О некоторых аддитивных задачах теории чисел

Шкредов И.Д.

1. Постановка задач и формулировка результатов.

Для простого числа p обозначим через Z_p кольцо вычетов по модулю p, а через Z_p^* – группу обратимых элементов Z_p. Пусть R – подгруппа Z_p^*. В работе [1] рассматривался вопрос о представимости произвольного элемента Z_p^* в виде суммы элементов из R и был получен следующий результат.

Теорема А. Пусть R – подгруппа Z_p^*. Если для некоторого натурального $l \geq 2$ выполнено $|R| > p^{1/2+1/2l}$, то для произвольного $b \in Z_p^*$ существуют $x_1, \ldots, x_l \in R$, что $b \equiv x_1 + \ldots + x_l (mod\ p)$.

В работах [2] и [3] изучалась другая аддитивная задача. Пусть g первообразный корень по модулю p, $m \geq 2$ – натуральное. Рассмотрим множество разностей

$$A^* := \{(g^{n_1} - g^{n_2},\ g^{n_2} - g^{n_3}, \ldots, g^{n_{m-1}} - g^{n_m})(mod\ p)\ :\ 1 \leq n_1, \ldots, n_m \leq N\} \quad (1)$$

В [2] была доказана следующая теорема.

Теорема Б. Пусть a произвольный вектор, $a \in Z_p^{m-1}$ такой, что все суммы $b_j := \sum_{k=j}^{m-1} a_k$, $1 \leq j \leq m-1$, $b_m := 0$ различны по модулю p. Пусть также $N \gg p^{1-1/2m+\varepsilon}$. Тогда a принадлежит A^*.

В работе [3] был рассмотрен случай $m = 2$ и исследован вопрос о принадлежности "почти всех"вычетов из Z_p множеству A^*.

Теорема В. Для произвольного простого p, первообразного корня g по $mod\ p$ и любого натурального $N < p$

$$\#\{h(mod\ p)\ :\ h \neq g^x - g^y, 1 \leq x, y \leq N\ \} \ll \frac{p^3 \log p}{N^3}.$$

В работах [4, 5, 6, 7] исследовались свойства чисел с ограничениями на цифры. Пусть $s > k \geq 2$ – натуральные числа, $D = \{d_1, \ldots, d_k\} \subseteq$

$\mathbf{N}_0 = \mathbf{N} \cup \{0\}$, $0 = d_1 < d_2 < \ldots < d_k < s$ – некоторое фиксированное множество цифр в системе счисления по основанию s. Будем считать, что $(d_1, \ldots, d_k) = 1$. Рассмотрим множества

$$K_s^D = \{x \in \mathbf{N} \ : \ x = \sum_{j=0}^{h} \delta_j s^j, \ \delta_j \in D\},$$

$$K_s^D(N) = \{x \in K_s^D \ : \ x < N\}.$$

Пусть натуральные N и q, $(q, s) = 1$ удовлетворяют следующему условию

$$N > \exp(\gamma \lg q \lg\lg q) \tag{2}$$

(здесь γ – некоторая постоянная, зависящая от s). В [6, 7] было, в частности, доказано, что при указанных условиях для всякого целого x найдется $a \in K_s^D(N)$ такое, что $a \equiv x(mod\ q)$. Заменить условие (2) на более слабое условие $N > q^\sigma, \sigma = \sigma(s)$ пока не удается. Тем не менее в [7] был доказан результат о числе сравнений.

Теорема Г. Пусть p – простое число, $s \geq 3$, $(p, s) = 1$, $l \geq 2$ и $(\lambda, p) = 1$. Для любого положительного ε найдется натуральное $r_2 = r_2(s, \varepsilon)$ такое, что при $N > p^{r_2}$ для числа $T_{l,\lambda}^{s,D}(N)$ решений сравнения $a_1 \ldots a_l \equiv \lambda(mod\ p), a_1, \ldots, a_l \in K_s^D(N)$, имеет место формула

$$T_{l,\lambda}^{s,D}(N) = \frac{|K_s^D(N)|^l}{p-1} + O\Big(|K_s^D(N)|^l p^{l(-\frac{1}{2}+\varepsilon)}\Big).$$

Отметим, что при $l \geq 3$ заключение теоремы Г дает асимптотическую формулу для числа решений.

В настоящей заметке будут доказаны утверждения о разрешимости сравнений, возникающих в данных аддитивных задачах, для "почти всех"вычетов. Также будет доказано небольшое усиление теоремы В.

Теорема 1. Для любого натурального $l \geq 2$, любого $\varepsilon > 0$ существует $C_\varepsilon > 0$, что для любой подгруппы $R \subseteq Z_p^*$ мощности $|R| \geq C_\varepsilon p^{l/(2l-1)}$, количество $x \in Z_p^*$ $\ x \equiv x_1 + \ldots + x_l(mod\ p),\ x_1, \ldots, x_l \in R$ больше, чем $(1-\varepsilon)p$.

Теорема 2. Для любого натурального $l \geq 2$, любого $\varepsilon > 0$ и любого набора $b_1, \ldots, b_l \in Z_p^*$ существует $C_\varepsilon > 0$, что для $N \geq C_\varepsilon p^{l/(2l-1)}$ количество $x \in Z_p^*$ представимых в виде $x \equiv b_1 g^{n_1} + \ldots + b_l g^{n_k}(mod\ p),\ 1 \leq n_1, \ldots, n_l \leq N$ больше, чем $(1-\varepsilon)p$.

Теорема 3. Для любого натурального $m \geq 2$ и любого $\varepsilon > 0$ существует $C_\varepsilon > 0$, что для $N \geq C_\varepsilon p^{m/(m+1)}$ выполнено $|A^*| > (1-\varepsilon)p^{m-1}$.
Замечание. При условии выполнения обобщенной гипотезы Римана в [2] было показано, что в случае $m = 2$ теорема Б верна для $N \gg p^{2/3+\varepsilon}$.
Теорема 4. Для любого $\varepsilon > 0$ найдутся натуральные p_ε и $r_2 = r_2(s, \varepsilon)$ такие, что для произвольного простого $p > p_\varepsilon$ и $N > p^{r_2}$ количество вычетов $\lambda \in Z_p^*$ представимых в виде $\lambda \equiv a_1 a_2 (mod\ p),\ a_1, a_2 \in K_s^D(N)$, больше, чем $(1-\varepsilon)(p-1)$.
Доказательство теорем основано на одном методе Фреймана из [8].

2. Доказательство теорем.

Пусть M подмножество Z_p. Обозначим через $\widehat{\chi}_M(r)$ r - й коэффициент Фурье характеристической функции $\chi_M(x)$ множества M $\widehat{\chi}_M(r) = \sum_{x \in M} e_p(rx)$, где $e_p(x) = e^{2\pi i x/p}$. Пусть lM означает сумму $M + \ldots + M$ l раз , то есть $lM = \{x\ :\ x \equiv x_1 + \ldots + x_l (mod\ p),\ x_1, \ldots, x_l \in M\}$.

Доказательство теоремы 1. Возьмем любое $\varepsilon > 0$, $\varepsilon < 1$. Пусть $C_\varepsilon \geq \varepsilon^{-2/(2l-1)}$ и $|R| \geq C_\varepsilon p^{l/(2l-1)}$. Тогда $p^{l/2}/|R|^{(2l-1)/2} < \varepsilon$. Рассмотрим сумму $\sum_{r \in Z_p} \widehat{\chi}_R^l(r) \widehat{\chi}_{lR}(-r)$. С одной стороны эта сумма равна
$\sum_{r \in Z_p} \widehat{\chi}_R^l(r) \widehat{\chi}_{lR}(-r) = \sum_r \sum_{x_1 \in R} \ldots \sum_{x_l \in R} \sum_{c \in lR} e_p(x_1 + \ldots + x_l - c) = p|R|^l$.
С другой стороны она равна $|R|^l |lR| + \sum_{r \in Z_p^*} \widehat{\chi}_R^l(r) \widehat{\chi}_{lR}(-r)$. Так как для $r \in Z_p^*$ имеем $|\widehat{\chi}_R(r)| < \sqrt{p}$ (см. [1]), то применяя неравенство Коши-Буняковского и равенство Парсеваля получаем

$$|R|^l (p - |lR|) \leq p^{(l-1)/2} |\sum_{r \in Z_p^*} \widehat{\chi}_R(r) \widehat{\chi}_{lR}(-r)| \leq p^{(l+2)/2} |R|^{1/2}.$$

Следовательно, по выбору C_ε, $|lR| \geq p(1 - \frac{p^{l/2}}{|R|^{(2l-1)/2}}) > (1-\varepsilon)p$. Теорема доказана.

Доказательство теоремы 2. Возьмем любое $\varepsilon > 0$, $\varepsilon < 1$. Пусть $C_\varepsilon^1 \geq \varepsilon^{-2/(2l-1)}$, $D = \{g^j : 0 \leq j \leq C_\varepsilon^1 p^{m/(m+1)}\}$, $E = \{xy : x, y \in D\}$. Пусть также $\lambda_E(z) = \#\{x, y \in D\ :\ xy \equiv z (mod\ p)\}$, а $\widehat{\lambda}_E(r) = \sum_{z \in E} \lambda_E(z) e_p(rz)$. Заметим, что $\sum_z \lambda_E(z) = |D|^2$, $\sum_z \lambda_E^2(z) \leq |D|^3$ и для $r \in Z_p^*$ имеем $|\widehat{\lambda}_E(r)| < \sqrt{p}|D|$ (см. [1]). Обозначим через M все $x \in Z_p$ вида $x \equiv b_1 e_1 + \ldots + b_l e_l (mod\ p),\ e_i \in E$. Рассмотрим сумму

$$\sum_{r \in Z_p} \widehat{\chi}_M(-r) \widehat{\lambda}_E(b_1 r) \ldots \widehat{\lambda}_E(b_l r) = p|D|^{2l} \qquad (3)$$

Главный член в (3) с $r = 0$ равен $|M||D|^{2l}$. Оценивая оставшуюся сумму сверху, получаем (3) $\leq |M||D|^{2l} + p(p|D|^3)^{1/2} p^{(l-1)/2} |D|^{l-1}$. Следовательно, по выбору C^1_ε, $|M| > (1-\varepsilon)p$. Значит, $|gM| = |M| > (1-\varepsilon)p$ и теорема 2 доказана с $C_\varepsilon = 3C^1_\varepsilon$.

Доказательство теоремы 3. Возьмем любое $\varepsilon > 0$, $\varepsilon < 1$. Пусть $D = \{g^j : 0 \le j \le C^1_\varepsilon p^{m/(m+1)}\}$, $E = \{xy : x, y \in D\}$, а C^1_ε выберем потом. Пусть обозначения $\lambda_E(z)$, $\widehat{\lambda}_E(r)$ имеют тот же смысл, что и в теореме 2. Обозначим через $\chi_A(x)$ характеристическую функцию множества $A \subseteq Z_p^{m-1}$ из (1) с $0 \le n_1, \dots, n_m \le 2|D|$, а через $\widehat{\chi}_A(\mathbf{r}) = \sum_{\mathbf{x}\in A} e_p(\mathbf{r}x)$ её $\mathbf{r}$- й коэффициент Фурье. Рассмотрим сумму

$$\sum_{r_1,\dots,r_{m-1}} \widehat{\chi}_A(-(r_1,\dots r_{m-1}))\widehat{\lambda}_E(r_1)\widehat{\lambda}_E(-r_1+r_2)\dots$$

$$\dots\widehat{\lambda}_E(-r_{m-2}+r_{m-1})\widehat{\lambda}_E(-r_{m-1}) = p^{m-1}|D|^{2m}. \qquad (4)$$

Член в (4) с $r_1 = \ldots = r_{m-1} = 0$ равен $|A||D|^{2m}$. Оценим сверху оставшуюся сумму. Разобьём её на сумму σ_1 по $r_1 \ne 0$ и на сумму σ_2 по $r_1 = 0$. Пользуясь оценкой для коэффициентов Фурье функции λ_E и неравенством Коши-Буняковского получаем

$$\sigma_1 \le \sqrt{p}|D|(\sum_{r_1,\dots,r_{m-1}} |\widehat{\chi}_A(-(r_1,\dots r_{m-1}))|^2)^{1/2} \cdot$$

$$(\sum_{r_1,\dots,r_{m-1}} |\widehat{\lambda}_E(-r_1+r_2)|^2\dots|\widehat{\lambda}_E(-r_{m-1})|^2)^{1/2} \le \sqrt{p}|D|p^{m-1}(p|D|^3)^{(m-1)/2}$$

При суммировании по $r_1 = 0$ второй множитель в (4) равен $|D|^2$. Как и выше разбиваем σ_2 на сумму по $r_2 \ne 0$ и на сумму по $r_2 = 0$ и так далее. Окончательно получаем

$$(4) \le |A||D|^{2m} + \sqrt{p}|D|p^{m-1}(p|D|^3)^{(m-1)/2}(1 + \frac{|D|^2}{\sqrt{p}|D|^{3/2}} + \frac{|D|^4}{p|D|^3} + \dots) \le$$

$$\le |A||D|^{2m} + 2\sqrt{p}|D|p^{m-1}(p|D|^3)^{(m-1)/2}.$$

Находя C^1_ε из неравенства $p^{m/2}/|D|^{(m+1)/2} < \varepsilon$, получаем $|A| \ge p^{m-1}(1 - p^{m/2}/|D|^{(m+1)/2}) > (1-\varepsilon)p^{m-1}$. Итак, существует $> (1-\varepsilon)p^{m-1}$ векторов из Z_p^{m-1} принадлежащих A. Ровно столько же векторов принадлежат $gA \subseteq A^*$, где в определении A^* имеем $N \ge 3C^1_\varepsilon p^{m/(m+1)}$. Теорема доказана.

Доказательство теоремы 4. Возьмем любое $\varepsilon > 0$, $\varepsilon < 1$ и $\delta > 0$, которое выберем потом. Пусть $K = K^D_s(N)$ ($N > p^{r_2}$ – выберем потом), $E = \{xy \ (mod\ p) : x, y \in K\}$. Докажем, что $|E| > (1-\varepsilon)(p-1)$. Пусть $\chi_r(x) =$

$e(r\, ind(x)/(p-1))$ характер группы Z_p^*. Число $\{x \in K, x \equiv t(mod\, p)\}$ обозначим через $\mu_K(t)$, Через $\widehat{\mu}_K(r)$ и $\widehat{f}_E(r)$ обозначим тригонометрические суммы $\widehat{\mu}_K(r) = \sum_{x \in Z_p^*} \mu_K(x)\chi_r(x)$ и $\widehat{f}_E(r) = \sum_{x \in Z_p^*} f_E(x)\chi_r(x)$, где $f(x)$ – характеристическая функция множества E. Для любого $\delta > 0$ и любого неглавного характера $\chi_r(x)$ при достаточно большом N справедлива следующая оценка $|\widehat{\mu}_K(r)| \leq p^{-1/2+\delta}|K|$ (см., например, [7]). Заметим, что $\sum_{x \in Z_p^*} \mu_K(x) = |K|$. Оценим второй момент P функции $\mu_K(x)$, то есть сумму $P = \sum_{x \in Z_p^*} \mu_K^2(x)$. Пусть $K = K_s^D(s^{r_1} - 1)$, $r_1 = \log_s p/2$, тогда $s^{r_1} < p$. В [?] было доказано, что при условии $s^{r_1} < p$ выполнено $P \leq (k+1)^{2r_1}(1+\lambda)^{r_1}/s^{r_1}$, где $0 < \lambda < 1$. Тогда при $\delta < (1-\lambda)/2$ и достаточно больших p получаем $P < \varepsilon^2|K|^2/p^{2\delta}$.
Рассмотрим сумму

$$\sum_{r \in Z_p^*} \widehat{\mu}_K^2(r)\widehat{f}_E(-r) = (p-1)|K|^2. \tag{5}$$

В (5) член с $r = p-1$ равен $|E||K|^2$. Оценим оставшуюся сумму

$$\sum_{r=1}^{p-2} \widehat{\mu}_K^2(r)\widehat{f}_E(-r) \leq |K|p^{-1/2+\delta}(p-1)((p-1)P)^{1/2} < (p-1)|K|^2\varepsilon.$$

Значит, $|E| > (1-\varepsilon)(p-1)$. Теорема доказана.

Список литературы

[1] S.Konyagin and I.Shparlinski. Character sums with exponential functions. Cambridge University Press, Cambridge, 1999.

[2] Z.Rudnick and A.Zaharescu. The distribution of spacings between small powers of a primitive root. Israel J.Math. 120 (2000), 271–287.

[3] M.Vâjâitu and A.Zaharescu. Differences between powers of a primitive root. Int. J.Math. Sci. 29 (2002), 325–331.

[4] P.Erdös, C.Mauduit, A.Sárközy. On arithmetic properties of integers with missing digits. I: Distribution in residue classes. J.Number Theory 70 (1998), 99–120.

[5] P.Erdös, C.Mauduit, A.Sárközy. On arithmetic properties of integers with missing digits. II: Prime factors. Discrete Math. 200 (1999), 149–164.

[6] S.Konyagin. Arithmetic properties of integers with missing digits: distribution in residue classes. Periodica Math. Hung. Vol. 42 (1–2), 2001, pp. 145–162.

[7] Н.Г. Мощевитин. О числах с ограничениями на цифры. ДАН, 2002, т. 384, N2, с. 167–170.

[8] Г.А.Фрейман. Основания структурной теории сложения множеств. Казанский гос. пед. инст., Казань, 1966.