ИЗВЕСТИЯ АКАДЕМИИ НАУК СССР
Серия математическая
33 (1969), 1171—1181

УДК 511

С. А. СТЕПАНОВ

# О ЧИСЛЕ ТОЧЕК ГИПЕРЭЛЛИПТИЧЕСКОЙ КРИВОЙ НАД ПРОСТЫМ КОНЕЧНЫМ ПОЛЕМ

В работе предлагается новый метод исследования алгебраических сравнений по простому модулю, приводящий в случае гиперэллиптических кривых к оценкам по порядку той же силы, что и классические оценки Хассе и Вейля.

1. Пусть $n \geqslant 3$ — нечетное число и $p > 9n^2$ — любое простое число. Обозначим через $k_p$ поле из $p$ элементов. Рассмотрим кривую

$$y^2 = f(x), \tag{1}$$

где

$$f(x) = x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$$

— многочлен с коэффициентами из поля $k_p$. Обозначим через $I_p$ количество решений уравнения (1) в элементах поля $k_p$.

Теоремы, относящиеся к числу решений сравнения (1) могут быть получены методом тригонометрических сумм — имеются в виду работы Давенпорта ([3]), ([4]) и Морделла ([6]) — однако этот метод в общей ситуации не привел к оптимальным результатам.

Для случая $n = 3$ Хассе ([5]) доказал, что для величины $I_p$ выполняется неравенство

$$|I_p - p| < 2\sqrt{p}.$$

Позже элементарное доказательство теоремы Хассе предложил Ю. И. Манин ([2]). Из общего результата А. Вейля ([7]) следует, что при $n \geqslant 3$

$$|I_p - p| \leqslant 2g\sqrt{p},$$

где $g$ — род кривой (1).

В настоящей работе доказывается следующий результат.

ТЕОРЕМА. *Для величины $I_p$ справедлива оценка*

$$|I_p - p| \leqslant \sqrt{3n}\, n \sqrt{p}. \tag{2}$$

Заметим, что оценка (2) несколько слабее результатов Хассе и А. Вейля. Получение предельной оценки для величины $I_p$ требует более тонких исследований и будет предметом нашего дальнейшего внимания.

2. Разделим элементы поля $k_p$ на три категории:

I. Элементы $\alpha \in k_p$, для которых $\left(\frac{f(\alpha)}{p}\right) = 1$. (Через $\left(\frac{a}{p}\right)$ мы обозначаем символ Лежандра.) Пусть их количество равно $I_1$. Заметим, что для

элементов $\alpha$

$$f(\alpha)^{\frac{p-1}{2}} - 1 = 0.$$

II. Элементы $\beta \in k_p$, для которых $\left(\frac{f(\beta)}{p}\right) = -1$. Пусть их количество будет $I_{-1}$. Для элементов $\beta$ справедливо равенство

$$f(\beta)^{\frac{p-1}{2}} + 1 = 0.$$

III. Элементы $\gamma \in k_p$, для которых $f(\gamma) = 0$. Пусть их количество будет $I_0$. Ясно, что

$$I_1 + I_0 + I_{-1} = p.$$

Далее, мы можем следующим образом выразить интересующую нас величину $I_p$:

$$I_p = 2I_1 + I_0.$$

Заметим, наконец, что все элементы поля $k_p$ удовлетворяют уравнению $x^p - x = 0$.

ЛЕММА 1. *Для каждого натурального $m \leqslant \sqrt{p/3n}$ существует не тождественно равный нулю в поле $k_p$ многочлен $R_0(x)$ степени, не превосходящей*

$$\frac{p-1}{2} n + (m-1)p + (n-1)m^2 + n,$$

*такой, что все элементы $\beta \in k_p$, для которых $(f(\beta)/p) = -1$, являются корнями этого многочлена кратности по меньшей мере $2m$.*

Доказательство. Критерий кратности корня см. ([1]) стр. 51. Многочлен $R_0(x)$ будем искать как многочлен с неопределенными полиномиальными коэффициентами

$$r_1^{(0)}(x), r_2^{(0)}(x), \ldots, r_m^{(0)}(x);\ t_1^{(0)}(x), t_2^{(0)}(x), \ldots, t_m^{(0)}(x)$$

вида

$$R_0(x) = \left(1 + f^{\frac{p-1}{2}}\right) \sum_{j=1}^{m} r_j^{(0)} (x^p - x)^{j-1} + \sum_{j=1}^{m} t_j^{(0)} (x^p - x)^j. \tag{3}$$

Введем оператор дифференцирования

$$D = 2\frac{d}{dx}$$

и будем определять $R_i(x)$ следующим образом:

$$R_i(x) = D^i R_0(x).$$

Найдем $R_1(x)$, учитывая, что мы работаем в поле $k_p$:

$$R_1(x) = \left(1 + f^{\frac{p-1}{2}}\right)\left(\sum_{j=1} (Dr_j^{(0)}) (x^p - x)^{j-1} - 2 \sum_{j=2}^{m} (j-1) r_j^{(0)} (x^p - x)^{j-2}\right) -$$

$$-f^{\frac{p-3}{2}} f' \sum_{j=1}^{m} r_j^{(0)} (x^p - x)^{j-1} + \sum_{j=1}^{m} (Dt_j^{(0)}) (x^p - x)^j -$$

$$-2 \sum_{j=1}^{m} j t_j^{(0)} (x^p - x)^{j-1} = \left(1 + f^{\frac{p-1}{2}}\right)\left(\sum_{j=1}^{m} (Dr_j^{(0)}) (x^p - x)^{j-1} -\right.$$

$$\left. -2 \sum_{j=2}^{m} (j-1) r_j^{(0)} (x^p - x)^{j-2}\right) - f^{\frac{p-1}{2}} \frac{f'}{f} \sum_{j=1}^{m} r_j^{(0)} (x^p - x)^{j-1} +$$

$$+ \sum_{j=1}^{m} (Dt_j^{(0)}) (x^p - x)^j - 2 \sum_{j=1}^{m} j t_j^{(0)} (x^p - x)^{j-1}.$$

Прибавим и вычтем в правой части выражение

$$\frac{f'}{f} \sum_{j=1}^{m} r_j^{(0)} (x^p - x)^{j-1}.$$

Мы получаем:

$$R_1(x) = \left(1 + f^{\frac{p-1}{2}}\right)\left(\sum_{j=1}^{m} (Dr_j^{(0)}) (x^p - x)^{j-1} -\right.$$

$$\left. -2 \sum_{j=2}^{m} (j-1) r_j^{(0)} (x^p - x)^{j-2} - \frac{f'}{f} \sum_{j=1}^{m} r_j^{(0)} (x^p - x)^{j-1}\right) +$$

$$+ \frac{f'}{f} \sum_{j=1}^{m} r_j^{(0)} (x^p - x)^{j-1} + \sum_{j=1}^{m} (Dt_j^{(0)}) (x^p - x)^j - 2 \sum_{j=1}^{m} j t_j^{(0)} (x^p - x)^{j-1} =$$

$$= \left(1 + f^{\frac{p-1}{2}}\right)\left(\sum_{j=1}^{m-1} \left(Dr_j^{(0)} - 2j r_{j+1}^{(0)} - \frac{f'}{f} r_j^{(0)}\right) (x^p - x)^{j-1} +\right.$$

$$\left. + \left(Dr_m^{(0)} - \frac{f'}{f} r_m^{(0)}\right) (x^p - x)^{m-1}\right) + \sum_{j=1}^{m-1} \left(Dt_j^{(0)} - 2(j+1) t_{j+1}^{(0)} +\right.$$

$$\left. + \frac{f'}{f} r_{j+1}^{0}\right) (x^p - x)^j + (Dt_m^{(0)}) (x^p - x)^m + \frac{f'}{f} r_1^{(0)} - 2t_1^{(0)}.$$

Если мы возьмем

$$2t_1^{(0)} = \frac{f'}{f} r_1^{(0)},$$

то $R_1(x)$ примет вид:

$$R_1(x) = \left(1 + f^{\frac{p-1}{2}}\right) \sum_{j=1}^{m} r_j^{(1)} (x^p - x)^{j-1} + \sum_{j=1}^{m} t_j^{(1)} (x^p - x)^j,$$

где

$$r_j^{(1)} = Dr_j^{(0)} - 2j r_{j+1}^{(0)} - \frac{f'}{f} r_j^{(0)}, \quad 1 \leqslant j \leqslant m-1,$$

$$r_m^{(1)} = Dr_m^{(0)} - \frac{f'}{f} r_m^{(0)},$$

$$t_j^{(1)} = Dt_j^{(0)} - 2(j+1)t_{j+1}^{(0)} + \frac{f'}{f} r_{j+1}^{(0)}, \quad 1 \leqslant j \leqslant m-1,$$
$$t_m^{(1)} = Dt_m^{(0)}. \tag{4}$$

Нам надо добиться, чтобы $R_2(x)$ имело вид

$$R_2(x) = (1 + f^{\frac{p-1}{2}}) \sum_{i=1}^{m} r_j^{(2)} (x^p - x)^{j-1} + \sum_{i=1}^{m} t_j^{(2)} (x^p - x)^j.$$

Для этого необходимо и достаточно, чтобы

$$2t_1^{(1)} = \frac{f'}{f} r_1^{(1)}.$$

Мы будем последовательно строить выражения $R_i(x)$, $i = 1, 2, \ldots, m$, которые лишь не равным нулю в поле $k_p$ постоянным множителем отличаются от производных $R_0(x)$. Если мы будем выбирать

$$2t_1^{(i-1)} = \frac{f'}{f} r_1^{(i-1)}, \quad i = 1, 2, \ldots, m, \tag{5}$$

то это будет обеспечивать нам нужный вид $i$-го выражения $R_i(x)$:

$$R_i(x) = \left(1 + f^{\frac{p-1}{2}}\right) \sum_{j=1}^{m} r_j^{(i)} (x^p - x)^{j-1} + \sum_{j=1}^{m} t_j^{(i)} (x^p - x)^j.$$

При этом переход коэффициентов от индекса $i-1$ к индексу $i$ задается формулами:

$$r_j^{(i)} = Dr_j^{(i-1)} - 2jr_{j+1}^{(i-1)} - \frac{f'}{f} r_j^{(i-1)}, \quad 1 \leqslant j \leqslant m-1,$$
$$r_m^{(i)} = Dr_m^{(i-1)} - \frac{f'}{f} r_m^{(i-1)},$$
$$t_j^{(i)} = Dt_j^{(i-1)} - 2(j+1)t_{j+1}^{(i-1)} + \frac{f'}{f} r_{j+1}^{(i-1)}, \quad 1 \leqslant j \leqslant m-1, \tag{6}$$
$$t_m^{(i)} = Dt_m^{(i-1)}.$$

Выразим величину $t_j$, $j = 1, 2, \ldots, m$, через величины $r_1^{(0)}, r_2^{(0)}, \ldots, r_j^{(0)}$.

При этом мы докажем, что величины $2^j j!\, t_j^{(0)}$ будут выражаться в виде линейных форм

$$2t_1^{(0)} = F_1^{(1)} r_1^{(0)},$$
$$8t_2^{(0)} = F_1^{(2)} r_1^{(0)} + F_2^{(2)} r_2^{(0)},$$
$$\cdots\cdots\cdots\cdots \tag{7}$$
$$\cdots\cdots\cdots\cdots$$
$$2^j j!\, t_j^{(0)} = F_1^{(j)} r_1^{(0)} + F_2^{(j)} r_2^{(0)} + \ldots + F_j^{(j)} r_j^{(0)}$$

от $r_1^{(0)}, r_2^{(0)}, \ldots, r_j^{(0)}$ с коэффициентами $F_j^{(i)}$, являющимися рациональными функциями.

Докажем это по индукции. Для $j = 1$ мы это уже доказали. По формулам (4) с заменой $j$ на $j - 1$ мы имеем:

$$t_{j-1}^{(1)} = Dt_{j-1}^{(0)} - 2jt_j^{(0)} + \frac{f'}{f} r_j^{(0)}.$$

По предположению индукции

$$2^{j-1}(j-1)!t_{j-1}^{(1)} = F_1^{(j-1)} r_1^{(1)} + F_2^{(j-1)} r_2^{(1)} + \ldots + F_{j-1}^{(j-1)} r_{j-1}^{(1)},$$
$$2^{j-1}(j-1)!t_{j-1}^{(0)} = F_1^{(j-1)} r_1^{(0)} + F_2^{(j-1)} r_2^{(0)} + \ldots + F_{j-1}^{(j-1)} r_{j-1}^{(0)}.$$

Это дает:

$$2^j j! t_j^{(0)} = 2^{j-1}(j-1)!Dt_{j-1}^{(0)} - 2^{j-1}(j-1)!t_{j-1}^{(1)} + 2^{j-1}(j-1)!\frac{f'}{f} r_j^{(0)} =$$
$$= D\sum_{k=1}^{j-1} F_k^{(j-1)} r_k^{(0)} - \sum_{k=1}^{j-1} F_k^{(j-1)} r_k^{(1)} + 2^{j-1}(j-1)!\frac{f'}{f} r_j^{(0)}.$$

Выражая по формулам (4) величины $r_1^{(1)}, r_2^{(1)}, \ldots, r_{j-1}^{(1)}$ через $r_1^{(0)}, r_2^{(0)}, \ldots, r_{j-1}^{(0)}$, получим:

$$2^j j! t_j^{(0)} = \sum_{k=1}^{j-1} (DF_k^{(j-1)}) r_k^{(0)} + 2\sum_{k=1}^{j-1} kF_k^{(j-1)} r_{k+1}^{(0)} +$$
$$+ \frac{f'}{f}\sum_{k=1}^{j-1} F_k^{(j-1)} r_k^{(0)} + 2^{j-1}(j-1)!\frac{f'}{f} r_j^{(0)} =$$
$$= \left(2(j-1)F_{j-1}^{(j-1)} + 2^{j-1}(j-1)!\frac{f'}{f}\right) r_j^{(0)} +$$
$$+ \sum_{k=1}^{j-1}\left(DF_k^{(j-1)} + 2(k-1)F_{k-1}^{(j-1)} + \frac{f'}{f}F_k^{(j-1)}\right) r_k^{(0)}.$$

Таким образом, для $j = 1, 2, \ldots, m$

$$\begin{aligned} F_k^{(j)} &= DF_k^{(j-1)} + 2(k-1)F_{k-1}^{(j-1)} + \frac{f'}{f}F_k^{(j-1)}, \quad 1 \leqslant k \leqslant j-1, \\ F_j^{(j)} &= 2(j-1)F_{j-1}^{(j-1)} + 2^{j-1}(j-1)!\frac{f'}{f}. \end{aligned} \tag{8}$$

Итерируя второе равенство, получим:

$$F_j^{(j)} = 2^{j-1} j! F_1^{(1)}, \quad j = 1, 2, \ldots, m. \tag{9}$$

Заметим, что формулы (7) совместно с формулами (6) дают формулы (5) и тем самым обеспечивают нужный вид выражений $R_i(x)$ для $i = 1, 2, \ldots, m$.

Условия того, что выражения $R_i(x)$, где $m + 1 \leqslant i \leqslant 2m - 1$, имеют нужный вид, позволяют найти связь между $r_1^{(0)}, r_2^{(0)}, \ldots, r_m^{(0)}$. Мы имеем:

$$2^m m! t_m^{(0)} = F_1^{(m)} r_1^{(0)} + F_2^{(m)} r_2^{(0)} + \ldots + F_m^{(m)} r_m^{(0)}.$$

Аналогично для $i = 1, 2, \ldots, 2m - 1$:

$$2^m m! t_m^{(i)} = F_1^{(m)} r_1^{(i)} + F_2^{(m)} r_2^{(i)} + \ldots + F_m^{(m)} r_m^{(i)}.$$

Но при $i = 1, 2, \ldots, 2m - 1$

$$t_m^{(i)} = D t_m^{(i-1)}.$$

Рассмотрим

$$2^m m! t_m^{(1)} = F_1^{(m)} r_1^{(1)} + F_2^{(m)} r_2^{(1)} + \ldots + F_m^{(m)} r_m^{(1)}.$$

Из (10), при $i = 1$, имеем:

$$D(F_1^{(m)} r_1^{(0)} + F_2^{(m)} r_2^{(0)} + \ldots + F_m^{(m)} r_m^{(0)}) = F_1^{(m)} r_1^{(1)} + F_2^{(m)} r_2^{(1)} + \ldots + F_m^{(m)} r_m^{(1)}$$

или, ввиду (4),

$$\sum_{j=1}^{m} (DF_j^{(m)}) r_j^{(0)} + \sum_{j=1}^{m} F_j^{(m)} (Dr_j^{(0)}) =$$

$$= \sum_{j=1}^{m-1} F_j^{(m)} \left( Dr_j^{(0)} - 2j r_{j+1}^{(0)} - \frac{f'}{f} r_j^{(0)} \right) + F_m^{(m)} \left( Dr_m^{(0)} - \frac{f'}{f} r_m^{(0)} \right),$$

т. е.

$$\sum_{j=1}^{m} \left( DF_j^{(m)} + 2(j-1) F_{j-1}^{(m)} + \frac{f'}{f} F_j^{(m)} \right) r_j^{(0)} = 0.$$

Запишем это соотношение между $r_1^{(0)}, r_2^{(0)}, \ldots, r_m^{(0)}$ в виде

$$\sum_{j=1}^{m} F_j^{(m+1)} r_j^{(0)} = 0,$$

где

$$F_j^{(m+1)} = DF_j^{(m)} + 2(j-1) F_{j-1}^{(m)} + \frac{f'}{f} F_j^{(m)} \qquad j = 1, 2, \ldots, m.$$

Это соотношение является следствием нужного вида для $R_{m+1}(x)$. Вообще же мы получим $m - 1$ таких соотношений:

$$\sum_{j=1}^{m} F_j^{(i)} r_j^{(0)} = 0, \qquad i = m + 1, \ldots, 2m - 1, \tag{11}$$

если потребуем, чтобы $R_{m+1}(x), \ldots, R_{2m-1}(x)$ имели нужный вид.

Найдем рекуррентные соотношения. Применяя к (11) оператор $D$, получим:

$$\sum_{j=1}^{m} (DF_j^{(i)}) r_j^{(0)} + \sum_{j=1}^{m} F_j^{(i)} Dr_j^{(0)} = 0. \tag{12}$$

Далее, имеем:

$$\sum_{j=1}^{m} F_j^{(i)} r_j^{(1)} = 0.$$

Отсюда находим:

$$\sum_{j=1}^{m-1} F_j^{(i)} \left( Dr_j^{(0)} - 2jr_{j+1}^{(0)} - \frac{f'}{f} r_j^{(0)} \right) + F_m^{(i)} \left( Dr_m^{(0)} - \frac{f'}{f} r_m^{(0)} \right) = 0.$$

Вычитая последнее равенство из (12), получим:

$$\sum_{j=1}^{m} \left( DF_j^{(i)} + 2(j-1) F_{j-1}^{(i)} + \frac{f'}{f} F_j^{(i)} \right) r_j^{(0)} = 0,$$

т. е.

$$F_j^{(i+1)} = DF_j^{(i)} + 2(j-1) F_{j-1}^{(i)} + \frac{f'}{f} F_j^{(i)}, \quad i = m+1, \ldots, 2m-2. \tag{13}$$

Найдем нетривиальное решение системы уравнений (11) в многочленах $r_j^{(0)}$. Будем считать, что ранг матрицы

$$\left\| \begin{matrix} F_1^{(m+1)} \ldots F_m^{(m+1)} \\ \ldots\ldots\ldots\ldots \\ F_1^{(2m-1)} \ldots F_m^{(2m-1)} \end{matrix} \right\| \tag{14}$$

в поле $k_p$ равен $m-1$, т. е. рассмотрим самый плохой случай.

Докажем с помощью индукции, что $F_j^{(i)}$, $i = 1, 2, \ldots, 2m-1$, $j = 1, 2, \ldots, m$, $j \leqslant i$,— рациональные функции вида

$$F_j^{(i)} = \frac{P_j^{(i)}}{f^{i-j+1}}$$

и что степень многочлена $P_j^{(i)}$ не превосходит

$$\nu_j^{(i)} = (i-j+1)(n-1), \quad i = 1, 2, \ldots, 2m-1, \quad j = 1, 2, \ldots, m. \tag{15}$$

Для $i = 1$ утверждение очевидно, так как

$$F_1^{(1)} = \frac{f'}{f}.$$

На основании формулы (9) утверждение очевидно, и для $j = i$ при всех $i = 1, 2, \ldots, m$. По предположению индукции

$$F_j^{(i-1)} = \frac{P_j^{(i-1)}}{f^{i-j}}, \quad F_{j-1}^{(i-1)} = \frac{P_{j-1}^{(i-1)}}{f^{i-j+1}},$$

а степени многочленов $P_j^{(i-1)}$ и $P_{j-1}^{(i-1)}$ не превосходят соответственно

$(i-j)(n-1)$ и $(i-j+1)(n-1)$. Но при $i \neq j$, в силу (8) и (13),

$$F_j^{(i)} = DF_j^{(i-1)} + 2(j-1)F_{j-1}^{(i-1)} + \frac{f'}{f} F_j^{(i-1)}, \quad i = 1,2,\ldots,2m-1. \quad (16)$$

Далее, легко видеть, что

$$DF_j^{(i-1)} = \frac{Q_j^{(i-1)}}{f^{i-j+1}}$$

и что степень многочлена $Q_j^{(i-1)}$ не выше $(i-j+1)(n-1)$. Тогда утверждение следует из (16) очевидным образом.

Таким образом, матрица (14) имеет вид

$$\left\| \begin{matrix} \dfrac{P_1^{(m+1)}}{f^{m+1}} & \cdots & \dfrac{P_m^{(m+1)}}{f^2} \\ \cdots & \cdots & \cdots \\ \dfrac{P_1^{(2m-1)}}{f^{2m-1}} & \cdots & \dfrac{P_m^{(2m-1)}}{f^m} \end{matrix} \right\|$$

и, значит, система (11) эквивалентна системе

$$\sum_{j=1}^{m} \bar{F}_j^{(i)} r_j^{(0)} = 0, \quad i = m+1,\ldots,2m-1, \quad (17)$$

в которой $\bar{F}_j^{(i)} = f^{i-m}F_j^{(i)}$. Будем искать $r_j^{(0)}$ в виде

$$r_j^{(0)} = f^{m-j+1}\bar{r}_j^{(0)}. \quad (18)$$

Тогда система (17) перейдет в систему

$$\sum_{j=1}^{m} P_j^{(i)} \bar{r}_j^{(0)} = 0, \quad i = m+1,\ldots,2m-1, \quad (19)$$

с полиномиальными коэффициентами $P_j^{(i)}$. Пусть

$$P_j^{(i)} = \sum_{k=0}^{\nu_j^{(i)}} a_{k,j}^{(i)} x^k, \quad i = m+1,\ldots,2m-1, \quad j = 1,2,\ldots,m.$$

Будем искать $\bar{r}_j^{(0)}$ в виде

$$\bar{r}_j^{(0)} = \sum_{s=0}^{\mu_j} b_{s,j}^{(0)} x^s,$$

где $\mu_j = (m^2 - m + j)(n-1)$. Тогда система (19) примет вид

$$\sum_{l=0}^{\mu_j+\nu_j^{(i)}} \left( \sum_{j=1}^{m} \sum_{k+s=l} a_{k,j}^{(i)} b_{s,j}^{(0)} \right) x^l = 0, \quad i = m+1,\ldots,2m-1.$$

Следовательно, должны выполняться равенства:

$$\sum_{j=1}^{m}\sum_{s=0}^{\mu_j} a_{l-s,\,j}^{(i)} b_{s,\,j}^{(0)} = 0, \quad l = 0, 1, \ldots, \nu_j^{(i)} + \mu_j, \quad i = m+1, \ldots, 2m-1. \tag{20}$$

В этой системе $M = \sum_{j=1}^{m} (\mu_j + 1)$ неизвестных $b_{s,\,j}^{(0)}$ и $N \leqslant \sum_{i=m+1}^{2m-1} (\mu_j + \nu_j^{(i)} + 1)$ уравнений. Мы имеем:

$$M = (n-1)\sum_{j=1}^{m} (j + m^2 - m) + m =$$

$$= (n-1)m^3 - \frac{n-1}{2} m^2 + \frac{n+1}{2} m,$$

$$N \leqslant (n-1)\sum_{i=1}^{m-1} (i + m^2 + 1) + (m-1) =$$

$$= (n-1)m^3 - \frac{n-1}{2} m^2 + \frac{n+1}{2} m - n.$$

Таким образом, $M - N \geqslant n$ и система (20) имеет нетривиальное решение в элементах $b_{s,j}^{(0)}$ поля $k_p$.

Из (7) и (18) видно, что $t_j^{(0)}$, $j = 1, 2, \ldots, m$, также являются многочленами. Ввиду того, что все $R_i(x)$, $i = 0, 1, \ldots, 2m-1$, имеют нужный вид, все производные многочлена $R_0(x)$ до порядка $2m-1$ включительно обращаются в нуль в точках $\beta \in k_p$, для которых $(f(\beta)/p) = -1$.

Остается только показать, что многочлен $R_0(x)$ не равен тождественно нулю. Обозначим через $\delta_j$ степень многочлена $r_j^{(0)}$, а через $\gamma_i$ — степень многочлена $t_i^{(0)}$. Ввиду того, что степень $r_j^{(0)}$ не превосходит $(m^2 - m + j)(n-1)$, в силу (18) получим, что $\delta_j \leqslant m^2(n-1) + m + n - j$. Далее, в силу формул (7) и (15), имеем: $\gamma_i \leqslant m^2(n-1) + m + n - i - 1$. По условию $p > 9n^2$, $m \leqslant \sqrt{p/3}\,n$ и, следовательно,

$$\delta_j + \frac{n}{2} \leqslant m^2(n-1) + m + \frac{3n}{2} - j < \frac{p}{2}, \quad j = 1, 2, \ldots, m,$$

$$\gamma_i + \frac{n}{2} \leqslant m^2(n-1) + m + \frac{3n}{2} - i < \frac{p}{2}, \quad i = 1, 2, \ldots, m. \tag{21}$$

Степень многочлена $(1 + f^{(p-1)/2}) r_j^{(0)} (x^p - x)^{j-1}$ равна

$$\rho_j = \frac{n}{2} p - \frac{n}{2} + \delta_j + p(j-1),$$

а степень многочлена $t_i^{(0)} (x^p - x)^i$ равна $\omega_i = pi + \gamma_i$. Ввиду нечетности $n$, из (21) следует, что $\rho_j \neq \omega_i$ при любых $i, j = 1, 2, \ldots, m$ и что $\rho_i > \rho_j$, $\omega_i > \omega_j$ при $i > j$. Следовательно, в выражении $R_0(x)$ члены

$$\left(1+f^{\frac{p-1}{2}}\right)r_1^{(0)},\ \left(1+f^{\frac{p-1}{2}}\right)r_2^{(0)}(x^p-x),\ldots,\ \left(1+f^{\frac{p-1}{2}}\right)r_m^{(0)}(x^p-x)^{m-1}$$

$$t_1^{(0)}(x^p-x),\ t_2^{(0)}(x^p-x)^2,\ldots,t_m^{(0)}(x^p-x)^m$$

не смогут проинтерферировать.

Оценим, наконец, степень многочлена $R_0(x)$. Степени многочленов $(1+f^{(p-1)/2})r_j^{(0)}(x^p-x)^{j-1}$, $j=1,2,\ldots,m$, как легко видеть, не превосходят

$$\frac{p-1}{2}n+(m-1)p+(n-1)m^2+n. \tag{22}$$

Степени же многочленов $t_j^{(0)}(x^p-x)^j$, $j=1,2,\ldots,m$, не превосходят

$$m^2(n-1)+n+mp-1. \tag{23}$$

Следовательно, сравнивая (22) и (23), заключаем, что степень $R_0(x)$ не выше

$$\frac{p-1}{2}n+(m-1)p+(n-1)m^2+n.$$

Лемма тем самым полностью доказана.

ЛЕММА 2. *Для каждого натурального $m\leqslant\sqrt{p/3n}$ существует не тождественно равный нулю в поле $k_p$ многочлен $S_0(x)$ степени, не превосходящей*

$$\frac{p-1}{2}n+(m-1)p+(n-1)m^2+n,$$

*такой, что все элементы $\alpha\in k_p$, для которых $\left(\frac{f(\alpha)}{p}\right)=1$, являются корнями этого многочлена кратности по меньшей мере $2m$.*

Доказательство аналогично доказательству леммы 1 с той лишь разницей, что многочлен $S_0(x)$ ищется в виде

$$S_0(x)=\left(1-f^{\frac{p-1}{2}}\right)\sum_{j=1}^{m}s_j^{(0)}(x^p-x)^{j-1}+\sum_{j=1}^{m}u_j^{(0)}(x^p-x)^j.$$

3. Докажем теорему. Так как количество корней многочлена не превосходит его степени, то в силу леммы 1 имеем неравенство

$$2mI_{-1}\leqslant\frac{p-1}{2}n+(m-1)p+(n-1)m^2+n,$$

или

$$2m(p-I_1-I_0)\leqslant\frac{p-1}{2}n+(m-1)p+(n-1)m^2+n.$$

Следовательно,

$$2m\left(p-\frac{I_p}{2}-\frac{I_0}{2}\right)\leqslant\frac{p-1}{2}n+(m-1)p+(n-1)m^2+n.$$

Но $I_0\leqslant n$, значит,

$$2m\left(p-\frac{I_p}{2}-\frac{n}{2}\right)\leqslant\frac{p-1}{2}n+(m-1)p+(n-1)m^2+n.$$

Отсюда получаем:

$$I_p\geqslant p+\frac{p}{m}-(n-1)m-\frac{n}{2}-\frac{p+1}{2m}n. \tag{24}$$

В силу леммы 2,

$$2m\frac{I_p-I_0}{2}\leqslant\frac{p-1}{2}n+(m-1)p+(n-1)m^2+n,$$

или

$$I_p\leqslant p-\frac{p}{m}+(n-1)m+n+\frac{p+1}{2m}n. \tag{25}$$

Возьмем $m=[\sqrt{p/3n}]$. Тогда (24) и (25) дают:

$$I_p\geqslant p-\sqrt{3n}\,n\sqrt{p},\quad I_p\leqslant p+\sqrt{3n}\,n\sqrt{p}.$$

Следовательно,

$$|I_p-p|\leqslant\sqrt{3n}\,n\sqrt{p}.$$

Теорема доказана.

Я благодарю Алексея Георгиевича Постникова за постоянную помощь и ценные советы.

Поступило
24.IX.1968

ЛИТЕРАТУРА

[1] Бурбаки Н., Алгебра. Многочлены и поля. Упорядоченные группы, М., 1965.
[2] Манин Ю. И., О сравнениях третьей степени по простому модулю, Изв. АН СССР, сер. матем., 20 (1956) 673—678.
[3] Davenport H., On the distribution of quadratic residues (mod $p$), J. London, Math. Soc., 6 (1931), 49—54.
[4] Davenport H., On the distribution of quadratic residues (mod $p$), J. London, Math. Soc., 8 (1933), 46—52.
[5] Hasse H., Abstrakte Begründung der komplexen Multiplikation und Riemannsche Vermutung in Funktionenkörpern, Abh. Math. Senc. Hamburg, 10 (1934), 325—348.
[6] Mordell L. I., The number of solutions of some congruences in two variables, Math. Z., 37 (1933), 193—209.
[7] Weil A., Sur les courbes algébriques et les variétés qui s'en déduisent, Act. Sci. Ind. 1041, Paris, Herman, 1948.