that the order of X^-/TX^- is just equal to the highest power of p which divides h^-. Hence, applying the above lemma for X^-, we see that

$$p^{\mu^-} \leqslant h^-.$$

On the other hand, the classical class number formula for k states that

$$h^- = 2p \prod_{\chi} \left(-\frac{1}{2p} \sum_{a=1}^{p-1} a\chi(a) \right),$$

where the product is taken over all Dirichlet characters χ defined $\bmod p$ with $\chi(-1) = -1$. Since

$$\left| \sum_{a=1}^{p-1} a\chi(a) \right| < \sum_{a=1}^{p-1} a = \frac{(p-1)p}{2},$$

we have

$$h^- < 2^{2-p} p (p-1)^{(p-1)/2} \leqslant p^{(p-1)/2}.$$

It then follows that

$$\mu^- < (p-1)/2$$

so that

$$\mu < p-1,$$

q.e.d.

Instead of the above elementary argument, we may estimate h^- also by using

$$|L(1;\chi)| < 2\log p, \quad \chi \neq 1.$$

We then see that for any given real number $c > \frac{1}{2}$, there exists an integer $N(c)$ such that

$$\mu < c(p-1)$$

whenever $p \geqslant N(c)$. It is also clear that by the same method, we can find an upper bound for the μ-invariant of a so-called $\boldsymbol{Z}_p$-extension K/k in many special cases. In particular, if K has only one prime divisor which divides the rational prime p (as in the special case discussed above), then

$$\mu(K/k) \leqslant \log h / \log p,$$

where h is the class number of k.

References

[1] K. Iwasawa, *On Γ-extensions of algebraic number fields*, Bull. Amer. Math. Soc. 65 (1959), pp. 183–226.

[2] — *On the theory of cyclotomic fields*, Ann. of Math. 70 (1959), pp. 530–561.

[3] J.-P. Serre, *Classes des corps cyclotomiques*, Seminaire Bourbaki, Exposé 174 (1958/1959).

PRINCETON UNIVERSITY

Received on 21. 2. 1971 (147)

ACTA ARITHMETICA
XXI (1972)

О числе решений одного сравнения

Г. И. Перельмутер (Саратов), А. Г. Постников (Москва)

Памяти В. Серпинского

Пусть $n \geqslant 1$, $m_1, \ldots, m_n$ — целые положительные числа

$$F(x, x_1, \ldots, x_n) = f_0(x) + f_1(x)x_1^{m_1} + \ldots + f_n(x)x_n^{m_n}, \tag{1}$$

где $f_0, f_1, \ldots, f_n$ — полиномы от неизвестного x с целыми коэффициентами. Мы будем изучать число $N_F(p)$ решений сравнения

$$F(x, x_1, \ldots, x_n) \equiv 0 \pmod p \tag{2}$$

при растущем простом p. Случай, когда все $f_j = \text{const}$, рассматривался А. Вейлем в работе [3].

Для формулировки результата введем некоторые обозначения:

δ_j — Н. О. Д. канонических показателей при разложении полинома $f_j(x)$ на множители над полем рациональных чисел $(0 \leqslant j \leqslant n)$, причем полагаем $\delta_j = 0$, если $f_j = \text{const}$;

допустимая система $\alpha = (\alpha_1, \ldots, \alpha_n)$ — это система рациональных чисел $\alpha_1, \ldots, \alpha_n$, удовлетворяющих условиям:

$$0 < \alpha_j < 1, \quad m_j \alpha_j \equiv 0 \pmod 1, \quad \sum_{j=1}^{n} \alpha_j \not\equiv 0 \pmod 1; \tag{3}$$

$r_\alpha = \left(\alpha_1\delta_1, \ldots, \alpha_n\delta_n, \delta_0 \sum_{j=1}^{n} \alpha_j\right)$, т.е.

$$r_\alpha = \prod_q q^{\gamma_q(r_\alpha)}, \quad \text{где} \quad \gamma_q(r_\alpha) = \operatorname{Min}\left\{\gamma_q(\alpha_1\delta_1), \ldots, \gamma_q(\alpha_n\delta_n), \gamma_q\left(\delta_0 \sum_j \alpha_j\right)\right\}. \tag{4}$$

Будет доказана

Теорема. *Предположим, что выполнены условия:*

1) *Полиномы $f_0(x), \ldots, f_n(x)$ попарно взаимно просты;*

2) *Для всех допустимых систем α (если они существуют)*

$$r_\alpha \not\equiv 0 \pmod 1. \tag{5}$$

that the order of X^-/TX^- is just equal to the highest power of p which divides h^-. Hence, applying the above lemma for X^-, we see that

$$p^{\mu^-} \leqslant h^-.$$

On the other hand, the classical class number formula for k states that

$$h^- = 2p \prod_{\chi} \left(-\frac{1}{2p} \sum_{a=1}^{p-1} a\chi(a) \right),$$

where the product is taken over all Dirichlet characters χ defined $\bmod p$ with $\chi(-1) = -1$. Since

$$\left| \sum_{a=1}^{p-1} a\chi(a) \right| < \sum_{a=1}^{p-1} a = \frac{(p-1)p}{2},$$

we have

$$h^- < 2^{2-p} p (p-1)^{(p-1)/2} \leqslant p^{(p-1)/2}.$$

It then follows that

$$\mu^- < (p-1)/2$$

so that

$$\mu < p-1,$$

q.e.d.

Instead of the above elementary argument, we may estimate h^- also by using

$$|L(1;\chi)| < 2\log p, \quad \chi \neq 1.$$

We then see that for any given real number $c > \frac{1}{2}$, there exists an integer $N(c)$ such that

$$\mu < c(p-1)$$

whenever $p \geqslant N(c)$. It is also clear that by the same method, we can find an upper bound for the μ-invariant of a so-called $\boldsymbol{Z}_p$-extension K/k in many special cases. In particular, if K has only one prime divisor which divides the rational prime p (as in the special case discussed above), then

$$\mu(K/k) \leqslant \log h / \log p,$$

where h is the class number of k.

References

[1] K. Iwasawa, *On Γ-extensions of algebraic number fields*, Bull. Amer. Math. Soc. 65 (1959), pp. 183–226.

[2] — *On the theory of cyclotomic fields*, Ann. of Math. 70 (1959), pp. 530–561.

[3] J.-P. Serre, *Classes des corps cyclotomiques*, Seminaire Bourbaki, Exposé 174 (1958/1959).

PRINCETON UNIVERSITY

Received on 21. 2. 1971 (147)

ACTA ARITHMETICA
XXI (1972)

О числе решений одного сравнения

Г. И. Перельмутер (Саратов), А. Г. Постников (Москва)

Памяти В. Серпинского

Пусть $n \geqslant 1$, $m_1, \ldots, m_n$ — целые положительные числа

$$F(x, x_1, \ldots, x_n) = f_0(x) + f_1(x)x_1^{m_1} + \ldots + f_n(x)x_n^{m_n}, \tag{1}$$

где $f_0, f_1, \ldots, f_n$ — полиномы от неизвестного x с целыми коэффициентами. Мы будем изучать число $N_F(p)$ решений сравнения

$$F(x, x_1, \ldots, x_n) \equiv 0 \pmod p \tag{2}$$

при растущем простом p. Случай, когда все $f_j = \text{const}$, рассматривался А. Вейлем в работе [3].

Для формулировки результата введем некоторые обозначения:

δ_j — Н. О. Д. канонических показателей при разложении полинома $f_j(x)$ на множители над полем рациональных чисел $(0 \leqslant j \leqslant n)$, причем полагаем $\delta_j = 0$, если $f_j = \text{const}$;

допустимая система $\alpha = (\alpha_1, \ldots, \alpha_n)$ — это система рациональных чисел $\alpha_1, \ldots, \alpha_n$, удовлетворяющих условиям:

$$0 < \alpha_j < 1, \quad m_j \alpha_j \equiv 0 \pmod 1, \quad \sum_{j=1}^{n} \alpha_j \not\equiv 0 \pmod 1; \tag{3}$$

$r_\alpha = \left(\alpha_1\delta_1, \ldots, \alpha_n\delta_n, \delta_0 \sum_{j=1}^{n} \alpha_j\right)$, т.е.

$$r_\alpha = \prod_q q^{\gamma_q(r_\alpha)}, \quad \text{где} \quad \gamma_q(r_\alpha) = \operatorname{Min}\left\{\gamma_q(\alpha_1\delta_1), \ldots, \gamma_q(\alpha_n\delta_n), \gamma_q\left(\delta_0 \sum_j \alpha_j\right)\right\}. \tag{4}$$

Будет доказана

Теорема. *Предположим, что выполнены условия:*

1) *Полиномы $f_0(x), \ldots, f_n(x)$ попарно взаимно просты;*

2) *Для всех допустимых систем α (если они существуют)*

$$r_\alpha \not\equiv 0 \pmod 1. \tag{5}$$

Тогда при $p \to \infty$

$$N_F(p) = p^n + O(p^{n/2}). \tag{6}$$

Так как требование 2) весьма сложно хоть оно, повидимому, является наиболее общим требованием, при котором теорема может быть доказана), то мы приведем два других условия, каждое из которых влечет (5). Положим $m_0 = m_1 m_2 \dots m_n$ и выведем

Следствие. *Теорема справедлива при условии* 1) *и любом из требований*:

2)′ *Существует такой индекс* j_0, $0 \leqslant j_0 \leqslant n$, *что для некоторого канонического показателя* λ *полинома* f_{j_0} *имеем* $(\lambda, m_{j_0}) = 1$.

2)″ *Существует такой индекс* j_0, $0 \leqslant j_0 \leqslant n$, *что* $(\deg f_{j_0}, m_{j_0}) = 1$.

Доказательство. В случае 2)′ непосредственно ясно, что $(\delta_{j_0}, m_{j_0}) = 1$. В случае 2)″ положим $f_{j_0} = P_1^{\lambda_1} \dots P_s^{\lambda_s}$, где $P_1, \dots, P_s$ неприводимы. Тогда $\deg f_{j_0} = \lambda_1 \deg P_1 + \dots + \lambda_s \deg P_s \equiv 0 \pmod{\delta_{j_0}}$ и снова $(\delta_{j_0}, m_{j_0}) = 1$. Из (3) при $j_0 \neq 0$ имеем $a_{j_0} \delta_{j_0} \not\equiv 0 \pmod 1$ и при $j_0 = 0$ $\delta_0 \sum_j a_j \not\equiv 0 \pmod 1$; в любом случае получаем $r_a \equiv 0 \pmod 1$.

Замечание. Условие 2) в определенном смысле необходимо. Например, уравнение $x^2 + x_1^2 + x_2^2 + x_3^2 = 0$ имеет $p^3 + p^2 - p$ решений. Здесь $f_0 = x^2$,

$$f_1 = f_2 = f_3 = 1, \quad m_1 = m_2 = m_3 = 2, \quad \delta_0 = 2, \quad \delta_1 = \delta_2 = \delta_3 = 0.$$

Для единственно возможной допустимой системы $a = (\frac{1}{2}, \frac{1}{2}, \frac{1}{2})$ условие (5) не выполняется.

Для удобства всюду в дальнейшем мы будем рассматривать f_j и F как многочлены над полем $k = [p]$, а сравнение (2) — как уравнение над k. Для всех достаточно больших p условие 1) теоремы выполняется, очевидно, и над k; точно также, если для f_j определить $\delta_j(p)$ как Н. О. Д. канонических показателей при разложении f_j над k, то $\delta_j(p) = \delta_j$ для всех достаточно больших p, несмотря на то, что неприводимый в характеристике 0 делитель $f_j(x)$ может быть разложим по модулю p. Без специальных оговорок мы будем считать p достаточно большим. Введем еще следующие обозначения.

$\sum_\xi, \sum_t, \sum_x$ — суммирование по всем элементам из k;

$\sum_t'$ — суммирование по всем ненулевым элементам из k;

e — аддитивный характер, точнее $e(\xi) = \exp\left(\frac{2\pi i}{p}\xi\right)$, $\xi \in k$;

χ — мультипликативный характер группы $k^* = k \setminus \{0\}$, причем доопределяем $\chi(0) = 0$, если $\chi \neq \chi_0$, $\chi_0(0) = 1$, χ_0 — главный характер; полагаем всегда $\chi^0 = \chi_0$, $\bar\chi$ — сопряженный характер;

$g(\chi) = \sum_\xi \chi(\xi) e(\xi)$ — гауссова сумма для χ;

$d_j = (m_j, p-1)$, $j = 1, 2, \dots, n$; χ_{d_j} — характер порядка d_j.

Нижеследующие леммы хорошо известны.

Лемма 1. $|g(\chi)| = \sqrt{p}$, *если* $\chi \neq \chi_0$; $g(\chi_0) = 0$.

Лемма 2. *Для* $a \in k$

$$\sum_\xi \chi(\xi) e(a\xi) = \begin{cases} p, & \text{если } \chi = \chi_0 \text{ и } a = 0, \\ \bar\chi(a) g(\chi), & \text{в остальных случаях.} \end{cases}$$

Лемма 3.

$$\sum_x e(ax^m) = \begin{cases} p, & \text{если } a = 0, \\ \sum_{k=0}^{d-1} \bar\chi_d^k(a) g(\chi_d^k), & \text{если } a \neq 0, \end{cases}$$

где $d = (m, p-1)$, χ_d — *характер порядка* d.

Центральную роль играет

Основная лемма. *В условиях теоремы предположим дополнительно, что* $d_j = (m_j, p-1) \geqslant 2$ *для* $j = 1, 2, \dots, n$. *Тогда, если* $\chi_{d_1}^{k_1} \dots \chi_{d_n}^{k_n} \neq \chi_0$ *для некоторого набора* $1 \leqslant k_j \leqslant d_j - 1$, *то*

$$S = \sum_x \bar\chi_{d_1}^{k_1}(f_1(x)) \dots \bar\chi_{d_n}^{k_n}(f_n(x)) \chi_{d_1}^{k_1} \dots \chi_{d_n}^{k_n}(f_0(x)) = O(\sqrt{p}), \tag{7}$$

где постоянная в символе O *не зависит от* p.

Доказательство. Воспользуемся терминологией и методом работы [2]. Рассмотрим проективную прямую P^1 и дивизор $\mathfrak{M} = \sum_{j=0}^n \mathfrak{M}_j + (\infty)$, где $\mathfrak{M}_j$ имеет своими компонентами все нули полинома f_j, взятые с кратностями 1. Степень $\mathfrak{M}$ зависит от $f_0, \dots, f_n$, но не от p. Построим характер X группы дивизоров прямой P^1 следующим образом.

Если $\mathfrak{A} = \sum_a n_a(a)$ — положительный рациональный над k дивизор, не имеющий общих компонент с $\mathfrak{M}$, то полином $f_{\mathfrak{A}} = \prod_a (x-a)^{n_a}$ взаимно прост с каждым f_j и однозначно определяется условием $f_{\mathfrak{A}} = \mathfrak{A} - \deg \mathfrak{A}(\infty)$. Положим

$$X(\mathfrak{A}) = \bar\chi_{d_1}^{k_1}(\langle f_{\mathfrak{A}}, f_1\rangle) \dots \bar\chi_{d_n}^{k_n}(\langle f_{\mathfrak{A}}, f_n\rangle) \chi_{d_1}^{k_1} \dots \chi_{d_n}^{k_n}(\langle f_{\mathfrak{A}}, f_0\rangle), \tag{8}$$

где $\langle f_{\mathfrak{A}}, f_j\rangle = \prod_a f_j^{n_a}(a)$ — результант. X является характером модуля $\mathfrak{M}$ и $S = \sum_{\deg \mathfrak{P} = 1} \chi(\mathfrak{P})$. Оценка (7) получается тогда из неравенства (4) работы [2], но при этом следует показать, что X — неособенный характер, для чего достаточно найти рациональную функцию φ с условием

$$((\varphi), \mathfrak{M}) = 1, \quad X((\varphi)) \neq 1. \tag{9}$$

Если вообще $\big((\varphi), \mathfrak{M}\big) = 1$ и $(\varphi) = \mathfrak{A} - \mathfrak{B}$, то $\deg\mathfrak{A} = \deg\mathfrak{B}$ и поэтому

$$\left(\frac{f_{\mathfrak{A}}}{f_{\mathfrak{B}}}\right) = (f_{\mathfrak{A}}) - (f_{\mathfrak{B}}) = \mathfrak{A} - \deg\mathfrak{A}(\infty) - \big(\mathfrak{B} - \deg\mathfrak{B}(\infty)\big) = \mathfrak{A} - \mathfrak{B} = (\varphi).$$

Следовательно, можно считать $\varphi = \dfrac{f_{\mathfrak{A}}}{f_{\mathfrak{B}}}$, т.е. выбираем φ с условием нормировки $\varphi(\infty) = 1$. Из (8) получаем

$$X\big((\varphi)\big) = \frac{X(\mathfrak{A})}{X(\mathfrak{B})} = \prod_{j=1}^{n} \overline{\chi}_{d_j}^{k_j}\left(\frac{\langle f_{\mathfrak{A}}, f_j\rangle}{\langle f_{\mathfrak{B}}, f_j\rangle}\right) \chi_{d_1}^{k_1} \dots \chi_{d_n}^{k_n}\left(\frac{\langle f_{\mathfrak{A}}, f_0\rangle}{\langle f_{\mathfrak{B}}, f_0\rangle}\right). \tag{10}$$

Но, как легко видеть, $\dfrac{\langle f_{\mathfrak{A}}, f_j\rangle}{\langle f_{\mathfrak{B}}, f_j\rangle} = \left\langle f_j, \dfrac{f_{\mathfrak{A}}}{f_{\mathfrak{B}}}\right\rangle = \langle f_j, \varphi\rangle$. Из (10) получаем, таким образом,

$$X\big((\varphi)\big) = \prod_{j=1}^{n} \overline{\chi}_{d_j}^{k_j}(\langle f_j, \varphi\rangle)\, \chi_{d_1}^{k_1} \dots \chi_{d_n}^{k_n}(\langle f_0, \varphi\rangle) \tag{11}$$

при условиях $\big((\varphi), \mathfrak{M}\big) = 1$, $\varphi(\infty) = 1$, где $\langle f_j, \varphi\rangle = \prod\limits_{\xi(f_j)} \varphi(\xi)$ для $j = 0, 1, \dots, n$ и произведение берется по всем нулям ξ полинома f_j с их кратностями. Полагая $\alpha_j = \dfrac{k_j}{d_j}$, можно при фиксированном порождающем элементе θ группы k^* считать, что

$$\chi_{d_j}^{k_j}(\theta) = \exp(2\pi i \alpha_j). \tag{12}$$

Тогда из условия леммы получим, что $\alpha = (\alpha_1, \dots, \alpha_n)$ — допустимая система. Далее, положим

$$f_j = P_{j1}^{\lambda_{j1}} \dots P_{jN_j}^{\lambda_{jN_j}}, \tag{13}$$

где P_{js} неприводимы над k, $0 \leqslant j \leqslant n$, $1 \leqslant s \leqslant N_j$. При некоторых целых b_{js} имеем

$$\delta_j = (\lambda_{j1}, \dots, \lambda_{jN_j}) = \sum_{s=1}^{N_j} \lambda_{js} b_{js}. \tag{14}$$

С другой стороны, при некоторых целых $x_0, \dots, x_n$

$$r_a = \Big(\alpha_1\delta_1, \dots, \alpha_n\delta_n, \delta_0 \sum_j \alpha_j\Big) = x_1\alpha_1\delta_1 + \dots + x_n\alpha_n\delta_n - x_0\delta_0 \sum_{j=1}^{n} \alpha_j.$$

Отсюда, из (14) и (5) получаем, что при целых $a_{js} = x_j b_{js}$

$$r_a = \sum_{j=1}^{n} \alpha_j \Big(\sum_{s=1}^{N_j} \lambda_{js} a_{js} - \sum_{s=1}^{N_0} \lambda_{0s} a_{0s}\Big) \not\equiv 0 \pmod 1. \tag{15}$$

Существуют полиномы $\varphi_{js} \in k(x)$, для которых

$$\langle P_{js}, \varphi_{js}\rangle = \theta^{-a_{js}}, \quad 0 \leqslant j \leqslant n,\ 1 \leqslant s \leqslant N_j. \tag{16}$$

В самом деле, если вообще P — неприводимый над k полином, то для $f \in k[x]$ на $\langle P, f\rangle$ можно смотреть как на норму элемента $\bar{f}$ из поля $k' = k[x]/(p)$ в k, но норменное отображение $N\colon k' \to k$ является отображением на k. Определим теперь какой-нибудь полином φ_0 из системы сравнений

$$\varphi_0 \equiv \varphi_{js} \pmod{P_{js}}, \quad 0 \leqslant j \leqslant n,\ 0 \leqslant s \leqslant N_j. \tag{17}$$

Эта система разрешима, ибо в силу условия 1) теоремы P_{js} суть попарно различные неприводимые многочлены. Наконец, выберем число N столь большим, чтобы $\deg(f_0 \dots f_n)^N > \deg\varphi_0$, и положим

$$\varphi = \frac{\varphi_0 + c(f_0 \dots f_n)^N}{1 + c(f_0 \dots f_n)^N}, \tag{18}$$

где константа $c \in k$ выбирается так, чтобы старший коэффициент полинома $c(f_0 \dots f_n)^N$ был равен 1. Тогда в силу (17) φ не содержит в каноническом разложении множителей P_{js}. Следовательно, φ удовлетворяет первому из требований (9), по построению $\varphi(\infty) = 1$ и поэтому $X\big((\varphi)\big)$ можно вычислить по формуле (11). Из (18) имеем $\langle f_j, \varphi\rangle = \langle f_j, \varphi_0\rangle$. Используя последовательно (13), (17) и (16) получаем

$$\langle f_j, \varphi\rangle = \theta^{-\sum_{s=1}^{N_j} \lambda_{js} a_{js}}, \quad 0 \leqslant j \leqslant n,\ 1 \leqslant s \leqslant N_j. \tag{19}$$

Из (19), (12) и (11) находим

$$X\big((\varphi)\big) = \exp\left(2\pi i\Big[\sum_{j=1}^{n} \alpha_j \Big(\sum_{s=1}^{N_j} \lambda_{js} a_{js} - \sum_{s=1}^{N_0} \lambda_{0s} a_{0s}\Big)\Big]\right) = \exp(2\pi i r_a).$$

Формула (15) показывает, что $X\big((\varphi)\big) \neq 1$ и выполнено второе из условий (9). Лемма полностью доказана.

Доказательство теоремы.

$$N_F(p) = \sum_x \sum_{x_1} \dots \sum_{x_n} \frac{1}{p} \sum_t e\big(tF(x, x_1, \dots, x_n)\big) = p^n + R, \tag{20}$$

где

$$R = \frac{1}{p} \sum_t{}' \sum_x \sum_{x_1} \dots \sum_{x_n} e\big(tF(x, x_1, \dots, x_n)\big).$$

Из (1) находим

$$R = \frac{1}{p} \sum_t{}' \sum_x e\big(tf_0(x)\big) \sum_{x_1} e\big(tf_1(x)x_1^{m_1}\big) \dots \sum_{x_n} e\big(tf_n(x)x_n^{m_n}\big).$$

Обозначим через $\sum_x^{(1)}$ суммирование по тем x, для которых $f_j(x) \neq 0$ при $j = 0, 1, \ldots, n$ и через $\sum_{x}^{(j)}$ суммирование по нулям функции $f_j(x)$, лежащим в k. Тогда в силу условия (1) получим

$$R = R^{(1)} + \sum_{j=0}^{n} R_j. \tag{21}$$

$R^{(1)}$ вычислим, пользуясь леммой 3.

$$R^{(1)} = \frac{1}{p} \sum_t{}' \sum_x^{(1)} e\big(tf_0(x)\big) \sum_{k_1=0}^{d_1-1} \overline{\chi}_{d_1}^{k_1}\big(tf_1(x)\big) g\big(\chi_{d_1}^{k_1}\big) \ldots \sum_{k_n=0}^{d_n-1} \overline{\chi}_{d_n}^{k_n}\big(tf_n(x)\big) g\big(\chi_{d_n}^{k_n}\big) =$$

$$= \frac{1}{p} \sum_{k_1=0}^{d_1-1} \ldots \sum_{k_n=0}^{d_n-1} g\big(\chi_{d_1}^{k_1}\big) \ldots g\big(\chi_{d_n}^{k_n}\big) \sum_x^{(1)} \overline{\chi}_{d_1}^{k_1}\big(f_1(x)\big) \ldots \overline{\chi}_{d_n}^{k_n}\big(f_n(x)\big) \times$$

$$\times \sum_t{}' \overline{\chi}_{d_1}^{k_1} \ldots \overline{\chi}_{d_n}^{k_n}(t)\, e\big(tf_0(x)\big).$$

Слагаемое, отвечающее набору $k_1, \ldots, k_n$, в котором хоть одно $k_j = 0$, равно 0 по лемме 1. Следовательно, мы можем предполагать, что все $d_j \geqslant 2$ и $k_j \geqslant 1$. Если для взятого набора $\overline{\chi}_{d_1}^{k_1} \ldots \overline{\chi}_{d_n}^{k_n} = \chi_0$, то внутренняя сумма по t равна -1 и в силу леммы 1 модуль слагаемого $\leqslant p^{n/2}$. Если $\overline{\chi}_{d_1}^{k_1} \ldots \overline{\chi}_{d_n}^{k_n} \neq \chi_0$, то по лемме 2 сумма по t равна

$$\chi_{d_1}^{k_1} \ldots \chi_{d_n}^{k_n}\big(f_0(x)\big)\, g\big(\overline{\chi}_{d_1}^{k_1} \ldots \overline{\chi}_{d_n}^{k_n}\big).$$

Рассматриваемое слагаемое равно тогда

$$\frac{1}{p} g\big(\chi_{d_1}^{k_1}\big) \ldots g\big(\chi_{d_n}^{k_n}\big) g\big(\overline{\chi}_{d_1}^{k_1} \ldots \overline{\chi}_{d_n}^{k_n}\big) \sum_x^{(1)} \overline{\chi}_{d_1}^{k_1}\big(f_1(x)\big) \ldots \overline{\chi}_{d_n}^{k_n}\big(f_n(x)\big) \chi_{d_1}^{k_1} \ldots \chi_{d_n}^{k_n}\big(f_0(x)\big);$$

по основной лемме сумма по x равна $O(\sqrt{p})$, а все произведение — $O(p^{n/2})$. Следовательно

$$R^{(1)} = O(p^{n/2}). \tag{22}$$

$$R_0 = \frac{1}{p} \sum_t{}' \sum_{x\,(0)} \sum_{k_1=0}^{d_1-1} \overline{\chi}_{d_1}^{k_1}\big(tf_1(x)\big) g\big(\chi_{d_1}^{k_1}\big) \ldots \sum_{k_n=0}^{d_n-1} \overline{\chi}_{d_n}^{k_n}\big(tf_n(x)\big) g\big(\chi_{d_n}^{k_n}\big) =$$

$$= \frac{1}{p} \sum_{k_1=0}^{d_1-1} \ldots \sum_{k_n=0}^{d_n-1} g\big(\chi_{d_1}^{k_1}\big) \ldots g\big(\chi_{d_n}^{k_n}\big) \sum_{x\,(0)} \overline{\chi}_{d_1}^{k_1}\big(f_1(x)\big) \ldots \overline{\chi}_{d_n}^{k_n}\big(f_n(x)\big) \sum_t{}' \overline{\chi}_{d_1}^{k_1} \ldots \overline{\chi}_{d_n}^{k_n}(t).$$

Мы снова можем считать $d_j \geqslant 2$ и $k_j \geqslant 1$, причем нужно рассматривать лишь случай $\overline{\chi}_{d_1}^{k_1} \ldots \overline{\chi}_{d_n}^{k_n} = \chi_0$. Так как в сумме $\sum_{x\,(0)}$ x пробегает $O(1)$ значений, легко получаем $R_0 = O(p^{n/2})$, $R_1, \ldots, R_n$ оцениваются одинаково. Оценим R_1

$$R_1 = \frac{1}{p} \sum_t{}' \sum_{x\,(1)} e\big(tf_0(x)\big) p \sum_{k_2=0}^{d_2-1} \overline{\chi}_{d_2}^{k_2}\big(tf_2(x)\big) g\big(\chi_{d_2}^{k_2}\big) \ldots \sum_{k_n=0}^{d_n-1} \overline{\chi}_{d_n}^{k_n}\big(tf_n(x)\big) g\big(\chi_{d_n}^{k_n}\big) =$$

$$= \sum_{k_2=1}^{d_2-1} \ldots \sum_{k_n=1}^{d_n-1} g\big(\chi_{d_2}^{k_2}\big) \ldots g\big(\chi_{d_n}^{k_n}\big) \sum_{x\,(1)} \overline{\chi}_{d_2}^{k_2}\big(f_2(x)\big) \ldots \overline{\chi}_{d_n}^{k_n}\big(f_n(x)\big) \times$$

$$\times \sum_t{}' \overline{\chi}_{d_2}^{k_2} \ldots \overline{\chi}_{d_n}^{k_n}(t)\, e\big(tf_0(x)\big).$$

Если $\overline{\chi}_{d_2}^{k_2} \ldots \chi_{d_n}^{k_n} = \chi_0$, то получаем $O(p^{(n-1)/2})$; в противном случае снова выносим множитель $g(\overline{\chi}_{d_2}^{k_2} \ldots \overline{\chi}_{d_n}^{k_n})$ и получаем $O(p^{n/2})$.

Таким образом, $R_j = O(p^{n/2})$ для $j = 0, 1, \ldots, n$ что вместе с (22), (21) и (20) завершает доказательство.

В заключение сделаем два замечания относительно возможностей метода работы [2].

1) К уравнению

$$f_0(x) + f_1(x) x_1^{m_1} + \ldots + f_n(x) x_n^{m_n} = 0 \tag{23}$$

могут быть приведены посредством бирациональных преобразований некоторые другие типы уравнений, что дает информацию о количестве решений последних. Рассмотрим например уравнение

$$y^3 = \big(t - \alpha_1(x)\big)\big(t^2 + \alpha_2(x) t + \alpha_3(x)\big),$$

где $\alpha_1(x)$, $\alpha_2(x)$, $\alpha_3(x)$ — полиномы. Замена переменных

$$x_1 = \frac{1}{t - \alpha_1(x)} + \alpha_4(x), \qquad x_2 = \frac{y}{t - \alpha_1(x)},$$

где $\alpha_4(x)$ некоторая рациональная функция, с допустимой погрешностью $O(p)$ приводит уравнение к виду

$$f_0(x) + f_1(x) x_1^2 - f_1(x) x_2^3 = 0.$$

2) Обратим внимание на то, что с помощью оценок сумм характеров вдоль кривой в работе Морделла [1] трактуется уравнение

$$x_2^2 - x_1^3 f_1(x) - x_1 f_2(x) = 0.$$

Цитированная литература

[1] L. J. Mordell, *On a cubic congruence in three variables, II*, Proc. Amer. Math. Soc. 14 (4) (1963), стр. 609–614.

[2] Г. И. Перельмутер, *Оценка суммы вдоль алгебраической кривой*, Математические заметки 5, вып. 3, (1969), стр. 373–380.

[3] A. Weil, *Number of solutions of equations in finite fields*, Bull. Amer. Math. Soc. 55 (5) (1949), стр. 497–508.

Получено 5. 4. 1971 (157)

ACTA ARITHMETICA
XXI (1972)

Two combinatorial problems in group theory

by

R. B. Eggleton and P. Erdös (Calgary, Alberta)

Abstract. Sequences of elements from (additive) abelian groups are studied. Conditions under which a nonempty subsequence has sum equal to the group identity 0 are established. For example, an n-sequence with exactly k distinct terms represents 0 if the group has order $g \leqslant n + \binom{k}{2}$ and $n \geqslant k\binom{k}{2}$.

The least number $f(k)$ of distinct partial sums is also considered, for the case of k-sequences of distinct elements such that no nonempty partial sum is equal to 0. For example, $2k-1 \leqslant f(k) \leqslant [\frac{1}{2}k^2]+1$.

In this paper a *sequence* is a selection of members of a set, possibly with repetitions, in which order is not important; *elements* are members of sets, and *terms* are members of sequences.

Definition. Let $*$ be a binary operation on a set A, and let $S = (a_i)_{i=1}^n$ be a sequence of elements from A. S will be said to *represent* the element $x \in A$ if

(i) x is a term in S, or

(ii) there exist $y, z \in A$ such that $x = y * z$, and y and z are represented by disjoint subsequences of S.

(Clearly this notion extends to general algebras.)

In particular, if $\langle G, + \rangle$ is an abelian group and $S = (a_i)_{i=1}^n$ is a sequence of elements from G, then S represents $x \in G$ just if there exists a sequence $E = (\varepsilon_i)_{i=1}^n$ of elements from $\{0, 1\}$, not all 0, such that $\sum_{i=1}^{n} \varepsilon_i a_i = x$.

We resolve here some aspects of the following two related problems.

(1) Under what circumstances does an n-sequence of elements from an abelian group represent the zero element?

(2) If an n-sequence of distinct elements from an abelian group does not represent the zero element, how many elements does it represent?