

РАЦИОНАЛЬНЫЕ ТРИГОНОМЕТРИЧЕСКИЕ СУММЫ
ВДОЛЬ КРИВОЙ

I. Пусть q - натуральное число и

$$f(x, y) = \sum_{0 \leq i+j \leq m} a_{ij} x^i y^j, \quad g(x, y) = \sum_{0 \leq i+j \leq n} b_{ij} x^i y^j$$

многочлены с целыми коэффициентами. Будем считать, что степени многочленов $f \pmod{q}$, $g \pmod{q}$ равны m , n соответственно, и что $mn \geq 1$.

Рассмотрим сумму

$$S(f, g, q) = \sum_{\substack{x, y=1 \\ f(x, y) \equiv 0 \pmod{q}}}^q e^{2\pi i \frac{g(x, y)}{q}} \quad (1)$$

и назовем ее рациональной тригонометрической суммой вдоль "кривой"

$$f(x, y) \equiv 0 \pmod{q}. \quad (2)$$

Пусть p - простое число и K_p - конечное поле из p - элементов. Обозначим $f(x, y)$ многочлен с коэффициентами из K_p , полученный редукцией по \pmod{p} многочлена $f(x, y) \in \mathbb{Z}[x, y]$. Пусть

$$\bar{f} = \bar{f}_1^{\alpha_1} \dots \bar{f}_s^{\alpha_s}$$

разложение многочлена \bar{f} на абсолютно неприводимые множители в некотором конечном расширении поля K_p . Если многочлен $\bar{g}(x, y)$, полученный редукцией по \pmod{p} многочлена $g(x, y)$, удовлетворяет условию, что

$$\bar{g} \equiv h_i^p - h_i \pmod{\bar{f}_i}$$

для каждого $i=1, 2, \dots, s$ и для каждой рациональной функции $h_i = h_i(x, y)$, определенной над алгебраическим замыканием \bar{K}_p поля K_p , то для суммы $S(f, g, p)$ имеет место [1], [2] оценка

$$|S(f, g, p)| \leq c_0(m, n) p^{1/2}.$$

Пусть теперь q - произвольное натуральное число и $g(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_n$ - многочлен с целыми коэффициентами. Если $(a_0, a_1, \dots, a_{n-1}) = 1$ и ε - произвольное положительное число, то для суммы

$$S(q, q) = \sum_{x=1}^q e^{2\pi i \frac{g(x)}{q}}$$

справедлива [3] оценка

$$|S(q, q)| \leq c(n, \varepsilon) q^{1 - \frac{1}{n} + \varepsilon},$$

которая в общем случае является неулучшенной. Заметим, что сумму $S(q, q)$ можно трактовать как сумму

$$S(y - ax - b, \tilde{g}, q) = \sum_{x, y=1}^q e^{2\pi i \frac{\tilde{g}(x, y)}{q}}$$

$$y = ax + b \pmod{q}$$

вдоль "прямой" $y = ax + b \pmod{q}$.

Обозначим

$$f_m(x, y) = \sum_{i+j=m} a_{ij} x^i y^j$$

старшую форму многочлена $f(x, y)$.

Целью работы является доказательство следующего результата.

ТЕОРЕМА. Пусть $\bar{f}(x, y)$, $\bar{g}(x, y)$ - многочлены, полученные редукцией по простому модулю p многочленов $f(x, y)$, $g(x, y)$ и пусть

$$\bar{f} = \bar{f}_1^{\alpha_1} \dots \bar{f}_s^{\alpha_s}$$

разложение многочлена \bar{f} на абсолютно неприводимые множители в некотором конечном расширении поля K_p . Предположим, что многочлены $\bar{f}(x, y)$, $\bar{g}(x, y)$ удовлетворяют условиям:

1. Для каждого простого числа $p \mid q$ результатанта $\bar{R}_i(x)$ многочленов \bar{f}_i и \bar{g} не постоянны на кривых $\bar{f}_i(x, y) = 0$, $1 \leq i \leq s$;

2. Результант $R^*(x)$ многочленов f и $F = \frac{\partial f}{\partial y} \frac{\partial g}{\partial x} - \frac{\partial f}{\partial x} \frac{\partial g}{\partial y}$ отличен от нуля по $\text{mod } q$;

3. Кривая $f(x, y) = 0 \pmod{p}$ - неособая в поле K_p для каждого простого $p \mid q$;

4. Сравнение $f_m(x, y) \equiv 1 \pmod{q}$ разрешимо. Тогда при любом $\varepsilon > 0$ имеет место оценка

$$\left| \sum_{\substack{x, y=1 \\ f(x, y) \equiv 0 \pmod{q}}^q e^{2\pi i \frac{g(x, y)}{q}} \right| \leq c(m, n, \varepsilon) q^{1 - \frac{1}{N+1} + \varepsilon},$$

где $N \leq m(m+n-2)$ - максимальная кратность пересечения в поле K_p кривых $f(x, y) \equiv 0 \pmod{p}$ и $F(x, y) \equiv 0 \pmod{p}$ для всех простых $p \mid q$.

2. Доказательству теоремы предположим ряд лемм.

ЛЕММА 1. Пусть δ - число различных простых делителей числа q и $d(q)$ - число всех его положительных делителей. Тогда справедливы неравенства

$$2^\delta \leq d(q) \leq c(\varepsilon) q^\varepsilon,$$

где ε - произвольное положительное число.

Доказательство леммы см. в монографии [3] (лемма I.2, стр.7).

ЛЕММА 2. Если $(q_1, q_2) = 1$, $q = q_1 q_2$ и $f(0, 0) \equiv g(0, 0) \equiv 0 \pmod{q}$, то

$$\begin{aligned} & S(f(x, y), g(x, y), q_1 q_2) = \\ & = S(f(x q_2, y q_2), \frac{g(x q_2, y q_2)}{q_2}, q_1) S(f(x q_1, y q_1), \frac{g(x q_1, y q_1)}{q_1}, q_2). \end{aligned}$$

Доказательство. Положим

$$x = x_1 q_2 + x_2 q_1$$

$$y = y_1 q_2 + y_2 q_1.$$

Тогда, если x_1, y_1 и x_2, y_2 пробегает полные системы вычетов по $\text{mod } q_1$ и $\text{mod } q_2$ соответственно, то x и y пробегает полные системы вычетов по $\text{mod } q_1 q_2$. Имеем

$$e^{2\pi i \frac{g(x, y)}{q}} = e^{2\pi i \frac{g(x_1 q_2, y_1 q_2)}{q_1 q_2}} e^{2\pi i \frac{g(x_2 q_1, y_2 q_1)}{q_1 q_2}},$$

$$f(x, y) \equiv f(x_1 q_2, y_1 q_2) + f(x_2 q_1, y_2 q_1) \pmod{q_1 q_2}$$

и, в таком случае,

$$S(f(x, y), g(x, y), q_1 q_2) =$$

$$= \sum_{x_1, x_2=1}^{q_1} \sum_{y_1, y_2=1}^{q_2} e^{2\pi i \frac{g(x_1 q_2, y_1 q_2)/q_2}{q_1}} e^{2\pi i \frac{g(x_2 q_1, y_2 q_1)/q_1}{q_2}} =$$

$$= f(x_1 q_2, y_1 q_2) + f(x_2 q_1, y_2 q_1) \equiv 0 \pmod{q_1 q_2}.$$

Но сравнение

$$f(x_1 q_2, y_1 q_2) + f(x_2 q_1, y_2 q_1) \equiv 0 \pmod{q_1 q_2}$$

эквивалентно системе сравнений

$$f(x_1 q_2, y_1 q_2) \equiv 0 \pmod{q_1}$$

$$f(x_2 q_1, y_2 q_1) \equiv 0 \pmod{q_2}$$

и тогда

$$S(f(x, y), g(x, y), q_1 q_2) =$$

$$= \sum_{x_1, y_1=1}^{q_1} e^{2\pi i \frac{g(x_1 q_2, y_1 q_2)/q_2}{q_1}} \sum_{x_2, y_2=1}^{q_2} e^{2\pi i \frac{g(x_2 q_1, y_2 q_1)/q_1}{q_2}} =$$

$$f(x_1 q_2, y_1 q_2) \equiv 0 \pmod{q_1} \quad f(x_2 q_1, y_2 q_1) \equiv 0 \pmod{q_2}$$

$$= S(f(x q_2, y q_2), \frac{g(x q_2, y q_2)}{q_2}, q_1) S(f(x q_1, y q_1), \frac{g(x q_1, y q_1)}{q_1}, q_2).$$

Лемма доказана.

Лемма 3. Пусть \bar{f} , \bar{g} — многочлены, полученные из f , g редукцией по простому модулю p и пусть $\bar{f}_1, \dots, \bar{f}_s$ — абсолютно неприводимые делители многочлена \bar{f} над некоторым конечным расширением поля K_p . Если

$$\bar{g} \equiv h_i^p - h_i \pmod{\bar{f}_i}$$

для каждого $i=1, 2, \dots, s$ и для каждой рациональной функции $h_i = h_i(x, y)$, определенной над алгебраическим замыканием \bar{K}_p поля K_p , то

$$\left| \sum_{x, y=1}^p e^{2\pi i \frac{g(x, y)}{p}} \right| \leq (m^2 + 2mn - 3m) \sqrt{p} + m^2.$$

$$f(x, y) \equiv 0 \pmod{p}$$

Данная лемма является частным случаем теоремы 6 работы Е. Бомбьери [I].

Лемма 4. Пусть p - простое число, $f_m(x, y)$ - старшая форма многочлена $f(x, y)$ и пусть многочлены $\bar{f}, \bar{g}, \bar{f}_1, \dots, \dots, \bar{f}_s$ определены как в предыдущей лемме. Если сравнение $f_m(x, y) \equiv 1 \pmod{p}$ разрешимо и результаты $\bar{R}_i(x)$ многочленов \bar{f}_i и \bar{g} не постоянны на кривых $\bar{f}_i(x, y) = 0, 1 \leq i \leq s$, то

$$\left| \sum_{x, y=1}^p e^{2\pi i \frac{g(x, y)}{p}} \right| \leq c_0(m, n) \sqrt{p}.$$

$f(x, y) \equiv 0 \pmod{p}$

ДОКАЗАТЕЛЬСТВО. Если $mn \geq p$, то тривиальная оценка приводит к неравенству

$$\left| \sum_{x, y=1}^p e^{2\pi i \frac{g(x, y)}{p}} \right| \leq p^2 \leq (mn)^{3/2} p^{1/2}$$

$f(x, y) \equiv 0 \pmod{p}$

и в этом случае утверждение леммы справедливо.

Предположим теперь, что $mn < p$. Пусть (β, δ) - решение сравнения $f_m(x, y) \equiv 1 \pmod{p}$. Выберем целые α, γ таким образом; чтобы выполнялось условие

$$\det \begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} \not\equiv 0 \pmod{p}$$

и положим

$$x = \alpha \xi + \beta \eta$$

$$y = \gamma \xi + \delta \eta.$$

Такая невырожденная по $\text{mod } p$ замена переменных переводит многочлен $f(x, y)$ в многочлен

$$\tilde{f}(\xi, \eta) = \eta^m + \tilde{a}_1(\xi) \eta^{m-1} + \dots + \tilde{a}_m(\xi)$$

и в дальнейшем без уменьшения общности будем считать, что многочлен $f(x, y)$ имеет вид

$$f(x, y) = y^m + a_1(x) y^{m-1} + \dots + a_m(x).$$

Пусть

$$\bar{f}_i = y^{m_i} + \bar{a}_{i,1}(x) y^{m_i-1} + \dots + \bar{a}_{i,m_i}(x),$$

$$\bar{q} = \bar{e}_0(x) y^l + \bar{e}_1(x) y^{l-1} + \dots + \bar{e}_l(x).$$

Если $y_{i1}(x), \dots, y_{im_i}(x)$ — корни уравнения $\bar{f}_i(x, y) = 0$, то

$$\bar{R}_i(x) = \prod_{v=1}^{m_i} \bar{q}(x, y_{iv}(x)),$$

и если предположить, что

$$\bar{q}(x, y) \equiv \text{const} \pmod{\bar{f}_i},$$

то отсюда будет следовать, что $\bar{q}(x, y_{iv}(x)) = \text{const}$ для всех $v=1, 2, \dots, m_i$, а тогда

$$\bar{R}_i(x) \equiv \text{const} \pmod{\bar{f}_i}.$$

Но это противоречит условию леммы II, значит, многочлен $\bar{q}(x, y)$ не постоянен на каждой кривой $\bar{f}_i(x, y) = 0$, $1 \leq i \leq s$.

Предположим, что для некоторого $i=1, 2, \dots, s$ имеет место равенство

$$\bar{q}(x, y) \equiv h_i^p - h_i \pmod{\bar{f}_i}$$

с непостоянной функцией $h_i \in \bar{K}_p(x, y)$. Мы имеем

$$1 \leq \deg \bar{q}(x, y) \leq n < p$$

и тогда $\bar{q} \neq h^p - h$. В таком случае многочлен $x^p - x - \bar{q}$ неприводим над полем $\bar{K}_p(x, y)$ и, если $\bar{q} \equiv h_i^p - h_i \pmod{\bar{f}_i}$, то он имеет корень h_i в поле функций $\bar{K}_p[x, y]/(\bar{f}_i(x, y))$ кривой $\bar{f}_i(x, y) = 0$. Но поле разложения многочлена $x^p - x - \bar{q}$ нормально над $\bar{K}_p(x, y)$ и тогда все $l \geq p$ корни многочлена $x^p - x - \bar{q} \pmod{\bar{f}_i}$ будут лежать в поле $\bar{K}_p[x, y]/(\bar{f}_i(x, y))$. Отсюда следует, что

$$[\bar{K}_p[x, y]/(\bar{f}_i(x, y)) : \bar{K}_p(x)] \geq p.$$

С другой стороны

$$[\bar{K}_p[x, y]/(\bar{f}_i(x, y)) : \bar{K}_p(x)] = \deg_y \bar{f}_i(x, y) = m_i \leq m < p$$

и мы приходим к противоречию. Следовательно,

$$\bar{q}(x, y) \not\equiv h_i^p - h_i \pmod{\bar{f}_i}$$

для всех $i=1, 2, \dots, s$ и тогда по лемме 3

$$\left| \sum_{\substack{x, y=1 \\ f(x, y) \equiv 0 \pmod{p}}}^p e^{2\pi i \frac{g(x, y)}{p}} \right| \leq c_0(m, n) \sqrt{p}.$$

Лемма 4 доказана.

ЛЕММА 5. Пусть p — простое число, r — натуральное число и $f(x, y)$ — неособый по $\text{mod } p$ многочлен со старшей формой $f_m(x, y)$. Предположим, что сравнение

$$f_m(x, y) \equiv 1 \pmod{p}$$

разрешимо. Тогда для каждого решения (ξ, η) сравнения

$$f(x, y) \equiv 0 \pmod{p}$$

удовлетворяющего условию

$$\frac{\partial f(\xi, \eta)}{\partial \eta} \not\equiv 0 \pmod{p}$$

и для каждого целого числа t , $1 \leq t \leq p^{r-1}$, существует единственное решение y сравнения

$$f(\xi + pt, y) \equiv 0 \pmod{p^2},$$

такое, что $y \equiv \eta \pmod{p}$.

ЛЕММА 6. В предположениях предыдущей леммы для каждого решения (ξ, η) сравнения $f(x, y) \equiv 0 \pmod{p}$ с условием

$$\frac{\partial f(\xi, \eta)}{\partial \eta} \not\equiv 0 \pmod{p}$$

существует такой многочлен

$$y(t) = \sum_{v=0}^{r-1} \alpha_v p^v t^v$$

с целыми $\alpha_v = \alpha_v(\xi, \eta)$, что

$$f(\xi + pt, y(t)) \equiv 0 \pmod{p^2}$$

и $y(t) \equiv \eta \pmod{p}$.

ДОКАЗАТЕЛЬСТВО. С помощью невырожденной по $\text{mod } p^2$ линейной замены переменных можно привести многочлен $f(x, y)$ к виду

$$f(x, y) = y^m + a_1(x)y^{m-1} + \dots + a_m(x)$$

и тогда утверждение лемм 5 и 6 следует из лемм 2 и 4 работы автора [4].

Следующая лемма представляет собой вариант теоремы Хуа-Ло-гена (см. [3], теорема I, стр.7).

ЛЕММА 7. Пусть p - простое число,

$$P(t) = \sum_{j=0}^k a_j t^j + \sum_{j=k+2}^k a_j p^{j-k-1} t^j$$

многочлен с целыми коэффициентами, такими, что $(a_1, 2a_2, \dots, \dots, (k+1)a_{k+1}, p) = 1$. Тогда для суммы

$$S(P(t), p^\ell) = \sum_{t=1}^{p^\ell} e^{2\pi i \frac{P(t)}{p^\ell}}$$

справедлива оценка

$$|S(P(t), p^\ell)| \leq c(k) p^{\ell(1 - \frac{1}{k+1})}$$

ДОКАЗАТЕЛЬСТВО. Докажем лемму индукцией по ℓ . Если $\ell=1$ то по теореме А.Вейля

$$|S(P(t), p)| \leq kp^{1/2} \leq kp^{1 - \frac{1}{k+1}}$$

и в этом случае утверждение леммы справедливо.

Пусть теперь $\ell \geq 2$ и пусть t_1, \dots, t_p , $0 \leq p \leq k$ - корни сравнения

$$P'(t) \equiv 0 \pmod{p}.$$

Положим

$$t = u + p^{\ell-1} v,$$

где $1 \leq u < p^{\ell-1}$, $1 \leq v < p$. Тогда

$$P(u + p^{\ell-1} v) \equiv P(u) + P'(u) p^{\ell-1} v \pmod{p^\ell}$$

и, следовательно,

$$S(P(t), p^\ell) = \sum_{u=1}^{p^{\ell-1}} e^{2\pi i \frac{P(u)}{p^\ell}} \sum_{v=1}^p e^{2\pi i \frac{P'(u)v}{p}}.$$

Если u не сравнимо по $\text{mod } p$ ни с одним из корней t_s , $1 \leq s \leq p$, то $S(P(t), p^\ell) = 0$ и, стало быть,

$$S(P(t), p^l) = \sum_{s=1}^j \sum_{x=1}^{p^l-1} e^{2\pi i} \frac{P(t_s + px)}{p^l}$$

Пусть

$$P(t_s + px) = P(t_s) + \sum_{j=1}^k b_{s,j} p^j x^j$$

разложение многочлена $P(t_s + px)$ по степеням величины px . Мы имеем

$$b_{s,j} = \frac{1}{j!} \frac{d^j P(t_s)}{dt_s^j} = j^{-1} \left(\frac{1}{(j-1)!} \frac{d^{j-1} P'(t_s)}{dt_s^{j-1}} \right)$$

и, если k_s - кратность корня t_s , то $k_s \leq k$ и

$$(k_s + 1) b_{s, k_s + 1} \equiv 0 \pmod{p}.$$

Пусть p^{M_s} - наивысшая степень числа p , делящая все коэффициенты многочлена

$$P_s^*(x) = P(t_s + px) - P(t_s).$$

Тогда

$$M_s \leq k_s + 1 \leq k + 1$$

и, если

$$P_s^*(x) = p^{M_s} \tilde{P}_s^*(x),$$

то

$$\frac{d \tilde{P}_s^*(x)}{dx} = \sum_{j=1}^{k_s+1} j \tilde{b}_{s,j} x^{j-1} + \sum_{j=k_s+2}^k j \tilde{b}_{s,j} p^{j-M_s} x^{j-1},$$

причем

$$j \tilde{b}_{s,j} \equiv 0 \pmod{p}$$

хотя бы для одного $j = 1, 2, \dots, k_s + 1$. Следовательно,

$$\left| S(P(t), p^l) \right| \leq p \max_{1 \leq s \leq j} \left| \sum_{x=1}^{p^l-1} e^{2\pi i} \frac{P(t_s + px)}{p^l} \right| =$$

$$= p \max_{1 \leq s \leq p} \left| \sum_{x=1}^{p^{\ell-1}} e^{2\pi i x \frac{p_0^*(x)}{p^\ell}} \right| \leq$$

$$\leq p \max_{1 \leq s \leq p} p^{M_0-1} \left| \sum_{x=1}^{p^{\ell-M_0}} e^{2\pi i x \frac{\tilde{P}^*(x)}{p^{\ell-M_0}}} \right| \leq$$

$$\leq p \max_{1 \leq s \leq p} p^{M_0(1-\frac{1}{k+1})} \left| \sum_{x=1}^{p^{\ell-M_0}} e^{2\pi i x \frac{\tilde{P}^*(x)}{p^{\ell-M_0}}} \right|$$

Если теперь $t_{s1}, \dots, t_{s\sigma}$ — корни сравнения

$$\frac{d\tilde{P}^*(x)}{dx} \equiv 0 \pmod{p},$$

то $\sigma \leq k_0$, и по индуктивному предположению

$$\left| \sum_{x=1}^{p^{\ell-M_0}} e^{2\pi i x \frac{\tilde{P}^*(x)}{p^{\ell-M_0}}} \right| \leq \tilde{C}(k_0) p^{(\ell-M_0)(1-\frac{1}{k+1})}$$

Значит

$$\left| S(P(t), p^\ell) \right| \leq c(k) p^{\ell(1-\frac{1}{k+1})}$$

и лемма тем самым доказана.

3. Перейдем к доказательству теоремы. Обозначим (b, d) — решение сравнения $f_m(x, y) \equiv 1 \pmod{q}$ и выберем целые числа a, c таким образом, чтобы определитель

$$\Delta = \det \begin{vmatrix} a & b \\ c & d \end{vmatrix}$$

был взаимно прост с q . Тогда линейная замена переменных

$$x = ax' + by'$$

$$y = cx' + dy'$$

переводит многочлен $f(x, y)$ в многочлен $\tilde{f}(x', y') =$

$$= y'^m + \tilde{a}_1(x')y'^{m-1} + \dots + \tilde{a}_m(x')$$

имеет вид

$$f(x, y) = y^m + a_1(x)y^{m-1} + \dots + a_m(x).$$

Кроме того без уменьшения общности будем считать, что $f(x, y)$ неприводим над полем \mathbb{Q} .

Если сравнение $f(x, y) \equiv 0 \pmod{q}$ не разрешимо, то $S(f, q, q) = 0$, и в этом случае утверждение теоремы справедливо.

Пусть сравнение $f(x, y) \equiv 0 \pmod{q}$ разрешимо и (α, β) — его решение. Замена

$$x = x' + \alpha$$

$$y = y' + \beta$$

переводит $f(x, y)$ в многочлен

$$f^*(x', y') = y'^m + a_1^*(x')y'^{m-1} + \dots + a_m^*(x'),$$

удовлетворяющий условию

$$f^*(0, 0) \equiv 0 \pmod{q}.$$

Поэтому без потери общности мы можем считать, что исходный многочлен $f(x, y)$ обладает свойством, что

$$f(0, 0) \equiv 0 \pmod{q}.$$

Далее, не нарушая общности можно предполагать, что $g(0, 0) \equiv 0 \pmod{q}$. Пусть $q = p_1^{r_1} \dots p_s^{r_s}$ — каноническое разложение числа q на простые множители. Тогда по лемме 2 имеем

$$S(f, g, q) = \prod_{i=1}^s S\left(f\left(\frac{xq}{p^{r_i}}, \frac{yq}{p^{r_i}}\right), \frac{g\left(\frac{xq}{p^{r_i}}, \frac{yq}{p^{r_i}}\right)}{\frac{q}{p^{r_i}}}, p^{r_i}\right)$$

и, стало быть, если мы докажем, что

$$\left| S(f, g, p^r) \right| \leq c(m, n) p^{r(1 - \frac{1}{n+1})}, \quad (3)$$

то получим

$$\left| S(f, g, q) \right| \leq c(m, n)^s q^{1 - \frac{1}{n+1}}.$$

Но по лемме I

$$c(m, n)^s = (2^s)^{\log_2 c(m, n)} \leq c(m, n, \varepsilon) q^\varepsilon$$

и, следовательно,

$$\left| S(f, g, q) \right| \leq c(m, n, \varepsilon) q^{1 - \frac{1}{n+1} + \varepsilon}.$$

Таким образом, для доказательства теоремы достаточно установить справедливость оценки (3).

Пусть p^r -наивысшая степень простого числа p , делящая коэффициенты многочлена

$$F(x, y) = \frac{\partial f}{\partial y} \frac{\partial g}{\partial x} - \frac{\partial f}{\partial x} \frac{\partial g}{\partial y},$$

и пусть

$$F(x, y) = p^r \tilde{F}(x, y).$$

Если $y_1(x), \dots, y_m(x)$ корни многочлена $f(x, y)$ в поле функций $\mathbb{Q}[x, y]/(f(x, y))$ кривой $f(x, y) = 0$, и $R(x)$ -результант многочленов $f(x, y)$ и $g(x, y)$, то

$$R(x) = \prod_{v=1}^m g(x, y_v(x))$$

и

$$\bar{R}(x) = \prod_{i=1}^s \bar{R}_i(x).$$

По условию теоремы все многочлены $\bar{R}_i(x)$ не постоянны на кривых $\bar{f}_i(x, y) = 0$ и тогда из последнего соотношения следует, что многочлен $R(x)$ не есть константа по mod p . В частности, если

$$R(x) = c_0 x^{mn} + c_1 x^{mn-1} + \dots + c_{mn},$$

то мы имеем

$$(c_0, c_1, \dots, c_{mn}, p) = 1.$$

Далее,

$$\begin{aligned} R'(x) &= \sum_{v=1}^m F(x, y_v) \prod_{\substack{i=1 \\ i \neq v}}^m g(x, y_i) \left(\frac{\partial f(x, y_i)}{\partial y_i} \right)^{-1} = \\ &= p^r \sum_{v=1}^m \tilde{F}(x, y_v) \prod_{\substack{i=1 \\ i \neq v}}^m g(x, y_i) \left(\frac{\partial f(x, y_i)}{\partial y_i} \right)^{-1}, \end{aligned}$$

и так как

$$\left(\frac{\partial f(x, y_i)}{\partial y_i}, p \right) = 1,$$

то все коэффициенты многочлена

$$R'(x) = mn c_0 x^{mn-1} + (mn-1) c_1 x^{mn-2} + \dots + c_{mn-1}$$

должны делиться на p^r . В таком случае

$$p^r \mid (mn c_0, (mn-1) c_1, \dots, c_{mn-1})$$

и, следовательно,

$$p^{\tau} \leq mn \quad (4)$$

При выводе оценки (3) рассмотрим два случая. Предположим сначала, что $\nu < 2(\tau+1)$. Если $\tau=0$, то $\nu=1$, и тогда по лемме 4

$$|S(f, g, p)| \leq c(m, n)p^{1/2} \leq c(m, n)p^{1-\frac{1}{N+1}}$$

Если же $\tau \geq 1$, то $\nu < 2\tau+1 \leq 3\tau$, и тогда тривиальным образом

$$|S(f, g, p^{\nu})| \leq p^{2\nu} \leq p^{6\tau} \leq (mn)^6 \leq c(m, n)p^{\nu(1-\frac{1}{N+1})}$$

Тем самым при $\nu < 2(\tau+1)$ неравенство (3) доказано.

Рассмотрим теперь случай $\nu \geq 2(\tau+1)$. Пусть (ξ, η) - решение сравнения

$$f(x, y) \equiv 0 \pmod{p}$$

с условием $\frac{\partial f(\xi, \eta)}{\partial \eta} \not\equiv 0 \pmod{p}$. Тогда по лемме 5 существует единственное решение θ сравнения

$$f(\xi, y) \equiv 0 \pmod{p^{\nu}}$$

такое, что

$$\theta \equiv \eta \pmod{p}$$

Далее, из леммы 6 следует, что существует такой многочлен

$$y(t) = \alpha_1 pt + \dots + \alpha_{\nu-1} p^{\nu-1} t^{\nu-1}$$

с целыми рациональными $\alpha_1, \dots, \alpha_{\nu-1}$, что

$$f(\xi + pt, \theta + y(t)) \equiv 0 \pmod{p^{\nu}}$$

Положим

$$S'_{\eta}(f, g, p^{\nu}) = \sum_{\xi, \eta=1}^p \sum_{t=1}^{p^{\nu-1}} e^{2\pi i \frac{g(\xi+pt, \theta+y(t))}{p^{\nu}}}$$

$f(\xi, \eta) \equiv 0 \pmod{p}$
 $f'_{\eta}(\xi, \eta) \not\equiv 0 \pmod{p}$

Аналогичным образом, если (ξ, η) - решение сравнения

$$f(x, y) \equiv 0 \pmod{p}$$

с условием $\frac{\partial f(\xi, \eta)}{\partial \xi} \not\equiv 0 \pmod{p}$ и

$$x(t) = \beta_1 p t + \dots + \beta_{r-1} p^{r-1} t^{r-1}$$

такой многочлен, что $f(\omega + x(t), \eta + p t) \equiv$

$$\equiv 0 \pmod{p^r}, \quad \text{то положим}$$

$$S'_\xi(f, g, p^r) = \sum_{\xi, \eta=1}^p \sum_{t=1}^{p^{r-1}} e^{2\pi i \frac{g(\omega+x(t), \eta+pt)}{p^r}}$$

$$\begin{aligned} f(\xi, \eta) &\equiv 0 \pmod{p} \\ f'_\xi(\xi, \eta) &\not\equiv 0 \pmod{p} \\ f'_\eta(\xi, \eta) &\equiv 0 \pmod{p} \end{aligned}$$

Так как кривая $f(x, y) \equiv 0 \pmod{p}$ неособая, то для каждой точки (ξ, η) этой кривой либо $\frac{\partial f(\xi, \eta)}{\partial \xi} \not\equiv 0 \pmod{p}$, либо $\frac{\partial f(\xi, \eta)}{\partial \eta} \not\equiv 0 \pmod{p}$ и, следовательно,

$$S(f, g, p^r) = S'_\xi(f, g, p^r) + S'_\eta(f, g, p^r).$$

Оценим сумму $S'_\eta(f, g, p^r)$ (сумма $S'_\xi(f, g, p^r)$ оценивается аналогичным образом). Положим

$$\alpha = \xi + p\mu, \quad \beta = \theta + \psi(\mu),$$

где $1 \leq \mu \leq p^r$, и

$$t = \mu + p^r u + p^{r-2} v,$$

где $1 \leq u \leq p^{r-2}$, $1 \leq v \leq p^{r+1}$. Пусть $y(t) = p\varphi(t)$

и $\psi(\mu + p^r u) = \psi(\mu) + p^{r+1} \psi(u)$.

Мы имеем

$$y(t) = \psi(\mu + p^r u + p^{r-2} v) \equiv \psi(\mu + p^r u) + \varphi'(\mu + p^r u) p^{r-1} v \pmod{p^r}$$

и, следовательно,

$$g(\xi + p t, \theta + \psi(t)) \equiv g(\alpha + p^{r+1} u + p^{r-1} v, \beta + p^{r+1} \psi(u) + \varphi'(\mu + p^r u) p^{r-1} v) \equiv$$

$$\equiv g(\alpha + p^{\tau+1}u, \beta + p^{\tau+1}\psi(u)) + A(\alpha, \beta, u) p^{\tau-\tau-1} v \pmod{p^{\tau}},$$

где

$$A(\alpha, \beta, u) = \frac{\partial g(x, y)}{\partial x} + \frac{\partial g(x, y)}{\partial y} \varphi'(\mu + p^{\tau}u) \Bigg|_{\substack{x = \alpha + p^{\tau+1}u \\ y = \beta + p^{\tau+1}\psi(u)}}$$

Далее,

$$f(\alpha + p^{\tau+1}u, \beta + p^{\tau+1}\psi(u)) \equiv 0 \pmod{p^{\tau+1}}$$

и, в таком случае,

$$\frac{\partial f(x, y)}{\partial x} + \frac{\partial f(x, y)}{\partial y} \varphi'(\mu + p^{\tau}u) \Bigg|_{\substack{x = \alpha + p^{\tau+1}u \\ y = \beta + p^{\tau+1}\psi(u)}} \equiv 0 \pmod{p^{\tau+1}}.$$

Значит

$$\varphi'(\mu + p^{\tau}u) \equiv - \frac{f'_x(x, y)}{f'_y(x, y)} \Bigg|_{\substack{x = \alpha + p^{\tau+1}u \\ y = \beta + p^{\tau+1}\psi(u)}} \pmod{p^{\tau+1}}$$

и, стало быть,

$$g(\xi + p^{\tau}t, \theta + y(t)) \equiv g(\alpha + p^{\tau+1}u, \beta + p^{\tau+1}\psi(u)) + B(\alpha, \beta, u) p^{\tau-\tau-1} v \pmod{p^{\tau}},$$

где

$$B(\alpha, \beta, u) \equiv \frac{F(x, y)}{f'_y(x, y)} \Bigg|_{\substack{x = \alpha + p^{\tau+1}u \\ y = \beta + p^{\tau+1}\psi(u)}} \pmod{p^{\tau+1}}$$

Если $F(\alpha, \beta) \not\equiv 0 \pmod{p^{\tau+1}}$, то

$$B(\alpha, \beta, u) \not\equiv 0 \pmod{p^{\tau+1}}$$

и тогда

$$S'_\eta(f, g, p^{\tau}) =$$

$$= \sum_{\xi, \eta=1}^p \sum_{\mu=1}^{p^{\tau}} \sum_{u=1}^{p^{\tau-2\tau-2}} e^{2\pi i \frac{g(\alpha+p^{\tau+1}u, \beta+p^{\tau+1}\psi(u))}{p^{\tau}}} \sum_{v=1}^{p^{\tau+1}} e^{2\pi i \frac{B(\alpha, \beta, u)v}{p^{\tau}}} = 0.$$

$f(\xi, \eta) \equiv 0 \pmod{p}$
 $f'_{\eta}(\xi, \eta) \not\equiv 0 \pmod{p}$

$F(\alpha, \beta) \equiv 0 \pmod{p^{\tau+1}}$
 $\alpha = \xi + p\mu$
 $\beta = \eta + \psi(\mu)$

Следовательно,

$$S'_{\eta}(f, g, p^{\tau}) = \sum_{\xi, \eta=1}^p \sum_{\mu=1}^{p^{\tau}} \sum_{t=1}^{p^{\tau-1}} e^{2\pi i \frac{g(\alpha+p^{\tau+1}t, \beta+p^{\tau+1}\psi(t))}{p^{\tau}}}$$

$f(\xi, \eta) \equiv 0 \pmod{p}$
 $f'_{\eta}(\xi, \eta) \not\equiv 0 \pmod{p}$

$F(\alpha, \beta) \equiv 0 \pmod{p^{\tau+1}}$
 $\alpha = \xi + p\mu$
 $\beta = \eta + \psi(\mu)$

Пусть \mathcal{M} - множество решений системы сравнений

$$f(\xi, \eta) \equiv 0 \pmod{p}$$

$$F(\alpha, \beta) \equiv 0 \pmod{p^{\tau+1}}$$

в элементах $\xi, \eta = 1, 2, \dots, p$ и $\alpha = \xi + p\mu, \beta = \eta + \psi(\mu)$, где $\mu = 1, 2, \dots, p^{\tau}$. Число M решений этой системы равно величине $\tilde{M} p^{\tau}$, где \tilde{M} - число решений системы сравнений

$$f(\xi, \eta) \equiv 0 \pmod{p}$$

$$\tilde{F}(\xi, \eta) \equiv 0 \pmod{p} \quad (5)$$

Из (4) следует, что

$$M \leq m \tilde{M}$$

и тогда

$$\left| S_{\eta}^*(f, g, p^v) \right| \leq M \max_{(\xi, \eta, \alpha, \beta) \in \mathcal{M}} \left| \sum_{t=1}^{p^{v-1}} e^{2\pi i \frac{g(\alpha+p^{v-1}t, \beta+p^{v-1}\psi(t))}{p^v}} \right| \leq$$

$$\leq m \tilde{M} \max_{(\xi, \eta, \alpha, \beta) \in \mathcal{M}} \left| \sum_{t=1}^{p^{v-1}} e^{2\pi i \frac{g(\alpha+p^{v-1}t, \beta+p^{v-1}\psi(t))}{p^v}} \right|.$$

Оценим величину \tilde{M} и сумму

$$S(\xi, \eta, \alpha, \beta) = \sum_{t=1}^{p^{v-1}} e^{2\pi i \frac{g(\alpha+p^{v-1}t, \beta+p^{v-1}\psi(t))}{p^v}}$$

Для оценки величины \tilde{M} рассмотрим результат $R^*(\xi)$ многочленов $f(\xi, \eta)$ и $F(\xi, \eta) = \frac{\partial f}{\partial \eta} \frac{\partial g}{\partial \xi} - \frac{\partial f}{\partial \xi} \frac{\partial g}{\partial \eta}$. Если $\eta_1(\xi), \dots, \eta_m(\xi)$ - корни многочлена $f(\xi, \eta)$ в поле функций $\mathbb{Q}[\xi, \eta]/(f(\xi, \eta))$ кривой $f(\xi, \eta) = 0$, то

$$R^*(\xi) = \prod_{i=1}^m \left(\frac{\partial f(\xi, \eta_i)}{\partial \eta_i} \frac{\partial g(\xi, \eta_i)}{\partial \xi} - \frac{\partial f(\xi, \eta_i)}{\partial \xi} \frac{\partial g(\xi, \eta_i)}{\partial \eta_i} \right) =$$

$$= p^{m\nu} \tilde{R}^*(\xi).$$

Мы имеем

$$g'(\xi, \eta_i) = \frac{F(\xi, \eta_i)}{f'_{\eta_i}}$$

и тогда

$$R^*(\xi) = \mathcal{D}(\xi) \prod_{i=1}^m g'(\xi, \eta_i), \quad (6)$$

где

$$\mathcal{D}(\xi) = \prod_{i=1}^m f'_{\eta_i}(\xi, \eta_i)$$

суть дискриминант многочлена $f(\xi, \eta)$. Число \tilde{M} решений системы (5) равно числу решений сравнения

$$\tilde{R}^*(\xi) \equiv 0 \pmod{p}$$

и, стало быть, не превосходит степени $m(m+n-2)$ многочлена $\tilde{R}^*(\xi)$. Таким образом

$$\tilde{M} \leq m(m+n-2)$$

и, следовательно,

$$\left| S_{\eta}(f, g, p^{\tau}) \right| \leq m^2 n(m+n-2) \max_{(\xi, \eta, \alpha, \beta) \in M} \left| S(\xi, \eta, \alpha, \beta) \right|.$$

Положим, для краткости

$$g(\alpha + p^{\tau+1}t, \beta + p^{\tau+1}\psi(t)) - g(\alpha, \beta) = g^*(t)$$

и оценим сумму

$$\tilde{S}(\xi, \eta, \alpha, \beta) = \sum_{t=1}^{p^{\tau}-1} e^{2\pi i} \frac{g^*(t)}{p^{\tau}}$$

Пусть

$$g^*(t) = \sum_{j=1}^{n(n-1)} a_j(\alpha, \beta) p^{j(\tau+1)} t^j$$

разложение многочлена $g^*(t)$ по степеням величины $p^{\tau+1}t$.
Тогда

$$a_j(\alpha, \beta) = \frac{1}{j!} \frac{d^j g(\alpha, \beta)}{d\alpha^j},$$

причем производные $\frac{d^j g(\alpha, \beta)}{d\alpha^j}$ вычисляются с учетом соотношения

$$\frac{d\beta}{d\alpha} = - \frac{f_{\alpha}^r(\alpha, \beta)}{f_{\beta}^r(\alpha, \beta)}$$

Пусть k - кратность нуля ξ алгебраической функции $p^{-\tau} \frac{dg(\xi, \eta)}{d\xi} \pmod{p}$, лежащей в поле функций $\overline{K}_p[\xi, \eta] / (\overline{f}_i(\xi, \eta))$ кривой $\overline{f}_i(\xi, \eta) = 0$. Тогда среди значений

$$\frac{1}{p^{\tau}(j-1)!} \frac{d^j g(\xi, \eta)}{d\xi^j}, \quad 1 \leq j \leq k+1,$$

хотя бы одно не сравнимо с нулем по $\text{mod } p$ и, значит, хотя бы одно из значений

$$j \frac{1}{j!} \frac{d^j g(\alpha, \beta)}{d\alpha^j}, \quad 1 \leq j \leq k+1$$

не сравнимо с нулем по $\text{mod } p^{\tau+1}$.

Пусть p^m - наивысшая степень простого числа p , делящая все коэффициенты многочлена $g^*(t)$. Тогда

$$\tau+1 \leq \mu \leq (\kappa+1)(\tau+1) + \tau$$

и

$$g^*(t) = p^\mu \tilde{g}^*(t),$$

где

$$\tilde{g}^*(t) = \sum_{j=1}^{\kappa+1} \tilde{a}_j(\alpha, \beta) t^j + \sum_{j=\kappa+2}^{n(\tau-1)} \tilde{a}_j(\alpha, \beta) p^{j(\tau+1)-\mu} t^j$$

и

$$j \tilde{a}_j(\alpha, \beta) \equiv 0 \pmod{p}$$

хотя бы для одного $j=1, 2, \dots, \kappa+1$. Мы имеем

$$\begin{aligned} |\tilde{S}(\xi, \eta, \alpha, \beta)| &\leq p^{\mu-\tau-1} \left| \sum_{t=1}^{p^{\tau-\mu}} e^{2\pi i t \frac{\tilde{g}^*(t)}{p^{\tau-\mu}}} \right| = \\ &= p^\tau p^{\mu(1-\frac{\tau+1}{\mu})} \left| \sum_{t=1}^{p^{\tau-\mu}} e^{2\pi i t \frac{\tilde{g}^*(t)}{p^{\tau-\mu}}} \right| \end{aligned}$$

и так как

$$1 - \frac{\tau+1}{\mu} \leq 1 - \frac{1 + \frac{\tau}{\tau+1}}{\kappa+1 + \frac{\tau}{\tau+1}} \leq 1 - \frac{1}{\kappa+1},$$

то

$$|\tilde{S}(\xi, \eta, \alpha, \beta)| \leq p^\tau p^{\mu(1-\frac{1}{\kappa+1})} \left| \sum_{t=1}^{p^{\tau-\mu}} e^{2\pi i t \frac{\tilde{g}^*(t)}{p^{\tau-\mu}}} \right|.$$

Учитывая теперь неравенство (4), получаем

$$|\tilde{S}(\xi, \eta, \alpha, \beta)| \leq m \mu p^{\mu(1-\frac{1}{\kappa+1})} \left| \sum_{t=1}^{p^{\tau-\mu}} e^{2\pi i t \frac{\tilde{g}^*(t)}{p^{\tau-\mu}}} \right|$$

и, стало быть,

$$|S_\eta(\xi, q, p^\tau)| \leq m^3 n^2 (m+n-2) \max_{(\xi, \eta, \alpha, \beta) \in m} p^{\mu(1-\frac{1}{\kappa+1})} \left| \sum_{t=1}^{p^{\tau-\mu}} e^{2\pi i t \frac{\tilde{g}^*(t)}{p^{\tau-\mu}}} \right|.$$

Оценим кратность κ корня ξ . Положим $p^{-\tau} \frac{d^j G(\xi, \eta)}{d\xi^j} = G(\xi, \eta)$ и будем считать, что $\eta = \eta_1$. Из равенства (6) мы имеем

$$\frac{1}{j!} \frac{d^j \tilde{R}^*(\xi)}{d\xi^j} = \frac{1}{j!} \frac{d^j G(\xi, \eta)}{d\xi^j} H(\xi, \eta), \quad 0 \leq j \leq \kappa-1,$$

и, так как

$$\frac{1}{j!} \frac{d^j G(\xi, \eta)}{d\xi^j} \equiv 0 \pmod{p}$$

для всех $j = 0, 1, \dots, k-1$, то ξ является по меньшей мере k -кратным корнем многочлена $\tilde{R}^*(\xi) \pmod{p}$. Следовательно, число k не превосходит степени $m(m+n-2)$ многочлена $\tilde{R}^*(\xi)$ и, если N — наибольшее из чисел k для всех ξ и для всех $p|q$, то

$$1 \leq k \leq N \leq m(m+n-2).$$

Таким образом,

$$\left| S_{\eta}^*(f, g, p^v) \right| \leq m^3 n^2 (m+n-2) \max_{(\xi, \eta, \alpha, \beta) \in M} p^{\mu(1-\frac{1}{N+1})} \left| \sum_{t=1}^{p^v-\mu} e^{2\pi i \frac{g^*(t)}{p^{\frac{v-\mu}{N+1}}}} \right|$$

и, так как по лемме 7

$$\left| \sum_{t=1}^{p^v-\mu} e^{2\pi i \frac{g^*(t)}{p^{\frac{v-\mu}{N+1}}}} \right| \leq o(k) p^{(v-\mu)(1-\frac{1}{N+1})},$$

то

$$\left| S_{\eta}^*(f, g, p^v) \right| \leq c_{\eta}(m, n) p^{v(1-\frac{1}{N+1})}.$$

Следовательно,

$$\left| S^*(f, g, p^v) \right| \leq c(m, n) p^{v(1-\frac{1}{N+1})}$$

и тем самым теорема доказана.

Литература

1. В о м б и е р и Е. On exponential sums in finite fields. - Amer. J. Math., 1966, 88, p. 71-105.
2. П е р е л ь м у т е р Г.И. Оценки суммы вдоль алгебраической кривой. - Матем. заметки, 1969, 5, № 33, с. 373-380.
3. Х у а Л о - г е н. Аддитивная теория простых чисел. - Тр. Мат. ин-та АН СССР, 1947, т. 22.
4. С т е п а н о в С.А. Сравнения по модулю, равному степени простого числа. - Изв. ВУЗов, Математика, 1980, 1(92), с. 80-90.