Общероссийский математический портал

В. А. Колывагин, Уравнение Ферма над башней круговых полей, *Изв. РАН. Сер. матем.*, 2001, том 65, выпуск 3, 85–122

DOI: <https://doi.org/10.4213/im337>

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: 52.205.19.152

26 апреля 2023 г., 15:32:08

УДК 513.6

В. А. Колывагин

Уравнение Ферма над башней круговых полей

Пусть $l > 3$ – простое число, $L_n = \mathbb{Q}(\sqrt[l^{n+1}]{1})$, R_n – максимальное вещественное подполе L_n , H_n – максимальное l -подрасширение поля R_n . Определены эффективно вычисляемые целочисленные функции $\varphi_1(l)$, $\varphi_2(l)$, $\varphi_3(l)$ такие, что $-1 \leq \varphi_1(l) \leq \varphi_2(l) \leq \varphi_3(l) \leq (l-3)/2 - I(l)$, где $I(l)$ – индекс иррегулярности числа l . При $\varphi_1(l) \geq 0$ доказан первый случай теоремы Ферма для l и полей $L_{\varphi_1(l)}$, $R_{\varphi_2(l)}$, $H_{\varphi_3(l)}$. Получены явные оценки снизу для функций $\varphi_1(l)$, $\varphi_2(l)$, $\varphi_3(l)$. Для регулярных l (тогда $\varphi_1(l) \geq 1$) доказан второй случай теоремы Ферма для l и поля $L_{(l-3)/2}$ и доказана теорема Ферма для l и полей $L_{\varphi_1(l)}$, $R_{\varphi_2(l)}$, что обобщает классический результат о справедливости теоремы Ферма для регулярного l и поля L_0 . Получены также некоторые другие результаты о решениях уравнения Ферма $x^l + y^l + z^l = 0$ над полями L_n , R_n , H_n .

Библиография: 14 наименований.

Введение

Пусть $l > 3$ – простое число. Пусть K – конечное расширение поля рациональных чисел $\mathbb{Q}$. Говорят, что ТФ (теорема Ферма) верна для l и K , если уравнение

$$x^l + y^l + z^l = 0 \quad (1)$$

не имеет решений в ненулевых числах поля K . Говорят, что 1СТФ (первый случай теоремы Ферма) верен для l и K , если (1) не имеет решений в целых числах поля K , взаимно простых с l .

Пусть L_n – поле $\mathbb{Q}(\sqrt[l^{n+1}]{1})$, $n \geq 0$. Число l называется *регулярным*, если число классов дивизоров поля L_0 не делится на l .

В XIX в. Куммер развил свою теорию идеальных делителей (теорию дивизоров на современном языке) и применил ее к исследованию уравнения (1). Он доказал [1], что для регулярного l уравнение (1) не имеет решений в попарно взаимно простых числах поля L_0 . Условие взаимной простоты может быть опущено, как показал Гильберт позднее, так что для регулярного простого числа l и поля L_0 справедлива ТФ. Заметим, что, хотя неизвестно, существует ли бесконечно много регулярных простых чисел (для иррегулярных простых это доказано), предполагается и хорошо согласуется с результатами вычислений то, что регулярные числа составляют $\approx 61\%$ от всех простых чисел.

Куммер также нашел замечательную явную форму для условия регулярности. Именно, пусть B_i обозначают числа Бернулли – рациональные числа, определяемые разложением

$$\frac{X}{\exp(X) - 1} = \sum_{i=0}^{\infty} B_i \left(\frac{X^i}{i!} \right).$$

Числа Бернулли могут быть также вычислены с помощью рекуррентных соотношений

$$1 + \sum_{i=1}^{j-1} C_j^i B_i = 0, \quad j \geq 2.$$

Известно (см. [2, гл. 5, § 8, теорема 5]), что при четных i , $2 \leq i \leq l-3$, l не делит знаменатель B_i . Куммер доказал, что l регулярно тогда и только тогда, когда l не делит B_i при четных i , $2 \leq i \leq l-3$.

Исследование уравнения (1) в поле L_0 и его подполях, начатое классическими работами Куммера, основано на разложении формы $x^l + y^l$ на линейные множители в L_0 с последующим использованием арифметических свойств поля L_0 (или его подполя). Данная работа продолжает серию работ автора [3], [4], развивающих этот классический подход.

Именно, мы исследуем решения уравнения (1) в поле L_n или его подполях R_n , H_n . Отправной точкой здесь является то, что для регулярного l , как известно, числа классов дивизоров полей L_n , R_n также не делятся на l . Это могло бы способствовать исследованию уравнения (1) подобно случаю поля L_0 .

Отметим, что большим успехом последних лет явилось доказательство ТФ для всех l и поля рациональных чисел $\mathbb{Q}$ (см. [14]). Однако применимость использованных при этом методов к исследованию решений (1) в полях L_n , R_n , H_n в настоящее время не ясна.

Пусть ℓ_n – единственный простой дивизор поля L_n , делящий l . Говорят, что 2СТФ (второй случай ТФ) верен для l и L_n , если уравнение (1) не имеет решений в ненулевых целых числах поля L_n , одно из которых делится на ℓ_n , а остальные взаимно просты с ℓ_n . Поскольку ℓ_n – главный дивизор, то ТФ верна для l и L_n тогда и только тогда, когда 1СТФ и 2СТФ верны для l и L_n .

Для произвольного n мы доказали следующий результат, включающий “ослабленный” 2СТФ.

ТЕОРЕМА 1. Пусть l регулярно, $n \geq 0$, ε – единица поля L_n . Тогда уравнение

$$x^l + y^l = \varepsilon \gamma^l \quad (2)$$

не имеет решений в целых числах x, y, γ поля L_n таких, что x, y взаимно просты с ℓ_n , а $0 \neq \gamma$ делится на ℓ_n^2 .

Отметим, что для $n = 0$ этот результат также был известен ранее (см. [2, гл. 5, § 7]).

Далее, доказана следующая

ТЕОРЕМА 2. Пусть l регулярно. Тогда 2СТФ верен для l и поля $L_{(l-3)/2}$.

Далее, 1СТФ доказан для произвольного l такого, что $\varphi_1(l) \geq 0$, и полей $L_{\varphi_1(l)}$, $R_{\varphi_2(l)}$, $H_{\varphi_3(l)}$, где числа $\varphi_1(l) \leq \varphi_2(l) \leq \varphi_3(l) \leq (l-3)/2 - I(l)$ будут определены ниже. Поскольку из теоремы 2 следует, что 2СТФ верен для регулярного l и L_n при $n = (l-3)/2$ (а значит, и для l и L_n при $n \leq (l-3)/2$), то ТФ верна для регулярного l и полей $L_{\varphi_1(l)}$, $R_{\varphi_2(l)}$ ($\varphi_3(l) = \varphi_2(l)$ для регулярного l).

Займемся определением чисел $\varphi_j(l)$. Нам потребуются некоторые определения и обозначения. Рассмотрим разложение

$$\frac{1}{1 - Y \exp(X)} = \sum_{i \geq 0} f_i(Y) \left(\frac{X^i}{i!} \right). \quad (3)$$

Легко доказать (см. [4, § 2]), что $f_i(Y) = P_i(Y)/(1-Y)^{n+1}$, где $P_i(Y)$ – унитарный многочлен степени i с целыми рациональными коэффициентами. Многочлены P_i могут быть последовательно вычислены с помощью рекуррентного соотношения

$$P_{i+1} = (i+1)YP_i + (Y - Y^2)P'_i,$$

учитывая, что $P_0 = 1$. В частности, $P_1 = Y$, $P_2 = Y^2 + Y$, $P_3 = Y^3 + 4Y^2 + Y$ и т.д. Известны также явные формулы для коэффициентов P_n и сравнение

$$P_i(Y)(1-Y)^{l-1-i} \equiv \sum_{r=1}^{l-1} r^i X^r \pmod{l} \quad \text{при } i = 1, \dots, l-1$$

(см. по этому поводу [4, § 2]).

Пусть Σ_l обозначает множество $\mathbb{Z}/l\mathbb{Z} \setminus \{0, 1\}$, а при $t \in \Sigma_l$ $\mathbf{G}_t$ обозначает подмножество $\{t, 1-t, 1/t, 1/(1-t), t/(t-1), (t-1)/t\}$ в Σ_l . Условие $P_i(\mathbf{G}_t) \neq 0$ обозначает, что $\exists \tau \in \mathbf{G}_t$ такой, что $P_i(\tau) \not\equiv 0 \pmod{l}$. Заметим, что $P_1(\mathbf{G}_t) \neq 0$, $P_2(\mathbf{G}_t) \neq 0$. Действительно, если $\tau \in \mathbf{G}_t$, $P_2(\tau) \equiv 0 \pmod{l}$, то $\tau \equiv -1 \pmod{l}$. Тогда $2 = 1 - \tau \in \mathbf{G}_t$, $2 \not\equiv -1 \pmod{l}$ (так как $l > 3$) и $P_2(1 - \tau) \not\equiv 0 \pmod{l}$.

Пусть $c(t)$ – максимальное натуральное (т.е. положительное целое) четное число c такое, что $P_c(\mathbf{G}_t) \neq 0$, $l \nmid B_{l-1-c}$, если такие числа существуют. Например (см. § 3), $c(t)$ определено и $c(t) \geq \lceil l/(1 + (I(l) + 1)(I(l) + 2)) \rceil$, если $l > 1 + (I(l) + 1)(I(l) + 2)$. Предположим, что $c(t)$ определено. Положим $d_0 = 0$. Пусть при $j = 1, 2, 3$ $\mathbf{A}_j(t)$ обозначает множество строго возрастающих последовательностей натуральных чисел $d_1, \dots, d_N$ таких, что $d_N \leq c(t)$ и $\forall 1 \leq i \leq N$ множество натуральных чисел m таких, что $d_{i-1} < m \leq d_i$, $P_m(\mathbf{G}_t) \neq 0$ содержит соответственно $I(l)+1$ четных и $I(l)+1$ нечетных чисел (случай $j = 1$), $I(l)+1$ нечетных чисел (случай $j = 2$), нечетное число m такое, что $l \nmid B_{l-m}$ (случай $j = 3$). Пусть $N_j(t)$ – максимум длин последовательностей из $\mathbf{A}_j(t)$ ($N_j(t) = 0$, если $\mathbf{A}_j(t)$ пусто). Очевидно, $\mathbf{A}_1(t) \subset \mathbf{A}_2(t) \subset \mathbf{A}_3(t)$, так что $N_1(t) \leq N_2(t) \leq N_3(t)$. Также очевидно, что

$$N_1(t) \leq \lceil c(t)/(2(I(l) + 1)) \rceil \leq (l-3)/(2(I(l) + 1)).$$

Для регулярного l $N_1(t) \geq 1$, так как последовательность $\{2\}$ содержится в $\mathbf{A}_1(t)$. Заметим, что $\mathbf{A}_j(t)$, $N_j(t)$ зависят фактически от $\mathbf{G}_t$. Если $c(t)$ не определено, то $N_j(t) \stackrel{\text{def}}{=} -1$.

Пусть $\varphi_j(l) = \min N_j(t)$, где минимум берется по $t \in \Sigma_l$.

Пусть (x, y, z) – решение (1) в целых числах поля L_n , взаимно простых с ℓ_n . Положим $t = -x/y \pmod{\ell_n} \in \Sigma_l$. Заметим, что $\mathbf{G}_t$ не меняется при перестановке (x, y, z) . Пусть F – подполе L_n , m – натуральное число. Говорим, что для l и F верна ТФ $\pmod{\ell_n^m}$, если для всякого решения (x, y, z) уравнения (1) в ℓ_n -целых числах поля F либо $x \equiv 0 \pmod{\ell_n^m}$, либо $y \equiv 0 \pmod{\ell_n^m}$, либо $z \equiv 0 \pmod{\ell_n^m}$. Очевидно,

$$\text{ТФ} \Rightarrow \text{ТФ} \pmod{\ell_n^m} \Rightarrow \text{1СТФ} \Leftrightarrow \text{ТФ} \pmod{\ell_n}.$$

Мы доказали следующую теорему.

ТЕОРЕМА 3. а) Пусть (x, y, z) – решение уравнения (1) в целых числах поля L_n , взаимно простых с ℓ_n . Положим $t = -x/y \pmod{\ell_n}$. Тогда $n > N_1(t)$. Если $x, y, z \in R_n$, то $n > N_2(t)$. Если $x, y, z \in H_n$, то $n > N_3(t)$.

б) Пусть ε – единица поля L_n . Пусть (x, y, γ) – решение уравнения (2) в целых числах поля L_n таких, что y взаимно прост с ℓ_n , а x делится на ℓ_n . Тогда:

1) если $n = 0$, то $x \equiv 0 \pmod{\ell_0^{l+1}}$;
 2) если $1 \leq n \leq \frac{l-3}{2(I(l)+1)}$, то $x \equiv 0 \pmod{\ell_0^{l-1-2n(I(l)+1)}}$ (в частности, $x \equiv 0 \pmod{\ell_0^2}$);

3) если $1 \leq n \leq \frac{l-3}{2} - I(l)$, а $x, y \in H_n$, то $x \equiv 0 \pmod{\ell_0^{l-1-d_n} \ell_n^{d_n}}$, где d_n – n -е по порядку нечетное натуральное число такое, что l не делит B_{l-d_n} .

с) 1СТФ верен для l и полей $L_{\varphi_1(l)}$, $R_{\varphi_2(l)}$, $H_{\varphi_3(l)}$, если $\varphi_1(l) \geq 0$ (т.е. $c(t)$ определено $\forall t \in \Sigma_l$).

д) При $\varphi_1(l) \geq 0$ для l и L_0 верна ТФ $\pmod{\ell_0^{l+1}}$.

При $1 \leq n \leq \varphi_1(l)$ для l и L_n верна ТФ $\pmod{\ell_0^{l-1-2n(I(l)+1)}}$.

При $1 \leq n \leq \varphi_2(l)$ для l и R_n верна ТФ $\pmod{\ell_0^{l-1-2n(I(l)+1)}}$.

При $1 \leq n \leq \varphi_3(l)$ для l и H_n верна ТФ $\pmod{\ell_0^{l-1-d_n} \ell_n^{d_n}}$, где число d_n – то же, что и в п. б).

Очевидно, п. с) следует из п. а), п. д) следует из пп. б) и с), усиливая п. с). Также очевидно, что теорема 2 следует из теоремы 1 и п. б) теоремы 3. Утверждение п. а) теоремы 3 в случае $n = 0$ следует из работы [4], так как решение (x, y, z) не может существовать, если $N_1(t) \geq 0$ (т.е. если $c(t)$ определено); тогда условие

$$B_{l-1-c(t)} P_{c(t)}(\mathbf{G}_t) \not\equiv 0 \pmod{l}$$

противоречило бы сравнениям [4, (2)]. В частности, справедливость 1СТФ для l и L_0 при $\varphi_1(l) \geq 0$ доказана в [4].

Поскольку $\varphi_1(l) \geq 1$ для регулярного l , то, учитывая п. с) теоремы 3 и теорему 2, мы, как уже отмечалось выше, получаем следующую теорему.

ТЕОРЕМА 4. Для регулярного l ТФ верна для l и полей $L_{\varphi_1(l)}$, $R_{\varphi_2(l)}$.

Результаты вычислений (см., в частности, §4) позволяют предположить, что возможное отклонение $\varphi_1(l)$ от своего максимального возможного значения $[(l-3)/(2(I(l)+1))]$ относительно невелико, как и отклонение $\varphi_3(l)$ от $(l-3)/2 - I(l)$. Однако доказательство этого представляется нелегкой проблемой. Нам удалось получить оценки снизу для функций $\varphi_j(l)$, показывающие, в частности, что $\varphi_j(l)$ стремится к бесконечности, когда l , имеющее ограниченный индекс иррегулярности, стремится к бесконечности (предполагается, что множество таких l бесконечно).

Развивая идеи работ Эйхлера и Краснера [6], [5], мы доказали следующую теорему.

ТЕОРЕМА 5. а) Пусть N – натуральное число такое, что

$$\left(\frac{(2N(I(l)+1))! ((2N(I(l)+1))! + 1)}{2} \right)^{N(I(l)+1)-1} < l.$$

Тогда $\varphi_1(l) \geq N$.

б) Если $l > 1 + (I(l) + 1)(I(l) + 2)$, то

$$\begin{aligned}\varphi_1(l) &\geq \psi_1(l) \stackrel{\text{def}}{=} \left\lceil \frac{1}{I(l) + 1} \left(\frac{\ln(l)}{2 \ln \ln(l)} \right)^{1/2} \right\rceil, \\ \varphi_2(l) &\geq \psi_2(l) \stackrel{\text{def}}{=} \left\lceil \frac{1}{I(l) + 1} \left(\left\lceil \sqrt{\frac{l}{1 + (I(l) + 1)(I(l) + 2)}} \right\rceil - 1 \right) \right\rceil, \\ \varphi_3(l) &\geq \psi_3(l) \stackrel{\text{def}}{=} \max \left(\left\lceil \sqrt{\frac{l}{1 + (I(l) + 1)(I(l) + 2)}} \right\rceil - 1 - I(l), 0 \right).\end{aligned}$$

Следствием теорем 3–5 является

ТЕОРЕМА 6. а) Пусть N – натуральное число, M – неотрицательное целое число. 1СТФ верен для l и поля L_N при всех l таких, что $I(l) \leq M$,

$$l > \left(\frac{(2N(M+1))!((2N(M+1))! + 1)}{2} \right)^{N(M+1)-1}.$$

б) Если $l > 1 + (I(l) + 1)(I(l) + 2)$, то 1СТФ верен для l и полей $L_{\psi_1(l)}$, $R_{\psi_2(l)}$, $H_{\psi_3(l)}$.

с) ТФ верна для l и полей $L_{\psi_1(l)}$, $R_{\psi_2(l)}$ при всех регулярных l .

Из теоремы 5 следует, что $\varphi_1(l) \geq N$ при всех достаточно больших l таких, что $I(l)$ ограничен. В § 4 мы, используя подход Вады [11], описываем способ, позволяющий путем вычислений для данных N, M уточнить множество тех l , для которых $I(l) = M$, $\varphi_1(l) \geq N$. Например, мы показываем, что $\varphi_1(l) \geq 5$ для всех регулярных $l \geq 17$, $\varphi_1(l) \geq 2$ для всех l таких, что $I(l) = 1$, и $\varphi_1(l) \geq 3$ для всех l таких, что $I(l) = 1$, кроме нескольких возможных исключений, и т.п.

Пусть $I(l, T)$ – количество тех нечетных натуральных чисел $1 < n < 2T$, для которых l делит B_{l-n} (в частности, $I(l) = I(l, (l-1)/2)$).

Из теорем 3, 4 и результатов § 4 следует

ТЕОРЕМА 7. а) ТФ верна для $l = 5$ и поля L_1 , $l = 7$ и поля L_2 , $l = 11$ и поля L_4 , $l = 13$ и поля L_4 . Кроме того, если при $l = 13$ (x, y, z) – решение (1) в L_5 , то $t^2 - t + 1 = 0$, где $t = -x/y \pmod{\ell_5}$ (заметьте, что $x/y - \ell_5$ – целое число, так как 2СТФ верен для $l = 13$ и поля L_5 согласно теореме 2). Далее, ТФ верна для любого регулярного $l \geq 17$ и поля L_5 , а при $l \notin \mathbf{E}_1 \cup \mathbf{E}_2$ (см. конец работы) и для поля L_6 .

б) 1СТФ верен для всех l индекса иррегулярности 1 и поля L_2 , а при $l \notin \mathbf{E}_2$ – и для поля L_3 . 1СТФ верен для всех l индекса иррегулярности 2, 3, 4 и поля L_1 , а для l индекса иррегулярности 2, $l \neq 691$, $l \notin \mathbf{E}_2$, – и для поля L_2 . 1СТФ верен для всех l индекса иррегулярности 5, не делящих Δ_{11} (см. § 4), $l \neq 20579903$, и поля L_1 .

с) 1СТФ верен для l и поля $H_{5-I(l,6)}$ при всех иррегулярных числах l таких, что $I(l,6) \leq 5$. 1СТФ верен для l и поля $H_{6-I(l,6)}$ при всех иррегулярных числах $l \notin \mathbf{E}_2$, $l \neq 691$, таких, что $I(l,6) \leq 6$.

§ 1. Свойства решений уравнения (2), доказательство теоремы 1

В этом параграфе будут установлены некоторые свойства решений уравнения (2). В частности, мы докажем теорему 1, осуществив бесконечный спуск соответствующих решений (2) подобно классическим работам Куммера и Вандивера.

Считая пока l произвольным простым числом, а n фиксированным, обозначим поле L_n через L . Пусть O_L – кольцо целых чисел поля L , $O'_L = O_L \setminus \{0\}$. Если $a, b \in O'_L$, то $\text{div}(a)$ обозначает главный дивизор L , соответствующий a , $\text{mcd}(a, b)$ обозначает максимальный общий делитель $\text{div}(a)$ и $\text{div}(b)$. Пусть $\ell = \ell_n$. Обозначим через T множество целых дивизоров L , взаимно простых с ℓ .

Пусть (x, y, γ) – решение (2) в O'_L такое, что y взаимно прост с ℓ . Положим $\mathcal{M} = \text{mcd}(x, y) \in T$, $d = \text{ord}_\ell(\text{div}(\gamma) \cdot \mathcal{M}^{-1})$, $\mathcal{X} = \text{div}(\gamma) \cdot \mathcal{M}^{-1} \ell^{-d} \in T$.

Пусть ζ – примитивный корень l -ой степени из 1. Положим

$$\omega_k = x + \zeta^k y, \quad k = 0, 1, \dots, l-1.$$

Определим $\mathcal{A}_k \in T$, $n_k \geq 0$ условием $\text{div}(\omega_k) = \mathcal{M} \mathcal{A}_k \ell^{n_k}$. Имеет место

ПРЕДЛОЖЕНИЕ 1. *Существуют и единственны попарно взаимно простые дивизоры $\mathcal{C}_k \in T$ такие, что $\mathcal{A}_k = \mathcal{C}_k^l$, причем $\prod_{k=0}^{l-1} \mathcal{C}_k = \mathcal{X}$. При $d < l^n$ будет $n_k = d$, при $d \geq l^n$ будет $d > l^n$ и $\exists! i$ такой, что $n_i = l^n + (d - l^n)l$, $n_k = l^n$ при $k \neq i$.*

ДОКАЗАТЕЛЬСТВО. Из разложения

$$\prod_{k=0}^{l-1} \omega_k = x^l + y^l \tag{4}$$

следует, что

$$\prod_{k=0}^{l-1} \mathcal{A}_k = \mathcal{X}^l, \quad \sum_{k=0}^{l-1} n_k = ld. \tag{5}$$

Имеем также очевидные соотношения

$$\omega_k - \omega_t = (\zeta^k - \zeta^t)y, \quad \zeta^k \omega_t - \zeta^t \omega_k = (\zeta^k - \zeta^t)x. \tag{6}$$

Поскольку $\text{div}(\zeta^k - \zeta^t) = \ell_0 = \ell^{l^n}$ при $k \neq t$, то из (5), (6) следует, что $\text{mcd}(\omega_k, \omega_t) = \mathcal{M} \ell^d$ (при $k \neq t$) и $n_k = d$ при $d < l^n$, а при $d \geq l^n$ $\text{mcd}(\omega_k, \omega_t) = \mathcal{M} \ell_0$ и $n_k \geq l^n$. В частности, $\mathcal{A}_k$ – попарно взаимно простые дивизоры, так что $\mathcal{A}_k = \mathcal{C}_k^l$ вследствие (5). Поскольку

$$(\zeta^k - 1)(\zeta - 1)^{-1} = \zeta^{k-1} + \dots + 1 \equiv k \pmod{\ell},$$

то

$$\omega_k y^{-1} (\zeta - 1)^{-1} = \omega_0 y^{-1} (\zeta - 1)^{-1} + (\zeta^k - 1)(\zeta - 1)^{-1}$$

пробегают $\pmod{\ell_n}$ полную систему вычетов. Значит, $\ell_0 \ell$ делит $\text{div}(\omega_i) \mathcal{M}^{-1}$ для некоторого единственного i , а $n_k = l^n$ для $k \neq i$. Из (5) имеем $ld = (l-1)l^n + n_i$, так что $n_i = l^n + l(d - l^n)$, а $d > l^n$, так как $n_i \geq l^n + 1$.

Имеется канонический инъективный гомоморфизм группы $(\mathbb{Z}/l\mathbb{Z})^*$ в группу Галуа G поля $L_\infty = \bigcup_n L_n$ над $\mathbb{Q}$, при котором $a \mapsto \sigma_a$ такой, что $\zeta^{\sigma_a} = \zeta^a$. Если $c \in \mathbb{Q}$, $c - l$ -целое число, то σ_c обозначает $\sigma_{\bar{c}}$, где $\bar{c} = c \pmod{l}$. Зафиксируем натуральное число $1 < c < l$ такое, что $c \pmod{l}$ есть образующая $(\mathbb{Z}/l\mathbb{Z})^*$. Определим $\delta \in \mathbb{Z}[G]$, полагая $\delta = \prod_{l \mid B_{l-m}} (\sigma_c - c^m)$, где произведение берется по нечетным m , $3 \leq m \leq l-2$, таким, что $l \mid B_{l-m}$, $\delta = 1$, если l регулярно. Пусть $\sigma = \sigma_{-1}$ – сужение автоморфизма комплексного сопряжения на L_∞ . Имеет место

ПРЕДЛОЖЕНИЕ 2. а) Пусть $n \geq 1$, (x, y, γ) – решение (2) в O'_L , причем γ , y взаимно просты с ℓ . Тогда

$$\left(\frac{\omega_k}{\omega_0}\right)^{(1-\sigma)\delta} \in (L^*)^l. \quad (7)$$

б) Пусть l регулярно и (x, y, γ) – решение (2) в O'_L такое, что x, y взаимно просты с ℓ , а $x + y$ делится на ℓ_0^{l+1} . Тогда при $k = 1, \dots, l-1$

$$b_k = \varepsilon \frac{\omega_k}{\omega_0(1-\zeta^k)l} \in (L^*)^l. \quad (8)$$

ДОКАЗАТЕЛЬСТВО. Докажем сначала п. а) предложения. Из предложения 1 следует, что

$$\operatorname{div}(\omega_k) = \mathcal{M}\mathcal{C}_k^l, \quad \operatorname{div}(\omega_0) = \mathcal{M}\mathcal{C}_0^l.$$

Значит, $\operatorname{div}(\omega_k/\omega_0) = (\mathcal{C}_k/\mathcal{C}_0)^l$, т.е. порядок образа $\mathcal{C}_k/\mathcal{C}_0$ в группу классов дивизоров поля L делит l . Из соотношений Штикельберга следует, что δ аннулирует l -периодическую подгруппу группы классов дивизоров поля L , так что $(\mathcal{C}_k/\mathcal{C}_0)^\delta$ есть главный дивизор, т.е. $(\omega_k/\omega_0)^\delta = u(v')^l$, где u – единица L , а v' – ℓ -целое ненулевое число L . Известно (см. [2, гл. 3, §1, лемма 4], доказательство легко переносится на случай поля L), что $u^{1-\sigma} = \pm \zeta_n^\alpha$, где ζ_n – примитивный корень l^{n+1} -ой степени из 1, $\alpha \in \mathbb{Z}$. Значит, $(\omega_k/\omega_0)^{(1-\sigma)\delta} = \zeta_n^\alpha v^l$, где v – ℓ -целое ненулевое число L . Поскольку

$$\frac{\omega_k}{\omega_0} = \frac{x + y + (\zeta^k - 1)y}{x + y} = 1 + (\zeta^k - 1)\frac{y}{x + y} \equiv 1 \pmod{\ell^{l^n}},$$

то $\zeta_n^\alpha \equiv 1 \pmod{\ell^l}$. Значит, α делится на l , так как иначе $\operatorname{div}(\zeta_n^\alpha - 1) = \ell$.

Перейдем к доказательству п. б) предложения. Пусть $x + y = (\zeta - 1)^{l+1}\beta$, где $\beta \in O_L$. Тогда $x = -y + (\zeta - 1)^{l+1}\beta$, откуда

$$x^l = (-y)^l + y^{l-1}(\zeta - 1)^{l+1}\beta l \pmod{l(\zeta - 1)^{2(l+1)}}.$$

Значит,

$$(x + y)l = (\zeta - 1)^{l+1}l\beta = y^{1-l}(x^l + y^l)(1 + (\zeta - 1)^{l+1}\eta_1),$$

где η_1 – ℓ -целое число L . Далее,

$$\frac{x + \zeta^k y}{1 - \zeta^k} = \frac{x + y + (\zeta^k - 1)y}{1 - \zeta^k} = -y(1 + (\zeta - 1)^l \eta_2),$$

где η_2 – ℓ -целое число L . Из полученных равенств, учитывая (2), получим, что $\varepsilon\omega_k/(\omega_0 l(1 - \zeta^k)) = (-y/\gamma)^l a$, где $a = 1 + (\zeta - 1)^l \eta_3$, η_3 – ℓ -целое число L . Кроме того, из предложения 1 следует, что $\operatorname{div}(a)$ есть l -я степень. Известно, что свойства a влекут, что $L(\sqrt[l]{a})$ неразветвлено над L , а следовательно, a есть l -я степень в L^* , так как по теории полей классов поле L не имеет нетривиальных неразветвленных абелевых расширений l -ой степени, поскольку число классов дивизоров поля L не делится на l .

Приступим теперь к доказательству теоремы 1. Пусть $s = (x, y, \gamma)$ – решение (2) в O'_L такое, что x, y взаимно просты с ℓ , а γ делится на ℓ_0^2 . Заменяя y на $\zeta^{-i}y$, можем

без ограничения общности считать, что $x + y$ делится на ℓ_0^{l+1} . Пусть $p(s)$ – число простых дивизоров поля L , делящих $\mathcal{Z}$. Мы докажем существование решения $s_1 = (x_1, y_1, \gamma_1)$ уравнения (2), отвечающего некоторой единице ε_1 поля L , такого, что x_1, y_1 взаимно просты с ℓ , γ_1 делится на ℓ_0^2 и $p(s) - p(s_1) \geq 1$. Тогда для всякого натурального числа N по индукции можно построить решение s_N такое, что $p(s) - p(s_N) \geq N$, так что $p(s) \geq N$. Так как это невозможно, то решение s не может существовать, что и утверждает теорема 1.

Займемся построением решения s_1 по решению s . Положим

$$f_k = \frac{\omega_k}{\omega_0(1 - \zeta^k)}.$$

Следующее соотношение, проверяемое непосредственно как тождество в $L(x, y)$, играет вместе с (8) важную роль в осуществлении спуска решений (2) в поле L (построения решения s_1 по решению s):

$$f_k f_{-k} - f_t f_{-t} = (\zeta^{-t} - \zeta^{-k})(1 - \zeta^{k+t})((1 - \zeta^k)(1 - \zeta^t)(1 - \zeta^{-k})(1 - \zeta^{-t}))^{-1}. \quad (9)$$

Обозначим правую часть (9) через $\xi_{k,t}$. Заметим, что $\xi_{k,t}$ вещественна.

Выберем вещественное $a \in O_L$ такое, что $\text{div}(a) = \mathcal{C}_0 \mathcal{N}$, где $\mathcal{N} \in T$. Положим $\kappa = (1 - \zeta_n)(1 - \zeta_n^{-1})$. Выберем ненулевые k, t такие, что $k \not\equiv \pm t \pmod{l}$ (это возможно, так как $l \geq 5$), и, учитывая (8), $x', y', \gamma' \in O'_L$ такие, что

$$(x')^l = b_k b_{-k} \kappa^{ld} a^{2l}, \quad (y')^l = -b_t b_{-t} \kappa^{ld} a^{2l}, \quad (\gamma')^l = \kappa^{l(d-l^n)} a^{2l}. \quad (10)$$

Пусть $\varepsilon' = \varepsilon^{2l-2} \kappa^{l^{n+1}} \xi_{k,t}$ – единица L . Из (9) следует, что $(x')^l + (y')^l = \varepsilon' (\gamma')^l$. Положим $s' = (x', y', \gamma')$. Из предположения 1 следует, что $\text{div}(\omega_r / \omega_0) = \mathcal{A}_r (\mathcal{A}_0 \ell^{l(d-l^n)})^{-1}$. Поскольку $\text{div}((1 - \zeta^r)l) = \ell_0^l = \ell^{l^{n+1}}$, то $\text{div}(b_r) = \mathcal{A}_r (\mathcal{A}_0 \ell^{ld})^{-1}$. Учитывая, что $\text{div}(\kappa) = \ell^2$, $\text{div}(a^l) = \mathcal{C}_0^l \mathcal{N}^l$, $\mathcal{A}_r = \mathcal{C}_r^l$, находим

$$\text{div}(x') = \mathcal{C}_k \mathcal{C}_{-k} \mathcal{N}^2, \quad \text{div}(y') = \mathcal{C}_t \mathcal{C}_{-t} \mathcal{N}^2, \quad \text{div}(\gamma') = \mathcal{C}_0^2 \ell^{2(d-l^n)} \mathcal{N}^2.$$

Значит, $d(s') = 2(d - l^n) \geq 2l^n$, так как $d = d(s) \geq 2l^n$ по условию. Поскольку $\mathcal{Z}(s') = \mathcal{C}_0^2$, $\mathcal{Z}(s) = \prod_{r=0}^{l-1} \mathcal{C}_r$, а $\mathcal{C}_r$ попарно взаимно просты, то $p(s') \leq p(s)$ и $p(s') < p(s)$, если $\mathcal{C}_k \neq 1$ хотя бы для одного ненулевого k . В противном случае при $k \neq 0$ $\chi = \omega_k / \omega_{-k}^{-1}$ является единицей, поскольку $\text{div}(\omega_{\pm k}) = \mathcal{C}_{\pm k}^l \mathcal{M} = \mathcal{M}$, так что $\text{div}(\chi) = 1$. Заметим, что

$$\chi = \frac{x + \zeta^k y}{x + \zeta^{-k} y} = \frac{x + y + (\zeta^k - 1)y}{x + y + (\zeta^{-k} - 1)y} \equiv \frac{\zeta^k - 1}{\zeta^{-k} - 1} \equiv -\zeta^k \pmod{\ell_0^l},$$

так как $x + y$ делится на ℓ_0^{1+l} . Если x, y вещественны, то $\chi = \pm \zeta_n^j$, будучи единицей L такой, что $\chi^\sigma = \chi^{-1}$. Поэтому $\pm \zeta_n^j = \chi \equiv -\zeta^k \pmod{\ell_0^l}$, откуда $\chi = -\zeta^k$. Значит,

$$x + \zeta^k y = -\zeta^k (x + \zeta^{-k} y) = -\zeta^k x - y,$$

т.е. $(x + y)(1 + \zeta^k) = 0$, что невозможно, так как $1 + \zeta^k \neq 0$ и $x + y \neq 0$, так как $\gamma \neq 0$ и имеет место (2), т.е. если x, y вещественны, то $p(s') < p(s)$ и мы располагаем нужным нам решением, полагая $s_1 = s'$.

В общем случае если $p(s') < p(s)$, то полагаем $s_1 = s'$. Если же $p(s') = p(s)$, то $\chi^{1-\sigma} = \pm \zeta_n^j \equiv \zeta^{2k} \pmod{\ell_0^l}$, откуда $\chi^{1-\sigma} = \zeta^{2k}$, т.е.

$$\begin{aligned} (x + \zeta^k y)(x^\sigma + \zeta^k y^\sigma) &= \zeta^{2k}(x + \zeta^{-k} y)(x^\sigma + \zeta^{-k} y^\sigma) \Leftrightarrow \\ &\Leftrightarrow xx^\sigma + xy^\sigma \zeta^k + yx^\sigma \zeta^k + \zeta^{2k} yy^\sigma = \zeta^{2k} xx^\sigma + xy^\sigma \zeta^k + yx^\sigma \zeta^k + yy^\sigma \Leftrightarrow \\ &\Leftrightarrow (xx^\sigma - yy^\sigma)(1 - \zeta^{2k}) = 0 \Leftrightarrow xx^\sigma = yy^\sigma \Leftrightarrow (x/y)^\sigma = y/x. \end{aligned}$$

Тогда

$$\begin{aligned} f_k^\sigma &= \frac{x^\sigma + \zeta^{-k} y^\sigma}{x^\sigma + y^\sigma} \cdot \frac{x^\sigma + \zeta^k y^\sigma}{x^\sigma + y^\sigma} = \frac{1 + \zeta^{-k}(y/x)^\sigma}{1 + (y/x)^\sigma} \cdot \frac{1 + \zeta^k(y/x)^\sigma}{1 + (y/x)^\sigma} \\ &= \frac{1 + \zeta^{-k}(x/y)}{1 + (x/y)} \cdot \frac{1 + \zeta^k(x/y)}{1 + (x/y)} = \frac{\zeta^{-k}(x + \zeta^k y)}{x + y} \cdot \frac{\zeta^k(x + \zeta^{-k} y)}{x + y} = f_k, \end{aligned}$$

т.е. f_k вещественно.

Пусть $\varepsilon = \zeta_n^j \varepsilon_0$, где $\varepsilon_0^\sigma = \varepsilon_0$. Поскольку

$$\varepsilon \gamma^l = x^l + y^l = (x + y)^l \prod_{k=1}^{(l-1)/2} f_k,$$

то $\zeta_n^{2j} = \varepsilon^{1-\sigma} \in (L^*)^l$. Значит, $j = li$ и $x^l + y^l = \varepsilon_0 \gamma_0^l$, где $\gamma_0 = \gamma \zeta_n^i$. Заменим s на решение $s_0 = (x, y, \gamma_0)$ уравнения (2), отвечающего вещественной единице ε_0 . Очевидно, $p(s_0) = p(s)$. Тогда правые части равенств (10) (соответствующих решению s_0) будут вещественны, поэтому x', y' можно выбрать вещественными (если $x^{l(1-\sigma)} = 1$, то $x^{1-\sigma} = \zeta^{2j}$, тогда $(x \zeta^{-j})^{1-\sigma} = 1$). Заметим, что $x' + y'$ делится на ℓ_0^{l+1} , так как иначе $\text{ord}_\ell(x' + y') = l^n$, что невозможно, так как $\text{ord}_\ell(x' + y')$ делится на 2, поскольку $x' + y'$ вещественно, т.е. мы построили решение $s'_0 = (x', y', \gamma')$ с вещественными x', y' такое, что $p(s'_0) \leq p(s_0) = p(s)$. Но для такого решения s'_0 мы доказали выше существование решения s_1 такого, что $p(s_1) < p(s'_0)$. Поскольку очевидно, что $p(s_1) < p(s)$, то решение s_1 будет искомым и доказательство теоремы 1 завершено.

Куммер первоначально использовал при проведении спуска в L_0 более простое соотношение

$$f_k - f_t = (\zeta^k - \zeta^t)((1 - \zeta^k)(1 - \zeta^t))^{-1} \quad (11)$$

и $d(s)$ в качестве параметра спуска.

Тогда, полагая $\eta = 1 - \zeta_n$, выберем $x', y', \gamma' \in O_L$, удовлетворяющие условиям

$$(x')^l = b_k \eta^{ld} a^l, \quad (y')^l = -b_t \eta^{ld} a^l, \quad (\gamma')^l = \eta^{l(d-l^n)} a^l, \quad (12)$$

и положим $\varepsilon' = \varepsilon l^{-1} \eta^{l^{n+1}} \rho_{k,t}$, где $\rho_{k,t}$ — правая часть (11). Тогда $(x')^l + (y')^l = \varepsilon' (\gamma')^l$ и $d(s') = d(s) - l^n \geq l^n$. Из предложения 1 следует, что $d(s') \geq l^n + 1$, что в случае $n = 0$ совпадает с неравенством $d(s') \geq 2l^n$. Так что при $n = 0$ s' можно использовать в качестве s_1 , а $d(s)$ в качестве параметра спуска. Однако при $n > 0$ условие $d(s') \geq 2l^n$ уже не гарантировано, так что s' может не удовлетворять нужным условиям.

В работе [7] Вандивер, развивая последующие идеи Куммера, использовал при исследовании решений (2) в R_0 соотношения (9) и $p(s)$ как параметр спуска. Как видно из вышеизложенного, этот вариант спуска удастся адаптировать к доказательству теоремы 1.

§ 2. Доказательство теорем 2 и 3

Напомним, что $l > 3$ – простое число (условие регулярности на l не накладывается).

Обозначим через K_n ℓ_n -адическое пополнение L_n , а через $K_{n,j}$, $j = 2, 3$, – $\ell_{n,j}$ -адическое пополнение соответственно поля R_n (при $j = 2$) и поля H_n (при $j = 3$), где $\ell_{n,j}$ – единственный простой дивизор соответствующего поля, делящийся на ℓ_n . Будем иногда обозначать K_n через $K_{n,1}$.

Если $x, y \in K_n$, $x + y \neq 0$, то $\omega_k(x, y)$ обозначает $(x + \zeta^k y)/(x + y)$. Ключевую роль в доказательстве теорем 2 и 3 играет следующее

ПРЕДЛОЖЕНИЕ 3. Пусть $n \geq 1$.

а) Пусть (x, y, z) – тройка единиц K_n такая, что $x^l + y^l + z^l = 0$ и для всякой перестановки (x_1, y_1, z_1) тройки (x, y, z) и $k \in \mathbb{Z}/l\mathbb{Z}$

$$\omega_k(x_1, y_1)^{(1-\sigma)\delta} \in (K_n^*)^l. \quad (13)$$

Тогда $N_1(t) < n$, где $t = -x/y \pmod{\ell_n}$, а если $j \in \{2, 3\}$ и $x, y, z \in K_{n,j}$, то $N_j(t) < n$.

б) Пусть $j \in \{1, 3\}$, $n \leq (l-3)/(2(I(l)+1))$ в случае $j = 1$, $n \leq (l-3)/2 - I(l)$ в случае $j = 3$. Пусть $x, y \in K_{n,j}$ такие, что $x \equiv 0 \pmod{\ell_n}$, y – единица и

$$\omega_k(x, y)^{(1-\sigma)\delta} \in (K_n^*)^l. \quad (14)$$

Пусть в случае $j = 1$ $d_n = 2n(I(l)+1)$, в случае $j = 3$ d_n – n -е по порядку нечетное натуральное число $< l-3$ такое, что $l \nmid B_{l-d_n}$. Тогда $x \equiv 0 \pmod{\ell_0^{l-1-d_n}}$ в случае $j = 1$, $x \equiv 0 \pmod{\ell_0^{l-1-d_n} \ell_n^{d_n}}$ в случае $j = 3$.

Фактически мы докажем предложение 3 в более общей формулировке, которая получается заменой в определении δ и $N_j(t)$ множества чисел m таких, что $l \mid B_{l-m}$, на любое множество нечетных чисел из отрезка $[1, l-3]$ и заменой $I(l)$ на количество чисел в этом множестве. Также можно заменить $(1-\sigma)\delta$ на δ и рассматривать любое множество натуральных чисел из отрезка $[1, l-3]$, опуская в определении $c(t)$ требование его четности и опуская случай $j = 2$.

Если (x, y, z) – тройка единиц поля K_n , удовлетворяющая уравнению (1), то

$$x + y + z \equiv x^l + y^l + z^l = 0 \pmod{\ell_n}$$

и любая перестановка (x_1, y_1, z_1) тройки (x, y, z) удовлетворяет (1). Поэтому п. а) предложений 2 и 3 влекут п. а) теоремы 3 в случае $n \geq 1$ (случай $n = 0$ следует из [4], см. введение). Также очевидно, что п. а) предложения 2 и п. б) предложения 3 влекут п. б) теоремы 3 в случае $n \geq 1$, а при $n = 0$ она следует из предложения 1.

Доказательство предложения 3 составит последующее содержание этого параграфа.

Пусть S_n – кольцо целых чисел поля K_n , $V_n = \{u \in S_n, u \equiv 1 \pmod{\ell_n}\}$ – группа главных единиц поля K_n . Ряд

$$\log(1+x) = \sum_{i=1}^{\infty} (-1)^{i-1} (x^i/i)$$

сходится при $x \in S_n$ таком, что $\ell_n | x$, так что определено отображение $\log: V_n \rightarrow K_n$, являющееся гомоморфизмом группы V_n в аддитивную группу поля K_n . При этом ряд

$$\exp(y) = \sum_{i=1}^{\infty} y^i / i!$$

сходится при $y \in S_n$, $y \equiv 0 \pmod{\ell_0 \ell_n}$ и $\forall m \geq 1$ отображение $\log$ индуцирует изоморфизм группы $(1 + \ell_0 \ell_n^m S_n)$ на $\ell_0 \ell_n^m S_n$, причем обратный изоморфизм задается отображением $y \mapsto \exp(y)$ (см. [2, гл. 4, § 5, теорема 3], а также [8, предложение 7.17]).

Группа V_0 есть прямое произведение группы μ_0 корней l -ой степени из 1 и $(1 + \ell_0^2 S_0)$. Поскольку $\log(\mu_0) = 0$ (так как K_0 не имеет нетривиального кручения), то $\log(V_0) = 1 + \ell_0^2 S_0$ и $v \in V_0$ является l -ой степенью тогда и только тогда, когда $v \equiv 1 \pmod{\ell_0^{l+1}}$. В случае $n \geq 1$ положение уже не такое простое. Группа $\log(V_n)$ имеет более сложную структуру (см. ниже), в частности $\log(V_n) \not\subset S_n$. Условие $v \equiv 1 \pmod{\ell_0^l \ell_n}$ является достаточным, но не необходимым, условием того, что $v \in V_n^l$, и анализировать следствия соотношений (13) и (14) становится сложнее.

Нам потребуется явное описание группы $\log(V_n)$, полученное Ивасавой (см. конец работы [9]).

Пусть G_n обозначает группу Галуа поля K_n над $\mathbb{Q}_l$. Пусть $\kappa: G_n \rightarrow (\mathbb{Z}/l^{n+1}\mathbb{Z})^*$ обозначает канонический изоморфизм, определяемый условием $\zeta_n^g = \zeta_n^{\kappa(g)}$.

Пусть при $i \geq 0$ ζ_i обозначает примитивный корень l^{i+1} -ой степени из 1, причем $\zeta_{i+1}^l = \zeta_i$. Положим

$$\eta_n = l^{-n} \left(\sum_{i=0}^n l^i (\zeta_i - 1) \right).$$

Тогда $\log(V_n)$ состоит из всех линейных комбинаций $al + \sum_g a_g g(\eta_n)$ с произвольными l -адическими целыми числами a и $\{a_g, g \in G_n\}$, удовлетворяющими условию

$$\sum_g \kappa(g) a_g \equiv 0 \pmod{l^{n+1}}.$$

Пусть C_n обозначает $\sum_{i=1}^{l-1} K_{n-1} \zeta_n^i$, A_n обозначает $\sum_{i=1}^{l-1} S_{n-1} \zeta_n^i$. Имеем разложение $K_n = K_{n-1} + C_n$ поля K_n в прямую сумму K_{n-1} -векторных пространств и соответствующее разложение $S_n = S_{n-1} + A_n$ кольца S_n в прямую сумму S_{n-1} -модулей. Поскольку $K_n = \mathbb{Q}_l[S_n]$, $S_n = \mathbb{Z}_l[\zeta_n]$, то C_n, A_n есть соответственно $\mathbb{Q}_l$ -, $\mathbb{Z}_l$ -линейная оболочка множества $\{\zeta_n^i, i \in (\mathbb{Z}/l^{n+1}\mathbb{Z})^*\} = \{g(\zeta_n), g \in G_n\}$. Заметим также, что A_n есть прямая сумма $\sum_{i=0, (i,l)=1}^{l^n-1} S_0 \zeta_n^i$, так как ζ_n^i , $0 \leq i < l^n$, образуют базис K_n над K_0 .

Следующая лемма нам потребуется при доказательстве предложения 3. Пусть π_i обозначает $\zeta_i - 1$, так что $\text{div}(\pi_i) = \ell_i$.

ЛЕММА 1. Пусть $c \in \log(V_n)$, $c = d + b$, где $d \in K_{n-1}$, $b \in C_n$. Если $b \in \pi_0 S_n$, то $d \in \log(V_{n-1})$.

ДОКАЗАТЕЛЬСТВО. Пусть

$$c = la + \sum_g a_g g(\eta_n),$$

где $\sum \kappa(g)a_g \equiv 0 \pmod{l^{n+1}}$, в соответствии с приведенным выше описанием $\log(V_n)$. Очевидно,

$$b = \sum_g a_g g(\zeta_n) = \sum_g a_g \zeta_n^{\kappa(g)} \equiv \sum_{i=0, (i,l)=1}^{l^n-1} a(i) \zeta_n^i \pmod{\pi_0},$$

где $a(i) = \sum_{g|\kappa(g) \equiv i \pmod{l^n}} a_g$. Так как $b \equiv 0 \pmod{\pi_0}$ по условию, то $a(i) \equiv 0 \pmod{\pi_0}$. Для $h \in G_{n-1}$ положим $a_h = a(\kappa(h))/l \in \mathbb{Z}_l$. Поскольку $d = al + \sum_h a_h h(\eta_{n-1})$, то остается (учитывая описание $\log(V_{n-1})$) лишь заметить, что

$$\sum_h a_h \kappa(h) = \sum_h \kappa(h) \frac{\sum_{g|\kappa(g) \equiv \kappa(h) \pmod{l^n}} a_g}{l} \equiv \frac{\sum_g \kappa(g) a_g}{l} \equiv 0 \pmod{l^n}.$$

Кроме отображения $\log$ нам потребуется использовать логарифмические производные Ω_n , которые мы определим ниже.

Положим $\rho_n = l^{n+1}/\pi_0$. Определим отображение $D_n: S_n \rightarrow S_n/\rho_n S_n$, полагая $D_n(P(\zeta_n)) = P'(\zeta_n)\zeta_n$, где $P \in \mathbb{Z}_l[X]$, P' — обычная производная от многочлена $P(X)$. Ядро эпиморфизма $\mathbb{Z}_l[X] \rightarrow S_n$ такого, что $P(X) \mapsto P(\zeta_n)$, есть идеал $\mathbb{Z}_l[X]Q_n$, где $Q_n = (X^{l^{n+1}} - 1)/(X^{l^n} - 1)$. Поскольку

$$Q'_n = l^{n+1}X^{l^{n+1}-1}/(X^{l^n} - 1) - l^n X^{l^n-1}(X^{l^{n+1}} - 1)/(X^{l^n} - 1)^2,$$

то $Q'_n(\zeta_n) = l^{n+1}\zeta_n^{-1}/(\zeta_0 - 1) = -\zeta_n^{-1}\rho_n$. Значит, D_n является корректно определенным дифференцированием кольца S_n в кольцо $S_n/\rho_n S_n$.

Имеет место

ЛЕММА 2. Пусть $n \geq 1$. Если $b \in A_n$ и $D_n(b) \equiv 0 \pmod{\pi_0^j}$, где $1 \leq j \leq l-1$, то $b \in \pi_0^j A_n$.

ДОКАЗАТЕЛЬСТВО. Пусть $b = \sum_{i=1, (i,l)=1}^{l^n-1} a_i \zeta_n^i$, где $a_i \in S_0$. Тогда

$$D_n(b) = \sum_i (ia_i + D_n(a_i))\zeta_n^i \equiv 0 \pmod{\pi_0^j} \Rightarrow \forall i \quad ia_i + D_n(a_i) \equiv 0 \pmod{\pi_0^j}.$$

Но $D_n(a_i) = l^n D_0(a_i) \equiv 0 \pmod{\pi_0^j}$. Значит, $\forall i \quad a_i \equiv 0 \pmod{\pi_0^j}$ и, следовательно, $b \in \pi_0^j A_n$.

Пусть U_n обозначает группу единиц поля K_n . Определим отображение $\Omega_n: U_n \rightarrow S_n/\rho_n S_n$, полагая $\Omega_n(u) = D_n(u)u^{-1}$. Поскольку D_n — дифференцирование, то Ω_n является гомоморфизмом группы U_n в аддитивную группу кольца $S_n/\rho_n S_n$.

Через λ обозначим единственный простой элемент S_0 такой, что $\lambda^{l-1} + l = 0$, $\lambda \equiv \pi_0 \pmod{\lambda^2}$ (см. [2, гл. 5, § 6, лемма 1]). Положим

$$E(X) = \sum_{i=0}^{l-1} \frac{X^i}{i!} \in \mathbb{Z}_l[X], \quad \zeta = \zeta_0.$$

Имеет место сравнение (см. [2, гл. 5, § 6, лемма 3])

$$\zeta^k \equiv E(k\lambda) \pmod{\lambda^l}. \quad (15)$$

Напомним, что рациональные функции $f_n(Y)$ определены с помощью разложения (3).

Пусть $\alpha \in K_n^*$, $\alpha \not\equiv -1 \pmod{\ell_n}$. Положим $g(Y) = f(Y)Y^{-1}$. Поскольку

$$-\alpha^{-1} \left(\frac{1}{1 + \alpha E(X)} - \frac{1}{1 + \alpha} \right) = \sum_{i=1}^{l-1} g_i(-\alpha) \frac{X^i}{i!} + x^l P(X),$$

где $P(X) \in S_n[X]$, то из (15) следует сравнение

$$-\alpha^{-1} \left(\frac{1}{1 + \alpha \zeta^k} - \frac{1}{1 + \alpha} \right) \equiv \sum_{i=1}^{l-1} g_i(-\alpha) \frac{(k\lambda)^i}{i!} \pmod{\lambda^l}. \quad (16)$$

Положим $\kappa_d(\alpha) = \prod_{k=1}^{l-1} ((\alpha + \zeta^{1/k})/(\alpha + 1))^{k^d}$ для $d = 1, 2, \dots, l-1$.

Имеет место

ЛЕММА 3. Пусть $n \geq 1$. Пусть α такое, как выше. Имеет место сравнение

$$\Omega_n(\kappa_d(\alpha)) \equiv \frac{(-1)^{d+1}}{d!} D_n(\alpha) g_d(-\alpha) \lambda^d \pmod{l}. \quad (17)$$

ДОКАЗАТЕЛЬСТВО. Имеем

$$\Omega_n \left(\frac{\alpha + \zeta^k}{\alpha + 1} \right) = \Omega_n(\alpha + \zeta^k) - \Omega_n(\alpha + 1) = D_n(\alpha) \left(\frac{1}{\alpha + \zeta^k} - \frac{1}{\alpha + 1} \right) \pmod{l},$$

так как $D_n(\zeta^k) = l^n D_0(\zeta^k)$, а $n \geq 1$ по условию. Далее имеем

$$\begin{aligned} \frac{1}{1 + \alpha \zeta^k} - \frac{1}{\alpha + 1} &= \alpha^{-1} \left(\frac{\alpha}{\alpha + \zeta^k} - \frac{\alpha}{\alpha + 1} \right) = -\alpha^{-1} \left(\frac{\zeta^k}{\alpha + \zeta^k} - \frac{1}{\alpha + 1} \right) \\ &= -\alpha^{-1} \left(\frac{1}{1 + \alpha \zeta^{-k}} - \frac{1}{\alpha + 1} \right). \end{aligned}$$

Учитывая сравнение (16), получаем

$$\begin{aligned} \Omega_n(\kappa_d(\alpha)) &= \sum_{k=1}^{l-1} k^d D_n(\alpha) \left(\frac{1}{\alpha + \zeta^{1/k}} - \frac{1}{\alpha + 1} \right) \\ &\equiv D_n(\alpha) \sum_{i=1}^{l-1} (-1)^i g_i(-\alpha) \left(\sum_{k=1}^{l-1} k^{d-i} \right) \frac{\lambda^i}{i!} \equiv \frac{(-1)^{d+1}}{d!} D_n(\alpha) g_d(-\alpha) \lambda^d \pmod{l}, \end{aligned}$$

так как $\sum k^{d-i} \equiv 0 \pmod{l}$ при $i \neq d$.

Нам потребуется также следующая

ЛЕММА 4. Пусть $\alpha \in S_n$, $\alpha \not\equiv -1 \pmod{\ell_n}$, $1 \leq d \leq l-1$. Тогда

$$\log(\kappa_d(\alpha)) \equiv \frac{(-1)^d}{d!} (\alpha^l + 1)^{-1} \left(\sum_{i=1}^{l-1} (-\alpha)^i i^{d-1} \right) \lambda^d \pmod{\lambda^l \pi_n^{\nu(d)}},$$

где $\nu(1) = 0$, $\nu(d) = 1$ при $d > 1$.

ДОКАЗАТЕЛЬСТВО. Имеем

$$\frac{(\alpha + \zeta^k)^l}{\alpha^l + 1} = 1 + l\beta(k),$$

где $k \in \mathbb{Z}$, $\beta(k) = (\alpha^l + 1)^{-1} \sum_{i=1}^{l-1} (C_l^i/l) \alpha^i \zeta^{-ki}$ (заметим, что $\beta(k)$ зависит лишь от $k \pmod{l}$). Отсюда

$$((\alpha + \zeta^k)/(\alpha + 1))^l = (1 + l\beta(k))/(1 + \beta(0)).$$

Значит,

$$\log \frac{\alpha + \zeta^k}{\alpha + 1} = \sum_{r=1}^{\infty} (-1)^{r-1} \frac{l^{r-1}}{r} (\beta(k)^r - \beta(0)^r)$$

и, следовательно,

$$\begin{aligned} \log(\kappa_d(\alpha)) &= \sum_{k=1}^{l-1} k^d \left(\beta\left(\frac{1}{k}\right) - \beta(0) \right) \\ &\quad + \sum_{r=2}^{\infty} (-1)^{r-1} \frac{l^{r-1}}{r} \sum_{k=1}^{l-1} k^d \left(\beta\left(\frac{1}{k}\right)^r - \beta(0)^r \right). \end{aligned} \quad (18)$$

Покажем, что $\beta(k) - \beta(0) \equiv 0 \pmod{\lambda \pi_n}$. Из (15) следует, что $(\zeta^{-ki} - 1) \equiv -ki\lambda \pmod{\lambda^2}$. Учитывая также, что

$$C_l^i/l = (l-1) \dots (l-(i-1))/i! \equiv (-1)^{i-1}/i \pmod{l},$$

имеем

$$\begin{aligned} \beta(k) - \beta(0) &\equiv (\alpha^l + 1)^{-1} \sum_{i=1}^{l-1} (-\alpha)^i k \lambda \\ &= (\alpha^l + 1)^{-1} \left(\frac{(-\alpha)^l - 1}{-\alpha - 1} - 1 \right) k \lambda \pmod{\lambda^2} \equiv 0 \pmod{\lambda \pi_n}, \end{aligned}$$

так как $(-\alpha)^l \equiv -\alpha \pmod{\pi_n}$.

Пусть $\mathcal{H}$ обозначает группу корней $(l-1)$ -ой степени из 1 в $\overline{\mathbb{Q}}_l$. Как известно, $\mathcal{H} \subset \mathbb{Z}_l$ и отображение $\Theta \mapsto \Theta \pmod{l}$ задает изоморфизм $\mathcal{H}$ и $(\mathbb{Z}/l\mathbb{Z})^*$. Пусть для $k \in \mathbb{Z}_l^*$ Θ_k обозначает элемент $\mathcal{H}$ такой, что $\Theta_k \equiv k \pmod{l}$.

Учитывая, что $\beta(1/k) - \beta(0) \equiv 0 \pmod{\lambda\pi_n}$, имеем

$$\begin{aligned} \sum_{k=1}^{l-1} k^d (\beta(1/k) - \beta(0)) &\equiv \sum_{k=1}^{l-1} \Theta_k^d (\beta(1/k) - \beta(0)) \pmod{\lambda^l \pi_n} \\ &= (\alpha^l + 1)^{-1} \sum_{i=1}^{l-1} \frac{C_l^i}{l} \alpha^i \sum_{k=1}^{l-1} \Theta_k^d (\zeta^{-i/k} - 1) \\ &= (\alpha^l + 1)^{-1} \left(\sum_{i=1}^{l-1} \frac{C_l^i}{l} \alpha^i \Theta_{-i}^d \right) \left(\sum_{k=1}^{l-1} \Theta_k^d (\zeta^{1/k} - 1) \right) \pmod{\lambda^l \pi_n}. \end{aligned}$$

Из сравнения (15) следует, что

$$\zeta - 1 = \sum_{i=1}^{l-1} \frac{\lambda^i}{i!} + l \sum_{i=1}^{l-1} \lambda^i a_i, \quad \text{где } a_i \in \mathbb{Z}_l. \quad (19)$$

Продолжая автоморфизм σ_k (см. § 1) по непрерывности на K_∞ , имеем $\frac{\sigma_k(\lambda)}{\lambda} \in \mathcal{H}$, так как $\lambda^{l-1} = -l$. Кроме того, поскольку $\lambda \equiv \zeta - 1 \pmod{\lambda^2}$, то $\sigma_k(\lambda)/\lambda \equiv (\zeta^k - 1)/(\zeta - 1) \equiv k \pmod{\lambda}$. Значит, $\sigma_k(\lambda) = \Theta_k \lambda$.

Поэтому, учитывая (19), имеем

$$\begin{aligned} \sum_{k=1}^{l-1} \Theta_k^d (\zeta^{1/k} - 1) &= \sum_{k=1}^{l-1} \Theta_k^d \sigma_{1/k}(\zeta - 1) = \sum_{i=1}^{l-1} \left(\frac{1}{i!} + l a_i \right) \left(\sum_{k=1}^{l-1} \Theta_k^{d-i} \right) \lambda^i \\ &= (l-1) \left(\frac{1}{d!} + l a_d \right) \lambda^d \equiv -\frac{\lambda^d}{d!} \pmod{\lambda^l \lambda^{d-1}} \equiv -\frac{\lambda^d}{d!} \pmod{\lambda^l \pi_n^{\nu(d)}}. \end{aligned}$$

Значит,

$$\begin{aligned} \sum_{k=1}^{l-1} k^d \left(\beta \left(\frac{1}{k} \right) - \beta(0) \right) &\equiv -(\alpha^l + 1)^{-1} \sum_{i=1}^{l-1} \left(\frac{C_l^i}{i} \right) \alpha^i \Theta_{-i}^d \left(\frac{\lambda^d}{d!} \right) \pmod{\lambda^l \pi_n^{\nu(d)}} \\ &\equiv \frac{(-1)^d}{d!} \left(\sum_{k=1}^{l-1} (-\alpha)^i i^{d-1} \right) \lambda^d \pmod{\lambda^l \pi_n^{\nu(d)}}. \end{aligned}$$

Далее, поскольку $\beta(s)^r = \sum_{j=0}^{l-1} a_{j,r} \zeta^{js}$, где $a_{j,r} \in S_n$, и вследствие (15)

$$\sum_{k=1}^{l-1} k^d (\zeta^{j/k} - 1) \equiv 0 \pmod{\lambda^d},$$

то имеем

$$\sum_{k=1}^{l-1} k^d \left(\beta \left(\frac{1}{k} \right)^r - \beta(0)^r \right) \equiv 0 \pmod{\lambda^d}.$$

Учитывая предыдущее и (18), для доказательства леммы остается лишь заметить, что $l^{r-1}/r \equiv 0 \pmod{l}$ при $r \geq 2$. Это так, поскольку показатель степени l , делящий l^r/r , больше (см. [2, гл. 4, § 5, (8)]), чем $r(1 - 1/(l-1)) > 1$ при $r \geq 2$.

Наконец, нам потребуется следующая лемма, легко вытекающая из леммы 4.

ЛЕММА 5. Пусть $n \geq 1$, $\alpha = \beta + \lambda^{l-1-m}b$, где $1 \leq m \leq l-3$, $b \in A_n$, $\beta \in S_{n-1}$, $0 \neq \beta \not\equiv -1 \pmod{\ell_{n-1}}$. Пусть $d \geq m$. Тогда

$$\log(\kappa_d(\alpha)) = \log(\kappa_d(\beta)) + ((-1)^{d+1}/d!)g_d(-\beta)\lambda^{l-1-m+d}b + \gamma,$$

где $\gamma \in \lambda^l \pi_n^{\nu(d)} S_n$.

ДОКАЗАТЕЛЬСТВО. Применяя лемму 4 для α и β , имеем

$$\begin{aligned} \log(\kappa_d(\alpha)) &\equiv \frac{(-1)^d}{d!}(\alpha^l + 1)^{-1} \left(\sum_{i=1}^{l-1} (-\beta - \lambda^{l-1-m}b)^i i^{d-1} \right) \lambda^d \\ &\equiv \frac{(-1)^d}{d!}(\beta^l + 1)^{-1} \left(\sum_{i=1}^{l-1} ((-\beta)^i - (-\beta)^{i-1} i \lambda^{l-1-m}b) i^{d-1} \right) \lambda^d \\ &\equiv \log(\kappa_d(\beta)) - \frac{(-1)^d}{d!}(\beta + 1)^{-l} \left(\sum_{i=1}^{l-1} (-\beta)^{i-1} i^d \right) \lambda^d \pmod{\lambda^l \pi_n^{\nu(d)}}. \end{aligned}$$

Остается учесть, что

$$g_d(-\beta) = (-\beta^{-1}) \frac{P_d(-\beta)}{(1+\beta)^{d+1}} \equiv (1+\beta)^{-l} \sum_{i=1}^{l-1} (-\beta)^{i-1} i^d \pmod{l}, \quad (20)$$

так как $P_d(Y)(1-Y)^{l-1-d} \equiv \sum_{i=1}^{l-1} (Y)^i i^d \pmod{l}$ (см. введение).

Пусть $x, y \in K_n$, $y \neq 0$, $0 \leq r \leq n$, $s = n - r$. Определим $\alpha_r(x, y) \in K_s$ условиями: $\alpha_0(x, y) = x/y$, при $r > 0$ $\alpha_r(x, y)$ — проекция $\alpha_{r-1}(x, y)$ на K_s относительно разложения $K_{s+1} = K_s + C_{s+1}$. Если $\tau = (x_1, y_1, z_1)$, где $x_1, y_1, z_1 \in K_n$, $y_1 \neq 0$, то положим $\alpha_r(\tau) = \alpha_r(x_1, y_1)$.

Для доказательства предложения 3 нам потребуется доказать следующее предложение.

ПРЕДЛОЖЕНИЕ 4. а) Пусть $j \in \{1, 2, 3\}$, $x, y, z \in K_{n,j}$ удовлетворяют условиям п. а) предложения 3, $t = -x/y \pmod{\ell_n}$, $N_j(t) \geq 1$, $N = N_j(t)$, $\{d_1, \dots, d_N\} \in \mathbf{A}_j(t)$, $d_0 = 1$. Пусть $0 \leq r \leq \min(N, n)$, $s = n - r$. Тогда для всякой перестановки $\tau = (x_1, y_1, z_1)$ тройки x, y, z имеет место сравнение $\alpha_r(\tau) - \alpha_0(\tau) \equiv 0 \pmod{l/\lambda^{d_r}}$ и для $d_r < d \leq l-1$

$$\kappa_d(\alpha_r(\tau))^{(1-\sigma)\delta} \in (K_s^*)^l. \quad (21)$$

б) Пусть $j \in \{1, 3\}$, $x, y \in K_{n,j}$ удовлетворяют условиям п. б) предложения 3. Пусть $N = [(l-3)/(2(I(l)+1))]$ при $j = 1$, $d_i = 2i(I(l)+1)$, где $0 \leq i \leq N$; $N = (l-3)/2 - I(l)$ при $j = 3$, $\{d_1, \dots, d_N\}$ — строго возрастающая последовательность нечетных натуральных чисел $d < l-3$ таких, что $l \nmid B_{l-d}$, $d_0 = 0$. Пусть $0 \leq r \leq n \leq N$, $s = n - r$. Тогда имеет место сравнение

$$\alpha_r(x, y) - \alpha_0(x, y) \equiv 0 \pmod{l/\lambda^{d_r}}$$

и для $d_r < d \leq l-1$ имеет место (21) (с $\alpha_r(x, y)$ вместо $\alpha_r(\tau)$).

ДОКАЗАТЕЛЬСТВО. Докажем предложение, применяя индукцию по r . Для $r = 0$ утверждения предложения выполнены вследствие условий предложения 3. Предполагая, что для некоторого $0 \leq r < \min(N, n)$ утверждения предложения выполнены, докажем их для $r + 1$.

Из определения дифференцирования D_s легко следует, что для любого $v \in S_s$ $D_s(v^{\sigma_a}) = a\sigma_a(D_s(v)) \pmod{l}$. Поэтому

$$\begin{aligned}\Omega_s(u^{(1-\sigma)^\delta}) &= (1 + \sigma) \prod_m (c\sigma_c - c^m) \Omega_s(u) \pmod{l} \\ &= (1 + \sigma) \left(\sum_{k=0}^{I(l)} a_k (c\sigma_c)^k \right) \Omega_s(u) \pmod{l},\end{aligned}$$

где u — единица S_s , целые числа a_k определены равенством

$$\prod_m (X - c^m) = \sum_{k=0}^{I(l)} a_k X^k,$$

где произведение берется по нечетным $3 \leq m \leq l - 2$ таким, что $l \mid B_{l-m}$. Пусть α_r обозначает $\alpha_r(\tau)$ или $\alpha_r(x, y)$ (в зависимости от доказываемой части предложения). Учитывая также, что $\sigma_a \lambda \equiv a\lambda \pmod{l}$, из (17) и (21) следует, что для $d_r < d \leq l - 1$ имеет место сравнение

$$(1 + (-1)^d \sigma) \left(\sum_{k=0}^{I(l)} a_k (c\sigma_c)^k c^{kd} \right) (D_s(\alpha_r) g_d(-\alpha_r)) \equiv 0 \pmod{l/\lambda^d}. \quad (22)$$

Мы собираемся вывести из сравнений (22) сравнение

$$D_s(\alpha_r) \equiv 0 \pmod{l/\lambda^{d_{r+1}}}. \quad (23)$$

В случае $j = 3$

$$a\sigma_a(D_s(\alpha_r) g_d(-\alpha_r)) \equiv D_s(\alpha_r) g_d(-\alpha_r) \pmod{l/\lambda^d} \quad \forall a \in (\mathbb{Z}/l\mathbb{Z})^*,$$

так как $\alpha_r \in K_{s,3}$, σ_a оставляет неподвижным $K_{s,3}$. Поэтому (22) эквивалентно сравнению

$$(1 + (-1)^{d-1}) \prod_m (c^d - c^m) D_s(\alpha_r) g_d(-\alpha_r) \equiv 0 \pmod{l/\lambda^d}. \quad (24)$$

Покажем в случае п. а) предложения 4, что

$$D_s(\alpha_r(\tau)) = u(\tau) D_s(\alpha_r(\tau_0)) \pmod{l/\lambda^{d_r}}, \quad (25)$$

где $\tau_0 = (x, y, z)$, $u(\tau)$ — единица $K_{s,j}$, если $(x, y, z) \in K_{s,j}$.

Из равенства $x^l + y^l + z^l = 0$ следует, что $\alpha_0(\tau_1)^l + \alpha_0(\tau_0)^l = 1$ для $\tau_1 = (z, y, x)$. Поэтому, учитывая, что $\alpha_r(\tau_i) \equiv \alpha_0(\tau_i) \pmod{l/\lambda^{d_r}}$, имеем

$$\alpha_r(\tau_1)^l + \alpha_r(\tau_0)^l \equiv 1 \pmod{l^2/\lambda^{d_r}}.$$

Применяя D_s (определенное $(\bmod l^{s+1}/\lambda)$, где $s \geq 1$) и сокращая на l , имеем сравнение

$$\alpha_r(\tau_1)^{l-1} D_s(\alpha_r(\tau_1)) + \alpha_r(\tau_0)^{l-1} D_s(\alpha_r(\tau_0)) \equiv 0 \pmod{l/\lambda^{d_r}},$$

из которого следует (24) для $\tau = \tau_1$.

Пусть $\tau_2 = (y, x, z)$. Тогда $\alpha_0(\tau_2) = \alpha_0(\tau_0)^{-1}$, откуда $\alpha_r(\tau_2) \equiv \alpha_r(\tau_0)^{-1} \pmod{l/\lambda^{d_r}}$, так что

$$D_s(\alpha_r(\tau_2)) = -D_s(\alpha_r(\tau_0))\alpha_r(\tau_0)^{-2} \pmod{l/\lambda^{d_r}}$$

и (25) имеет место для $\tau = \tau_2$. Так как доказанное верно и для любой перестановки (x, y, z) , то (25) верно для произвольной перестановки τ .

По определению $g_d(Y) = f_d(Y)/Y = P_d(Y)/(Y(1-Y)^{d+1})$. В случае п. б) предложения 4 $\alpha_r \equiv 0 \pmod{\pi_s}$, откуда, учитывая, что $P_d(Y) \equiv Y \pmod{Y^2}$, следует, что

$$g_d(-\alpha_r) \not\equiv 0 \pmod{\pi_s}. \quad (26)$$

В случае п. а) свойство (26), очевидно, имеет место, если

$$P_d(-\alpha_r) \not\equiv 0 \pmod{\pi_s}.$$

Пусть $d = d_{r+1}$ в случае б), когда $j = 3$, а в случае а), когда $j = 3$, пусть d – нечетное натуральное число такое, что $d \leq d_{r+1}$ при $r = 0$, $d_r < d \leq d_{r+1}$ при $r > 0$; и $l \nmid B_{l-d}$ и

$$P_d(\mathbf{G}_t) \neq 0. \quad (27)$$

Такое d существует, поскольку $\{d_1, \dots, d_N\} \in \mathbf{A}_j$. В случае а), когда $j = 3$, выберем τ так, что (26) имеет место $(-\alpha_r(\tau) \pmod{\pi_s})$ пробегает $\mathbf{G}_t$, когда τ пробегает перестановки (x, y, z) . Тогда в обоих случаях

$$(1 + (-1)^{d-1}) \prod_m (c^d - c^m) g_d(-\alpha_r) \not\equiv 0 \pmod{\pi_s}$$

и (23) следует из (24). Кроме того, в случае а) из (25) следует, что (23) верно для любой перестановки τ . Таким образом, в случаях, когда $j = 3$, сравнение (23) доказано.

Пусть в остальных случаях M_1 – множество $I(l) + 1$ нечетных натуральных чисел d , а в случаях, когда $j = 1$, также M_2 – множество $I(l) + 1$ четных натуральных чисел d таких, что $d \leq d_{r+1}$ при $r = 0$, $d_r < d \leq d_{r+1}$ при $r > 0$, и в случае а) для всех d из этих множеств имеет место (27). Существование таких множеств очевидно в случае б), а в случае а) следует из условия $\{d_1, \dots, d_N\} \in \mathbf{A}_j$.

Выберем в случае а) для всякого d из определенных только что множеств перестановку $\tau(d)$ такую, что имеет место (26) с $\alpha_r = \alpha_r(\tau(d))$.

Положим $x_k = a_k(c\sigma_c)^k D_s(\alpha_{r,0})$, где $k = 0, \dots, I(l)$, $\alpha_{r,0} = \alpha_r(\tau_0)$ в случае а), $\alpha_{r,0} = \alpha_r(x, y)$ в случае б).

Положим $a_{d,k} = \sigma_c^k(u(\tau(d))g_d(-\alpha_r(\tau(d))))$ в случае а), $a_{d,k} = \sigma_c^k g_d(-\alpha_r(x, y))$ в случае б).

Положим $\chi = l/\lambda^{d_{r+1}}$. Учитывая (25), сравнение (22) $(\bmod \chi)$, соответствующее d в случае б) и паре $(d, \tau(d))$ в случае а), можно представить в виде

$$\sum_{k=0}^{I(l)} a_{d,k} x_k + \sum_{k=0}^{I(l)} (-1)^d \sigma(a_{d,k}) \sigma(x_k) \equiv 0 \pmod{\chi}.$$

Рассмотрим матрицу $(a_{d,k})$, где d пробегает M_1 или M_2 . Покажем, что $\det(a_{d,k})$ есть единица. Имеем

$$\det(a_{d,k}) \pmod{\pi_s} = u \det(b_{d,k}) \pmod{\pi_s},$$

где $u = \prod_d u(\tau(d)) g_d(-\alpha_r(\tau(d)))$ – единица, $b_{d,k} = c^{dk}$, так что $\det(b_{d,k})$ – единица, поскольку является определителем Вандермонда, соответствующим попарно различным $(\bmod l)$ числам c^d . Значит, $\det(a_{d,k})$ есть единица.

Рассмотрим случай а), $j = 2$. Тогда $\sigma(x_k) = -x_k$, $\sigma(a_{d,k}) = a_{d,k}$, так как $\alpha_r(\tau) \in K_{s,2}$, $u(\tau) \in K_{s,2}$ при любой перестановке τ . Поскольку $d \in M_1$ нечетно, то сравнения, соответствующие $d \in M_1$, эквивалентны системе сравнений $\sum a_{d,k} x_k \equiv 0 \pmod{\chi}$. Поскольку $\det(a_{d,k})$ есть единица, из этой системы следует, что $x_k \equiv 0 \pmod{\chi}$ при $k = 0, \dots, I(l)$. В частности,

$$x_{I(l)} = (c\sigma_c)^{I(l)} D_s(\alpha_{r,0}) \equiv 0 \pmod{\chi},$$

откуда, учитывая (25), получим (23).

Рассмотрим случаи а), $j = 1$; б), $j = 1$. В этих случаях интерпретируем сравнения, соответствующие $d \in M_1 \cup M_2$, как систему $2(I(l) + 1)$ уравнений относительно $2(I(l) + 1)$ неизвестных $x_k, \sigma(x_k)$, $k = 0, \dots, I(l)$. Достаточно доказать, что определитель матрицы этой системы есть единица, тогда $x_k \equiv 0 \pmod{\chi}$, и мы получаем (23) так же, как в предыдущем случае. Преобразуем матрицу системы $(\bmod \pi_s)$ следующим образом. Прибавим к каждому столбцу, умножаемому на $\sigma(x_k)$, столбец, умножаемый на x_k , и разделим результат на 2. Очевидно, получаем 0 в местах, соответствующих нечетным d , $a_{d,k} \pmod{\pi_s}$ в местах, соответствующих четным d . Затем вычтем из столбцов при x_k соответственно полученные столбцы при $\sigma(x_k)$. Очевидно, вновь полученная матрица будет иметь вид

$$\begin{pmatrix} (a_{d,k} \pmod{\pi_s}, d \in M_1) & 0_{I(l)+1} \\ 0_{I(l)+1} & (a_{d,k} \pmod{\pi_s}, d \in M_2) \end{pmatrix},$$

где $0_{I(l)+1}$ – нулевая квадратная матрица размера $(I(l) + 1) \times (I(l) + 1)$. Определитель этой матрицы есть произведение определителей матриц, стоящих соответственно в левом верхнем и в правом нижнем углах, которые, по доказанному выше, есть единицы $(\bmod \pi_s)$. Значит, и определитель начальной матрицы есть единица, что и требовалось доказать. Итак, сравнение (23) доказано во всех случаях.

Пусть $\alpha_r = \alpha_{r+1} + b'$, где $b' \in A_s$. Поскольку $D_s(S_{s-1}) \equiv 0 \pmod{l}$, то из (23) следует, что $D_s(b') \equiv 0 \pmod{\chi}$, так что по лемме $2b' = \chi b$, где $b \in A_s$, так что

$$\alpha_r = \alpha_{r+1} + \left(\frac{l}{\lambda^{d_{r+1}}} \right) b.$$

Из леммы 5 в случае, когда $\alpha = \alpha_r$, $\beta = \alpha_{r+1}$, $m = d_{r+1}$, следует, что при $d_{r+1} < d \leq l - 1$

$$\frac{\log(\kappa_d(\alpha))}{l} - \frac{\log(\kappa_d(\beta))}{l} \in \lambda A_s + \lambda \pi_s S_s,$$

откуда

$$\frac{(1 - \sigma)\delta \log(\kappa_d(\alpha))}{l} - \frac{(1 - \sigma)\delta \log(\kappa_d(\beta))}{l} \in \lambda A_s + \lambda \pi_s S_s.$$

Значит, по лемме 1

$$\frac{(1 - \sigma)\delta \log(\kappa_d(\beta))}{l} \in \log(V_s),$$

так как

$$\frac{(1 - \sigma)\delta \log(\kappa_d(\alpha))}{l} = \frac{\log(\kappa_d(\alpha)^{(1 - \sigma)\delta})}{l} \in \log(V_s)$$

вследствие (21),

$$\lambda \pi_s S_s = \log(1 + \lambda \pi_s S_s) \subset \log(V_s).$$

Значит, $\kappa_d(\beta)^{(1 - \sigma)\delta} = \zeta_{s-1}^i \gamma^l$, где $\gamma \in V_{s-1}$. Имеем

$$\frac{\beta + \zeta^k}{\beta + 1} = 1 + \frac{\zeta^k - 1}{\beta + 1} = 1 + \frac{k}{1 - t}(\zeta - 1) \pmod{\lambda \pi_{s-1}},$$

где $t = -\beta \pmod{\pi_{s-1}} \in \mathbb{Z}/l\mathbb{Z} \setminus \{1\}$. Учитывая, что $d > d_{r+1} \geq 1$, имеем

$$\kappa_d(\beta) \equiv 1 + \frac{1}{1 - t} \sum_{k=1}^{l-1} k^{d-1}(\zeta - 1) \equiv 1 \pmod{\lambda \pi_{s-1}}.$$

Так как $\gamma^l \equiv 1 \pmod{\pi_{s-1}^l}$, то $\zeta_{s-1}^i = \frac{\kappa_d(\beta)}{\gamma^l} \equiv 1 \pmod{\pi_{s-1}^2}$, откуда $i \equiv 0 \pmod{l}$.

Итак, шаг индукции сделан и предложение 4 доказано.

Закончим доказательство предложения 3. Предположим, что $x, y, z \in K_{n,j}$ удовлетворяют условиям п. а) предложения 3 и $n \leq N_j(t)$. Тогда по предложению 4 (учитывая, что $v \in V_0^l$, если $v \in V_0$ и $v \in (K_0^*)^l$)

$$\kappa_d(\alpha_n(\tau))^{(1 - \sigma)\delta} \in V_0^l,$$

где $d = c(t) + 1$ (см. определение числа $c(t)$ во введении). Отсюда и из леммы 4 для $\alpha = \alpha_n(\tau)$ следует, что

$$(1 - (-1)^d \sigma) \prod_m (c^d \sigma_c - c^m) \left((\alpha^l + 1)^{-1} \sum_{i=1}^{l-1} (-\alpha)^i i^{d-1} \right) \equiv 0 \pmod{\lambda^{l+1-d}}. \quad (28)$$

Так как по определению $c(t)$ число d нечетно и не совпадает ни с одним нечетным m таким, что $3 \leq m \leq l - 2$, $l \mid B_{l-m}$ (а $\prod_m$ — произведение именно по таким числам m), то из (28), учитывая (20), получим

$$(\alpha^l + 1)^{-1} \sum_{i=1}^{l-1} (-\alpha)^i i^{d-1} \equiv P_{d-1}(-\alpha)(\alpha^l + 1)^{-d} \equiv 0 \pmod{\lambda},$$

откуда $P_{d-1}(-\alpha) \equiv 0 \pmod{\lambda}$. С другой стороны, так как $P_{d-1}(\mathbf{G}_t) \neq 0$, существует τ такая, что $P_{d-1}(t_1) \not\equiv 0 \pmod{l}$, где $t_1 = -\alpha \pmod{\lambda} \in \mathbb{Z}/l\mathbb{Z}$. Противоречие. Значит, $n > N_j(t)$, что и требовалось доказать.

В случае п. б) предложения 3 из п. б) предложения 4 следует, что для $\alpha = \alpha_n(x, y) \in S_0$

$$\kappa_d(\alpha)^{(1-\sigma)\delta} \in V_0^l$$

при $d = d_n + 1, d_n + 2$. Отсюда и из леммы 4 тогда следует (28) для этих значений d . Учтем, что согласно предложению 4 $\alpha \equiv \alpha_0 \pmod{l/\lambda^{d_n}}$, а $d_n \leq l - 3$. Так что $\alpha \equiv 0 \pmod{\lambda}$, поскольку $\alpha_0 = -\frac{x}{y} \equiv 0 \pmod{\pi_n}$. Из (28) для $d = d_n + 1, d_n + 2$ тогда следует, что $(1 \pm \sigma)\alpha \equiv 0 \pmod{\gcd(\alpha^2, l/\lambda^{d_n})}$, откуда следует, что $\alpha \equiv 0 \pmod{l/\lambda^{d_n}}$. Значит, $\alpha_0 \equiv 0 \pmod{l/\lambda^{d_n}}$, т.е. $x \equiv 0 \pmod{l/\lambda^{d_n}}$. Пусть $x \in R_{n,3}$. Нам остается доказать, что тогда $x \equiv 0 \pmod{(l/\lambda^{d_n})\pi_n^{d_n}}$. Это очевидно, если $x = 0$. Пусть $x \neq 0$. Поскольку l/λ^{d_n} ассоциировано с $\pi_n^{l^n(l-1-d_n)}$, то $x = \pi_n^{l^n(l-1-d_n)+i}u$, где u — единица, i — неотрицательное целое число. Кроме того, $l^n(l-1-d_n) + i \equiv 0 \pmod{(l-1)}$, так как $\ell_{n,3} = \ell_n^{l-1}$. Значит, $i - d_n \equiv 0 \pmod{(l-1)}$, откуда следует, что $i \geq d_n$, так как $i - d_n \geq -d_n > -(l-1)$. Предложение 3 доказано.

§ 3. Оценки снизу для функций $\varphi_j(l)$

Как видно из вышеизложенного (см. введение), частота необращения в нуль значений $P_m(t) \pmod{l}$, $t \in \Sigma_l$, играет важную роль для приложений к 1СТФ для l и полей L_n (о приложениях к 1СТФ для l и поля L_0 см. также [4, теоремы 1 и 2] и ниже). Вопрос этот также исследовался ранее в связи с тем, что упомянутые критерии из [4] для 1СТФ в случае поля $\mathbb{Q}$ являются классическими результатами.

Пусть $m \geq 0$, $M \geq 1$, $t \in \Sigma_l$, $\nu = 0, 1$, $N(t, \nu, m, M)$ обозначает количество тех $n \equiv \nu \pmod{2}$, $m < n < m + M$, для которых $P_n(t) \not\equiv 0 \pmod{l}$.

Имеет место

ПРЕДЛОЖЕНИЕ 5. Пусть целые числа $m \geq 0$, $M \geq 1$ таковы, что $m + M \leq l - 1$, $t \in \Sigma_l$ при $\nu = 1$, $t \in \Sigma_l \setminus \{-1\}$ при $\nu = 0$. Пусть натуральное число N таково, что $N(N+1)(m+1) < M + \kappa(t, \nu, m)$, где $\kappa(t, \nu, m) = 1$, если $\nu + m$ нечетно или $\nu + m$ четно и $P_m(t) \equiv 0 \pmod{l}$, $\kappa(t, \nu, m) = 0$, если $\nu + m$ четно и $P_m(t) \not\equiv 0 \pmod{l}$. Тогда

$$N(t, \nu, m, M) \geq N. \quad (29)$$

Последующее доказательство предложения 5 обобщает доказательство Эйхлера [6] неравенства (29) при $\nu = 0$, $m = 0$, $M = l - 1$.

Из (16) следует сравнение

$$\frac{1}{1 - t\zeta^k} \equiv \sum_{i=0}^{l-2} f_i(t) \frac{(k\lambda)^i}{i!} \pmod{l}. \quad (30)$$

Из (30) и очевидного равенства $1/(1 - t\zeta^{-k}) = 1 - 1/(1 - t^{-1}\zeta^k)$ следует сравнение

$$\begin{aligned} & \frac{1}{1 - t\zeta^k} + (-1)^{\nu+1} \frac{1}{1 - t^{-1}\zeta^k} = \\ & = \left((-1)^{\nu+1} + 2 \sum_{i=0, i \equiv \nu \pmod{2}}^{l-2} f_i(t) \frac{(k\lambda)^i}{i!} \right) \pmod{l}. \end{aligned} \quad (31)$$

Пусть S обозначает кольцо S_0 , D обозначает D_0 , т.е. $D: S \rightarrow S/\lambda^{l-2}S$ — дифференцирование такое, что $D(\zeta) = \zeta$. Заметим, что из (15) следует, что $D(\lambda) = 1$. Дифференцирование D индуцирует дифференцирования $D: S/\lambda^i S \rightarrow S/\lambda^{i-1}S$, $i = l-1, \dots, 1$. Обозначим через D^0 естественное отображение $S \rightarrow S/\lambda^{l-1}S$, а отображение $D^m: S \rightarrow S/\lambda^{l-1-m}S$ определим по индукции как композицию D^{m-1} и $D: S/\lambda^{l-1-(m-1)}S \rightarrow S/\lambda^{l-1-m}S$.

Положим

$$e_k(t, \nu, m) = (f_m(t\zeta^k)) + (-1)^{\nu+1} f_m(t^{-1}\zeta^k) \pmod{l}.$$

Поскольку

$$\frac{d^m}{dX^m} \frac{1}{1 - Y \exp(X)} = f_m(Y \exp(X))$$

(см. [4, §2]), то из формальных свойств дифференцирования D и неравенства $l-1-m \geq M$ следует сравнение

$$e_k(t, \nu, m) \equiv \left(\delta(\nu, m) + 2 \sum_{j=0, m+j \equiv \nu \pmod{2}}^{M-1} f_{m+j}(t) \frac{(k\lambda)^j}{j!} \right) \pmod{\lambda^M}, \quad (32)$$

получающееся применением к (31) отображения $D^m \pmod{\lambda^M}$. Здесь $\delta(\nu, m) = 0$, если $m > 0$, $\delta(\nu, 0) = (-1)^{\nu+1}$.

Будем сокращенно обозначать $e_k(t, \nu, m)$, $\kappa(t, \nu, m)$ через $e_k(\nu, m)$, $\kappa(\nu, m)$ соответственно. Покажем, что элементы $e_k(\nu, m) \pmod{\lambda^M}$, $k = \kappa(\nu, m), \dots, N$, линейно независимы как элементы $\mathbb{Z}/l\mathbb{Z}$ -векторного пространства $S/\lambda^M S$. Этого будет достаточно для доказательства предложения 5, так как тогда из (32) следует, что

$$N(t, \nu, m, M) + (1 - \kappa(\nu, m)) \geq (1 - \kappa(\nu, m)) + N,$$

что эквивалентно (29).

Условимся, что для элемента $a \in S/lS$ запись $a \sim \zeta^r$ означает, что $a = c\zeta^r + P(\zeta)$, где $c \in (\mathbb{Z}/l\mathbb{Z})^*$, $P \in \mathbb{Z}/l\mathbb{Z}[X]$, причем $P = 0$ при $r = 0$, $\deg P < r$ при $r > 0$.

Положим $e'_k(\nu, m) = e_k(\nu, m)((1-t\zeta^k)(1-t^{-1}\zeta^k))^{m+1}$. Учитывая, что $f_m(Y) = P_m(Y)(1-Y)^{-(m+1)}$, имеем равенство

$$\begin{aligned} e'_k(\nu, m) &= (P_m(t\zeta^k)(1-t^{-1}\zeta^k)^{m+1} \\ &\quad + (-1)^{\nu+1} P_m(t^{-1}\zeta^k)(1-t\zeta^k)^{m+1}) \pmod{l}. \end{aligned} \quad (33)$$

Покажем, что

$$e'_k(\nu, m) \sim \zeta^{r(m)k}, \quad (34)$$

где $\kappa(\nu, m) \leq k \leq N$, $0 \leq r(m) \leq 2m+1$.

Рассмотрим сначала случай $\kappa(\nu, m) = 0$, $k = 0$. Тогда достаточно показать, что $e_0(\nu, m) \neq 0 \pmod{l}$. Нам потребуется соотношение

$$f_m(Y^{-1}) = (-1)^{m+1} f_m(Y),$$

если $m > 0$. Оно следует из (2) и равенства

$$(1 - Y^{-1} \exp(X))^{-1} = 1 - (1 - Y \exp(-X))^{-1}.$$

Заметим, что условие $\kappa(\nu, m) = 0$ означает, что $(-1)^{\nu+m} = 1$ и $f_m(t) \not\equiv 0 \pmod{l}$. Так что при $m > 0$

$$e_0(\nu, m) = f_m(t) + (-1)^{\nu+1} f_m(t^{-1}) = (1 + (-1)^{\nu+m}) f_m(t) \not\equiv 0 \pmod{l}.$$

Если же $m = 0$, то $\nu = 0$ и

$$e_0(\nu, m) = f_0(t) - f_0(t^{-1}) = (1 - t)^{-1} - (1 - t^{-1})^{-1} \not\equiv 0 \pmod{l},$$

так как $t \not\equiv -1 \pmod{l}$ по условию.

Рассмотрим теперь случай $k \geq 1$. Поскольку $P_m(Y) = Y^m + q_m(Y)$, где $\deg q_m < m$ ($q_m = 0$ при $m = 0$), то из (33) следует, что

$$e'_k(\nu, m) = ((-1)^{m+1}(t^{-1} + (-1)^{\nu+1}t)\zeta^{(2m+1)k} + \dots) \sim \zeta^{(2m+1)k},$$

если только $t^2 \neq -1$ в случае $\nu = 1$ (напомним, что при $\nu = 0$ $t \neq \pm 1$ по условию). Если же $\nu = 1$, $t^2 = -1$, то, учитывая, что

$$P_m(Y) = Y^m + (2^m - (m+1))Y^{m-1} + \dots$$

(см. [4, §2]), находим из (33), что

$$\begin{aligned} e'_k(\nu, m) &= ((-1)^{m+1}((2^m - (m+1))(t^{-2} + t^2) - 2(m+1))\zeta^{2mk} + \dots) \\ &= ((-1)^m 2^{m+1} \zeta^{2mk} + \dots) \sim \zeta^{2mk}. \end{aligned}$$

Итак, свойство (34) доказано.

Пусть $x_k \in \mathbb{Z}/l\mathbb{Z}$, $\kappa(\nu, m) \leq k \leq N$. Имеем равенство

$$\prod_k ((1 - t\zeta^k)(1 - t^{-1}\zeta^k))^{m+1} \left(\sum_k x_k e_k(\nu, m) \right) = \sum_k x_k e''_k(\nu, m), \quad (35)$$

где

$$e''_k(\nu, m) = \prod_{s \neq k} (\zeta^{2s} - (t + t^{-1})\zeta^s + 1) e'_k(\nu, m).$$

Из (34) следует, что $e''_k(\nu, m) \sim \zeta^{r_k}$, где

$$\begin{aligned} r_k &= \sum_{s=\kappa(\nu, m)}^N 2s(m+1) + (r(m) - 2(m+1))k \\ &= N(N+1)(m+1) - (2(m+1) - r(m))k. \end{aligned}$$

Поскольку $r(m) \leq 2m+1$, то $2(m+1) - r(m) \geq 1$. Поэтому r_k есть строго убывающая функция от k , и, учитывая, что $k \geq 1$ при $\kappa(\nu, m) = 1$, имеем неравенство

$$r_k \leq N(N+1)(m+1) - \kappa(\nu, m). \quad (36)$$

Поэтому, предполагая, что не все x_k равны нулю, и полагая i равным минимальному k такому, что $x_k \neq 0$, получаем, что

$$a = \sum_k x_k e''_k(\nu, m) \sim \zeta^{r_i}.$$

Покажем, что $a \not\equiv 0 \pmod{\lambda^M}$. Действительно, пусть $b = (\zeta - 1)^{l-1-M}a$. Тогда $b \sim \zeta^r$, где $r = l - 1 - M + r_i$. При этом $r_i \leq M - 1$ вследствие (36) и условия $N(N+1)(m+1) < M + \kappa(\nu, m)$ из предложения 5. Значит, $r \leq l - 2$. Но тогда $b \not\equiv 0 \pmod{l}$, так как $1, \zeta, \dots, \zeta^{l-2}$ образуют базис S/lS над $\mathbb{Z}/l\mathbb{Z}$. Значит, $a \not\equiv 0 \pmod{\lambda^M}$. Из (35) следует, что

$$\sum_k x_k e_k(\nu, m) \not\equiv 0 \pmod{\lambda^M}.$$

Следовательно, элементы $e_k(\nu, m) \pmod{\lambda^M}$ линейно независимы, что и требовалось доказать. Предложение 5 доказано.

В качестве следствия теоремы 1 из [4] и предложения 5 имеем следующий результат, обобщающий теорему 6 из [4] (напомним, что B_i обозначает i -е число Бернулли).

ТЕОРЕМА 8. Пусть целые $m \geq 0$, $M \geq 1$ таковы, что $m + M \leq l - 1$, N — натуральное число такое, что $N(N+1)(m+1) < M$, если $B_{l-1-m} \not\equiv 0 \pmod{l}$, и $N(N+1)(m+1) < M + 1$, если $B_{l-1-m} \equiv 0 \pmod{l}$. Если число четных чисел i таких, что $m < l - 1 - i < m + M$, $l \mid B_i$, меньше N , то для l и поля L_0 справедлив 1СТФ.

ДОКАЗАТЕЛЬСТВО. Если 1СТФ неверен для l и поля L_0 , то согласно [4, сравнение (2)] $\exists t \in \mathbb{Z}/l\mathbb{Z} \setminus \{0, 1, -1\}$ такой, что

$$B_i P_{l-1-i}(\tau) \equiv 0 \pmod{l} \quad \forall \tau \in \mathbf{G}_t, \quad i = 2, 4, \dots, l-3. \quad (37)$$

Из предложения 5, условий теоремы 8 и (37) тогда следует, что $N(t, 0, m, M) \geq N$. Учитывая (37), заключаем, что число тех четных i , для которых $m < l - 1 - i < m + M$, $B_i \equiv 0 \pmod{l}$, не меньше N , что противоречит условиям теоремы 8.

Заметим, что фактически мы доказали, что $\varphi_1(l) \geq 0$ при условиях теоремы 8, а справедливость 1СТФ для l и L_0 есть следствие этого в силу [4, теорема 1].

Положим $J(l) = 1 + (I(l) + 1)(I(l) + 2)$. В качестве другого следствия предложения 5 докажем

ПРЕДЛОЖЕНИЕ 6. Пусть $l > J(l)$. Тогда для всякого $t \in \Sigma_l$ число $c(t)$ определено (см. введение), так что $\varphi_1(l) \geq 0$ и $c(t) \geq [l/J(l)]$.

ДОКАЗАТЕЛЬСТВО. Положим $N = I(l) + 1$, $m = [l/J(l)] - 1$, $M = l - 1 - m$. Поскольку

$$m < l/J(l) - 1 = l/(1 + N(N+1)) - 1,$$

то $N(N+1)(m+1) < l - 1 - m = M$. По предложению 5 если $t' \in \Sigma_l \setminus \{-1\}$, то существует не менее N четных чисел n таких, что $m + 1 \leq n \leq l - 3$, $P_n(t') \not\equiv 0 \pmod{l}$. Хотя бы для одного из них $l \nmid B_{l-1-n}$, так как $I(l) = N - 1$. Значит, $c(t') \geq m + 1 = [l/J(l)]$. Поскольку для всякого $t \in \Sigma_l$ существует $t' \neq -1$, $t' \in \mathbf{G}_t$, то $c(t) = c(t')$ удовлетворяет нужному неравенству. Предложение доказано. Заметим, что существование $c(t)$ было доказано ранее Эйхлером [6].

Докажем оценки снизу в теореме 5 функций $\varphi_2(l)$, $\varphi_3(l)$. Положим $N' = [\sqrt{l/J(l)}] - 1$. Тогда

$$N'(N' + 1) < (\sqrt{l/J(l)} - 1)\sqrt{l/J(l)} < l/J(l) - 1.$$

Значит, $N'(N' + 1) \leq [l/J(l)] - 1$. Тогда для $t \in \Sigma_l$ по предложению 5 число нечетных натуральных чисел n таких, что $n < [l/J(l)]$, $P_n(t) \not\equiv 0 \pmod{l}$, не меньше N' . Учитывая, что при $l > J(l)$ по предложению 6 $[l/J(l)] \leq c(t)$, отсюда, очевидно, следует, что

$$N_2(t) \geq [N'/(I(l) + 1)] = \psi_2(l), \quad N_3(t) \geq \max(N' - I(l), 0) = \psi_3(l),$$

если $l > J(l)$. Так как это верно для любого $t \in \Sigma_l$, то $\varphi_2(l) \geq \psi_2(l)$, $\varphi_3(l) \geq \psi_3(l)$, если $l > J(l)$.

Перейдем к оценкам снизу для функции $\varphi_1(l)$. Мы выведем их из следующего предложения.

ПРЕДЛОЖЕНИЕ 7. Пусть натуральное число n удовлетворяет условию $(n!(n! + 1))^{(n-1)/2} < l$, если n нечетно, и условию $(n!(n! + 1)/2)^{(n-2)/2} < l$, если n четно. Тогда

$$\begin{aligned} \forall t \in (\mathbb{Z}/l\mathbb{Z})^* \quad \text{либо} \quad P_n(t) \not\equiv 0 \pmod{l}, \quad \text{либо} \quad P_n(1-t) \not\equiv 0 \pmod{l}, \\ \text{либо} \quad P_n\left(1 - \frac{1}{t}\right) \not\equiv 0 \pmod{l}. \end{aligned}$$

В частности, $P_n(G_t) \neq 0$, если $t \in \Sigma_l$.

Предложение 7 дополняет результат Краснера [5], согласно которому либо $P_n(t) \not\equiv 0 \pmod{l}$, либо $P_n(1-t) \not\equiv 0 \pmod{l}$, если $t \in \mathbb{Z}/l\mathbb{Z}$ и n удовлетворяет неравенству

$$(n!)^{2(n-1)} < l. \quad (38)$$

ДОКАЗАТЕЛЬСТВО. Из рекуррентного соотношения для полиномов P_n (см. введение) по индукции следует, что $P_n(1) = n!$. Значит, $P_n(1) \not\equiv 0 \pmod{l}$ при $n < l$. Поэтому можно предполагать, что $t \in \Sigma_l$.

Пусть $\Phi_i(Z) = f_{i-1}(Z/(Z-1))$, $i \geq 2$. Тогда $\Phi_i(Z) = Z(1-Z)A_i(Z)$, где $A_i(Z) \in \mathbb{Z}[Z]$ — многочлен степени $i-2$, имеющий коэффициент $a_0(i) = (-1)^{i-1} \times (i-1)!$. Это следует из того, что

$$f_{i-1}(Y) = P_{i-1}(Y)(1-Y)^{-i},$$

где

$$P_{i-1}(Y) = Y^{i-1} + \dots + Y \in \mathbb{Z}[Y] \quad \text{и} \quad P_{i-1}(1) = (i-1)!.$$

Заметим, что $A_2(Z) = -1$. Далее, имеет место соотношение

$$\Phi_{i+1}(Z) = Z(1-Z)\Phi'_i(Z). \quad (39)$$

Соотношение (39) следует из соотношения $f_i(Y) = Yf'_{i-1}(Y)$, которое выводится путем сравнения результатов дифференцирования (3) по X и Y .

Как заметил Краснер, (39) влечет то, что $A_i(z)$ имеет $i-2$ различных вещественных корня в интервале $(0, 1)$. Это легко доказывается индукцией по i . Действительно, поскольку Φ_i имеет нули при $Z = 0, 1$ и по предположению индукции имеет $i-2$ различных нуля в интервале $(0, 1)$, то Φ_i (являясь гладкой ограниченной функцией в интервале $(0, 1)$) имеет не менее $i-1$ экстремум в интервале $(0, 1)$. Значит, Φ'_i имеет не менее $i-1$ различных нулей в $(0, 1)$. Из (39) следует тогда, что Φ_{i+1} , а значит, и A_{i+1} , имеет не менее $i-1$ различных нулей в $(0, 1)$. Поскольку

A_{i+1} – многочлен $(i-1)$ -ой степени, то A_{i+1} имеет ровно $i-1$ различных корней в $(0, 1)$. В частности, имеет место разложение

$$A_i(Z) = a_0(i) \prod_u (Z - u), \quad (40)$$

где u пробегает корни A_i в $(0, 1)$.

Пусть $B_i(Z) = Z^{i-2}A_i(Z^{-1}) \in \mathbb{Z}[Z]$. Из (40) следует равенство

$$B_i(Z) = a_0(i) \prod_u (1 - Zu). \quad (41)$$

Пусть $R_i \in \mathbb{Z}$ обозначает результат многочленов $A_i(Z)$ и $B_i(Z)$. Из формулы [10, гл. 5, § 10, (2)] следует, что

$$R_i = (a_0(i))^{i-2} \prod_v B_i(v),$$

где v пробегает корни $A_i(Z)$. Учитывая также (41), получаем равенство

$$R_i = a_0(i)^{2(i-2)} \prod_{u,v} (1 - vu),$$

где u, v независимо пробегает корни A_i , которые, как мы знаем, принадлежат интервалу $(0, 1)$. В частности, R_i – ненулевое целое число и

$$0 < |R_i| \leq |a_0(i)|^{2(i-2)} = ((i-1)!)^{2(i-2)}. \quad (42)$$

Полагая $i = n+1$ и предполагая выполнение условия (38), Краснер заключает из (42), что l не делит R_i (так как $0 < |R_i| < l$), и, следовательно, многочлены $A_i(Z) \pmod{l}$ и $B_i(Z) \pmod{l}$ не имеют общих корней, откуда легко следует, что $P_n(Y) \pmod{l}$ и $P_n(1-Y) \pmod{l}$ не имеют общих корней.

Для доказательства предложения 7 мы используем вместо многочленов A_i и B_i подходящие многочлены меньших степеней, имеющие меньший результат.

Из соотношения (39) следует, что многочлены A_i удовлетворяют следующему рекуррентному соотношению:

$$A_{i+1}(Z) = (1 - 2Z)A_i(Z) + (Z - Z^2)A'_i(Z). \quad (43)$$

Из соотношения (43) по индукции следует, что при четном i $A_i(Z) = Q_i(Z^2 - Z)$, где $Q_i \in \mathbb{Z}[W]$ – многочлен степени $(i-2)/2$ с коэффициентом при $W^{(i-2)/2}$, равным $a_0(i)$; при нечетном $i \geq 3$ $A_i(Z) = (2Z - 1)Q_i(Z^2 - Z)$, где $Q_i \in \mathbb{Z}[W]$ – многочлен степени $(i-3)/2$ с коэффициентом при $W^{(i-3)/2}$, равным $a_0(i)/2$.

Нам потребуется следующая

ЛЕММА 6. Пусть $T(X) \in \mathbb{Z}[X]$ – многочлен степени m . Если $T(1-X) = T(X)$, то m четно и $T(X) = C(X^2 - X)$, где $C(W) \in \mathbb{Z}[W]$ – многочлен степени $m/2$.

ДОКАЗАТЕЛЬСТВО. Пусть $T(X) = aX^m \pmod{\deg(m-1)}$. Тогда, очевидно, $a(-1)^m = a$, откуда $(-1)^m = 1$, так что m четно. Далее, многочлен $T_1(X) = T(X) - a(X^2 - X)^{m/2}$ имеет меньшую степень и удовлетворяет соотношению $T_1(1 - X) = T_1(X)$. Применение индукции по m заканчивает доказательство.

Положим $T_i(Z) = B_i(Z) + B_i(1 - Z)$. Очевидно, $T_i(1 - Z) = T_i(Z)$. Поскольку T_i — многочлен степени $i - 2$, если i четно, степени $i - 3$, если i нечетно, то согласно лемме 6 существует многочлен $C_i(W) \in \mathbb{Z}[W]$ такой, что $T_i(Z) = C_i(Z^2 - Z)$, степень C_i равна $(i - 2)/2$, если i четно, степень C_i равна $(i - 3)/2$, если i нечетно.

Рассмотрим теперь пару многочленов $Q_i(W)$, $C_i(W)$ и оценим их результат r_i . Поскольку A_i не имеет кратных корней и $A_i(1/2) = 0$ при нечетном i , то из (43) следует, что $A_i(1/2) \neq 0$ при четном i . Из определения многочленов Q_i следует, что при отображении $v \mapsto v^2 - v$ корни A_i в интервале $(0, 1/2)$ взаимно однозначно отображаются на корни Q_i . Используя ту же формулу для результата из [10], что и выше, и учитывая, что $C_i(v^2 - v) = B_i(v) + B_i(1 - v)$, получаем равенства

$$\begin{aligned} r_i &= a_0(i)^{(i-2)/2} \prod_{v < 1/2} (B_i(v) + B_i(1 - v)), & \text{если } i \text{ четно,} \\ r_i &= (a_0(i)/2)^{(i-3)/2} \prod_{v < 1/2} (B_i(v) + B_i(1 - v)), & \text{если } i \text{ нечетно,} \end{aligned} \quad (44)$$

в которых произведения берутся по корням A_i в интервале $(0, 1/2)$.

Пусть $v \in (0, 1)$. Заметим, что из равенств (41) следует, что $B_i(v)$ — ненулевое число, знак которого совпадает со знаком $a_0(i)$. Поскольку $1 - v \in (0, 1)$, то $B_i(v) + B_i(1 - v) \neq 0$. В частности, из (44) следует, что $r_i \neq 0$, т.е. r_i — ненулевое целое число. Оценим сверху абсолютную величину числа r_i . Для этого докажем следующую лемму.

ЛЕММА 7. Пусть $v \in [0, 1/2]$. Тогда

$$|B_i(v) + B_i(1 - v)| \leq |a_0(i)| + 1 = (i - 1)! + 1.$$

ДОКАЗАТЕЛЬСТВО. Из равенств (40), (41) следует, что

$$|B_i(0) + B_i(1)| = |a_0(i)| + |A_i(1)|, \quad |A_i(1)| = 1,$$

что следует по индукции из (43). Так что для доказательства леммы достаточно показать, что функция $|B_i(v) + B_i(1 - v)|$ на отрезке $[0, 1/2]$ достигает максимума при $v = 0$. В силу (41) это эквивалентно тому, что функция $F(v) = \prod_u (1 - vu) + \prod_u (1 - (1 - v)u)$ достигает максимума в $[0, 1/2]$ при $v = 0$. Это так, поскольку

$$F'(v) = - \sum_{u_1} \left(\prod_{u \neq u_1} (1 - vu) - \prod_{u \neq u_1} (1 - (1 - v)u) \right) < 0 \quad \text{при } v \in [0, 1/2),$$

так как $1 - vu > 1 - (1 - v)u \quad \forall u \in (0, 1)$.

Из леммы 7 и равенств (44) следуют оценки

$$\begin{aligned} |r_i| &< ((i - 1)!((i - 1)! + 1))^{(i-2)/2}, & \text{если } i \text{ четно,} \\ |r_i| &< ((i - 1)!((i - 1)! + 1)/2)^{(i-3)/2}, & \text{если } i \text{ нечетно.} \end{aligned} \quad (45)$$

Положим $i = n + 1$, где n удовлетворяет условию предложения 7. Тогда $|r_i| < l$ вследствие (45) и условия на n . Поскольку $r_i \neq 0$, то r_i не делится на l . Значит $Q_i \pmod{l}$ и $C_i \pmod{l}$ не имеют общих корней в $\mathbb{Z}/l\mathbb{Z}$, так как их результат есть $r_i \pmod{l} \neq 0$. Предположим, что $P_n(t) \equiv 0 \pmod{l}$, $P_n(1-t) \equiv 0 \pmod{l}$, $P_n(1-1/t) \equiv 0 \pmod{l}$ для некоторого $t \in \Sigma_l$. Пусть $z(y) = y/(y-1)$. Положим $z = z(t)$. Тогда

$$z(1-t) = (1-t)/(-t) = 1/z, \quad z(1-(1/t)) = (1-(1/t))/(-1/t) = 1-t = 1/(1-z).$$

Поскольку равенство $P_n(y) \equiv 0 \pmod{l}$ при $y \in \Sigma_l$ влечет равенство $A_i(z(y)) \equiv 0 \pmod{l}$, то имеем соответственно, что $A_i(z) \equiv 0 \pmod{l}$, $A_i(1/z) \equiv 0 \pmod{l}$, $A_i(1/(1-z)) \equiv 0 \pmod{l}$. Положим $\omega = z^2 - z$. Тогда $C_i(\omega) \equiv 0 \pmod{l}$, поскольку $B_i(z) \equiv 0 \pmod{l}$, $B_i(1-z) \equiv 0 \pmod{l}$. Если $z \neq 1/2$ при нечетном i , то также $Q_i(\omega) \equiv 0 \pmod{l}$, и мы получили противоречие: ранее было доказано, что $Q_i \pmod{l}$ и $C_i \pmod{l}$ не имеют общих корней. Значит, остается доказать, что $z \neq 1/2$ в случае нечетного i . Достаточно показать, что $|A_i(2)| \not\equiv 0 \pmod{l}$ в этом случае. Из (40) следует, что

$$|A_i(2)| \leq (i-1)!2^{i-2} = n!2^{n-1}.$$

Но при четном $n \geq 4$

$$n!2^{n-1} < (n!(n!+1)/2)^{(n-2)/2} < l,$$

а $A_3(Z) = 2Z - 1$. Так что $|A_i(2)| \not\equiv 0 \pmod{l}$. Предложение 7 доказано.

Докажем п. а) теоремы 5. Пусть N – натуральное число такое, что

$$((2n)!((2n)!+1)/2)^{n-1} < l, \quad n = N(I(l)+1).$$

Тогда условие из предложения 7, очевидно, выполняется для всех $1 \leq i \leq 2n$ и $P_i(\mathbf{G}_t) \neq 0$ при таких i для любого $t \in \Sigma_l$ по предложению 7. Из определения $N_1(t)$ тогда следует, что $N_1(t) \geq N$, если только $c(t) \geq 2n$. Это верно, если $n = 1$, так как тогда l регулярно. Предположим, что $n \geq 2$. Из предложения 6 следует, что $c(t) \geq 2n$, если $2n \leq [l/(1+M(M+1))]$, где $M = I(l)+1$. Покажем, что это верно. Достаточно доказать, что $2n \leq l/(1+M(M+1))-1$, т.е. $(2n+1)(1+M(M+1)) \leq l$. Поскольку $n-1 \geq 1$, то, учитывая условие на n , достаточно доказать, что

$$(2n+1)(1+M(M+1)) \leq (2n)!((2n)!+1)/2.$$

Так как $2n \geq M+1$, то $(2n)!+1 \geq (M+1)M+1$, и остается проверить, что $2(2n+1) \leq (2n)!$. Это так, поскольку $(2n)! \geq 2n(2n-1) \geq 2(2n+1)$ при $n \geq 2$. Значит, $c(t) \geq 2n$ и $N_1(t) \geq N$ для любого $t \in \Sigma_l$, откуда следует оценка $\varphi_1(l) \geq N$, что и утверждает п. а) теоремы 5.

Для доказательства теоремы 5 нам остается доказать оценку $\varphi_1(l) \geq \psi_1(l)$ при $l > J(l)$.

Пусть четное натуральное число m удовлетворяет неравенству

$$m \leq \left(\frac{2 \ln(l)}{\ln \ln(l)} \right)^{1/2}. \quad (46)$$

Тогда $m^2 \leq 2 \ln(l) / \ln \ln(l)$. Логарифмируя (46), получаем также неравенство

$$\ln(m) \leq \frac{1}{2} (\ln \ln(l) + \ln 2 - \ln \ln \ln(l)).$$

Значит, при $\ln \ln(l) > 2$

$$\ln(m) \leq \frac{1}{2} \ln \ln(l), \quad m^2 \ln(m) < \ln(l).$$

Экспонируя последнее неравенство, имеем $m^{m^2} < l$. Отсюда следует, что

$$\left(\frac{m!(m! + 1)}{2} \right)^{(m-2)/2} \leq (m^m m^m)^{m/2} = m^{m^2} < l.$$

Поэтому из п. а) теоремы 5 следует, что $\varphi_1(l) > N$ при $\ln \ln(l) > 2$, если N – натуральное число такое, что $m = 2N(I(l) + 1)$ удовлетворяет (46). В частности,

$$\varphi_1(l) \geq \psi_1(l) = \left\lceil \frac{1}{I(l) + 1} \left(\frac{\ln(l)}{2 \ln \ln(l)} \right)^{1/2} \right\rceil, \quad (47)$$

если $N = \psi_1(l) \geq 1$ и $\ln \ln(l) > 2$.

Докажем (47) в остальных случаях, предполагая, что $l > 1 + (I(l) + 1)(I(l) + 2)$. Тогда $\varphi_1(l) \geq 0$ по предложению 6, так что (47) имеет место, если $\psi_1(l) < 1$, т.е. $\psi_1(l) = 0$. Остается доказать (47), если $\ln \ln(l) \leq 2$. Предположим, что $F(l) = \ln(l)/2 \ln \ln(l) < 4$. Тогда $\psi_1(l) = 0$ при $I(l) \geq 1$, так что (47) имеет место. Если же $I(l) = 0$, т.е. l регулярно, то $\psi_1(l) \leq 1$ и (47) выполняется, так как $\varphi_1(l) \geq 1$ для регулярного l . Итак, остается проверить, что $F(l) < 4$, если $\ln \ln(l) \leq 2$. Если $e^2 \geq \ln(l) \geq 4$, то $\ln \ln(l) > 1$ и $F(l) \leq e^2/2 < 4$. Если $4 > \ln(l) \geq 2$, то $2 \ln \ln(l) \geq 2 \ln 2 > 1$, так что $F(l) < 4$. Если $\ln(l) < 2$, то достаточно показать, что $\ln \ln(l) \geq \ln \ln 5 > 1/4$, что проверяется непосредственно.

В заключение этого параграфа получим приложение к 1СТФ для l и поля L_0 .

Из полученных выше результатов следует, что $P_{2m}(\mathbf{G}_t) \neq 0$ при $t \in \Sigma_l$ для $m \leq N$, где натуральное число N удовлетворяет условию

$$((2N)!((2N)! + 1)/2)^{N-1} < l, \quad (48)$$

в частности $N = \lceil (\ln(l)/2 \ln \ln(l))^{1/2} \rceil$. Из [4, теорема 1] (см. сравнение (37)) тогда следует, что $l \nmid B_{l-1-2m}$ для таких m , если 1СТФ не верен для l и поля L_0 . Согласно [4, теорема 5] 1СТФ верен для l и поля L_0 , если числитель хотя бы одного из чисел Бернулли B_{l-1-2m} , $m = 1, \dots, \max(22, \lceil \ln(l)^{1/3} \rceil)$, не делится на l . Значит, в формулировке [4, теорема 5] функцию $\ln(l)^{1/3}$ можно заменить на быстрее растущую функцию $(\ln(l)/(2 \ln \ln(l)))^{1/2}$, или, более точно, на $N(l)$, где $N(l)$ – максимальное число, удовлетворяющее условию (48), т.е. имеет место

ТЕОРЕМА 9. Пусть $M = \max\{22, \lceil (\ln(l)/(2 \ln \ln(l)))^{1/2} \rceil\}$ или $M = \max\{22, N(l)\}$. 1СТФ верен для l и поля L_0 , если числитель хотя бы одного числа Бернулли B_{l-1-2m} , $m = 1, \dots, M$, не делится на l .

§ 4. Дальнейшие оценки функций $\varphi_j(l)$

Пусть N – натуральное число, I – неотрицательное целое число. Из теоремы 5 следует, что $\varphi_1(l) \geq N$ для всех достаточно больших чисел l индекса иррегулярности I , а именно если

$$l > ((2N(I+1))!((2N(I+1))! + 1)/2)^{N(I+1)-1}.$$

В принципе, для чисел l , не удовлетворяющих последнему неравенству, можно было бы проверить условие $\varphi_1(l) \geq N$ путем прямого вычисления значений $\varphi_1(l)$, но это потребовало бы слишком большого объема вычислений уже при небольших значениях N и I . В этом параграфе мы, следуя подходу Вады [11], введем некоторые ненулевые целые числа, полезные для уточнения, путем вычислений для данных N и I множества тех l , для которых $I(l) = I$, $\varphi_1(l) \geq N$. Например, используя эти числа, мы покажем, что $\varphi_1(l) \geq 5$ для регулярных $l \geq 17$, так что по теореме 4 ТФ верна для l и поля L_5 при всех регулярных простых числах $l \geq 17$. О других приложениях см. теорему 7.

Из соотношения $f_n(Y^{-1}) = (-1)^{n+1}f_n(Y)$ при $n \geq 1$ (см. §3, после соотношения (34)) и равенства $f_n(Y) = P_n(Y)/(1-Y)^{n+1}$ следует, что $P_n(-1) = 0$ при четном $n \geq 2$. Положим при $n \geq 1$

$$F_n(Y) = \frac{P_n(Y)}{Y(1+Y)^{\nu(n)}}, \quad (49)$$

где $\nu(n) = 0$, если n нечетно, и $\nu(n) = 1$, если n четно. Таким образом, $F_n(Y) \in \mathbb{Z}[Y]$ – многочлен степени $n-1-\nu(n)$.

Из соотношений $f_n(Z/(Z-1)) = Z(1-Z)A_{n+1}(Z)$, $f_n(Y) = Yf'_{n-1}(Y)$ и того, что все корни A_{n+1} вещественны, просты и принадлежат интервалу $(0, 1)$, следует, что F_n имеет простые вещественные отрицательные корни, причем $F_n(-1) \neq 0$. В частности, $F_n(2)$ – ненулевое целое число.

Заметим, что $\mathbf{G}_{-1} = \{-1, 2, 1/2\} \pmod{l}$. Учитывая, что $P_n(Y^{-1})Y^{n+1} = P_n(Y)$, ясно, что $P_n(\mathbf{G}_{-1}) = 0 \Leftrightarrow l \mid F_n(2)$, если n четно, и $l \mid \gcd(F_n(-1), F_n(2))$, если n нечетно.

Из рекуррентного соотношения $P_{n+1} = (n+1)YP_n + (Y-Y^2)P'_n$ по индукции следует, что

$$Y^{-(n-1-\nu(n))/2}F_n(Y) = E_n(Y+Y^{-1}-1), \quad (50)$$

где $E_n(X) \in \mathbb{Z}[X]$ – многочлен степени $(n-1-\nu(n))/2$, и для натуральных чисел k имеют место рекуррентные соотношения

$$\begin{aligned} E_{2k}(X) &= kE_{2k-1}(X) + (1-X)E'_{2k-1}(X), \\ E_{2k+1}(X) &= (kX+3k+2)E_{2k}(X) + (1-X)(X+3)E'_{2k}(X). \end{aligned} \quad (51)$$

Учитывая, что $E_1(X) = 1$, соотношения (51) позволяют последовательно вычислить многочлены E_n .

Пусть ξ' – примитивный кубический корень из 1, так что $(-\xi')^{-1} + (-\xi') - 1 = 0$. Поскольку $-\xi' \notin \mathbb{R}$, то $F_n(-\xi') \neq 0$. Из (50), подставляя $Y = -\xi'$, заключаем, что $E_n(0) \neq 0$, так что $E_n(0)$ – ненулевое целое число. Пусть $l \equiv 1 \pmod{3}$, ξ – примитивный кубический корень из 1 в $(\mathbb{Z}/l\mathbb{Z})^*$. Тогда $\mathbf{G}_{-\xi} = \{-\xi, -\xi^2\}$ и, очевидно, $P_n(\mathbf{G}_{-\xi}) \neq 0 \Leftrightarrow l$ не делит $E_n(0)$.

Пусть $t \in \Sigma_l$. Нетрудно проверить, что $\mathbf{G}_t$ может содержать 2, 3 или 6 элементов, при этом в первом случае $l \equiv 1 \pmod{3}$, $\mathbf{G}_t = \mathbf{G}_{-\xi}$, во втором случае $\mathbf{G}_t = \mathbf{G}_{-1}$. В первых двух случаях мы интерпретировали выше условие $P_n(\mathbf{G}_t) \neq 0$ как условие, что l не делит некоторое ненулевое целое число, зависящее от n и $|\mathbf{G}_t|$. Сейчас мы собираемся, несколько модифицируя определение Вады [11], ввести ненулевые целые числа Δ_n , обладающие тем свойством, что $l \nmid \Delta_n \Rightarrow P_n(\mathbf{G}_t) \neq 0 \ \forall t$ таких, что $|\mathbf{G}_t| = 6$.

Положим

$$F(Y, Z) = (Y - Z) \left(Y - \frac{1}{Z} \right) (Y - (1 - Z)) \\ \times \left(Y - \frac{1}{1 - Z} \right) \left(Y - \frac{Z - 1}{Z} \right) \left(Y - \frac{Z}{Z - 1} \right).$$

Прямое вычисление показывает, что

$$F(Y, Z) = Y^6 - 3Y^5 + aY^4 - (2a - 5)Y^3 + aY^2 - 3Y + 1,$$

где

$$a = a(Z) = -\frac{Z^6 + 3Z^5 - 5Z^3 + 3Z - 1}{Z^4 - 2Z^3 + Z^2}.$$

Имеет место также следующее равенство, проверяемое непосредственно:

$$Y^{-3}F(Y, Z) = H(Y + Y^{-1} - 1, b),$$

где $H(X, b) = X^3 + bX - b$, $b = a - 6$.

Пусть $U_{n,i} \in \mathbb{Z}[b]$, $i = 0, 1, 2$, — многочлены, определяемые однозначно представлением

$$E_n(X) = H(X, b)V_n(X, b) + U_{n,0}X^2 + U_{n,1}X + U_{n,2},$$

где $V_n(X, b) \in \mathbb{Z}[X, b]$.

Предположим, что многочлены $U_{n,i}$ имеют общий делитель в $\mathbb{Q}[b]$, отличный от константы. Тогда, очевидно, существует $\tau \in \mathbb{C} \setminus \{0, 1\}$ такое, что $U_{n,i}(b(\tau)) = 0$, $i = 0, 1, 2$. Тогда $H(y + y^{-1} - 1, b(\tau)) = 0$ для $y = \tau, 1 - \tau$, так как $F(y, \tau) = 0$ для $y = \tau, 1 - \tau$. Значит, $E_n(y + y^{-1} - 1) = 0$, а вследствие (50) и $F_n(y) = 0$ для $y = \tau, 1 - \tau$. Но это невозможно, так как корни $F_n(y)$ — вещественные отрицательные числа, а $\tau + (1 - \tau) = 1$.

Значит, идеал, порожденный $U_{n,i}$ в $\mathbb{Q}[b]$, есть $\mathbb{Q}[b]$, так что $(\mathbb{Z}[b]U_{n,0} + \mathbb{Z}[b]U_{n,1} + \mathbb{Z}[b]U_{n,2}) \cap \mathbb{Z}$ есть ненулевой идеал в $\mathbb{Z}$. Обозначим через Δ_n положительную образующую этого идеала.

Предположим, что $t \in \Sigma_l$ такой, что $|\mathbf{G}_t| = 6$ и $P_n(\mathbf{G}_t) = 0$. Тогда $F_n(\tau) \equiv 0 \pmod{l} \ \forall \tau \in \mathbf{G}_t$, откуда следует, что $E_n(X) \pmod{l}$ делится на $H(X, b(t)) \pmod{l}$, так что $U_{n,i}(b(t)) \equiv 0 \pmod{l}$, откуда, очевидно, $\Delta_n \equiv 0 \pmod{l}$. Значит, если $l \nmid \Delta_n$, то $P_n(\mathbf{G}_t) \neq 0$ для всех t таких, что $|\mathbf{G}_t| = 6$.

Укажем, как введенные нами числа соотносятся с числами, используемыми в [11], [12]. Вада [11] рассматривает многочлены $\tilde{P}_m$ (обозначаемые в [11] как P_m) для нечетных чисел $m \geq 3$. Он определяет для таких m ненулевые целые числа S_m ,

$Q_m(-2)$, D_m . Учитывая, что для четных $n \geq 2$ $P_n(Y) = -\tilde{P}_{n+1}(-Y)$ (что следует из сравнения коэффициентов этих многочленов, приведенных соответственно в [4], [11]), нетрудно проверить, что для четных $n \geq 2$

$$F_n(2) = Q_{n+1}(-2), \quad E_n(0) = (-1)^{(n/2)-1} S_{n+1}, \quad \Delta_n = D_{n+1}, \quad (52)$$

где $Q_{n+1}(-2)$, S_{n+1} , D_n — числа, определенные в [11].

В работах [11], [12] приведены разложения на степени простых чисел чисел S_m , $Q_m(-2)$, D_m для нечетных $11 \leq m \leq 19$ и нечетных $21 \leq m \leq 45$ соответственно. К сожалению, четные индексы не рассматривались в [11], [12] (это не требовалось для цели этих работ).

Пусть $B_m(X)$ обозначает m -й многочлен Бернулли (см. [13, 1.13]). В частности, $B_m(0) = B_m$ — m -е число Бернулли. Имеет место следующее

ПРЕДЛОЖЕНИЕ 8. Если n нечетно, $n \geq 1$, то

$$F_n(-1) = -P_n(-1) = 2^{n+1}(2^{n+1} - 1) \frac{B_{n+1}}{n+1}, \quad (53)$$

$$E_n(0) = (-1)^{\frac{n-1}{2}} \frac{1}{2} (2^{n+1} - 1)(3^{n+1} - 1) \frac{B_{n+1}}{n+1}. \quad (54)$$

Если n четно, $n \geq 2$, то

$$E_n(0) = (-1)^{\frac{n}{2}+1} 3^n (2^{n+1} + 1) \frac{B_{n+1}(\frac{1}{3})}{n+1}, \quad (55)$$

причем знаменатель рационального числа $B_{n+1}(\frac{1}{3})/(n+1)$ есть степень 3.

ДОКАЗАТЕЛЬСТВО. Из [13, 1.14, (2) и (7)] следует, что имеет место разложение

$$\frac{\exp(\omega Z)}{1 + \exp(Z)} = \sum_{n=0}^{\infty} \frac{1}{n+1} \left(B_{n+1}(\omega) - 2^{n+1} B_{n+1}\left(\frac{\omega}{2}\right) \right) \frac{Z^n}{n!}. \quad (56)$$

Полагая в (56) $\omega = 0$ и учитывая (3), получаем, что

$$f_n(-1) = (1 - 2^{n+1})(B_{n+1}/(n+1)),$$

откуда следует (53), так как $P_n(-1) = f_n(-1)2^{n+1}$.

Пусть ξ обозначает примитивный кубический корень из 1. Из (50) следует, что $F_n(-\xi) = (-\xi)^{(n-1-\nu(n))/2} E_n(0)$. Поскольку $P_n(-\xi) = -\xi(1-\xi)^{\nu(n)} F_n(-\xi)$, то

$$\begin{aligned} \frac{P_n(-\xi)}{E_n(0)} &= (-\xi)^{(n+1-\nu(n))/2} (1-\xi)^{\nu(n)} = (-\xi^4)^{(n+1-\nu(n))/2} \xi^{2\nu(n)} (\xi - \xi^2)^{\nu(n)} \\ &= (-1)^{(n+1-\nu(n))/2} \xi^{2(n+1)} (\xi - \xi^2)^{\nu(n)}. \end{aligned}$$

Учитывая, что $f_n(-\xi) = P_n(-\xi)(1+\xi)^{-(n+1)} = P_n(-\xi)(-\xi^2)^{-(n+1)}$, имеем

$$f_n(-\xi) = (-1)^{(n+1+\nu(n))/2} (\xi - \xi^2)^{\nu(n)} E_n(0). \quad (57)$$

Далее, имеет место равенство

$$\sum_{i=0}^2 \frac{a_i}{1 + \xi^i \exp(X)} = \frac{a_0 + a_1 + a_2 - (a_0 + a_1 \xi + a_2 \xi^2) \exp(X) + (a_0 + a_1 \xi^2 + a_2 \xi) \exp(2X)}{1 + \exp(3X)}. \quad (58)$$

Полагая в (58) $a_0 = a_1 = a_2 = 1$, имеем равенство

$$\frac{1}{1 + \xi \exp(X)} + \frac{1}{1 + \xi^2 \exp(X)} = \frac{3}{1 + \exp(3X)} - \frac{1}{1 + \exp(X)},$$

откуда $f_n(-\xi) + f_n(-\xi^2) = (3^{n+1} - 1)f_n(-1)$. Учитывая то, что при нечетном n $f_n(-\xi) = f_n(-\xi^2) = (-1)^{(n+1)/2} E_n(0)$ вследствие (57), и полученное выше выражение для $f_n(-1)$, получаем (54).

Положим в (58) $a_0 = -1$, $a_1 = -\xi^2$, $a_2 = -\xi$. Получаем равенство

$$-\frac{\xi^2}{1 + \xi \exp(X)} - \frac{\xi}{1 + \xi^2 \exp(X)} - \frac{1}{1 + \exp(X)} = \frac{3 \exp(X)}{1 + \exp(3X)}.$$

Пусть $n \geq 2$, n четно, так что $f_n(-1) = 0$. Учитывая полученное равенство, соотношения (3) и (56) при $Z = 3X$, $\omega = 1/3$, имеем равенство

$$-\xi^2 f_n(-\xi) - \xi f_n(-\xi^2) = \frac{3^{n+1}}{n+1} \left(B_{n+1} \left(\frac{1}{3} \right) - 2^{n+1} B_{n+1} \left(\frac{1}{6} \right) \right). \quad (59)$$

Согласно [13, 1.13, (11), $m = 2$] имеет место соотношение

$$B_{n+1}(X) + B_{n+1} \left(X + \frac{1}{2} \right) = 2^{-n} B_{n+1}(2X).$$

Поскольку $B_{n+1} \left(X + \frac{1}{2} \right) = -B_{n+1} \left(\frac{1}{2} - X \right)$ вследствие [13, 1.13, (12)] и того, что n четно, имеем равенство

$$B_{n+1}(X) = 2^{-n} B_{n+1}(2X) + B_{n+1} \left(\frac{1}{2} - X \right).$$

Полагая в нем $X = 1/6$, находим, что $B_{n+1}(1/6) = (2^{-n} + 1)B_{n+1}(1/3)$, откуда правая часть равенства (59) равна

$$-3^{n+1}(2^{n+1} + 1)B_{n+1}(1/3)/(n+1).$$

Поскольку левая часть (59) вследствие (57) равна

$$(-1)^{n/2} (\xi^2(\xi - \xi^2) + \xi(\xi^2 - \xi)) E_n(0) = (-1)^{n/2} 3 E_n(0),$$

то имеет место (55).

Согласно [13, 1.13, (6)] имеет место равенство

$$B_{n+1}(X)/(n+1) = B_{n+1}(X+1)/(n+1) - X^n.$$

Применяя индукцию, находим, что для любого натурального числа N

$$\frac{B_{n+1}(X)}{n+1} = \frac{B_{n+1}(X+N)}{n+1} - (X^n + \dots + (X+N-1)^n). \quad (60)$$

Пусть q – ненулевое рациональное число. Для любого натурального числа M и простого числа p , не делящего знаменатель q (в несократимой записи), существует такое натуральное число N , что $q+N$ делится на p^M .

Поскольку $B_{n+1}(X) \in \mathbb{Q}[X]$, $B_{n+1}(0) = B_{n+1} = 0$ (так как $n \geq 2$, n четно), то, очевидно, $B_{n+1}(q+N)/(n+1) - p$ -целое число при подходящем числе N . Подставляя $X = q$ в (60), видим, что $B_{n+1}(q)/(n+1) - p$ -целое число. Итак, рациональное число $B_{n+1}(q)/(n+1) - p$ -целое число, если p не делит знаменатель q . В частности, знаменатель числа $B_{n+1}(1/3)/(n+1)$ не делится на $p \neq 3$, т.е. он есть степень 3. Предложение 8 доказано.

Если l регулярно, то l не делит l -целые числа $B_{n+1}/(n+1)$ для нечетных $1 \leq n \leq l-4$. Поэтому из предложения 8 следует

ПРЕДЛОЖЕНИЕ 9. Пусть l регулярно, $1 \leq n \leq l-3$ нечетно. Тогда

$$\begin{aligned} l \text{ делит } F_n(-1) &\Leftrightarrow l \text{ делит } 2^{n+1} - 1, \\ l \text{ делит } E_n(0) &\Leftrightarrow l \text{ делит } (2^{n+1} - 1)(3^{n+1} - 1). \end{aligned}$$

Определим для натуральных чисел n ненулевые целые числа $\Delta(d, n)$, где $d = 2, 3, 6$, полагая $\Delta(2, n) = E_n(0)$; $\Delta(3, n) = \gcd(F_n(-1), F_n(2))$, если n нечетно, $\Delta(3, n) = F_n(2)$, если n четно; $\Delta(6, n) = \Delta_n$.

Пусть $t \in \Sigma_l$, $d(t) = |\mathbf{G}_t|$. Как мы показали выше, имеет место следующий критерий:

$$\begin{aligned} \text{если } d(t) = 2, 3, \text{ то } P_n(\mathbf{G}_t) \neq 0 &\Leftrightarrow l \nmid \Delta(d(t), n), \\ \text{если } d(t) = 6, \text{ то } l \nmid \Delta(6, n) &\Rightarrow P_n(\mathbf{G}_t) \neq 0. \end{aligned} \quad (61)$$

Пусть T – натуральное число. Положим $\mathbf{D}(l) = \{2, 3, 6\}$, если $l \equiv 1 \pmod{3}$, $\mathbf{D}(l) = \{3, 6\}$, если $l \equiv 2 \pmod{3}$. Пусть $d \in \mathbf{D}(l)$. Пусть $h(l, d, T)$ – максимальное натуральное четное число c такое, что $c \leq 2T$, $l \nmid \Delta(d, c)$. Такие числа c всегда существуют, так как $\Delta(d, 2) = 1$ (см. ниже). Положим $d_0 = 0$. Пусть при $j = 1, 2, 3$ $\mathbf{C}_j(l, d, T)$ обозначает множество строго возрастающих последовательностей натуральных чисел $d_1, \dots, d_N$ таких, что $d_N \leq h(l, d, T)$, и $\forall i, 1 \leq i \leq N$, множество натуральных чисел m таких, что $d_{i-1} < m \leq d_i$, $l \nmid \Delta(d, m)$, содержит соответственно $I(l) + 1$ четных и $I(l) + 1$ нечетных чисел (случай $j = 1$), $I(l) + 1$ нечетных чисел (случай $j = 2$), нечетное число (случай $j = 3$). Пусть $M_j(l, d, T)$ – максимум длин последовательностей из $\mathbf{C}_j(l, d, T)$. Пусть $M_j(l, T) = \min M_j(l, d, T)$, где минимум берется по $d \in \mathbf{D}(l)$. Напомним, что

$$J(l) = 1 + (I(l) + 1)(I(l) + 2).$$

Из определения чисел $N_j(t)$ (см. введение), критерия (61) и предложения 6 следует

ПРЕДЛОЖЕНИЕ 10. Пусть $l \geq 2T + 3$, а если l иррегулярно, то $l \geq 2TJ(l)$. Пусть $t \in \Sigma_l$, $d(t)$ – число элементов $\mathbf{G}_t$. Тогда при $j \in \{1, 2\}$ $N_j(t) \geq M_j(l, d(t), T)$, причем $N_j(t) = M_j(l, d(t), T)$, если $d(t) = 2, 3$, а $T = (l - 3)/2$. Далее, $N_3(t) \geq M_3(l, d(t), T) - I(l, T)$, где $I(l, T)$ – количество тех нечетных натуральных чисел $m < 2T$, для которых $l \mid B_{l-m}$. В частности, имеют место оценки $\varphi_j(l) \geq M_j(l, T)$ при $j \in \{1, 2\}$, $\varphi_3(l) \geq M_3(l, T) - I(l, T)$.

Предложение 10 показывает, как получать оценки снизу для $N_j(t)$, $\varphi_j(l)$, используя числа $\Delta(d, n)$, $1 \leq n \leq 2T$. Например, $\varphi_j(l) \geq [T/(I(l) + 1)]$ при $j = 1, 2$, $\varphi_3(l) \geq T - I(l, T)$ для всех простых регулярных чисел $l \geq 2T + 3$ и всех простых иррегулярных чисел $l \geq 2TJ(l)$, не делящих $\Delta(d, n)$ при $d \in \mathbf{D}(l)$, $1 \leq n \leq 2T$. Действительно, тогда, очевидно, $M_j(l, T) = [T/(I(l) + 1)]$, T , когда соответственно $j \in \{1, 2\}$, $j = 3$. Если число l , имеющее индекс иррегулярности I , принадлежит конечному множеству делителей чисел $\Delta(d, n)$, где $d \in \mathbf{D}(l)$, $1 \leq n \leq 2T$, то можно, например, пытаться доказать неравенство $\varphi_j(l) \geq N = [T/(I + 1)]$, $j \in \{1, 2\}$, найдя K (последовательно пробуя $K = T + 1, T + 2$ и т.д.) такое, что $2K + 3 \leq l$ при $I = 0$, $2K(1 + (I + 1)(I + 2)) \leq l$ при $I > 0$, и $M_j(l, K) = N$.

Можно использовать числа $\Delta(d, n)$, основываясь на критерии (61), и более обще, чем позволяет предложение 10. Например, пусть $I(l) = I > 0$, $N = [T/(I + 1)]$, $2T + 3 \leq l < 2TJ(l)$. Пусть $j \in \{1, 2\}$, последовательность $\{d_1, \dots, d_N\}$ принадлежит $\mathbf{C}_j(l, d, T)$ для всех $d \in \mathbf{D}(l)$, причем d_N четно и $l \nmid B_{l-1-d_N}$, $l \nmid \Delta(d, d_N)$ для всех $d \in \mathbf{D}(l)$. Тогда, учитывая критерий (61), $\{d_1, \dots, d_N\} \in \mathbf{A}_j(t)$ для всех $t \in \Sigma_l$. Значит, $\varphi_j(l) \geq N$.

Проиллюстрируем эту стратегию оценивания функций $\varphi_j(l)$ снизу. Вычисляя $E_n(X)$ с помощью (51) и разлагая $E_n(0)$ на простые множители, имеем

$$\begin{array}{ll} E_1 = 1, & E_1(0) = 1, \\ E_2 = 1, & E_2(0) = 1, \\ E_3 = X + 5, & E_3(0) = 5, \\ E_4 = X + 11, & E_4(0) = 11, \\ E_5 = X^2 + 28X + 91, & E_5(0) = 7 \cdot 13, \\ E_6 = X^2 + 58X + 301, & E_6(0) = 7 \cdot 43, \\ E_7 = X^3 + 123X^2 + 1431X + 3485, & E_7(0) = 5 \cdot 17 \cdot 41, \\ E_8 = X^3 + 249X^2 + 4539X + 15371, & E_8(0) = 19 \cdot 809, \\ E_9 = X^4 + 506X^3 + 16116X^2 + 117446X + 228811, & E_9(0) = 11^2 \cdot 31 \cdot 61. \end{array}$$

Учитывая, что $F_n(2) = 2^{(n-1-\nu(n)/2)} E_n(3/2)$, вычисляем и разлагаем на простые множители следующие числа:

$$F_2(2) = 1, \quad F_4(2) = 5^2, \quad F_6(2) = 7 \cdot 223, \quad F_8(2) = 5 \cdot 36389.$$

Кроме того, из (52) и [11] следует, что

$$E_{10}(0) = 683 \cdot 1847, \quad F_{10}(2) = 11 \cdot 41 \cdot 75571.$$

Нам также потребуются следующие разложения на простые множители:

$$2^2 - 1 = 3, \quad 2^4 - 1 = 3 \cdot 5, \quad 2^6 - 1 = 3^2 \cdot 7, \quad 2^8 - 1 = 3 \cdot 5 \cdot 17, \quad 2^{10} - 1 = 3 \cdot 11 \cdot 31.$$

Приведем также значения следующих чисел Бернулли (см. [2, гл. 5, § 8]):

$$B_2 = \frac{1}{6}, \quad B_4 = -\frac{1}{30}, \quad B_6 = \frac{1}{42}, \quad B_8 = -\frac{1}{30}, \quad B_{10} = \frac{5}{66}.$$

Очевидно, что $\Delta_n = 1$ при $1 \leq n \leq 6$ (тогда одно из $U_{n,i} = 1$).

Далее, имеем следующие равенства, определяющие значения $U_{n,i}$ для $n = 7, 8, 9$:

$$\begin{aligned} E_7 &= H(X) + 123X^2 + (1431 - b)X + 3485 + b, \\ E_8 &= H(X) + 249X^2 + (4539X - b)X + 15371 + b, \\ E_9 &= H(X)(X + 506) + (16116 - b)X^2 + (117446 - 505b)X + 228811 + 506b. \end{aligned}$$

Поскольку $U_{7,1} + U_{7,2} = 4916$ взаимно просто с $U_{7,0} = 123 = 3 \cdot 41$, то $\Delta_7 = 1$. Аналогично, $U_{8,1} + U_{8,2} = 19910$ взаимно просто с $U_{8,0} = 249 = 3 \cdot 81$, откуда следует, что $\Delta_8 = 1$. Далее имеем $U_{9,0} + U_{9,1} + U_{9,2} = 362373 = 1529 \cdot 3 \cdot 79$. С другой стороны, $505U_{9,0} - U_{9,1} = 8021134 = 1529 \cdot 5246$. Поскольку 5246 взаимно просто с $3 \cdot 79$, то Δ_9 делит 1529. С другой стороны, 1529 делит Δ_9 , так как $U_{9,0}(826) = 1529 \cdot 10$, $U_{9,1}(826) = -1529 \cdot 196$, $U_{9,2}(826) = 1529 \cdot 423$. Значит, $\Delta_9 = 1529 = 11 \cdot 139$. Значение Δ_{10} находим [11], учитывая (52): $\Delta_{10} = 1$.

Подведем некоторые итоги, анализируя полученные данные и используя предположение 10.

Очевидно, $\varphi_1(5) = 1$, так как $\varphi_1(5) \geq M_1(5, 1) = 1$, $\varphi_1(5) \leq 1$, поскольку $\varphi_1(l) \leq (l - 3)/2$ для любого l .

Рассмотрим случай $l = 7$. Очевидно, $M_1(7, d, 2) = 2$ ($d = 2, 3, 6$, используем (53) для анализа значений $F_n(-1)$ при нечетных n , см. также предположение 9). Поэтому $\varphi_1(7) \geq 2$, т.е. $\varphi_1(7)$ равно 2 $= (7 - 3)/2$.

Далее имеем $M_1(11, 3, 4) = M_1(11, 6, 4) = 4$ ($d = 2$ не рассматривается, так как $11 \equiv 2 \pmod{3}$). Так что $\varphi_1(11) = 4$.

Рассмотрим случай $l = 13$. Тогда $M_1(13, 2, 5) = M_2(13, 2, 5) = 4$, $M_1(13, d, 5) = 5$ при $d = 3, 6$. Поэтому $\varphi_1(13) = \varphi_2(13) = 4$, при этом $N_1(t) = 5$, если $d(t) \neq 2$, т.е. $t \notin \{-\xi, -\xi^2\}$, где $\xi^3 = 1$, $\xi \neq 1$.

Предположим, что регулярное $l \geq 17$. Анализ приведенных выше данных показывает, что $M_1(l, d, 5) = 5$ при $d \in \mathbf{D}(l)$, кроме следующих исключений:

$$\begin{aligned} M_1(l, 2, 5) &= 4 && \text{при } l = 19, 31, 43, 61, \\ M_1(l, 3, 5) &= 4 && \text{при } l = 41, 223, 36389, 75571, \\ M_1(l, 6, 5) &= 4 && \text{при } l = 139. \end{aligned}$$

Заметим, что 17 делит $F_7(-1)$, так как 17 делит $2^8 - 1$, и 31 делит $F_9(-1)$, так как 31 делит $2^{10} - 1$. В этих случаях дополнительная проверка показывает, что 17 не делит $F_7(2) = 2^3 \cdot E_7(3/2)$ и 31 не делит $F_9(2) = 2^4 \cdot E_9(3/2)$, так что $M_1(l, 3, 5) = 5$ и при $l = 17, 31$.

Имеем следующие разложения на простые множители:

$$2^{12} - 1 = 3^2 \cdot 5 \cdot 7 \cdot 13, \quad 3^{12} - 1 = 2^4 \cdot 5 \cdot 7 \cdot 13 \cdot 73.$$

Также имеем $B_{12} = -\frac{691}{2730}$ (см. [2, гл. 5, § 8]), а, учитывая (52), находим [11]

$$F_{12}(2) = 5 \cdot 7 \cdot 13 \cdot 20579903, \quad E_{12}(0) = 7 \cdot 13^2 \cdot 47 \cdot 2731, \quad \Delta_{12} = 13.$$

Учитывая (53), (54) и то, что ни одно из простых чисел, входящих в исключительный список, не появляется в этих разложениях, заключаем, что $M_1(l, d, 6) \geq 5$ при регулярных $l \geq 17$ и $d \in \mathbf{D}(l)$, кроме, возможно, случая $d = 6$ и $l = 139$. Значит, $\varphi_1(l) \geq 5$ при регулярных $l \geq 17$, $l \neq 139$.

Для полного описания множества тех регулярных l , для которых $\varphi_1(l) \geq 5$, остается разобрать случай $l = 139$. Поскольку (см. выше) $U_{9,i}(826) \equiv 0 \pmod{139}$ при $i = 0, 1, 2$ и $826 \equiv -8 \pmod{139}$, то

$$E_9 = H(X, -8)(X + 506) \pmod{139}.$$

Непосредственно проверяется, что

$$F\left(Y, \frac{-1 + \sqrt{5}}{2}\right) = H(Y + Y^{-1} - 1, -8),$$

что, конечно, эквивалентно тому, что $b((-1 + \sqrt{5})/2) = -8$. Учитывая, что $5 = 12^2 \pmod{139}$, отсюда следует, что $P_9(\mathbf{G}_t) = 0$ для $t = \frac{-1+12}{2} = \frac{11}{2} \pmod{139}$. При этом, конечно, $|\mathbf{G}_t| = 6$, что проверяется непосредственно, а также следует из предыдущего (139 не делит $E_9(0)F_9(-1)$), откуда $P_9(\mathbf{G}_t) \neq 0$, если $d(t) = 2, 3$. Орбита $\mathbf{G}_t$ является единственной, на которой обращается в нуль P_9 , так как $P_9(\mathbf{G}_{t'}) = 0 \Rightarrow |\mathbf{G}_{t'}| = 6$ и, следовательно, $E_9 \pmod{139}$ делится на $H(X, b(t'))$, откуда

$$U_{9,0}(b(t')) = 0 \Rightarrow b(t') = -8 \pmod{139} = b(t) \Rightarrow F(Y, t') = F(Y, t) \Rightarrow \mathbf{G}_{t'} = \mathbf{G}_t.$$

Поскольку $P_n(\mathbf{G}_{t'}) \neq 0$ при $d(t') = 6$, $1 \leq n \leq 8$ и $n = 10, 12$ (так как 139 не делит Δ_n для этих значений n), то для доказательства неравенства $N_1(t') \geq 5$ для t' таких, что $d(t') = 6$, достаточно проверить, что $P_{11}(\mathbf{G}_t) \neq 0$. Тогда, учитывая, что $N_1(t') \geq 5$ при $d(t') = 2, 3$, так как $M_1(139, d, 5) = 5$ для $d = 2, 3$, мы докажем, что $\varphi_1(139) \geq 5$. Достаточно показать, что $E_{11}(2) \not\equiv 0 \pmod{139}$, так как $P_{11}(\mathbf{G}_t) = 0 \Rightarrow E_{11} \pmod{139}$ делится на $H(X, b(t)) = H(x, -8) \pmod{139}$, а $H(2, -8) = 0$. Вычисляя $E_{11}(2) \pmod{139}$, используя E_9 и рекуррентные соотношения (51), убеждаемся в том, что $E_{11}(2) \not\equiv 0 \pmod{139}$.

Итак, мы доказали то, что $\varphi_1(l) \geq 5$ при регулярных $l \geq 17$, а также то, что $\varphi_1(5) = 1$, $\varphi_1(7) = 2$, $\varphi_1(11) = 4$, $\varphi_1(13) = \varphi_2(13) = 4$, причем для $l = 13$ $N_1(t) = 5$, если $d(t) \neq 2$, т.е. $t^2 - t + 1 \neq 0$.

Пусть $\mathbf{E}_1 = \{19, 31, 41, 43, 47, 61, 73, 139, 223, 2731\}$, $\mathbf{E}_2 = \{36389, 75571, 20579903, \text{простые делители } \Delta_{11}\}$. Поскольку $M_1(l, 6) = 6$ для регулярных $l \geq 17$, $l \notin \mathbf{E}_1 \cup \mathbf{E}_2$, то $\varphi_1(l) \geq 6$ для таких l .

Ясно также, что $M_3(l, 6) \geq 5$ для иррегулярных l (тогда $l \geq 37$), причем $M_3(l, 6) = 6$ для иррегулярных $l \notin \mathbf{E}_2$, $l \neq 691$.

Анализируя полученные выше данные, легко находим также, что при $I(l) = 1$ $M_1(l, 6) \geq 2$, а если $l \notin \mathbf{E}_2$, то $M_1(l, 6) = 3$. Далее, при $I(l) = 2$ $M_1(l, 6) \geq 1$, а если $l \notin \mathbf{E}_2$, $l \neq 691$, то $M_1(l, 6) = 2$. При $I(l) = 3, 4$ $M_1(l, 6) = 1$. При $I(l) = 5$ $M_1(l, 6) = 1$, если $l \neq 20579903$, $l \nmid \Delta_{11}$.

Из предложения 10 тогда следуют соответствующие оценки для $\varphi_1(l)$, $\varphi_3(l)$, если только $l \geq 12J(l)$. Используя [2, таблицы 11, 12], находим, что $l \geq 12J(l)$ при $1 \leq I(l) \leq 5$, кроме случаев $l = 37, 59, 67$, когда $I(l) = 1$. Для этих значений l , используя приведенные выше соображения для оценок снизу $\varphi_j(l)$ при $2T + 3 \leq$

$l < 2TJ(l)$, проверяется, что также $\varphi_1(l) \geq 2$, а если $l \notin \mathbf{E}_2$, то $\varphi_1(l) \geq 3$. Также проверяется, что $\varphi_3(37) \geq 4$, $\varphi_3(67) \geq 4$, $\varphi_3(59) \geq 5$, а если соответствующее простое число не делит Δ_{11} , то $\varphi_3(37) \geq 5$, $\varphi_3(67) \geq 5$, $\varphi_3(59) \geq 6$.

Из этих результатов и теорем 3, 4 следует теорема 7.

Список литературы

1. *Kummer E. E.* Allgemeiner Beweis des Fermat'schen Satzes, dass die Gleichung $x^\lambda + y^\lambda = z^\lambda$ durch ganze Zahlen unlösbar ist, für alle diejenigen Potenz-Exponenten λ , welche ungeza Primzahlen sind und in den Zählern der ersten $(\lambda - 3)/2$ Bernoulli'schen Zahlen als Factoren nicht vorkommen // J. für Math. 1850. V. 40. P. 130–138.
2. *Боревич З. И., Шафаревич И. Р.* Теория чисел. М.: Наука, 1985.
3. *Колывагин В. А.* Уравнения Ферма над круговыми полями // Тр. Матем. ин-та им. В. А. Стеклова РАН. 1995. Т. 208. С. 163–185.
4. *Колывагин В. А.* О первом случае теоремы Ферма для круговых полей // Изв. РАН. Сер. матем. 1999. Т. 63. № 5. С. 147–158.
5. *Krasner M.* Sur le premier cas du theoreme de Fermat // C. R. Acad. Sci. Paris. 1934. V. 199. P. 256–258.
6. *Eichler M.* Eine Bemerkung zur Fermat'schen Vermutung // Acta arithm. 1965. V. 11. P. 129–134.
7. *Vandiver H. S.* On Fermat's last theorem // Trans. Amer. Math. Soc. 1929. V. 31. P. 613–642.
8. *Колывагин В. А.* Формальные группы и символ норменного вычета // Изв. АН СССР. Сер. матем. 1979. Т. 43. № 5. С. 1054–1120.
9. *Iwasawa K.* Explicit formulas for the norm residue symbol // J. Math. Soc. Japan. 1968. V. 20. № 1–2. P. 151–165.
10. *Ленг С.* Алгебра. М.: Мир, 1968.
11. *Wada H.* Criteria of Kummer // Tokyo J. of Math. 1980. V. 3. № 1. P. 173–176.
12. *Keller W., Löh G.* The criteria of Kummer and Mirimanoff extended to include 22 consecutive irregular pairs // Tokyo J. of Math. 1983. V. 6. P. 397–402.
13. *Бейтмен Г., Эрдейи А.* Высшие трансцендентные функции. Т. I. М.: Наука, 1973.
14. *Wiles A.* Modular curves and Fermat's Last Theorem // Annals of Math. 1995. V. 141. P. 443–551.

Поступило в редакцию
7.VIII.2000