Общероссийский математический портал

В. А. Колывагин, О первом случае теоремы Ферма для круговых полей, *Изв. РАН. Сер. матем.*, 1999, том 63, выпуск 5, 147–158

DOI: <https://doi.org/10.4213/im262>

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

Параметры загрузки:

IP: 54.198.55.26

26 апреля 2023 г., 16:10:18

УДК 513.6

В. А. Колывагин

О первом случае теоремы Ферма для круговых полей

Классические критерии Куммера, Мириманова и Вандивера справедливости первого случая теоремы Ферма для поля рациональных чисел $\mathbb{Q}$ и простого показателя l обобщены на случай поля $\mathbb{Q}(\sqrt[l]{1})$ и показателя l . В качестве следствий получен ряд более простых критериев; например, доказана справедливость первого случая теоремы Ферма для поля $\mathbb{Q}(\sqrt[l]{1})$ и показателя l при условии, что l^2 не делит $2^l - 2$.

Библиография: 15 наименований.

Введение

Пусть $l > 3$ – простое число. Пусть K – поле. Говорят, что ТФ (теорема Ферма) верна для K и l , если уравнение

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

не имеет решений в ненулевых числах поля K .

Пусть K – конечное расширение поля рациональных чисел $\mathbb{Q}$ (числовое поле). Говорят, что 1СТФ (первый случай теоремы Ферма) верен для K и l , если (1) не имеет решений в целых числах поля K , взаимно простых с l .

Замечательное достижение последних лет – доказательство более чем трехсотлетней проблемы – ТФ для $\mathbb{Q}$ и всех $l > 3$ (см. [1]).

Вместе с тем исследование решений уравнений Ферма в более широких областях, чем поле $\mathbb{Q}$, а именно в его конечных (или даже бесконечных) расширениях, является, по-видимому, еще более трудной и интригующей проблемой.

Данная работа посвящена обобщению классических критериев Куммера, Мириманова и Вандивера справедливости 1СТФ для поля $\mathbb{Q}$ и l . Коротко говоря, мы доказываем при тех же условиях на l , которые накладываются в соответствующем классическом критерии, справедливость 1СТФ для поля L и l . Здесь L – круговое поле, порожденное над $\mathbb{Q}$ корнями l -й степени из 1.

Некоторыми авторами были получены более простые достаточные условия выполнения требований, налагаемых на l в вышеупомянутых критериях. Следствием стали соответствующие критерии справедливости 1СТФ для $\mathbb{Q}$ и l , например критерий Вифериха [2]: 1СТФ верен для $\mathbb{Q}$ и l , если l^2 не делит $2^l - 2$. Конечно, эти критерии для $\mathbb{Q}$ потеряли актуальность в силу полного доказательства ТФ для $\mathbb{Q}$ другими методами. Наш результат влечет, что при соответствующих условиях на l 1СТФ верен для поля L и l . В частности, 1СТФ верен для L и l , если l^2 не делит $2^l - 2$.

Сформулируем детально полученные результаты.

Пусть ζ – примитивный корень l -й степени из 1. Пусть O – кольцо целых поля $L = \mathbb{Q}(\zeta)$, $\alpha = (\zeta - 1)O$ – единственный простой идеал O , содержащий l . Поле

вычетов O/α может быть отождествлено с $\mathbb{Z}/l\mathbb{Z}$ с помощью канонического изоморфизма $\mathbb{Z}/l\mathbb{Z} \rightarrow O/\alpha$.

Пусть (x, y, z) – решение уравнения (1) в $O \setminus \alpha$. Пусть $G = G_{(x,y,z)}$ – подмножество в $\mathbb{Z}/l\mathbb{Z}$, состоящее из классов $(\bmod \alpha)$ чисел $-x/y, -x/z, -y/x, -y/z, -z/x, -z/y$. Поскольку $x+y+z \equiv x^l+y^l+z^l = 0 \pmod{\alpha}$, то G не содержит 0 и 1, а если $t \in G$, то G есть в точности множество $\{t, 1-t, 1/t, 1/(1-t), t/(t-1), 1-1/t\}$.

Пусть рациональные числа B_n определены разложением

$$\frac{X}{e^X - 1} = \sum_{n \geq 0} B_n \frac{X^n}{n!}.$$

Число B_n называется n -м числом Бернулли.

Рассмотрим также разложение

$$\frac{1}{1 - Y e^X} = \sum_{n \geq 0} f_n(Y) \frac{X^n}{n!}.$$

Легко доказать, что $f_n(Y) = P_n(Y)/(1-Y)^{n+1}$, где $P_n(Y)$ – унитарный многочлен степени n с целыми рациональными коэффициентами. Многочлены P_n могут быть последовательно вычислены с помощью рекуррентного соотношения

$$P_{n+1} = (n+1)Y P_n + (Y - Y^2) P'_n,$$

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. По поводу этих и других фактов о многочленах P_n см. § 2.

Докажем следующие теоремы.

ТЕОРЕМА 1. Пусть (x, y, z) – решение (1) в $O \setminus \alpha$. Если $t \in G_{(x,y,z)}$, то

$$B_{l-1-n} P_n(t) \equiv 0 \pmod{l} \quad \text{для } n = 1, 2, \dots, l-2. \quad (2)$$

ТЕОРЕМА 2. Пусть $(x, y, z), (x', y', z')$ – решения (1) в $O \setminus \alpha$. Если $t \in G_{(x,y,z)}$ и $u \in G_{(x',y',z')}$, то

$$P_n(t) P_{l-2-n}(u) \equiv 0 \pmod{l} \quad \text{для } n = 0, 1, \dots, l-2. \quad (3)$$

В частном случае рациональных решений $(x, y, z), (x', y', z')$ сравнения (2) и (3) были известны ранее: сравнение (2) было доказано Куммером [4], сравнение (3) с $u = t$ выведено Миримановым [5] из результата Куммера, Вандивер [6] расширил результат Мириманова на случай произвольной пары $t, u \in G_{(x,y,z)}, G_{(x',y',z')}$.

Исследование рациональных решений (1) в этих работах Куммера и Вандивера основано на разложении формы $x^l + y^l$ на линейные множители в L с последующим использованием арифметических свойств поля L . Данная работа, как и работа [3], развивает этот классический подход с целью исследования решений (1) во всем поле L . Отметим, что применимость к этой более общей проблеме методов, приведших к доказательству ТФ для $\mathbb{Q}$, в настоящее время не ясна.

Пусть H обозначает группу дробно-линейных преобразований $\{z, 1-z, 1/z, 1/(1-z), z/(z-1), 1-1/z\}$ множества $\mathbb{Z}/l\mathbb{Z} \setminus \{0, 1\}$. Орбиту G группы H назовем *допустимой*, если для любых $t, u \in G$ выполнены условия (2) и (3). Пусть $A(l)$ обозначает множество всех допустимых орбит группы H . Из теорем 1 и 2 следует

ТЕОРЕМА 3. Пусть $A(l)$ пусто. Тогда 1СТФ верен для L и l .

Соответственно результаты Куммера, Мириманова и Вандивера влекут, что пустота $A(l)$ влечет 1СТФ для $\mathbb{Q}$ и l .

Как уже отмечалось, с учетом результатов некоторых авторов, следствием теоремы 3 является серия более простых достаточных условий справедливости 1СТФ для L и l . Именно, имеют место следующие теоремы.

ТЕОРЕМА 4. Пусть l^2 не делит $q^l - q$ хотя бы для одного простого числа $q \leq 89$. Тогда 1СТФ верен для L и l . В частности, 1СТФ верен для L и l при $l \leq 7568 \cdot 10^{14}$.

ДОКАЗАТЕЛЬСТВО. Из работы [7] следует, что множество $A(l)$ пусто при выполнении первого условия на l из теоремы 4. В работе [14] показано, что это условие выполняется при $l \leq 7568 \cdot 10^{14}$. Остается применить теорему 3.

Пусть $[\rho]$ обозначает целую часть числа ρ .

ТЕОРЕМА 5. Пусть $v = \max\{22, [\sqrt[3]{\ln l}]\}$. 1СТФ верен для L и l , если числитель хотя бы одного числа Бернулли B_{l-1-2i} , $i = 1, 2, \dots, v$, не делится на l .

ДОКАЗАТЕЛЬСТВО. Из работ [8], [9] следует, что условие на l из теоремы 5 влечет пустоту $A(l)$ или условие $l^2 \nmid (2^l - 2)$. Но условие $l^2 \nmid (2^l - 2)$ само влечет пустоту $A(l)$. Поэтому теорема 5 следует из теоремы 3.

Обозначим через $ii(l)$ число тех чисел Бернулли $B_2, B_4, \dots, B_{l-3}$, числители которых делятся на l ($B_{2k+1} = 0$ при $k \geq 1$). Число $ii(l)$ называется *индексом иррегулярности* числа l .

Имеет место также

ТЕОРЕМА 6. 1СТФ верен для L и l , если $ii(l) \leq [\sqrt{l}] - 2$.

ДОКАЗАТЕЛЬСТВО. Пусть $t \in \mathbb{Z}/l\mathbb{Z} \setminus \{0, 1\}$, $N(t)$ обозначает число тех $n \in \{2, 4, \dots, l-3\}$, для которых $P_n(t) \equiv 0 \pmod{l}$. Пусть $M(t, r)$ обозначает размерность $\mathbb{Z}/l\mathbb{Z}$ -оболочки множества

$$\left\{ (1 - \zeta^{-1})i \left(\frac{1}{1 - \zeta^{-i}t} - \frac{1}{1 - \zeta^{-i}t^{-1}} \right), \quad i = 1, 2, \dots, r; \quad (1 - \zeta^{-1}) \right\}$$

в O/lO . В § 1 данной работы мы доказываем, что $M(t, r) \leq N(t) + 1$. Эйхлер [10] очень просто доказал, что $M(t, r) = r + 1$, если $t \neq 0, 1, -1$ и $r(r + 1) < l - 2$. Положим $r = [\sqrt{l}] - 1$. Тогда

$$r(r + 1) = ([\sqrt{l}] - 1)[\sqrt{l}] < l - \sqrt{l} < l - 2,$$

так как $l \geq 5$. Значит, $N(t) \geq M(t, r) - 1 = r$, если $t \neq 0, 1, -1$.

Предположим, что $ii(l) \leq r - 1$ и существует решение (x, y, z) уравнения (1) в $O \setminus \alpha$. Выберем $t \in G_{(x, y, z)}$ такое, что $t \neq -1$. Такое t всегда найдется, поскольку если $-1 \in G$, то $2 = 1 - (-1) \in G$, а $2 \not\equiv -1 \pmod{l}$ при $l > 3$. Из теоремы 1 следует, что $N(t) \leq ii(l)$. Значит, $N(t) \leq r - 1$, так как $ii(l) \leq r - 1$ по условию. Но выше мы показали, что $N(t) \geq r$. Противоречие.

Отметим, что ранее справедливость 1СТФ для L и l была известна при условии $ii(l) = 0$ (Куммер) и, более общо, в случае, если l не делит числители B_{l-3} и B_{l-5} [3].

Таким образом, 1СТФ верен для L и l , если l удовлетворяет одному из условий теорем 4–6. Результаты вычислений вызывают ощущение, что это условие на l выполняется с огромным запасом. Например, индекс иррегулярности $ii(l)$ в пределах вычислений (например, при $l \leq 125000$ [11]) мажорируется гораздо медленнее растущей функцией от l , чем $\sqrt{l}$, например $\ln l$. Далее, насколько автор знает, известны лишь два числа: $l = 1093$ и $l = 3511$, удовлетворяющие сравнению $2^l - 2 \equiv 0 \pmod{l^2}$, два числа: $l = 11$ и $l = 1006003$, удовлетворяющие сравнению $3^l - 3 \equiv 0 \pmod{l^2}$. В частности, не известно ни одного l такого, что l^2 делит одновременно $2^l - 2$ и $3^l - 3$. При $l < 125000$ нет ни одного l такого, что B_{l-7} делится на l и т. д.

С другой стороны, пока нет доказательства даже того, что эти казалось бы очень слабые условия на l выполняются для бесконечного числа чисел l . Так что 1СТФ (тем более, ТФ) для L и l не доказан пока для бесконечного числа чисел l .

Отметим, что существование бесконечного числа чисел l таких, что l^2 не делит $2^l - 2$, доказано [15] при условии верности абс-гипотезы Массера–Остерле для $\mathbb{Q}$. Следствием теоремы 4 и этого результата является

ТЕОРЕМА 7. 1СТФ верен для L и l для бесконечного числа простых чисел l , если верна абс-гипотеза Массера–Остерле для $\mathbb{Q}$.

§ 1. Доказательство теорем 1 и 2

Пусть γ – простой дивизор поля L , делящий l , K – γ -адическое пополнение L . Для доказательства теорем 1 и 2 нам потребуются некоторые факты, касающиеся арифметики поля K .

Пусть S – кольцо целых чисел поля K . Через λ обозначим единственный простой элемент S такой, что $\lambda^{l-1} + l = 0$, $\lambda \equiv \zeta - 1 \pmod{\lambda^2}$ (см. [12, гл. 5, § 6, лемма 1]). Существует единственное дифференцирование $D: S \rightarrow S/\lambda^{l-2}S$ такое, что

$$D(g(\lambda)) = g'(\lambda) \pmod{\lambda^{l-2}} \quad \forall g \in \mathbb{Z}_l[X].$$

Это так, поскольку гомоморфизм $g \mapsto g(\lambda)$ индуцирует изоморфизм $\mathbb{Z}_l[X]/g_0\mathbb{Z}_l[X] \rightarrow S$, где $g_0 = X^{l-1} + l$, а $g'_0(\lambda) = (l-1)\lambda^{l-2}$ ассоциировано с λ^{l-2} .

Из сравнения $\zeta \equiv 1 + \lambda + \lambda^2/2! + \dots + \lambda^{l-1}/(l-1)! \pmod{\lambda^l}$ (см. [12, гл. 5, § 6, лемма 3]) следует, что $D(\zeta) \equiv \zeta \pmod{\lambda^{l-2}}$.

Пусть U обозначает группу единиц кольца S . Определим гомоморфизм логарифмической производной $\varphi: U \rightarrow S/\lambda^{l-2}S$, положив $\varphi(u) = D(u)u^{-1}$.

Пусть V обозначает подгруппу U , состоящую из единиц $\equiv 1 \pmod{\lambda^2}$. Ряд

$$\ln(1 + X) = X - X^2/2 + \dots + (-1)^{n-1}X^n/n + \dots$$

сходится при $X \in \lambda S$, так что определено отображение $\ln: U \rightarrow K$. При этом $\ln(V) \subset \lambda^2 S$ и отображение $\ln: V \rightarrow \lambda^2 S$ является изоморфизмом группы V и аддитивной группы идеала $\lambda^2 S$ (см. [12, гл. 4, § 5, теорема 3]). Легко проверяется, что при $v \in V$ имеет место стандартная формула

$$D(\ln v) = \varphi(v).$$

Поле K содержит группу μ корней l -й степени из 1. Согласно локальной теории полей классов имеется невырожденное спаривание $K^*/(K^*)^l \times K^*/(K^*)^l \rightarrow \mu$, называемое *символом Гильберта l -й степени*, ассоциированным с полем K .

Пусть $\text{Tr}: K \rightarrow \mathbb{Q}_l$ – гомоморфизм следа. Нам потребуется следующая классическая явная формула (см. [13]) для значения $(u, v) := (u(K^*)^l, v(K^*)^l)$ при $u \in U$, $v \in V$:

$$(u, v) = \zeta^{\frac{\text{Tr}(\varphi(u) \ln(v))}{l}}. \quad (4)$$

Приступим непосредственно к доказательству теорем 1 и 2.

Пусть $k \in \{1, 2, \dots, l-1\}$, $i(k)$ обозначает элемент множества $\{1, 2, \dots, l-1\}$ такой, что $i(k)k \equiv 1 \pmod{l}$.

Положим $\omega_k = \omega_k(x, y, z) = (x + \zeta^{i(k)}y)/(x + y)$, $k = 1, 2, \dots, l-1$.

Положим $\kappa_m = \kappa_m(x, y, z) = \prod_{k=1}^{l-1} \omega_k^{k^m} \in L^*$, $m = 1, 2, \dots, l-2$.

Из предложения 1 работы [3] следует, что дивизор κ_m является l -й степенью. Поскольку

$$\begin{aligned} \frac{x + \zeta^{i(k)}y}{x + y} &\equiv \frac{x + (1 + \zeta - 1)^{i(k)}y}{x + y} \equiv \frac{x + (1 + i(k)(\zeta - 1))y}{x + y} \\ &\equiv 1 + \frac{i(k)(\zeta - 1)y}{x + y} \equiv \left(1 + \frac{(\zeta - 1)y}{x + y}\right)^{i(k)} \pmod{\lambda^2}, \end{aligned}$$

а $\sum_{k=1}^{l-1} k^m i(k) \equiv 0 \pmod{l}$ при $m = 2, \dots, l-2$, то $\kappa_m \in V$ при $m = 2, \dots, l-2$.

Пусть $\beta \in \{0, 1, \dots, l-1\}$ такой, что $\beta \pmod{l}$ является образующей группы $(\mathbb{Z}/l\mathbb{Z})^*$.

Положим $\theta_m = \prod_{k=1}^{l-1} \left(\frac{\zeta^{\beta i(k)} - 1}{\zeta^{i(k)} - 1}\right)^{k^m}$, $m = 2, \dots, l-3$.

Известно (см. [12, гл. 3, § 1, лемма 1]), что θ_m является единицей поля L .

Пусть δ пробегает множество простых дивизоров поля L , $(,)_\delta$ обозначает символ Гильберта l -й степени, ассоциированный с δ -адическим пополнением L_δ поля L . Согласно закону взаимности имеет место соотношение

$$\prod_{\delta} (a, b)_\delta = 1 \quad \forall a, b \in L^*. \quad (5)$$

Предположим теперь, что $a, b \in L^*$ таковы, что их дивизоры являются l -ми степенями. Пусть $\delta \neq \gamma$. Тогда L_δ – неразветвленное расширение поля $\mathbb{Q}_p$, где p – простое рациональное число, делящееся на δ . Значит, $(a, b)_\delta = 1$, так как $a, b \in U_\delta(L_\delta^*)^l$, где U_δ – группа единиц L_δ , а группа U_δ ортогональна самой себе относительно $(,)_\delta$ в случае неразветвленного расширения L_δ . Таким образом, в этом случае соотношение (5) эквивалентно соотношению

$$(a, b)_\gamma = 1.$$

Любая перестановка тройки (x, y, z) , очевидно, является решением (1) в $O \setminus \alpha$. Пусть (x_1, y_1, z_1) , (x_2, y_2, z_2) – любые две перестановки (x, y, z) , (x', y', z') соответственно. Положим $\kappa_{m,j} = \kappa_m(x_j, y_j, z_j)$, $j = 1, 2$. Через $(,)_\gamma$ обозначим символ $(,)_\gamma$. В частности, имеют место соотношения

$$(\kappa_{m,1}, \kappa_{l-m,2}) = 1, \quad (\theta_{l-m}, \kappa_{m,1}) = 1, \quad m = 2, \dots, l-2.$$

Пользуясь явной формулой (4), заключаем, что имеют место следующие сравнения:

$$\frac{\text{Tr}(\varphi(\kappa_{m,1}) \ln(\kappa_{l-m,2}))}{l} \equiv 0 \pmod{l}, \quad m = 2, \dots, l-2, \quad (6)$$

$$\frac{\text{Tr}(\varphi(\theta_{l-m}) \ln(\kappa_{m,1}))}{l} \equiv 0 \pmod{l}, \quad m = 2, \dots, l-2. \quad (7)$$

Вычислим $\varphi(\kappa_m)$. Пусть c обозначает x/y , $d = -c = -x/y$. Учитывая, что $\varphi(U^l) = 0$, $\varphi(\zeta) = 1$, имеем

$$\begin{aligned} \varphi(\kappa_m) &= \varphi\left(\prod_{k=1}^{l-1} (c + \zeta^{i(k)})^{k^m}\right) = \sum_{k=1}^{l-1} k^m \frac{D(c) + i(k)\zeta^{i(k)}}{c^l + 1} \cdot \frac{c^l + (\zeta^{i(k)})^l}{c + \zeta^{i(k)}} \\ &= \sum_{k=1}^{l-1} k^m \frac{D(c) + i(k)\zeta^{i(k)}}{c^l + 1} \left(\sum_{j=0}^{l-1} d^{l-1-j} \zeta^{i(k)j}\right) \\ &= \left(\frac{D(c)}{c^l + 1} \sum_{j=0}^{l-1} d^{l-1-j} \sum_{k=1}^{l-1} k^m \zeta^{i(k)j} \right. \\ &\quad \left. + \frac{1}{c^l + 1} \sum_{j=0}^{l-1} d^{l-1-j} \sum_{k=1}^{l-1} k^m i(k) \zeta^{i(k)(j+1)}\right) \pmod{\lambda^{l-2}}. \end{aligned}$$

Пусть $\xi_m = \sum_{k=1}^{l-1} k^m \zeta^{i(k)}$. Заметим, что при $r \in \{1, \dots, l-1\}$

$$\sum_{k=1}^{l-1} k^m \zeta^{i(k)r} \equiv r^m \sum_{k=1}^{l-1} (kr^{-1})^m \zeta^{i(k)r} \equiv r^m \xi_m \pmod{l}.$$

Поэтому имеем

$$\begin{aligned} \varphi(\kappa_m) &= \left(\frac{D(c)}{c^l + 1} \left(\sum_{j=1}^{l-1} d^{l-1-j} j^m\right) \xi_m \right. \\ &\quad \left. + \frac{1}{c^l + 1} \left(\sum_{j=0}^{l-2} d^{l-1-j} (j+1)^{m-1}\right) \xi_{m-1} - \frac{\delta_m^1}{c^l + 1}\right) \pmod{\lambda^{l-2}}, \end{aligned}$$

где δ_i^j – символ Кронекера.

Положим $Q_n(Y) = \sum_{r=1}^{l-1} r^n Y^r \in \mathbb{Z}[Y]$ при $n \geq 1$. Полагая $r = l - j$, имеем

$$\begin{aligned} \sum_{j=1}^{l-1} d^{l-1-j} j^m &= d^{-1} \sum_{j=1}^{l-1} d^{l-j} j^m = d^{-1} \sum_{r=1}^{l-1} d^r (l-r)^m \\ &\equiv d^{-1} (-1)^m Q_m(d) \pmod{l}. \end{aligned}$$

Полагая $r = l - 1 - j$, имеем

$$\sum_{j=0}^{l-2} d^{l-1-j} (j+1)^{m-1} = \sum_{r=1}^{l-1} d^r (l-r)^{m-1} \equiv (-1)^{m-1} Q_{m-1}(d) \pmod{l}.$$

Поэтому имеем соотношение:

$$\begin{aligned} \varphi(\kappa_m) = & \left(\frac{(-1)^{m-1}}{c^l + 1} Q_{m-1}(d) \xi_{m-1} - \frac{\delta_m^1}{c^l + 1} \right. \\ & \left. + \frac{(-1)^m d^{-1} D(c)}{c^l + 1} Q_m(d) \xi_m \right) \pmod{\lambda^{l-2}}. \end{aligned} \quad (8)$$

Пусть $E(X) = 1 + X/1! + \dots + X^{l-1}/(l-1)!$. Согласно [12, гл. 5, § 6, лемма 3] имеет место сравнение $\zeta^{i(k)} \equiv E(i(k)\lambda) \pmod{\lambda^l}$. Отсюда имеем

$$\xi_m \equiv \sum_{k=1}^{l-1} k^m E(i(k)\lambda) \equiv -\lambda^m \pmod{l}. \quad (9)$$

Заметим, что $c^l + 1 = (x/y)^l + 1 = -(z/y)^l \not\equiv 0 \pmod{\lambda}$.

Учитывая (8) и (9), получаем сравнение

$$\varphi(\kappa_m) \equiv \left(s_m Q_{m-1}(t) \lambda^{m-1} - \frac{\delta_m^1}{1-t} \right) \pmod{\lambda^m}, \quad (10)$$

где $t, s_m \in (\mathbb{Z}/l\mathbb{Z})^*$, $t \equiv d \pmod{\lambda}$, $s_m = (-1)^{m-1}/(1-t)$.

Пусть ниже m принимает значения $2, \dots, l-2$.

Пусть $\ln \kappa_m = \eta_2 \lambda^2 + \dots + \eta_{l-2} \lambda^{l-2} \pmod{\lambda^{l-1}}$, где $\eta_j \in \mathbb{Z}_l$. Тогда

$$\begin{aligned} 2\eta_2 \lambda + \dots + (l-2)\eta_{l-2} \lambda^{l-3} & \equiv D(\ln \kappa_m) \\ & = \varphi(\kappa_m) \equiv s_m Q_{m-1}(t) \lambda^{m-1} \pmod{\lambda^m}. \end{aligned}$$

Отсюда заключаем, что

$$\ln \kappa_m \equiv s_m Q_{m-1}(t) \frac{\lambda^m}{m} \pmod{\lambda^{m+1}}. \quad (11)$$

Пусть $t \in G_{(x,y,z)}$, $u \in G_{(x',y',z')}$. Очевидно, найдутся перестановки (x_1, y_1, z_1) , (x_2, y_2, z_2) троек (x, y, z) , (x', y', z') такие, что $t \equiv -x_1/y_1 \pmod{\lambda}$, $u \equiv -x_2/y_2 \pmod{\lambda}$. Из сравнения (10), примененного к решению (x_1, y_1, z_1) , и сравнения (11), примененного к решению (x_2, y_2, z_2) , следует, что при некоторых $r_m, h_{l-m} \in S$ имеем

$$\begin{aligned} \varphi(\kappa_{m,1}) & = (s_{m,1} Q_{m-1}(t) \lambda^{m-1} + r_m \lambda^m) \pmod{\lambda^{l-2}}, \\ \ln(\kappa_{l-m,2}) & = s_{l-m,2} Q_{l-m-1}(u) \frac{\lambda^{l-m}}{l-m} + h_{l-m} \lambda^{l-m+1}, \end{aligned}$$

где

$$s_{m,1} = \frac{(-1)^{m-1}}{1-t}, \quad s_{l-m,2} = \frac{(-1)^{l-m-1}}{1-u}.$$

Значит, учитывая равенство $\lambda^{l-1} = -l$, имеем

$$\varphi(\kappa_{m,1}) \ln(\kappa_{l-m,2}) = \frac{s_{m,1} s_{l-m,2}}{(l-m)} Q_{m-1}(t) Q_{l-1-m}(u) (-l) \pmod{\lambda^l}.$$

Учитывая (6), заключаем, что при $m = 2, \dots, l-2$

$$\begin{aligned} & \frac{\text{Tr}(\varphi(\kappa_{m,1}) \ln(\kappa_{l-m,2}))}{l} \\ & \equiv \frac{(1-l)}{(l-m)} s_{m,1} s_{l-m,2} Q_{m-1}(t) Q_{l-1-m}(u) \equiv 0 \pmod{\lambda}. \end{aligned}$$

Поскольку $s_{m,1}, s_{l-m,2} \in (\mathbb{Z}/l\mathbb{Z})^*$, это эквивалентно сравнениям

$$Q_n(t) Q_{l-2-n}(u) \equiv 0 \pmod{l}, \quad n = 1, 2, \dots, l-3. \quad (12)$$

Далее, при $n \geq 1$, $v \in \mathbb{Z}/l\mathbb{Z} \setminus \{0, 1\}$ имеет место сравнение (см. [7, с. 332])

$$Q_n(v) \equiv f_n(v)(1-v)^l \pmod{l}.$$

Поскольку $f_n(v) = P_n(v)/(1-v)^{n+1}$, то имеем сравнение

$$Q_n(v) \equiv (1-v)^{l-1-n} P_n(v) \pmod{l}.$$

Вариант доказательства этого сравнения приведен также в § 2.

Значит, сравнения (12) эквивалентны сравнениям (3) при $n = 1, 2, \dots, l-3$.

Чтобы завершить доказательство теоремы 2, нам остается только доказать сравнение $P_0(t)P_{l-2}(u) \equiv 0 \pmod{l}$, т. е. сравнение $P_{l-2}(u) \equiv 0 \pmod{l}$. Достаточно показать, что $Q_{l-2}(u) \equiv 0 \pmod{l}$. Имеем

$$Q_{l-2}(u) = \sum_{r=1}^{l-1} r^{l-2} u^r \equiv \sum_{r=1}^{l-1} r^{-1} u^r \pmod{l}.$$

Поскольку $(x_2/y_2)^l + 1 + (z_2/y_2)^l = 0$, то

$$z_2/y_2 \equiv (z_2/y_2)^l \equiv -1 - (x_2/y_2)^l \equiv (-1 + u) \pmod{\lambda}.$$

Значит, $x_2/y_2 = -a + \lambda h$, $z_2/y_2 = a - 1 + \lambda g$, где $h, g \in S$, $a \in \mathbb{Z}$, $a \equiv u \pmod{l}$. Следовательно,

$$0 = (-a + \lambda h)^l + 1 + (a - 1 + \lambda g)^l \equiv -a^l + 1 + (a - 1)^l \pmod{l\lambda}.$$

Значит, $(a - 1)^l - a^l + 1 \equiv 0 \pmod{l^2}$. Остается заметить, что

$$\frac{(a - 1)^l - a^l + 1}{l} = \sum_{r=1}^{l-1} \left(\frac{C_l^r}{l} \right) (-1)^{l-r} a^r \pmod{l} \equiv \sum_{r=1}^{l-1} r^{-1} u^r,$$

так как $C_l^r/l = (l-1) \dots (l-(r-1))/r! \equiv (-1)^{r-1}/r \equiv (-1)^{l-r}/r \pmod{l}$.

Докажем оценку $M(t, r) \leq N(t) + 1$, используемую во введении. Итак, пусть t – произвольный элемент множества $\mathbb{Z}/l\mathbb{Z} \setminus \{0, 1\}$. Пусть $b \in \mathbb{Z}$ такое, что $b \equiv t \pmod{l}$. Соотношение (8) доказано нами при произвольных $x, y \in S$ таких, что $y \not\equiv 0 \pmod{\lambda}$, $x + y \not\equiv 0 \pmod{\lambda}$. Положим $x = -b$, $y = 1$, $\beta_m = \prod_{k=1}^{l-1} (-b + \zeta^{i(k)})^{k^m}$, $m = 0, 1, \dots, l-2$.

Поскольку $D(\mathbb{Z}_l) = 0$, соотношение (8), с учетом сравнения (9), влечет сравнение

$$\varphi(\beta_m) = \left(s_m Q_{m-1}(t) \lambda^{m-1} - \frac{\delta_m^1}{1-t} \right) \pmod{\lambda^{l-2}}, \quad m = 1, \dots, l-2. \quad (13)$$

Кроме того, $\varphi(\beta_0) = 0$, так как $\beta_0 \in \mathbb{Z}_l$.

Поскольку $\sum_{k=1}^{l-1} k^m \equiv 0 \pmod{l}$ при $m = 1, \dots, l-2$, $\sum_{k=1}^{l-1} k^0 \equiv -1 \pmod{l}$, имеем

$$(-b + \zeta)^{-1} = \prod_{m=0}^{l-1} \beta_m \pmod{(K^*)^l}.$$

Переходя к значению φ , получаем соотношение

$$\frac{\zeta}{-t + \zeta} \equiv \sum_{m=1}^{l-1} \varphi(\beta_m) \pmod{\lambda^{l-2}}. \quad (14)$$

Далее, имеем

$$\begin{aligned} i \left(\frac{1}{1-t\zeta^{-i}} - \frac{1}{1-t^{-1}\zeta^{-i}} \right) + i &= \frac{i\zeta^i}{-t + \zeta^i} - \frac{it^{-1}\zeta^{-i}}{1-t^{-1}\zeta^{-i}} \\ &= \frac{i\zeta^i}{-t + \zeta^i} + \frac{i\zeta^{-i}}{-t + \zeta^{-i}} = \sigma_i(\sigma_1 + \sigma_{-1}) \left(\frac{\zeta}{-t + \zeta} \right), \end{aligned}$$

где σ_j – автоморфизм K над $\mathbb{Q}_l$ такой, что $\sigma_j(\zeta) = \zeta^j$, $j \in (\mathbb{Z}/l\mathbb{Z})^*$.

Аutomорфизм σ_j действует на λ умножением на η_j , где η_j – корень $(l-1)$ -й степени из 1 в $\mathbb{Z}_l^*$, $\eta_j \equiv j \pmod{l}$. В частности, $\sigma_{-1}(\lambda) = -\lambda$. Поэтому из (13), (14) и соотношения, полученного выше, следует, что $M(t, r)$ не превосходит размерности $\mathbb{Z}/l\mathbb{Z}$ -оболочки в $S/lS = O/lO$ множества, состоящего из 1 и $\{\lambda^n, n \in \{2, 4, \dots, l-3\}, Q_n(t) \neq 0\}$. Поскольку $P_n(t) \neq 0$, если $Q_n(t) \neq 0$, то $M(t, r) \leq N(t) + 1$.

Займемся теперь доказательством теоремы 1. Для этого нам потребуется вычислить $\varphi(\theta_m)$. Пусть $i \in \{1, 2, \dots, l-1\}$. Имеем

$$\begin{aligned} \varphi \left(\frac{\zeta^{\beta i} - 1}{\zeta^i - 1} \right) &= \varphi(1 + \zeta^i + \dots + \zeta^{i(\beta-1)}) \\ &= i(\zeta^i + 2\zeta^{2i} + \dots + (\beta-1)\zeta^{(\beta-1)i}) \frac{\zeta^i - 1}{\zeta^{\beta i} - 1} \\ &= i(\zeta^{2i} + 2\zeta^{3i} + \dots + (\beta-1)\zeta^{\beta i} - \zeta^i - 2\zeta^{2i} - \dots - (\beta-1)\zeta^{(\beta-1)i}) \frac{1}{\zeta^{\beta i} - 1} \\ &= i((\beta-1)\zeta^{\beta i} - \zeta^i - \zeta^{2i} - \dots - \zeta^{(\beta-1)i}) \frac{1}{\zeta^{\beta i} - 1} \\ &= i \left(\beta\zeta^{\beta i} - \zeta^i \frac{\zeta^{\beta i} - 1}{\zeta^i - 1} \right) \frac{1}{\zeta^{\beta i} - 1} \\ &= \frac{i\beta\zeta^{\beta i}}{\zeta^{\beta i} - 1} - \frac{i\zeta^i}{\zeta^i - 1} = \left(i\sigma_i(\beta\sigma_\beta - 1) \frac{\zeta}{\zeta - 1} \right) \pmod{\lambda^{l-2}}. \end{aligned}$$

Значит,

$$\varphi(\theta_m) = \left(\sum_{k=1}^{l-1} k^{m-1} \sigma_{i(k)} \right) \left((\beta \sigma_\beta - 1) \frac{\zeta}{\zeta - 1} \right) \pmod{\lambda^{l-2}}. \quad (15)$$

Заметим, что $\zeta/(\zeta - 1) = (\zeta + 2\zeta^2 + \dots + (l-1)\zeta^{l-1} + l)/l$. Действительно,

$$\begin{aligned} & (\zeta - 1)(\zeta + 2\zeta^2 + \dots + (l-1)\zeta^{l-1} + l\zeta^l) \\ &= \zeta((\zeta + 2\zeta^2 + \dots + l\zeta^l) - (1 + 2\zeta + \dots + l\zeta^{l-1})) \\ &= \zeta(l - (1 + \zeta + \dots + \zeta^{l-1})) = \zeta l, \end{aligned}$$

так как $1 + \zeta + \dots + \zeta^{l-1} = (\zeta^l - 1)/(\zeta - 1) = 0$. Итак,

$$\frac{\zeta}{\zeta - 1} = \left(\frac{1}{l} \sum_{j=1}^{l-1} j \sigma_j \right) \zeta + 1.$$

Заметим, что $\left(\sum_{k=1}^{l-1} \eta_k^{m-1} \sigma_{i(k)} \right) \sigma_j = \eta_j^{m-1} \left(\sum_{k=1}^{l-1} \eta_k^{m-1} \sigma_{i(k)} \right)$. Учитывая (15) и сравнение $\eta_k \equiv k^{l^{n-1}} \pmod{l^n}$, имеем

$$\begin{aligned} \varphi(\theta_m) &\equiv \left(\sum_{k=1}^{l-1} \eta_k^{m-1} \sigma_{i(k)} \right) \left((\beta \sigma_\beta - 1) \frac{\zeta}{\zeta - 1} \right) \\ &\equiv \left(\left(\sum_{k=1}^{l-1} \eta_k^{m-1} \sigma_{i(k)} \right) (\beta \sigma_\beta - 1) \frac{1}{l} \left(\sum_{j=1}^{l-1} j \sigma_j \right) \right) \zeta \\ &\equiv \left((\beta^m - 1) \left(\sum_{j=1}^{l-1} j \eta_j^{m-1} \right) l^{-1} \right) \left(\sum_{k=1}^{l-1} \eta_k^{m-1} \sigma_{i(k)} \right) \zeta \\ &\equiv \left((\beta^m - 1) \left(\sum_{j=1}^{l-1} j \eta_j^{m-1} \right) l^{-1} \right) \xi_{m-1} \pmod{\lambda^{l-2}}. \end{aligned}$$

Далее, имеем

$$\left(\sum_{j=1}^{l-1} j \eta_j^{m-1} \right) l^{-1} \equiv \left(\sum_{j=1}^{l-1} j^{1+l(m-1)} \right) l^{-1} \equiv B_{1+l(m-1)} \pmod{l}$$

согласно равенству (5) из [12, гл. 5, § 8].

Учитывая, что имеет место сравнение [12, гл. 5, § 8, теорема 5]

$$\frac{B_{1+l(m-1)}}{1+l(m-1)} \equiv \frac{B_m}{m} \pmod{l},$$

получаем соотношение

$$\varphi(\theta_m) = -\frac{(\beta^m - 1)}{m} B_m \lambda^{m-1} \pmod{\lambda^{l-2}}. \quad (16)$$

Поскольку мы доказали, что $P_{l-2}(t) \equiv 0 \pmod{l}$, то достаточно доказать сравнение (2) для $n = 1, \dots, l-3$. Оно следует немедленно из (7), (11) и (16), при этом учитываем, что $Q_n(t) \equiv (1-t)^{l-1-n} P_n(t) \pmod{l}$.

§ 2. Многочлены P_n

Докажем приведенные во введении утверждения о коэффициентах разложения

$$\frac{1}{1 - Ye^X} = \sum_{n \geq 0} f_n(Y) \frac{X^n}{n!}.$$

Положим $f_n(Y, X) = \frac{d^n}{dX^n} \left(\frac{1}{1 - Ye^X} \right)$, $n \geq 0$. Покажем индукцией по n , что

$$f_n(Y, X) = \frac{P_n(Ye^X)}{(1 - Ye^X)^{n+1}},$$

где P_n – унитарный многочлен степени n с целыми рациональными коэффициентами. Очевидно, утверждение имеет место при $n = 0$ с $P_0 = 1$. Предположим, что оно верно при $n \geq 0$. Тогда

$$\begin{aligned} f_{n+1}(Y, X) &= \frac{d}{dX} f_n(Y, X) = \frac{d}{dX} \left(\frac{P_n(Ye^X)}{(1 - Ye^X)^{n+1}} \right) \\ &= \frac{P'_n(Ye^X)Ye^X}{(1 - Ye^X)^{n+1}} + \frac{(n+1)P_n(Ye^X)Ye^X}{(1 - Ye^X)^{n+2}} \\ &= \frac{(n+1)P_n(Ye^X)Ye^X + P'_n(Ye^X)Ye^X(1 - Ye^X)}{(1 - Ye^X)^{n+2}}. \end{aligned}$$

Значит,

$$f_{n+1}(Y, X) = \frac{P_{n+1}(Ye^X)}{(1 - Ye^X)^{n+2}},$$

где

$$P_{n+1}(Z) = (n+1)P_n(Z)Z + P'_n(Z)(Z - Z^2). \quad (17)$$

В частности, имеем представление

$$f_n(Y) = f_n(Y, 0) = \frac{P_n(Y)}{(1 - Y)^{n+1}}$$

и рекуррентное соотношение (17) для многочленов P_n .

Многочлены P_n могут быть вычислены явно. Именно, из определений следует, что имеет место соотношение

$$P_n(Y) = -\tilde{P}_{n+1}(-Y), \quad n \geq 1, \quad (18)$$

где $\tilde{P}_m(Y)$ – многочлены, рассматриваемые в [5] (мы заменяем обозначение P_m в [5] на $\tilde{P}_m$).

Мириманов приводит явные формулы для коэффициентов $\tilde{P}_m$. Эти формулы в силу (18) позволяют явно определить коэффициенты многочленов $P_n(Y)$. Именно,

$$P_n(Y) = b_{n,1}Y + b_{n,2}Y^2 + \dots + b_{n,n}Y^n,$$

где

$$b_{n,k} = k^n - C_{n+1}^1(k-1)^n + \dots + (-1)^{k-1}C_{n+1}^{k-1}, \quad k = 1, \dots, n.$$

Здесь C_i^j обозначают биномиальные коэффициенты.

В частности, $b_{n,1} = 1$, $b_{n,2} = 2^n - (n+1)$ и т. д.

При этом имеют место соотношения $b_{n,k} = b_{n,n+1-k}$.

Заметим, что из работы [5] в силу (18) следует, что сравнения (2) для любого $t \in \mathbb{Z}/l\mathbb{Z} \setminus \{0, 1\}$ эквивалентны сравнениям (3) при $u = t$. Поэтому, учитывая результаты Мириманова, видим, что теорема 1 является следствием теоремы 2, что дает другое доказательство теоремы 1.

Напомним, что при $n \geq 1$ $Q_n(Y)$ обозначает многочлен $\sum_{r=1}^{l-1} r^n Y^r$. Положим $Q_0(Y) = 1 + \sum_{r=1}^{l-1} Y^r$. Многочлены $P_n(Y)$ связаны с многочленами $Q_n(Y)$ известным сравнением:

$$Q_n(Y) \equiv (1 - Y)^{l-1-n} P_n(Y) \pmod{l}, \quad n = 0, 1, \dots, l-1. \quad (19)$$

Сравнение (19) непосредственно проверяется при $n = 0$:

$$Q_0(Y) = \frac{1 - Y^l}{1 - Y} \equiv \frac{(1 - Y)^l}{1 - Y} = (1 - Y)^{l-1} = (1 - Y)^{l-1} P_0 \pmod{l},$$

затем можно применить индукцию по n , учитывая (17) и очевидное рекуррентное соотношение $Q_{n+1} = YQ'_n$.

Список литературы

1. Wiles A. Modular curves and Fermat's Last Theorem // Annals of Math. 1995. V. 141. P. 443–551.
2. Wieferich A. Zum letzten Fermat'schen Theorem // J. Reine Angew. Math. 1909. V. 136. P. 293–302.
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. Kummer E. E. Einige Sätze über die aus den Wurzeln der Gleichung $\alpha^\lambda = 1$ gebildeten complexen Zahlen, für den Fall dass die Klassensahl durch λ theilbar ist, nebst Anwendungen derselben auf einen weiteren Beweis des letzten Fermat'schen Lehrsatzes // Math. Abh. Akad. Wiss. Berlin. 1857. P. 41–74.
5. Mirimanoff D. L'équation indéterminée $x^l + y^l + z^l = 0$ et le criterium de Kummer // J. Reine Angew. Math. 1905. V. 128. P. 45–68.
6. Vandiver H. S. Laws of reciprocity and the first case of Fermat's last theorem // Proc. Nat. Acad. Sci. U.S.A. 1925. V. 11. P. 292–298.
7. Granville A., Monagan M. B. The first case of Fermat's last theorem is true for all prime exponents up to 714,591,416,091,389 // Transactions of the American Math. Soc. 1988. V. 306. P. 329–359.
8. Krasner M. Sur le premier cas du théorème de Fermat // C.R. Acad. Sci. Paris. 1934. V. 199. P. 256–258.
9. Keller W., Löh G. The criteria of Kummer and Mirimanoff extended to include 22 consecutive irregular pairs // Tokyo J. Math. 1983. V. 6. P. 397–402.
10. Eichler M. Eine Bemerkung zur Fermat'schen Vermutung // Acta arithm. 1965. V. 11. P. 129–131.
11. Wagstaff S. S. The irregular primes to 125000 // Math. Comput. 1978. V. 32. P. 583–591.
12. Борович З. И., Шафаревич И. Р. Теория чисел. М.: Наука, 1985.
13. Iwasawa K. On explicit formulas for the norm residue symbol // J. Math. Soc. Japan. 1968. V. 20. P. 151–164.
14. Coppersmith D. Fermat's last theorem (case 1) and the Weiferich criterion // Math. Comput. 1990. V. 54. P. 895–902.
15. Silverman J. H. Wieferich's Criterion and abc-Conjecture // J. Number Theory. 1988. V. 30. P. 226–237.

Поступило в редакцию
14.VII.1998