Шаг 4. Увеличиваем поток из источника s в сток t:

$$x_{ij} := \begin{cases} x_{ij} + \varepsilon, \text{ если } (i, j) \in L \setminus L^{-}, \\ x_{ij} - \varepsilon, \text{ если } (i, j) \in L^{-}. \end{cases}$$

Если $C_{\varepsilon} < C$, то переходим к шагу 1. В противном случае алгоритм заканчивает работу. Вычисляем элементы матрицы оптимального синтеза $\overline{\mathbf{Y}}^0 = \|\overline{y}^0{}_{ij}\|$ приведенной сети

$$\overline{\mathbf{y}}_{ij}^0 = \begin{cases} x_{ij}^0 - \overline{d}_{ij}, \text{ если } x_{ij}^0 > \overline{d}_{ij}; \\ 0, \quad \text{в остальных случаях.} \end{cases}$$

По формулам (6) находим матрицу оптимального преобразования $\mathbf{Y}^0$ исходной задачи.

Корректность алгоритма следует из того, что, как это было доказано, в сети не возникает циклов отрицательного веса, и по построению матрицы $\overline{\mathbf{C}} = \|\overline{c}_{ij}\|$ стоимость оптимального синтеза исходной многополюсной и приведенной сети совпадают.

ВЫВОД

Получены алгоритмы оптимального синтеза многополюсных сетей, которые могут использоваться при решении любых задач, связанных оптимальным преобразованием динамических систем, допускающих формулировку в терминах теории графов.

ЛИТЕРАТУРА

1. **Корзников А. Д., Корзников В. А.** Моделирование и оптимизация процесса перемещения грузов в логистической транспортной системе // Вестник БНТУ. – 2003. – № 6. – С. 54–60.

2. **Меламед И. И.** Методы оптимизации в транспортном процессе // ИНТ ВИНИТИ. Сер. организации управления транспортом. – 1991. – № 10. – 165 с.

3. **Fulkerson D. R.** Increasing the Capacity of a Network, the Parametric Budget Problem // Man. Sci., 5(4), 1959. – P. 472–483.

4. **Hu T. C.** Minimum Convex Cost Flows // NRLQ, 13(1), 1966. – P. 1–9.

УДК 511.522.2

ПОЛНОЕ ДОКАЗАТЕЛЬСТВО ВЕЛИКОЙ ТЕОРЕМЫ ФЕРМА

Студ. ЛЕЩИНСКИЙ А. С.

Белорусский национальный технический университет

История великой теоремы Ферма началась в 1637 г., когда французский математик Пьер Ферма (1601…1665) сформулировал теорему, согласно которой при натуральном $n > 2$ уравнение $x^n + y^n = z^n$ не имеет решений в целых положительных числах x, y, z.

Для полного доказательства достаточно доказать две теоремы.

Теорема 1.0. *$h_2 \not\equiv 0$ mod$p$, где h_2 – второй множитель числа классов идеалов кругового поля $Q(\zeta_p)$; p – простое нечетное число.*

Теорема 2.0. *Для простого показателя $p \geq 5$ справедлив второй случай теоремы Ферма, если $h_2 \not\equiv 0$ mod$p$.*

Первый случай теоремы Ферма при $h_2 \not\equiv 0$ mod$p$ был доказан Вандивером. В дальнейшем будем использовать обозначение $\zeta_p = \zeta = e^{\frac{2\pi}{p}i}$.

Теорема 2.1. *Уравнение*

$$x^p + y^p = \varepsilon \pi^{np} z^p,$$

где $x, y, z, \varepsilon \in Z[\zeta + \zeta^{-1}]$, ε – единица кольца, целое $n \geq 1$, простое $p \geq 5$, $\pi = (1 - \zeta)(1 - \zeta^{-1})$, не имеет решений в ненулевых x, y, z.

☐ Пусть уравнение имеет решение в ненулевых x, y, z.

Из всех этих решений выберем такое, у которого $|Nz|$, модуль нормы элемента z, принимает минимальное значение

$$(\pi)^{np}(z)^p=(x^p+y^p)=(x+y)\prod_{i=1}^{m}(x^2+y^2+xy(\zeta^i+\zeta^{-i})),$$

где $m = (p-1)/2$.

Так как кольцо $Z(\zeta+\zeta^{-1})$ допускает теорию дивизоров с числом классов, равным h_2, имеем:

$$(x+y)^2=(\pi)^{(2n-1)p+1}\aleph^2\Re_0^2;$$

$$(x^2+y^2+xy(\zeta^i+\zeta^{-i}))=(\pi)\aleph^2\Re_i,\ i=1,\ \ldots,\ m,$$

где $\aleph$ – наибольший общий делитель главных дивизоров (x) и (y), который не делится на (π).

Так как $\Re_0$, $\Re_i$ взаимно просты, то:

$$(x^2+y^2+2xy)=(\pi)^{(2n-1)p+1}\aleph^2\Im_0^{2p};$$

$$(x^2+y^2+xy(\zeta^i+\zeta^{-i}))=(\pi)\aleph^2\Im_i^p,$$

где $\Re_0=\Im_0^p$, $\Re_i=\Im_i^p$.

После перекрестного умножения этих уравнений имеем

$$(x^2+y^2+2xy)\ \Im_i^p=$$
$$=(x^2+y^2+xy(\zeta^i+\zeta^{-i}))(\pi)^{(2n-1)p}\Im_0^{2p}.$$

Умножим уравнение на дивизор $\Im^p$, такой что $\Im_0^{2p}\Im^p=N\Im_0^{2p}=(\gamma)^p$. Так как $h_2\not\equiv 0 \bmod p$, то дивизоры $\Im^p\Im_i^p=(\alpha_i)^p$ – главные, тогда

$$(x^2+y^2+2xy)\ (\alpha_i)^p=$$
$$=(x^2+y^2+xy(\zeta^i+\zeta^{-i}))(\pi)^{(2n-1)p}(\gamma)^p.$$

Так как все дивизоры в уравнении главные, для $i = 1, 2$ имеем:

$$\varepsilon_1(x^2+y^2+2xy)\ \alpha_1^p=$$
$$=(x^2+y^2+xy(\zeta+\zeta^{-1}))\pi^{(2n-1)p}\gamma^p;$$

$$\varepsilon_2(x^2+y^2+2xy)\ \alpha_2^p=$$
$$=(x^2+y^2+xy(\zeta^2+\zeta^{-2}))\pi^{(2n-1)p}\gamma^p,$$

где ε_1 и ε_2 – единицы кольца $Z[\zeta+\zeta^{-1}]$.

После элементарных преобразований из последних двух уравнений с учетом равенства

$$\frac{\varepsilon_1(x^2+y^2+2xy)\alpha_1^p-(x^2+y^2+2xy)\pi^{(2n-1)p}\gamma^p}{\varepsilon_2(x^2+y^2+2xy)\alpha_2^p-(x^2+y^2+2xy)\pi^{(2n-1)p}\gamma^p}=$$
$$=\frac{xy(\zeta+\zeta^{-1}-2)\pi^{(2n-1)p}\gamma^p}{xy(\zeta^2+\zeta^{-2}-2)\pi^{(2n-1)p}\gamma^p}$$

получаем

$$\varepsilon_1\alpha_1^p+\varepsilon\varepsilon_2\alpha_2^p=(1+\varepsilon)\pi^{(2n-1)p}\gamma^p,$$

где $\varepsilon=\dfrac{(1-\zeta)(1-\zeta^{-1})}{(1-\zeta^2)(\zeta^{-2}-1)}$ – единица.

Так как $\varepsilon_3=\varepsilon_1^{-1}\varepsilon\varepsilon_2$ – единица, $\varepsilon_4=(1+\varepsilon)\,\varepsilon_1^{-1}$ – единица, тогда

$$\alpha_1^p+\varepsilon_3\alpha_2^p=\varepsilon_4\pi^{(2n-1)p}\gamma^p.$$

Пусть $\alpha_1^p\equiv t \bmod p$, $\alpha_2^p\equiv q \bmod p$, $t+\varepsilon_3 q\equiv 0 \bmod p$ и $\varepsilon_3\equiv r \bmod p$, где $t, q, r\in\mathbf{Z}$. Но если верно последнее сравнение, то $\varepsilon_3=\varepsilon_5^p$ (доказательство этого факта будет приведено ниже). Тогда

$$\alpha_1^p+\beta_1^p=\varepsilon_4\pi^{(2n-1)p}\gamma^p,$$

где $\beta_1 = \varepsilon_5\alpha_2$.

В итоге получим уравнение

$$x_1^p+y_1^p=\varepsilon_4\pi^{n_1p}z_1^p,$$

где $\alpha_1 = x_1$; $\beta_1 = y_1$; $\gamma = z_1$; $2n-1 = n_1$.

Теперь докажем, что $|Nz|>|Nz_1|$:

$$N((x^2+y^2+2xy)\frac{1}{4}(2+\zeta^i+\zeta^{-i}))=$$
$$=N((\pi)^{(2n-1)p+1}\aleph^2\Im_0^{2p}\frac{1}{4}(1+\zeta^i)\ (1+\zeta^{-i}));$$

$$N(x^2+y^2+xy(\zeta^i+\zeta^{-i}))=N((\pi)\aleph^2\Im_i^p);$$

$$\left|N((x^2+y^2+2xy)\frac{1}{4}(2+\zeta^i+\zeta^{-i}))\right|=$$

$$=\left|N\left(\frac{1}{4}(x^2+y^2)(2+\zeta^i+\zeta^{-i})+\frac{1}{2}xy(2+\zeta^i+\zeta^{-i})\right)\right|<$$
$$<\left|N(x^2+y^2+xy(\zeta^i+\zeta^{-i}))\right|.$$

Это неравенство верно, поскольку для любых вещественных x и y и для любого i

$$\left|\frac{1}{4}(x^2+y^2)(2+\zeta^i+\zeta^{-i})+\frac{1}{2}xy(2+\zeta^i+\zeta^{-i})\right|<$$
$$<\left|x^2+y^2+xy(\zeta^i+\zeta^{-i})\right|.$$

Значит, $\left|N((\pi)^{(2n-1)p+1}\aleph^2\Im_0^{2p}\frac{1}{4}(2+\zeta^i+\zeta^{-i}))\right|<$ $<\left|N((\pi)\aleph^2\Im_i^p)\right|$, так как $N(\pi)=p$, то

$$p^{(2n-1)p}\left(\frac{1}{2}\right)^{2m}|N\Im_0^{2p}|<|N\Im_i^p|.$$

Так как $n\geq 1$, то $|N\Im_0^{2p}|<|N\Im_i^p|$ и $|N\Im_0^2|<|N\Im_i|$. Следовательно,

$$|Nz|=|N\aleph|\prod_{i=0}^{m}|N\Im_i|\geq\prod_{i=0}^{m}|N\Im_i|>|N\Im_0||N\Im_0^{2m}|;$$

$|Nz|>|N\Im_0||Nz_1|$, значит, $|Nz|>|Nz_1|$.

Пришли к противоречию, так как $|Nz|$ выбирали минимальным. ■

Из теоремы 2.1. следует теорема 2.0.

Единицы вида

$$\pm\zeta^a\prod_{i=1}^{m}(1-\sigma^i\zeta)^{n_i},$$

где $n=\sum_{i=1}^{m}n_i=0$, $a=0,1,\ldots,p-1$, $\sigma^k\zeta=\zeta^{g_k}$, $g_k\equiv g^k \bmod p$, $1\leq g_k\leq p-1$, $k=0,1,\ldots,p-2$,

где g – первообразный корень по модулю p, образуют подгруппу группы всех единиц кольца $Z[\zeta]$ и называются специальными [1].

Фактор-группа единиц кольца $Z[\zeta]$ по подгруппе специальных единиц имеет порядок h_2.

Теорема 1.1. *Любая специальная единица, для которой существует такое целое число c, что $\varepsilon\equiv c \bmod p$, является p-й степенью некоторой, тоже специальной единицы η.*

□ По условию теоремы имеем:

$$\pm\zeta^a\prod_{i=1}^{m}(1-\sigma^i\zeta)^{n_i}\equiv c \bmod p;$$

$$\pm\sigma^s\zeta^a\prod_{i=1}^{m}(1-\sigma^{s+i}\zeta)^{n_i}\equiv c \bmod p.$$

Пусть g – первообразный корень по модулю p такой, что $g^{p-1}\equiv 1 \bmod p^2$.

Тождество

$$\zeta^{a(g_s-1)}\prod_{i=1}^{m}\left(\frac{1-\sigma^{s+i}\zeta}{1-\sigma^i\zeta}\right)^{n_i}\equiv 1 \bmod p$$

верно при $s=1,2,\ldots,p-2$.

Так как

$$\prod_{i=1}^{p-1}\left(\frac{1-\sigma^{s+i}\zeta}{1-\sigma^i\zeta}\right)=1,$$

то

$$\prod_{i=1}^{m}\left(\frac{1-\sigma^{s+i}\zeta}{1-\sigma^i\zeta}\right)=\pm\zeta^d,\ d\in\mathbf{Z};$$

$$\prod_{i=1}^{m}\left(\frac{1-\sigma^{s+i}\zeta}{1-\sigma^i\zeta}\right)^{n_j}=(\pm\zeta^d)^{n_j},$$

$$\zeta^{a(g_s-1)+dn_j}\prod_{i=1}^{m}\left(\frac{1-\sigma^{s+i}\zeta}{1-\sigma^i\zeta}\right)^{n_i-n_j}\equiv\pm 1 \bmod p,$$
$$j=1,\ldots,m.$$

Из последнего следует, что существуют многочлены, удовлетворяющие равенству

$$X^{a(g_s-1)+dn_j}\prod_{i=1}^{m}\left(\frac{1-X^{g_{s+i}}}{1-X^{g_i}}\right)^{n_i-n_j}=$$
$$=\pm 1+pF_{1S}(X)+\varphi(X)F_{2S}(X),$$

где $F_{2S}(X)=\dfrac{R_{1S}(X)}{R_{2S}(X)}$, $F_{2S}(X)$ – отношение многочленов с целыми коэффициентами; $\varphi(X)=X^{p-1}+X^{p-2}+\ldots+X+1$.

Берем логарифмическую производную от обеих частей равенства и умножаем ее на X. Далее подставляем вместо $X=\zeta$ и вводим многочлен $E(X)$

$$E(X)=\sum_{i=1}^{m}(n_i-n_j)(gX)^i.$$

После этих преобразований получаем равенство по модулю p

$$(a(g_s-1)+dn_j)+(g_s\sigma^s-1)E(\sigma)\left(\frac{\zeta}{\zeta-1}\right)\equiv$$

$$\equiv\zeta\varphi'(\zeta)\frac{R_{1S}(\zeta)}{R_{2S}(\zeta)\varepsilon}\mod p,$$

$R_{2S}(\zeta)$ – единица.

Пусть $a(g_s-1)+dn_j=-b$, тогда $b+(g_s\sigma^s-1)\times$ $\times E(\sigma)\left(\frac{1}{\zeta-1}\right)\equiv b_s\varpi(\sigma)\zeta \mod p,$

$$\varpi(\sigma)\zeta=\zeta+g_1\zeta^{g_1}+\ldots+g_{p-2}\zeta^{g_{p-2}},\quad b_s\in \mathbf{Z}.$$

Так как

$$g^s\equiv g_s \mod p,$$

то

$$b+(g^s\sigma^s-1)E(\sigma)\left(\frac{1}{\zeta-1}\right)\equiv b_s\varpi(\sigma)\zeta \mod p;$$

$$bp+(g^s\sigma^s-1)E(\sigma)\left(\frac{p}{\zeta-1}\right)\equiv b_s p\varpi(\sigma)\zeta \mod p^2;$$

$$bp+(g^s\sigma^s-1)E(\sigma)\varpi(\sigma)\zeta\equiv b_s p\varpi(\sigma)\zeta \mod p^2.$$

Для любого многочлена $K(X)$ верно

$$K(\sigma)\zeta_1\equiv K(g^{p-2})\zeta_1 \mod p^2,$$

где $\zeta_1=\zeta+g\sigma\zeta+g^2\sigma^2\zeta+\ldots+g^{p-2}\sigma^{p-2}\zeta$.

Значит,

$$bp\omega(g)+(g^s\sigma^s-1)E(\sigma)\varpi(\sigma)\zeta_1\equiv b_s p\varpi(\sigma)\zeta_1 \mod p^2;$$

$$\omega(g)=1+g+\ldots+g^{p-2}\equiv 0 \mod p^2;$$

$$(g^{s(p-1)}-1)E(g^{p-2})\varpi(g^{p-2})\zeta_1\equiv b_s p\varpi(g^{p-2})\zeta_1 \mod p^2;$$

$$g^{s(p-1)}\equiv 1 \mod p^2,$$

$\varpi(g^{p-2})\not\equiv 0 \mod p$, следовательно, $b_s\equiv 0 \mod p$ при $s=1,2,\ldots,p-2$.

Таким образом,

$$(g_s\sigma^s-1)E(\sigma)\left(\frac{p}{\zeta-1}\right)\equiv -bp \mod p^2,$$

$$(g_s\sigma^s-1)E(\sigma)\varpi(\sigma)\zeta\equiv -bp \mod p^2;$$

$$(g_s\sigma^s-1)E(\sigma)\varpi(\sigma)\zeta_1\equiv -bp\omega(g) \mod p^2;$$

$$(g_s g^{s(p-2)}-1)E(g^{p-2})\varpi(g^{p-2})\zeta_1\equiv -bp\omega(g) \mod p^2.$$

Так как $\sum_{i=1}^{m}n_i=0$, то $E(g^{p-2})\equiv -n_j m \mod p^2$, после умножения на g^s

$$(g_s-g^s)n_j m\varpi(g^{p-2})\zeta_1\equiv 0 \mod p^2$$
при $s=0,1,\ldots,p-2.$

$$\sum_{s=0}^{p-2}(g_s-g^s)n_j m\varpi(g^{p-2})\zeta_1\equiv 0 \mod p^2,$$

$$\sum_{s=0}^{p-2}g^s\equiv 0 \mod p^2,$$

$$\sum_{s=0}^{p-2}g_s=pm\not\equiv 0 \mod p^2,$$

следовательно, $n_j\equiv 0 \mod p$, где $j=1,2,\ldots,m$, $a=0$.

Пусть $r_j=\frac{n_j}{p}$, тогда $\eta=\pm\prod_{i=1}^{m}(1-\sigma^i\zeta)^{r_i}$ и $\varepsilon=\eta^p$. ■

Следствие 1. Если верна теорема 1.1, то любая единица ε такая, что $\varepsilon\equiv c \mod p$, является р-й степенью некоторой единицы.

□ Действительно, ε^{h_2} – специальная, по теореме 1.1, $\varepsilon^{h_2}=\eta^p$.

$h_2\not\equiv 0 \mod p$, следовательно, существуют такие целые числа ν и υ, что $h_2\nu+p\upsilon=1$.

$$\varepsilon=\varepsilon^{h_2\upsilon}\varepsilon^{p\nu}=\eta^{p\upsilon}\varepsilon^{p\nu}=(\eta^{\upsilon}\varepsilon^{\nu})^p.\ ■$$

Следствие 2. Если верна теорема 1.1, то верна теорема 1.0.

Допустим $h_2\equiv 0 \mod p$, тогда по теореме Коши в фактор-группе группы единиц по подгруппе специальных единиц существует элемент порядка p, и, значит, в группе единиц существует неспециальная единица ε, для которой единица ε^p – специальная.

$\varepsilon^p\equiv c \mod p$, поэтому в силу теоремы 1.1 в кольце $Z[\zeta]$ существует такая специальная единица η, что $\varepsilon^p = \eta^p$ и $\varepsilon\eta^{-1} = \zeta^a$ для некоторого a.

Следовательно, вопреки предположению, единица $\varepsilon = \zeta^a\eta$ – специальная. Приходим к противоречию. ■

Для полноты следует отметить, что я располагаю собственным вариантом доказательства первого случая теоремы Ферма.

Теорема. *Для нерегулярного простого числа p справедлив первый случай теоремы Ферма при условии, что $h_2 \not\equiv 0$ modp.*

Однако здесь оно не приводится.

Итак, доказаны теоремы (2.1) ⇒ (2.0); (1.1) ⇒ (1.0) и вместе с ними доказана великая теорема Ферма.

ВЫВОДЫ

В работе доказаны теоремы (1.0) и (2.0), что, как известно, достаточно для полного доказательства теоремы Ферма.

Эти теоремы рассмотрены с помощью двух других теорем (1.1) и (2.1). Доказательство последних основано на арифметической теории кругового поля Куммера с использованием теории дивизоров и специальных единиц.

ЛИТЕРАТУРА

1. **Постников М. М.** Введение в теорию алгебраических чисел. – М., 1982.