Math-Net.Ru

Общероссийский математический портал

Е. Ониши, Обобщенные числа Бернулли–Гурвица и универсальные числа Бернулли, *УМН*, 2011, том 66, выпуск 5, 47–108

DOI: <https://doi.org/10.4213/rm9441>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением <http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.224.60.19

26 апреля 2023 г., 10:40:26

УДК 511.217+512.772+512.741

Обобщенные числа Бернулли–Гурвица и универсальные числа Бернулли

Ё. Ониши

Три фундаментальных свойства чисел Бернулли, а именно теорема фон Штаудта–Клаузена, вторая теорема фон Штаудта и исходное сравнение Куммера, обобщаются на новые числа, которые мы называем обобщенными числами Бернулли–Гурвица. Это коэффициенты разложения в степенной ряд алгебраической функции высшего рода относительно подходящей переменной. Наше обобщение сильно отличается от предыдущих работ. Действительно, порядок степени простого числа модуля наших сравнений типа Куммера в точности такой же, как в случае тригонометрических функций, а именно как в сравнении самого Куммера для исходных чисел Бернулли, и как в случае эллиптических функций, а именно как для обобщений Х. Лэнга чисел Гурвица. Однако в других более ранних результатах об алгебраических функциях высшего рода модуль был не более половины того, что в этих классических случаях. Это отличие разъясняется путем исследования аналога трех вышеупомянутых свойств для универсальных чисел Бернулли.

Библиография: 34 названия.

Ключевые слова: числа Бернулли, абелевы функции, формальные группы.

СОДЕРЖАНИЕ

Введение	49
Соглашения и обозначения	53
1. Предварительные сведения из комбинаторики	54
1.1. Основные сведения об операции факториала	54
1.2. Формула обращения Лагранжа	54
1.3. Основные сведения о биномиальных коэффициентах	54
2. Теорема Кларка	55
2.1. Определение универсальных чисел Бернулли	55
2.2. Разложение универсальных чисел Бернулли	56
2.3. Теорема Кларка	56

Работа выполнена при поддержке Гранта-в-Помощь Научных Исследований (С) Японского Общества Содействия Науке (№ 16540002, № 19540002 и № 22540006).

3. Универсальные сравнения типа Куммера	57
3.1. Основная теорема	57
3.2. Первый инструмент для доказательства	58
3.3. Второй инструмент для доказательства	62
3.4. Доказательство сравнений типа Куммера	64
3.5. Сравнение Куммера–Аделберга	66
4. Гиперэллиптические функции	67
4.1. Основные сведения о гиперэллиптических функциях	67
4.2. Гиперэллиптические функции и их переменная	68
5. Дифференциальные уравнения	69
5.1. Общая постановка	69
5.2. Случай $y(u)^2 = x(u)^{2g+1} - 1$	70
5.3. Случай $y(u)^2 = x(u)^{2g+1} - x(u)$	70
6. Теоремы фон Штаудта в алгебраических функциях	71
6.1. Случай $y(u)^2 = x(u)^{2g+1} - 1$	71
6.2. Случай $y(u)^2 = x(u)^{2g+1} - x(u)$	71
6.3. Замечание об A_p	72
7. Сравнение Куммера в алгебраических функциях	72
7.1. Случай $y(u)^2 = x(u)^{2g+1} - 1$	72
7.2. Случай $y(u)^2 = x(u)^{2g+1} - x(u)$	73
8. Целые по Гурвицу ряды	73
8.1. Определение и основные свойства	73
8.2. Целостность по Гурвицу ряда $x(u)^{1/2}$	74
8.3. Целостность по Гурвицу ряда $1/y(u)^{1/5}$	75
9. Схема доказательства	75
9.1. Теоремы фон Штаудта в алгебраических функциях	76
9.2. Сравнения Куммера в алгебраических функциях	77
10. Теорема Кларка для $x(u)$ над $\mathbb{Z}\left[\frac{1}{2}\right]$	78
10.1. Теорема Кларка для $x(u)^{1/2}$	78
10.2. Сравнение между $x(u)^{k/2}$ и $x(u)^{(k+1)/2}$	79
10.3. Теорема Кларка для $x(u)^2$ над $\mathbb{Z}\left[\frac{1}{2}\right]$	80
11. Теорема Кларка для $y(u)$ над $\mathbb{Z}\left[\frac{1}{5}\right]$	81
11.1. Теорема Кларка для $y(u)^{1/5}$	81
11.2. Сравнение между $y(u)^{k/5}$ и $y(u)^{(k+1)/5}$	82
11.3. Теорема Кларка для $y(u)$ над $\mathbb{Z}\left[\frac{1}{5}\right]$	83
12. Теорема Кларка для $x(u)$ и $y(u)$ над $\mathbb{Z}$	84
12.1. Сравнение между $y(u)$ и $x^2(u)$	84
12.2. От $x^2(u)$ к $x(u)$	85
13. Доказательство сравнений типа Куммера	85
13.1. Теорема Хонды и формальные группы	85
13.2. Формула Хохшильда и теорема Хонды	88
13.3. Доказательство сравнений	90

14. Другие сравнения	91
14.1. Обобщенные числа Бернулли–Гурвица высшего порядка	91
14.2. Коэффициенты Гурвица функций $t(u_g)$ и $s(u_g)$	92
14.3. Обобщение сравнения Вандивера–Карлица	93
15. Численные примеры для классических чисел	95
15.1. Числа Бернулли	95
15.2. Числа Гурвица для кривой $y^2 = x^3 - 1$	96
15.3. Числа Гурвица для кривой $y^2 = x^3 - x$	97
16. Численные примеры для новых чисел	98
16.1. Функция $x(u)$ для кривой $y^2 = x^5 - 1$	98
16.2. Функция $y(u)$ для кривой $y^2 = x^5 - 1$	100
16.3. Функция $x(u)$ для кривой $y^2 = x^5 - x$	101
17. Негиперэллиптические кривые, вполне разветвленные на бесконечно- сти	103
18. Дополнения	104
18.1. Соотношения на биномиальные коэффициенты	104
18.2. Связи с некоторыми рядами типа Эйзенштейна	105
18.3. Проблемы	106
Список литературы	106

Введение

Чтобы напомнить материал по числам Бернулли и Гурвица и объяснить наши новые числа, рассмотрим кривую $\mathcal{C}$ рода $g \geq 0$, заданную уравнением

$$y^2 = x^{2g+1} - 1 \quad \text{или} \quad y^2 = x^{2g+1} - x. \quad (0.1)$$

Здесь мы считаем, что $\mathcal{C}$ собственная, добавляя естественным образом бесконечно удаленную точку ∞ . Интеграл

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

принимает конечные значения для всех $(x, y) \in \mathcal{C}$ и имеет нуль порядка 1 на ∞ . Рассматривая (0.2) как уравнение на u и x , рассмотрим функцию $x \mapsto u$ на окрестности точки ∞ . Если $g = 1$, а именно, если $\mathcal{C}$ – эллиптическая кривая, то обратная функция $u \mapsto x$ продолжается на всю комплексную плоскость и является просто эллиптической функцией Вейерштрасса $\wp(u)$.

Если $g \geq 2$, то вышеупомянутая обратная функция глобально не продолжается, так что следует рассматривать обратные функции системы суммирований

$$(u_1, u_2, \dots, u_g) = \sum_{j=1}^g \int_{\infty}^{(x_j, y_j)} \left(\frac{dx}{2y}, \frac{x dx}{2y}, \dots, \frac{x^{g-1} dx}{2y} \right) \quad (0.3)$$

g интегралов до g точек $(x_1, y_1), (x_2, y_2), \dots, (x_g, y_g)$ естественной базы голоморфных 1-форм. Это классическая теория абелевых функций со времен Якоби.

Вернемся к (0.2) при $g = 0$ для первой кривой в (0.1). Функция $u \mapsto x$ – это просто $1/\sin^2(u)$, а ее коэффициенты Лорана – числа Бернулли B_{2n} :

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

Более того, если $g = 1$ и $\mathcal{C}$ задана уравнением $y^2 = x^3 - x$, то числа Гурвица E_{4n} , важные аналоги чисел Бернулли, определяются как коэффициенты Лорана функции $x(u) = \wp(u)$:

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

Представляется крайне трудной задачей, по крайней мере автору, найти обобщение этих чисел при $g \geq 2$ в случае, когда в (0.3) входят несколько переменных.

Однако разложение Лорана обратной функции $u \mapsto x$ вблизи $u = 0$ для нескольких случаев, когда $g \geq 2$, обладает неожиданным свойством коэффициентов, а именно аналогами для высшего рода некоторых знаменитых свойств чисел Бернулли [1]–[4] и чисел Гурвица [5]–[7]. Они сформулированы как наши основные теоремы 6.1, 6.3, 7.1 и 7.5.

Здесь мы объясним ситуацию и результаты более явно. Предположим, что $g \geq 1$. Напомним, что значения $\mathbf{u} = (u_1, u_2, \dots, u_g)$ суммы (0.3) для g переменных точек $(x_1, y_1), (x_2, y_2), \dots, (x_g, y_g)$ на $\mathcal{C}$ и для всех g путей интегралов от ∞ до (x_j, y_j) заполняют все g -мерное линейное пространство над комплексными числами $\mathbb{C}$. Обозначим это пространство через $\mathbb{C}^g$. Периоды системы (0.3), а именно значения $\mathbf{u} = (u_1, u_2, \dots, u_g)$ для всех g замкнутых путей дают решетку в $\mathbb{C}^g$, скажем, Λ . Тогда $\mathbb{C}^g/\Lambda$ является многообразием Якоби кривой $\mathcal{C}$. Обозначим через ι каноническое вложение $(x, y) \mapsto \mathbf{u}$ кривой $\mathcal{C}$ в $\mathbb{C}^g/\Lambda$, заданное с помощью

$$\mathbf{u} = \int_{\infty}^{(x,y)} \left(\frac{dx}{2y}, \frac{x dx}{2y}, \dots, \frac{x^{g-1} dx}{2y} \right) \quad (0.6)$$

по модулю Λ . Наша ситуация резюмируется следующим образом:

$$\begin{array}{ccc} \kappa^{-1}\iota(\mathcal{C}) & \longrightarrow & \mathcal{C} \\ \downarrow & & \downarrow \iota \\ \mathbb{C}^g & \xrightarrow{\kappa} & \mathbb{C}^g/\Lambda \end{array}$$

где κ – отображение факторизации по модулю Λ . Объект $\kappa^{-1}\iota(\mathcal{C})$ является универсальным абелевым накрытием кривой $\mathcal{C}$ и обозначается в этой работе через $\tilde{\mathcal{C}}$. Если $g = 1$, то вертикальное отображение слева является эпиморфизмом.

Если $\mathbf{u}$ изменяется вдоль $\tilde{\mathcal{C}}$, то $\mathbf{u}$ однозначно определяет точку (x, y) на $\mathcal{C}$ посредством (0.6). Обозначим координаты через

$$x(\mathbf{u}) \quad \text{и} \quad y(\mathbf{u}).$$

Можно взять g -ю координату u_g в качестве локального параметра на $\tilde{\mathcal{C}}$ вблизи точки $\mathbf{0} = (0, 0, \dots, 0)$, как объясняется в п. 4.2. Значит, у нас есть разложение Лорана функций $x(\mathbf{u})$ и $y(\mathbf{u})$ относительно u_g . Их коэффициенты Лорана, которые мы называем *обобщенными числами Бернулли–Гурвица*, неожиданным образом похожи на классические числа Бернулли и Гурвица; в частности, они удовлетворяют вполне естественным обобщениям теоремы фон Штаудта–Клаузена [2], [1], второй теоремы фон Штаудта [4] и исходному сравнению Куммера [3].

Обсуждаемые выше свойства обобщенных чисел Бернулли–Гурвица были известны из компьютерных вычислений на начальном этапе этой работы. Затем автор, после размышлений о доказательствах, касающихся обобщенных чисел Бернулли–Гурвица, пришел к *универсальным числам Бернулли*.

Хотя существует много исследований, обобщающих эти свойства, например, [8]–[17] и т. д., следует отметить, что в тех работах, где обобщалось сравнение Куммера, порядок степени соответствующего простого числа p *меньше половины* модуля исходного сравнения Куммера. Насколько известно автору, Карлиц был первым, кто попытался найти обобщение чисел Гурвица для гиперэллиптических функций, как явствует из его работ [18] и [8]. Он не рассматривал наши функции $x(\mathbf{u})$ и $y(\mathbf{u})$ и не добился полного успеха. В отличие от этого, наше обобщение исходного сравнения Куммера для обобщенных чисел Бернулли–Гурвица в этой работе является сравнением по модулю *той же степени* соответствующего простого числа, что и в случае $g = 0$ [4], т. е. в классическом сравнении самого Куммера для чисел Бернулли, и в случае $g = 1$ [7], т. е. в сравнении типа Куммера, полученном Х. Лэнгом для чисел Гурвица.

Самое замечательное состоит в том, что порядок степени в модуле нашего сравнения Куммера (теорема 3.1) для универсальных чисел Бернулли, который является неупрощаемым, как объясняется в замечании 3.2, (2), *также меньше половины* порядка в случаях классических чисел Бернулли и наших обобщенных чисел Бернулли–Гурвица.

Так же как классические числа Бернулли связаны с формальным групповым законом, формальный логарифм которого есть $t \mapsto \log(1 + t)$, универсальные числа Бернулли связаны с *универсальным формальным групповым законом*, который является коммутативным формальным групповым законом от одной переменной и задан над кольцом, известным как кольцо Лазара (см. § 1.5 в [19]). Эти числа больше используются в теории стабильных гомотопий, чем в теории чисел (см. § 31.1 в [19]).

Обобщенные числа Бернулли–Гурвица связаны с некоторыми коммутативными формальными групповыми законами от одной переменной, как объясняется в п. 13.1. Аналогичным образом числа, изучавшиеся Карлицом и др., также связаны с коммутативными формальными групповыми законами. Поскольку любой коммутативный формальный групповой закон от одной переменной получается из универсального формального группового закона его специализацией, в силу универсальности любые свойства универсальных чисел Бернулли наследуются не только обобщенными числами Бернулли–Гурвица, но также обобщениями Карлица и т. п.

В конце концов, сравнение Куммера для универсальных чисел Бернулли нельзя использовать для доказательства такого сравнения для обобщенных чисел Бернулли–Гурвица, потому что неувлучшаемый порядок степени в первом меньше половины ожидаемого порядка в последнем.

Результат в разделе 2, а именно теорема Кларка, являющаяся красивым обобщением и объединением теоремы фон Штаудта–Клаузена и второй теоремы фон Штаудта, используется в доказательстве таких теорем для обобщенных чисел Бернулли–Гурвица. С другой стороны, сравнение Куммера для универсальных чисел Бернулли доказывается в разделе 3 и не используется далее. Так что читатель, интересующийся только обобщенными числами Бернулли–Гурвица, может пропустить весь раздел 3.

Так как записывание доказательства в самой общей постановке очень сложно, мы доказываем свойства обобщенных чисел Бернулли–Гурвица только для гиперэллиптических кривых рода два, заданных уравнением

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

Кольцо эндоморфизмов якобиана этой кривой содержит корни 10-й степени из единицы. Тогда, например, один из типов наших чисел, обозначаемых через C_{10n} , задается равенством

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

Наши результаты справедливы также для негиперэллиптических кривых типа, описываемого в п. 14.1 (*кривые циклотомического типа*). Автор считает, что читателю не так уж трудно доказать свойства этих чисел для таких общих кривых. С другой стороны, наш метод дает новое доказательство трех свойств для чисел Бернулли и для чисел Гурвица.

Автор ожидает, что подобные числа могут быть получены из более общей кривой, для которой формальное пополнение ее многообразия Якоби над подходящим локальным кольцом имеет одномерный фактор формальных групп.

Доказательство нашей теоремы типа фон Штаудта–Клаузена сильно зависит от красивой работы Карлица [18]. Для случая $g \geq 2$ использование классических алгебраических формул сложения и умножения для доказательства теорем представляется слишком трудным. В вышеупомянутой работе Карлиц дал интересное доказательство, избегающее формул сложения и умножения эллиптических функций. Грубо говоря, его метод является техническим обобщением теоремы обращения Лагранжа (см. [20; § 7.3])¹. Однако дивизор (в смысле алгебраической геометрии) n -й степени данной функции является просто n -умножением дивизора этой функции. Следует считать, что доказательство Карлица и наши доказательства используют формулы умножения на многообразиях Якоби².

¹Это было отмечено Такаюки Ода.

²Это было отмечено Шигеки Мацутани.

На эту работу автора вдохновили предложение Масао Койке во время визита автора в университет Кюсю и уникальная книга [21]. Предложение 3.4, (2), теоремы 7.1 и 7.5 были проблематичными гипотезами на ранних стадиях настоящей работы, до тех пор пока Сейдаи Ясуда не рассказал мне их доказательство. Я сожалею, что Ясуда отклонил предложение стать соавтором этой работы, но я хотел бы выразить мою искреннюю благодарность за его важный вклад в эту работу. Доктор Наруо Каноу предоставил мне красивую компьютерную программу, работающую на `pari/GP`, которая состоит всего из нескольких строк, но так быстро дает результаты. Его программа была очень полезной для численной проверки результатов на протяжении этой работы и приводится с его разрешения в п. 16.1. А. Адельберг тщательно прочитал раздел 3 и высказал важные замечания. Очень полезными были обсуждения с Шигеки Мацутани и Такаюки Ода. Хироши Сузуки в Нагойском университете показал мне некоторую лемму (см. [22; лемма 18.3.2]), которая не упоминается в настоящей работе, но была полезна автору для понимания предложения 13.13. Я хотел бы выразить мою глубокую благодарность всем этим коллегам.

Соглашения и обозначения

(1) Для рационального числа α обозначим через $\lfloor \alpha \rfloor$ наибольшее целое число, не превосходящее α , а через $\lceil \alpha \rceil$ наименьшее целое число, не меньшее α .

(2) Мы используем обозначение

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

для целого $n \neq 0$. Здесь область значений z каждый раз определяется из контекста. Биномиальный коэффициент записывается как

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

(3) Обобщая символ факториала, обозначим через $n!!$ произведение

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

последовательности с шагом -2 от n до 1 или 2. Аналогично, $n!!!$ означает произведение последовательности натуральных чисел от n с шагом -3 . Более того, например, обозначим $n!!!! = n!^{(5)}$. Так, $12!^{(5)} = 12 \cdot 7 \cdot 2$.

(4) Если p – простое число и p -часть данного рационального числа r есть p^e , то мы пишем $e = \text{ord}_p r$. Если τ – многочлен (возможно, от нескольких переменных) с рациональными коэффициентами, то $\text{ord}_p \tau$ обозначает наименьшее из чисел $\text{ord}_p r$ для всех коэффициентов r многочлена τ .

(5) Для простого числа p и целого числа a обозначим через $a|_p$ частное от деления на p -часть a , а именно $a|_p = a/p^{\text{ord}_p a}$.

(6) Если $F(z)$ – формальный степенной ряд относительно z , то его коэффициент при z^n обозначается через $[z^n]F(z)$. Мы также будем использовать обозначения $\left[\frac{z^n}{n!}\right]F(z) := n! [z^n]F(z)$ и $\left[\frac{z}{n}\right]F(z) := n[z^n]F(z)$.

(7) Если $\varphi(z)$ – формальный степенной ряд относительно z (допускающий члены отрицательных степеней), то мы называем $\left[\frac{z^n}{n!}\right]\varphi(z)$ ($n \geq 0$) *коэффициентом Гурвица* для $\varphi(z)$ при z^n . Мы называем $\left[\frac{z}{n}\right]\varphi(z)$ его *коэффициентом Карлица*.

(8) Пусть R – коммутативное кольцо. Обозначим через $R\langle\langle v \rangle\rangle$ кольцо формальных степенных рядов относительно z , состоящее только из членов неотрицательного порядка таких, что все соответствующие коэффициенты Гурвица принадлежат R .

(9) В выражении степенного ряда относительно z символ $(d^\circ(z) \geq m)$ обозначает его часть, состоящую из членов степени не меньше m . Когда m очевидно, мы, как обычно, обозначаем их просто $+\dots$.

1. Предварительные сведения из комбинаторики

1.1. Основные сведения об операции факториала. Следующие свойства операции факториала часто используются в этой работе. Пусть n и k – неотрицательные целые числа, и пусть p – простое число. Если $n = kp + a$ при $0 \leq a < p$, то

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

Обозначим через $S_p(n)$ сумму цифр выражения числа n по основанию p . Тогда

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

1.2. Формула обращения Лагранжа. Для степенного ряда $F(z)$ от z обозначим через $[z^n]F(z)$ коэффициент при z^n . Следующая формула называется формулой обращения Лагранжа.

ПРЕДЛОЖЕНИЕ 1.3. Пусть $\varphi(u) = u + \dots$ – степенной ряд от u , имеющий только члены положительной степени, у которого коэффициент при члене первой степени равен 1. Пусть $\psi(t) = \varphi^{-1}(t)$ – его формальный обратный ряд, а именно, степенной ряд относительно t , для которого $\varphi(\psi(t)) = t$. Тогда

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

Доказательство этого факта можно найти, например, в [23; с. 148–153]. См. также [20; § 7.3] (теорема Лагранжа–Бюрманна).

1.3. Основные сведения о биномиальных коэффициентах. Следующая лемма используется в п. 10.1.

ЛЕММА 1.4. Пусть $n \geq 0$, $q > 0$, r – три целых числа. Тогда

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

ДОКАЗАТЕЛЬСТВО. Число в формулировке есть не что иное, как коэффициент $[u^{n+1}](-(1-u)^{r/q})$. Пусть $t = q\{(1-u)^{1/q} - 1\}$, так что $u = 1 - \left(1 + \frac{1}{q}t\right)^q$. Применяя формулу обращения Лагранжа из предложения 1.3 при $\ell = -1$, имеем

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

Правая часть принадлежит $\mathbb{Z}\left[\frac{1}{q}\right]$, и, значит, то же верно для левой части.

Следовательно, $[u^n]((1-u)^{1/q}) \in \mathbb{Z}\left[\frac{1}{q}\right]$. Таким образом, $[u^n]((1-u)^{r/q}) \in \mathbb{Z}\left[\frac{1}{q}\right]$ для всех n .

Приведем другое доказательство леммы 1.4.

ЛЕММА 1.5. Пусть p – простое число, $n \geq 0$ – целое число и $z \in \mathbb{Z}_{(p)}$. Тогда

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

ДОКАЗАТЕЛЬСТВО. Для данного целого числа $n \geq 0$ функция $z \mapsto \binom{z}{n}$ является непрерывным отображением из $\mathbb{Z}_p$ в $\mathbb{Q}_p$. Так как $\mathbb{Z}$ всюду плотно в $\mathbb{Z}_p$ и $\binom{z}{n} \in \mathbb{Z}$ для $z \in \mathbb{Z}$, получаем требуемое утверждение.

Хотя лемма 1.5 слабее леммы 1.4, лемма 1.4 получается из леммы 1.5 путем изменения p в силу равенства

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

2. Теорема Кларка

2.1. Определение универсальных чисел Бернулли. Пусть $f_1, f_2, \dots$ – бесконечное множество неизвестных. Рассмотрим степенной ряд

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

и его формальный обратный ряд

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

а именно, такой ряд, что $u(t(u)) = u$. Тогда определяем $\hat{B}_n \in \mathbb{Q}[f_1, f_2, \dots]$ из равенства

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

и называем их *универсальными числами Бернулли* (порядка 1). Если мы специализируем $f_n = (-1)^n$, то $u(t) = \log(1+t)$ и $t(u) = e^u - 1$. Тогда $\hat{B}_n$ специализируется в классическое число Бернулли B_n .

2.2. Разложение универсальных чисел Бернулли. Для конечной последовательности $U = (U_1, U_2, \dots)$ неотрицательных целых чисел обозначим $w(U) = \sum_j jU_j$ и назовем эту величину *весом* последовательности U . Число $d(U) = \sum_j U_j$ называется *степенью* последовательности U . Можно рассматривать U как разбиение $w(U)$. Для простоты мы пишем

$$U! = U_1! U_2! \dots, \quad \binom{d}{U} = \frac{d!}{U!}. \quad (2.4)$$

Используя обозначения $\Lambda^U = 2^{U_1} 3^{U_2} 4^{U_3} \dots$ и $f^U = f_1^{U_1} f_2^{U_2} f_3^{U_3} \dots$, определим

$$\gamma_U = \Lambda^U U!. \quad (2.5)$$

Если положить $h(t) = \frac{u(t)}{t} - 1$, то

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

Отсюда, записывая

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

и применяя предложение 1.3 при $\ell = 1$, получаем следующее выражение для $\widehat{B}_n$.

ПРЕДЛОЖЕНИЕ 2.8. Имеем $\frac{\widehat{B}_n}{n} = \sum_{w(U)=n} \tau_U f^U$.

2.3. Теорема Кларка. Теперь мы опишем теорему Кларка об универсальных числах Бернулли. Для простого числа p и целого числа a обозначим через $a|_p$ частное от деления на p -часть числа a , а именно $a|_p = a/p^{\text{ord}_p a}$.

ПРЕДЛОЖЕНИЕ 2.9. Справедливы равенства

$$\widehat{B}_1 = \frac{1}{2} f_1, \quad \frac{\widehat{B}_2}{2} = -\frac{1}{4} f_1^2 + \frac{1}{3} f_2,$$

$$\frac{\widehat{B}_n}{n} \equiv \begin{cases} \sum_{\substack{n=a(p-1) \\ p - \text{простое число}}} \frac{a|_p^{-1} \bmod p^{1+\text{ord}_p a}}{p^{1+\text{ord}_p a}} f_{p-1}^a & (\text{если } n \equiv 0 \bmod 4), \\ \frac{f_1^{n-6} f_3^2}{2} - \frac{n f_1^n}{8} + \sum_{\substack{n=a(p-1) \\ p - \text{нечетное простое}}} \frac{a|_p^{-1} \bmod p^{1+\text{ord}_p a}}{p^{1+\text{ord}_p a}} f_{p-1}^a & (\text{если } n \neq 2 \text{ и } n \equiv 2 \bmod 4), \\ \frac{f_1^n + f_1^{n-3} f_3}{2} & (\text{если } n \neq 1 \text{ и } n \equiv 1, 3 \bmod 4) \end{cases}$$

mod (множество многочленов веса n из $\mathbb{Z}[f_1, f_2, \dots]$).

Доказательство см. в [24]; оно опирается на достаточно сложное использование предложения 2.8.

ЗАМЕЧАНИЕ 2.10. (1) Конечно, имеется сравнение на само $\widehat{B}_n$. Например, если $n \equiv 0 \pmod{4}$, то предложение 2.9 показывает, что

$$\widehat{B}_n \equiv - \sum_{\substack{p - \text{простое число} \\ (p-1)|n}} \frac{f_{p-1}^{n/(p-1)}}{p} \pmod{\mathbb{Z}[f_1, f_2, \dots]}. \quad (2.11)$$

Действительно, для простого числа p , если $n = a(p-1)$ и $\text{ord}_p a = \nu$, то

$$\frac{n \cdot (a|_p^{-1} \pmod{p^{1+\nu}})}{p^{1+\nu}} \equiv 1 - \frac{1}{p} \equiv -\frac{1}{p} \pmod{\mathbb{Z}}.$$

Отсюда следует (2.11). Если выполнено дополнительное условие $(p-1) \nmid n$, то легко видеть, что

$$\frac{\widehat{B}_n}{n} \in \mathbb{Z}_{(p)}[f_1, f_2, \dots]. \quad (2.12)$$

Свойство (2.11) является аналогом теоремы фон Штаудта–Клаузена для классических чисел Бернулли, а (2.12) – аналогом второй теоремы фон Штаудта. Теорема Кларка является красивым объединением аналогов этих двух теорем.

(2) Хотя в [24] сравнение берется по модулю всего кольца $\mathbb{Z}[f_1, f_2, \dots]$, очевидно, что в силу предложения 2.8 его можно заменить как указано выше.

3. Универсальные сравнения типа Куммера

3.1. Основная теорема. Универсальные числа Бернулли удовлетворяют сравнению типа исходного сравнения Куммера по модулю $p^{\lfloor a/2 \rfloor}$.

ТЕОРЕМА 3.1. Пусть p – простое число и a, n – натуральные числа. Предположим, что $n > a$ и $n \not\equiv 0 \pmod{p-1}$. Тогда

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

ЗАМЕЧАНИЕ 3.2. (1) Если $a = 1$ и $n > a = 1$ при $n \not\equiv 0, 1 \pmod{p-1}$, то вышеприведенное сравнение выполняется по модулю p . Этот факт впервые был отмечен в [25; теорема 3.2]. Более короткое доказательство и распространение на случай, когда $n \equiv 1 \pmod{p-1}$, даны в [26; теорема 1].

(2) Для нечетного простого числа $p \geq 7$ рассмотрим U такое, что $U_1 = p$, $U_{2p-1} = (p-3)/2$, а остальные U_j равны 0. Тогда $w(U) = p + (p-5) \times (2p-1)/2 \equiv -1 \pmod{p-1}$. Для этого U можно легко показать, что

$$\text{ord}_p(\tau_U) = \frac{p-5}{2} = \left\lfloor \frac{p-4}{2} \right\rfloor.$$

Заметим, что $n > a$ при $a = p-4$ и $n = w(U)$. Формула (3.13) ниже показывает, что оценка в теореме 3.1 неумлучшаема.

(3) В вышеприведенном примере при $p = 5$ имеем $\text{ord}_5(\tau_U) = 0$. Тогда $n = w(U) = 5 \equiv 1 \pmod{5-1}$, и это один из исключенных случаев в [25; теорема 3.2]. Имея в виду этот случай и слегка модифицируя доказательство предложения 3.11 ниже, можно показать, что сравнение в теореме 3.1 выполняется по модулю p при $a = 1$, если выполнено дополнительное условие $n \not\equiv 1 \pmod{p-1}$.

В п. 3.5 мы дадим новое доказательство следующего сравнения Адельберга (см. [27; часть (i) теоремы]), непосредственно опирающееся на теорему 3.1 и замечание 3.2, (1).

СЛЕДСТВИЕ 3.3 (сравнение Адельберга). *Если $n \not\equiv 0, 1 \pmod{p-1}$ и $n > a$, то*

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

Теорема 3.1 дает более сложное, но похожее на следствие 3.3 сравнение, если $n \equiv 1 \pmod{p-1}$; это есть часть (ii) теоремы в [27].

3.2. Первый инструмент для доказательства. В доказательстве теоремы 3.1 мы используем два предложения. Следующее – первое из них.

ПРЕДЛОЖЕНИЕ 3.4. *Пусть p – простое число и a, n – неотрицательные целые числа. Пусть*

$$M = \begin{cases} \text{ord}_p(n!) & (\text{если } n \geq ap), \\ a - \left\lfloor \frac{n}{p} \right\rfloor + \text{ord}_p(n!) - \left\lfloor \frac{a - \lfloor n/p \rfloor}{p} \right\rfloor & (\text{если } n < ap). \end{cases}$$

Тогда выполняются следующие сравнения.

(1) *Если q – неотрицательное целое число, то*

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

(2) *Если r_0 – целое число такое, что $0 < r_0 \leq a$ и $n \geq r_0 p$ – целое число, то*

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

Для двух вещественных чисел $\alpha > 0$ и β определим

$$\mathbb{Z}_p \langle\langle v \rangle\rangle^{(\alpha), \beta} = \left\{ \varphi \in \mathbb{Q}_p[[v]] \mid \left(\frac{d}{dv} \right)^{pa} \varphi \in p^{\lceil \alpha(a+\beta) \rceil} \mathbb{Z}_p \langle\langle v \rangle\rangle \text{ для всех } a \geq 0 \right\}. \quad (3.5)$$

ЗАМЕЧАНИЕ 3.6. (1) Возможно, доказательство будет понять легче, если рассматривать $\mathbb{Z}_p \langle\langle v \rangle\rangle^{(\alpha), \beta}$ как “ $p^{\alpha\beta} \mathbb{Z}_p \langle\langle p^{\alpha/p} v \rangle\rangle$ ”.

(2) Для доказательства предложения 3.4 мы используем только случай $\alpha = 1 - 1/p$.

ЛЕММА 3.7. (1) $\mathbb{Z}_p \langle\langle v \rangle\rangle^{(\alpha), \beta}$ является $\mathbb{Z}_p$ -подмодулем в $\mathbb{Q}_p[[v]]$.

(2) $\mathbb{Z}_p \langle\langle v \rangle\rangle^{(\alpha), \beta} \subset p^{\lceil \alpha\beta \rceil} \mathbb{Z}_p \langle\langle v \rangle\rangle$; в частности, если $\beta \geq 0$, то $\mathbb{Z}_p \langle\langle v \rangle\rangle^{(\alpha), \beta} \subset \mathbb{Z}_p \langle\langle v \rangle\rangle$.

(3) Для $f(v) = \sum_{n=0}^{\infty} a_n v^n \in \mathbb{Q}_p[[v]]$ включение $f(v) \in \mathbb{Z}_p \langle\langle v \rangle\rangle^{(\alpha), \beta}$ выполняется тогда и только тогда, когда $\sum_{n=0}^m a_n v^n \in \mathbb{Z}_p \langle\langle v \rangle\rangle^{(\alpha), \beta}$ для всех $m \geq 0$.

(4) Если $\alpha_1 \geq \alpha_2 > 0$, то $\mathbb{Z}_p \langle\langle v \rangle\rangle^{(\alpha_1), \beta} \subset \mathbb{Z}_p \langle\langle v \rangle\rangle^{(\alpha_2), \beta}$.

(5) Если $\beta_1 \geq \beta_2$, то $\mathbb{Z}_p \langle\langle v \rangle\rangle^{(\alpha), \beta_1} \subset \mathbb{Z}_p \langle\langle v \rangle\rangle^{(\alpha), \beta_2}$.

(6) Если $n \in \mathbb{Z}$ (допускаются отрицательные значения n), то выполнено включение $p^n \mathbb{Z}_p \langle\langle v \rangle\rangle^{(\alpha), \beta} \subset \mathbb{Z}_p \langle\langle v \rangle\rangle^{(\alpha), \beta + n/\alpha}$.

(7) Если $\varphi \in \mathbb{Z}_p \langle\langle v \rangle\rangle^{(\alpha), \beta}$, то $\frac{d}{dv} \varphi \in \mathbb{Z}_p \langle\langle v \rangle\rangle^{(\alpha), \beta}$.

(8) Если $\varphi \in \mathbb{Z}_p \langle\langle v \rangle\rangle^{(\alpha), \beta}$, то $\left(\frac{d}{dv}\right)^p \varphi \in \mathbb{Z}_p \langle\langle v \rangle\rangle^{(\alpha), \beta + 1}$.

(9) Пусть $m \geq 0$ и $b \in \mathbb{Q}_p$. Включение $bv^m/m! \in \mathbb{Z}_p \langle\langle v \rangle\rangle^{(\alpha), \beta}$ выполняется тогда и только тогда, когда $\text{ord}_p b \geq \alpha(\lfloor m/p \rfloor + \beta)$.

ДОКАЗАТЕЛЬСТВО. (1) Для $\varphi_1, \varphi_2 \in \mathbb{Z}_p \langle\langle v \rangle\rangle^{(\alpha), \beta}$, очевидно, имеем $\varphi_1 + \varphi_2 \in \mathbb{Z}_p \langle\langle v \rangle\rangle^{(\alpha), \beta}$. Для $\varphi \mathbb{Z}_p \langle\langle v \rangle\rangle^{(\alpha), \beta}$ и $a \in \mathbb{Z}_p$, очевидно, имеем $a\varphi \in \mathbb{Z}_p \langle\langle v \rangle\rangle^{(\alpha), \beta}$.

(2) Если $\varphi \in \mathbb{Z}_p \langle\langle v \rangle\rangle^{(\alpha), \beta}$, то $\left(\frac{d}{dv}\right)^{pa} \varphi \in p^{\lceil \alpha(a+\beta) \rceil} \mathbb{Z}_p \langle\langle v \rangle\rangle$ по определению.

Если положить $a = 0$, то как раз получается требуемое утверждение.

(3) Записывая для $f(v) \in \mathbb{Q}_p[[v]]$ определение $\mathbb{Z}_p \langle\langle v \rangle\rangle^{(\alpha), \beta}$, видим, что $f(v) \in \mathbb{Z}_p \langle\langle v \rangle\rangle^{(\alpha), \beta}$ тогда и только тогда, когда $a_n v^n \in \mathbb{Z}_p \langle\langle v \rangle\rangle^{(\alpha), \beta}$ для всех $n \geq 0$.

(4) Это следует из неравенства $\lceil \alpha_1(a + \beta) \rceil \geq \lceil \alpha_2(a + \beta) \rceil$ для всех $a \geq 0$.

(5) В силу (доказательства) утверждения (3) достаточно показать, что из включения $a_n v^n \in \mathbb{Z}_p \langle\langle v \rangle\rangle^{(\alpha), \beta_1}$ следует включение $a_n v^n \in \mathbb{Z}_p \langle\langle v \rangle\rangle^{(\alpha), \beta_2}$. Это очевидно из определения $\mathbb{Z}_p \langle\langle v \rangle\rangle^{(\alpha), \beta}$.

(6) Это тривиально.

(7) Если $\left(\frac{d}{dv}\right)^{pa} a_n v^n \in p^{\lceil \alpha(a+\beta) \rceil} \mathbb{Z}_p \langle\langle v \rangle\rangle$, то $\left(\frac{d}{dv}\right)^{pa} n a_n v^{n-1} \in p^{\lceil \alpha(a+\beta) \rceil} \mathbb{Z}_p \langle\langle v \rangle\rangle$.

Таким образом, утверждение следует из (доказательства) (3).

(8) Предположим, что $\varphi \in \mathbb{Z}_p \langle\langle v \rangle\rangle^{(\alpha), \beta}$. Тогда $\left(\frac{d}{dv}\right)^{pa} \varphi \in p^{\lceil \alpha(a+\beta) \rceil} \mathbb{Z}_p \langle\langle v \rangle\rangle$ по определению. Заменяя a на $a + 1$, получаем

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

и требуемое утверждение.

(9) Для $\varphi = bv^m/m!$ свойство

$$\left(\frac{d}{dv}\right)^{pa} \varphi \in p^{\lceil \alpha(a+\beta) \rceil} \mathbb{Z}_p \langle\langle v \rangle\rangle \quad \text{для всех } a \geq 0$$

эквивалентно свойству

$$\left(\frac{d}{dv}\right)^{pa} \varphi \in p^{\lceil \alpha(a+\beta) \rceil} \mathbb{Z}_p \langle\langle v \rangle\rangle \quad \text{для всех } \left\lfloor \frac{m}{p} \right\rfloor \geq a \geq 0$$

(поскольку $(d/dv)^{(m+1)} v^m = 0$), а также свойству

$$\frac{bv^{m-pa}}{(m-pa)!} \in \frac{p^{\lceil \alpha(a+\beta) \rceil} \mathbb{Z}_p v^{m-pa}}{(m-pa)!} \quad \text{для всех } \left\lfloor \frac{m}{p} \right\rfloor \geq a \geq 0.$$

Так как последнее эквивалентно

$$b \in p^{\lceil \alpha(a+\beta) \rceil} \mathbb{Z}_p \quad \text{для всех } \left\lfloor \frac{m}{p} \right\rfloor \geq a \geq 0,$$

немедленно получаем требуемое утверждение.

СЛЕДСТВИЕ 3.8. Если $0 < \alpha \leq 1$ и $\varphi \in \mathbb{Z}_p \langle\langle v \rangle\rangle^{(\alpha), \beta}$, то

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

ДОКАЗАТЕЛЬСТВО. Для наших целей достаточно доказать утверждение в случае $p \neq 2$. Правило Лейбница показывает, что

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

Это принадлежит $\mathbb{Z}_p \langle\langle v \rangle\rangle^{(\alpha), \beta+1} + p\mathbb{Z}_p \langle\langle v \rangle\rangle^{(\alpha), \beta}$. Поэтому требуемое утверждение следует из леммы 3.7 (утверждения (6), (5)) и предположения для α .

ЛЕММА 3.9. Пусть $0 < \alpha \leq 1$. Тогда:

(1) $\mathbb{Z}_p[[v]] \subset \mathbb{Z}_p \langle\langle v \rangle\rangle^{(\alpha), 0}$;

(2) если $\varphi_1 \in \mathbb{Z}_p \langle\langle v \rangle\rangle^{(\alpha), \beta_1}$ и $\varphi_2 \in \mathbb{Z}_p \langle\langle v \rangle\rangle^{(\alpha), \beta_2}$, то $\varphi_1 \varphi_2 \in \mathbb{Z}_p \langle\langle v \rangle\rangle^{(\alpha), \beta_1 + \beta_2}$.

В частности, если $0 < \alpha \leq 1$, то $\mathbb{Z}_p \langle\langle v \rangle\rangle^{(\alpha), 0}$ является $\mathbb{Z}_p$ -подалгеброй в $\mathbb{Z}_p \langle\langle v \rangle\rangle$, а $\mathbb{Z}_p \langle\langle v \rangle\rangle^{(\alpha), \beta}$ является $\mathbb{Z}_p \langle\langle v \rangle\rangle^{(\alpha), 0}$ -модулем.

ДОКАЗАТЕЛЬСТВО. (1) Предположим, что $\varphi \in \mathbb{Z}_p[[v]]$. Так как для произвольного $a \geq 0$ выполнено включение $\frac{1}{(pa)!} \left(\frac{d}{dv} \right)^{pa} \varphi \in \mathbb{Z}_p[[v]] \subset \mathbb{Z}_p \langle\langle v \rangle\rangle$, то

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

Поскольку $\alpha \leq 1$, это содержится в $p^{\lceil \alpha a \rceil} \mathbb{Z}_p \langle\langle v \rangle\rangle$, и, значит, $\varphi \in \mathbb{Z}_p \langle\langle v \rangle\rangle^{(\alpha), 0}$.

(2) По правилу Лейбница видим, что

$$\begin{aligned} \left(\frac{d}{dv} \right)^{pa} (\varphi \psi) &= \sum_{j=0}^{pa} \binom{pa}{j} \left(\left(\frac{d}{dv} \right)^j \varphi \right) \left(\left(\frac{d}{dv} \right)^{pa-j} \psi \right) \\ &= \sum_{j=0}^a \binom{pa}{pj} \left(\left(\frac{d}{dx} \right)^{pj} \varphi \right) \left(\left(\frac{d}{dv} \right)^{pa-pj} \psi \right) \\ &\quad + \sum_{0 \leq j \leq pa, p \nmid j} \binom{pa}{j} \left(\left(\frac{d}{dv} \right)^j \varphi \right) \left(\left(\frac{d}{dv} \right)^{pa-j} \psi \right). \end{aligned}$$

Если $p \nmid j$, то $p \mid \binom{pa}{j}$. Из определения (3.5) и леммы 3.7, (7) следует, что

$$\begin{aligned} \left(\frac{d}{dv} \right)^{pa} (\varphi \psi) &\in \sum_{j=0}^a p^{\lceil \alpha(j+\beta_1) \rceil} p^{\lceil \alpha(a-j+\beta_2) \rceil} \mathbb{Z}_p \langle\langle v \rangle\rangle \\ &\quad + \sum_{0 \leq j \leq pa, p \nmid j} pp^{\lceil \alpha(\lfloor j/p \rfloor + \beta_1) \rceil} p^{\lceil \alpha(\lfloor (pa-j)/p \rfloor + \beta_2) \rceil} \mathbb{Z}_p \langle\langle v \rangle\rangle \\ &\subset p^{\lceil \alpha(a+\beta_1+\beta_2) \rceil} \mathbb{Z}_p \langle\langle v \rangle\rangle + pp^{\lceil \alpha(a-1+\beta_1+\beta_2) \rceil} \mathbb{Z}_p \langle\langle v \rangle\rangle. \end{aligned}$$

В силу $\alpha \leq 1$ это содержится в $p^{\lceil \alpha(a+\beta_1+\beta_2) \rceil} \mathbb{Z}_p \langle\langle v \rangle\rangle$, и мы показали, что $\varphi \psi \in \mathbb{Z}_p \langle\langle v \rangle\rangle^{(\alpha), \beta_1 + \beta_2}$, как и требовалось.

ЛЕММА 3.10. *Имеем*

$$\exp\left(v + \frac{v^p}{p}\right) \in \mathbb{Z}_p\langle\langle v \rangle\rangle^{(1-1/p),0}.$$

ДОКАЗАТЕЛЬСТВО. В силу леммы 3.9, (2) и леммы 3.7, (3) достаточно показать, что

$$(1) \exp\left(\sum_{n=0}^{\infty} \frac{v^{p^n}}{p^n}\right) \in \mathbb{Z}_p[[v]] \text{ и}$$

$$(2) \exp\left(-\frac{v^{p^n}}{p^n}\right) \in \mathbb{Z}_p\langle\langle v \rangle\rangle^{(1-1/p),0} \text{ для всех } n \geq 2.$$

Так как свойство (1) хорошо известно и доказано в [28; с. 238, п. 5.4] и [29; теорема на с. 388], мы докажем только свойство (2). Для этого в силу леммы 3.7, (3) достаточно показать, что

$$(2)' \frac{1}{m!} \left(\frac{v^{p^n}}{p^n}\right)^m \in \mathbb{Z}_p\langle\langle v \rangle\rangle^{(1-1/p),0} \text{ для всех } n \geq 2 \text{ и } m \geq 0.$$

В силу леммы 3.7, (9) утверждение (2)' эквивалентно следующему:

$$(2)'' \operatorname{ord}_p\left(\frac{(p^n m)!}{m! p^{mn}}\right) \geq \left(1 - \frac{1}{p}\right)p^{n-1}m \text{ для всех } n \geq 2 \text{ и } m \geq 0.$$

Поскольку

$$\operatorname{ord}_p\left(\frac{(p^n m)!}{m!}\right) = \sum_{j=0}^{n-1} p^j m \geq p^{n-1}m + m,$$

то для доказательства (2)'' достаточно проверить, что

$$p^{n-1}m + m - mn \geq \left(1 - \frac{1}{p}\right)p^{n-1}m,$$

т. е. что $m(p^{n-2} - n + 1) \geq 0$. А это легко проверяется.

ДОКАЗАТЕЛЬСТВО ПРЕДЛОЖЕНИЯ 3.4. Пусть $n \geq 0$ и $m = -\lceil n/p \rceil$. В силу леммы 3.7, (9)

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

В силу лемм 3.10 и 3.9, (2) имеем $\frac{v^n}{n!} \exp\left(v + \frac{v^p}{p}\right) \in \mathbb{Z}_p\langle\langle v \rangle\rangle^{(1-1/p),m} \cap \mathbb{Z}_p\langle\langle v \rangle\rangle$; а в силу следствия 3.8 имеем

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

для всех $a \geq 0$. Это содержится в $p^{\lceil (1-1/p)(m+a) \rceil} \mathbb{Z}_p\langle\langle v \rangle\rangle \cap \mathbb{Z}_p\langle\langle v \rangle\rangle$ в силу леммы 3.7, (2). Поскольку

$$\left(\left(\frac{d}{dv} - 1\right)^p + 1\right)^a \left(\frac{v^n}{n!} \exp\left(v + \frac{v^p}{p}\right)\right) = \exp(v) \left(\left(\frac{d}{dv} - 1\right)^p + 1\right)^a \left(\frac{v^n}{n!} \exp\left(\frac{v^p}{p}\right)\right)$$

и $\exp(v)$ является единицей в $\mathbb{Z}_p\langle\langle v \rangle\rangle$, видим, что

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

Подставляя $m = -\lfloor n/p \rfloor$, получаем

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

Рассматривая коэффициенты при $v^{n+qp}/(n+qp)!$ или $v^{n-r_0p}/(n-r_0p)!$ этого выражения, умноженного на $n!$, получаем требуемые сравнения.

3.3. Второй инструмент для доказательства. Докажем второе предложение, которое используется в доказательстве теоремы 3.1.

ПРЕДЛОЖЕНИЕ 3.11. Пусть p – нечетное простое число и U – разбиение, в котором $U_{p-1} = 0$, $d(U) \neq 0$. Тогда для τ_U , заданного формулой (2.7), выполняется неравенство

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

ЗАМЕЧАНИЕ 3.12. Как упомянуто в замечании 3.2, (2), равенство $\text{ord}_p(\tau_U) = (p-5)/2$ выполнено для любого простого числа $p \geq 5$ и любого разбиения U , в котором $U_1 = p$, $U_{2p-1} = (p-5)/2$, а остальные элементы U_j равны 0. Для такого U вышеприведенная оценка неуллучшаема, поскольку

$$w(U) = p + \frac{(2p-1)(p-5)}{2}, \quad d(U) = p + \frac{p-5}{2}$$

и

$$\left\lfloor \frac{w(U) + d(U) - 2}{2p} \right\rfloor = \left\lfloor \frac{p^2 - 3p - 2}{2p} \right\rfloor = \left\lfloor \frac{p-5}{2} + \frac{p-1}{p} \right\rfloor = \frac{p-5}{2}.$$

ДОКАЗАТЕЛЬСТВО ПРЕДЛОЖЕНИЯ 3.11. Так как $d(U) \neq 0$, то $w(U) + d(U) - 2 > 0$. При $U_{2p-1} \neq 0$ оценка доказывается следующим образом:

$$\begin{aligned} \text{ord}_p(\tau_U) &= \text{ord}_p((n+d-2)!) - \text{ord}_p(\gamma_U) \\ &= \text{ord}_p \left(\left(-2 + \sum_{j \neq p-1} (j+1)U_j \right)! \right) - \sum_{(\varepsilon, k) \neq (1,1)} kU_{\varepsilon p^k-1} - \sum_{j \neq p-1} \text{ord}_p(U_j!) \end{aligned}$$

(здесь и ниже ε пробегает множество натуральных чисел, взаимно простых с p)

$$\begin{aligned} &\geq \text{ord}_p \left(\left(-2 + \sum_{j \neq p-1, 2p-1} jU_j + 2pU_{2p-1} \right)! \right) - \sum_{(\varepsilon, k) \neq (1,1)} kU_{\varepsilon p^k-1} - \text{ord}_p(U_{2p-1}!) \\ &= \text{ord}_p \left(\left(-2 + \sum_{p \nmid (j+1)} jU_j + \sum_{(\varepsilon, k) \neq (1,1), (2,1)} (\varepsilon p^k - 1)U_{\varepsilon p^k-1} + 2pU_{2p-1} \right)! \right) \\ &\quad - \sum_{(\varepsilon, k) \neq (1,1)} kU_{\varepsilon p^k-1} - \text{ord}_p(U_{2p-1}!) \end{aligned}$$

$$\begin{aligned}
&\geq \sum_{\nu=1}^{\infty} \left\lfloor \frac{1}{p^{\nu}} \left(-2 + \sum_{p \nmid (j+1)} jU_j + \sum_{(\varepsilon, k) \neq (1,1), (2,1)} (\varepsilon p^k - 1)U_{\varepsilon p^k - 1} + 2pU_{2p-1} \right) \right\rfloor \\
&\quad - \sum_{(\varepsilon, k) \neq (1,1)} kU_{\varepsilon p^k - 1} - \text{ord}_p(U_{2p-1}!) \quad \left(\text{так как } \text{ord}_p(N!) = \sum_{\nu=1}^{\infty} \left\lfloor \frac{N}{p^{\nu}} \right\rfloor \right) \\
&= \left\lfloor \frac{1}{p} \left(-2 + \sum_{p \nmid (j+1)} jU_j + \sum_{(\varepsilon, k) \neq (1,1), (2,1)} (\varepsilon p^k - 1)U_{\varepsilon p^k - 1} + 2pU_{2p-1} \right) \right\rfloor \\
&\quad + \sum_{\nu=2}^{\infty} \left\lfloor \frac{1}{p^{\nu}} \left(-2 + \sum_{p \nmid (j+1)} jU_j + \sum_{(\varepsilon, k) \neq (1,1), (2,1)} (\varepsilon p^k - 1)U_{\varepsilon p^k - 1} + 2pU_{2p-1} \right) \right\rfloor \\
&\quad - \sum_{(\varepsilon, k) \neq (1,1)} kU_{\varepsilon p^k - 1} - \text{ord}_p(U_{2p-1}!) \\
&\geq \left\lfloor \frac{1}{p} \left(-2 + \sum_{p \nmid (j+1)} jU_j + \sum_{(\varepsilon, k) \neq (1,1), (2,1)} (\varepsilon p^k - 1)U_{\varepsilon p^k - 1} + 2pU_{2p-1} \right) \right\rfloor \\
&\quad + \sum_{\nu=2}^{\infty} \left\lfloor \frac{-2 + 2pU_{2p-1}}{p^{\nu}} \right\rfloor - \sum_{(\varepsilon, k) \neq (1,1)} kU_{\varepsilon p^k - 1} - \text{ord}_p(U_{2p-1}!) \\
&= \left\lfloor \frac{1}{p} \left(-2 + \sum_{p \nmid (j+1)} jU_j + \sum_{(\varepsilon, k) \neq (1,1), (2,1)} (\varepsilon p^k - 1)U_{\varepsilon p^k - 1} + 2pU_{2p-1} \right) \right\rfloor \\
&\quad - \sum_{(\varepsilon, k) \neq (1,1)} kU_{\varepsilon p^k - 1} + \sum_{\nu=2}^{\infty} \left\lfloor \frac{-2 + 2pU_{2p-1}}{p^{\nu}} \right\rfloor - \text{ord}_p(U_{2p-1}!) \\
&= \left\lfloor \frac{1}{p} \left(-2 + \sum_{p \nmid (j+1)} jU_j + \sum_{(\varepsilon, k) \neq (1,1), (2,1)} (\varepsilon p^k - kp - 1)U_{\varepsilon p^k - 1} + 2pU_{2p-1} \right) \right\rfloor \\
&\quad - U_{2p-1} + \sum_{\nu=2}^{\infty} \left\lfloor \frac{-2 + 2pU_{2p-1}}{p^{\nu}} \right\rfloor - \text{ord}_p(U_{2p-1}!) \\
&= \left\lfloor \frac{1}{p} \left(-2 + \sum_{p \nmid (j+1)} jU_j + \sum_{(\varepsilon, k) \neq (1,1), (2,1)} (\varepsilon p^k - kp - 1)U_{\varepsilon p^k - 1} + 2pU_{2p-1} \right) \right\rfloor \\
&\quad - U_{2p-1} + \text{ord}_p((-2 + 2pU_{2p-1})!) - \left\lfloor \frac{-2 + 2pU_{2p-1}}{p} \right\rfloor - \text{ord}_p(U_{2p-1}!).
\end{aligned}$$

Здесь первый член $-2/p$ можно заменить на $-1/p$, поскольку если в первых скобках $\lfloor \cdot \rfloor$ сумма остальных членов – целое число, то и $-2/p$ и $-1/p$ дают вклад как -1 , а если эта сумма – не целое число, то его дробная часть больше или равна $1/p$. Более того, так как $j \geq (j+1)/2$ для jU_j во втором члене суммы, а $\varepsilon p^k - kp - 1 > \varepsilon p^k/2$, если $(\varepsilon, k) \neq (1,1), (2,1)$ для третьего члена суммы, то, используя (1.1), видим, что выкладку можно продолжить следующим образом:

$$\begin{aligned}
&\geq \left\lfloor \frac{1}{2p} \left(-2 + \sum_{p \nmid (j+1)} (j+1)U_j + \sum_{(\varepsilon, k) \neq (1,1), (2,1)} \varepsilon p^k U_{\varepsilon p^k - 1} + 2pU_{2p-1} \right) + U_{2p-1} \right\rfloor \\
&\quad - U_{2p-1} + \text{ord}_p((-2 + 2pU_{2p-1})!) - \left\lfloor \frac{-2 + 2pU_{2p-1}}{p} \right\rfloor - \text{ord}_p(U_{2p-1}!)
\end{aligned}$$

$$\begin{aligned}
&= \left\lfloor \frac{-2 + w(U) + d(U)}{2p} \right\rfloor + \text{ord}_p((2U_{2p-1})!) + 2U_{2p-1} - \text{ord}_p(2pU_{2p-1}) \\
&\quad - \left\lfloor \frac{-2 + 2pU_{2p-1}}{p} \right\rfloor - \text{ord}_p(U_{2p-1}!) \\
&= \left\lfloor \frac{-2 + w(U) + d(U)}{2p} \right\rfloor + \text{ord}_p((2U_{2p-1})!) + 2U_{2p-1} - \text{ord}_p(2U_{2p-1}) - 1 \\
&\quad - (-1 + 2U_{2p-1}) - \text{ord}_p(U_{2p-1}!) \\
&\geq \left\lfloor \frac{-2 + w(U) + d(U)}{2p} \right\rfloor + \text{ord}_p\left(\frac{(2U_{2p-1} - 1)!}{U_{2p-1}!}\right).
\end{aligned}$$

Это завершает доказательство для случая $U_{2p-1} \neq 0$. Если же $U_{2p-1} = 0$, то требуемую оценку легко доказать, подставив это значение в начало вычислений.

3.4. Доказательство сравнений типа Куммера. Завершим доказательство теоремы 3.1. В силу предложения 2.8, левая часть сравнения в теореме 3.1, умноженная на $(-1)^a$, переписывается в виде

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

где τ_U определено в (2.7). Выбирая f_{p-1}^r или $f_{p-1}^{r-r_0}$ из f^U , мы знаем, что (3.13) равно

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

где $U[r]$ обозначает $(p-1)$ -й член из U , увеличенный на r . Переставив суммы по r и по U и учитывая выражения для $\tau_{U[r]}$ и $\tau_{U[r-r_0]}$, видим, что (3.14) равно

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

Здесь $U|_{p-1}$ — величина, получающаяся заменой $(p-1)$ -го члена из U на 0, так что $\gamma_{U|_{p-1}}$ в первой сумме есть то, что получается удалением $(p-1)$ -й части $p^{U_{p-1}}U_{p-1}!$ из γ_U . Заметим, что для каждого r выполнены равенства

$$\gamma_{U[r]|_{p-1}} = \gamma_{U|_{p-1}}, \quad \gamma_{U[r]|_{p-1}} p^{r+U_{p-1}}(r+U_{p-1})! = \gamma_{U[r]} \quad (3.16)$$

и в последней сумме выражение

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

не содержит $(p-1)$ -ю часть. Пусть $\sum_1$ и $\sum_2$ обозначают первую и вторую суммы из (3.15) соответственно; кроме того, обозначим

$$\sum_1 + \sum_2 = \sum_{w(U)=n} S_1(U) + \sum_{r_0=1}^a \sum_{\substack{w(U)=n+r_0(p-1) \\ U_{p-1}=0}} S_2(U). \quad (3.18)$$

Тогда для $S_1(U)$ от U при $n = w(U)$ имеем

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

Заметим, что

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

Для $S_2(U)$ от U при $w(U) = n + r_0(p-1)$ видим, что

$$\begin{aligned} w(U[r - r_0]) + d(U[r - r_0]) - 2 \\ &= n + r_0(p-1) + (p-1)(r - r_0) + d(U) + (r - r_0) - 2 \\ &= (r - r_0)p + n + r_0p + d(U) - r_0 - 2. \end{aligned} \quad (3.21)$$

Разобьем $\sum_1$ (соответственно $\sum_2$) на две части в зависимости от того, удовлетворяет $n - pU_{p-1} + d(U) - 2$ в (3.20) (соответственно $n + r_0p + d(U) - r_0 - 2$ в (3.21)) неравенству $\geq ap$ или $< ap$, и обозначим эту сумму через $\sum'_1 + \sum''_1$ (соответственно $\sum'_2 + \sum''_2$). Здесь обратим внимание на то, что в (3.20) выполняется неравенство $n - pU_{p-1} + d(U) - 2 > 0$, поскольку $n \not\equiv 0 \pmod{p-1}$.

(а) Для суммы $\sum'_1$, так как $n - pU_{p-1} + d(U) - 2 \geq ap$, имеем

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

в силу предложений 3.4, (1) и 3.11.

(б) Для суммы $\sum''_1$ положим $N = n - pU_{p-1} + d(U) - 2$ и $N = pb + e$ ($0 \leq e < p$). Тогда видим, что $b < a$, потому что $0 < n - pU_{p-1} + d(U) - 2 < ap$. Поэтому в силу предложения 3.11 имеем

$$\begin{aligned} \text{ord}_p(N!) - \text{ord}_p(\gamma_{U|_{p-1}}) &= \text{ord}_p((w(U|_{p-1}) + d(U|_{p-1}) - 2)!) - \text{ord}_p(\gamma_{U|_{p-1}}) \\ &= \text{ord}_p(\tau_{U|_{p-1}}) \geq \left\lfloor \frac{N}{2p} \right\rfloor. \end{aligned} \quad (3.23)$$

Это и предложение 3.4, (1) дают

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

Так как левая часть – целое число, она должна быть $\geq \lfloor a/2 \rfloor$. Следовательно, $\text{ord}_p(\sum_1) \geq \lfloor a/2 \rfloor$. Можно доказать, что $\text{ord}_p(\sum_2) \geq \lfloor a/2 \rfloor$, используя предложение 3.4, (2) вместо предложения 3.4, (1). Относительно такого доказательства мы должны иметь в виду, что для случая $n + r_0p + d(U) - r_0 - 2 < ap$ в (3.21), чтобы использовать утверждение (2) предложения 3.4, нужно иметь $n + r_0p + d(U) - r_0 - 2 \geq r_0p$. Однако, так как $d(U) \geq 1$, это условие выполняется, если $n + r_0p + 1 - r_0 - 2 \geq r_0p$, т.е. $n - r_0 - 1 \geq 0$. Последнее условие справедливо для всех $r_0 = 1, \dots, a$ в силу нашего предположения $n > a$.

ЗАМЕЧАНИЕ 3.25. Если в теореме 3.1 заменить условие $a < n$ на $a = n$, то сравнение типа Куммера для обобщенных чисел Бернулли–Гурвица, описываемое далее, выполняется только по модулю p^{n-1} . С помощью численных подсчетов можно видеть, что модуль такого сравнения неулучшаем. Это означает, что условие $a < n$ в теореме 3.1 существенно, потому что обобщенные числа Бернулли–Гурвица задаются специализацией универсальных чисел Бернулли.

3.5. Сравнение Куммера–Аделберга. Докажем сравнение Аделберга в следствии 3.3, используя теорему 3.1 и замечание 3.2, (1).

ДОКАЗАТЕЛЬСТВО СЛЕДСТВИЯ 3.3. Заметим, что если $p = 3$, то условие $n \not\equiv 0, 1 \pmod{p-1}$ всегда неверно и утверждение следствия 3.3 пусто. Таким образом, мы можем предполагать, что $p \geq 5$. Докажем сравнение индукцией по a . Так как мы уже упоминали случай $a = 1$ в замечании 3.2, (1), считаем, что $a > 1$. Выбирая p^{a-1} в качестве a в теореме 3.1, видим, что

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

Здесь имеем $\lfloor p^{a-1}/2 \rfloor > a$, так как $a \geq 2$ и $p \geq 5$. Если $r \neq 0$ и $r \neq p^{a-1}$, то

$$\text{ord}_p \binom{p^{a-1}}{r} = \frac{S_p(p^{a-1}-r) + S_p(r) - S_p(p^{a-1})}{p-1} = \frac{S_p(p^{a-1}-r) + S_p(r) - 1}{p-1} \tag{3.27}$$

в силу (1.2). Обозначим $\nu = \text{ord}_p r$. Пусть

$$\begin{aligned}
 p^{a-1} - r &= d_{a-2}p^{a-2} + d_{a-3}p^{a-3} + \dots + d_1p + d_0 & (0 \leq d_j \leq p-1), \\
 r &= h_{a-2}p^{a-2} + h_{a-3}p^{a-3} + \dots + h_1p + h_0 & (0 \leq h_j \leq p-1)
 \end{aligned}$$

– представления по основанию p . Тогда, очевидно,

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

А именно,

$$S_p(p^{a-1} - r) + S_p(r) = (p-1)(a-2-\nu) + p.$$

Таким образом, $\text{ord}_p \binom{p^{a-1}}{r} = a-1-\nu$. Имея в виду, что p – нечетное число, рассмотрим сумму

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

при $0 < r \leq (p^{a-1}-1)/2$. Подводя итог вышеприведенным рассмотрениям, видим, используя предположение индукции по $\nu = \text{ord}_p r = \text{ord}_p(p^{a-1}-r)$

($< a$), что D_r делится на p^a . Так как $f_{p-1} p^{a-1} \frac{\widehat{B}_n}{n} - \frac{\widehat{B}_{n+p^{a-1}(p-1)}}{n+p^{a-1}(p-1)}$ является разностью левой части из (3.26) и $\sum_{r=1} D_r$, получаем следствие 3.3.

4. Гиперэллиптические функции

4.1. Основные сведения о гиперэллиптических функциях. Рассмотрим гиперэллиптическую кривую $\mathcal{C}$ рода g , заданную уравнением $y^2 = f(x)$, где

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

– многочлен от x над $\mathbb{C}$ и $f(x) = 0$ не имеет кратных корней. Положим для удобства $\lambda_0 = 1$. Кривая $\mathcal{C}$ рассматривается как невырожденная алгебраическая кривая с единственной бесконечно удаленной точкой ∞ . Как хорошо известно, множество дифференциалов

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

образует базис дифференциальных форм первого рода на $\mathcal{C}$. Пусть $[\omega \ \omega'']$ – матрица периодов, определяемая выбором подходящего множества порождающих фундаментальной группы кривой $\mathcal{C}$, и пусть

$$\Lambda := \omega'^t [\mathbb{Z} \ \mathbb{Z} \ \dots \ \mathbb{Z}] + \omega''^t [\mathbb{Z} \ \mathbb{Z} \ \dots \ \mathbb{Z}] \quad (\subset \mathbb{C}^g)$$

– решетка в $\mathbb{C}^g$ относительно дифференциалов (4.1). Обозначим через J многообразие Якоби кривой $\mathcal{C}$, а через $\text{Sym}^g(\mathcal{C})$ симметрическое произведение g копий $\mathcal{C}$. Тогда имеем бирациональное отображение

$$\text{Sym}^g(\mathcal{C}) \rightarrow \text{Pic}^\circ(\mathcal{C}) = J, \quad (P_1, \dots, P_g) \mapsto \text{класс дивизора } P_1 + \dots + P_g - g \cdot \infty.$$

Отождествим J как аналитическое многообразие с $\mathbb{C}^g/\Lambda$. Обозначим естественное отображение $\mathbb{C}^g \mapsto \mathbb{C}^g/\Lambda = J$ через κ . Отображение

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

является вложением $\mathcal{C}$ в J . Поднятие $\kappa^{-1}\iota(\mathcal{C})$ отображения ι относительно κ является *универсальным абелевым накрытием* кривой $\mathcal{C}$. Вышеупомянутое бирациональное отображение посылает каждый элемент $(P_1, \dots, P_g) \in \text{Sym}^g(\mathcal{C})$ в точку $\mathbf{u} \bmod \Lambda \in \mathbb{C}^g/\Lambda$, где

$$\mathbf{u} = (u_1, \dots, u_g) = \left(\int_{\infty}^{P_1} + \dots + \int_{\infty}^{P_g} \right) (\omega_1, \dots, \omega_g). \quad (4.2)$$

Важно следующее соглашение об обозначениях.

Соглашение: в этой работе обозначаем u_g просто через u .

4.2. Гиперэллиптические функции и их переменная. В этой работе для каждой точки $\mathbf{u} \in \kappa^{-1}\iota(\mathcal{C})$ обозначаем через

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

координаты (x, y) на $\mathcal{C}$ такие, что $\kappa(\mathbf{u}) = \iota(x(\mathbf{u}), y(\mathbf{u}))$. Мы называем рациональное выражение в терминах $x(\mathbf{u})$ и $y(\mathbf{u})$ гиперэллиптической функцией и рассматриваем его также как функцию на $\kappa^{-1}\iota(\mathcal{C})$. Мы подтверждаем следующий фундаментальный факт.

ЛЕММА 4.3. *Члены наименьшей степени в разложениях Лорана функций $x(\mathbf{u})$ и $y(\mathbf{u})$ в точке $\mathbf{u} = (0, \dots, 0)$ относительно $u = u_g$ задаются как*

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

ДОКАЗАТЕЛЬСТВО. Возьмем $t = 1/\sqrt{x}$ в качестве локального параметра в точке ∞ . Здесь мы рассматриваем ту ветвь, где $t > 0$ при $x > 0$. Предположим, что точка $\mathbf{u} \in \kappa^{-1}\iota(\mathcal{C})$ достаточно близка к $(0, 0, \dots, 0)$ и что координаты трех типов t , $\mathbf{u} = (u_1, \dots, u_g)$, (x, y) соответствуют одной и той же точке из $\mathcal{C}$. Тогда

$$\begin{aligned} u = u_g &= \int_{\infty}^{(x,y)} \frac{x^{g-1} dx}{2y} = \int_{\infty}^{(x,y)} \frac{x^{-3/2} dx}{2\sqrt{1 + \lambda_1 \frac{1}{x} + \dots + \lambda_{2g+1} \frac{1}{x^{2g+1}}}} \\ &= \int_0^t \frac{t^3 \cdot (-\frac{2}{t^3}) dt}{2 + (d^\circ \geq 1)} = -t + (d^\circ(t) \geq 2). \end{aligned}$$

Таким образом, $x(\mathbf{u}) = 1/u^2 + (d^\circ(u) \geq -1)$. Аналогичный факт доказывается для $y(\mathbf{u})$. По определению видим, что $x(-\mathbf{u}) = x(\mathbf{u})$, $y(-\mathbf{u}) = -y(\mathbf{u})$. Доказательство завершено.

Следующие свойства доказываются аналогичными рассуждениями и их доказательства опускаются.

5.2. Случай $y(\mathbf{u})^2 = x(\mathbf{u})^{2g+1} - 1$. В этом случае уравнение (5.2) принимает вид

$$x(\mathbf{u})^{2g-2}x'(\mathbf{u})^2 = 4x^{2g+1}(\mathbf{u}) - 4 \quad \left(' \text{ означает } \frac{d}{du} \right). \quad (5.5)$$

Это является обобщением уравнения $\wp'(u)^2 = 4\wp(u)^3 - 1$. Здесь мы описываем автоморфизмы кривой $\mathcal{C}$, заданной уравнением $y^2 = x^{2g+1} - 1$, и ее многообразие Якоби J . Пусть $\zeta = e^{2\pi\sqrt{-1}/(2g+1)}$. Тогда $\mathcal{C}$ обладает автоморфизмами

$$\pm[\zeta^j]: \mathcal{C} \rightarrow \mathcal{C}, \quad (x, y) \mapsto (\zeta^j x, \pm y) \quad (j = 0, \dots, 2g).$$

Они индуцируют автоморфизмы многообразия $\text{Pic}^\circ(\mathcal{C})$ по правилу

$$\pm[\zeta^j]: P_1 + \dots + P_g - g \cdot \infty \mapsto (\pm[\zeta^j])P_1 + \dots + (\pm[\zeta^j])P_g - g \cdot \infty,$$

где $P_1, \dots, P_g \in \mathcal{C}$, а также дают автоморфизмы многообразия J . Из (4.1) и (4.2) мы видим, что

$$-[\zeta](u_1, u_2, \dots, u_g) = (-\zeta u_1, -\zeta^2 u_2, \dots, -\zeta^g u_g).$$

А именно,

$$x(-[\zeta]\mathbf{u}) = \zeta x(\mathbf{u}), \quad y(-[\zeta]\mathbf{u}) = -y(\mathbf{u}). \quad (5.6)$$

Поэтому, если n не делится на $2(2g+1)$, то $C_n = D_n = 0$.

5.3. Случай $y(\mathbf{u})^2 = x(\mathbf{u})^{2g+1} - x(\mathbf{u})$. В этом случае уравнение (5.2) принимает вид

$$x(\mathbf{u})^{2g-2}x'(\mathbf{u})^2 = 4x(\mathbf{u})^{2g+1} - 4x(\mathbf{u}) \quad \left(' \text{ означает } \frac{d}{du} \right). \quad (5.7)$$

Это является обобщением уравнения $\wp'(u)^2 = 4\wp(u)^3 - 4\wp(u)$. Опишем автоморфизмы кривой $\mathcal{C}$, заданной уравнением $y^2 = x^{2g+1} - x$, и ее якобиан J . Пусть $\zeta = e^{2\pi\sqrt{-1}/(2g)}$. Тогда $\mathcal{C}$ обладает автоморфизмами

$$[\zeta^j]: \mathcal{C} \rightarrow \mathcal{C}, \quad (x, y) \mapsto (\zeta^{2j} x, \zeta^j y) \quad (j = 0, \dots, 2g).$$

Они индуцируют автоморфизмы многообразия $\text{Pic}^\circ(\mathcal{C})$ по правилу

$$\pm[\zeta^j]: P_1 + \dots + P_g - g \cdot \infty \mapsto (\pm[\zeta^j])P_1 + \dots + (\pm[\zeta^j])P_g - g \cdot \infty,$$

где $P_1, \dots, P_g \in \mathcal{C}$, а также дают автоморфизмы якобиана J . Из (4.1) и (4.2) мы видим, что

$$[\zeta](u_1, u_2, \dots, u_g) = (\zeta u_1, \zeta^3 u_2, \dots, \zeta^{2g-1} u_g).$$

А именно,

$$x([\zeta]\mathbf{u}) = \zeta^2 x(\mathbf{u}), \quad y([\zeta]\mathbf{u}) = \zeta y(\mathbf{u}). \quad (5.8)$$

Поэтому, если n взаимно просто с $4g$, то $C_n = D_n = 0$.

6. Теоремы фон Штаудта в алгебраических функциях

6.1. Случай $y(u)^2 = x(u)^{2g+1} - 1$. В этом случае теоремы типа Кларка для $C_{(4g+2)n}$ и $D_{(4g+2)n}$ формулируются следующим образом.

ТЕОРЕМА 6.1. *Для каждого из чисел $C_{(4g+2)n}$ и $D_{(4g+2)n}$, определенных соответственно в (5.3) и (5.4) для кривой $y^2 = x^{2g+1} - 1$, имеем*

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

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

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

Эти результаты, очевидно, доказывают следующие обобщения теоремы фон Штаудта–Клаузена и второй теоремы фон Штаудта для $C_{(4g+2)n}$ и $D_{(4g+2)n}$.

СЛЕДСТВИЕ 6.2. (1) *Для каждого из чисел $C_{(4g+2)n}$ и $D_{(4g+2)n}$ существуют рациональные целые числа $G_{(4g+2)n}$ и $H_{(4g+2)n}$ такие, что*

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

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

где A_p то же, что в теореме 6.1.

(2) *Если $(p-1) \nmid (4g+2)n$, то $\frac{C_{(4g+2)n}}{(4g+2)n}$ и $\frac{D_{(4g+2)n}}{(4g+2)n}$ принадлежат $\mathbb{Z}_p$.*

ДОКАЗАТЕЛЬСТВО. Пусть $p \equiv 1 \pmod{2g+1}$, $(4g+2)m = a(p-1)$ и $\text{ord}_p a = \nu$. Тогда

$$\frac{(4g+2)m \cdot (a|_p^{-1} \pmod{p^{1+\nu}})}{p^{1+\nu}} \equiv 1 - \frac{1}{p} \equiv -\frac{1}{p} \pmod{\mathbb{Z}}.$$

Из этого следуют требуемые результаты.

6.2. Случай $y(u)^2 = x(u)^{2g+1} - x(u)$. В этом случае теоремы типа Кларка для C_{4gn} и D_{4gn} формулируются следующим образом.

ТЕОРЕМА 6.3. Для каждого из чисел C_{4gn} и D_{4gn} , определенных соответственно в (5.3) и (5.4) для кривой $y^2 = x^{2g+1} - x$, имеем

$$\frac{C_{4gn}}{4gn} \equiv - \sum_{\substack{p \equiv 1 \pmod{4g} \\ 4gn = a(p-1)}} \frac{a|_p^{-1} \pmod{p^{1+\text{ord}_p a}}}{p^{1+\text{ord}_p a}} A_p^a \pmod{\mathbb{Z}},$$

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

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

Эти результаты доказывают следующие обобщения теоремы фон Штаудта–Клаузена и второй теоремы фон Штаудта для C_{4gn} и D_{4gn} .

СЛЕДСТВИЕ 6.4. (1) Для каждого из чисел C_{4gn} и D_{4gn} существуют целые числа G_{4gn} и H_{4gn} такие, что

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

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

где A_p то же, что в теореме 6.3.

(2) Если $(p-1) \nmid 4gn$, то $C_{4gn}/(4gn)$ и $D_{4gn}/(4gn)$ принадлежат $\mathbb{Z}_p$.

ДОКАЗАТЕЛЬСТВО. Аналогично доказательству следствия 6.2.

6.3. Замечание об A_p . Предположим, что p – простое число такое, что $p \equiv 1 \pmod{2g+1}$ или $p \equiv 1 \pmod{4g}$ в зависимости от того, задана $\mathcal{C}$ уравнением $y^2 = x^{2g+1} - 1$ или $y^2 = x^{2g+1} - x$.

Возьмем множество дифференциалов (4.1), а именно

$$\left(\frac{1}{2y}, \frac{x}{2y}, \dots, \frac{x^{g-1}}{2y} \right),$$

в качестве базиса дифференциальных форм первого рода на $\mathcal{C} \pmod{p}$. Тогда матрица Хассе–Витта (размера $g \times g$) относительно этого базиса является диагональной матрицей [30; с. 381], а ее (g, g) -элемент – это просто число A_p . Как отметил, что в случае чисел Гурвица A_p равно инварианту Хассе (единственный элемент матрицы Хассе–Витта!), см. [31; с. 2]. Наши результаты являются вполне естественным обобщением этого факта.

7. Сравнение Куммера в алгебраических функциях

7.1. Случай $y(u)^2 = x(u)^{2g+1} - 1$. В этом случае сравнение типа исходного сравнения Куммера для $C_{(4g+2)n}$ и $D_{(4g+2)n}$ формулируются следующим образом.

ТЕОРЕМА 7.1. Пусть $C_{(4g+2)n}$ и $D_{(4g+2)n}$ – числа, определенные соответственно в (5.3) и (5.4) для кривой $y^2 = x^{2g+1} - 1$. Для простого числа $p \equiv 1 \pmod{2g+1}$ и натуральных чисел a и n таких, что $(4g+2)n - 2 \geq a$, если $(p-1) \nmid (4g+2)n$, то имеем

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

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

где

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

Эти сравнения в точности того же вида, как в исходной работе Куммера [4] и как в случае чисел Гурвица [7; с. 193, формула (26)].

ЗАМЕЧАНИЕ 7.4. (1) При выполнении соотношений (10.1), (10.2) и (10.3), доказываемых ниже, теорема 7.1 выполняется по модулю $p^{\lfloor a/2 \rfloor}$.

(2) Если в теореме 7.1 заменить условие $(4g+2)n - 2 \geq a$ на $(4g+2)n - 2 < a$, то, по-видимому, сравнение будет выполняться по модулю p^{n-1} , и этот модуль неулучшаем.

7.2. Случай $y(u)^2 = x(u)^{2g+1} - x(u)$. В этом случае сравнение типа исходного сравнения Куммера для C_{4gn} и D_{4gn} формулируются следующим образом.

ТЕОРЕМА 7.5. Пусть C_{4gn} и D_{4gn} – числа, определенные соответственно в (5.3) и (5.4) для кривой $y^2 = x^{2g+1} - x$. Для простого числа $p \equiv 1 \pmod{4g}$ и натуральных a и n , удовлетворяющих $4gn - 2 = a$, если $(p-1) \nmid 4gn$, то

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

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

где

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

Эти соотношения также имеют такой же вид, как в исходной работе [4] для чисел Бернулли и как в [7; с. 193, формула (23)] для чисел Гурвица.

ЗАМЕЧАНИЕ 7.6. В силу легко доказываемых простых соотношений (11.1), (11.2), (11.3) (см. ниже), видим, что теорема 7.5 выполняется по модулю $p^{\lfloor a/2 \rfloor}$.

8. Целые по Гурвицу ряды

8.1. Определение и основные свойства. Мы опишем здесь понятие целостности по Гурвицу и его свойства. В этом пункте буква R всегда означает подкольцо поля p -адических чисел $\mathbb{Q}_p$ для фиксированного простого числа p .

В нашей практике R будет $\mathbb{Z}\left[\frac{1}{q}\right]$ с ненулевым целым числом q , локализацией $\mathbb{Z}_{(p)}$ кольца целых чисел $\mathbb{Z}$ относительно p или его p -адическим пополнением $\mathbb{Z}_p$.

ОПРЕДЕЛЕНИЕ 8.1. Пусть z – неизвестная или переменная. Пусть

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

– степенной ряд относительно z . Если все коэффициенты h_n принадлежат R , то $h(z)$ называется целым по Гурвицу над R . Кольцо, состоящее из целых по Гурвицу рядов над R относительно z , обозначается через $R\langle\langle z \rangle\rangle$.

Кольцо $R\langle\langle z \rangle\rangle$ является областью целостности и замкнуто относительно операций $\frac{d}{dz}$ и $\int_0^z \cdot dz$. Ряд $h(z) \in R\langle\langle z \rangle\rangle$ является единицей в $R\langle\langle z \rangle\rangle$ тогда и только тогда, когда его постоянный член является единицей в R . Более того, легко доказываются следующие свойства (см. [6; § 1]).

ПРЕДЛОЖЕНИЕ 8.2. Пусть

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

(1) Если первые n коэффициентов $h_0, \dots, h_{n-1}$ принадлежат R и существует многочлен F от n переменных над R такой, что выполняется соотношение

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

для производных ряда $h(z)$, то $h(z) \in R\langle\langle z \rangle\rangle$.

(2) Если $h(z) \in R\langle\langle z \rangle\rangle$, $h_0 = 0$ и $h_1 = 1$, то формальный обратный ряд

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

ряда $w = h(z)$ также принадлежит $R\langle\langle z \rangle\rangle$.

(3) Если $h(z) \in R\langle\langle z \rangle\rangle$, $h_0 = 0$ и $h_1 = 1$, то для любого натурального m ряд

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

также принадлежит $R\langle\langle z \rangle\rangle$.

8.2. Целостность по Гурвицу ряда $x(u)^{1/2}$. Здесь мы проверяем следующий факт.

ПРЕДЛОЖЕНИЕ 8.3. На кривой $y^2 = x^{2g+1} - 1$ или $y^2 = x^{2g+1} - x$ имеем

$$t := -\frac{1}{x(u)^{1/2}} (= u + \dots) \in \mathbb{Z}\langle\langle u \rangle\rangle.$$

ДОКАЗАТЕЛЬСТВО. Для простоты мы рассмотрим только случай кривой $y^2 = x^5 - 1$. Обозначим $t' = dt/du$, $t'' = d^2t/du^2$, ... В силу (5.5) видим, что

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

Продифференцировав это уравнение по u и разделив на $2t'$, имеем

$$t'' = -5t^9. \quad (8.5)$$

Так как $t(0) = t'(0) = 0$, предложение 8.2, (1) дает

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

для кривой $y^2 = x^5 - 1$.

8.3. Целостность по Гурвицу ряда $1/y(\mathbf{u})^{1/5}$. Здесь мы докажем следующий факт.

ПРЕДЛОЖЕНИЕ 8.7. *На кривой $y^2 = x^{2g+1} - 1$ или $y^2 = x^{2g+1} - x$ имеем*

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

ДОКАЗАТЕЛЬСТВО. Мы снова ограничимся рассуждением только для кривой $y^2 = x^5 - 1$. В силу (5.1) видим, что

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

и

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

Записывая для простоты $s' = \frac{ds}{du}$, $s'' = \frac{d^2s}{du^2}$, $\dots$, имеем $\frac{dy}{du} = -5s^{-6} \frac{ds}{du}$. Отсюда следует, что

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

Из этой формулы по индукции получаем, что n -я производная функции s для каждого целого числа $n \geq 1$ записывается как конечная сумма вида

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

где каждое P_{nj} означает многочлен от n переменных над $\mathbb{Z}$, а L_{nj} – целое число. Сочетая это с равенством $s(0) = 0$, видим, что $s'(0), s''(0), s^{(3)}(0), \dots$ все являются целыми числами. Поэтому мы заключаем, что для кривой $y^2 = x^5 - 1$

$$\frac{1}{y(\mathbf{u})^{1/5}} = -u - 48 \cdot 9! \frac{u^{11}}{11!} + \dots \in \mathbb{Z}\langle\langle u \rangle\rangle. \quad (8.12)$$

9. Схема доказательства

Мы дадим набросок доказательств теорем 6.1 и 7.1 (а также теорем 6.3 и 7.5), рассматривая для примера случай кривой $y^2 = x^5 - 1$. Напомним наше соглашение о том, что для данного степенного ряда $\varphi(z)$ относительно z каждый коэффициент $\left[\frac{z^n}{n!} \right] \varphi(z)$ ($n \geq 0$) называется его *коэффициентом Гурвица*. В дальнейшем любые коэффициенты Гурвица – это коэффициенты Гурвица разложений относительно u .

9.1. Теоремы фон Штаудта в алгебраических функциях. Доказательство теоремы 6.1 разделено на следующие три шага.

1. Доказать теорему типа Кларка для коэффициентов Гурвица C_n/n функции $x(\mathbf{u})$ над $\mathbb{Z}\left[\frac{1}{2}\right]$.

2. Доказать теорему типа Кларка для коэффициентов Гурвица D_n/n функции $y(\mathbf{u})$ над $\mathbb{Z}\left[\frac{1}{5}\right]$.

3. Связать вышеупомянутые результаты. Используя простые формулы, касающиеся $D = d/du$ для функций $x(\mathbf{u})$, $x^2(\mathbf{u})$, $y(\mathbf{u})$, можно связать коэффициенты Гурвица этих функций и доказать, что оба результата в шагах 1 и 2 справедливы над $\mathbb{Z} = \mathbb{Z}\left[\frac{1}{2}\right] \cap \mathbb{Z}\left[\frac{1}{5}\right]$.

Более детальная схема такова.

Шаг 1. Доказываем теорему в стиле Кларка (10.7) для коэффициентов Гурвица $C_{10m}^{(1)}/(10m)$ функции $x^{1/2}(\mathbf{u})$ над $\mathbb{Z}\left[\frac{1}{2}\right]$. На следующем этапе доказываем соотношения между коэффициентами Гурвица функций $x(\mathbf{u})$ и $x^{1/2}(\mathbf{u})$, $x^{3/2}(\mathbf{u})$ и $x(\mathbf{u})$, а также $x^2(\mathbf{u})$ и $x^{3/2}(\mathbf{u})$. Это (10.11) при $k = 1, 2, 3$. Эти соотношения дают теоремы в стиле Кларка для этих коэффициентов Гурвица над $\mathbb{Z}\left[\frac{1}{2}\right]$ с помощью свойства целостности (10.3) коэффициентов Карлица (см. соглашение на с. 68) формального обратного ряда u относительно $t = x^{-1/2}(\mathbf{u})$.

Упомянутая выше теорема в стиле Кларка для коэффициентов Гурвица функции $x^2(\mathbf{u}) = (x^{1/2}(\mathbf{u}))^4$ (а именно, (10.15)) будет важна на шаге 3.

Шаг 2. В п. 11.1 доказываем теорему в стиле Кларка (11.7) для чисел Гурвица $D_{10m}^{(1)}/(10m)_4$ функции $y^{1/5}(\mathbf{u})$, используя целостность (11.3) коэффициентов Карлица формального обратного ряда u относительно $s = y^{-1/5}(\mathbf{u})$. С другой стороны, мы показываем, что выполняется соотношение (11.11) при $k = 1, 2, 3, 4$, а именно, соотношения между коэффициентами Гурвица функций $y^{(k+1)/5}(\mathbf{u})$ и $y^{k/5}(\mathbf{u})$ при $k = 1, 2, 3, 4$.

Суммируя эти соотношения, можно связать коэффициенты Гурвица $D_{10m} \times (10m)^{-1}$ функции $y(\mathbf{u}) = (y^{1/5}(\mathbf{u}))^5$ с $D_{10m}^{(1)}/(10m)$ (см. (11.12) и (11.13)). Поэтому получаем соотношение (11.14) для $D_{10m}/(10m)$ над $\mathbb{Z}\left[\frac{1}{5}\right]$ и завершаем шаг 2.

Шаг 3. Пусть $D = d/du$. Используя

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

можно показать, что D_{10m} и $C_{10m}^{(4)}$ — по существу одни и те же числа. Так как $D_{10m}/(10m) \in \mathbb{Z}_{(2)}$, то знаменатель числа $C_{10m}^{(4)}/(10m)_4$ не содержит ни степени 2, ни степени 5. Отсюда получаем соотношение (12.4) для $D_{10m}/(10m)$ над $\mathbb{Z}$, а именно, вторую формулу в теореме 6.1. Наконец, формула

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

с $D = d/du = (2y/x) d/dx$ и целостность по Гурвицу (8.6) функции $1/x^3(u)$ связывают $C_{10m}^{(4)}/(10m)_4$ с $C_{10m}/(10m)$. Таким образом, получаем желаемую теорему для $C_{10m}/(10m)$, которая является специализацией теоремы Кларка 2.9.

В [25; теорема 3.4] имеется также сравнение, связывающее универсальные числа Бернулли различного порядка и универсальный случай коэффициентов Гурвица различных степеней функции $1/t(u)$ относительно u . Хотя автор предполагает, что оно может быть тесно связано с нашим методом, использовать его не удалось.

9.2. Сравнения Куммера в алгебраических функциях. Пусть $p \equiv 1 \pmod{5}$ – фиксированное простое число. Мы опишем доказательство только для C_{10m} , теорема для D_{10m} доказывается аналогично. Схема доказательства такова.

Шаг 1. Показываем, что формальный обратный ряд $u(t) \in \mathbb{Z}_p\langle\langle t \rangle\rangle$ ряда $u \mapsto t = x(u)^{-1/2}$ удовлетворяет критерию Хонды (13.10). Отсюда следует, что формальный групповой закон F , формальным логарифмом которого является $u(t)$, а именно

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

определен над $\mathbb{Z}_p$ (см. предложение 13.1).

Шаг 2. Используя формулу Хохшильда и свойство Хонды (13.10), видим в п. 13.2, что

$$\left(\left(\frac{d}{du} \right)^p - A_p \frac{d}{du} \right) t(u) \in p\mathbb{Z}_p[[t(u)]] \quad (9.1)$$

для $t = t(u) = x(u)^{-1/2} \in \mathbb{Z}_p\langle\langle u \rangle\rangle$.

Шаг 3. Пусть $\xi \in \mathbb{Z}_p$ – примитивный корень $(p-1)$ -й степени из 1. Умножение на ξ

$$F_\xi(t) := u^{-1}(\xi u(t)) = \xi + \dots,$$

определяемое по F , принадлежит $\xi t + t^2 \mathbb{Z}_p[[t]]$ в силу результатов шага 1. Теперь мы используем обозначение

$$x\langle u \rangle = x(u) \in 1/u^2 + \mathbb{Q}_p[[u]],$$

чтобы избежать недоразумений. Благодаря существованию такого $F_\xi(t)$, легко показать, что

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

Прибавляя (9.1) к (9.2), получаем, что для любого целого числа $a > 0$

$$\left(\left(\frac{d}{du} \right)^p - A_p \frac{d}{du} \right)^a (x\langle u(t) \rangle - \xi^2 x\langle \xi u(t) \rangle) \in p^a \mathbb{Z}_p[[t]] \subset p^a \mathbb{Z}_p\langle\langle u \rangle\rangle. \quad (9.3)$$

Коэффициент при $u^{10n-a-2}/(10n-a-2)!$ есть не что иное, как левая часть первой формулы в теореме 7.1, и доказательство завершено.

Упомянем здесь, что сравнения типа Куммера для $C_{10m}^{(\nu)}$ и $D_{10m}^{(\nu)}$ без деления на $10m$ доказаны в п. 14.1.

10. Теорема Кларка для $x(u)$ над $\mathbb{Z}\left[\frac{1}{2}\right]$

В этом разделе мы имеем дело только с кривой $y^2 = x^5 - 1$.

10.1. Теорема Кларка для $x(u)^{1/2}$. Рассмотрим формальный обратный ряд ряда $u \mapsto \sqrt{x(u)}$, а именно, степенной ряд u относительно

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

т. е.

$$\begin{aligned} u &= \int_{\infty}^x \frac{x \, dx}{2y} = \int_0^{-t} \frac{(1/t^2) \cdot (-2 \, dt/t^3)}{2\sqrt{1/t^{10} - 1}} = - \int_0^{-t} \frac{1}{\sqrt{1 - t^{10}}} \, dt \\ &= - \int_0^{-t} \left(1 + \sum_{m=1}^{\infty} (-1)^m \binom{-\frac{1}{2}}{m} t^{10m} \right) dt = t + \sum_{m=1}^{\infty} (-1)^m \binom{-\frac{1}{2}}{m} \frac{t^{10m+1}}{10m+1}. \end{aligned}$$

Для удобства ссылок запишем это снова:

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

Обозначим коэффициент Карлица через

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

Это обозначение соответствует обозначению в определении универсальных чисел Бернулли. В силу леммы 1.4 и равенства (1.6) видим, что

$$f_{10m} \in \mathbb{Z}\left[\frac{1}{2}\right]. \quad (10.3)$$

Остальные коэффициенты f_n равны 0. Тогда деленное универсальное число Бернулли $\widehat{B}_{10m}/(10m)$ специализируется в $C_{10m}^{(1)}/(10m)$, а выражение из предложения 2.8 дает, что

$$\frac{C_{10m}^{(1)}}{10m} \in 3! \mathbb{Z}\left[\frac{1}{2}\right]. \quad (10.4)$$

Чтобы это доказать, применим предложение 3.11 при $p = 2$ и $p = 3$. Так как в этом случае $f_{2-1} = 0$ и $f_{3-1} = 0$, то можно рассматривать только те разбиения U , в которых $U_{2-1} = U_{3-1} = 0$. При этом, так как

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

видим, что

$$\text{ord}_2(\tau_U) \geq \left\lfloor \frac{10+1-2}{4} \right\rfloor = 2, \quad \text{ord}_3(\tau_U) \geq \left\lfloor \frac{10+1-2}{6} \right\rfloor = 1.$$

Отсюда следует, что в выражении из предложения 2.8 для $C_{10m}^{(1)}/(10m)$ все его коэффициенты делятся на $3!$. Добавляя это к (10.3), заключаем, что выполняется (10.4).

Если $p = 10m + 1$ – простое число, то коэффициент f_{p-1} при $t^{10m+1}/(10m+1)$ по модулю p совпадает с $(2, 2)$ -элементом матрицы Хассе–Витта относительно нашей канонической базы дифференциалов первого рода на кривой $\mathcal{C}$ редукции по модулю p ; а именно,

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

Об этом см. п. 18.1.

В условиях вышеприведенного рассмотрения применим теорему Кларка 2.9 для функции $u \mapsto x(u)^{1/2}$. Пусть

$$\frac{1}{t} = \sum_{m=0}^{\infty} \frac{C_{10m}^{(1)}}{10m} \frac{u^{10m-1}}{(10m-1)!}. \quad (10.6)$$

Из предложения 2.9 и включения (10.4) выводим, что

$$\frac{1}{3!} \frac{C_{10m}^{(1)}}{10m} \in \sum_{\substack{p \equiv 1 \pmod{5} \\ 10m = a(p-1)}} \frac{(3!a)_p^{-1} \pmod{p^{1+\text{ord}_p a}}}{p^{1+\text{ord}_p a}} A_p^a + \mathbb{Z} \left[\frac{1}{2} \right]. \quad (10.7)$$

10.2. Сравнение между $x(u)^{k/2}$ и $x(u)^{(k+1)/2}$. В этом пункте мы предполагаем, что $k = 1, 2$ или 3 . Для кривой $y^2 = x^5 - 1$ и для

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

положим

$$\frac{1}{t^j} = x(u) = \frac{1}{u^j} + \sum_{m=1}^{\infty} \frac{C_{10m}^{(j)}}{(10m)_j} \frac{u^{10m-j}}{(10m-j)!} \quad (C_0^{(j)} = 1) \quad (10.8)$$

при $j = 1, 2, 3, 4$. Тогда

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

С другой стороны, продифференцировав (10.1) по u и разделив на t^{k+1} , получаем

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

Следовательно,

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

Приравнивая это к (10.9) и используя (10.6), видим, что

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

Так как $C_0^{(k)} = 1$, можно опустить члены отрицательной степени и получить

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

Правая часть этого равенства принадлежит $\mathbb{Z} \left[\frac{1}{2} \right] \langle\langle u \rangle\rangle$ в силу леммы 1.4, предложения 8.2, (3) и включения (8.6). Добавив это к (10.3), видим, что

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

На этом этапе, так как $C_{10m}/(10m) = C_{10m}^{(2)}/(10m)_2$ по определению, из (10.11) при $k = 1$ получаем

$$\frac{C_{10m}}{10m} \in -\frac{C_{10m}^{(1)}}{10m} + 3! \mathbb{Z} \left[\frac{1}{2} \right]. \quad (10.12)$$

Заметим, что (10.12) и (10.7) позволяют завершить доказательство теоремы Кларка для C_{10m} над $\mathbb{Z} \left[\frac{1}{2} \right]$. Однако чтобы доказать теорему Кларка над $\mathbb{Z}$, нам нужно пойти довольно длинным путем, описанным в п. 9.1.

10.3. Теорема Кларка для $x(u)^2$ над $\mathbb{Z} \left[\frac{1}{2} \right]$. Подведем итог результатов этого раздела. Результаты (10.11) при $k = 1, 2, 3$ показывают, что

$$\frac{C_{10m}^{(1)}}{10m} + 3! \frac{C_{10m}^{(4)}}{(10m)_4} \in 3! \mathbb{Z} \left[\frac{1}{2} \right]. \quad (10.13)$$

Таким образом,

$$\frac{1}{3!} \frac{C_{10m}^{(1)}}{10m} + \frac{C_{10m}^{(4)}}{(10m)_4} \in \mathbb{Z} \left[\frac{1}{2} \right]. \quad (10.14)$$

Это включение и (10.7) дают, что

$$\frac{C_{10m}^{(4)}}{(10m)_4} \in - \sum_{\substack{p \equiv 1 \pmod{5} \\ 10m = a(p-1)}} \frac{(3!a)_p^{-1} \pmod{p^{1+\text{ord}_p a}}}{p^{1+\text{ord}_p a}} A_p^a + \mathbb{Z} \left[\frac{1}{2} \right]. \quad (10.15)$$

В частности, видим, что

$$\frac{C_{10m}^{(4)}}{(10m)_4} \in \mathbb{Z}_{(5)}. \quad (10.16)$$

11. Теорема Кларка для $y(\mathbf{u})$ над $\mathbb{Z}\left[\frac{1}{5}\right]$

В этом разделе мы также работаем только с кривой $y^2 = x^5 - 1$.

11.1. Теорема Кларка для $y(\mathbf{u})^{1/5}$. Аналогично разделу 10 рассмотрим формальный обратный ряд ряда $u \mapsto y(\mathbf{u})^{1/5}$. Пусть

$$y(\mathbf{u}) = -\frac{1}{s^5}.$$

Тогда

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

Для удобства ссылок перепишем это:

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

Обозначим каждый коэффициент Карлица этого ряда через

$$f_{10m} = \binom{-\frac{3}{5}}{m}. \quad (11.2)$$

В силу леммы 1.4 и равенства (1.6) видим, что

$$f_{10m} \in \mathbb{Z}\left[\frac{1}{5}\right]. \quad (11.3)$$

Остальные коэффициенты f_n равны 0. Здесь мы рассматриваем каждый коэффициент как специализацию коэффициента f_j из п. 2.1. Тогда деленное универсальное число Бернулли $\widehat{B}_{10m}/(10m)$ специализируется в $D_{10m}^{(1)}/(10m)$. Мы утверждаем, что

$$\frac{D_{10m}^{(1)}}{10m} \in 4! \mathbb{Z}\left[\frac{1}{5}\right]. \quad (11.4)$$

Чтобы это доказать, применим предложение 3.11 при $p = 2$ и $p = 3$. В этом случае, так как $f_{2-1} = 0$ и $f_{3-1} = 0$, можно рассматривать только те разбиения U , в которых $U_{2-1} = U_{3-1} = 0$. Если $m = 1$, то число $D_{10}^{(1)}/10 = (3/5)(9!/11) = 2^7 \cdot 3^5 \cdot 7/11$ делится на $4!$. Если $m \geq 2$, то в силу

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

имеем

$$\text{ord}_2(\tau_U) \geq \left\lfloor \frac{20+1-2}{4} \right\rfloor = 4, \quad \text{ord}_3(\tau_U) \geq \left\lfloor \frac{20+1-2}{6} \right\rfloor = 3.$$

Благодаря выражению в предложении 2.8 отсюда следует, что все коэффициенты $D_{10m}^{(1)}/(10m)$ делятся на $4!$. Это и (11.3) дают (11.4).

Если $p = 10m+1$ – простое число, то коэффициент f_{p-1} совпадает с $(2, 2)$ -элементом матрицы Хассе–Витта относительно естественного базиса дифференциальных форм первого рода на C редукции по модулю p :

$$f_{p-1} = - \left(\begin{matrix} -3/5 \\ (p-1)/10 \end{matrix} \right) \equiv A_p \pmod{p}. \quad (11.5)$$

См. также п. 18.1.

В условиях рассмотрения выше, применяя теорему Кларка 2.9 к разложению Лорана функции $u \mapsto -y(u)^{1/5}$ в точке $u = 0$, а именно, к

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

получаем

$$\frac{1}{4!} \frac{D_{10m}^{(1)}}{10m} \in - \sum_{\substack{p \equiv 1 \pmod{5} \\ 10m = a(p-1)}} \frac{(4!a)_p^{-1} \pmod{p^{1+\text{ord}_p a}}}{p^{1+\text{ord}_p a}} A_p^a + \mathbb{Z} \left[\frac{1}{5} \right]. \quad (11.7)$$

11.2. Сравнение между $y(u)^{k/5}$ и $y(u)^{(k+1)/5}$. В этом пункте мы предполагаем, что $k = 1, 2, 3$ или 4 . Мы доказываем здесь сравнение между коэффициентами Гурвица функций $y(u)^{(k+1)/5}$ и $y(u)^{k/5}$ для $y^2 = x^5 - 1$. Для

$$s = \frac{-1}{y(u)^{1/5}} \quad (= u + \dots)$$

положим

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

при $j = 1, 2, 3, 4, 5$. Тогда

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

С другой стороны, продифференцировав (11.1) по u и разделив на s^{k+1} , получаем

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

Следовательно,

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

Приравнявая это к (11.9) и используя (11.6), видим, что

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

Так как $D_0^{(1)} = 1$, то можно опустить члены отрицательной степени и получить

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

Правая часть принадлежит $\mathbb{Z}\left[\frac{1}{5}\right]\langle\langle u \rangle\rangle$ в силу предложения 8.2, (3) и включения (8.12). Добавляя это к (11.3), заключаем, что

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

11.3. Теорема Кларка для $y(\mathbf{u})$ над $\mathbb{Z}\left[\frac{1}{5}\right]$. Результат (11.11) при $k = 1, 2, 3, 4$ состоит в том, что

$$\begin{aligned} & \frac{D_{10m}^{(4)}}{(10m)_4} + 4 \frac{D_{10m}^{(5)}}{(10m)_5} \in 4! \mathbb{Z}\left[\frac{1}{5}\right], \\ & \frac{D_{10m}^{(3)}}{(10m)_3} + 3 \frac{D_{10m}^{(4)}}{(10m)_4} \in 4! \mathbb{Z}\left[\frac{1}{5}\right], \\ & \frac{D_{10m}^{(2)}}{(10m)_2} + 2 \frac{D_{10m}^{(3)}}{(10m)_3} \in 4! \mathbb{Z}\left[\frac{1}{5}\right], \\ & \frac{D_{10m}^{(1)}}{10m} + \frac{D_{10m}^{(2)}}{(10m)_2} \in 4! \mathbb{Z}\left[\frac{1}{5}\right]. \end{aligned}$$

Суммируя эти включения, получаем

$$\frac{D_{10m}^{(1)}}{10m} - 4! \frac{D_{10m}^{(5)}}{(10m)_5} \in 4! \mathbb{Z}\left[\frac{1}{5}\right]. \quad (11.12)$$

Отсюда следует, что

$$\frac{1}{4!} \frac{D_{10m}^{(1)}}{10m} - \frac{D_{10m}^{(5)}}{(10m)_5} \in \mathbb{Z}\left[\frac{1}{5}\right].$$

Так как $y(\mathbf{u}) = -1/s(\mathbf{u})^5$, видим, что

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

Это равенство и (11.7) доказывают результат, который и был целью этого раздела, а именно,

$$\frac{D_{10m}}{10m} \in - \sum_{\substack{p \equiv 1 \pmod{5} \\ 10m = a(p-1)}} \frac{(4!a|_p)^{-1} \bmod p^{1+\text{ord}_p a}}{p^{1+\text{ord}_p a}} A_p^a + \mathbb{Z} \left[\frac{1}{5} \right]. \quad (11.14)$$

12. Теорема Кларка для $x(u)$ и $y(u)$ над $\mathbb{Z}$

В этом разделе мы все еще имеем дело только с кривой $y^2 = x^5 - 1$.

12.1. Сравнение между $y(u)$ и $x^2(u)$. Пусть

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

Если $D = \frac{d}{du} = \frac{2y}{x} \frac{d}{dx}$, то

$$D(x^2) = 2x D x = 2x \frac{2y}{x} = 4y. \quad (12.2)$$

Следовательно,

$$\frac{C_{10m}^{(4)}}{(10m)_4} = 4 \frac{D_{10m}}{10m}. \quad (12.3)$$

Поэтому (10.15) и (11.14) доказывают, что знаменатель числа $C_{10m}^{(4)}/(10m)_4$ не содержит никакой степени 2 и что $C_{10m}^{(4)}/(10m)_4$ обладает тем свойством, что

$$\frac{C_{10m}^{(4)}}{(10m)_4} \in - \sum_{\substack{p \equiv 1 \pmod{5} \\ 10m = a(p-1)}} \frac{(3!a|_p)^{-1} \bmod p^{1+\text{ord}_p a}}{p^{1+\text{ord}_p a}} A_p^a + \mathbb{Z}. \quad (12.4)$$

При этом, так как $\frac{1}{4} \frac{C_{10m}^{(4)}}{(10m)_4} = \frac{D_{10m}}{10m}$ в силу (12.3), видим, что

$$\frac{D_{10m}}{10m} \in \mathbb{Z} \left[\frac{1}{5}, \frac{1}{p}; p \equiv 1 \pmod{5}, (p-1) \mid 10m \right] \subset \mathbb{Z}_{(2)}$$

и что знаменатель числа $D_{10m}/(10m)$ не содержит никакой степени 2. Таким образом, числитель числа $C_{10m}^{(4)}/(10m)_4$ делится на 4. Это рассуждение и (11.14) приводят к

$$\frac{D_{10m}}{10m} \in - \sum_{\substack{p \equiv 1 \pmod{5} \\ 10m = a(p-1)}} \frac{(4!a|_p)^{-1} \bmod p^{1+\text{ord}_p a}}{p^{1+\text{ord}_p a}} A_p^a + \mathbb{Z}. \quad (12.5)$$

Это вторая формула в теореме 6.1.

12.2. От $x^2(u)$ к $x(u)$. Наконец, используем тот факт, что

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

Применяя оператор D к дифференциальному уравнению (5.5), получаем

$$D^2 \left(\frac{1}{x} \right) = 3 \frac{1}{x} \left(D \frac{1}{x} \right)^2 - 10. \quad (12.7)$$

Поэтому $1/x(u) \in \mathbb{Z}\langle\langle u \rangle\rangle$ в силу предложения 8.2, (1), и, кроме того, $1/x^3 \in \mathbb{Z}\langle\langle u \rangle\rangle$. Эти факты были доказаны также предложением 8.3 и утверждением (3) предложения 8.2. Итак, мы видим, что

$$\frac{C_{10m}}{10m} = 6 \frac{C_{10m}^{(4)}}{(10m)_4} + (\text{целое число}). \quad (12.8)$$

В силу (12.4) заключаем, что

$$\begin{aligned} \frac{C_{10m}}{10m} &= 3! \frac{C_{10m}^{(4)}}{(10m)_4} + (\text{целое число}) \\ &= G_{10m} - \sum_{\substack{p \equiv 1 \pmod{5} \\ 10m = a(p-1)}} \frac{a|p|^{-1} \bmod p^{1+\text{ord}_p a}}{p^{1+\text{ord}_p a}} A_p^a \end{aligned} \quad (12.9)$$

с подходящим $G_{10m} \in \mathbb{Z}$. Это есть искомая первая формула в теореме 6.1.

13. Доказательство сравнений типа Куммера

13.1. Теорема Хонды и формальные группы. Теперь мы начинаем доказывать теорему 7.1 (и теорему 7.5). Покажем, что существует формальная группа над $\mathbb{Z}$, формальный логарифм которой есть (10.1) (или (11.1)).

ПРЕДЛОЖЕНИЕ 13.1. *Предположим, что p – фиксированное простое число. Пусть t – неизвестная, и пусть $u(t) \in \mathbb{Q}_p[[t]]$. Если существует $\beta \in \mathbb{Z}_p$ такое, что*

$$pu(t) - \beta u(t^p) \in p\mathbb{Z}_p[[t]], \quad (13.2)$$

то формальный групповой закон F , заданный по правилу

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

определен над $\mathbb{Z}_p$ (т.е. $\in \mathbb{Z}_p[[t_1, t_2]]$). Здесь $u^{-1}(t) \in \mathbb{Q}_p[[t]]$ означает единственный степенной ряд такой, что $u^{-1}(u(t)) = t$. В частности, если $\alpha \in \mathbb{Z}_p$, то

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

Это получается путем применения теоремы Хонды [28; с. 223, теорема 2] при $n = 1$, $q = p$, $P = 1$, $u = p - \beta T$, $f = u(t)$. Эту теорему можно применить

к $t \mapsto u = u_g$ из (10.1) и $s \mapsto u$ из (11.1). Чтобы это сделать, введем p -адическую Γ -функцию

$$\Gamma_p: \mathbb{Z}_p \rightarrow \mathbb{Z}_p^\times. \quad (13.5)$$

Эта функция удовлетворяет равенству

$$\Gamma_p(n) = (-1)^n \prod_{1 \leq j < n, p \nmid j} j \quad (13.6)$$

для любого натурального числа n . Важнейшими ее свойствами являются равенства

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

и то, что для любого натурального числа ν справедлива импликация

$$z \equiv w \pmod{p^\nu \mathbb{Z}_p} \Rightarrow \Gamma_p(z) \equiv \Gamma_p(w) \pmod{p^\nu \mathbb{Z}_p}. \quad (13.8)$$

Подробнее см. [32] или [29].

Обозначая через $u(t)$ разложение в степенной ряд функции

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

относительно $t = -x^{-1/2}$, мы утверждаем следующее.

ЛЕММА 13.9. *Для кривой $y^2 = x^{2g+1} - 1$ (соответственно $y^2 = x^{2g+1} - x$) и простого числа $p \equiv 1 \pmod{2g+1}$ (соответственно $p \equiv 1 \pmod{4g}$) пусть*

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

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

Тогда ряд $u(t)$ удовлетворяет включению

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

Этому включению также удовлетворяет разложение в степенной ряд функции $s = -y^{-1/(2g+1)}$ относительно u .

ДОКАЗАТЕЛЬСТВО. Для простоты мы доказываем это утверждение только для кривой $y^2 = x^5 - 1$ ($g = 2$). Пусть $f_{10n}/(10n+1) = [t^{10n+1}]u(t)$. Тогда, как сформулировано в (10.2), имеем $f_{10n} = (-1)^n \binom{-1/2}{n}$. Нам достаточно доказать, что если $p(10m+1) = 10n+1$, то

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

Заметим, что $\left\lfloor \frac{n}{p} \right\rfloor = \left\lfloor m + \frac{1}{10} - \frac{1}{10p} \right\rfloor = m$. Это равенство и неравенства

$$p \left(2 \left\lfloor \frac{n}{p} \right\rfloor - 1 \right) \leq 2n - 1 \leq p \cdot 2 \left\lfloor \frac{n}{p} \right\rfloor \leq p \left(2 \left(\left\lfloor \frac{n}{p} \right\rfloor + 1 \right) - 1 \right)$$

показывают, что наибольшее нечетное целое число, делящееся на p и не превосходящее $2n - 1$, есть $p(2m - 1)$. Следовательно,

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

Множественно используя (13.7), получаем, что последнее выражение равно

$$\begin{aligned} &\frac{(-1)^{m+\frac{p-1}{10}}}{10m+1} \left\{ \frac{(-1)^n \Gamma_p\left(-\frac{1}{2}+1\right) p^m \prod_{k=1}^m \left(-\frac{2k-1}{2}\right)}{\Gamma_p\left(-\frac{2n-1}{2}\right) (-1)^{n+1} \Gamma_p(n+1) p^m m!} - (-1)^{\frac{p-1}{10}} \beta_p \frac{\prod_{j=1}^m \left(-\frac{2j-1}{2}\right)}{m!} \right\} \\ &= \frac{(-1)^{m+\frac{p-1}{10}}}{10m+1} \left\{ -\frac{\Gamma_p\left(\frac{1}{2}\right)}{\Gamma_p(n+1) \Gamma_p\left(-n+\frac{1}{2}\right)} \frac{\prod_{k=1}^m \left(-\frac{2k-1}{2}\right)}{m!} \right. \\ &\quad \left. + \frac{\Gamma_p\left(\frac{1}{2}\right)}{\Gamma_p\left(\frac{9}{10}\right) \Gamma_p\left(\frac{6}{10}\right)} \frac{\prod_{j=1}^m \left(-\frac{2j-1}{2}\right)}{m!} \right\} \\ &= \frac{(-1)^{m+\frac{p-1}{10}}}{10m+1} \binom{-\frac{1}{2}}{m} \left\{ -\frac{\Gamma_p\left(\frac{1}{2}\right)}{\Gamma_p\left(\frac{1}{10}p(10m+1) + \frac{9}{10}\right) \Gamma_p\left(-\frac{1}{10}p(10m+1) + \frac{6}{10}\right)} \right. \\ &\quad \left. + \frac{\Gamma_p\left(\frac{1}{2}\right)}{\Gamma_p\left(\frac{9}{10}\right) \Gamma_p\left(\frac{6}{10}\right)} \right\}. \end{aligned}$$

Пусть ν – целое число такое, что $\text{ord}_p(10m+1) = \nu$. Тогда (13.7) и (13.8) показывают, что

$$\frac{\Gamma_p\left(\frac{1}{2}\right)}{\Gamma_p\left(\frac{1}{10}p(10m+1) + \frac{9}{10}\right) \Gamma_p\left(-\frac{1}{10}p(10m+1) + \frac{6}{10}\right)} \equiv \frac{\Gamma_p\left(\frac{1}{2}\right)}{\Gamma_p\left(\frac{9}{10}\right) \Gamma_p\left(\frac{6}{10}\right)} \pmod{p^{\nu+1}\mathbb{Z}_p}.$$

Лемма 1.5 показывает, что

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

Поэтому

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

и доказательство завершено.

ЗАМЕЧАНИЕ 13.11. (1) Рассматривая отображение $\iota: \mathcal{C} \rightarrow J$ как определенное над $\mathbb{Z}_p$, обозначим его формальное пополнение в бесконечно удаленной точке по правилу

$$\infty \mapsto (\text{начало координат в } J)$$

через $\hat{\iota}: \hat{\mathcal{C}} \rightarrow \hat{J}$. В силу действия (5.6) (соответственно (5.8)) $\hat{J}$ разлагается в произведение 1-мерных формальных групп. Композиция $\hat{\pi} \circ \hat{\iota}: \hat{\mathcal{C}} \rightarrow G$ отображения $\hat{\iota}$ с проекцией $\pi: \hat{J} \rightarrow G$, где G – какой-то фактор произведения, была бы изоморфизмом формальных групп.

(2) Высота формальной группы F над $\mathbb{Z}_p$, связанной с вышеупомянутой функцией $u(t)$, равна 1, а именно, существует $b \in \mathbb{Z}_p^\times$ такое, что $u^{-1}(pu(t)) \equiv bt^p \pmod{p\mathbb{Z}_p[[t]]}$. Этот факт следует из равенства

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

и включения $f_{p-1} \in \mathbb{Z}_p^\times$, которое в свою очередь вытекает из сравнения (10.5). Тот же самый факт имеет место для формальной группы, связанной с разложением в ряд функции $s \mapsto u$.

13.2. Формула Хохшильда и теорема Хонды. Напомним следующий результат, называемый формулой Хохшильда, – он потребуется нам для доказательства предложения 13.13 ниже. Пусть R – коммутативное кольцо. Дифференцирование D кольца R – это отображение кольца R в себя такое, что

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

для $a, b \in R$.

ПРЕДЛОЖЕНИЕ 13.12. Пусть p – простое число, пусть R – коммутативное кольцо и D – дифференцирование кольца R . Пусть M – $(\mathbb{Z})$ -подмодуль в R такой, что DM лежит в подкольце A , в котором pA – первичный идеал. Таким образом, A/pA является $\mathbb{F}_p$ -алгеброй. Тогда для $b \in A$ выполняется сравнение

$$(bD)^p \equiv b^p D^p + ((bD)^{p-1}(b)) \cdot D \pmod{pA}$$

для операторов из M в A/pA .

ДОКАЗАТЕЛЬСТВО. Это небольшая модификация теоремы 25.5 в [33; с. 197] и доказательство точно такое же. Поэтому мы его опускаем.

В то время как следующее общее равенство доказывается с использованием вышеприведенной формулы, довольно слабая его версия для случая $g = 1$ описывается в [12] по-другому.

ПРЕДЛОЖЕНИЕ 13.13. Для кривой $y^2 = x^{2g+1} - 1$ (соответственно $y^2 = x^{2g+1} - x$) пусть $t = t(u)$ и $s = s(u)$ – степенные ряды соответственно из предложений 8.3 и 8.7. Пусть $p \equiv 1 \pmod{(2g+1)}$ (соответственно $\pmod{4g}$) – простое число. Если $\varphi \in \mathbb{Z}_{(p)}[[t]]$ или $\varphi \in \mathbb{Z}_{(p)}[[s]]$, то

$$\left(\left(\frac{d}{du} \right)^p - A_p \frac{d}{du} \right) \varphi \in p\mathbb{Z}_{(p)}[[t]] \quad \text{или} \quad \in p\mathbb{Z}_{(p)}[[s]].$$

ДОКАЗАТЕЛЬСТВО. Применим предложение 13.12, полагая

$$R = \mathbb{Q}[[t]], \quad M = \left(\int_0^t u(t) dt \right) \cdot \mathbb{Z}_{(p)}, \quad A = \mathbb{Z}_{(p)}[[t]], \quad D = \frac{d}{dt}.$$

Тогда $A/pA = \mathbf{F}_p[[t]]$. Далее в этом доказательстве символ “=” означает равенство в $\mathbf{F}_p[[t]]$. Прежде всего обратим внимание на тот факт, что

$$\frac{du}{dt} = 1 + \sum_{n=1}^{\infty} (-1)^n \binom{-\frac{1}{2}}{n} t^{(2g+2)n} \in 1 + t\mathbb{Z}\left[\frac{1}{2}\right] [[t]], \quad \frac{dt}{du} \in 1 + t\mathbb{Z}\left[\frac{1}{2}\right] [[t]], \quad (13.14)$$

как следует из (10.1) и (10.3). В силу предложения 13.12 при $b := \frac{dt}{du}$ и $D = \frac{d}{dt}$ имеем

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

Следовательно,

$$\frac{d^p t}{du^p} = - \left(\frac{du}{dt} \right)^{-p-1} \frac{d^p u}{dt^p}. \quad (13.15)$$

Снова используя предложение 13.12 для φ , D и b , получаем

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

Здесь мы воспользовались предположением $\varphi \in \mathbb{Z}_p[[t]]$. Подставляя (13.15) в последнюю формулу, получим

$$\left(\frac{d}{du} \right)^p \varphi = - \left(\frac{du}{dt} \right)^{-p} \frac{d^p u}{dt^p} \cdot \frac{d}{du} \varphi. \quad (13.16)$$

Так как $\left(\frac{d}{dt} \right)^p \mathbb{Z}_{(p)}[[t]] \in p\mathbb{Z}_{(p)}[[t]]$, то, применяя $\left(\frac{d}{dt} \right)^p$ к (13.10), получаем

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

Из свойств (13.6) и (13.8) следует, что

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

Таким образом, $\frac{d^p u}{dt^p} = -A_p \left(\frac{du}{dt}\right)^p$. Подстановка этого в (13.16) показывает, что $\left(\frac{d}{du}\right)^p \varphi = A_p \frac{d}{du} \varphi$, как и требовалось. Утверждение для $s = s(u)$ доказывается аналогично.

13.3. Доказательство сравнений. Инструменты, необходимые нам для доказательства теоремы 7.1 (и теоремы 7.5), полностью подготовлены. Здесь мы приводим доказательство для кривой $y^2 = x^5 - 1$. Во избежание недоразумений, если мы рассматриваем

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

как элемент из $\mathbb{Q}_p[[u]]$, то мы обозначаем это через

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

Пусть $\xi \in \mathbb{Z}_p$ — примитивный корень $(p-1)$ -й степени из 1. Тогда, так как

$$x\langle u \rangle - \xi^2 x\langle \xi u \rangle = \sum_{\substack{n=1 \\ (p-1) \nmid 10n}}^{\infty} \frac{(1 - \xi^{10n}) C_{10n}}{10n} \frac{u^{10n-2}}{(10n-2)!}, \quad (13.17)$$

достаточно доказать, что для любого натурального числа a и для $D = d/du$

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

Действительно, если выполнено неравенство $10n \geq a + 2$ и $(p-1) \nmid 10n$, то коэффициент при $u^{10n-a-2}/(10n-a-2)!$ равен

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

и $1 - \xi^{10n} \notin p\mathbb{Z}_p$. Благодаря предложению 13.13 для доказательства (13.18) достаточно доказать, что

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

Если мы положим

$$\begin{aligned} F_\xi(t) &= u^{-1}(\xi u(t)) \quad (u^{-1} - \text{формальный обратный ряд ряда } t \mapsto u) \\ &= t(\xi u(t)), \end{aligned} \quad (13.20)$$

то предложение 13.1 и лемма 13.9 дают, что

$$x\langle u(t) \rangle - \xi^2 x\langle \xi u(t) \rangle = \frac{1}{t^2} - \frac{\xi^2}{t(\xi u(t))^2} = \frac{1}{t^2} - \frac{\xi^2}{(\xi t + \dots)^2} \in \mathbb{Z}_p[[t]],$$

потому что $F_\xi(t) \in \xi t + t^2 \mathbb{Z}_p[[t]]$. Отсюда следует доказательство теоремы 7.1.

14. Другие сравнения

В этом разделе мы не ограничиваемся кривой $y^2 = x^5 - 1$ и описываем гиперэллиптические кривые, заданные любым из уравнений

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

14.1. Обобщенные числа Бернулли–Гурвица высшего порядка.

Как обычно, пусть $t = -1/x(\mathbf{u})^{1/2}$ и $s = -1/y(\mathbf{u})^{1/5}$. Докажем сравнение Куммера для коэффициентов Гурвица функции $t^{-\nu}$ ($1 \leq \nu \leq 4g+2$), обобщающее сравнение для $t^{-2} = x(\mathbf{u})$, доказанное в разделе 13.

Случай $y(\mathbf{u})^2 = x(\mathbf{u})^{2g+1} - 1$. Для кривой $y^2 = x^{2g+1} - 1$ напомним определение чисел $C_{(4g+2)n}^{(\nu)}$ (см. раздел 10) и $D_{(4g+2)n}^{(\nu)}$ (см. раздел 11): для $\nu = 1, 2, \dots$ мы полагаем

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

Конечно, если $(4g+2) \nmid n$, то полагаем $C_n^{(\nu)} = D_n^{(\nu)} = 0$.

Пусть $p \equiv 1 \pmod{4g+2}$ – простое число, а $\xi \in \mathbb{Z}_p$ – примитивный корень $(p-1)$ -й степени из 1. Используя вместо (13.17) равенство

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

получаем следующее утверждение.

ТЕОРЕМА 14.3. Пусть $p \equiv 1 \pmod{2g+1}$ – простое число, a – натуральное число. Пусть ν – целое число такое, что $1 \leq \nu \leq 4g+2$. Предположим, что $(4g+2)n \geq a + \nu$ и $(p-1) \nmid (4g+2)n$. Тогда

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

Случай $y(u)^2 = x(u)^{2g+1} - x(u)$. Для кривой $y^2 = x^{2g+1} - x$ и для $\nu = 1, 2, \dots$ определим $C_{4gn}^{(\nu)}$ и $D_{4gn}^{(\nu)}$ из равенств

$$\frac{1}{t^\nu} = \frac{1}{u^\nu} + \sum_{n=1}^{\infty} \frac{C_{4gn}^{(\nu)}}{(4gn)_\nu} \frac{u^{4gn-\nu}}{(4gn-\nu)!}, \quad \frac{1}{s^\nu} = \frac{1}{u^\nu} + \sum_{n=1}^{\infty} \frac{D_{4gn}^{(\nu)}}{(4gn)_\nu} \frac{u^{4gn-\nu}}{(4gn-\nu)!}. \quad (14.4)$$

Положим также, что если $(4g+2) \nmid n$, то $C_n^{(\nu)} = D_n^{(\nu)} = 0$.

Пусть $p \equiv 1 \pmod{4g}$ – простое число, а $\xi \in \mathbb{Z}_p$ – примитивный корень $(p-1)$ -й степени из 1. Используя вместо (13.17) равенство

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

получаем следующее утверждение.

ТЕОРЕМА 14.6. Пусть $p \equiv 1 \pmod{4g}$ – простое число, a – натуральное число. Пусть ν – целое число такое, что $1 \leq \nu \leq 4g+2$. Предположим, что $4gn = a + \nu$ и $(p-1) \nmid 4gn$. Тогда

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

14.2. Коэффициенты Гурвица функций $t(u_g)$ и $s(u_g)$. Теперь рассмотрим коэффициенты Гурвица $c_m^{(h)}$, $d_m^{(h)}$ степеней $t = t(u)$ в предложении 8.3 и $s = s(t)$ в предложении 8.7, а именно, коэффициенты Гурвица рядов

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

Здесь, очевидно, $c_h^{(h)} = d_h^{(h)} = 1$. Результаты таковы.

ЛЕММА 14.8. Если $\nu > 0$ и $m \geq a+1$, то

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

ДОКАЗАТЕЛЬСТВО. В силу предложения 8.2 (утверждения (2), (3)) и предложения 8.3 имеем

$$\mathbb{Z}_p \langle\langle u \rangle\rangle = \mathbb{Z}_p \langle\langle t \rangle\rangle. \quad (14.10)$$

Для $D = d/du$ и любого целого числа $h \geq 1$ покажем по индукции, что

$$(D^p - A_p D) \left(\frac{t^h}{h!} \right) \in b + p\mathbb{Z}_p \langle\langle u \rangle\rangle \quad (b \in \mathbb{Z}_p). \quad (14.11)$$

Если $h = 1$, то это включение проверяется с помощью предложения 13.13 и равенства (14.10). Так как

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

то, используя предположение индукции, равенство (13.15) и предложение 13.13, видим, что это принадлежит $p\mathbb{Z}_p \langle\langle u \rangle\rangle$. Следовательно,

$$(D^p - A_p D) \left(\frac{t^{h+1}}{(h+1)!} \right) \in b + p\mathbb{Z}_p \langle\langle u \rangle\rangle \quad (b \in \mathbb{Z}_p).$$

Таким образом, мы доказали (14.11). Многократно используя (14.11), получаем, что при $a > 0$

$$(D^p - A_p D)^a \left(\frac{t^h}{h!} \right) \in b + p^a \mathbb{Z}_p \langle\langle u \rangle\rangle \quad (b \in \mathbb{Z}_p). \quad (14.12)$$

В силу

$$(D^p - A_p D)^a \left(\frac{t^h}{h!} \right) = \sum_{m=h}^{\infty} \left\{ \sum_{r=0}^a \binom{a}{r} (-A_p)^{a-r} c_{m+r(p-1)}^{(h)} \right\} D^a \frac{u^m}{m!},$$

получаем первую формулу леммы. Вторая доказывается аналогично.

14.3. Обобщение сравнения Вандивера–Карлица. В этом пункте мы докажем сравнение типа Вандивера–Карлица. Г.Ш. Вандивер [17] доказал такое сравнение для чисел Бернулли, а Л. Карлиц [8] исследовал его для чисел Гурвица.

ПРЕДЛОЖЕНИЕ 14.13. Пусть $a > 0$ и $\nu > 0$ – целые числа. Пусть $n = a + 1$. Для чисел $\{C_n^{(\nu)}\}$ и $\{D_n^{(\nu)}\}$, определенных в (14.1) или (14.4), имеем

$$\begin{aligned} \sum_{r=0}^a \binom{a}{r} (-A_p)^{a-r} C_{n+r(p-1)}^{(\nu)} &\equiv 0 \pmod{p^{a-\nu}}, \\ \sum_{r=0}^a \binom{a}{r} (-A_p)^{a-r} D_{n+r(p-1)}^{(\nu)} &\equiv 0 \pmod{p^{a-\nu}}. \end{aligned}$$

ЗАМЕЧАНИЕ 14.14. В отличие от теорем 7.1, 7.5, 14.3, 14.6 эти сравнения не требуют условия $(p-1) \nmid n$. Однако, так как предложение 14.13 можно

доказать без использования (13.10) и предложения 13.1, это были бы не такие уж глубокие результаты.

ДОКАЗАТЕЛЬСТВО. Как и в п. 10.1, положим $[t^{n+1}/(n+1)]u(t) = f_n$. Здесь мы все еще используем обозначения $u = u_g$, $D = d/du$. Так как

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

имеем

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

Поэтому

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

Если $m \geq a+1$, то внутренняя сумма делится на p^a в силу леммы 14.8. Если $\text{ord}_p(h+1) = w$ ($w \geq 1$), то $p^w - 1 \leq h$ и $\text{ord}_p((p^w - 1)!) \leq \text{ord}_p(h!)$. В силу (1.2) видим, что

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

В нашей ситуации можно считать, что $p \leq 3$. Отсюда следует, что последнее выражение не меньше w , если $w \geq 2$. Наихудшим является случай, когда $w = 1$, так что

$$w \leq \text{ord}_p(h!) + 1 \quad (w \geq 1). \quad (14.16)$$

Поэтому

$$\sum_{r=0}^a \binom{a}{r} (-A_p)^{a-r} C_{m+r(p-1)}^{(1)} \in p^{a-1} \mathbb{Z}_{(p)} \quad (m \geq a+1). \quad (14.17)$$

Это в точности случай $\nu = 1$ первой формулы в предложении 14.13. Общий случай доказывается аналогично следующим образом. Так как $u = \sum_{h=0}^{\infty} f_h \frac{t^{h+1}}{h+1}$, видим, что

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

Отсюда следует, что

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

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

и

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

Это разложение дает, что

$$c_m^{(\nu)} = \sum_{h=0}^m h! \sum_{h_1+\dots+h_\nu=h} \frac{f_{h_1}}{h_1+1} \cdots \frac{f_{h_\nu}}{h_\nu+1} c_m^{(h)} \quad (14.18)$$

и

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

Если предположить, что $\text{ord}_p(h_j+1) = w_j$, то так же, как в (14.16), заключаем, что

$$w_1 + \dots + w_\nu \leq \text{ord}_p(h_1! h_2! \cdots h_\nu!) + \nu \leq \text{ord}_p(h!) + \nu,$$

так как $w_j \leq \text{ord}_p(h_j!) + 1$. Это показывает, что правая часть равенства (14.19) делится на $p^{a-\nu}$. Таким образом, доказано первое сравнение в предложении 14.13. Второе доказывается аналогично.

15. Численные примеры для классических чисел

15.1. Числа Бернулли. Несколько первых значений $C_{2n} = (-1)^{n-1} \cdot 2^{2n} \times B_{2n}$ (где $B_{2n} - 2n$ -е число Бернулли) для кривой $y^2 = x - 1$ ($g = 0$) таковы:

$$\begin{aligned}
2^2 B_2 &= \frac{1}{3} \cdot 2, & -2^4 B_4 &= \frac{1}{3 \cdot 5} \cdot 2^3, & 2^6 B_6 &= \frac{1}{3 \cdot 7} \cdot 2^5, \\
-2^8 B_8 &= \frac{1}{3 \cdot 5} \cdot 2^7, & 2^{10} B_{10} &= \frac{1}{3 \cdot 11} \cdot 2^9 \cdot 5, \\
-2^{12} B_{12} &= \frac{1}{3 \cdot 5 \cdot 7 \cdot 13} \cdot 2^{11} \cdot 691, & 2^{14} B_{14} &= \frac{1}{3} \cdot 2^{15} \cdot 7, \\
-2^{16} B_{16} &= \frac{1}{3 \cdot 5 \cdot 17} \cdot 2^{15} \cdot 3617, & 2^{18} B_{18} &= \frac{1}{3 \cdot 5 \cdot 19} \cdot 2^{17} \cdot 43867, \\
-2^{20} B_{20} &= \frac{1}{3 \cdot 5 \cdot 11} \cdot 2^{19} \cdot 283 \cdot 617, \\
2^{22} B_{22} &= \frac{1}{3 \cdot 23} \cdot 2^{21} \cdot 11 \cdot 131 \cdot 593, \\
-2^{24} B_{24} &= \frac{1}{3 \cdot 5 \cdot 7 \cdot 13} \cdot 2^{23} \cdot 103 \cdot 2294797, \\
2^{26} B_{26} &= \frac{1}{3} \cdot 2^{25} \cdot 13 \cdot 657931,
\end{aligned}$$

$$\begin{aligned}
-2^{28} B_{28} &= \frac{1}{3 \cdot 5 \cdot 29} \cdot 2^{27} \cdot 7 \cdot 9349 \cdot 362903, \\
2^{30} B_{30} &= \frac{1}{3 \cdot 7 \cdot 11 \cdot 31} \cdot 2^{29} \cdot 5 \cdot 1721 \cdot 1001259881, \\
-2^{32} B_{32} &= \frac{1}{3 \cdot 5 \cdot 17} \cdot 2^{31} \cdot 37 \cdot 683 \cdot 305065927, \\
2^{34} B_{34} &= \frac{1}{3} \cdot 2^{33} \cdot 2^{33} \cdot 17 \cdot 151628697551, \\
-2^{36} B_{36} &= \frac{1}{3 \cdot 5 \cdot 7 \cdot 13 \cdot 19 \cdot 37} \cdot 2^{35} \cdot 26315271553053477373, \\
2^{38} B_{38} &= \frac{1}{3} \cdot 2^{37} \cdot 19 \cdot 154210205991661, \\
-2^{40} B_{40} &= \frac{1}{3 \cdot 5 \cdot 11 \cdot 41} \cdot 2^{39} \cdot 137616929 \cdot 1897170067619, \\
2^{42} B_{42} &= \frac{1}{3 \cdot 7 \cdot 43} \cdot 2^{41} \cdot 1520097643918070802691, \\
-2^{44} B_{44} &= \frac{1}{3 \cdot 5 \cdot 23} \cdot 2^{43} \cdot 11 \cdot 59 \cdot 8089 \cdot 2947939 \cdot 1798482437, \\
2^{46} B_{46} &= \frac{1}{3 \cdot 47} \cdot 2^{45} \cdot 23 \cdot 383799511 \cdot 67568238839737, \\
-2^{48} B_{48} &= \frac{1}{3 \cdot 5 \cdot 7 \cdot 13 \cdot 17} \cdot 2^{47} \cdot 653 \cdot 56039 \cdot 153289748932447906241, \\
2^{50} B_{50} &= \frac{1}{3 \cdot 11} \cdot 2^{49} \cdot 5^2 \cdot 417202699 \cdot 47464429777438199.
\end{aligned}$$

15.2. Числа Гурвица для кривой $y^2 = x^3 - 1$. Несколько первых значений числа C_{6n} для кривой $y^2 = x^3 - 1$ ($g = 1$) таковы:

$$\begin{aligned}
C_6 &= \frac{1}{7} \cdot 2^4 \cdot 3^2, & C_{12} &= \frac{-1}{7 \cdot 13} \cdot 2^{10} \cdot 3^5 \cdot 5^2, \\
C_{18} &= \frac{1}{7 \cdot 19} \cdot 2^{16} \cdot 3^8 \cdot 5^3 \cdot 11, & C_{24} &= \frac{-1}{7 \cdot 13} \cdot 2^{22} \cdot 3^{11} \cdot 5^3 \cdot 11^2 \cdot 17, \\
C_{30} &= \frac{1}{7 \cdot 31} \cdot 2^{28} \cdot 3^{14} \cdot 5^6 \cdot 11^2 \cdot 17 \cdot 23, \\
C_{36} &= \frac{-1}{7 \cdot 13 \cdot 19 \cdot 37} \cdot 2^{34} \cdot 3^{17} \cdot 5^7 \cdot 11^3 \cdot 17^2 \cdot 23 \cdot 29 \cdot 43, \\
C_{42} &= \frac{1}{7 \cdot 43} \cdot 2^{40} \cdot 3^{20} \cdot 5^8 \cdot 11^3 \cdot 17^2 \cdot 23 \cdot 29 \cdot 431, \\
C_{48} &= \frac{-1}{7 \cdot 13} \cdot 2^{46} \cdot 3^{23} \cdot 5^8 \cdot 11^4 \cdot 17^2 \cdot 23^2 \cdot 29 \cdot 41 \cdot 313, \\
C_{54} &= \frac{1}{7 \cdot 19} \cdot 2^{52} \cdot 3^{26} \cdot 5^{10} \cdot 11^4 \cdot 17^3 \cdot 23^2 \cdot 29 \cdot 41 \cdot 47 \cdot 1201, \\
C_{60} &= \frac{-1}{7 \cdot 13 \cdot 31 \cdot 61} \cdot 2^{58} \cdot 3^{29} \cdot 5^{13} \cdot 11^5 \cdot 17^3 \cdot 23^2 \cdot 29^2 \cdot 41^2 \cdot 47 \cdot 53 \cdot 1823, \\
C_{66} &= \frac{1}{7 \cdot 67} \cdot 2^{64} \cdot 3^{32} \cdot 5^{13} \cdot 11^6 \cdot 17^3 \cdot 23^2 \cdot 29^2 \cdot 41 \cdot 47 \cdot 53 \cdot 59 \cdot 79 \cdot 733, \\
C_{72} &= \frac{-1}{7 \cdot 13 \cdot 19 \cdot 37 \cdot 73} \cdot 2^{70} \cdot 3^{35} \cdot 5^{13} \cdot 11^6 \cdot 17^4 \cdot 23^3 \cdot 29^2 \cdot 41 \cdot 47 \cdot 53 \cdot 59 \\
&\quad \times 1153 \cdot 13963 \cdot 29059,
\end{aligned}$$

$$C_{78} = \frac{1}{7 \cdot 79} \cdot 2^{76} \cdot 3^{38} \cdot 5^{15} \cdot 11^7 \cdot 13 \cdot 17^4 \cdot 23^3 \cdot 29^2 \cdot 41 \cdot 43 \cdot 47 \cdot 53 \cdot 59 \cdot 71 \\ \times 26471111,$$

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

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

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

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

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

15.3. Числа Гурвица для кривой $y^2 = x^3 - x$. Несколько первых значений числа $C_{4n} = 2^{4n} E_{4n}$ (где E_{4n} — $4n$ -е исходное число Гурвица) для кривой $y^2 = x^3 - x$ ($g = 1$) таковы:

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

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

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

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

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

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

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

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

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

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

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

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

$$\begin{aligned}
2^{64}E_{64} &= \frac{1}{5 \cdot 17} \cdot 2^{63} \cdot 3^{22} \cdot 7^9 \cdot 11^5 \cdot 19^3 \cdot 23^2 \cdot 31^2 \cdot 43 \cdot 47 \cdot 59 \cdot 109 \cdot 814903, \\
2^{68}E_{68} &= \frac{1}{5} \cdot 2^{67} \cdot 3^{24} \cdot 7^9 \cdot 11^6 \cdot 17 \cdot 19 \cdot 23^2 \cdot 31^2 \cdot 43 \cdot 47 \cdot 59 \cdot 80232721, \\
2^{72}E_{72} &= \frac{1}{5 \cdot 13 \cdot 37 \cdot 73} \cdot 2^{71} \cdot 3^{25} \cdot 7^{10} \cdot 11^6 \cdot 19^3 \cdot 23^3 \cdot 31^2 \cdot 43 \cdot 47 \cdot 59 \cdot 67 \\
&\quad \times 48316510111193, \\
2^{76}E_{76} &= \frac{1}{5} \cdot 2^{75} \cdot 3^{27} \cdot 7^{10} \cdot 11^6 \cdot 19^4 \cdot 23^3 \cdot 31^2 \cdot 43 \cdot 47 \cdot 59 \cdot 67 \cdot 71 \cdot 3469 \\
&\quad \times 1330177.
\end{aligned}$$

16. Численные примеры для новых чисел

16.1. Функция $x(u)$ для кривой $y^2 = x^5 - 1$. Вычислим несколько первых значений числа C_{10n} для кривой $y^2 = x^5 - 1$ ($g = 2$). Приведем программу на `pari/GP`, написанную Нарую Каноу, которая дает разложение в ряд функции $x(u)$ относительно 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;

```

Используя это, получаем следующие числа:

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

$$\begin{aligned}
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 \times 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 \\
&\quad \times 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 \\
&\quad \times 47^2 \cdot 53^2 \cdot 59 \cdot 67 \cdot 73 \cdot 79 \cdot 83 \cdot 89 \cdot 97 \cdot 103 \cdot 107 \\
&\quad \times 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 \\
&\quad \times 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 \\
&\quad \times 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 \\
&\quad \times 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 \\
&\quad \times 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 \\
&\quad \times 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 \\
&\quad \times 137 \cdot 3191 \cdot 79927801 \cdot 2927519326077590415331021, \\
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 \\
&\quad \times 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 \\
&\quad \times 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 \\
&\quad \times 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 \\
&\quad \times 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 \\
&\quad \times 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 \\
&\quad \times 137 \cdot 139 \cdot 149 \cdot 157 \cdot 163 \cdot 167 \\
&\quad \times 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 \\
&\quad \times 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 \\
&\quad \times 137 \cdot 139 \cdot 149 \cdot 157 \cdot 163 \cdot 167 \cdot 173 \\
&\quad \times 239 \cdot 1471 \cdot 1579 \cdot 7030999221688667065861742323016843138707.
\end{aligned}$$

Каждое C_{10n} записывается с помощью определенного целого числа G_{10n} (теорема типа фон Штаудта–Клаузена) следующим образом:

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

16.2. Функция $y(u)$ для кривой $y^2 = x^5 - 1$. Несколько первых значений числа D_{10n} для кривой $y^2 = x^5 - 1$ ($g = 2$) таковы:

$$\begin{aligned}
D_{10} &= \frac{1}{11} \cdot 2^4 \cdot 3^2 \cdot 5^2, \\
D_{20} &= \frac{1}{11} \cdot 2^{15} \cdot 3^6 \cdot 5^4 \cdot 7 \cdot 13,
\end{aligned}$$

$$\begin{aligned}
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 \times 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 \times 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 \times 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 \times 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 \times 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 \times 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 \times 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 \times 1759 \cdot 2027 \cdot 2278423765903.
\end{aligned}$$

16.3. Функция $x(u)$ для кривой $y^2 = x^5 - x$. Несколько первых значений числа C_{8n} для кривой $y^2 = x^5 - x$ ($g = 2$) таковы:

$$\begin{aligned}
C_8 &= 2^7 \cdot 5, \\
C_{16} &= \frac{-1}{17} \cdot 2^{15} \cdot 3^2 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13, \\
C_{24} &= 2^{22} \cdot 3^4 \cdot 5^3 \cdot 7^3 \cdot 11^3 \cdot 13 \cdot 19, \\
C_{32} &= \frac{-1}{17} \cdot 2^{31} \cdot 3^6 \cdot 5^6 \cdot 7^4 \cdot 11 \cdot 13^2 \cdot 19 \cdot 23 \cdot 29 \cdot 1741, \\
C_{40} &= \frac{1}{41} \cdot 2^{40} \cdot 3^8 \cdot 5^8 \cdot 7^5 \cdot 11^2 \cdot 13^2 \cdot 19^2 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 5693, \\
C_{48} &= \frac{-1}{17} \cdot 2^{46} \cdot 3^{10} \cdot 5^8 \cdot 7^5 \cdot 11^3 \cdot 13^3 \cdot 19^2 \cdot 23^2 \cdot 29 \cdot 31 \cdot 37 \cdot 43 \cdot 41957857, \\
C_{56} &= 2^{54} \cdot 3^{12} \cdot 5^{11} \cdot 7^8 \cdot 11^5 \cdot 13^4 \cdot 19 \cdot 23^2 \cdot 29 \cdot 31 \cdot 37 \cdot 43 \cdot 47 \cdot 53 \cdot 715991,
\end{aligned}$$

$$C_{64} = \frac{-1}{17} \cdot 2^{63} \cdot 3^{14} \cdot 5^{12} \cdot 7^9 \cdot 11^3 \cdot 13^4 \cdot 19^2 \cdot 23^2 \cdot 29^2 \cdot 31^2 \cdot 37 \cdot 43 \cdot 47 \\ \times 53 \cdot 59 \cdot 61 \cdot 89 \cdot 32591401,$$

$$C_{72} = \frac{1}{73} \cdot 2^{72} \cdot 3^{16} \cdot 5^{13} \cdot 7^{10} \cdot 11^4 \cdot 13^5 \cdot 19^2 \cdot 23^3 \cdot 29^2 \cdot 31^2 \cdot 37 \cdot 43 \cdot 47 \\ \times 53 \cdot 59 \cdot 61 \cdot 67 \cdot 19346595547931,$$

$$C_{80} = \frac{-1}{17 \cdot 41} \cdot 2^{80} \cdot 3^{18} \cdot 5^{17} \cdot 7^{11} \cdot 11^5 \cdot 13^6 \cdot 19^3 \cdot 23^3 \cdot 29^2 \cdot 31^2 \cdot 37^2 \cdot 43 \cdot 47 \\ \times 53 \cdot 59 \cdot 61^2 \cdot 67 \cdot 71 \cdot 5826608412403.$$

Каждое C_{8n} записывается с помощью определенного целого числа G_{8n} (теорема типа фон Штаудта–Клаузена) следующим образом:

$$\begin{array}{ll} C_8 = & \text{целое число,} \\ C_{16} = \frac{11}{17} & + G_{16}, \\ C_{24} = & \text{целое число,} \\ C_{32} = \frac{11^2}{17} & + G_{32}, \\ C_{40} = \frac{35}{41} & + G_{40}, \\ C_{48} = \frac{11^3}{17} & + G_{48}, \\ C_{56} = & \text{целое число,} \\ C_{64} = \frac{11^4}{17} & + G_{64}, \\ C_{72} = \frac{2}{73} & + G_{72}, \\ C_{80} = \frac{11^6}{17} + \frac{35^2}{41} & + G_{80}, \\ C_{88} = \frac{18}{89} & + G_{88}, \\ C_{96} = \frac{11^7}{17} + \frac{10}{97} & + G_{96}, \\ C_{104} = & \text{целое число,} \\ C_{112} = \frac{11^8}{17} + \frac{18}{113} & + G_{112}, \\ C_{120} = \frac{35^3}{41} & + G_{120}, \\ C_{128} = \frac{11^9}{17} & + G_{128}, \\ C_{136} = & \frac{131}{137} + G_{136}, \\ C_{144} = \frac{11^{10}}{17} + \frac{2^2}{73} & + G_{144}. \end{array}$$

17. Негиперэллиптические кривые, вполне разветвленные на бесконечности

Здесь мы описываем, как выбирается естественная переменная u для общей кривой циклотомического типа.

Пусть a и b – пара взаимно простых натуральных чисел, и пусть

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

– сепарабельный многочлен, где пара (i, j) пробегает множество целых чисел таких, что

$$0 \leq i < b-1, \quad 0 \leq j < a-1, \quad ia + jb < ab. \quad (17.2)$$

Обсудим алгебраическую кривую $\mathcal{C}$, заданную уравнением

$$f(x, y) = 0. \quad (17.3)$$

Здесь $\mathcal{C}$ рассматривается естественным образом как кривая с единственной бесконечно удаленной точкой ∞ . Род кривой $\mathcal{C}$ задается формулой $g = (a-1) \times (b-1)/2$. На этой кривой $\mathcal{C}$ множество

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

образует базис дифференциальных форм первого рода, где $f_y(x, y) = \frac{\partial f}{\partial y}(x, y)$.

Выбирая порождающий элемент фундаментальной группы кривой $\mathcal{C}$, определим матрицу периодов $[\omega \ \omega'']$. Определим также решетку периодов в $\mathbb{C}^g$ следующим образом:

$$\Lambda := \omega'^t [\mathbb{Z} \ \mathbb{Z} \ \cdots \ \mathbb{Z}] + \omega''^t [\mathbb{Z} \ \mathbb{Z} \ \cdots \ \mathbb{Z}] \quad (\subset \mathbb{C}^g). \quad (17.5)$$

Обозначим многообразие Якоби кривой $\mathcal{C}$ через J , а симметрическое произведение g копий $\mathcal{C}$ через $\text{Sym}^g(\mathcal{C})$. Тогда имеем бирациональное отображение

$$\text{Sym}^g(\mathcal{C}) \rightarrow \text{Pic}^\circ(\mathcal{C}) = J, \quad (P_1, \dots, P_g) \mapsto \text{класс дивизора } P_1 + \cdots + P_g - g \cdot \infty.$$

Как аналитическое многообразие, J отождествляется с $\mathbb{C}^g/\Lambda$. Обозначим через κ естественное отображение $\mathbb{C}^g \rightarrow \mathbb{C}^g/\Lambda = J$. Отображение

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

дает вложение кривой $\mathcal{C}$ в J . Поднятие $\kappa^{-1}\iota(\mathcal{C})$ образа ι под действием κ является универсальным абелевым накрытием кривой $\mathcal{C}$. Бирациональное отображение представляется аналитически путем отображения каждого $(P_1, \dots, P_g) \in \text{Sym}^g(\mathcal{C})$ в точку $\mathbf{u} \bmod \Lambda \in \mathbb{C}^g/\Lambda$, где

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

Для каждой точки $\mathbf{u} \in \kappa^{-1}\iota(\mathcal{C})$ обозначим через

$$x(\mathbf{u}), \ y(\mathbf{u}) \quad (17.6)$$

значение (x, y) -координаты кривой $\mathcal{C}$, для которой $\kappa(\mathbf{u}) = \iota(x(\mathbf{u}), y(\mathbf{u}))$. Рассматриваем $x(\mathbf{u})$ и $y(\mathbf{u})$ как функцию на $\kappa^{-1}\iota(\mathcal{C})$. Справедлива следующая основная лемма.

ЛЕММА 17.7. *Разложение Лорана функций $x(\mathbf{u})$ и $y(\mathbf{u})$ около начала координат $(0, \dots, 0)$ относительно u_g имеет вид*

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

Более того, имеется результат, соответствующий лемме 4.4, и мы видим, что естественно взять $u := u_g$ в качестве локального параметра около точки $\mathbf{u} = (0, \dots, 0)$ на $\kappa^{-1}\iota(\mathcal{C})$.

Назовем кривую $\mathcal{C}$, заданную уравнением $f(x, y) = 0$, где

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

кривой *циклотомического типа*. Для такой кривой $\mathcal{C}$ коэффициенты Гурвица разложения в степенной ряд функций $u = u_g \mapsto x(\mathbf{u})$, $u_g \mapsto y(\mathbf{u})$ относительно u удовлетворяют теореме типа Кларка (теорема типа фон Штаудта–Клаузена плюс обобщение второй теоремы фон Штаудта) и теореме типа Куммера. Мы можем доказать их теми же рассуждениями из этой работы.

18. Дополнения

18.1. Соотношения на биномиальные коэффициенты. Матрица Хасе–Витта относительно базиса (4.1) для кривой $y^2 = x^5 - 1 \pmod p$ диагональна [30], а ее $(2, 2)$ -элемент задается, как и в теореме 6.3, следующим образом:

$$A_p \equiv (-1)^{(p-1)/10} \binom{(p-1)/2}{(p-1)/10} \pmod p.$$

Покажем, что он совпадает со значением (11.5). Другими словами, мы утверждаем, что если для простого числа $p \equiv 1 \pmod 5$ положить $p = 10m + 1$, то

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

Так как это сравнение эквивалентно сравнению

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

докажем последнее. Поскольку

$$2(5m), 2(5m-1), \dots, 2(5m-(m-1)) \pmod p$$

совпадают соответственно с

$$-1, -3, \dots, -(2m-1) \pmod p,$$

получаем вышеприведенное равенство. Аналогично можно доказать, что

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

Хотя эти факты доказываются с использованием основных свойств p -адической Γ -функции, мы описали их вполне элементарным образом.

18.2. Связи с некоторыми рядами типа Эйзенштейна. Естественным является вопрос, связаны ли числа C_n и D_n с какого-то рода L -функцией. Ниже мы объясняем, что такой вопрос не совсем лишен смысла.

Напомним доказательство формулы Гурвица, т. е.

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

в духе работы [5] (см. также [21; с. 193–198]); здесь

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

Если приравнять два типа разложений

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

удалить $1/u^2$ и продифференцировать результат $4n-2$ раз, то, подставив $u = 0$, мы получим (18.1). Это рассуждение похоже на доказательство формулы Эйлера (а именно, выражения специального значения $\zeta(2m)$ дзета-функции Римана через число Бернулли и π), использующее два типа разложений для $1/\sin^2(u)$.

Для случая гиперэллиптической кривой произвольного рода g функция $x(\mathbf{u})$ имеет разложение Лорана около каждой точки решетки $\ell = (\ell_1, \ell_2, \dots, \ell_g) \in \Lambda$ ($\subset \mathbb{C}^g$):

$$x(\mathbf{u}) = \frac{1}{(u_g - \ell_g)^2} + \dots \quad (18.3)$$

Хотя у нас и нет на это никаких оснований, все же можно ожидать, что верна формула

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

где $*$ означает, что сумма не обоснована. Если такая формула существует, то с помощью рассуждения, аналогичного рассуждению для $\wp(u)$, приходим к формулам следующего типа:

– для кривой $y^2 = x^{2g+1} - 1$ имеем

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

где $\Omega = \int_1^\infty \frac{x^{g-1} dx}{y} > 0$, а L – умноженный на $1/\Omega$ образ проекции $\Lambda \subset \mathbb{C}^g$ на g -й фактор $\mathbb{C}$ (например, если $2g+1$ – простое число, то $L = \mathbb{Z}[e^{2\pi i/(2g+1)}]$);
– для кривой $y^2 = x^{2g+1} - x$ имеем

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

где $\Omega = \int_1^\infty \frac{x^{g-1} dx}{y} > 0$, а L – умноженный на $1/\Omega$ образ проекции $\Lambda \subset \mathbb{C}^g$ на g -й фактор $\mathbb{C}$.

Если бы удалось получить такой результат, то это стало бы открытием новых L -функций, которые находятся в другой категории L -функций Гекке, связанной с характерами Гекке (Größencharakter). Автор также предполагает, что эта история имеет отношение к тому, что написано в [34] на с. 240.

18.3. Проблемы. Перечислим некоторые еще не доказанные утверждения и проблемы, подлежащие исследованию.

(1) Судя по численным примерам, сигнатура чисел C_n или D_n чередующаяся или постоянная, как и в случае чисел Бернулли и Гурвица. Доказать этот феномен. Это может быть не так уж трудно.

(2) Например, для кривой $y^2 = x^5 - 1$, если $p \equiv 1 \pmod{5}$ и $(p-1) \nmid 10m$, то $p \nmid C_{10m}$.

(3) Насколько велики порядки 2-частей чисел C_n и D_n ? Для случая чисел Бернулли и Гурвица они точно определены. Например, верно ли, что $\text{ord}_2(C_{15n}) = 12n - 3$ для $y^3 = x^5 - 1$ ($g = 4$)?

(4) Например, простые факторы в числителях чисел C_{10m} и D_{10m} очень похожи, хотя и не в точности те же самые. Объяснить это теоретически.

Список литературы

- [1] T. Clausen, “Theorem”, *Astronomische Nachrichten*, **17**:22 (1840), 351–352.
- [2] K. G. C. von Staudt, “Beweis eines Lehrsatzes, die Bernoullischen Zahlen betreffend”, *J. Reine Angew. Math.*, **21** (1840), 372–374, //1840.
- [3] K. G. C. von Staudt, *De Numeris Bernoullianis, commentatio altera*, Erlangen, 1845.
- [4] E. E. Kummer, “Über eine allgemeine Eigenschaft der rationalen Entwicklungskoeffizienten einer bestimmten Gattung analytischer Functionen”, *J. Reine Angew. Math.*, **41** (1851), 368–372.
- [5] A. Hurwitz, “Ueber die Entwicklungskoeffizienten der lemniskatischen Functionen”, *Nachr. Acad. Wiss. Göttingen*, 1897, 273–276; *Mathematische Werke*, **II**, Birkhäuser, Basel, 1963, 338–341.

- [6] A. Hurwitz, “Ueber die Entwicklungskoeffizienten der lemniskatischen Funktionen”, *Math. Ann.*, **51** (1899), 196–226; *Mathematische Werke*, **II**, Birkhäuser, Basel, 1963, 342–373.
- [7] H. Lang, “Kummersche Kongruenzen für die normierten Entwicklungskoeffizienten der Weierstrasschen $\wp$ -Funktionen”, *Abh. Math. Sem. Univ. Hamburg*, **33** (1969), 183–196.
- [8] L. Carlitz, “Congruences for the coefficients of hyperelliptic and related functions”, *Duke Math. J.*, **19** (1952), 329–337.
- [9] N.M. Katz, “Formal groups and p -adic interpolation”, *Journées Arithmétiques de Caen* (Univ. Caen, Caen, 1976), *Astérisque*, **41–42**, Soc. Math. France, Paris, 1977, 55–65.
- [10] K.H. Rosen, W.M. Snyder, “A Kummer congruence for the Hurwitz–Herglotz function”, *Tokyo J. Math.*, **6** (1983), 125–133.
- [11] C. Snyder, “A concept of Bernoulli numbers in algebraic function fields”, *J. Reine Angew. Math.*, **307/308** (1979), 295–308.
- [12] C. Snyder, “The coefficients of the Hessian elliptic functions”, *J. Reine Angew. Math.*, **306** (1979), 60–87.
- [13] C. Snyder, “A concept of Bernoulli numbers in algebraic function fields. II”, *Manuscripta Math.*, **35**:1-2 (1981), 69–89.
- [14] C. Snyder, “Kummer congruences for the coefficients of Hurwitz series”, *Acta Arith.*, **40**:2 (1981/82), 175–191.
- [15] C. Snyder, “Kummer congruences in formal groups and algebraic groups of dimension one”, *Rocky Mountain J. Math.*, **15**:1 (1985), 1–11.
- [16] C. Snyder, “ p -adic interpolation of the coefficients of Hurwitz series attached to height one formal groups”, *Rocky Mountain J. Math.*, **23**:1 (1993), 339–351.
- [17] H.S. Vandiver, “Certain congruence involving the Bernoulli numbers”, *Duke Math. J.*, **5** (1939), 548–551.
- [18] L. Carlitz, “The coefficients of the reciprocal of a series”, *Duke Math. J.*, **8** (1941), 689–700.
- [19] M. Hazewinkel, *Formal groups and applications*, Pure Appl. Math., **78**, Academic Press, New York–London, 1978, xxii+573 pp.
- [20] Э. Т. Уиттекер, Дж. Н. Ватсон, *Курс современного анализа*, 2-е изд., Физматгиз, М., 1963, 342, 515 с.; пер. с англ.: E.T. Whittaker, G.N. Watson, *A course of modern analysis*, Cambridge Univ. Press, Cambridge, 1927, vi+608 pp.
- [21] T. Arakawa, T. Ibukiyama, M. Kaneko, *Bernoulli numbers and zeta functions*, Makino Shoten Ltd., Tokyo, 2001 (in Japanese).
- [22] Y. Ônishi, *Theory of the generalized Bernoulli–Hurwitz numbers for the algebraic functions of cyclotomic type and the universal Bernoulli numbers*, arXiv: math/0406096 [math.NT].
- [23] L. Comtet, *Advanced combinatorics. The art of finite and infinite expansions*, Reidel, Dordrecht, 1974, xi+343 pp.
- [24] F. Clarke, “The universal von Staudt theorem”, *Trans. Amer. Math. Soc.*, **315**:2 (1989), 591–603.
- [25] A. Adelberg, “Universal higher order Bernoulli numbers and Kummer and related congruences”, *J. Number Theory*, **84**:1 (2000), 119–135.
- [26] A. Adelberg, “Kummer congruences for universal Bernoulli numbers and related congruences for poly-Bernoulli numbers”, *Int. Math. J.*, **1**:1 (2002), 53–63.
- [27] A. Adelberg, “Universal Kummer congruences mod prime powers”, *J. Number Theory*, **109**:2 (2004), 362–378.
- [28] T. Honda, “On the theory of commutative formal groups”, *J. Math. Soc. Japan*, **22** (1970), 213–246.

- [29] A. M. Robert, *A course in p -adic analysis*, Grad. Texts in Math., **198**, Springer-Verlag, New York, 2000, xvi+437 pp.
- [30] N. Yui, “On the Jacobian varieties of hyperelliptic curves over fields of characteristic $p > 2$ ”, *J. Algebra*, **52**:2 (1978), 378–410.
- [31] N. M. Katz, “The congruence of Clausen–von Staudt and Kummer for Bernoulli–Hurwitz numbers”, *Math. Ann.*, **216** (1975), 1–4.
- [32] Y. Morita, “A p -adic analogue of the Γ -function”, *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, **22**:2 (1975), 255–266.
- [33] H. Matsumura, *Commutative ring theory*, Cambridge Stud. Adv. Math., **8**, Cambridge Univ. Press, Cambridge, 1986, xiv+320 pp.
- [34] T. Ibukiyama, “Memoirs on ‘easy’ zeta functions”, *Proceedings of the 9th summer school on “Zeta functions”*, 2001, 235–248.

Ё. ОНИШИ (Y. Onishi)

University of Yamanashi, Japan

E-mail: yonishi@yamanashi.ac.jp

Поступила в редакцию

14.02.2011