Записки научных
семинаров ПОМИ
Том 523, 2023 г.

Н. В. Проскурин

О СУММАХ ГАУССА СТЕПЕНИ 6

Введение. Для простого конечного поля $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ порядка p, обозначим через e_p характер $z \mapsto \exp(2\pi i z/p)$ его аддитивной группы и рассмотрим суммы Гаусса

$$G_n(p) = \sum_{x\in\mathbb{F}_p} e_p\big(x^n\big), \quad n \geqslant 1, \quad n \in \mathbb{Z}\,. \tag{1}$$

Числа n и p — степень и модуль суммы (1). Положим

$$D = \big\{z \in \mathbb{C} \;\big|\; |z| \leqslant 1\big\}.$$

Имеет место оценка $|\,G_n(p)\,| \leqslant (n-1)\sqrt{p}$ и представление

$$G_n(p) = (n-1)\sqrt{p}\,E_n(p) \quad \text{с некоторым} \quad E_n(p) \in D. \tag{2}$$

См. [1–3]. С фиксированным n, точки $E_n(p)$ с простыми $p \leqslant X$ составляют конечное множество, которое, при достаточно больших X, может служить визуализацией распределения сумм Гаусса.
Например, с нечётным n имеем $G_n(p) \in \mathbb{R}$ и все точки $E_n(p)$ распределены по отрезку $[-1,1] \subset D$.
Рассмотрим суммы Гаусса $G_6(p)$, то есть суммы степени 6. Ниже, на рисунке, изображены вещественная и мнимая оси координат на комплексной плоскости $\mathbb{C}$, единичный круг $D \subset \mathbb{C}$ и точки $E_6(p) \in D$ с простыми $p < 300000$, определённые по $G_6(p)$ равенством (2). Мы видим, что точки $E_6(p)$ выстраиваются вдоль некоторых кривых.
В настоящей публикации мы дадим описание этих кривых, включающее определяющие их уравнения. Затем мы рассмотрим более общий вопрос о распределении сумм Гаусса $G_6(c,p)$ с параметром $c \in \mathbb{Z}$, отвечающих произвольным аддитивным харктерам $z \mapsto \exp(2\pi i c z/p)$ поля $\mathbb{F}_p$, см. (10). Мы опять обнаружим кривые, лежащие в круге D, и дадим их описание.

Ключевые слова: конечные поля, суммы Гаусса, кривые Крамера.

Предварительные наблюдения. Рассмотрим наш рисунок более детально. Точки $E_6(p)$ соответствующие $G_6(p)$ с $p \not\equiv 1 \bmod 6$ суть только 0, $1/5$ и $i/5$. Поясним. Числу $p = 2$ соответствует сумма $G_6(2) = 0$ и точка $E_6(2) = 0$ на рисунке. Числу $p = 3$ соответствует сумма $G_6(3) = i\sqrt{3}$ и точка $E_6(3) = i/5$ — изолированная точка на мнимой оси. В случае $p \equiv -1 \bmod 6$, функция $x \mapsto x^3$ отображает биективно $\mathbb{F}_p$ на $\mathbb{F}_p$ и

$$G_6(p) = G_2(p) = \begin{cases} \sqrt{p}, & \text{если } p \equiv 1 \bmod 4, \\ i\sqrt{p}, & \text{если } p \equiv 3 \bmod 4, \end{cases}$$

см. [1–3]. Соответственно, $E_6(p) = 1/5$ или $E_6(p) = i/5$.

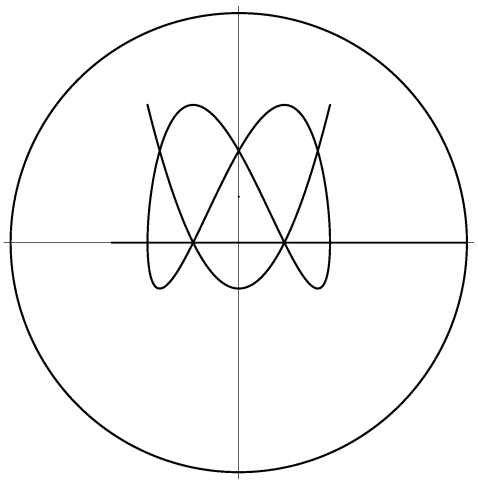

Рис. 1

В основном, рисунок сформирован точками $E_6(p)$ с $p \equiv 1 \bmod 6$. Мы видим, он составлен из трёх компонент:

отрезок $\mathcal{L} \subset \mathbb{R}$;
кривая $\mathcal{P}$, похожая на сегмент параболы;
кривая $\mathcal{C}$, слегка похожая на символ ∞;

Множество всех точек $E_6(p)$ не более чем счётно, но изображения этих точек на рисунке расположены весьма плотно и сливаются в компоненты $\mathcal{L}$, $\mathcal{P}$ и $\mathcal{C}$. Именно это мы подразумеваем заявляя, что та или иная компонента сформирована теми или иными точками. *Мы ожидаем, что точки $E_6(p)$ составляют всюду плотные (в топологическом*

смысле) *подмножества на компонентах* $\mathcal{L}$, $\mathcal{P}$ *и* $\mathcal{C}$. В связи с этим заметим, что из исследований сумм Гаусса, связанных с проблемой Куммера, известно, что точки $E_3(p)$ с простыми $p \equiv 1 \bmod 3$ составляют всюду плотное подмножество отрезка $[-1, 1]$, см. [5].

Компоненты $\mathcal{L}$, $\mathcal{P}$, $\mathcal{C}$. Мы намерены воспользоваться формулами из [4] и [3], связывающими суммы степени 6 с суммами степени 3. Для простого числа $p \equiv 1 \bmod 6$ имеем

$$G_6(p) - G_3(p) = \frac{h}{\sqrt{p}}\big\{G_3(p)^2 - p\big\}, \tag{3}$$

если 2 — кубический вычет $\bmod p$, и имеем

$$G_6(p) - G_3(p) = \frac{h}{2\sqrt{p}}\big\{4p - G_3(p)^2 + l\,G_3(p)\sqrt{12p - 3G_3(p)^2}\,\big\}, \tag{4}$$

в противном случае. Здесь $h = 1$ в случае $p \equiv 1 \bmod 12$ и $h = i$ в случае $p \equiv 7 \bmod 12$. Параметр $l = \pm 1$ также некоторым образом зависит от p, но для наших целей достаточно знать, что $l^2 = 1$. Эти формулы можно найти в [4], теорема 3.8, и в [3], теорема 4.1.4.
Равенства (3) и (4) эквивалентны равенствам

$$5u = 2v + h(4v^2 - 1), \tag{5}$$

$$5u = 2v + 2h\big\{1 - v^2 + lv\sqrt{3 - 3v^2}\big\} \tag{6}$$

для параметров

$$u = E_6(p) = \frac{G_6(p)}{5\sqrt{p}} \quad \text{и} \quad v = E_3(p) = \frac{G_3(p)}{2\sqrt{p}}. \tag{7}$$

Чудесным образом из уравнений исчезла зависимость от p. Положим

$$x = \operatorname{Re} E_6(p), \quad y = \operatorname{Im} E_6(p) \tag{8}$$

и напомним, что $v \in [-1, 1] \subset \mathbb{R}$.

Предложение 1. *Точки* $E_6(p)$ *с простыми* p *под условиями* $p \equiv 7 \bmod 12$ *и* 2 *— кубический вычет* $\bmod p$ *составляют некоторое подмножество сегмента параболы* $\mathcal{P}$, *определённого уравнением* $5y = 25x^2 - 1$ *и условием* $x \in [-2/5, 2/5]$. □

Доказательство. Параметры u и v связаны равенством (5) с $h = i$. Имеем $x = 2v/5 \in [-2/5, 2/5]$ и $5y = 4v^2 - 1 = 25x^2 - 1$. □

Предложение 2. *Точки $E_6(p)$ с простыми p под условиями $p \equiv 7 \bmod 12$ и 2 — кубический невычет $\bmod p$ составляют некоторое подмножество кривой Крамера $\mathcal{C}$, определённой уравнением*

$$(y - 2/5)^2 + 5x^2(y - 2/5) + 25x^4 - 3x^2 = 0. \tag{9}$$

Кривая $\mathcal{C}$ симметрична относительно мнимой оси и имеет единственную двойную точку. □

Доказательство. Параметры u и v связаны равенством (6) с $h = i$. Имеем $x = 2v/5$ и

$$\begin{aligned} 5y &= 2\bigl\{1 - v^2 + lv\sqrt{3 - 3v^2}\bigr\} \\ &= 2 - 25x^2/2 + 5lx\sqrt{3 - 75x^2/4}. \end{aligned}$$

Из последнего равенства очевидным образом следует полиномиальное уравнение $(y - 2/5 + 5x^2/2)^2 = 3x^2(1 - 25x^2/4)$, связывающее x и y и эквивалентное (9). □

Предложение 3. *Точки $E_6(p)$ с простыми p под условием $p \equiv 1 \bmod 12$ составляют некоторое подмножество отрезка $\mathcal{L} = [k, 1]$ с начальной точкой $k = -0,5566806\ldots$ определяемой как минимум функций $v \mapsto 2\bigl\{1 + v - v^2 \pm v\sqrt{3 - 3v^2}\bigr\}/5$ с $v \in [-1, 1]$.* □

Доказательство. В обозначениях (1), если $p \equiv 1 \bmod n$, то $G_n(p) \in \mathbb{R}$ при условии $p \equiv 1 \bmod 2n$ и $G_n(p) \notin \mathbb{R}$ при условии $p \not\equiv 1 \bmod 2n$, см. [3], теорема 4.0.1. Следовательно, компонента $\mathcal{L}$ на нашем рисунке содержится в отрезке $[-1, 1] \subset \mathbb{R}$ и сформирована точками $E_6(p)$ с $p \equiv 1 \bmod 12$. Из уравнений (5) и (6) с $h = 1$ получаем более точное описание. С $v \in [-1, 1]$, правая часть (5) варьируется в отрезке $[-5/4, 5]$ и x варьируется в отрезке $[-1/4, 1]$, см. (7), (8). Аналогично, с $v \in [-1, 1]$ и $l = \pm 1$, правая часть (6) варьируется в отрезке $[5k, 5]$ и x варьируется в отрезке $[k, 1]$. □

Замечание. Для простого числа $p \equiv 1 \bmod 3$, число 2 является кубическим вычетом по модулю p в том и только в том случае, если p представимо как суммма $p = a^2 + 27b^2$ с некоторыми a, $b \in \mathbb{Z}$, см. предложение 9.6.2 в [6]. Из теоремы Чеботарёва следует, что множество таких простых чисел имеет положительную плотность в множестве всех простых чисел.

Кривые Крамера. Если x и y связаны определяющим $\mathcal{C}$ уравнением (9) и

$$k = \frac{1}{\sqrt{3}}\,, \quad X = \frac{5}{2}\,x\,, \quad Y = \frac{5}{2\sqrt{3}}\,y - \frac{1}{\sqrt{3}}\,,$$

то X и Y связаны уравнением

$$(Y + kX^2)^2 = X^2 - X^4.$$

Кривые, определённые этим уравнением с произвольным параметром $k \in \mathbb{R}$, были рассмотрены в трактате Крамера [7] опубликованом в 1750 году. Они известны под названием Cramer's besace curves, содержащим трудноперводимое слово besace. См. [7], гл. X, § 174, стр. 451 и 470.

Более общие суммы Гауссы. Рассмотрим суммы Гаусса

$$G_n(c,p) = \sum_{x\in\mathbb{F}_p} e_p\big(cx^n\big), \quad n \geqslant 1, \quad n \in \mathbb{Z}, \tag{10}$$

степени n с параметром $c \in \mathbb{Z}$, $c \neq 0$. Суммы $G_n(p)$ из (1) есть не что иное, как $G_n(1,p)$. Имеет место неравенство

$$|G_n(c,p)| \leqslant (n-1)\sqrt{p}\,,$$

которое следует из (13) и (12), и представление

$$G_n(c,p) = (n-1)\sqrt{p}\,E_n(c,p) \quad \text{с} \quad E_n(c,p) \in D \tag{11}$$

для всех $n, c \in \mathbb{Z}$ под условиями $n \geqslant 1$ и $p \nmid c$. Здесь условием $p \nmid c$ исключён из рассмотрения вырожденный случай $G_n(c,p) = p$ с $p \mid c$. Без каких-либо ограничений на c и p, имеем

$$G_n(c,p) \in \mathbb{R} \quad \text{для всех нечётных } n.$$

Суммами Гаусса также называют, суммы

$$G(\theta) = \sum_{z\in\mathbb{F}_p^\star} \theta(z)\,e_p(z)$$

с характером θ мультипликативной группы $\mathbb{F}_p^\star$ поля $\mathbb{F}_p$, обладающие свойством

$$|G(\theta)|^2 = p, \tag{12}$$

если характер θ не тривиален, см. [1–3].

Пусть $p \equiv 1 \bmod n$. Сумма (10) с $p \nmid c$ может быть представлена как линейная комбинация

$$G_n(c,p) = \sum_{\theta} \bar{\theta}(c)\, G(\theta) \tag{13}$$

с суммированием распространенным на все характеры θ группы $\mathbb{F}_p^\star$ под условиями $\theta^n = \epsilon,\ \theta \neq \epsilon$, где ϵ — тривиальный характер.
Для квадратичного характера η имеем равенство

$$G_2(c,p) = \eta(c)\, G(\eta) \tag{14}$$

и формулы Гаусса

$$G(\eta) = i^{(p-1)^2/4}\sqrt{p} = \begin{cases} \sqrt{p}\,, & \text{если } p \equiv 1 \bmod 4, \\ i\sqrt{p}\,, & \text{если } p \equiv 3 \bmod 4. \end{cases} \tag{15}$$

В случае $n = 3$, в разложении (13) имеются два слагаемых соответствующих кубическим характерам ψ и $\bar{\psi}$. Это доставляет нам равенство

$$G_3(c,p) = \bar{\psi}(c)\, G(\psi) + \psi(c)\, G(\bar{\psi}) \tag{16}$$

при условии $p \nmid c$. Не сложно показать, что $G(\bar{\psi}) = \overline{G(\psi)}$ и что слагаемые в правой части (16) комплексно сопряжены одно другому.

Несколько формул для сумм Гаусса степеней 2, 3 и 6. Воспользуемся (16) и (12) чтобы вывести представления сумм Гаусса модуля $p \equiv 1 \bmod 3$ с кубическими характерами ψ и $\bar{\psi}$ через кубические суммы Гаусса $G_3(c,p)$ с $p \nmid c$. С некоторыми $S, T \in \mathbb{R}$ имеем равенства

$$\bar{\psi}(c)\, G(\psi) = (S + iT)/2, \quad \psi(c)\, G(\bar{\psi}) = (S - iT)/2. \tag{17}$$

Из (16) и (12) находим

$$S = G_3(c,p), \quad T = \pm\sqrt{4p - S^2}, \quad S^2 + T^2 = 4p. \tag{18}$$

Из (17) и (18) получаем

$$\begin{aligned} G(\psi) &= \psi(c)\big\{S + il\sqrt{4p - S^2}\big\}/2, \\ G(\bar{\psi}) &= \bar{\psi}(c)\big\{S - il\sqrt{4p - S^2}\big\}/2, \\ l &= \pm 1, \quad S = G_3(c,p). \end{aligned} \tag{19}$$

Параметр l зависит от ψ, p и c. Возведя в квадрат, выводим из (19) ещё пару равенств

$$G(\psi)^2 = \bar{\psi}(c)\big\{2S^2 - 4p + 2ilS\sqrt{4p - S^2}\big\}/4, \qquad (20)$$
$$G(\bar{\psi})^2 = \psi(c)\big\{2S^2 - 4p - 2ilS\sqrt{4p - S^2}\big\}/4.$$

Если χ — характер порядка n, то все характеры, удовлетворяющие условиям суммирования в (13), суть χ^m с целыми m от 1 до $n-1$. В частности, с таким χ порядка $n = 6$ и с $p \equiv 1 \bmod 6$, положив $\psi = \chi^2$ и $\eta = \chi^3$, выводим[1] из (13) равенство

$$G_6(c,p) = \bar{\chi}(c)\, G(\chi) + \chi(c)\, G(\bar{\chi}) \qquad (21)$$
$$+ \bar{\psi}(c)\, G(\psi) + \psi(c)\, G(\bar{\psi}) + \eta(c)\, G(\eta).$$

Здесь, см. (16) и (19), сумма двух слагаемых содержащих ψ равна S. Суммы $G(\chi)$ и $G(\bar{\chi})$ исключим из правой части (21) по формулам

$$G(\chi) = \frac{\bar{\psi}(2)}{p}\, G(\eta)\, G^2(\psi), \quad G(\bar{\chi}) = \frac{\psi(2)}{p}\, G(\eta)\, G^2(\bar{\psi}),$$

за которыми мы отсылаем к теореме 3.1 в [4] и к лемме 4.1.1 в [3]. Выразим $G^2(\psi)$ и $G^2(\bar{\psi})$ по формулам (20) и заметим, что произведение характеров $\chi\psi$ есть не что иное, как квадратичный характер η. Так мы, отправляясь от равенства (21), получаем равенство

$$G_6(c,p) = \frac{\bar{\psi}(2)}{4p}\, Q\left\{2S^2 - 4p + 2ilS\sqrt{4p - S^2}\right\} \qquad (22)$$
$$+ \frac{\psi(2)}{4p}\, Q\left\{2S^2 - 4p - 2ilS\sqrt{4p - S^2}\right\} + Q + S$$

с $Q = \eta(c)\, G(\eta) = G_2(c,p)$, $S = G_3(c,p)$, $l = \pm 1$, $p \equiv 1 \bmod 6$, $p \nmid c$.

Предложение 4. *Если p — простое число под условиями $p \equiv 1 \bmod 6$ и 2 — кубический вычет $\bmod p$, то равенство*

$$G_6(c,p) = \frac{1}{p}\, G_2(c,p)\, G_3(c,p)^2 + G_3(c,p) - G_2(c,p), \qquad (23)$$

имеет место с каждым целым c под условием $p \nmid c$. □

[1] Заметим, что $\chi^4 = \bar{\chi}^2 = \bar{\psi}$, $\chi^5 = \bar{\chi}$ и $\eta = \bar{\eta}$.

Доказательство. В (22) с $\psi(2)=1$ слагаемые, содержащие радикалы, сокращаются и мы получаем равенство

$$G_6(c,p)=\frac{1}{4p}\,Q\left\{4S^2-8p\right\}+S+Q=\frac{1}{p}\,Q\,S^2+S-Q,$$

то есть (23). □

Предложение 5. *Пусть p — простое число под условием $p\equiv 1 \bmod 6$ и пусть 2 — кубический невычет* mod$p$. *Для каждого целого числа c под условием $p\nmid c$ имеет место равенство*

$$G_6(c,p)=-\frac{1}{2p}\,G_2(c,p)\,G_3(c,p)\Big\{G_3(c,p)\pm\sqrt{12p-3G_3(c,p)^2}\Big\}\\ +G_3(c,p)+2\,G_2(c,p), \tag{24}$$

с надлежащим образом выбранным знаком $+$ или $-$. □

Доказательство. Воспользуемся равенством (22). Поскольку $\psi(2)$ есть один из кубических корней $(-1\pm i\sqrt{3})/2$ из 1, имеем

$$\psi(2)+\bar\psi(2)=-1,\quad \psi(2)-\bar\psi(2)=\pm i\sqrt{3}. \tag{25}$$

Из (22) и (25) следует

$$\begin{aligned}G_6(c,p)&=\frac{\bar\psi(2)}{4p}\,Q\left\{2S^2-4p\right\}+\frac{\bar\psi(2)}{4p}\,Q\left\{2ilS\sqrt{4p-S^2}\right\}\\ &\quad+\frac{\psi(2)}{4p}\,Q\left\{2S^2-4p\right\}-\frac{\psi(2)}{4p}\,Q\left\{2ilS\sqrt{4p-S^2}\right\}+S+Q\\ &=-\frac{1}{4p}\,Q\left\{2S^2-4p\right\}\pm\frac{\sqrt{3}}{4p}\,Q\left\{2lS\sqrt{4p-S^2}\right\}+S+Q.\\ &=-\frac{1}{2p}\,QS^2\pm l\frac{1}{2p}\,Q\,S\sqrt{12p-3S^2}+S+2Q\end{aligned}$$

со знаком $\pm$ из (25) и с $l=\pm1$ из (19). Чтобы получить (24) остаётся заменить здесь Q и S на $G_2(c,p)$ и $S=G_3(c,p)$ □

Замечание. В формуле (24) надлежит выбрать знак $+$, если знаки в (19) и (25) различны. В противном случае надлежит выбрать знак $-$.

Распределение сумм Гаусса. С фиксированным целым числом c, рассмотрим суммы Гаусса $G_6(c,p)$ и соответствующие им точки $E_6(c,p) \in D$ со всевозможными простыми p. Мы опишем распределение точек $E_6(c,p)$ в круге D. Если $c=1$, то точки $E_6(c,p)$ с $p \equiv 1 \bmod 6$ лежат на отрезке $\mathcal{L}$ и на кривых $\mathcal{P}$ и $\mathcal{C}$, а точки $E_6(c,p)$ с $p \not\equiv 1 \bmod 6$ суть 0, $1/5$ и $i/5$. Эти $\mathcal{L}$, $\mathcal{P}$ и $\mathcal{C}$ определены в Предложениях 1, 2 и 3. Для описания ситуации в общем случае нам потребуются ещё:

отрезок $\overline{\mathcal{L}}$ вещественной прямой, который получается из $\mathcal{L}$ отражением относительно мнимой оси;
кривые $\overline{\mathcal{P}}$ и $\overline{\mathcal{C}}$, которые получаются из $\mathcal{P}$ и $\mathcal{C}$ отражением относительно вещественной оси.

Обратимся к предложениям 4 и 5. Равенства (23) и (24) эквивалентны равенствам

$$5\,u = 2\,v + h\,(4\,v^2 - 1), \tag{26}$$

$$5\,u = 2\,v + 2\,h\,\bigl\{1 - v^2 \pm v\,\sqrt{3 - 3v^2}\bigr\}, \tag{27}$$

для параметров

$$u = E_6(c,p) = \frac{G_6(c,p)}{5\sqrt{p}} \quad \text{и} \quad v = E_3(c,p) = \frac{G_3(c,p)}{2\sqrt{p}},$$

$v \in [-1,1]$. Здесь множитель $h = \eta(c)\,i^{(p-1)^2/4}$ появляется из формул (14) и (15) для квадратичных сумм Гаусса. Зависимость от p и c локализована в один только множитель $h = \pm 1, \pm i$. Положим

$$x = \operatorname{Re} E_6(p), \quad y = \operatorname{Im} E_6(p) \tag{28}$$

и напомним, что $v \in [-1,1] \subset \mathbb{R}$.

Предложение 6. *Для целого числа c и простого числа p под условиями $c \neq 0$, $p \nmid c$, $p \equiv 7 \bmod 12$ и 2 – кубический вычет $\bmod p$, имеем: точка $E_6(c,p)$ лежит на $\mathcal{P}$ или на $\overline{\mathcal{P}}$ смотря по тому c – квадратичный вычет или невычет $\bmod p$.* □

Доказательство. Из (28) и равенства (26) с $h = i\eta(c)$ находим

$$x = \operatorname{Re} u = 2v/5 \in [-2/5, 2/5],$$
$$y = \operatorname{Im} u = \eta(c)\,(4\,v^2 - 1)/5 = \eta(c)\,(5\,x^2 - 1/5),$$

что и требовалось. □

Предложение 7. *Для целого числа c и простого числа p под условиями $c \neq 0$, $p \nmid c$, $p \equiv 7 \bmod 12$ и 2 – кубический невычет* $\bmod p$, *имеем: точка $E_6(c,p)$ лежит на $\mathcal{C}$ или на $\overline{\mathcal{C}}$ смотря по тому c – квадратичный вычет или невычет* $\bmod p$. □

Доказательство. Из (28) и равенства (27) с $h = i\eta(c)$ находим

$$\begin{aligned} x &= \operatorname{Re} u = 2v/5 \in [-2/5, 2/5] \quad \text{и} \\ y &= \operatorname{Im} u = 2\,\eta(c)\,\bigl\{1 - v^2 \pm v\,\sqrt{3 - 3v^2}\bigr\}/5 \\ &= \eta(c)\,\bigl\{2/5 - 5x^2/2 \pm x\,\sqrt{3 - 75x^2/4}\bigr\}. \end{aligned}$$

Из последнего равенства очевидным образом следует

$$\bigl(y - (2/5 - 5x^2/2)\eta(c)\bigr)^2 = 3x^2(1 - 25x^2/4),$$

что эквивалентно уравнению определяющему $\mathcal{C}$ или $\overline{\mathcal{C}}$ смотря по тому $\eta(c) = 1$ или $\eta(c) = -1$. □

Предложение 8. *Для целого числа c и простого числа p под условиями $c \neq 0$, $p \nmid c$, $p \equiv 1 \bmod 12$ имеем: точка $E_6(c,p)$ лежит в отрезке $\mathcal{L}$ или в отрезке $\overline{\mathcal{L}}$ смотря по тому c – квадратичный вычет или невычет* $\bmod p$. *В частности, если 2 – кубический вычет* $\bmod p$, *то точка $E_6(c,p)$ лежит в отрезке $[-1/4, 1] \subset \mathcal{L}$ или в отрезке $[-1, 1/4] \subset \overline{\mathcal{L}}$ смотря по тому c – квадратичный вычет или невычет* $\bmod p$. □

Доказательство. С $p \equiv 1 \bmod 12$ множитель h в (26) и (27) вещественный, $h = \eta(c) = \pm 1$. При этом $x = u$, $y = 0$, см. (28).
Если $\eta(c) = 1$, то равенство (27) идентично (6). Следовательно, с $v \in [-1, 1]$, параметр u варьируется по отрезку $\mathcal{L}$. Если $\eta(c) = -1$, заменим в (27) параметр v на $-v$ и увидим, что u варьируется по отрезку $\overline{\mathcal{L}}$.
Из (28) и равенства (26) с $h = \eta(c)$ следует $5\,u = 4\,\eta(c)\,v^2 + 2\,v - \eta(c)$. Здесь $v \in [-1, 1]$ и u варьируется в $[-1/4, 1]$ или в $[-1, 1/4]$ смотря по тому $\eta(c) = 1$ или $\eta(c) = -1$. □

Рисунки. Изобразим вещественную и мнимую оси координат комплексной плоскости $\mathbb{C}$ и единичный круг $D \subset \mathbb{C}$. Выберем как-либо целое число $c \neq 0$ и добавим на рисунок точки $E_6(c,p) \in D$, определённые по суммам Гаусса $G_6(c,p)$ равенством (11). Из предложений 6, 7, 8 и квадратичного закона взаимности мы выводим следующие утверждения.

Каждое число $c = m^2$ и $c = -3m^2$ с $m \in \mathbb{Z}$, $m \neq 0$, является квадратичным вычетом по модулю p для всех простых $p \equiv 7 \bmod 12$. С таким c, точки $E_6(c,p)$ с $p \nmid c$, $p \equiv 7 \bmod 12$, формируют компоненты $\mathcal{C}$ и $\mathcal{P}$, как это показано на Рис. 1 на примере $c = 1$.

Каждое число $c = -m^2$ и $c = 3m^2$ с $m \in \mathbb{Z}$, $m \neq 0$, является квадратичным невычетом по модулю p для всех простых $p \equiv 7 \bmod 12$. С таким c, точки $E_6(c,p)$ с $p \nmid c$, $p \equiv 7 \bmod 12$, формируют компоненты $\overline{\mathcal{C}}$ и $\overline{\mathcal{P}}$. Это показано на Рис. 2, построенном по вычислениям с $c = 3$.

Каждое число $c = \pm m^2$ и $c = \pm 3m^2$ с $m \in \mathbb{Z}$, $m \neq 0$, является квадратичным вычетом по модулю p для всех простых $p \equiv 1 \bmod 12$. С таким c, точки $E_6(c,p)$ с $p \nmid c$, $p \equiv 1 \bmod 12$, формируют компоненту $\mathcal{L}$, что мы видим на Рис. 1 и на Рис. 2.

Если целое число c не представимо как $\pm m^2$ или $\pm 3m^2$ с $m \in \mathbb{Z}$, то точки $E_6(c,p)$ с $p \nmid c$, $p \equiv 1 \bmod 6$, формируют компоненты $\mathcal{C}$, $\mathcal{P}$, $\overline{\mathcal{C}}$, $\overline{\mathcal{P}}$ и отрезок $\mathcal{L} \cup \overline{\mathcal{L}}$ равный $[-1, 1]$. Это показано на Рис. 3, построенном по вычислениям с $c = 2$.

Простым числам $p \not\equiv 1 \bmod 6$ соответствуют точки 0, $\pm 1/5$, $\pm i/5$.

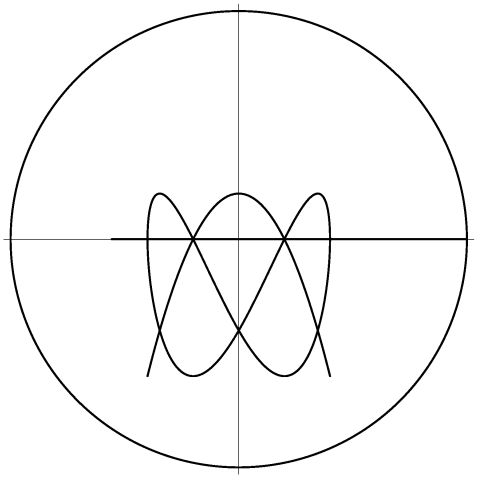

Рис. 2

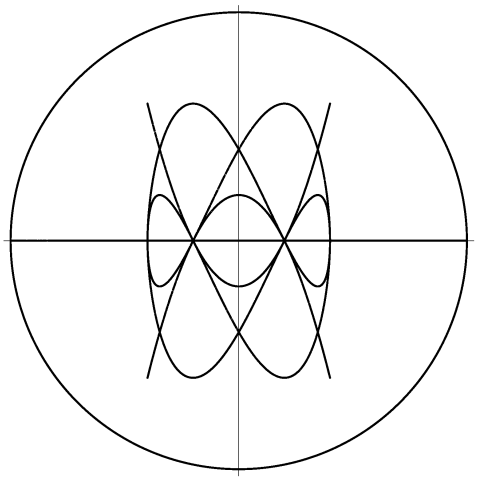

Рис. 3

Список литературы

1. С. А. Степанов, *Арифметика алгебраических кривых*, Москва, Наука, 1991.
2. R. Lidl, H. Niederreiter, *Finite fields*, Cambridge Univ. Press, second edition, 1997.
3. B. C. Berndt, R. J. Evans, K. S. Williams, *Gauss and Jacobi sums*, Wiley-Interscience Publication, 1998.
4. B. C. Berndt, R. J. Evans, *Sums of Gauss, Jacobi, and Jacobsthal*. — J. Number theory **11** (1979), 349–398.
5. D. R. Heath-Brown, S. J. Patterson, *The distribution of Kummer sums at prime arguments*. — J. Reine Angew. Math. **310** (1979), 111–130.
6. K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Grad. Texts in Math., 84. Springer-Verlag (1990).
7. G. Cramer, *Introduction a l'analyse des lignes courbes algébriques*, A Geneve, Chez les Freres Cramer & Cl. Philibert, 1750.

Proskurin N. V. On Gauss sums of degree 6.

The Gauss sums of degree 6 in prime finite fields are considered. It is shown that the normalized values of these sums are located on intervals of real line, on fragments of parabolas, and on some Cramer curves within the unit circle on the complex plane.

Санкт-Петербургское отделение
Математического института
им. В. А. Стеклова РАН,
Санкт-Петербург, Россия

E-mail: np@pdmi.ras.ru

Поступило 24 октября 2023 г.