ACTA ARITHMETICA
XXI (1972)

О полных системах сравнений

Н. М. Коробов (Москва)

В этой работе изучается вопрос о числе решений системы сравнений

$$(1)\qquad \begin{array}{l} x_1+\ldots+x_k \equiv \lambda_1 \pmod{q_1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x_1^n+\ldots+x_k^n \equiv \lambda_n \pmod{q_n}. \end{array}$$

Здесь $\lambda_1, \ldots, \lambda_n$ — произвольные целые, $k \geqslant n \geqslant 2$ и переменные $x_1, \ldots, x_k$ пробегают полные системы вычетов по модулю $q = \text{ОНК}(q_1, \ldots, q_n)$. При этом предполагается, что всякое простое p, делящее q, будет больше чем n и рассматриваются только такие наборы $x_1, \ldots, x_k$, в которых для каждого p можно найти n величин x_ν принадлежащих разным классам по модулю p. В дальнейшем для таких $x_1, \ldots, x_k$ будем пользоваться обозначением $(x_1, \ldots, x_k)_n \pmod q$, а систему (1) записывать в виде

$$\left.\begin{array}{l} x_1+\ldots+x_k \equiv \lambda_1 \pmod{q_1} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x_1^n+\ldots+x_k^n \equiv \lambda_n \pmod{q_n} \end{array}\right\}; \qquad (x_1, \ldots, x_k)_n \pmod q.$$

При $q_\nu = p^\nu$ $(\nu = 1, 2, \ldots, n)$ и $k = n$ оценка числа решений системы (1) была указана Ю. В. Линником [3] (см. также [1] и [2]). В настоящей работе при произвольном выборе модулей q_ν и любом $k \geqslant n$ получены явные формулы, позволяющие выразить число решений системы (1) через число решений систем вида

$$\left.\begin{array}{l} x_1^{m_1}+\ldots+x_k^{m_1} \equiv \lambda_{m_1} \\ \ldots\ldots\ldots\ldots\ldots \\ x_1^{m_r}+\ldots+x_k^{m_r} \equiv \lambda_{m_r} \end{array}\right\} \pmod p; \qquad (x_1, \ldots, x_k)_n \pmod p$$

где p — простой делитель q и $1 \leqslant m_1 < \ldots < m_r \leqslant n$. Из этих формул при $k = n$ и соответствующем выборе модулей $q_1, \ldots, q_n$ следуют в частности оценки, полученные в работах [1]–[3].

Введем некоторые обозначения. Через $T_k(\lambda_1, \ldots, \lambda_n; q)$ будем обозначать число решений системы

$$\left.\begin{array}{l} x_1+\ldots+x_k \equiv \lambda_1 \\ \cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot \\ x_1^n+\ldots+x_k^n \equiv \lambda_n \end{array}\right\} \pmod q; \qquad (x_1, \ldots, x_k)_n \pmod q.$$

Пусть, далее, для любого целого m величина $\delta_q(m)$ определена равенством

$$\delta_q(m) = \begin{cases} 1 & \text{если} \quad q \mid m, \\ 0 & \text{если} \quad q \nmid m. \end{cases}$$

Легко видеть, что тогда

$$\sum_{x=1}^{q} e^{2\pi i \frac{mx}{q}} = q\delta_q(m)$$

и, следовательно,

$$(2) \qquad T_k(\lambda_1, \ldots, \lambda_n; q) = \sum_{(x_1, \ldots, x_k)_n}^{q} \prod_{\nu=1}^{n} \delta_q(x_1^\nu+\ldots+x_k^\nu-\lambda_\nu) =$$
$$= \frac{1}{q^n} \sum_{a_1, \ldots, a_n=1}^{q} \sum_{(x_1, \ldots, x_k)_n}^{q} e^{2\pi i \frac{f(x_1)+\ldots+f(x_k)-(a_1\lambda_1+\ldots+a_n\lambda_n)}{q}},$$

где $\sum\limits_{(x_1,\ldots,x_k)_n}^{q}$ — сумма, распространенная на все системы вида $(x_1, \ldots, x_k)_n$ и $f(x) = a_1x+\ldots+a_nx^n$. Наконец, при любом натуральном α, через $S_\alpha[f(x)]$ будем обозначать тригонометрическую сумму

$$S_\alpha[f(x)] = \sum_{y=1}^{p^{\alpha-1}} e^{2\pi i \frac{f(x+py)}{p^\alpha}}.$$

Как показано в лемме 2, произведение таких сумм $S_\alpha[f(x_1)] \ldots \ldots S_\alpha[f(x_k)]$ можно точно вычислить для любого полинома $f(x)$ и любой системы $(x_1, \ldots, x_k)_n \pmod p$. На этом свойстве сумм $S_\alpha[f(x)]$ основывается, в конечном счете, вывод наиболее общих явных формул, полученных в теореме 3 для числа решений системы сравнений (1).

Лемма 1. *При простом $p > n$ в случае разрешимости системы*

$$(3) \qquad \left.\begin{array}{l} x_1+\ldots+x_n \equiv \lambda_1 \\ \cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot \\ x_1^n+\ldots+x_n^n \equiv \lambda_n \end{array}\right\} \pmod p; \qquad (x_1, \ldots, x_n)_n \pmod p$$

выполняется равенство

$$T_n(\lambda_1, \ldots, \lambda_n; p) = n!.$$

Доказательство. Так как система (3) по условию разрешима и $p > n$, то значения элементарных симметрических функций величин $x_1, \ldots, x_n$ можно выразить по модулю p через $\lambda_1, \ldots, \lambda_n$. Но тогда $x_1, \ldots, x_n$ будут совпадать с перестановками корней некоторого фиксированного сравнения. Все n корней этого сравнения, в силу условия $(x_1, \ldots, x_n)_n \pmod p$, различны. Следовательно число различных перестановок корней равно $n!$ и

$$T_n(\lambda_1, \ldots, \lambda_n; p) = n!.$$

Лемма 2. *Пусть $\alpha \geqslant 2$, $k \geqslant n \geqslant 2$, $f(x) = a_1x+\ldots+a_nx^n$, $d = (a_1, \ldots, a_n)$ и $p > n$ — простое. Тогда для величин $x_1, \ldots, x_k$, входящих в любую из систем $(x_1, \ldots, x_k)_n \pmod p$, выполняется равенство*

$$(4) \qquad \prod_{\nu=1}^{k} S_\alpha[f(x_\nu)] = \begin{cases} p^{(\alpha-1)k} e^{2\pi i \frac{f(x_1)+\ldots+f(x_k)}{p^\alpha}} & \textit{если} \quad p^{\alpha-1} \mid d, \\ 0 & \textit{если} \quad p^{\alpha-1} \nmid d. \end{cases}$$

Доказательство. Пользуясь равенством

$$\sum_{x=1}^{p} e^{2\pi i \frac{mx}{p}} = p\delta_p(m)$$

при любом целом $\alpha \geqslant 2$ получим

$$S_\alpha[f(x)] = \sum_{y=1}^{p^{\alpha-2}} \sum_{z=1}^{p} e^{2\pi i \frac{f(x+py+p^{\alpha-1}z)}{p^\alpha}} = \sum_{y=1}^{p^{\alpha-2}} \sum_{z=1}^{p} e^{2\pi i \frac{f(x+py)+f'(x)p^{\alpha-1}z}{p^\alpha}} =$$
$$= p\delta_p[f'(x)] \sum_{y=1}^{p^{\alpha-2}} e^{2\pi i \frac{f(x+py)}{p^\alpha}}.$$

Но тогда, очевидно,

$$\prod_{\nu=1}^{k} S_\alpha[f(x_\nu)] = p^k \prod_{\nu=1}^{k} \delta_p[f'(x_\nu)] \sum_{y_\nu=1}^{p^{\alpha-2}} e^{2\pi i \frac{f(x_\nu+py_\nu)}{p^\alpha}}.$$

Так как, по условию, не меньше чем n из величин $x_1, \ldots, x_k$ принадлежат различным классам по модулю p, то

$$\prod_{\nu=1}^{k} \delta_p[f'(x_\nu)] = \begin{cases} 1 & \text{если} \quad p \mid d, \\ 0 & \text{если} \quad p \nmid d, \end{cases}$$

где d — общий наибольший делитель коэффициентов многочлена $f(x)$. Отсюда следует, что

$$\prod_{\nu=1}^{k} S_\alpha[f(x_\nu)] = \begin{cases} p^k \prod\limits_{\nu=1}^{k} \sum\limits_{y_\nu=1}^{p^{\alpha-2}} e^{2\pi i \frac{f(x_\nu+py_\nu)}{p^\alpha}} & \text{если} \quad p \mid d, \\ 0 & \text{если} \quad p \nmid d. \end{cases}$$

Пусть $p^j | d$ и при $j = 1, 2, \ldots, \alpha-1$ целочисленные полиномы $f_j(x)$ определены равенством $f(x) = p^j f_j(x)$. Тогда, замечая, что при $p|d$

$$\sum_{y_\nu=1}^{p^{\alpha-2}} e^{2\pi i \frac{f(x_\nu+py_\nu)}{p^\alpha}} = \sum_{y_\nu=1}^{p^{\alpha-2}} e^{2\pi i \frac{f_1(x_\nu+py_\nu)}{p^{\alpha-1}}} = S_{\alpha-1}[f_1(x_\nu)],$$

получим

$$\prod_{\nu=1}^{k} S_\alpha[f(x_\nu)] = \begin{cases} p^k \prod\limits_{\nu=1}^{k} S_{\alpha-1}[f_1(x_\nu)] & \text{если} \quad p|d, \\ 0 & \text{если} \quad p\nmid d. \end{cases}$$

Отсюда, после $\alpha-2$ кратного применения этого равенства, следует что

$$\prod_{\nu=1}^{k} S_\alpha[f(x_\nu)] = \begin{cases} p^{(\alpha-1)k} \prod\limits_{\nu=1}^{k} S_1[f_{\alpha-1}(x_\nu)] & \text{если} \quad p^{\alpha-1}|d, \\ 0 & \text{если} \quad p^{\alpha-1}\nmid d. \end{cases} \tag{5}$$

Но, по определению,

$$S_1[f_{\alpha-1}(x_\nu)] = e^{2\pi i \frac{f_{\alpha-1}(x_\nu)}{p}} = e^{2\pi i \frac{f(x_\nu)}{p^\alpha}}$$

и, следовательно, равенство (5) совпадает с утверждением леммы:

$$\prod_{\nu=1}^{k} S_\alpha[f(x_\nu)] = \begin{cases} p^{(\alpha-1)k} \prod\limits_{\nu=1}^{k} e^{2\pi i \frac{f(x_\nu)}{p^\alpha}} & \text{если} \quad p^{\alpha-1}|d, \\ 0 & \text{если} \quad p^{\alpha-1}\nmid d. \end{cases}$$

Теорема 1. *Пусть $k \geqslant n \geqslant 2$ и $p > n$ — простое. Тогда при любом $\alpha \geqslant 1$ для числа решений системы сравнений*

$$\left.\begin{array}{l} x_1+\ldots+x_k \equiv \lambda_1 \\ \ldots\ldots\ldots\ldots \\ x_1^n+\ldots+x_k^n \equiv \lambda_n \end{array}\right\} \pmod{p^\alpha}; \qquad (x_1, \ldots, x_k)_n \pmod{p^\alpha},$$

справедливо равенство

$$T_k(\lambda_1, \ldots, \lambda_n; p^\alpha) = p^{(\alpha-1)(k-n)} T_k(\lambda_1, \ldots, \lambda_n; p).$$

Доказательство. Пусть $f(x) = a_1x+\ldots+a_nx^n$. Тогда, согласно (2),

$$T_k(\lambda_1, \ldots, \lambda_n; p^\alpha) = \frac{1}{p^{\alpha n}} \sum_{a_1,\ldots,a_n=1}^{p^\alpha} \sum_{(x_1,\ldots,x_k)_n}^{p^\alpha} e^{2\pi i \frac{f(x_1)+\ldots+f(x_k)-(a_1\lambda_1+\ldots+a_n\lambda_n)}{p^\alpha}}.$$

Отсюда, пользуясь тем, что

$$\sum_{(x_1,\ldots,x_k)_n}^{p^\alpha} e^{2\pi i \frac{f(x_1)+\ldots+f(x_k)}{p^\alpha}} = \sum_{(x_1,\ldots,x_k)_n}^{p} \prod_{\nu=1}^{k} \sum_{y_\nu=1}^{p^{\alpha-1}} e^{2\pi i \frac{f(x_\nu+py_\nu)}{p^\alpha}} = \sum_{(x_1,\ldots,x_k)_n}^{p} \prod_{\nu=1}^{k} S_\alpha[f(x_\nu)],$$

получим

$$T_k(\lambda_1, \ldots, \lambda_n; p^\alpha) = \frac{1}{p^{\alpha n}} \sum_{a_1,\ldots,a_n=1}^{p^\alpha} e^{-2\pi i \frac{a_1\lambda_1+\ldots+a_n\lambda_n}{p^\alpha}} \sum_{(x_1,\ldots,x_k)_n}^{p} \prod_{\nu=1}^{k} S_\alpha[f(x_\nu)].$$

Так как при $\alpha=1$ утверждение теоремы очевидно, то будем предполагать, что $\alpha \geqslant 2$. Согласно лемме 2 при $\alpha \geqslant 2$ произведение $\prod\limits_{\nu=1}^{k} S_\alpha[f(x_\nu)]$ отлично от нуля только при условии $p^{\alpha-1}|d$, где $d = (a_1, \ldots, a_n)$. Следовательно, полагая $a_\nu = p^{\alpha-1}b_\nu$ при $\varphi(x) = b_1x+\ldots+b_nx^n$ получим

$$T_k(\lambda_1, \ldots, \lambda_n; p^\alpha) = \frac{1}{p^{\alpha n}} \sum_{b_1,\ldots,b_n=1}^{p} e^{-2\pi i \frac{\lambda_1b_1+\ldots+\lambda_nb_n}{p}} \sum_{(x_1,\ldots,x_k)_n}^{p} \prod_{\nu=1}^{k} S_\alpha[f(x_\nu)], \tag{6}$$

где в силу (4)

$$\sum_{(x_1,\ldots,x_k)_n}^{p} \prod_{\nu=1}^{k} S_\alpha[f(x_\nu)] = p^{(\alpha-1)k} \sum_{(x_1,\ldots,x_k)_n}^{p} e^{2\pi i \frac{f(x_1)+\ldots+f(x_k)}{p^\alpha}} =$$
$$= p^{(\alpha-1)k} \sum_{(x_1,\ldots,x_k)_n}^{p} e^{2\pi i \frac{\varphi(x_1)+\ldots+\varphi(x_k)}{p}}.$$

Подставляя это выражение в (6) получаем утверждение теоремы:

$$T_k(\lambda_1, \ldots, \lambda_n; p^\alpha) =$$
$$= \frac{p^{(\alpha-1)(k-n)}}{p^n} \sum_{b_1,\ldots,b_n=1}^{p} \sum_{(x_1,\ldots,x_k)_n}^{p} e^{2\pi i \frac{\varphi(x_1)+\ldots+\varphi(x_k)-(b_1\lambda_1+\ldots+b_n\lambda_n)}{p}} =$$
$$= p^{(\alpha-1)(k-n)} T_k(\lambda_1, \ldots, \lambda_n; p).$$

Следствие. *Пусть $n \geqslant 2$ и $p > n$ — простое. Тогда разрешимость системы*

$$\left.\begin{array}{l} x_1+\ldots+x_n \equiv \lambda_1 \\ \ldots\ldots\ldots\ldots \\ x_1^n+\ldots+x_n^n \equiv \lambda_n \end{array}\right\} \pmod{p^\alpha}; \qquad (x_1, \ldots, x_n)_n \pmod{p^\alpha}$$

при $\alpha=1$ является необходимым и достаточным условием разрешимости при любом $\alpha > 1$; в случае разрешимости число ее решений при любом α равно $n!$.

Действительно, полагая в теореме 1 $k = n$, получим

$$T_n(\lambda_1, \ldots, \lambda_n; p^\alpha) = T_n(\lambda_1, \ldots, \lambda_n; p).$$

Отсюда, пользуясь леммой 1, получаем утверждение следствия.

Теорема 2. *Пусть $k \geqslant n \geqslant 2$, $q = p_1^{a_1} \ldots p_s^{a_s}$ — каноническое разложение q на простые множители и $p_j > n$ $(j = 1, 2, \ldots, s)$. Тогда для числа решений системы сравнений*

$$\left.\begin{array}{l} x_1 + \ldots + x_k \equiv \lambda_1 \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ x_1^n + \ldots + x_k^n \equiv \lambda_n \end{array}\right\} \pmod q; \qquad (x_1, \ldots, x_k)_n \pmod q$$

справедливы равенства

$$T_k(\lambda_1, \ldots, \lambda_n; q) = \prod_{j=1}^{s} T_k(\lambda_1, \ldots, \lambda_n; p_j^{a_j}),$$

$$T_k(\lambda_1, \ldots, \lambda_n; q) = \left(\frac{q}{p_1 \ldots p_s}\right)^{k-n} \prod_{j=1}^{s} T_k(\lambda_1, \ldots, \lambda_n; p_j).$$

Доказательство. Заметим прежде всего, что при взаимно простых q' и q'' переменные $x_1, \ldots, x_k$ пробегают все системы $(x_1, \ldots, x_k)_n$ $(\mathrm{mod}\ q'q'')$ тогда и только тогда, когда переменные $y_1, \ldots, y_k$ и $z_1, \ldots, z_k$, определенные условиями

$$x_i \equiv q''y_i + q'z_i \pmod{q'q''}, \qquad 1 \leqslant y_i \leqslant q',\ 1 \leqslant z_i \leqslant q'' \ (i = 1, 2, \ldots, k),$$

пробегают соответственно все системы $(y_1, \ldots, y_k)_n \pmod{q'}$ и $(z_1, \ldots, z_k)_n$ $(\mathrm{mod}\ q'')$.

Так как, очевидно, при $1 \leqslant i \leqslant k$ и $1 \leqslant \nu \leqslant n$

$$x_i^\nu \equiv (q''y_i)^\nu + (q'z_i)^\nu \pmod{q'q''},$$

то число решений системы

$$x_1^\nu + \ldots + x_k^\nu \equiv \lambda_\nu \pmod{q'q''} \qquad (\nu = 1, 2, \ldots, n) \tag{7}$$

с переменными вида $(x_1, \ldots, x_k)_n \pmod{q'q''}$ равно числу решений системы

$$(q''y_1)^\nu + \ldots + (q''y_k)^\nu + (q'z_1)^\nu + \ldots + (q'z_k)^\nu \equiv \lambda_\nu \pmod{q'q''} \qquad (\nu = 1, 2, \ldots, n) \tag{8}$$

с переменными вида $(y_1, \ldots, y_k)_n \pmod{q'}$ и $(z_1, \ldots, z_k)_n \pmod{q''}$. Но система (8) равносильна системе

$$\begin{array}{ll} (q''y_1)^\nu + \ldots + (q''y_k)^\nu \equiv \lambda_\nu \pmod{q'}; & (y_1, \ldots, y_k)_n \pmod{q'}, \\ (q'z_1)^\nu + \ldots + (q'z_k)^\nu \equiv \lambda_\nu \pmod{q''}; & (z_1, \ldots, z_k)_n \pmod{q''} \end{array}$$
$$(\nu = 1, 2, \ldots, n).$$

Наконец число решений этой системы равно числу решений системы

$$\begin{array}{ll} y_1^\nu + \ldots + y_k^\nu \equiv \lambda_\nu \pmod{q'}; & (y_1, \ldots, y_k)_n \pmod{q'}, \\ z_1^\nu + \ldots + z_k^\nu \equiv \lambda_\nu \pmod{q''}; & (z_1, \ldots, z_k)_n \pmod{q''} \end{array} \tag{9}$$
$$(\nu = 1, 2, \ldots, n).$$

Отсюда видно, что системы (7) и (9) имеют одинаковое число решений и, следовательно,

$$T_k(\lambda_1, \ldots, \lambda_n; q'q'') = T_k(\lambda_1, \ldots, \lambda_n; q')\, T_k(\lambda_1, \ldots, \lambda_n; q'').$$

Последовательное применение этого равенства приводит к первому утверждению теоремы:

$$T_k(\lambda_1, \ldots, \lambda_n; q) = \prod_{j=1}^{s} T_k(\lambda_1, \ldots, \lambda_n; p_j^{a_j}).$$

Второе утверждение теоремы получается отсюда с помощью теоремы 1:

$$T_k(\lambda_1, \ldots, \lambda_n; q) = \prod_{j=1}^{s} p_j^{(a_j-1)(k-n)} T_k(\lambda_1, \ldots, \lambda_n; p_j) = \left(\frac{q}{p_1 \ldots p_s}\right)^{k-n} \prod_{j=1}^{s} T_k(\lambda_1, \ldots, \lambda_n; p_j).$$

Следствие. *Пусть $k \geqslant n \geqslant 2$, $q = p_1^{a_1} \ldots p_s^{a_s}$ — каноническое разложение q на простые множители и $p_j > n$ $(j = 1, 2, \ldots, s)$. Система*

$$\left.\begin{array}{l} x_1 + \ldots + x_n \equiv \lambda_1 \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ x_1^n + \ldots + x_n^n \equiv \lambda_n \end{array}\right\} \pmod q; \qquad (x_1, \ldots, x_n)_n \pmod q \tag{10}$$

разрешима тогда и только тогда, когда система

$$\left.\begin{array}{l} x_1 + \ldots + x_n \equiv \lambda_1 \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ x_1^n + \ldots + x_n^n \equiv \lambda_n \end{array}\right\} \pmod{p_j}; \qquad (x_1, \ldots, x_n)_n \pmod{p_j}$$

разрешима для каждого p_j $(j = 1, 2, \ldots, s)$. В случае разрешимости для числа решений системы (10) *выполняется равенство*

$$T_n(\lambda_1, \ldots, \lambda_n; q) = n^s.$$

Действительно, полагая в теореме 2 $k = n$, получим

$$T_n(\lambda_1, \ldots, \lambda_n; q) = \prod_{j=1}^{s} T_n(\lambda_1, \ldots, \lambda_n; p_j).$$

Отсюда, пользуясь леммой 1, получаем утверждение следствия.

Обозначим через T_k число решений системы сравнений

$$(11)\qquad \left.\begin{array}{l} x_1+\ldots+x_k \equiv \lambda_1 \,(\mathrm{mod}\, q_1)\\ \ldots\ldots\ldots\ldots\ldots\ldots\\ x_1^n+\ldots+x_k^n \equiv \lambda_n \,(\mathrm{mod}\, q_n)\end{array}\right\}; \qquad (x_1, \ldots, x_k)_n \,(\mathrm{mod}\, q),$$

где $k \geqslant n \geqslant 2$, $q = \text{ОНК}\,(q_1, \ldots, q_n) = p_1^{a_1} \ldots p_s^{a_s}$ и $p_j > n$ $(j = 1, 2, \ldots \ldots, s)$. Пусть, далее, $T_k(p_j)$ — число решений системы

$$(12)\qquad \left.\begin{array}{l} x_1+\ldots+x_k \equiv \lambda_1 \,(\mathrm{mod}\, p_j^{\tau_{1j}})\\ \ldots\ldots\ldots\ldots\ldots\ldots\\ x_1^n+\ldots+x_k^n \equiv \lambda_n \,(\mathrm{mod}\, p_j^{\tau_{nj}})\end{array}\right\}; \qquad (x_1, \ldots, x_k)_n \,(\mathrm{mod}\, p_j),$$

где величины τ_{ij} определены равенствами

$$\tau_{ij} = \begin{cases} 1 & \text{если} \quad p_j \mid q_i, \\ 0 & \text{если} \quad p_j \nmid q_i, \end{cases} \qquad (1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant s).$$

Обозначим через r_j число тех из величин $q_1, \ldots, q_n$, которые не кратны p_j. Тогда r_j из величин $\tau_{1j}, \ldots, \tau_{nj}$ равны нулю и, следовательно, система (12) состоит из $n - r_j$ сравнений по модулю p_j.

Теорема 3. *Для числа решений системы* (11) *выполняются соотношения*

$$T_k = \frac{q^k T_k(p_1) \ldots T_k(p_s)}{q_1 \ldots q_n p_1^{k-n+r_1} \ldots p_s^{k-n+r_s}}, \qquad T_k \leqslant (n!)^s q^k (q_1 \ldots q_n)^{-1}.$$

Доказательство. Обозначим через W_k число решений системы сравнений

$$(13)\qquad \left.\begin{array}{l} x_1+\ldots+x_k \equiv \lambda_1 + q_1 z_1\\ \ldots\ldots\ldots\ldots\ldots\\ x_1^n+\ldots+x_k^n \equiv \lambda_n + q_n z_n\end{array}\right\} (\mathrm{mod}\, q); \qquad (x_1, \ldots, x_k)_n \,(\mathrm{mod}\, q),$$

где переменные $z_1, \ldots, z_n$ пробегают полные системы вычетов по модулю q. Так как, очевидно,

$$W_k = \sum_{z_1, \ldots, z_n = 1}^{q} T_k(\lambda_1 + q_1 z_1, \ldots, \lambda_n + q_n z_n; q),$$

то, пользуясь теоремой 2, получим

$$(14)\qquad W_k = \left(\frac{q}{p_1 \ldots p_s}\right)^{k-n} \sum_{z_1, \ldots, z_n = 1}^{q} \prod_{j=1}^{s} T_k(\lambda_1 + q_1 z_1, \ldots, \lambda_n + q_n z_n; p_j) =$$
$$= \left(\frac{q}{p_1 \ldots p_s}\right)^{k} \sum_{z_1, \ldots, z_s = 1}^{p_1 \ldots p_s} \prod_{j=1}^{s} T_k(\lambda_1 + q_1 z_1, \ldots, \lambda_n + q_n z_n; p_j).$$

Определим величины p_j' и переменные z_{ij} с помощью условий

$$p_1 \ldots p_s = p_j p_j' \qquad (1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant s),$$
$$z_i \equiv p_1' z_{i1} + \ldots + p_s' z_{is} \,(\mathrm{mod}\, p_1 \ldots p_s), \qquad 1 \leqslant z_{ij} \leqslant p_j.$$

Так как при этом $z_i \equiv p_j' z_{ij} \,(\mathrm{mod}\, p_j)$, то из (14) получим

$$(15)\qquad W_k = \left(\frac{q}{p_1 \ldots p_s}\right)^{k} \prod_{j=1}^{s} \sum_{z_{1j}, \ldots, z_{nj} = 1}^{p_j} T_k(\lambda_1 + q_1 p_j' z_{1j}, \ldots, \lambda_n + q_n p_j' z_{nj}; p_j) =$$
$$= \left(\frac{q}{p_1 \ldots p_s}\right)^{k} \prod_{j=1}^{s} p_j^{n-r_j} T_k(p_j)$$

где $T_k(p_j)$ — число решений системы (12).

С другой стороны, записывая число решений системы (13) в виде

$$W_k = \sum_{(x_1, \ldots, x_k)_n}^{q} \sum_{z_1, \ldots, z_n = 1}^{q} \prod_{\nu=1}^{n} \delta_q(x_1^\nu + \ldots + x_k^\nu - \lambda_\nu - q_\nu z_\nu) =$$
$$= \sum_{(x_1, \ldots, x_k)_n}^{q} \prod_{\nu=1}^{n} \sum_{z_\nu = 1}^{q} \delta_q(x_1^\nu + \ldots + x_k^\nu - \lambda_\nu - q_\nu z_\nu),$$

и замечая, что

$$\sum_{z_\nu = 1}^{q} \delta_q(x_1^\nu + \ldots + x_k^\nu - \lambda_\nu - q_\nu z_\nu) = q_\nu \delta_{q_\nu}(x_1^\nu + \ldots + x_k^\nu - \lambda_\nu),$$

получим

$$(16)\qquad W_k = \sum_{(x_1, \ldots, x_k)_n}^{q} \prod_{\nu=1}^{n} q_\nu \delta_{q_\nu}(x_1^\nu + \ldots + x_k^\nu - \lambda_\nu) = q_1 \ldots q_n T_k,$$

где T_k — число решений системы (11). Отсюда в силу (15) следует первое утверждение теоремы:

$$q_1 \ldots q_n T_k = \left(\frac{q}{p_1 \ldots p_s}\right)^{k} \prod_{j=1}^{s} p_j^{n-r_j} T_k(p_j),$$
$$T_k = \frac{q^k T_k(p_1) \ldots T_k(p_s)}{q_1 \ldots q_n p_1^{k-n+r_1} \ldots p_s^{k-n+r_s}}.$$

Наконец, пользуясь очевидной оценкой

$$T_k(\lambda_1, \ldots, \lambda_n; p) \leqslant n!\ p^{k-n}$$

из (15) и (16) получим второе утверждение теоремы:

$$W_k \leqslant \left(\frac{q}{p_1 \ldots p_s}\right)^{k} \prod_{j=1}^{s} \sum_{z_{1j}, \ldots, z_{nj} = 1}^{p_j} n!\ p_j^{k-n} = (n!)^s q^k,$$
$$T_k = W_k (q_1 \ldots q_n)^{-1} \leqslant (n!)^s q^k (q_1 \ldots q_n)^{-1}.$$

Замечание. Пусть $p > n$ — простое. Выбирая в теореме 3 $k = n$ и $q_\nu = p^\nu$ $(\nu = 1, 2, \ldots, n)$ для числа решений системы

$$\left.\begin{array}{l} x_1 + \ldots + x_n \equiv \lambda_1 \pmod{p} \\ \cdots\cdots\cdots\cdots\cdots \\ x_1^n + \ldots + x_n^n \equiv \lambda_n \pmod{p^n} \end{array}\right\}; \qquad (x_1, \ldots, x_n)_n \pmod{p^n}$$

получим оценки из работ [3] и [1]:

$$T_n = p^{n(n-1)/2} T_n(\lambda_1, \ldots, \lambda_n; p) \leqslant n!\, p^{n(n-1)/2}.$$

Аналогично этому, (ср. [2]) выбирая $k = n$ и

$$q_\nu = \begin{cases} p^\nu & \text{если} \quad 1 \leqslant \nu \leqslant r, \\ p^r & \text{если} \quad r \leqslant \nu \leqslant n, \end{cases}$$

при $1 \leqslant r \leqslant n$ для числа решений системы

$$\left.\begin{array}{l} x_1 + \ldots + x_n \equiv \lambda_1 \pmod{p} \\ \cdots\cdots\cdots\cdots\cdots \\ x_1^r + \ldots + x_n^r \equiv \lambda_r \pmod{p^r} \\ \cdots\cdots\cdots\cdots\cdots \\ x_1^n + \ldots + x_n^n \equiv \lambda_n \pmod{p^r} \end{array}\right\}; \qquad (x_1, \ldots, x_n)_n \pmod{p^r}$$

получим

$$T_n^{(r)} = p^{r(r-1)/2} T_n(\lambda_1, \ldots, \lambda_n; p) \leqslant n!\, p^{r(r-1)/2}.$$

Цитированная литература

[1] А. А. Карацуба, Н. М. Коробов, *О теореме о среднем*, ДАН СССР 149, 2 (1963), стр. 245–248.

[2] А. А. Карацуба, *О системах сравнений*, Изв. АН СССР, сер. матем., 29 (1965), стр. 959–968.

[3] Ю. В. Линник, *О суммах Weyl'я*, ДАН СССР 34, 7 (1942), стр. 201–203.

МАТЕМАТИЧЕСКИЙ ИНСТИТУТ ИМ В. А. СТЕКЛОВА АН СССР

Получено 8. 8. 1971 (205)

ACTA ARITHMETICA
XXI (1972)

On some special quartic reciprocity laws

by

EMMA LEHMER (Berkeley, Calif.)

In memory of Wacław Sierpiński

In a recent paper [6] we gave an elementary proof of a theorem due to Scholz [9], which can be stated as follows:

Let $p \equiv q \equiv 1 \pmod 4$ be two distinct primes which are quadratic residues of each other and let ε_p and ε_q be the fundamental units in the quadratic fields $Q(\sqrt{p})$ and $Q(\sqrt{q})$, then

$$\left(\frac{\varepsilon_p}{q}\right) = \left(\frac{\varepsilon_q}{p}\right) = \left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4. \tag{1}$$

Traditionally, the quartic character of q with respect to p is expressed in terms of the quadratic partition $p = a^2 + 4b^2$. Thus for $q = 5$ we have

5 is a quartic residue of p if and only if 5 divides b.

In a recent paper of Muskat and Whiteman [7] it was shown, using cyclotomy of order 20, that for $p \equiv 1 \pmod{20}$ this can also be stated in terms of the partition $p = c^2 + 5d^2$ as follows:

5 is a quartic residue of $p \equiv 1 \pmod{20}$ if and only if d is even.

Using (1) this gives at once

$$\left(\frac{\varepsilon_5}{p}\right) = \left(\frac{(1+\sqrt{5})/2}{p}\right) = (-1)^d. \tag{2}$$

About the same time Brandler [2], using the theory of quartic fields, showed that if $p = c^2 + qd^2$, then

$$\left(\frac{\varepsilon_q}{p}\right) = (-1)^d \quad \text{for} \quad q = 5, 13 \tag{3}$$

and that for $q = 17$ we have $\left(\frac{\varepsilon_{17}}{p}\right) = \pm 1$, according as p or $2p$ is represented by $c^2 + 17d^2$.