\big(t+\cdots+f_{p-1}\frac{t^p}{p}+\cdots\big)$$

and that $f_{p-1}\in\mathbf{Z}_p^\times$ which follows from (10.5). The same fact is seen for the formal group associated to the series development of $s\mapsto u$.

13.2 Hochschild's formula and Honda's theorem

We recall the following Proposition called Hochschild's formula in order to show 13.13 below. Let R be a commutative ring. A *derivation* D of R is a map form R to itself such that

$$D(a+b)=Da+Db,\quad D(ab)=(Da)b+aDb$$

for a, $b\in R$.

PROPOSITION 13.12. *Let p be a prime, Let R be a commutative ring and D be a derivation of R. Let M be ($\mathbf{Z}$-)submodule in R such that DM is in a subring $A \subset R$ in which pA is a prime ideal with satisfying $DA \subset A$. So that, A/pA is a $\mathbf{F}_p$-algebra. Then, for $b \in A$, we have*

$$(bD)^p M \equiv \big(b^p D^p + ((bD)^{p-1}(b))\cdot D\big)M \mod pA.$$

PROOF. This is a slight modification of Theorem 25.5 in [Ma], p.197, and is proved exactly in the same way. So, we omit it. □

While the following general equality is proved by using the formula above, rather weak version for the case of $g = 1$ is described in [G] by a different way.

PROPOSITION 13.13. *For the curve $y^2 = x^{2g+1} - 1$ (resp. $y^2 = x^{2g+1} - x$), let $t = t(u)$ and $s = s(u)$ be the power series of* 8.3 *and of* 8.7*, respectively. Let $p \equiv 1 \pmod{(2g+1)}$ (resp. $\pmod{4g}$) be a prime. If $\varphi \in \mathbf{Z}_{(p)}[[t]]$ or $\varphi \in \mathbf{Z}_{(p)}[[s]]$ then*

$$\Big(\Big(\frac{d}{du}\Big)^p - A_p \frac{d}{du}\Big)\varphi \in p\mathbf{Z}_{(p)}[[t]] \quad \text{or} \quad \in p\mathbf{Z}_{(p)}[[s]].$$

PROOF. We apply 13.12 by taking $R = \mathbf{Q}[[t]]$, $M = \int_0^t \mathbf{Z}_{(p)}[[t]]dt$, $A = \mathbf{Z}_{(p)}[[t]]$, and $D = \frac{d}{dt}$. Then $A/pA = \mathbf{F}_p[[t]]$. In the sequel of this proof, the symbol "=" means the equality in $\mathbf{F}_p[[t]]$. First of all, we pay attention to the fact

$$\begin{aligned} &\frac{du}{dt} = 1 + \sum_{n=1}^{\infty} (-1)^n \binom{-\frac{1}{2}}{n} t^{(2g+2)n} \in 1 + t\,\mathbf{Z}[\tfrac{1}{2}][[t]], \\ &\frac{dt}{du} \in 1 + t\,\mathbf{Z}[\tfrac{1}{2}][[t]] \end{aligned} \tag{13.14}$$

given by (10.1) and (10.3). By using 13.12 for this $b := \frac{dt}{du}$ and D above, we see that

$$\begin{aligned} 0 &= \Big(\frac{d}{du}\Big)^p u = (bD)^p u \\ &= \big(b^p D^p + ((bD)^{p-1}(b)) \cdot D\big)u \\ &= \Big(\frac{dt}{du}\Big)^p \frac{d^p u}{dt^p} + \Big\{\Big(\frac{dt}{du}\frac{d}{dt}\Big)^{p-1}\frac{dt}{du}\Big\}\frac{du}{dt} \\ &= \Big(\frac{dt}{du}\Big)^p \frac{d^p u}{dt^p} + \Big\{\Big(\frac{d}{du}\Big)^{p-1}\frac{dt}{du}\Big\}\frac{du}{dt} \\ &= \Big(\frac{dt}{du}\Big)^p \frac{d^p u}{dt^p} + \frac{d^p t}{du^p}\frac{du}{dt}. \end{aligned}$$

Hence

$$\frac{d^p t}{du^p} = -\Big(\frac{du}{dt}\Big)^{-p-1}\frac{d^p u}{dt^p}. \tag{13.15}$$

By using 13.12 again for φ, D, and b, we have

$$\Big(\frac{d}{du}\Big)^p \varphi = (bD)^p \varphi$$

$$
\begin{aligned}
&= \big(b^p D^p + \big((bD)^{p-1}(b)\big)\cdot D\big)\varphi \\
&= \Big(\frac{dt}{du}\Big)^p \Big(\frac{d}{dt}\Big)^p \varphi + \Big(\Big(\frac{dt}{du}\frac{d}{dt}\Big)^{p-1}\frac{dt}{du}\Big)\frac{d}{dt}\varphi \\
&= \Big(\frac{du}{dt}\Big)^{-p}\frac{d^p}{dt^p}\varphi + \frac{d^p t}{du^p}\frac{du}{dt}\frac{d}{du}\varphi \\
&= \frac{d^p t}{du^p}\frac{du}{dt}\frac{d}{du}\varphi.
\end{aligned}
$$

Here we have used the assumption $\varphi \in \mathbf{Z}_p[[t]]$. By substituting (13.15) into the last formula, we obtain

$$
\Big(\frac{d}{du}\Big)^p \varphi = -\Big(\frac{du}{dt}\Big)^{-p}\frac{d^p u}{dt^p}\cdot\frac{d}{du}\varphi. \tag{13.16}
$$

Since $(\frac{d}{dt})^p \mathbf{Z}_{(p)}[[t]] \in p\mathbf{Z}_{(p)}[t]]$, by applying $(\frac{d}{dt})^p$ to (13.10), we have

$$
\frac{d^p u}{dt^p} = \Big(\frac{d}{dt}\Big)^{p-1}\big(\beta_p t^{p-1} u'(t^p)\big) = (p-1)!\,\beta_p\, u'(t^p) = -\beta_p u'(t)^p.
$$

The properties (13.6) and (13.8) imply

$$
\begin{aligned}
A_p &= (-1)^{(p-1)/(4g+2)}\binom{\frac{p-1}{2}}{\frac{p-1}{4g+2}} \\
&= (-1)^{(p-1)/(4g+2)}(-1)\frac{\Gamma_p(\frac{p-1}{2}+1)}{\Gamma_p(\frac{p-1}{4g+2}+1)\Gamma_p(\frac{p-1}{2}-\frac{p-1}{4g+2}+1)} \\
&= -(-1)^{(p-1)/(4g+2)}\frac{\Gamma_p(\frac{p+1}{2})}{\Gamma_p(\frac{p+4g+1}{4g+2})\Gamma_p(\frac{2gp+2g+2}{4g+2})} \\
&\equiv -(-1)^{(p-1)/(4g+2)}\frac{\Gamma_p(\frac{1}{2})}{\Gamma_p(\frac{4g+1}{4g+2})\Gamma_p(\frac{2g+2}{4g+2})} \mod p \\
&= \beta_p.
\end{aligned}
$$

So that

$$
\frac{d^p u}{dt^p} = -A_p\Big(\frac{du}{dt}\Big)^p.
$$

To Substitute this into (13.16) shows

$$
\Big(\frac{d}{du}\Big)^p \varphi = A_p \frac{d}{du}\varphi
$$

as desired. The statement for $s = s(u)$ is proved similarly. □

13.3 Proof of the congruence relations

The tools for the proof of 7.1 (and 7.5) have been completely prepared. Here we demonstrate the proof for the curve $y^2 = x^5 - 1$. To avoid confusion, if we regard

$$
x(\boldsymbol{u}) = \frac{1}{u^2} + \sum_{n=2}^{\infty}\frac{C_{10n}}{10n}\frac{u^{10n-2}}{(10n-2)!}
$$

to be an element in $\mathbf{Q}_p[[u]]$, we denote this by

$$x\langle u\rangle = x(\boldsymbol{u})$$

Let $\xi \in \mathbf{Z}_p$ be a primitive $(p-1)$-st root of 1. Then, as

$$x\langle u\rangle - \xi^2 x\langle \xi u\rangle = \sum_{\substack{n=1 \\ p-1\not| 10n}}^{\infty} \frac{(1-\xi^{10n})C_{10n}}{10n} \frac{u^{10n-2}}{(10n-2)!} \tag{13.17}$$

it suffice to prove for any positive integer a and $D = d/du$ that

$$(D^p - A_p D)^a (x\langle u\rangle - \xi^2 x\langle \xi u\rangle) \in p^a \mathbf{Z}_p\langle\langle u\rangle\rangle. \tag{13.18}$$

Indeed, if $10n \geqq a+2$ and $(p-1)\not| 10n$, then the coefficient of $u^{10n-a-2}/(10n-a-2)!$ is

$$(1-\xi^{10n}) \sum_{r=0}^{a} \binom{r}{a} (-A_p)^{a-r} \frac{C_{10n+r(p-1)}}{10n+r(p-1)}$$

and $1-\xi^{10n} \notin p\mathbf{Z}_p$. Thanks to 13.13, it suffice for proving (13.18) to prove

$$x\langle u(t)\rangle - \xi^2 x\langle \xi u(t)\rangle \in \mathbf{Z}_p[[t]]. \tag{13.19}$$

If we set

$$\begin{aligned} F_\xi(t) &= u^{-1}(\xi u(t)) \quad (u^{-1} \text{ is the formal inverse series of } t \mapsto u) \\ &= t(\xi u(t)) \\ &= \xi\, t + \tfrac{\xi^{11}-\xi}{22}\, t^{11} + \cdots, \end{aligned} \tag{13.20}$$

then 13.1 and 13.9 yield that

$$x\langle u(t)\rangle - \xi^2 x\langle \xi u(t)\rangle = \frac{1}{t^2} - \frac{\xi^2}{t(\xi u(t))^2} = \frac{1}{t^2} - \frac{\xi^2}{(\xi t + \frac{\xi^{11}-\xi}{22} t^{11} + \cdots)^2} \in \mathbf{Z}_p[[t]]$$

because $F_\xi(t) \in \xi t + t^2 \mathbf{Z}_p[[t]]$. Hence, 7.1 has been proved. □

14 Other congruence relations

In this Section we do not restrict to the curve $y^2 = x^5 - 1$, and describe hyperelliptic curves defined by either equation of

$$y^2 = x^{2g+1} - 1, \qquad y^2 = x^{2g+1} - x.$$

14.1 Generalized Bernoulli-Hurwitz numbers of higher order

Let $t = -1/x(\boldsymbol{u})^{1/2}$ and $s = -1/y(\boldsymbol{u})^{1/5}$ as usual. We prove the Kummer congruence relations for the Hurwitz coefficients of $t^{-\nu}$ $(1 \leqq \nu \leqq 4g+2)$ generalizing the congruence for $t^{-2} = x(\boldsymbol{u})$ proved in the Section 13.

The case of $y(\boldsymbol{u})^2 = x(\boldsymbol{u})^{2g+1} - 1$. For the curve $y^2 = x^{2g+1} - 1$, we recall the numbers $C^{(\nu)}_{(4g+2)n}$ (defined in the Section 10) and $D^{(\nu)}_{(4g+2)n}$ (defined in the Section 11). Namely, for $\nu = 1, 2, \cdots$, we let

$$\begin{aligned} \frac{1}{t^\nu} &= \frac{1}{u^\nu} + \sum_{n=1}^{\infty} \frac{C^{(\nu)}_{(4g+2)n}}{((4g+2)n)_\nu} \frac{u^{(4g+2)n-\nu}}{((4g+2)n-\nu)!}, \\ \frac{1}{s^\nu} &= \frac{1}{u^\nu} + \sum_{n=1}^{\infty} \frac{D^{(\nu)}_{(4g+2)n}}{((4g+2)n)_\nu} \frac{u^{(4g+2)n-\nu}}{((4g+2)n-\nu)!}. \end{aligned} \tag{14.1}$$

Of course, if $(4g+2) \nmid n$ then we assume $C^{(\nu)}_n = D^{(\nu)}_n = 0$.

Let $p \equiv 1 \pmod{(4g+2)}$ be a prime number, and $\xi \in \mathbf{Z}_p$ be a primitive $(p-1)$-st root of 1. By using

$$\frac{1}{t(u)^\nu} - \xi^\nu \frac{1}{t(\xi u)^\nu} = \sum_{\substack{n=1 \\ p-1 \nmid (4g+2)n}}^{\infty} \frac{(1-\xi^{(4g+2)n}) C^{(\nu)}_{(4g+2)n}}{((4g+2)n)_\nu} \frac{u^{(4g+2)n-\nu}}{((4g+2)n-\nu)!} \tag{14.2}$$

instead of (13.17), we have the following.

THEOREM 14.3. *Let $p \equiv 1 \bmod (2g+1)$ be a prime number, a be a positive integer. Let ν be an integer such that $1 \leqq \nu \leqq 4g+2$. Assume $(4g+2)n \geqq a+\nu$ and $p-1 \nmid (4g+2)n$. Then we have*

$$\begin{aligned} \sum_{r=0}^{a} \binom{r}{a} (-A_p)^{a-r} \frac{C^{(\nu)}_{(4g+2)n+r(p-1)}}{((4g+2)n+r(p-1))_\nu} &\equiv 0 \mod p^a, \\ \sum_{r=0}^{a} \binom{r}{a} (-A_p)^{a-r} \frac{D^{(\nu)}_{(4g+2)n+r(p-1)}}{((4g+2)n+r(p-1))_\nu} &\equiv 0 \mod p^a. \end{aligned}$$

The case of $y(\boldsymbol{u})^2 = x(\boldsymbol{u})^{2g+1} - x(\boldsymbol{u})$. For the curve $y^2 = x^{2g+1} - x$ and $\nu = 1, 2, \cdots$, we define $C^{(\nu)}_{4gn}$ and $D^{(\nu)}_{4gn}$ by

$$\begin{aligned} \frac{1}{t^\nu} &= \frac{1}{u^\nu} + \sum_{n=1}^{\infty} \frac{C^{(\nu)}_{4gn}}{(4gn)_\nu} \frac{u^{4gn-\nu}}{(4gn-\nu)!}, \\ \frac{1}{s^\nu} &= \frac{1}{u^\nu} + \sum_{n=1}^{\infty} \frac{D^{(\nu)}_{4gn}}{(4gn)_\nu} \frac{u^{4gn-\nu}}{(4gn-\nu)!}. \end{aligned} \tag{14.4}$$

We also assume that, if $(4g+2) \nmid n$ then $C^{(\nu)}_n = D^{(\nu)}_n = 0$.

Let $p \equiv 1 \pmod{4g}$ be a prime, and $\xi \in \mathbf{Z}_p$ be a primitive $(p-1)$-st root of 1. By using

$$\frac{1}{t(u)^\nu} - \xi^\nu \frac{1}{t(\xi u)^\nu} = \sum_{\substack{n=1 \\ p-1 \nmid 4gn}}^{\infty} \frac{(1-\xi^{4gn}) C_{4gn}^{(\nu)}}{(4gn)_\nu} \frac{u^{4gn-\nu}}{(4gn-\nu)!} \tag{14.5}$$

instead of (13.17), we have

THEOREM 14.6. *Let $p \equiv 1 \pmod{4g}$ be a prime number, a be a positive integer. Let ν be an integer such that $1 \leqq \nu \leqq 4g+2$. Assume $4gn = a + \nu$ and $p - 1 \nmid 4gn$. Then we have*

$$\sum_{r=0}^{a} \binom{r}{a} (-A_p)^{a-r} \frac{C_{4gn+r(p-1)}^{(\nu)}}{(4gn+r(p-1))_\nu} \equiv 0 \pmod{p^a},$$
$$\sum_{r=0}^{a} \binom{r}{a} (-A_p)^{a-r} \frac{D_{4gn+r(p-1)}^{(\nu)}}{(4gn+r(p-1))_\nu} \equiv 0 \pmod{p^a}.$$

14.2 Hurwitz coefficients of $t(u_g)$ and of $s(u_g)$

We consider now the Hurwitz coefficients $c_m^{(h)}$, $d_m^{(h)}$ of powers of $t = t(u)$ in 8.3 and $s = s(t)$ in 8.7, namely, those of

$$\frac{t(u)^h}{h!} = \sum_{m=h}^{\infty} c_m^{(h)} \frac{u^m}{m!} \in \mathbf{Z}_p\langle\langle u \rangle\rangle., \qquad \frac{s(u)^h}{h!} = \sum_{m=h}^{\infty} d_m^{(h)} \frac{u^m}{m!} \in \mathbf{Z}_p\langle\langle u \rangle\rangle. \tag{14.7}$$

Here, obviously $c_h^{(h)} = d_h^{(h)} = 1$. The results are as follows.

LEMMA 14.8. *If $\nu > 0$ and $m \geqq a+1$, then*

$$\sum_{r=0}^{a} \binom{a}{r} (-A_p)^{a-r} c_{m+r(p-1)}^{(h)} \equiv 0 \pmod{p^a},$$
$$\sum_{r=0}^{a} \binom{a}{r} (-A_p)^{a-r} d_{m+r(p-1)}^{(h)} \equiv 0 \pmod{p^a}. \tag{14.9}$$

PROOF. By 8.2(2), (3), and 8.3, we have

$$\mathbf{Z}_p\langle\langle u \rangle\rangle = \mathbf{Z}_p\langle\langle t \rangle\rangle. \tag{14.10}$$

For $D = d/du$ and any integer $h \geqq 1$, we show that

$$(D^p - A_p D)\Big(\frac{t^h}{h!}\Big) \in b + p\mathbf{Z}_p\langle\langle u \rangle\rangle, \qquad (b \in \mathbf{Z}_p) \tag{14.11}$$

by induction. If $h = 1$, this is checked by 13.13 and (14.10). Since

$$\begin{aligned} D(D^p - A_pD)\Big(\frac{t^{h+1}}{(h+1)!}\Big) &= (D^p - A_pD)\Big(\frac{t^h}{h!}\frac{dt}{du}\Big) \\ &= \Big(D^p\frac{t^h}{h!}\Big)\frac{dt}{du} + \sum_{j=1}^{p-1}\binom{p}{j}\Big(D^{p-j}\frac{t^h}{h!}\Big)\Big(D^j\frac{dt}{du}\Big) + \frac{t^h}{h!}\Big(D^p\frac{dt}{du}\Big) \\ &\quad - A_pD\Big(\frac{t^h}{h!}\Big)\frac{dt}{du} - A_p\frac{t^h}{h!}\Big(D\frac{dt}{du}\Big) \\ &\in \Big\{(D^p - A_pD)\frac{u^h}{h!}\Big\}\frac{dt}{du} + \frac{t^h}{h!}\Big\{(D^p - A_pD)\frac{dt}{du}\Big\} + p\mathbf{Z}_p\langle\langle u\rangle\rangle \end{aligned}$$

by using the hypothesis of induction, (13.15), and 13.13, we see that this belongs to $p\mathbf{Z}_p\langle\langle u\rangle\rangle$. Hence, we have

$$(D^p - A_pD)\Big(\frac{t^{h+1}}{(h+1)!}\Big) \in b + p\mathbf{Z}_p\langle\langle u\rangle\rangle \qquad (b \in \mathbf{Z}_p).$$

Thus, we have concluded (14.11). Using (14.11) repeatedly, we have, for $a > 0$, that

$$(D^p - A_pD)^a\Big(\frac{t^h}{h!}\Big) \in b + p^a\mathbf{Z}_p\langle\langle u\rangle\rangle \qquad (b \in \mathbf{Z}_p). \tag{14.12}$$

Because of

$$(D^p - A_pD)^a\Big(\frac{t^h}{h!}\Big) = \sum_{m=h}^{\infty}\Big\{\sum_{r=0}^{a}\binom{a}{r}(-A_p)^{a-r}c^{(h)}_{m+r(p-1)}\Big\}D^a\frac{u^m}{m!},$$

we obtain the first formula. The second one is proved similarly. □

14.3 Generalization of the Vandiver-Carlitz congruence

In this subsection, we prove the congruence relation of Vandiver-Carlitz style. Vandiver gave in [V] such the congruence for Bernoulli numbers, and Carlitz investigated in [Ca4] for Hurwitz numbers.

Proposition 14.13. *Let $a > 0$ and $\nu > 0$ are integers. Let $n = a + 1$. For the numbers $\{C_n^{(\nu)}\}$ and $\{D_n^{(\nu)}\}$ defined in* (14.1) *or* (14.4)*, we have*

$$\sum_{r=0}^{a}\binom{a}{r}(-A_p)^{a-r}C^{(\nu)}_{n+r(p-1)} \equiv 0 \mod p^{a-\nu},$$
$$\sum_{r=0}^{a}\binom{a}{r}(-A_p)^{a-r}D^{(\nu)}_{n+r(p-1)} \equiv 0 \mod p^{a-\nu}.$$

Remark 14.14. These congruence relations need not the condition $(p-1)\nmid n$ in contrary to 7.1, 7.5, 14.3, 14.6. However, since 14.13 can be proved without (13.10) and 13.1, it would be not so deep results.

PROOF. As in 10.1, we let $[t^{n+1}/(n+1)]u(t) = f_n$. Here we use still the notation $u = u_g$, $D = d/du$. Since

$$\sum_{m=0}^{\infty} C_m^{(1)} \frac{u^m}{m!} = \frac{u}{t(u)} = \frac{1}{t} \sum_{m=\nu}^{\infty} f_h \frac{t^{h+1}}{h+1}$$
$$= \sum_{h=0}^{\infty} \frac{f_h h!}{h+1} \sum_{m=h}^{\infty} c_m^{(h)} \frac{u^m}{m!} = \sum_{m=0}^{\infty} \left(\sum_{h=0}^{m} \frac{f_h h!}{h+1} c_m^{(h)} \right) \frac{u^m}{m!}$$

we have

$$C_m^{(1)} = \sum_{h=0}^{m} \frac{f_h h!}{h+1} c_m^{(h)}. \tag{14.15}$$

Therefore,

$$\sum_{r=0}^{a} \binom{a}{r} (-A_p)^{a-r} C_{m+r(p-1)}^{(1)} = \sum_{r=0}^{a} \binom{a}{r} (-A_p)^{a-r} \sum_{h=0}^{m+r(p-1)} \frac{f_h h!}{h+1} c_{m+r(p-1)}^{(h)}$$
$$= \sum_{h=0}^{m+r(p-1)} \frac{f_h h!}{h+1} \sum_{m=0}^{a} \binom{a}{r} (-A_p)^{a-r} c_{m+r(p-1)}^{(h)}.$$

If $m \geqq a+1$, then the inner sum is divisible by p^a because of (14.8). If $p^w || (h+1)$ $(w \geqq 1)$, then $p^w - 1 \leqq h$, and $\mathrm{ord}_p(p^w-1)! \leqq \mathrm{ord}_p h!$. By (1.2), we see that

$$\mathrm{ord}_p(p^w-1)! = \frac{(p^w-1)-(p-1)w}{p-1} = p^{w-1} + p^{w-2} + \cdots + p + 1 - w.$$

In our situation, we may assume $p \leqq 3$. Hence, the above is $\geqq w$ if $w \geqq 2$. The worst case is when $w = 1$, so that

$$w \leqq \mathrm{ord}_p h! + 1, \qquad (w \geqq 1). \tag{14.16}$$

Therefore

$$\sum_{r=0}^{a} \binom{a}{r} (-A_p)^{a-r} C_{m+r(p-1)}^{(1)} \ \in \ p^{a-1} \mathbf{Z}_{(p)} \qquad (m \geqq a+1). \tag{14.17}$$

This is just the case of $\nu = 1$ of the first formula in Theorem 14.3. The general case is proved similarly as follows. Since $u = \sum_{h=0}^{\infty} f_h \frac{t^{h+1}}{h+1}$, we see

$$u^\nu = \sum_{h=0}^{\infty} \sum_{\substack{h_1+h_2+\cdots \\ +h_\nu = h}} \frac{f_{h_1}}{h_1+1} \frac{f_{h_2}}{h_2+1} \cdots \frac{f_{h_\nu}}{h_\nu+1} t^{h+\nu}.$$

Hence

$$\left(\frac{u}{t}\right)^\nu = \sum_{h=0}^{\infty} \sum_{\substack{h_1+h_2+\cdots \\ +h_\nu = h}} \frac{f_{h_1}}{h_1+1} \frac{f_{h_2}}{h_2+1} \cdots \frac{f_{h_\nu}}{h_\nu+1} t^h$$

$$
\begin{aligned}
&=\sum_{h=0}^{\infty}\sum_{\substack{h_1+h_2+\cdots\\+h_\nu=h}}\frac{f_{h_1}}{h_1+1}\frac{f_{h_2}}{h_2+1}\cdots\frac{f_{h_\nu}}{h_\nu+1}\,h!\sum_{m=h}^{\infty}c_m^{(h)}\frac{u^m}{m!}\\
&=\sum_{m=0}^{\infty}\left(\sum_{h=0}^{m}h!\sum_{\substack{h_1+h_2+\cdots\\+h_\nu=h}}\frac{f_{h_1}}{h_1+1}\frac{f_{h_2}}{h_2+1}\cdots\frac{f_{h_\nu}}{h_\nu+1}c_m^{(h)}\right)\frac{u^m}{m!},
\end{aligned}
$$

and that

$$
\frac{1}{t^\nu}=\sum_{m=0}^{\infty}\frac{1}{(m)_\nu}\left(\sum_{h=0}^{m}h!\sum_{\substack{h_1+h_2+\cdots\\+h_\nu=h}}\frac{f_{h_1}}{h_1+1}\frac{f_{h_2}}{h_2+1}\cdots\frac{f_{h_\nu}}{h_\nu+1}c_m^{(h)}\right)\frac{u^{m-\nu}}{(m-\nu)!}.
$$

This development yields that

$$
C_m^{(\nu)}=\sum_{h=0}^{m}h!\sum_{\substack{h_1+h_2+\cdots\\+h_\nu=h}}\frac{f_{h_1}}{h_1+1}\frac{f_{h_2}}{h_2+1}\cdots\frac{f_{h_\nu}}{h_\nu+1}c_m^{(h)}. \tag{14.18}
$$

and that

$$
\begin{aligned}
\sum_{r=0}^{a}\binom{a}{r}(-A_p)^{a-r}C_{n+r(p-1)}^{(\nu)}=\sum_{h=0}^{m}&\left(h!\sum_{\substack{h_1+h_2+\cdots\\+h_\nu=h}}\frac{f_{h_1}}{h_1+1}\frac{f_{h_2}}{h_2+1}\cdots\frac{f_{h_\nu}}{h_\nu+1}\right)\\
&\cdot\left\{\sum_{r=0}^{a}\binom{a}{r}(-A_p)^{a-r}c_{n+r(p-1)}^{(h)}\right\}.
\end{aligned} \tag{14.19}
$$

If we assume $p^{w_j}||(h_j+1)$, then, as in (14.16), we conclude

$$
w_1+\cdots+w_\nu\leqq \mathrm{ord}_p(h_1!h_2!\cdots h_\nu!)+\nu\leqq \mathrm{ord}_p(h!)+\nu
$$

because $w_j\leqq \mathrm{ord}_p h_j!+1$. This shows that the right hand side of (14.19) is divisible by $p^{a-\nu}$. Thus, we have proved the first congruence in (14.13). The second one is proved similarly. □

15 Numerical examples on classical numbers

15.1 Bernoulli numbers

First several values of $C_{2n} = (-1)^{n-1}2^{2n}B_{2n}$ (B_{2n} is the $2n$-th Bernoulli number) of the curve $y^2 = x - 1$ ($g = 0$) are as follows:

$$
\begin{aligned}
2^2B_2 &= \frac{1}{3}\cdot 2, \qquad -2^4B_4 = \frac{1}{3\cdot 5}\cdot 2^3, \qquad 2^6B_6 = \frac{1}{3\cdot 7}\cdot 2^5,\\
-2^8B_8 &= \frac{1}{3\cdot 5}\cdot 2^7, \qquad 2^{10}B_{10} = \frac{1}{3\cdot 11}\cdot 2^9\cdot 5,\\
-2^{12}B_{12} &= \frac{1}{3\cdot 5\cdot 7\cdot 13}\cdot 2^{11}\cdot 691, \qquad 2^{14}B_{14} = \frac{1}{3}\cdot 2^{15}\cdot 7,\\
-2^{16}B_{16} &= \frac{1}{3\cdot 5\cdot 17}\cdot 2^{15}\cdot 3617, \qquad 2^{18}B_{18} = \frac{1}{3\cdot 5\cdot 19}\cdot 2^{17}\cdot 43867,\\
-2^{20}B_{20} &= \frac{1}{3\cdot 5\cdot 11}\cdot 2^{19}\cdot 283\cdot 617,\\
2^{22}B_{22} &= \frac{1}{3\cdot 23}\cdot 2^{21}\cdot 11\cdot 131\cdot 593,\\
-2^{24}B_{24} &= \frac{1}{3\cdot 5\cdot 7\cdot 13}\cdot 2^{23}\cdot 103\cdot 2294797,\\
2^{26}B_{26} &= \frac{1}{3}\cdot 2^{25}\cdot 13\cdot 657931,\\
-2^{28}B_{28} &= \frac{1}{3\cdot 5\cdot 29}\cdot 2^{27}\cdot 7\cdot 9349\cdot 362903,\\
2^{30}B_{30} &= \frac{1}{3\cdot 7\cdot 11\cdot 31}\cdot 2^{29}\cdot 5\cdot 1721\cdot 1001259881,\\
-2^{32}B_{32} &= \frac{1}{3\cdot 5\cdot 17}\cdot 2^{31}\cdot 37\cdot 683\cdot 305065927,\\
2^{34}B_{34} &= \frac{1}{3}\cdot 2^{33}\cdot 2^{33}\cdot 17\cdot 151628697551,\\
-2^{36}B_{36} &= \frac{1}{3\cdot 5\cdot 7\cdot 13\cdot 19\cdot 37}\cdot 2^{35}\cdot 26315271553053477373,\\
2^{38}B_{38} &= \frac{1}{3}\cdot 2^{37}\cdot 19\cdot 154210205991661,\\
-2^{40}B_{40} &= \frac{1}{3\cdot 5\cdot 11\cdot 41}\cdot 2^{39}\cdot 137616929\cdot 1897170067619,\\
2^{42}B_{42} &= \frac{1}{3\cdot 7\cdot 43}\cdot 2^{41}\cdot 1520097643918070802691,\\
-2^{44}B_{44} &= \frac{1}{3\cdot 5\cdot 23}\cdot 2^{43}\cdot 11\cdot 59\cdot 8089\cdot 2947939\cdot 1798482437,\\
2^{46}B_{46} &= \frac{1}{3\cdot 47}\cdot 2^{45}\cdot 23\cdot 383799511\cdot 67568238839737,\\
-2^{48}B_{48} &= \frac{1}{3\cdot 5\cdot 7\cdot 13\cdot 17}\cdot 2^{47}\cdot 653\cdot 56039\cdot 153289748932447906241,\\
2^{50}B_{50} &= \frac{1}{3\cdot 11}\cdot 2^{49}\cdot 5^2\cdot 417202699\cdot 47464429777438199.
\end{aligned}
$$

15.2 Hurwitz numbers for the curve $y^2 = x^3 - 1$

First several values of C_{6n} for the curve $y^2 = x^3 - 1$ ($g = 1$) are as follows:

$$C_6 = \frac{1}{7} \cdot 2^4 \cdot 3^2, \qquad C_{12} = \frac{-1}{7 \cdot 13} \cdot 2^{10} \cdot 3^5 \cdot 5^2,$$

$$C_{18} = \frac{1}{7 \cdot 19} \cdot 2^{16} \cdot 3^8 \cdot 5^3 \cdot 11, \qquad C_{24} = \frac{-1}{7 \cdot 13} \cdot 2^{22} \cdot 3^{11} \cdot 5^3 \cdot 11^2 \cdot 17,$$

$$C_{30} = \frac{1}{7 \cdot 31} \cdot 2^{28} \cdot 3^{14} \cdot 5^6 \cdot 11^2 \cdot 17 \cdot 23,$$

$$C_{36} = \frac{-1}{7 \cdot 13 \cdot 19 \cdot 37} \cdot 2^{34} \cdot 3^{17} \cdot 5^7 \cdot 11^3 \cdot 17^2 \cdot 23 \cdot 29 \cdot 43,$$

$$C_{42} = \frac{1}{7 \cdot 43} \cdot 2^{40} \cdot 3^{20} \cdot 5^8 \cdot 11^3 \cdot 17^2 \cdot 23 \cdot 29 \cdot 431,$$

$$C_{48} = \frac{-1}{7 \cdot 13} \cdot 2^{46} \cdot 3^{23} \cdot 5^8 \cdot 11^4 \cdot 17^2 \cdot 23^2 \cdot 29 \cdot 41 \cdot 313,$$

$$C_{54} = \frac{1}{7 \cdot 19} \cdot 2^{52} \cdot 3^{26} \cdot 5^{10} \cdot 11^4 \cdot 17^3 \cdot 23^2 \cdot 29 \cdot 41 \cdot 47 \cdot 1201,$$

$$C_{60} = \frac{-1}{7 \cdot 13 \cdot 31 \cdot 61} \cdot 2^{58} \cdot 3^{29} \cdot 5^{13} \cdot 11^5 \cdot 17^3 \cdot 23^2 \cdot 29^2 \cdot 41^2 \cdot 47 \cdot 53 \cdot 1823,$$

$$C_{66} = \frac{1}{7 \cdot 67} \cdot 2^{64} \cdot 3^{32} \cdot 5^{13} \cdot 11^6 \cdot 17^3 \cdot 23^2 \cdot 29^2 \cdot 41 \cdot 47 \cdot 53 \cdot 59 \cdot 79 \cdot 733,$$

$$C_{72} = \frac{-1}{7 \cdot 13 \cdot 19 \cdot 37 \cdot 73} \cdot 2^{70} \cdot 3^{35} \cdot 5^{13} \cdot 11^6 \cdot 17^4 \cdot 23^3 \cdot 29^2 \cdot 41 \cdot 47 \cdot 53 \cdot 59 \cdot 1153 \cdot 13963 \cdot 29059,$$

$$C_{78} = \frac{1}{7 \cdot 79} \cdot 2^{76} \cdot 3^{38} \cdot 5^{15} \cdot 11^7 \cdot 13 \cdot 17^4 \cdot 23^3 \cdot 29^2 \cdot 41 \cdot 43 \cdot 47 \cdot 53 \cdot 59 \cdot 71 \cdot 2647111,$$

$$C_{84} = \frac{-1}{7 \cdot 13 \cdot 43} \cdot 2^{82} \cdot 3^{41} \cdot 5^{17} \cdot 11^7 \cdot 17^4 \cdot 23^3 \cdot 29^2 \cdot 41^2 \cdot 47 \cdot 53 \cdot 59 \cdot 71 \cdot 8431097574437,$$

$$C_{90} = \frac{1}{7 \cdot 19 \cdot 31} \cdot 2^{88} \cdot 3^{44} \cdot 5^{19} \cdot 11^8 \cdot 17^5 \cdot 23^3 \cdot 29^3 \cdot 41^2 \cdot 47 \cdot 53 \cdot 59 \cdot 71 \cdot 83 \cdot 998039409083,$$

$$C_{96} = \frac{-1}{7 \cdot 13 \cdot 97} \cdot 2^{94} \cdot 3^{47} \cdot 5^{18} \cdot 11^8 \cdot 17^5 \cdot 23^4 \cdot 29^3 \cdot 41^2 \cdot 47^2 \cdot 53 \cdot 59 \cdot 71 \cdot 83 \cdot 89 \cdot 253013 \cdot 826151671,$$

$$C_{102} = \frac{1}{7 \cdot 103} \cdot 2^{100} \cdot 3^{50} \cdot 5^{20} \cdot 11^9 \cdot 17^6 \cdot 23^4 \cdot 29^4 \cdot 41^2 \cdot 47^2 \cdot 53 \cdot 59 \cdot 71 \cdot 83 \cdot 89 \cdot 433 \cdot 1493 \cdot 532620611,$$

$$C_{108} = \frac{-1}{7 \cdot 13 \cdot 19 \cdot 37 \cdot 109} \cdot 2^{106} \cdot 3^{53} \cdot 5^{22} \cdot 11^9 \cdot 17^6 \cdot 23^4 \cdot 29^3 \cdot 41^2 \cdot 47^2 \cdot 53^2 \cdot 59 \cdot 71 \cdot 83 \cdot 89 \cdot 101 \cdot 38543 \cdot 72745827951021097.$$

15.3 Hurwitz numbers for the curve $y^2 = x^3 - x$

First several values of $C_{4n} = 2^{4n}E_{4n}$ (E_{4n} is the $4n$-th original Hurwitz number) for the curve $y^2 = x^3 - x$ ($g = 1$) are as follows:

$$2^4E_4 = \frac{1}{5}\cdot 2^3\cdot 3, \qquad 2^8E_8 = \frac{1}{5}\cdot 2^7\cdot 3, \qquad 2^{12}E_{12} = \frac{1}{5\cdot 13}\cdot 2^{11}\cdot 3^4\cdot 7,$$

$$2^{16}E_{16} = \frac{1}{5\cdot 17}\cdot 2^{15}\cdot 3^4\cdot 7^2\cdot 11, \qquad 2^{20}E_{20} = \frac{1}{5}\cdot 2^{19}\cdot 3^6\cdot 7^2\cdot 11,$$

$$2^{24}E_{24} = \frac{1}{5\cdot 13}\cdot 2^{23}\cdot 3^7\cdot 7^3\cdot 11^2\cdot 19,$$

$$2^{28}E_{28} = \frac{1}{5\cdot 29}\cdot 2^{27}\cdot 3^9\cdot 7^4\cdot 11^2\cdot 19\cdot 23,$$

$$2^{32}E_{32} = \frac{1}{5\cdot 17}\cdot 2^{31}\cdot 3^{10}\cdot 7^4\cdot 11^2\cdot 19\cdot 23\cdot 223,$$

$$2^{36}E_{36} = \frac{1}{5\cdot 13\cdot 37}\cdot 2^{35}\cdot 3^{14}\cdot 7^5\cdot 11^3\cdot 19\cdot 23\cdot 31\cdot 61,$$

$$2^{40}E_{40} = \frac{1}{5\cdot 41}\cdot 2^{39}\cdot 3^{13}\cdot 7^5\cdot 11^3\cdot 19^2\cdot 23\cdot 31\cdot 2381,$$

$$2^{44}E_{44} = \frac{1}{5}\cdot 2^{43}\cdot 3^{15}\cdot 7^6\cdot 11^4\cdot 19^4\cdot 23\cdot 31,$$

$$2^{48}E_{48} = \frac{1}{5\cdot 13\cdot 17}\cdot 2^{47}\cdot 3^{16}\cdot 7^5\cdot 11^4\cdot 19^2\cdot 23^2\cdot 31\cdot 43\cdot 1162253,$$

$$2^{52}E_{52} = \frac{1}{5\cdot 53}\cdot 2^{51}\cdot 3^{18}\cdot 7^7\cdot 11^4\cdot 13\cdot 19^2\cdot 23^2\cdot 31\cdot 43\cdot 47\cdot 8887,$$

$$2^{56}E_{56} = \frac{1}{5\cdot 29}\cdot 2^{55}\cdot 3^{19}\cdot 7^8\cdot 11^5\cdot 19^2\cdot 23^2\cdot 31\cdot 43\cdot 47\cdot 61\cdot 52289,$$

$$2^{60}E_{60} = \frac{1}{5\cdot 13\cdot 61}\cdot 2^{59}\cdot 3^{22}\cdot 7^8\cdot 11^5\cdot 19^3\cdot 23^2\cdot 31\cdot 43\cdot 47\cdot 2630966033,$$

$$2^{64}E_{64} = \frac{1}{5\cdot 17}\cdot 2^{63}\cdot 3^{22}\cdot 7^9\cdot 11^5\cdot 19^3\cdot 23^2\cdot 31^2\cdot 43\cdot 47\cdot 59\cdot 109\cdot 814903,$$

$$2^{68}E_{68} = \frac{1}{5}\cdot 2^{67}\cdot 3^{24}\cdot 7^9\cdot 11^6\cdot 17\cdot 19\cdot 23^2\cdot 31^2\cdot 43\cdot 47\cdot 59\cdot 80232721,$$

$$2^{72}E_{72} = \frac{1}{5\cdot 13\cdot 37\cdot 73}\cdot 2^{71}\cdot 3^{25}\cdot 7^{10}\cdot 11^6\cdot 19^3\cdot 23^3\cdot 31^2\cdot 43\cdot 47\cdot 59\cdot 67 \cdot 48316510111193,$$

$$2^{76}E_{76} = \frac{1}{5}\cdot 2^{75}\cdot 3^{27}\cdot 7^{10}\cdot 11^6\cdot 19^4\cdot 23^3\cdot 31^2\cdot 43\cdot 47\cdot 59\cdot 67\cdot 71\cdot 3469 \cdot 1330177.$$

16 Numerical examples for new numbers

16.1 $x(\boldsymbol{u})$ of the curve $y^2 = x^5 - 1$

First several values of C_{10n} for the curve $y^2 = x^5 - 1$ ($g = 2$) are computed. The following is a progrm for `pari/GP` written by Naruoa Kano which gives the series expansion of $x\langle u\rangle$ with respect to u.

```
/*
Formal expansion of  x(u)  for the curve  y^2 = x^5 - 1  (by N. Kanou)
*/
\ps190;allocatemem(10^10);
serintgl(f,v=x)={
sum(n=0,poldegree(Pol(f)),polcoeff(Pol(f),n)*v^(n+1)/(n+1))+f-f};
x_of_u=1/subst(serreverse(-serintgl(1/sqrt(1-x^10)))^2,x,u);
print("x(u)=",x_of_u);
end;
```

Using this, we have the following numbers:

$$
\begin{aligned}
C_{10} &= \frac{1}{11}\cdot 2^8\cdot 3^2\cdot 5^2\cdot 7,\\
C_{20} &= \frac{-1}{11}\cdot 2^{18}\cdot 3^9\cdot 5^4\cdot 7\cdot 13\cdot 17,\\
C_{30} &= \frac{1}{11\cdot 31}\cdot 2^{28}\cdot 3^{14}\cdot 5^7\cdot 7^3\cdot 13^2\cdot 17\cdot 19\cdot 23^2,\\
C_{40} &= \frac{-1}{11\cdot 41}\cdot 2^{38}\cdot 3^{17}\cdot 5^9\cdot 7^3\cdot 13^2\cdot 17^2\cdot 19^2\cdot 23\cdot 29\cdot 37\cdot 31991,\\
C_{50} &= \frac{1}{11}\cdot 2^{47}\cdot 3^{23}\cdot 5^{12}\cdot 7^6\cdot 13^3\cdot 17\cdot 19^2\cdot 23^2\cdot 29\cdot 37\cdot 43\cdot 47\cdot 4999,\\
C_{60} &= \frac{-1}{11\cdot 31\cdot 61}\cdot 2^{59}\cdot 3^{28}\cdot 5^{15}\cdot 7^6\cdot 13^4\cdot 17^2\cdot 19^3\cdot 23^2\cdot 29^2\cdot 37\cdot 43\\
&\quad\cdot 47\cdot 53\cdot 351453077,\\
C_{70} &= \frac{1}{11\cdot 71}\cdot 2^{72}\cdot 3^{31}\cdot 5^{16}\cdot 7^9\cdot 13^5\cdot 17^3\cdot 19^3\cdot 23^2\cdot 29^2\cdot 37\cdot 43\\
&\quad\cdot 47\cdot 53\cdot 59\cdot 67\cdot 6740734411,\\
C_{80} &= \frac{-1}{11\cdot 41}\cdot 2^{78}\cdot 3^{34}\cdot 5^{19}\cdot 7^8\cdot 13^6\cdot 17^3\cdot 19^4\cdot 23^3\cdot 29^2\cdot 37^2\cdot 43\\
&\quad\cdot 47\cdot 53\cdot 59\cdot 67\cdot 73\cdot 109\cdot 460903\cdot 121384433,\\
C_{90} &= \frac{1}{11\cdot 31}\cdot 2^{87}\cdot 3^{42}\cdot 5^{21}\cdot 7^{10}\cdot 13^6\cdot 17^4\cdot 19^4\cdot 23^3\cdot 29^3\cdot 37^2\cdot 43^2\\
&\quad\cdot 47\cdot 53\cdot 59\cdot 67^2\cdot 73\cdot 79\cdot 83\cdot 131\cdot 881\cdot 2799606697,\\
C_{100} &= \frac{-1}{11\cdot 101}\cdot 2^{97}\cdot 3^{47}\cdot 5^{24}\cdot 7^{11}\cdot 13^7\cdot 17^3\cdot 19^5\cdot 23^4\cdot 29^3\cdot 37^2\cdot 43^2
\end{aligned}
$$

$$\cdot 47^2 \cdot 53 \cdot 59 \cdot 67 \cdot 73 \cdot 79 \cdot 83 \cdot 89 \cdot 97 \cdot 10343 \cdot 1938718187373563,$$

$$C_{110} = \frac{1}{11} \cdot 2^{107} \cdot 3^{51} \cdot 5^{27} \cdot 7^{13} \cdot 13^{8} \cdot 17^{4} \cdot 19^{5} \cdot 23^{4} \cdot 29^{3} \cdot 37 \cdot 43^2$$
$$\cdot 47^2 \cdot 53^2 \cdot 59 \cdot 67 \cdot 73 \cdot 79 \cdot 83 \cdot 89 \cdot 97 \cdot 103 \cdot 107$$
$$\cdot 3019729 \cdot 865724129494813,$$

$$C_{120} = \frac{-1}{11 \cdot 31 \cdot 41 \cdot 61} \cdot 2^{119} \cdot 3^{56} \cdot 5^{29} \cdot 7^{13} \cdot 13^{9} \cdot 17^{5} \cdot 19^{6} \cdot 23^{5} \cdot 29^{4} \cdot 37^2 \cdot 43^2$$
$$\cdot 47^2 \cdot 53^2 \cdot 59^2 \cdot 67 \cdot 73 \cdot 79 \cdot 83 \cdot 89 \cdot 97 \cdot 103 \cdot 107 \cdot 109 \cdot 113$$
$$\cdot 863833294249 \cdot 7389430581319,$$

$$C_{130} = \frac{1}{11 \cdot 131} \cdot 2^{128} \cdot 3^{61} \cdot 5^{32} \cdot 7^{15} \cdot 13^{11} \cdot 17^{5} \cdot 19^{6} \cdot 23^{5} \cdot 29^{4} \cdot 37^2 \cdot 43^2$$
$$\cdot 47^2 \cdot 53^2 \cdot 59^2 \cdot 67 \cdot 73 \cdot 79 \cdot 83 \cdot 89 \cdot 97 \cdot 103 \cdot 107 \cdot 109 \cdot 113 \cdot 127$$
$$\cdot 5303 \cdot 97785319 \cdot 175363749323953511,$$

$$C_{140} = \frac{-1}{11 \cdot 71} \cdot 2^{139} \cdot 3^{65} \cdot 5^{34} \cdot 7^{15} \cdot 13^{10} \cdot 17^{6} \cdot 19^{7} \cdot 23^{6} \cdot 29^{4} \cdot 37^2 \cdot 43^3$$
$$\cdot 47 \cdot 53^2 \cdot 59^2 \cdot 67^2 \cdot 73 \cdot 79 \cdot 83 \cdot 89 \cdot 97 \cdot 103 \cdot 107 \cdot 109 \cdot 113 \cdot 127$$
$$\cdot 137 \cdot 3191 \cdot 79927801 \cdot 29275193260775904153310 21,$$

$$C_{150} = \frac{1}{11 \cdot 31 \cdot 151} \cdot 2^{150} \cdot 3^{70} \cdot 5^{37} \cdot 7^{17} \cdot 13^{12} \cdot 17^{5} \cdot 19^{7} \cdot 23^{6} \cdot 29^{5} \cdot 37^3 \cdot 43^3$$
$$\cdot 47^2 \cdot 53^2 \cdot 59^2 \cdot 67^2 \cdot 73^2 \cdot 79 \cdot 83 \cdot 89 \cdot 97 \cdot 103 \cdot 107 \cdot 109 \cdot 113 \cdot 127$$
$$\cdot 137 \cdot 139 \cdot 50951 \cdot 450127 \cdot 1464426640811 \cdot 58871719018640089,$$

$$C_{160} = \frac{-1}{11 \cdot 41} \cdot 2^{158} \cdot 3^{72} \cdot 5^{40} \cdot 7^{17} \cdot 13^{12} \cdot 17^{6} \cdot 19^{8} \cdot 23^{6} \cdot 29^{5} \cdot 37^3 \cdot 43^3$$
$$\cdot 47^2 \cdot 53^2 \cdot 59^2 \cdot 67^2 \cdot 73^2 \cdot 79^2 \cdot 83 \cdot 89 \cdot 97 \cdot 103 \cdot 107 \cdot 109 \cdot 113 \cdot 127 \cdot 137$$
$$\cdot 139 \cdot 149 \cdot 157 \cdot 5473709 \cdot 22543502622365730931551293201565706511,$$

$$C_{170} = \frac{1}{11} \cdot 2^{167} \cdot 3^{78} \cdot 5^{42} \cdot 7^{19} \cdot 13^{12} \cdot 17^{8} \cdot 19^{8} \cdot 23^{7} \cdot 29^{5} \cdot 37^3 \cdot 43^3$$
$$\cdot 47^2 \cdot 53^3 \cdot 59^2 \cdot 67^2 \cdot 73^2 \cdot 79^2 \cdot 83^2 \cdot 89 \cdot 97 \cdot 103 \cdot 107 \cdot 109 \cdot 113 \cdot 127$$
$$\cdot 137 \cdot 139 \cdot 149 \cdot 157 \cdot 163 \cdot 167$$
$$\cdot 587 \cdot 22573 \cdot 18793 \cdot 246289 \cdot 311203545376580358674935387,$$

$$C_{180} = \frac{-1}{11 \cdot 31 \cdot 61 \cdot 181} \cdot 2^{177} \cdot 3^{87} \cdot 5^{45} \cdot 7^{19} \cdot 13^{15} \cdot 17^{7} \cdot 19^{9} \cdot 23^{7} \cdot 29^{6} \cdot 37^3 \cdot 43^4$$
$$\cdot 47^2 \cdot 53^3 \cdot 59^3 \cdot 67^2 \cdot 73^2 \cdot 79^2 \cdot 83^2 \cdot 89^2 \cdot 97 \cdot 103 \cdot 107 \cdot 109 \cdot 113 \cdot 127$$
$$\cdot 137 \cdot 139 \cdot 149 \cdot 157 \cdot 163 \cdot 167 \cdot 173$$
$$\cdot 239 \cdot 1471 \cdot 1579 \cdot 703099922168866706586174232301684313 8707.$$

Each C_{10n} is writen by a certain integer G_{10n} (von Staudt-Clausen type theorem) as follows:

$$
\begin{aligned}
C_{10} &= \frac{6}{11} + G_{10},\\
C_{20} &= \frac{6^2}{11} + G_{20},\\
C_{30} &= \frac{6^3}{11} + \frac{10}{31} + G_{30},\\
C_{40} &= \frac{6^4}{11} + \frac{7}{41} + G_{40},\\
C_{50} &= \frac{6^5}{11} + G_{50},\\
C_{60} &= \frac{6^6}{11} + \frac{10^2}{31} + \frac{1}{61} + G_{60},\\
C_{70} &= \frac{6^7}{11} + \frac{32}{71} + G_{70},\\
C_{80} &= \frac{6^8}{11} + \frac{7^2}{41} + G_{80},\\
C_{90} &= \frac{6^9}{11} + \frac{10^3}{31} + G_{90},\\
C_{100} &= \frac{6^{10}}{11} + \frac{46}{101} + G_{100},\\
C_{110} &= \frac{6^{11}}{11} + G_{110},\\
C_{120} &= \frac{6^{12}}{11} + \frac{10^4}{31} + \frac{7^3}{41} + \frac{1}{61} + G_{120},\\
C_{130} &= \frac{6^{13}}{11} + \frac{64}{131} + G_{130},\\
C_{140} &= \frac{6^{14}}{11} + \frac{32^2}{71} + G_{140},\\
C_{150} &= \frac{6^{15}}{11} + \frac{10^5}{31} + \frac{52}{151} + G_{150},\\
C_{160} &= \frac{6^{16}}{11} + \frac{7^4}{41} + G_{160},\\
C_{170} &= \frac{6^{17}}{11} + G_{170},\\
C_{180} &= \frac{6^{18}}{11} + \frac{10^6}{31} + \frac{1}{61} + \frac{37}{181} + G_{180}.
\end{aligned}
$$

16.2 $y(\boldsymbol{u})$ of the curve $y^2 = x^5 - 1$

First several values of D_{10n} for the curve $y^2 = x^5 - 1$ ($g = 2$) are as follows:

$$
\begin{aligned}
D_{10} &= \frac{1}{11} \cdot 2^4 \cdot 3^2 \cdot 5^2, \\
D_{20} &= \frac{1}{11} \cdot 2^{15} \cdot 3^6 \cdot 5^4 \cdot 7 \cdot 13, \\
D_{30} &= \frac{-1}{11 \cdot 31} \cdot 2^{23} \cdot 3^{11} \cdot 5^7 \cdot 7^2 \cdot 13^2 \cdot 17 \cdot 19 \cdot 23, \\
D_{40} &= \frac{1}{11 \cdot 41} \cdot 2^{35} \cdot 3^{17} \cdot 5^{10} \cdot 7^3 \cdot 13^2 \cdot 17^2 \cdot 19 \cdot 23 \cdot 29 \cdot 53, \\
D_{50} &= \frac{-1}{11} \cdot 2^{43} \cdot 3^{21} \cdot 5^{12} \cdot 7^4 \cdot 13^3 \cdot 17 \cdot 19^2 \cdot 23^2 \cdot 29 \cdot 37 \cdot 43 \cdot 683, \\
D_{60} &= \frac{1}{11 \cdot 31 \cdot 61} \cdot 2^{57} \cdot 3^{28} \cdot 5^{15} \cdot 7^6 \cdot 13^4 \cdot 17^2 \cdot 19^2 \cdot 23^2 \cdot 29 \cdot 37 \cdot 43 \cdot 47 \\
&\quad \cdot 53 \cdot 115781, \\
D_{70} &= \frac{-1}{11 \cdot 71} \cdot 2^{64} \cdot 3^{32} \cdot 5^{16} \cdot 7^8 \cdot 13^6 \cdot 17^2 \cdot 19^3 \cdot 23^2 \cdot 29^2 \cdot 37 \cdot 43 \cdot 47 \\
&\quad \cdot 53 \cdot 59 \cdot 22703881, \\
D_{80} &= \frac{1}{11 \cdot 41} \cdot 2^{75} \cdot 3^{33} \cdot 5^{19} \cdot 7^8 \cdot 13^6 \cdot 17^3 \cdot 19^4 \cdot 23^3 \cdot 29^2 \cdot 37^2 \cdot 43 \cdot 47 \\
&\quad \cdot 53 \cdot 59 \cdot 67 \cdot 73 \cdot 4580521741, \\
D_{90} &= \frac{-1}{11 \cdot 31} \cdot 2^{83} \cdot 3^{42} \cdot 5^{22} \cdot 7^9 \cdot 13^6 \cdot 17^4 \cdot 19^5 \cdot 23^3 \cdot 29^2 \cdot 37^2 \cdot 43^2 \cdot 47 \\
&\quad \cdot 53 \cdot 59 \cdot 67 \cdot 73 \cdot 79 \cdot 83 \cdot 9601 \cdot 1285049, \\
D_{100} &= \frac{1}{11 \cdot 101} \cdot 2^{94} \cdot 3^{44} \cdot 5^{24} \cdot 7^{11} \cdot 13^7 \cdot 17^3 \cdot 19^5 \cdot 23^4 \cdot 29^3 \cdot 37^2 \cdot 43^2 \cdot 47^2 \\
&\quad \cdot 53 \cdot 59 \cdot 67 \cdot 73 \cdot 79 \cdot 83 \cdot 89 \cdot 4002942001952573, \\
D_{110} &= \frac{-1}{11} \cdot 2^{102} \cdot 3^{48} \cdot 5^{27} \cdot 7^{12} \cdot 13^8 \cdot 17^4 \cdot 19^5 \cdot 23^4 \cdot 29^3 \cdot 37 \cdot 43^2 \cdot 47^2 \\
&\quad \cdot 53^2 \cdot 59 \cdot 67 \cdot 73 \cdot 79 \cdot 83 \cdot 89 \cdot 97 \cdot 103 \cdot 9747003959677530439, \\
D_{120} &= \frac{1}{11 \cdot 31 \cdot 41 \cdot 61} \cdot 2^{116} \cdot 3^{56} \cdot 5^{29} \cdot 7^{13} \cdot 13^9 \cdot 17^4 \cdot 19^6 \cdot 23^6 \cdot 29^4 \cdot 37^2 \\
&\quad \cdot 43^2 \cdot 47^2 \cdot 53^2 \cdot 59 \cdot 67 \cdot 73 \cdot 79 \cdot 83 \cdot 89 \cdot 97 \cdot 103 \cdot 107 \cdot 109 \cdot 113 \\
&\quad \cdot 1759 \cdot 2027 \cdot 2278423765903.
\end{aligned}
$$

16.3 $x(\boldsymbol{u})$ of the curve $y^2 = x^5 - x$

First several values of C_{8n} for the curve $y^2 = x^5 - x$ ($g = 2$) are as follows:

$$
\begin{aligned}
C_8 &= 2^7 \cdot 5, \\
C_{16} &= \frac{-1}{17} \cdot 2^{15} \cdot 3^2 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13, \\
C_{24} &= 2^{22} \cdot 3^4 \cdot 5^3 \cdot 7^3 \cdot 11^3 \cdot 13 \cdot 19, \\
C_{32} &= \frac{-1}{17} \cdot 2^{31} \cdot 3^6 \cdot 5^6 \cdot 7^4 \cdot 11 \cdot 13^2 \cdot 19 \cdot 23 \cdot 29 \cdot 1741, \\
C_{40} &= \frac{1}{41} \cdot 2^{40} \cdot 3^8 \cdot 5^8 \cdot 7^5 \cdot 11^2 \cdot 13^2 \cdot 19^2 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 5693, \\
C_{48} &= \frac{-1}{17} \cdot 2^{46} \cdot 3^{10} \cdot 5^8 \cdot, 7^5 \cdot 11^3 \cdot 13^3 \cdot 19^2 \cdot 23^2 \cdot 29 \cdot 31 \cdot 37 \cdot 43 \cdot 41957857, \\
C_{56} &= 2^{54} \cdot 3^{12} \cdot 5^{11} \cdot 7^8 \cdot 11^5 \cdot 13^4 \cdot 19 \cdot 23^2 \cdot 29 \cdot 31 \cdot 37 \cdot 43 \cdot 47 \cdot 53 \cdot 715991, \\
C_{64} &= \frac{-1}{17} \cdot 2^{63} \cdot 3^{14} \cdot 5^{12} \cdot 7^9 \cdot 11^3 \cdot 13^4 \cdot 19^2 \cdot 23^2 \cdot 29^2 \cdot 31^2 \cdot 37 \cdot 43 \cdot 47 \\
&\quad \cdot 53 \cdot 59 \cdot 61 \cdot 89 \cdot 32591401, \\
C_{72} &= \frac{1}{73} \cdot 2^{72} \cdot 3^{16} \cdot 5^{13} \cdot 7^{10} \cdot 11^4 \cdot 13^5 \cdot 19^2 \cdot 23^3 \cdot 29^2 \cdot 31^2 \cdot 37 \cdot 43 \cdot 47 \\
&\quad \cdot 53 \cdot 59 \cdot 61 \cdot 67 \cdot 19346595547931, \\
C_{80} &= \frac{-1}{17 \cdot 41} \cdot 2^{80} \cdot 3^{18} \cdot 5^{17} \cdot 7^{11} \cdot 11^5 \cdot 13^6 \cdot 19^3 \cdot 23^3 \cdot 29^2 \cdot 31^2 \cdot 37^2 \cdot 43 \cdot 47 \\
&\quad \cdot 53 \cdot 59 \cdot 61^2 \cdot 67 \cdot 71 \cdot 5826608412403.
\end{aligned}
$$

Each C_{8n} is written by a certain integer G_{8n} (von Staudt-Clausen type theorem) as follows:

$$\begin{aligned}
&C_{8} && \text{"an integer"},\\
&C_{16} = \frac{11}{17} && + G_{16},\\
&C_{24} && \text{"an integer"},\\
&C_{32} = \frac{11^2}{17} && + G_{32},\\
&C_{40} = \frac{35}{41} && + G_{40},\\
&C_{48} = \frac{11^3}{17} && + G_{48},\\
&C_{56} && \text{"an integer"},\\
&C_{64} = \frac{11^4}{17} && + G_{64},\\
&C_{72} = \frac{2}{73} && + G_{72},\\
&C_{80} = \frac{11^6}{17} + \frac{35^2}{41} && + G_{80},\\
&C_{88} = \frac{18}{89} && + G_{88},\\
&C_{96} = \frac{11^7}{17} + \frac{10}{97} && + G_{96},\\
&C_{104} && \text{"an integer"},\\
&C_{112} = \frac{11^8}{17} + \frac{18}{113} && + G_{112},\\
&C_{120} = \frac{35^3}{41} && + G_{120},\\
&C_{128} = \frac{11^9}{17} && + G_{128},\\
&C_{136} = \frac{131}{137} && + G_{136},\\
&C_{144} = \frac{11^{10}}{17} + \frac{2^2}{73} && + G_{144}.
\end{aligned}$$

17 Non-hyperelliptic curves

17.1 Algebraic curves ramified completely at infinity

We here describe how the natural variable u is chosen for a general curve of cyclotomic type.

Let a and b be coprime pair of positive integers, and let

$$f(x,y) = y^a - x^b - \sum_{(i,j)} \lambda_{ia+jb} x^i y^j \tag{17.1}$$

be separable polynomial, where the pair (i,j) runs through the integers such that

$$0 \leqq i < b-1, \quad 0 \leqq j < a-1, \quad ia+jb < ab \tag{17.2}$$

We discuss with the algebraic curve defined by

$$\mathscr{C} : f(x,y) = 0. \tag{17.3}$$

Here $\mathscr{C}$ is regarded naturally as a curve with unique point ∞ at infinity. The genus of $\mathscr{C}$ is given by $g = (a-1)(b-1)/2$. On this curve $\mathscr{C}$, the set

$$\frac{x^{i-1}y^{a-j-1}dx}{f_y(x,y)} \tag{17.4}$$

forms a basis of the differential forms of the first kind, where $f_y(x,y) = \frac{\partial f}{\partial y}(x,y)$. By choosing a generator of the fundamental group of $\mathscr{C}$, we define the period matrix $[\omega'\ \omega'']$. We also define the lattice of periods in $\mathbf{C}^g$ by

$$\Lambda := \omega'^t \begin{bmatrix} \mathbf{Z} & \mathbf{Z} & \cdots & \mathbf{Z} \end{bmatrix} + \omega''^t \begin{bmatrix} \mathbf{Z} & \mathbf{Z} & \cdots & \mathbf{Z} \end{bmatrix} \ (\subset \mathbf{C}^g). \tag{17.5}$$

We denote the Jacobian variety of $\mathscr{C}$ by J, and the symmetric product of g copies of $\mathscr{C}$ by $\mathrm{Sym}^g(\mathscr{C})$. Then we have a birational map

$$\begin{aligned} \mathrm{Sym}^g(\mathscr{C}) &\to \mathrm{Pic}^\circ(\mathscr{C}) = J \\ (P_1, \ldots, P_g) &\mapsto \text{the class of the divisor } P_1 + \cdots + P_g - g \cdot \infty. \end{aligned}$$

As an analytic manifold, J is identified with $\mathbf{C}^g/\Lambda$. We denote by κ the natural map $\mathbf{C}^g \to \mathbf{C}^g/\Lambda = J$. The map

$$\iota : Q \mapsto Q - \infty$$

gives an embedding of $\mathscr{C}$ into J. The pull-back $\kappa^{-1}\iota(\mathscr{C})$ of the image of ι by κ is a universal Abelian covering of $\mathscr{C}$. The birational map is represented analytically by sending each $(P_1, \ldots, P_g) \in \mathrm{Sym}^g(\mathscr{C})$ to the point $\boldsymbol{u} \mod \Lambda \in \mathbf{C}^g/\Lambda$, where

$$\boldsymbol{u} = (u_1, \ldots, u_g) = \left(\int_\infty^{P_1} + \cdots + \int_\infty^{P_g} \right) (\omega_1, \ \ldots, \ \omega_g).$$

For each point $\boldsymbol{u} \in \kappa^{-1}\iota(\mathscr{C})$, we denote by

$$x(\boldsymbol{u}), \qquad y(\boldsymbol{u}) \tag{17.6}$$

the value of (x, y)-coordinate of $\mathscr{C}$ such that $\kappa(\boldsymbol{u}) = \iota\,(x(\boldsymbol{u}),\ y(\boldsymbol{u}))$ We regard a rational function of $x(\boldsymbol{u})$ and $y(\boldsymbol{u})$ as a function on $\kappa^{-1}\iota(\mathscr{C})$. Basically, we have

LEMMA 17.7. *The Laurent development of* $x(\boldsymbol{u})$ *and* $y(\boldsymbol{u})$ *around the origin* $(0, \cdots, 0)$ *with respect to* u_g *is of the form*

$$x(\boldsymbol{u}) = \frac{1}{{u_g}^a} + (d^\circ(u_g \geqq -a+1)), \quad y(\boldsymbol{u}) = -\frac{1}{{u_g}^b} + (d^\circ(u_g \geqq -b+1)).$$

Moreover, we have a result correspond to 4.4, and we see that *It is natural to take* $u := u_g$ *as a local parameter around* $\boldsymbol{u} = (0, \cdots, 0)$ *on* $\kappa^{-1}\iota(\mathscr{C})$.

We call a curve $\mathscr{C}$ defined by $f(x, y) = 0$, where

$$f(x, y) = y^a - x^b + 1, \quad \text{or} \quad f(x, y) = y^a - x^b + x, \tag{17.8}$$

to be a curve *of cyclotomic type*. For such a curve $\mathscr{C}$, the Hurwitz coefficients of the power series development of the functions $u = u_g \mapsto x(\boldsymbol{u})$, $u_g \mapsto y(\boldsymbol{u})$ with respect to u satisfy the Clarke type theorem (von Staudt-Clausen type theorem plus the extension of von Staudt second theorem) and the Kummer type theorem. We can prove them by the same argument of this paper.

18 Appendices

18.1 Relations on binomial coefficients

The Hasse-Witt matrix with respect to the basis (4.1) for the curve $y^2 = x^5 - 1 \bmod p$ is diagonal ([Yu]), and its $(2,2)$-entry is, as in 6.3, given by

$$A_p = (-1)^{(p-1)/10} \cdot \binom{(p-1)/2}{(p-1)/10} \mod p.$$

We show that it coincide with the value (11.5). In other words, we claim, for a prime $p \equiv 1 \bmod 5$ by letting $p = 10m + 1$, that

$$\frac{(2m-1)!!}{m!2^m} \equiv (-1)^m \binom{5m}{m} \mod p.$$

Since this is equivalent to

$$\frac{(2m-1)!!}{m!} \equiv (-2)^m \binom{5m}{m} \mod p$$

we prove this. Because

$$2(5m), \quad 2(5m-1), \cdots, 2(5m-(m-1)) \mod p$$

are coincide with

$$-1, \quad -3, \cdots, \ -(2m-1) \mod p$$

respectively. Thus, we see the equation above. Similarly, we can prove

$$\frac{(5m-3)!!}{m!(-5)^m} \equiv (-1)^m \binom{5m}{m} \mod p.$$

Although, the facts above are proved by using basic properties of p-adic Γ-function, we have described them quite elementary way.

18.2 Links with certain Eisenstein type series

It is a natural question whether the numbers C_n and D_n relate a kind of L-function. In the below, we explain that such a question is not completely nonsense.

We recall the proof of Hurwitz formula, that is

$$\sum_{\substack{\lambda \in \mathbf{Z}+\mathbf{Z}\sqrt{-1} \\ \lambda \neq 0}} \frac{1}{\lambda^{4n}} = \frac{\varpi^{4n}}{(4n)!} 2^{4n} E_{4n} \tag{18.1}$$

along [Hu1](see also [AIK], pp.193-198), where

$$\varpi = \int_1^\infty \frac{dx}{\sqrt{x^3 - x}} (> 0).$$

After equating the two kinds of developments

$$
\begin{aligned}
\wp(u) &= \frac{1}{u^2} + \sum_{n=2}^{\infty} \frac{2^n E_n}{n} \frac{u^{n-2}}{(n-2)!}, \\
\wp(u) &= \frac{1}{u^2} + \sum_{\substack{\ell \in \mathbf{Z}\varpi + \mathbf{Z}\varpi\sqrt{-1} \\ \ell \neq 0}} \left(\frac{1}{(u-\ell)^2} - \frac{1}{\ell^2} \right),
\end{aligned} \tag{18.2}
$$

by removing $1/u^2$, and by differentiating them $4n-2$ times, we have (18.1) by substituting $u = 0$. This argument is similar to the proof of Euler's formula, namely the expression of the special value $\zeta(2m)$ of the Riemann zeta function by a Bernoulli number and π, by using two kinds of developments for $1/\sin^2(u)$.

For the case of a hyperelliptic curve of arbitrary genus g, $x(\boldsymbol{u})$ has Laurent expansion around each lattice point $\ell = (\ell_1, \ell_2, \cdots, \ell_g) \in \Lambda$ ($\subset \mathbf{C}^g$):

$$
x(\boldsymbol{u}) = \frac{1}{(u_g - \ell_g)^2} + \cdots . \tag{18.3}
$$

Although we do not have any justification, we could expect such the formula that

$$
x(\boldsymbol{u}) = \frac{1}{{u_g}^2} + \sum_{\substack{\ell \in \Lambda \\ \ell \neq 0}}^{*} \left(\frac{1}{(u_g - \ell_g)^2} - \frac{1}{{\ell_g}^2} \right), \tag{18.4}
$$

where $*$ means the sum is not justified. If such the formula exists, then, by the similar argument as in $\wp(u)$, we have the following type formulae:

—. for the curve $y^2 = x^{2g+1} - 1$,

$$
\sum_{\substack{\lambda \in L \\ \lambda \neq 0}}^{*} \frac{1}{\lambda^{2(2g+1)n}} = \frac{\Omega^{2(2g+1)n}}{(2(2g+1)n)!} C_{2(2g+1)n} \tag{18.5}
$$

where

$$
\Omega = \int_1^{\infty} \frac{x^{g-1} dx}{y} > 0
$$

and L is $1/\Omega$ times the image of the projection of $\Lambda \subset \mathbf{C}^g$ to the g-th factor $\mathbf{C}$ (For example, if $2g+1$ is a prime, then $L = \mathbf{Z}[e^{2\pi i/(2g+1)}]$), and

—. for the curve $y^2 = x^{2g+1} - x$,

$$
\sum_{\substack{\lambda \in L \\ \lambda \neq 0}}^{*} \frac{1}{\lambda^{4gn}} = \frac{\Omega^{4gn}}{(4gn)!} C_{4gn} \tag{18.6}
$$

where

$$
\Omega = \int_1^{\infty} \frac{x^{g-1} dx}{y} > 0
$$

and L is $1/\Omega$ times the image of the projection of $\Lambda \subset \mathbf{C}^g$ to the g-th factor $\mathbf{C}$.

If such results is obtained, it would be a discovery of new L-functions which is in the different category of Hecke's L-function associated to Grössen characters. The author also expects that this story relates to the thing written in [I], p.240.

18.3 Problems

We list some problems not yet proved and things to be investigated:

(1) Looking at the numerical examples, the signature of C_n or D_n are alternative or stable as in the cases of the Bernoulli and Hurwitz numbers. Prove this phenomena. This might be not so difficult.

(2) For example, about the curve $y^2 = x^5 - 1$, if $p \equiv 1 \mod 5$ and $(p-1) \not| \, 10m$ then $p \not| \, C_{10m}$.

(3) How large are the orders of 2-part of the numbers C_n and D_n? For the case of the Bernoulli and Hurwitz numbers, they are exactly determined. For instance, is it true that, for $y^3 = x^5 - 1$ ($g = 4$), $\mathrm{ord}_2 C_{15n} = 12n - 3$?

(4) For example, the prime factors in the numerators of C_{10m} and D_{10m} are quite similar though it is not exactly the same. Explain this theoretically.

References

[Ad1] A. Adelberg: Universal higher order Bernoulli numbers and Kummer and related congruences, J. Number Theory, **84** (2000) 119–135.

[Ad2] A. Adelberg: Kummer congruences for universal Bernoulli numbers and related congruences for poly-Bernoulli numbers, Int. Math. J., **1** (2002) 53–63.

[Ad3] A. Adelberg: Universal Kummer congruences mod prime powers, J. Number Theory, **109** (2004) 362–378

[AIK] T. Arakawa, T. Ibukiyama, M. Kaneko: Bernoulli numbers and zeta functions (in Japanese), Makino-shoten, (2001).

[Ca1] L. Carlitz: The coefficients of the reciprocal of a series, Duke Math. J., **8** (1941) 689–700.

[Ca2] L. Carlitz: Some properties of Hurwitz series, Duke Math. J., **16** (1949) 285–295.

[Ca3] L. Carlitz: Congruences for the coefficients of the Jacobi elliptic functions, Duke Math. J., **16** (1949) 297–302.

[Ca4] L. Carlitz: Congruences for the coefficients of hyperelliptic and related functions, Duke Math. J., **19** (1952) 329–337.

[Clau] T. Clausen: Theorem, Astronomische Nachrichten, **17** (1840) 351–352

[Clar] F. Clarke: The universal von Staudt theorem, Trans. Amer. Math. Soc., **315** (1989) 591–603.

[Co] L. Comtet: Advanced Combinatorics, The art of finite and infinite expansions (revised and enlarged edition), D.Reidel Pub. Company, (1974).

[G] H. Gunji: The Hasse invariant and p-division points of an elliptic curve, Arch. Math., **27** (1976) 148–157.

[Ha] M. Hazewinkel: Formal Groups and Applications, Pure and Applied Math. 78, Academic Press (1978).

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

[Hu1] A. Hurwitz: Über die Entwicklungskoeffizienten der lemniskatishen Funktionen, Nachr. Acad. Wiss. Göttingen, (1897)273-276, (Werke, Bd.II, pp.338–341).

[Hu2] A. Hurwitz: Über die Entwicklungskoeffizienten der lemniskatishen Funktionen, Math. Ann., **51** (1899) 196–226, (Werke, Bd.II, pp.342–373).

[I] T. Ibukiyama: Memoirs on "easy" zeta functions, Proceedings of the 9th summer school on "Zeta functions", (2001) 235–248.

[Ka1] N.M. Katz: The congruence of Clausen-von Staudt and Kummer for Bernoulli-Hurwitz numbers, Math. Ann., **216** (1975) 1–4.

[Ka2] N.M. Katz: Formal groups and p-adic interpolation, Astérisque, **41**/**42** (1977) 55–65.

[Ku] E.E. Kummer: Über eine allgemeine Eigenschaft der rationalen Entwickelungscoëffi-cienten einer bestimmten Gattung analytischer Functionen, J. für die reine und angew. Math., **41** (1851) 368–372.

[L] H. Lang: Kummersche Kongruenzen für die normierten Entwicklungskoeffizienten der Weierstrasschen $\wp$-Funktionen, Abh. Math. Sem. Hamburg, **33** (1969) 183–196.

[Ma] H. Matsumura: Commutative ring theory, Cambridge Univ. Press, (1980).

[Mo] Y. Morita: A p-adic analogue of the Γ-function, J. Fac. Sci. Univ. Tokyo Sect. IA Math., **22** (1975) 255–266.

[O] Y. Ônishi: Theory of The generalized Bernoulli-Hurwitz Numbers for the algebraic functions of cyclotomic type and the universal Bernoulli numbers, `http://arxiv.org/abs/math.NT/0406096`

[R] A.M. Robert: A course in p-adic analysis, G.T.M. **198**, Springer Verlag, (2000).

[RS] K.H. Rosen and W.M. Snyder: A Kummer congruence for the Hurwitz-Herglotz function, Tokyo J. Math., **6** (1983) 125–133.

[Sn1] C. Snyder: A concept of Bernoulli numbers in algebraic function fields, J. Reine Angew. Math., **307**/**308** (1978) 295–308.

[Sn2] C. Snyder: The coefficients of the Hessian elliptic functions, J. Reine Angew. Math., **306** (1979) 60–87.

[Sn3] C. Snyder: A concept of Bernoulli numbers in algebraic function fields (II), Manuscripta math., **35** (1981) 69–89.

[Sn4] C. Snyder: Kummer congruences for the coefficients of Hurwitz series, Acta Arith., **40** (1982) 175–191.

[Sn5] C. Snyder: Kummer congruences in formal groups and algebraic groups of dimension one, Rocky Mountain J. Math. **15** (1985) 1–11

[Sn6] C. Snyder: p-adic interpolation of the coefficients of Hurwitz series attached to height one formal groups, Rocky Mountain J. Math. **23** (1993) 339–351

[V] H.S. Vandiver: Certain congruence involving the Bernoulli numbers, Duke Math. J., **5** (1939) 548–551.

[vS1] K.G.C. von Staudt: Beweis eines Lehrsatzes, die Bernoullischen Zahlen betreffend, J. Reine Angew. Math., **21** (1840) 373–374

[vS2] K.G.C. von Staudt: De Numeris Bernoullianis, commentatio altera, Erlangen, (1845)

[Yu] N. Yui: On the Jacobian varieties of hyperelliptic curves over fields of characteristic $p > 2$, Journ. of Algebra, **52** (1978) 378–410.

[WW] E.T. Whittaker and G.N. Watson: A course of modern analysis, Cambridge Univ. Press, (1927).

Faculty of Education
and Human Sciences
University of Yamanashi
Kofu 400-8510
Japan

E-mail address: yonishi@yamanashi.ac.jp