Записки научных
семинаров ПОМИ
Том 469, 2018 г.

Н. Д. Филонов

О КОЛИЧЕСТВЕ НЕНУЛЕВЫХ КУБИЧЕСКИХ СУММ

§1. Формулировка результата

Пусть q и a – взаимно простые натуральные числа, $m \in \mathbb{Z}$. Введем обозначение

$$S_q(a,m) = \sum_{l=1}^{q} e\left(\frac{al^3+ml}{q}\right), \quad \text{где} \quad e(x) = e^{2\pi i x}. \tag{1.1}$$

Ясно, что эта функция q-периодична по обоим аргументам. Такие суммы встречаются в связи с проблемой Варинга, проблемой Куммера, гипотезой Сато-Тейта и в вопросах о приближенном вычислении кратных интегралов (см., например, [1,3–5,7]). Кроме того, эти суммы возникли в недавней работе [2], где изучались спектральные свойства оператора Штарка-Ваннье

$$H = -\frac{d^2}{dx^2} + 2\cos(2\pi x) - \epsilon x \quad \text{в} \quad L_2(\mathbb{R}),$$

ϵ – вещественный параметр. Суммы (1.1) возникают при описании резонансов оператора H. Авторов интересовало, в частности, каково количество ненулевых сумм среди

$$S_q(a,0),\ S_q(a,1),\ \ldots,\ S_q(a,q-1).$$

В настоящей работе мы отвечаем на этот вопрос. Обозначим это количество через

$$F(a,q) = \#\left\{m \mod q : S_q(a,m) \neq 0\right\}.$$

При $a = 1$ будем писать

$$S_q(m) \equiv S_q(1,m) = \sum_{l=1}^{q} e\left(\frac{l^3+ml}{q}\right), \quad F(q) \equiv F(1,q).$$

При $q = 1$ естественно считать

$$S_1(a,m) = 1, \quad F(a,1) = 1.$$

Ключевые слова: экспоненциальные кубические суммы.
Работа выполнена при поддержке гранта РФФИ-CNRS 17-51-150008-а.

Явное выражение для $F(a,q)$ содержится в следующих четырех теоремах.

Теорема 1.1. *Функция $F(a,q)$ не зависит от a (взаимно простого с q) и мультипликативна по q. Если*

$$q = p_1^{\alpha_1} \dots p_r^{\alpha_r} \tag{1.2}$$

– разложение числа q на простые множители, то

$$F(a,q) = F(q) = F(p_1^{\alpha_1}) \dots F(p_r^{\alpha_r}).$$

Теорема 1.2. $F(2) = 1$. *При* $n \geqslant 1$

$$F(2^{3n-1}) = \frac{2^{3n-2} + 5 \cdot 2^n}{3}, \quad F(2^{3n}) = \frac{2^{3n-1} + 4 \cdot 2^n}{3},$$
$$F(2^{3n+1}) = \frac{2^{3n} + 5 \cdot 2^n}{3}.$$

Теорема 1.3. *При* $n \geqslant 0$

$$F(3^{3n}) = \frac{3^{3n} + 7 \cdot 3^n}{8}, \quad F(3^{3n+1}) = \frac{3^{3n+1} + 5 \cdot 3^n}{8},$$
$$F(3^{3n+2}) = \frac{3^{3n+2} + 5 \cdot 3^{n+1}}{8}.$$

Теорема 1.4. *Пусть p – простое число, $p > 3$, $k = 3n + m$, $n \geqslant 0$, $m = 0, 1, 2$. Тогда*

$$F(p^k) = \frac{p^{3n+m+1} - p^{n+m+1}}{2(p+1)} + p^n F(p^m), \tag{1.3}$$

$$F(1) = 1, \quad F(p) = \begin{cases} p, & \text{если } p \equiv 1 (\mathrm{mod} 3), \\ p-1, & \text{если } p \equiv 2 (\mathrm{mod} 3), \end{cases} \tag{1.4}$$
$$F(p^2) = \frac{p^2 + p}{2}.$$

Следствие 1.5. а) $F(q) > 0$ *при всех* $q \in \mathbb{N}$.

б) $F(q) = 1$ *тогда и только тогда, когда* $q = 1, 2, 3$ *или* 6.

в) $F(q) \neq 2$ *при всех* $q \in \mathbb{N}$.

г) $F(q) = 3$ *тогда и только тогда, когда* $q = 9$ *или* $q = 18$.

д) *Существуют такие положительные постоянные* c_1 *и* c_2, *что* $F(q) \geqslant c_1 q^{1 - \frac{c_2}{\ln \ln q}}$.

Доказательство. Пункты а)–г) вытекают из явных формул предыдущих теорем.

Докажем пункт д). Из теорем 1.2 и 1.3 вытекают неравенства

$$F(2^k) > \frac{2^k}{6} \text{ и } F(3^k) > \frac{3^k}{8}$$

соответственно. Из формулы (1.4) вытекает $F(p^m) > \frac{p^{m+1}}{2(p+1)}$, $m = 0, 1, 2$, поэтому из (1.3) следует

$$F(p^k) > \frac{p^{k+1}}{2(p+1)} \geqslant \frac{5}{12}p^k \quad \text{при всех} \quad k.$$

Поэтому для числа q, представленного формулой (1.2), выполняется оценка

$$F(q) > \frac{1}{48}\left(\frac{5}{12}\right)^{r-2} q = \frac{3}{25}qe^{r\ln\frac{5}{12}} > \frac{3}{25}qe^{-r}. \tag{1.5}$$

Из формулы Стирлинга и очевидного неравенства $q > r!$ вытекает известная оценка количества r простых делителей числа q, $r \leqslant \frac{c\ln q}{\ln\ln q}$. Остается подставить ее в (1.5). □

Замечание 1.6. Пункты а) и б) следствия 1.5 можно вывести не из теорем 1.1–1.4, а из хорошо известной простой формулы

$$\sum_{m=0}^{q-1} |S_q(a,m)|^2 = q^2. \tag{1.6}$$

Замечание 1.7. В работе [2] на основании (1.6) и оценок Хуа доказано (лемма 2 в [2]) неравенство $F(a,q) \geqslant Cq^{2/3}$. Наша оценка из пункта д) точнее.

В §2 мы приведем критерий равенства нулю суммы корней q-й степени из единицы, когда q – степень простого числа (теорема 2.1), и докажем теорему 1.1. В §3 на основании теоремы 2.1 мы покажем, что

$$S_{p^k}(p^2 n) = p^2 S_{p^{k-3}}(n)$$

(следствие 3.5), и что при больших k и для m не кратных p^2 выполняется равенство $S_{p^k}(m) = 0$, за исключением следующих случаев:

- $m \equiv 5(\mathrm{mod}8)$ при $p = 2$;
- $m \equiv 6(\mathrm{mod}9)$ при $p = 3$;
- при $p > 3$ такие m, не кратные p, что уравнение $3x^2 + m \equiv 0(\mathrm{mod}p)$ разрешимо.

В §4 мы докажем, что в этих случаях $S_{p^k}(m) \neq 0$. Таким образом, мы получим рекуррентные формулы, выражающие $F(p^k)$ через $F(p^{k-3})$ для всех простых p (теорема 5.1). Останется вычислить $F(q)$ в случае, когда $q = p$ – простое число, $p > 3$. Оказывается, что тогда $S_p(m) \neq 0$ при всех m, кроме, быть может, $m = 0$ (леммы 5.6 и 5.7).

§2. Доказательство теоремы 1.1

Нам понадобится следующий факт о суммах корней из единицы.

Теорема 2.1. *Пусть p – простое число, k – натуральное, a_j – целые, $j = 1, \dots, p^k$. Тогда*

$$\sum_{j=1}^{p^k} a_j e\left(jp^{-k}\right) = 0$$

тогда и только тогда, когда

$$\begin{cases} a_j = a_l \quad \textit{при} \quad j \equiv l (\mathrm{mod} p^{k-1}) \quad \textit{при} \quad k \geqslant 2, \\ a_1 = a_2 = \dots = a_p \quad \textit{при} \quad k = 1. \end{cases}$$

Эта теорема известна, см. например, [6]. Доказательство опирается на неприводимость многочлена деления круга. Геометрический смысл теоремы состоит в следующем. Рассмотрим правильный p^k-угольник с центром в нуле. Множество его вершин является объединением p^{k-1} множеств вершин правильных p-угольников. Если мы расположим в вершинах исходного p^k-угольника целые массы, то центр тяжести окажется в нуле тогда и только тогда, когда массы в вершинах каждого из p^{k-1} правильных p-угольников равны.

Следствие 2.2. *Пусть p – простое число, k – натуральное, b_l – целые, $l = 1, \dots, p^k$. Если существует такое l_*, что*

$$\{b_l - b_{l_*}\}_{l=1}^{p^k} \not\supset \{jp^{k-1}\}_{j=0}^{p-1} (\mathrm{mod} p^k),$$

то

$$\sum_{l=1}^{p^k} e(b_l p^{-k}) \neq 0.$$

Лемма 2.3. *Пусть p – простое число, $q = p^k$, и a не делится на p. Тогда $F(a, q)$ не зависит от a, $F(a, q) = F(q)$.*

Доказательство. Пусть r таково, что $ar \equiv 1(\mathrm{mod} q)$. Если $\{b_l\}_{l=1}^q$ – какой-то набор целых чисел, то из теоремы 2.1 следует, что

$$\sum_{l=1}^{q} e\left(b_l q^{-1}\right) = 0 \iff \sum_{l=1}^{q} e\left(r b_l q^{-1}\right) = 0.$$

Поэтому

$$S_q(a,m)=\sum_{l=1}^{q} e\left(\frac{al^3+ml}{q}\right)=0 \iff S_q(1,mr)=\sum_{l=1}^{q} e\left(\frac{l^3+mrl}{q}\right)=0.$$

Числа mr с $m = 0, 1, \ldots, q-1$, составляют полную систему вычетов по модулю q. Следовательно, $F(a,q) = F(1,q)$. □

Лемма 2.4. *Пусть натуральные числа a, q_1 и q_2 попарно взаимно просты. Тогда*

$$S_{q_1 q_2}(a,m) = S_{q_1}(aq_2^2, m) S_{q_2}(aq_1^2, m).$$

Замечание 2.5. Эта формула содержится, например, в доказательстве леммы 4.1 [7, глава 4]. Для полноты изложения мы приведем

Доказательство. Имеем

$$a(q_1x+q_2y)^3+m(q_1x+q_2y) \equiv q_1(aq_1^2x^3+mx)+q_2(aq_2^2y^3+my)(\mathrm{mod}\, q_1q_2).$$

Следовательно,

$$\begin{aligned} S_{q_1}(aq_2^2,m)S_{q_2}(aq_1^2,m) &= \sum_{x=1}^{q_2} e\left(\frac{aq_1^2x^3+mx}{q_2}\right)\sum_{y=1}^{q_1} e\left(\frac{aq_2^2y^3+my}{q_1}\right) \\ &= \sum_{x=1}^{q_2}\sum_{y=1}^{q_1} e\left(\frac{a(q_1x+q_2y)^3+m(q_1x+q_2y)}{q_1q_2}\right). \end{aligned}$$

В последней двойной сумме числа вида (q_1x+q_2y) составляют полную систему вычетов $\mathrm{mod}\, q_1q_2$. Поэтому сумма равна $S_{q_1q_2}(a,m)$. □

Следствие 2.6. *В условиях леммы* 2.4

$$F(a, q_1q_2) = F(aq_2^2, q_1)F(aq_1^2, q_2).$$

Отсюда по индукции получается

Следствие 2.7. *Пусть числа a, $q_1, \ldots, q_r$ – попарно взаимно просты. Тогда*

$$F(a, q_1 \ldots q_r) = \prod_{j=1}^{r} F(aq_1^2 \ldots q_{j-1}^2 q_{j+1}^2 \ldots q_r^2, q_j).$$

Доказательство теоремы 1.1. Пусть $(a,q) = 1$, $q = \prod_{j=1}^{r} p_j^{\alpha_j}$, p_j – простые числа. В силу следствия 2.7

$$F(a,q) = \prod_{j=1}^{r} F\left(ap_1^{2\alpha_1}\dots p_{j-1}^{2\alpha_{j-1}} p_{j+1}^{2\alpha_{j+1}}\dots p_r^{2\alpha_r}, p_j^{\alpha_j}\right) = \prod_{j=1}^{r} F(p_j^{\alpha_j}).$$

В последнем равенстве мы воспользовались леммой 2.3. □

§3. Суммы, равные нулю

Теорема 3.1. *Пусть p – простое число, $k \geqslant 2$,*

$$c \leqslant \frac{k}{2} - 1 \quad \textit{при} \quad p \neq 3, \quad c \leqslant \frac{k-1}{2} \quad \textit{при} \quad p = 3. \tag{3.1}$$

Для целого m введем множество

$$L(m,c) = \left\{ l \mod p^k : 3l^2 + m = bp^c, \ \textit{где} \ p \nmid b \right\}.$$

Тогда

$$\sum_{l \in L(m,c)} e\left(\frac{l^3 + ml}{p^k}\right) = 0.$$

Эта теорема также известна, см. доказательство леммы 4.1 [7, глава 4]. Мы приводим доказательство для полноты изложения.

Доказательство. Достаточно доказать, что для каждого фиксированного $b \in \{1, \dots, p-1\}$

$$\sum_{l \in L(m,c,b)} e\left(\frac{l^3 + ml}{p^k}\right) = 0, \tag{3.2}$$

где

$$L(m,c,b) = \left\{ l \mod p^k : 3l^2 + m \equiv bp^c (\mathrm{mod} p^{c+1}) \right\}.$$

Сравнение

$$l_1 \equiv l_2 (\mathrm{mod} p^{k-c-1})$$

не выводит из множества $L(m,c,b)$, так как

$$l_1 \equiv l_2 (\mathrm{mod} p^{k-c-1}) \quad \Longrightarrow \quad 3l_1^2 \equiv 3l_2^2 (\mathrm{mod} p^{c+1})$$

при c, подчиняющемся (3.1). Тем самым, это сравнение является отношением эквивалентности на $L(m,c,b)$. Поэтому достаточно доказать, что

$$\sum_{j=1}^{p^{c+1}} e\left(\frac{(l + jp^{k-c-1})^3 + m(l + jp^{k-c-1})}{p^k}\right) = 0$$

при всех $l \in L(m,c,b)$. Далее,

$$\begin{aligned}(l+jp^{k-c-1})^3 &+ m(l+jp^{k-c-1}) \\ &= l^3+ml+(3l^2+m)jp^{k-c-1}+3lj^2p^{2k-2c-2}+j^3p^{3k-3c-3} \\ &\equiv l^3+ml+bjp^{k-1}(\mathrm{mod}p^k).\end{aligned} \tag{3.3}$$

Предпоследнее слагаемое (содержащее j^2) можно отбросить, поскольку по условию $k \geqslant 2c+2$ при $p \neq 3$, а при $p=3$ достаточно $k \geqslant 2c+1$ за счет множителя 3. Последнее слагаемое в (3.3) можно отбросить, так как $2k \geqslant 3c+3$. Теперь из (3.3) вытекает

$$\sum_{j=1}^{p^{c+1}} e\left(\frac{(l+jp^{k-c-1})^3+m(l+jp^{k-c-1})}{p^k}\right) = e\left(\frac{l^3+ml}{p^k}\right)\sum_{j=1}^{p^{c+1}} e\left(\frac{bj}{p}\right) = 0.$$

□

Следствие 3.2. *Пусть $k \geqslant 2$. Тогда*

$$\sum_{l \in M(m,k)} e\left(\frac{l^3+ml}{p^k}\right) = 0,$$

где

$$M(m,k) = \left\{l \mod p^k : p^{[\frac{k}{2}]} \nmid 3l^2+m\right\} \quad \textit{при} \quad p \neq 3,$$

$$M(m,k) = \left\{l \mod 3^k : 3^{[\frac{k+1}{2}]} \nmid 3l^2+m\right\} \quad \textit{при} \quad p = 3.$$

Следствие 3.3. *Пусть $k \geqslant 2$. Если m таково, что*

$$p^{[\frac{k}{2}]} \nmid (3l^2+m) \ \ \forall\, l \quad \textit{при} \quad p \neq 3, \quad 3^{[\frac{k+1}{2}]} \nmid (3l^2+m) \ \ \forall\, l \quad \textit{при} \quad p = 3,$$

то $S_{p^k}(m) = 0$.

Следствие 3.4. *Пусть $k \geqslant 2$. Если m таково, что уравнение $3x^2 + m \equiv 0(\mathrm{mod}p)$ неразрешимо, то $S_{p^k}(m) = 0$.*

Следствие 3.5. *Пусть $k \geqslant 3$, $m = p^2n$. Тогда*

$$S_{p^k}(m) = p^2 S_{p^{k-3}}(n).$$

Доказательство. Поскольку $p^2 \mid m$, теорема 3.1 (при $c=0$, если $p \neq 3$, при $c=1$, если $p=3$) влечет

$$\sum_{l \in \{1,\ldots,p^k\} : p \nmid l} e\left(\frac{l^3+ml}{p^k}\right) = 0. \tag{3.4}$$

Поэтому в сумме $S_{p^k}(m)$ останутся только слагаемые вида $l = pr$,

$$S_{p^k}(m) = \sum_{r=1}^{p^{k-1}} e\left(\frac{(pr)^3 + mpr}{p^k}\right) = \sum_{r=1}^{p^{k-1}} e\left(\frac{r^3 + nr}{p^{k-3}}\right) = p^2 S_{p^{k-3}}(n). \quad \square$$

Следствие 3.6. *Пусть $p \neq 3$, $m = np$, $p \nmid n$. Тогда*

$$S_{p^k}(m) = 0 \quad \textit{при} \quad k \geqslant 3.$$

Доказательство. Ясно, что $p^2 \nmid (3l^2 + m)$ при всех l. Поэтому при $k \geqslant 4$ утверждение вытекает из следствия 3.3. Пусть $k = 3$. Из теоремы 3.1 при $c = 0$ снова вытекает (3.4), и в сумме $S_{p^3}(m)$ остаются только слагаемые с $l = pr$,

$$S_{p^3}(m) = \sum_{r=1}^{p^2} e\left(\frac{(pr)^3 + mpr}{p^3}\right) = \sum_{r=1}^{p^2} e\left(\frac{nr}{p}\right) = 0. \quad \square$$

Следствие 3.7. *Пусть $p \neq 3$, $m = np$. Тогда*

$$S_{p^2}(m) = p.$$

Доказательство. Из теоремы 3.1 вытекает (3.4), и в сумме $S_{p^2}(m)$ остаются только слагаемые с $l = pr$,

$$S_{p^2}(m) = \sum_{r=1}^{p} e\left(\frac{(pr)^3 + mpr}{p^2}\right) = p. \quad \square$$

Следствие 3.8. *Пусть $p = 3$. Если $3 \nmid m$, то $S_{3^k}(m) = 0$ при $k \geqslant 2$. Если $m \equiv 3 (\mathrm{mod} 9)$, то $S_{3^k}(m) = 0$ при $k \geqslant 3$.*

Доказательство. Случай $3 \nmid m$ вытекает из следствия 3.4. Случай $m \equiv 3(\mathrm{mod}9)$ вытекает из следствия 3.3, поскольку $9 \nmid (3l^2 + m)$ при всех l. $\square$

Следствие 3.9. *Пусть $p = 2$. Если $m \equiv 2(\mathrm{mod}4)$, то $S_{2^k}(m) = 0$ при $k \geqslant 3$. Если $m \equiv 3(\mathrm{mod}4)$, то $S_{2^k}(m) = 0$ при $k \geqslant 4$. Если $m \equiv 1(\mathrm{mod}8)$, то $S_{2^k}(m) = 0$ при $k \geqslant 6$.*

Доказательство. Случай $m \equiv 2(\mathrm{mod}4)$ вытекает из следствия 3.6. Случай $m \equiv 3(\mathrm{mod}\,4)$ вытекает из следствия 3.3, поскольку $4 \nmid (3l^2 + m)$ при всех l. Случай $m \equiv 1(\mathrm{mod}8)$ снова вытекает из следствия 3.3, поскольку $8 \nmid (3l^2 + m)$ при всех l. $\square$

Лемма 3.10. *Если $m \equiv 5(\mathrm{mod}8)$, то $S_{32}(m) = 0$.*

Доказательство. По теореме 3.1

$$S_{32}(m)=\sum_{l=1,3,\dots,31} e\left(\frac{l^3+ml}{32}\right)$$
$$=\sum_{j=0}^{7} e\left(\frac{(4j+1)^3+m(4j+1)}{32}\right)+\sum_{j=0}^{7} e\left(\frac{(4j-1)^3+m(4j-1)}{32}\right).$$

Далее,

$$(4j\pm 1)^3+m(4j\pm 1)\equiv \pm 48j^2+(3+m)4j\pm(m+1)\equiv \pm\big(16j^2+m+1\big)$$
$$\equiv\begin{cases}\pm(m+1)(\mathrm{mod}32), & \text{если } \ j \text{ – четное},\\ \pm(m+17)(\mathrm{mod}32), & \text{если } \ j \text{ – нечетное}.\end{cases}$$

Поэтому обе суммы равны нулю. □

§4. Суммы, не равные нулю

Лемма 4.1. *Пусть число m удовлетворяет одному из следующих условий:*

- $p\nmid m$, *m таково, что уравнение* $3x^2+m\equiv 0(\mathrm{mod}p)$ *разрешимо,* $p>3$;
- $m\equiv 6(\mathrm{mod}9)$, $p=3$;
- $m\equiv 5(\mathrm{mod}8)$, $p=2$;

Пусть r – любое натуральное, если $p>3$; $r\geqslant 2$, если $p=3$; $r\geqslant 3$, если $p=2$. Тогда существует натуральное l, такое что

$$p^r\mid(3l^2+m)\quad и\quad p^{r+1}\nmid(3l^2+m).$$

Эта лемма доказывается индукцией по r.

Теорема 4.2. *Пусть m удовлетворяет условиям леммы* 4.1, $p\neq 2$. *Тогда*

$$S_{p^k}(m)\neq 0$$

при $k\geqslant 2$, если $p>3$, при $k\geqslant 3$, если $p=3$.

Доказательство. Согласно следствию 3.2

$$S_{p^k}(m)=\sum_{l\in A} e\left(\frac{l^3+ml}{p^k}\right),\quad \text{где}\quad A=\left\{l\in\{1,\dots,p^k\}: p^r\mid 3l^2+m\right\},$$

$r = [\frac{k}{2}]$ при $p > 3$, $r = [\frac{k+1}{2}]$ при $p = 3$. По лемме 4.1 найдется l_*, такое что

$$p^k \mid (3l_*^2 + m).$$

По следствию 2.2 достаточно показать, что

$$\left\{l^3 + ml - l_*^3 - ml_*\right\}_{l\in A} \not\supset \{jp^{k-1}\}_{j=0}^{p-1} (\mathrm{mod} p^k). \tag{4.1}$$

Случай $p > 3$, $k \geqslant 2$. Если $l \in A$, то $p^r \mid 3l^2 + m$ и $p^r \mid 3(l^2 - l_*^2)$. Поскольку $p \nmid m$, то $p \nmid l_*$, поэтому из чисел $(l - l_*)$ и $(l + l_*)$ только одно делится на p. Таким образом,

$$A = \{l_* + jp^r\}_{j=1}^{p^{k-r}} \cup \{-l_* - jp^r\}_{j=1}^{p^{k-r}}, \tag{4.2}$$

где, напомним, $r = [\frac{k}{2}]$. Далее,

$$\begin{aligned}(l_* + jp^r)^3 + m(l_* + jp^r) - l_*^3 - ml_* &= (3l_*^2 + m)jp^r + 3l_*j^2p^{2r} + j^3p^{3r} \\ &\equiv 3l_*j^2p^{2r} (\mathrm{mod} p^k).\end{aligned}$$

Если k – четное, то $2r = k$, и правая часть обращается в ноль по модулю p^k, то есть дает только один вариант из множества $\{jp^{k-1}\}_{j=0}^{p-1}(\mathrm{mod}\ p^k)$. Если k – нечетное, то $2r = k - 1$,

$$(l_* + jp^r)^3 + m(l_* + jp^r) - l_*^3 - ml_* \equiv 3l_*j^2p^{k-1} (\mathrm{mod} p^k),$$

и правая часть дает $\frac{p+1}{2}$ остатков из множества $\{jp^{k-1}\}_{j=0}^{p-1} (\mathrm{mod} p^k)$. Таким образом, первая часть в разложении (4.2) множества A дает не более $\frac{p+1}{2}$ остатков из множества $\{jp^{k-1}\}_{j=0}^{p-1} (\mathrm{mod} p^k)$. Покажем, что вторая часть в (4.2) не дает остатков вида jp^{k-1} вовсе. Учитывая равенство $m \equiv -3l_*^2 (\mathrm{mod} p)$ имеем

$$(-l_* - jp^r)^3 + m(-l_* - jp^r) - l_*^3 - ml_* \equiv -2(l_*^3 + ml_*) \equiv 4l_*^3 (\mathrm{mod} p).$$

Тем самым, все эти разности не делятся на p, и (4.1) доказано.

Случай $p = 3$, $k \geqslant 3$, $m \equiv 6 (\mathrm{mod} 9)$. Если $l \in A$, то $3^r \mid 3l^2 + m$ и $3^{r-1} \mid (l^2 - l_*^2)$. Поскольку $3 \nmid l_*$, из чисел $(l - l_*)$ и $(l + l_*)$ только одно делится на 3, поэтому

$$A = \{l_* + j3^{r-1}\}_{j=1}^{3^{k-r+1}} \cup \{-l_* - j3^{r-1}\}_{j=1}^{3^{k-r+1}}, \tag{4.3}$$

где, напомним, $r = [\frac{k+1}{2}] \geqslant 2$. Далее,

$$(l_* + j3^{r-1})^3 + m(l_* + j3^{r-1}) - l_*^3 - ml_* \\ = (3l_*^2 + m)j3^{r-1} + l_* j^2 3^{2r-1} + j^3 3^{3r-3} \\ \equiv l_* j^2 3^{2r-1} + j^3 3^{3r-3} (\mathrm{mod} 3^k).$$

Если k – нечетное, то $2r - 1 = k$, $3r - 3 \geqslant k$, и правая часть обращается в ноль по модулю 3^k. Покажем, что если k – четное, то правая часть принимает ровно два значения из множества $\{0, 3^{k-1}, 2 \cdot 3^{k-1}\}$. Действительно, если k – четное, $k \geqslant 6$, то $r = \frac{k}{2}$, $3r - 3 \geqslant k$ и

$$(l_*+j3^{r-1})^3+m(l_*+j3^{r-1})-l_*^3-ml_* \equiv l_* j^2 3^{k-1} \equiv 0 \text{ или } l_* 3^{k-1} \pmod{3^k}.$$

Если $k = 4$, то $r = 2$ и

$$(l_* + j3^{r-1})^3 + m(l_* + j3^{r-1}) - l_*^3 - ml_* \equiv (l_* j^2 + j^3)3^3 (\mathrm{mod} 3^4).$$

Далее,

$$\{l_* j^2 + j^3\}_{j=0,1,2} \equiv \{0, l_* + 1, l_* + 2\} (\mathrm{mod} 3),$$

и в правой части есть повторяющиеся остатки, так как $3 \nmid l_*$. Наконец, вторая часть в разложении (4.3) множества A снова не дает остатков вида $j3^{k-1}$. Действительно,

$$(-l_*-j3^{r-1})^3+m(-l_*-j3^{r-1})-l_*^3-ml_* \equiv -2(l_*^3+ml_*) \equiv -2l_*^3 (\bmod 3),$$

то есть все эти разности не делятся на 3, и (4.1) доказано. □

Теорема 4.3. *Пусть $k \geqslant 2$, m – нечетное. Если существует l_*, такое что*

$$3l_*^2 + m = a \cdot 2^{[\frac{k}{2}]},$$

a – нечетное, то

$$S_{2^k}(m) \neq 0.$$

Доказательство. По теореме 3.1 при $c = 0$

$$S_{2^k}(m) = \sum_{l-\text{нечет}} e\left(\frac{l^3 + ml}{2^k}\right).$$

С учетом следствия 2.2 достаточно показать, что

$$B := l^3 + ml - l_*^3 - ml_* \not\equiv 2^{k-1} (\mathrm{mod} 2^k), \tag{4.4}$$

если l и l_* – нечетные. Пусть $l = l_* + b \cdot 2^c$, b – нечетное, $c \geqslant 1$. Тогда

$$B = 3l_*^2 b 2^c + 3l_* b^2 2^{2c} + b^3 2^{3c} + mb2^c = ab2^{[\frac{k}{2}]+c} + 3l_* b^2 2^{2c} + b^3 2^{3c}.$$

Если $c > [\frac{k}{2}]$, то

$$B \equiv 0(\mathrm{mod} 2^k).$$

Если $c = [\frac{k}{2}]$, то

$$B \equiv (ab + 3l_* b^2)2^{2c} \equiv 0(\mathrm{mod} 2^{2c+1}),$$

так как a, b и l_* – нечетные. При этом $2c+1 \geqslant k$, то есть $B \equiv 0(\mod 2^k)$. Если $c < [\frac{k}{2}]$, то

$$B \equiv 3l_* b^2 2^{2c}(\mathrm{mod} 2^{2c+1}) \quad \Longrightarrow \quad 2^{2c+1} \nmid B \quad \Longrightarrow \quad 2^{k-1} \nmid B,$$

поскольку $2c + 1 \leqslant k - 1$. Таким образом, (4.4) доказано. □

Теперь из леммы 4.1 и теоремы 4.3 вытекает

Следствие 4.4. а) *Если* $m \equiv 3(\mathrm{mod}4)$, $k = 2$ *или* 3, *то* $S_{2^k}(m) \neq 0$.
б) *Если* $m \equiv 1(\mathrm{mod}8)$, $k = 4$ *или* 5, *то* $S_{2^k}(m) \neq 0$.
в) *Если* $m \equiv 5(\mathrm{mod}8)$, $k \geqslant 6$, *то* $S_{2^k}(m) \neq 0$.

Лемма 4.5. *Если* $m \equiv 5(\mathrm{mod}8)$, *то* $S_{16}(m) \neq 0$.

Доказательство. По лемме 4.1 существует такое l_*, что $16 \mid (3l_*^2 + m)$. Как и в доказательстве теоремы 4.3 достаточно показать, что $B \not\equiv 8(\mathrm{mod}16)$ при любом нечетном l, где B определено (4.4). Пусть снова $l = l_* + b \cdot 2^c$, b – нечетное, $c \geqslant 1$. Тогда

$$B \equiv 3l_* b^2 2^{2c} + b^3 2^{3c}(\mathrm{mod}16).$$

Если $c \geqslant 2$, то $B \equiv 0(\mathrm{mod}16)$. Если $c = 1$, то $B \equiv 4(\mathrm{mod}8)$. □

§5. Доказательство теорем 1.2, 1.3 и 1.4

Теорема 5.1. *Имеют место следующие рекуррентные формулы:*

$$F(p^k) = pF(p^{k-3}) + \frac{p^k - p^{k-1}}{2}, \quad p > 3, \ \ k \geqslant 3,$$
$$F(3^k) = 3F(3^{k-3}) + 3^{k-2}, \quad k \geqslant 3,$$
$$F(2^k) = 2F(2^{k-3}) + 2^{k-3}, \quad k \geqslant 5.$$

Доказательство. Если $p > 3$, то в силу следствия 3.6

$$F(p^k) = \#\left\{m \mod p^k : S_{p^k}(m) \neq 0, p^2 \mid m\right\}$$
$$+\#\left\{m \mod p^k : S_{p^k}(m) \neq 0, p \nmid m\right\}.$$

В силу следствия 3.5

$$\#\left\{m \mod p^k : S_{p^k}(m) \neq 0, p^2 \mid m\right\} = pF(p^{k-3}).$$

В силу следствия 3.4 и теоремы 4.2, если $p \nmid m$, то $S_{p^k}(m) \neq 0$ тогда и только тогда, когда уравнение $3x^2 + m \equiv 0 (\mathrm{mod} p)$ разрешимо. Следовательно,

$$\#\left\{m \mod p^k : S_{p^k}(m) \neq 0, p \nmid m\right\} = \frac{p^k - p^{k-1}}{2},$$

и первое утверждение теоремы доказано.

Второе утверждение теоремы вытекает из следствия 3.5, следствия 3.8 и теоремы 4.2.

Если $p = 2$, то в силу следствия 3.5 и следствия 3.9

$$F(2^k) = 2F(2^{k-3}) + \#\left\{m \mod 2^k : S_{2^k}(m) \neq 0, m \equiv 1(\mathrm{mod}8)\right\} \quad (5.1)$$
$$+\#\left\{m \mod 2^k : S_{2^k}(m) \neq 0, m \equiv 5(\mathrm{mod}8)\right\} \quad \text{при} \quad k \geqslant 4.$$

Из следствий 3.9, 4.4 и леммы 3.10 вытекает, что при $k \geqslant 6$ будет

$$\#\left\{m \mod 2^k : S_{2^k}(m) \neq 0, m \equiv 1(\mathrm{mod}8)\right\} = 0,$$
$$\#\left\{m \mod 2^k : S_{2^k}(m) \neq 0, m \equiv 5(\mathrm{mod}8)\right\} = 2^{k-3},$$

а при $k = 5$ – наоборот. □

Остается вычислить значения функции $F(q)$ для чисел вида $q = p$, $q = p^2$, где p – простое, а также $q = 8$ и $q = 16$.

Лемма 5.2. *$F(2) = 1$, $F(4) = F(8) = 4$, $F(16) = 6$.*

Доказательство. Непосредственно вычисляем значения

$$S_2(0) = 0, \quad S_2(1) = 2;$$
$$S_4(0) = 2, \ S_4(1) = -2, \ S_4(2) = S_4(3) = 2; \ S_8(1) = S_8(5) = 0.$$

С учетом следствий 3.5, 3.9 и 4.4 получаем $F(8) = 4$. Далее, в силу (5.1)

$$F(16) = 2F(2) + \#\{m \mod 16 : S_{16}(m) \neq 0, m \equiv 1(\mathrm{mod}8)\}$$
$$+\#\{m \mod 16 : S_{16}(m) \neq 0, m \equiv 5(\mathrm{mod}8)\} = 6$$

в силу следствия 4.4 и леммы 4.5. □

Из этой леммы и теоремы 5.1 вытекает теорема 1.2.

Лемма 5.3. *$F(3) = 1$, $F(9) = 3$.*

Доказательство. Явно вычисляем $S_3(0) = S_3(1) = 0$, $S_3(2) = 3$;

$$S_9(0) = 3 + 6\cos\frac{2\pi}{9}, \quad S_9(3) = 3 + 6\cos\frac{8\pi}{9}, \quad S_9(6) = 3 + 6\cos\frac{4\pi}{9};$$

$S_9(m) = 0$ при m не кратных трем в силу следствия 3.8. □

Из этой леммы и теоремы 5.1 вытекает теорема 1.3.

Из следствий 3.4, 3.7 и теоремы 4.2 вытекает

Лемма 5.4. *Если p – простое число, $p > 3$, то $F(p^2) = \frac{p^2+p}{2}$.*

Остается вычислить $F(p)$ для простых $p > 3$.

Лемма 5.5. *Пусть $p \nmid m$. Тогда*

$$\prod_{l=1}^{p-1}(l^2 + m) \equiv 0 \quad \textit{или} \quad 4 (\mathrm{mod} p).$$

Доказательство. Над полем $\mathbb{F}_p$ рассмотрим многочлен $P(x) = x^{\frac{p-1}{2}} - 1$ и множество его нулей $V = \{l^2\}_{l=1}^{p-1}$. Ясно, что $P(x) = \prod_{v \in V}(x - v)$. Поэтому

$$\prod_{l=1}^{p-1}(l^2 + m) = \left(\prod_{v \in V}(v + m)\right)^2 = P(-m)^2.$$

Если $-m \in V$, то это произведение обращается в ноль. Если $-m \notin V$, то $(-m)^{\frac{p-1}{2}} = -1$ и $P(-m) = -2$ в $\mathbb{F}_p$. □

Лемма 5.6. *Пусть $p > 3$ и $p \nmid m$. Тогда $S_p(m) \neq 0$.*

Доказательство. Хорошо известно, что $\prod_{l=1}^{p-1} l \equiv -1 (\mathrm{mod} p)$. Поэтому из предыдущей леммы вытекает, что

$$\prod_{l=1}^{p-1}(l^3 + ml) = \prod_{l=1}^{p-1} l \cdot \prod_{l=1}^{p-1}(l^2 + m) \equiv 0 \quad \text{или} \quad -4 (\mathrm{mod} p).$$

Тем самым, $\prod_{l=1}^{p-1}(l^3 + ml) \not\equiv -1 (\mathrm{mod} p)$, и числа $\{l^3 + ml\}_{l=1}^{p}$ не могут быть все различны по модулю p. Теперь из теоремы 2.1 при $k = 1$ вытекает, что $S_p(m) \neq 0$. □

Лемма 5.7. *Пусть $p > 3$. Тогда*

$$S_p(0) = 0 \quad \Longleftrightarrow \quad p \equiv 2 (\mathrm{mod} 3).$$

Доказательство. При $p \equiv 2 (\mathrm{mod} 3)$ уравнение $x^3 = 1$ в поле $\mathbb{F}_p$ не имеет решений, кроме $x = 1$. Поэтому все остатки чисел $\{l^3\}_{l=1}^{p-1}$ различны по модулю p, и

$$S_p(0) = \sum_{l=1}^{p} e\left(l^3 p^{-1}\right) = \sum_{s=1}^{p} e\left(sp^{-1}\right) = 0.$$

Если $p \equiv 1(\mathrm{mod}3)$, то уравнение $x^3 = 1$ имеет в поле $\mathbb{F}_p$ три различных корня (числа вида $y^{\frac{p-1}{3}}$). Поэтому среди чисел $\{l^3\}_{l=1}^{p-1}$ ровно $\frac{p-1}{3}$ различных по модулю p. В силу теоремы 2.1 при $k = 1$ получаем $S_p(0) \neq 0$. □

Из лемм 5.4, 5.6 и 5.7 вытекают формулы (1.4). Из формул (1.4) и теоремы 5.1 следует теорема 1.4.

Список литературы

1. B. C. Berndt, R. J. Evans, *The determination of Gauss sums.* — Bull. of Amer. Math. Soc., **5**, No. 2 (1981), 107–129.
2. Ф. Клопп, А. А. Федотов, *Лестницы Штарка–Ваннье и кубические экспоненциальные суммы.* — Функц. анализ и его прил., **50**, No. 3 (2016), 81–85.
3. Н. М. Коробов, *Тригонометрические суммы и их приложения.* М, Наука, 1989.
4. S. J. Patterson, *The asymptotic distribution of exponential sums*, I. — Experimental Math., **12**, No. 2 (2003), 135–153.
5. S. J. Patterson, *The asymptotic distribution of exponential sums*, II. — Experimental Math., **14**, No. 1 (2005), 87–98.
6. I. J. Schoenberg, *A note on the cyclotomic polynomial.* — Mathematika, **11** (1964), 131–136.
7. Р. Вон, *Метод Харди–Литтлвуда.* М, Мир, 1985.

Filonov N. D. Number of non-zero cubic sums.

The exponential sums $S_q(a,m) = \sum\limits_{l=1}^{q} \exp\left(2\pi i(al^3 + ml)q^{-1}\right)$ are considered. For every natural q, the explicit formulas for the number of non-zero sums among $S_q(a,0), \ldots, S_q(a,q-1)$ are found.

С.-Петербургское отделение
Математического института
им. В. А. Стеклова РАН
Фонтанка 27, 191023 Санкт-Петербург;
С.-Петербургский
государственный университет,
Университетская наб. д.7–9,
199034 Санкт-Петербург, Россия
E-mail: filonov@pdmi.ras.ru

Поступило 19 июня 2018 г.