ACTA ARITHMETICA
XVII (1970)

Elementary method in the theory of congruences for a prime modulus

by

S. A. STEPANOV (Moscow)

1. Let $m, n \geqslant 2$ be coprime natural numbers and let $p > 4m^2n(n-1)^2$ be any prime number. We denote a finite field of order p by k_p. Let I_p be the number of solutions in $x, y \in k_p$ of the equation

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

where

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

is a polynomial with integral coefficients.

In the case $n = 2$, $m = 3$ Hasse [2] proved that

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

Later Yu. I. Manin [3] proposed an elementary proof of Hasse's theorem. The inequality

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

where g is the genus of curve (1) follows from Weil's result [4]. In [1] I proved for $n = 2$ and every odd m by an elementary method the following result

$$|I_p - p| < \sqrt{3m}\, m\sqrt{p}.$$

In the present paper I prove by the same method the following:

THEOREM. *Let* $q = (n, p-1)$. *Then*

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

2. We divide the all elements of k_p into three classes:

I. The first class consists of such $a \in k_p$ for which $f(a) \neq 0$ and the equation $y^n = f(a)$ is solvable in k_p. Let I_{+1} be the number of those a.

Those a and only they satisfy the equation

$$1-f(a)^{\frac{p-1}{q}}=0.$$

II. The second class consists of $\beta\in k_p$ for which the equation $y^n=f(\beta)$ is insolvable in k_p. Let I_{-1} be the number of those β. Those β and only they satisfy the equation

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

III. The third class consists of $\gamma\in k_p$ for which $f(\gamma)=0$. Let I_0 be the number of those γ.

Obviously

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

Further we can write

$$I_p=qI_{+1}+I_0.$$

At last we note that for all $x\in k_p$

$$x^p-x=0.$$

LEMMA 1. *Let $q\geqslant 2$. For any natural $N\leqslant\sqrt{p/2qm}$ there exists a polynomial $R_0(x)$, not identically equal to zero, of degree at most*

$$\frac{(q-1)(p-1)}{q}m+Np+(m-1)N^2+m$$

such that all the elements of the second class are roots of $R_0(x)$ of order at least $N+\left[\frac{N-1}{q-1}\right]+1$.

Proof. We shall look for $R_0(x)$ in the form

$$R_0(x)=\sum_{i=0}^{q-1}f(x)^{\frac{i(p-1)}{q}}\sum_{j=1}^{N}r_j^{(0)}(x)(x^p-x)^{j-1}+\sum_{i=0}^{q-2}f(x)^{\frac{i(p-1)}{q}}\sum_{j=1}^{N}t_{i,j}^{(0)}(x)(x^p-x)^j,$$

where $r_j^{(0)}(x)$, $t_{i,j}^{(0)}(x)$, $i=0,1,\ldots,q-2$; $j=1,2,\ldots,N$, are indeterminate polynomial coefficients. Define the operator of differentiation

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

and denote

$$R_k(x)=D^kR_0(x),\quad k=1,2,\ldots$$

Let us find $R_1(x)$ taking into account that k_p has a characteristic p.

$$\begin{aligned}R_1(x)=&\sum_{i=0}^{q-1}f^{\frac{i(p-1)}{q}}\sum_{j=1}^{N}(Dr_j^{(0)})(x^p-x)^{j-1}-\\&-q\sum_{i=0}^{q-1}f^{\frac{i(p-1)}{q}}\sum_{j=1}^{N}(j-1)r_j^{(0)}(x)(x^p-x)^{j-2}-\\&-\frac{df}{dx}f^{-1}\sum_{i=0}^{q-1}if^{\frac{i(p-1)}{q}}\sum_{j=1}^{N}r_j^{(0)}(x)(x^p-x)^{j-1}+\\&+\sum_{i=0}^{q-2}f^{\frac{i(p-1)}{q}}\sum_{j=1}^{N}(Dt_{i,j}^{(0)})(x^p-x)^j-\\&-q\sum_{i=0}^{q-2}f^{\frac{i(p-1)}{q}}\sum_{j=1}^{N}jt_{i,j}^{(0)}(x)(x^p-x)^{j-1}-\\&-\frac{df}{dx}f^{-1}\sum_{i=0}^{q-2}if^{\frac{i(p-1)}{q}}\sum_{j=1}^{N}t_{i,j}^{(0)}(x)(x^p-x)^j.\end{aligned}$$

If we add and subtract the following expression

$$(q-1)\frac{df}{dx}f^{-1}\sum_{i=0}^{q-2}f^{\frac{i(p-1)}{q}}\sum_{j=1}^{N}r_j^{(0)}(x)(x^p-x)^{j-1}$$

on the right-hand side of the last equality, we get

$$\begin{aligned}R_1(x)=&\sum_{i=0}^{q-1}f^{\frac{i(p-1)}{q}}\Bigg(\sum_{j=1}^{N}(Dr_j^{(0)})(x^p-x)^{j-1}-q\sum_{j=1}^{N}(j-1)r_j^{(0)}(x)(x^p-x)^{j-2}-\\&-(q-1)\frac{df}{dx}f^{-1}\sum_{j=1}^{N}r_j^{(0)}(x)(x^p-x)^{j-1}\Bigg)+\\&+\frac{df}{dx}f^{-1}\sum_{i=0}^{q-2}(q-1-i)f^{\frac{i(p-1)}{q}}\sum_{j=1}^{N}r_j^{(0)}(x)(x^p-x)^{j-1}-\\&-\frac{df}{dx}f^{-1}\sum_{i=0}^{q-2}if^{\frac{i(p-1)}{q}}\sum_{j=1}^{N}t_{i,j}^{(0)}(x)(x^p-x)^j+\\&+\sum_{i=0}^{q-2}f^{\frac{i(p-1)}{q}}\sum_{j=1}^{N}(Dt_{i,j}^{(0)})(x^p-x)^j-q\sum_{i=0}^{q-2}f^{\frac{i(p-1)}{q}}\sum_{j=1}^{N}jt_{i,j}^{(0)}(x)(x^p-x)^{j-1}\end{aligned}$$

$$= \sum_{i=0}^{q-1} f^{\frac{i(p-1)}{q}} \sum_{j=1}^{N-1} \Big(Dr_j^{(0)} - qjr_{j+1}^{(0)} - (q-1)\frac{df}{dx} f^{-1} r_j^{(0)}\Big)(x^p-x)^{j-1} +$$
$$+ \sum_{i=0}^{q-1} f^{\frac{i(p-1)}{q}} \Big(Dr_N^{(0)} - (q-1)\frac{df}{dx} f^{-1} r_N^{(0)}\Big)(x^p-x)^{N-1} +$$
$$+ \sum_{i=0}^{q-2} f^{\frac{i(p-1)}{q}} \sum_{j=1}^{N-1} \Big(Dt_{i,j}^{(0)} - q(j+1)t_{i,j+1}^{(0)} - i\frac{df}{dx} f^{-1} t_{i,j}^{(0)} +$$
$$+ (q-1-i)\frac{df}{dx} f^{-1} r_{j+1}^{(0)}\Big)(x^p-x)^j + \sum_{i=0}^{q-2} f^{\frac{i(p-1)}{q}} \Big(Dt_{i,N}^{(0)} - i\frac{df}{dx} f^{-1} t_{i,N}^{(0)}\Big)\times$$
$$\times (x_p - x)^N + \sum_{i=0}^{q-2} f^{\frac{i(p-1)}{q}} \Big((q-1-i)\frac{df}{dx} f^{-1} r_1^{(0)} - qt_{i,1}^{(0)}\Big).$$

If we take

(2) $$qt_{i,1}^{(0)} = (q-1-i)\frac{df}{dx} f^{-1} r_1^{(0)}, \quad i = 0, 1, \ldots, q-2,$$

then $R_1(x)$ can be written in the form

$$R_1(x) = \sum_{i=0}^{q-1} f^{\frac{i(p-1)}{q}} \sum_{j=1}^{N} r_j^{(1)}(x)(x^p-x)^{j-1} + \sum_{i=0}^{q-2} f^{\frac{i(p-1)}{q}} \sum_{j=1}^{N} t_{i,j}^{(1)}(x)(x^p-x)^j,$$

where

(3) $$\begin{cases} r_j^{(1)} = Dr_j^{(0)} - qjr_{j+1}^{(0)} - (q-1)\dfrac{df}{dx} f^{-1} r_j^{(0)}, \quad j = 1, 2, \ldots, N-1, \\ r_N^{(1)} = Dr_N^{(0)} - (q-1)\dfrac{df}{dx} f^{-1} r_N^{(0)}, \\ t_{i,j}^{(1)} = Dt_{i,j}^{(0)} - q(j+1)t_{i,j+1}^{(0)} - i\dfrac{df}{dx} f^{-1} t_{i,j}^{(0)} + (q-1-i)\dfrac{df}{dx} f^{-1} r_{j+1}^{(0)}, \\ \qquad\qquad i = 0, 1, \ldots, q-2;\ j = 1, 2, \ldots, N-1, \\ t_{i,N}^{(1)} = Dt_{i,N}^{(0)} - i\dfrac{df}{dx} f^{-1} t_{i,N}^{(0)}, \quad i = 0, 1, \ldots, q-2. \end{cases}$$

Similarly, the relations

$$qt_{i,1}^{(1)} = (q-1-i)\frac{df}{dx} f^{-1} r_1^{(1)}, \quad i = 0, 1, \ldots, q-2,$$

are sufficient for $R_2(x)$ to have the form

$$R_2(x) = \sum_{i=0}^{q-1} f^{\frac{i(p-1)}{q}} \sum_{j=1}^{N} r_j^{(2)}(x)(x^p-x)^{j-1} + \sum_{i=0}^{q-2} f^{\frac{i(p-1)}{q}} \sum_{j=1}^{N} t_{i,j}^{(2)}(x)(x^p-x)^j.$$

We shall successively construct $R_k(x)$, $k = 1, 2, \ldots, N + \left[\frac{N-1}{q-1}\right]$ which differ from the corresponding derivatives of $R_0(x)$ by constant factors unequal to zero in k_p. If we take

(4) $$qt_{i,1}^{(k-1)} = (q-1-i)\frac{df}{dx} f^{-1} r_1^{(k-1)},$$
$$i = 0, 1, \ldots, q-2;\ k = 1, 2, \ldots, N + \left[\frac{N-1}{q-1}\right],$$

then $R_k(x)$ will be written in the form

$$R_k(x) = \sum_{i=0}^{q-1} f^{\frac{i(p-1)}{q}} \sum_{j=1}^{N} r_j^{(k)}(x)(x^p-x)^{j-1} + \sum_{i=0}^{q-2} f^{\frac{i(p-1)}{q}} \sum_{j=1}^{N} t_{i,j}^{(k)}(x)(x^p-x)^j,$$

where

(5) $$\begin{cases} r_j^{(k)} = Dr_j^{(k-1)} - qjr_{j+1}^{(k-1)} - (q-1)\dfrac{df}{dx} f^{-1} r_j^{(k-1)}, \quad i = 1, 2, \ldots, N-1, \\ r_N^{(k)} = Dr_N^{(k-1)} - (q-1)\dfrac{df}{dx} f^{-1} r_N^{(k-1)}, \\ t_{i,j}^{(k)} = Dt_{i,j}^{(k-1)} - q(j+1)t_{i,j+1}^{(k-1)} - i\dfrac{df}{dx} f^{-1} t_{i,j}^{(k-1)} + (q-1-i)\dfrac{df}{dx} f^{-1} r_{j+1}^{(k-1)}, \\ \qquad\qquad i = 0, 1, \ldots, q-2;\ j = 1, 2, \ldots, N-1, \\ t_{i,N}^{(k)} = Dt_{i,N}^{(k-1)} - i\dfrac{df}{dx} f^{-1} t_{i,N}^{(k-1)}, \quad i = 0, 1, \ldots, q-2. \end{cases}$$

In the following, such a form of $R_k(x)$ will be called "necessary".

The condition that $R_k(x)$, $k = 1, 2, \ldots, N$, has the "necessary" form allows us to find the connection between $t_{i,j}^{(0)}$ and $r_j^{(0)}$, $i = 0, 1, \ldots, q-2$; $j = 1, 2, \ldots, N$. We shall prove by induction on j that $q^j j!\, t_{i,j}^{(0)}$ will be present as linear forms

(6) $$q^j j!\, t_{i,j}^{(0)} = \sum_{l=1}^{j} F_{i,l}^{(j)} r_l^{(0)}, \quad i = 0, 1, \ldots, q-2;\ j = 1, 2, \ldots, N,$$

where the coefficients $F_{i,l}^{(j)}$ are rational functions. By (2) the result is obviously true for $j = 1$. In accordance with (3) we get changing j to $j-1$

$$t_{i,j-1}^{(1)} = Dt_{i,j-1}^{(0)} - qjt_{i,j}^{(0)} - i\frac{df}{dx} f^{-1} t_{i,j-1}^{(0)} + (q-1-i)\frac{df}{dx} f^{-1} r_j^{(0)},$$
$$i = 0, 1, \ldots, q-2.$$

By assumption of induction we have

$$q^{j-1}(j-1)!\, t^{(1)}_{i,j-1} = \sum_{l=1}^{j-1} F^{(j-1)}_{i,l} r^{(1)}_l, \qquad q^{j-1}(j-1)!\, t^{(0)}_{i,j-1} = \sum_{l=1}^{j-1} F^{(j-1)}_{i,l} r^{(0)}_l, \qquad i = 0, 1, \ldots, q-2.$$

Hence for $i = 0, 1, \ldots, q-2$, we have

$$q^j j!\, t^{(0)}_{i,j} = q^{j-1}(j-1)!\, Dt^{(0)}_{i,j-1} - q^{j-1}(j-1)!\, t^{(1)}_{i,j-1} - q^{j-1}(j-1)!\, i \frac{df}{dx} f^{-1} t^{(0)}_{i,j-1} + q^{j-1}(j-1)!\,(q-1-i)\frac{df}{dx} f^{-1} r^{(0)}_j$$
$$= D\sum_{l=1}^{j-1} F^{(j-1)}_{i,l} r^{(0)}_l - \sum_{l=1}^{j-1} F^{(j-1)}_{i,l} r^{(1)}_l - i\frac{df}{dx} f^{-1} \sum_{l=1}^{j-1} F^{(j-1)}_{i,l} r^{(0)}_l + q^{j-1}(j-1)!\,(q-1-i)\frac{df}{dx} f^{-1} r^{(0)}_j.$$

Expressing $r^{(1)}_1, r^{(1)}_2, \ldots, r^{(1)}_{j-1}$ in terms of $r^{(0)}_1, r^{(0)}_2, \ldots, r^{(0)}_j$ by (3) we get

$$q^j j!\, t^{(0)}_{i,j} = \sum_{l=1}^{j-1} (DF^{(j-1)}_{i,l}) r^{(0)}_l + \sum_{l=1}^{j-1} F^{(j-1)}_{i,l} Dr^{(0)}_l - \sum_{l=1}^{j-1} F^{(j-1)}_{i,l} Dr^{(0)}_l + q\sum_{l=1}^{j-1} l F^{(j-1)}_{i,l} r^{(0)}_{l+1} + (q-1)\frac{df}{dx} f^{-1} \sum_{l=1}^{j-1} F^{(j-1)}_{i,l} r^{(0)}_l -$$
$$- i\frac{df}{dx} f^{-1} \sum_{l=1}^{j-1} F^{(j-1)}_{i,l} r^{(0)}_l + q^{j-1}(j-1)!\,(q-1-i)\frac{df}{dx} f^{-1} r^{(0)}_j$$
$$= \left(q(j-1)F^{(j-1)}_{i,j-1} + q^{j-1}(j-1)!\,(q-1-i)\frac{df}{dx} f^{-1}\right) r^{(0)}_j + \sum_{l=1}^{j-1}\left(DF^{(j-1)}_{i,l} + q(l-1)F^{(j-1)}_{i,l-1} + (q-1-i)\frac{df}{dx} f^{-1} F^{(j-1)}_{i,l}\right) r^{(0)}_l.$$

Thus the result has been proved for all $i = 0, 1, \ldots, q-2$; $j = 1, 2, \ldots, N$ and furthermore

(7) $$F^{(j)}_{i,l} = DF^{(j-1)}_{i,l} + q(l-1)F^{(j-1)}_{i,l-1} + (q-1-i)\frac{df}{dx} f^{-1} F^{(j-1)}_{i,l},$$
$$i = 0, 1, \ldots, q-2;\ j = 1, 2, \ldots, N;\ l = 1, 2, \ldots, j-1,$$

(8) $$F^{(j)}_{i,j} = q(j-1)F^{(j-1)}_{i,j-1} + q^{j-1}(j-1)!\,(q-1-i)\frac{df}{dx} f^{-1},$$
$$i = 0, 1, \ldots, q-2;\ j = 1, 2, \ldots, N.$$

From (8) we get

(9) $$F^{(j)}_{i,j} = q^{j-1} j!\, F^{(1)}_{i,1}, \qquad i = 0, 1, \ldots, q-2;\ j = 1, 2, \ldots, N.$$

The condition, that $R_k(x)$ for $k = N+1, \ldots, N+\left[\frac{N-1}{q-1}\right]$ has the "necessary" form allows us to find the connection between $r^{(0)}_1, r^{(0)}_2, \ldots, r^{(0)}_N$. We have

$$q^N N!\, t^{(0)}_{i,N} = \sum_{j=1}^{N} F^{(N)}_{i,j} r^{(0)}_j, \qquad i = 0, 1, \ldots, q-2.$$

In a similar way

$$q^N N!\, t^{(1)}_{i,N} = \sum_{j=1}^{N} F^{(N)}_{i,j} r^{(1)}_j, \qquad i = 0, 1, \ldots, q-2.$$

But in view of (3)

$$t^{(1)}_{i,N} = Dt^{(0)}_{i,N} - i\frac{df}{dx} f^{-1} t^{(0)}_{i,N}, \qquad i = 0, 1, \ldots, q-2.$$

Hence we have for $i = 0, 1, \ldots, q-2$

$$D\sum_{j=1}^{N} F^{(N)}_{i,j} r^{(0)}_j = \sum_{j=1}^{N} F^{(N)}_{i,j} r^{(1)}_j + i\frac{df}{dx} f^{-1} \sum_{j=1}^{N} F^{(N)}_{i,j} r^{(0)}_j$$

or in accordance with (3)

$$\sum_{j=1}^{N} (DF^{(N)}_{i,j}) r^{(0)}_j + \sum_{j=1}^{N} F^{(N)}_{i,j} Dr^{(0)}_j = \sum_{j=1}^{N} F^{(N)}_{i,j} Dr^{(0)}_j - q\sum_{j=1}^{N} (j-1) F^{(N)}_{i,j-1} r^{(0)}_j - (q-1)\frac{df}{dx} f^{-1} \sum_{j=1}^{N} F^{(N)}_{i,j} r^{(0)}_j + i\frac{df}{dx} f^{-1} \sum_{j=1}^{N} F^{(N)}_{i,j} r^{(0)}_j;$$

that is

$$\sum_{j=1}^{N}\left(DF^{(N)}_{i,j} + q(j-1)F^{(N)}_{i,j-1} + (q-1-i)\frac{df}{dx} f^{-1} F^{(N)}_{i,j}\right) r^{(0)}_j = 0, \qquad i = 0, 1, \ldots, q-2.$$

We shall write it in the form

$$\sum_{j=1}^{N} F^{(N+1)}_{i,j} r^{(0)}_j = 0, \qquad i = 0, 1, \ldots, q-2,$$

where

$$F^{(N+1)}_{i,j} = DF^{(N)}_{i,j} + q(j-1)F^{(N)}_{i,j-1} + (q-1-i)\frac{df}{dx} f^{-1} F^{(N)}_{i,j},$$
$$i = 0, 1, \ldots, q-2;\ j = 1, 2, \ldots, N.$$

These relations are corollaries of the fact that $R_{N+1}(x)$ has the "necessary" form. If we demand that $R_{N+1}(x), \ldots, R_{N+\left[\frac{N-1}{q-1}\right]}(x)$ should have the "necessary" form, we shall get $(q-1)\left[\frac{N-1}{q-1}\right]$ analogous relations

$$(10)\qquad \sum_{j=1}^{N} F_{i,j}^{(k)} r_j^{(0)} = 0, \quad i = 0, 1, \ldots, q-2;\ k = N+1, \ldots, N+\left[\frac{N-1}{q-1}\right].$$

Find recurrence relations between $F_{i,j-1}^{(k)}, F_{i,j}^{(k)}$ and $F_{i,j}^{(k+1)}$. Applying the operator D to (10) for some $k, N+1 \leqslant k < N+\left[\frac{N-1}{q-1}\right]$, we get

$$(11)\qquad \sum_{j=1}^{N}(DF_{i,j}^{(k)}) r_j^{(0)} + \sum_{j=1}^{N} F_{i,j}^{(k)} Dr_j^{(0)} = 0, \quad i = 0, 1, \ldots, q-2.$$

Further

$$\sum_{j=1}^{N} F_{i,j}^{(k)} r_j^{(1)} = 0, \quad i = 0, 1, \ldots, q-2.$$

This gives by (3)

$$\sum_{j=1}^{N} F_{i,j}^{(k)} Dr_j^{(0)} - q\sum_{j=1}^{N}(j-1)F_{i,j-1}^{(k)} r_j^{(0)} - (q-1)\frac{df}{dx}f^{-1}\sum_{j=1}^{N} F_{i,j}^{(k)} r_j^{(0)} = 0,$$
$$i = 0, 1, \ldots, q-2.$$

Subtracting the last equalities from the corresponding equalities (11), we get

$$(12)\qquad \sum_{j=1}^{N}\left(DF_{i,j}^{(k)} + q(j-1)F_{i,j-1}^{(k)} + (q-1)\frac{df}{dx}f^{-1}F_{i,j}^{(k)}\right) r_j^{(0)} = 0,$$
$$i = 0, 1, \ldots, q-2.$$

At last subtracting the equalities

$$i\frac{df}{dx}f^{-1}\sum_{j=1}^{N} F_{i,j}^{(k)} r_j^{(0)} = 0, \quad i = 0, 1, \ldots, q-2,$$

from the corresponding equalities (12) we get

$$\sum_{j=1}^{N}\left(DF_{i,j}^{(k)} + q(j-1)F_{i,j-1}^{(k)} + (q-1-i)\frac{df}{dx}f^{-1}F_{i,j}^{(k)}\right) r_j^{(0)} = 0,$$
$$i = 0, 1, \ldots, q-2,$$

that is

$$(13)\qquad F_{i,j}^{(k+1)} = DF_{i,j}^{(k)} + q(j-1)F_{i,j-1}^{(k)} + (q-1-i)\frac{df}{dx}f^{-1}F_{i,j}^{(k)},$$

$$i = 0, 1, \ldots, q-2;\ j = 1, 2, \ldots, N;\ k = N, N+1, \ldots, N+\left[\frac{N-1}{q-1}\right]-1.$$

Find non-trivial solutions of the system (10) in polynomial $r_1^{(0)}, r_2^{(0)}, \ldots \ldots, r_N^{(0)}$. At first we prove by induction on k that

$$F_{i,j}^{(k)}, \quad i = 0, 1, \ldots, q-2;\ j = 1, 2, \ldots, N;\ k = 1, 2, \ldots, N+\left[\frac{N-1}{q-1}\right];\ j \leqslant k,$$

are rational functions of the type

$$(14)\qquad F_{i,j}^{(k)} = \frac{P_{i,j}^{(k)}}{f^{k-j+1}}$$

and that the degree of the polynomials $P_{i,j}^{(k)}$ does not exceed

$$(15)\qquad d_{i,j}^{(k)} = (k-j+1)(m-1).$$

This result is obviously true for $k = 1$ since by (2)

$$F_{i,1}^{(1)} = (q-1-i)\frac{df}{dx}f^{-1}, \quad i = 0, 1, \ldots, q-2.$$

By (9) the result is true for $k = j, j = 1, 2, \ldots, N$. By the assumption of induction we have for $i = 0, 1, \ldots, q-2;\ j = 1, 2, \ldots, k-2;\ j \leqslant N$, that

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

and we infer that the degrees of polynomials $P_{i,j}^{(k-1)}$ and $P_{i,j-1}^{(k-1)}$ do not exceed $(k-j)(m-1)$ and $(k-j+1)(m-1)$. But for $k \neq j$ by (7) and (13)

$$(16)\qquad F_{i,j}^{(k)} = DF_{i,j}^{(k-1)} + q(j-1)F_{i,j-1}^{(k-1)} + (q-1-i)\frac{df}{dx}f^{-1}F_{i,j}^{(k-1)},$$
$$i = 0, 1, \ldots, q-2;\ j = 1, 2, \ldots, k-1;\ j \leqslant N.$$

Further it is clear that

$$DF_{i,j}^{(k-1)} = \frac{Q_{i,j}^{(k-1)}}{f^{k-j+1}}, \quad i = 0, 1, \ldots, q-2;\ j = 1, 2, \ldots, k-1;\ j \leqslant N$$

and that the degree of the polynomial $Q_{i,j}^{(k-1)}$ does not exceed $(k-j+1)\times\times(m-1)$. In this case the result easily follows from (16). Then (14) shows that system (10) is equivalent to the following system

$$(17)\qquad \sum_{j=1}^{N}\bar{F}_{i,j}^{(k)} r_j^{(0)} = 0, \quad i = 0, 1, \ldots, q-2;\ k = N+1, \ldots, N+\left[\frac{N-1}{q-1}\right],$$

where

$$\bar{F}_{i,j}^{(k)} = f^{k-N}F_{i,j}^{(k)}.$$

We shall look for $r_j^{(0)}$ in the form

$$r_j^{(0)} = f^{N-j+1}\bar{r}_j^{(0)}, \quad j = 1, 2, \ldots, N. \tag{18}$$

Then system (17) turns into the system

$$\sum_{j=1}^{N} P_{i,j}^{(k)}\bar{r}_j^{(0)} = 0, \quad i = 0, 1, \ldots, q-2; \; k = N+1, \ldots, N+\left[\frac{N-1}{q-1}\right], \tag{19}$$

with polynomial coefficients $P_{i,j}^{(k)}$.

Let

$$P_{i,j}^{(k)} = \sum_{\mu=0}^{d_{i,j}^{(k)}} a_{i,j}^{(k,\mu)} x^{\mu},$$

$$i = 0, 1, \ldots, q-2; \; j = 1, 2, \ldots, N; \; k = N+1, \ldots, N+\left[\frac{N-1}{q-1}\right].$$

We shall look for $\bar{r}_j^{(0)}$, $j = 1, 2, \ldots, N$, in the form

$$\bar{r}_j^{(0)} = \sum_{\tau=0}^{e_j} b_j^{(\tau)} x^{\tau},$$

where $e_j = (N^2-N+j)(m-1)$. Then system (19) takes the form

$$\sum_{\varrho=0}^{d_{i,j}^{(k)}+e_j} \Big(\sum_{j=1}^{N} \sum_{\mu+\tau=\varrho} a_{i,j}^{(k,\mu)} b_j^{(\tau)}\Big) x^{\varrho} = 0,$$

$$i = 0, 1, \ldots, q-2; \; k = N+1, \ldots, N+\left[\frac{N-1}{q-1}\right].$$

Hence there are equalities

$$\sum_{j=1}^{N} \sum_{\tau=0}^{e_j} a_{i,j}^{(k,\varrho-\tau)} b_j^{(\tau)} = 0, \tag{20}$$

$$i = 0, 1, \ldots, q-2; \; k = N+1, \ldots, N+\left[\frac{N-1}{q-1}\right]; \; \varrho = 0, 1, \ldots, d_{i,j}^{(k)}+e_j.$$

In the last system there are

$$L = \sum_{j=1}^{N} (e_j+1)$$

variables $b_j^{(\tau)}$ and

$$M \leqslant \sum_{i=0}^{q-2} \sum_{k=N+1}^{N+\left[\frac{N-1}{q-1}\right]} (d_{i,j}^{(k)}+e_j+1)$$

equations. We have by (15)

$$L = (m-1)\sum_{j=1}^{N} (N^2-N+j)+N = (m-1)N^3 - \frac{m-1}{2}N^2 + \frac{m+1}{2}N,$$

$$M \leqslant (m-1)(q-1)\sum_{l=1}^{\left[\frac{N-1}{q-1}\right]} (N^2+l+1)+(q-1)\left[\frac{N-1}{q-1}\right]$$

$$\leqslant (m-1)N^3 - \frac{m-1}{2}N^2 + \frac{m+1}{2}N - m.$$

Thus $L-M \geqslant m$ and system (20) has non-trivial solutions in elements $b_j^{(\tau)}$ of k_p. It is clear from (6) and (18) that

$$t_{i,j}^{(0)}, \quad i = 0, 1, \ldots, q-2; \; j = 1, 2, \ldots, N$$

are also polynomials.

Further we note that the relations (6) and (10) are not only necessary but sufficient for $R_k(x)$, $k = 1, 2, \ldots, N+\left[\frac{N-1}{q-1}\right]$ to have the "necessary" form. Since all the $R_k(x)$, $k = 0, 1, \ldots, N+\left[\frac{N-1}{q-1}\right]$ have the "necessary" form, all the derivatives of order to $N+\left[\frac{N-1}{q-1}\right]$ inclusive of the polynomial $R_0(x)$ vanish at the points $\beta \in k_p$ for which the equation $y^n = f(\beta)$ is insolvable in k_p. To finish the proof of the lemma, we must show that the polynomial $R_0(x)$ is not identical to zero and estimate the degree of $R_0(x)$. Denote the degree of the polynomial $r_j^{(0)}$ by δ_j and the degree of the polynomial $t_{i,j}^{(0)}$ by $\gamma_{i,j}$. Since the degree of the polynomial $\bar{r}_j^{(0)}$ does not exceed $(N^2-N+j)(m-1)$, we infer from (18) that $\delta_j \leqslant N^2(m-1)+ +N+m-j$. Further, by (6) and (15), $\gamma_{i,j} \leqslant N^2(m-1)+N+m-j-1$ for all $i = 0, 1, \ldots, q-2$. Under the condition $p > 4m^2n(n-1)^2$, $N \leqslant \sqrt{p/2qm}$. Hence

$$\begin{aligned} &\delta_j + m \leqslant N^2(m-1)+N+2m-j < p/q, \quad j = 1, 2, \ldots, N, \\ &\gamma_{i,j} + m \leqslant N^2(m-1)+N+2m-j < p/q, \\ &\qquad i = 0, 1, \ldots, q-2; \; j = 1, 2, \ldots, N. \end{aligned} \tag{21}$$

The degree of the polynomial

$$\sum_{i=0}^{q-1} f^{\frac{i(p-1)}{q}} r_j^{(0)}(x)(x^p-x)^{j-1}$$

is equal to

$$\omega_j = \frac{(q-1)(p-1)}{q}m + \delta_j + p(j-1)$$

and the degree of the polynomial

$$f^{\frac{i(p-1)}{q}} t_{i,j}^{(0)}(x)(x^p-x)^j$$

is equal to

$$\nu_{i,j} = \frac{i(p-1)}{q}m+\gamma_{i,j}+pj.$$

Since $i \leqslant q-2$, $(m, q) = 1$, it follows from (21) that $\omega_j \neq \nu_{i,k}$ for any $= 0, 1, \ldots, q-2$; $j, k = 1, 2, \ldots, N$ and that $\omega_i > \omega_j$ for $i > j$ if $r_i^{(0)}(x)$, $r_j^{(0)}(x)$, $t_{i,k}^{(0)}(x)$ do not equal to zero. Hence the members

$$\sum_{i=0}^{q-1} f^{\frac{i(p-1)}{q}} r_j^{(0)}(x)(x^p-x)^{j-1}, \qquad f^{\frac{i(p-1)}{q}} t_{i,k}^{(0)}(x)(x^p-x)^k$$

in the polynomial $R_0(x)$ cannot be cancelled out. At last we estimate the degree of the polynomial $R_0(x)$. The degrees of polynomials

$$\sum_{i=0}^{q-1} f^{\frac{i(p-1)}{q}} r_j^{(0)}(x)(x^p-x)^{j-1}, \quad j = 1, 2, \ldots, N,$$

do not exceed

$$\frac{(q-1)(p-1)}{q}m+(m-1)N^2+(N-1)p+m$$

and the degrees of the polynomials

$$f^{\frac{i(p-1)}{q}} t_{i,j}^{(0)}(x)(x^p-x)^j, \quad i = 0, 1, \ldots, q-2;\ j = 1, 2, \ldots, N$$

do not exceed

$$\frac{(q-2)(p-1)}{q}m+(m-1)N^2+Np+m-1.$$

Hence the degree of $R_0(x)$ is at most

$$\frac{(q-1)(p-1)}{q}m+(m-1)N^2+Np+m.$$

Lemma 1 is fully proved.

LEMMA 2. *Let $q \geqslant 2$. For any natural $N \leqslant \frac{1}{q-1}\sqrt{\frac{p}{2qm}}$ there exists a polynomial $T_0(x)$, not identically equal to zero in k_p, of degree at most*

$$\frac{(q-1)(p-1)}{q}m+(m-1)(q-1)^2N^2+Np+m$$

such that all the elements of the first class are roots of polynomial $T_0(x)$ of order at least Nq.

Proof. We shall look for $T_0(x)$ in the form

$$T_0(x) = \sum_{i=1}^{q-1}\left(1-f^{\frac{i(p-1)}{q}}\right)\sum_{j=1}^{N} r_{i,j}^{(0)}(x)(x^p-x)^{j-1}+\sum_{j=1}^{N} t_j^{(0)}(x)(x^p-x)^j$$

where

$$r_{i,j}^{(0)}(x), \quad t_j^{(0)}(x), \quad i = 1, 2, \ldots, q-1;\ j = 1, 2, \ldots, N,$$

are indeterminate polynomial coefficients. Define $T_k(x)$ as

$$T_k(x) = D^k T_0(x), \quad k = 1, 2, \ldots$$

By analogy with Lemma 1 one can show that condition

$$qt_1^{(k-1)} = \frac{df}{dx}f^{-1}\sum_{i=1}^{q-1} ir_{i,1}^{(k-1)}$$

is sufficient for $T_k(x)$ to have the next form

$$T_k(x) = \sum_{i=1}^{q-1}\left(1-f^{\frac{i(p-1)}{q}}\right)\sum_{j=1}^{N} r_{i,j}^{(k)}(x)(x^p-x)^{j-1}+\sum_{j=1}^{N} t_j^{(k)}(x)(x^p-x)^j,$$

where

$$r_{i,j}^{(k)} = Dr_{i,j}^{(k-1)}-qjr_{i,j+1}^{(k-1)}-i\frac{df}{dx}f^{-1}r_{i,j}^{(k-1)},$$

$$i = 1, 2, \ldots, q-1;\ j = 1, 2, \ldots, N-1,$$

$$r_{i,N}^{(k)} = Dr_{i,N}^{(k-1)}-i\frac{df}{dx}f^{-1}r_{i,N}^{(k-1)}, \quad i = 1, 2, \ldots, q-1,$$

$$t_j^{(k)} = Dt_j^{(k-1)}-q(j+1)t_{j+1}^{(k-1)}+\frac{df}{dx}f^{-1}\sum_{i=1}^{q-1} ir_{i,j+1}^{(k-1)}, \quad j = 1, 2, \ldots, N-1,$$

$$t_N^{(k)} = Dt_N^{(k-1)}.$$

In the following such a form of $T_k(x)$ will be called "necessary".

As was done in Lemma 1, we can prove by induction on j, that if

$$(22) \qquad q^j j!\, t_j^{(0)} = \sum_{i=1}^{q-1}\sum_{l=1}^{j} F_{i,l}^{(j)} r_{i,l}^{(0)}, \quad j = 1, 2, \ldots, N,$$

then $T_k(x)$, $k = 1, 2, \ldots, N$, has the "necessary" form and, furthermore that

$$F_{i,l}^{(j)} = DF_{i,l}^{(j-1)}+q(l-1)F_{i,l}^{(j-1)}+i\frac{df}{dx}f^{-1}F_{i,l}^{(j-1)},$$

$$i = 1, 2, \ldots, q-1;\ j = 1, 2, \ldots, N;\ l = 1, 2, \ldots, j-1,$$

$$F_{i,j}^{(j)} = q(j-1)F_{i,j-1}^{(j-1)}+iq^{j-1}(j-1)!\frac{df}{dx}f^{-1},$$

$$i = 1, 2, \ldots, q-1;\ j = 1, 2, \ldots, N.$$

By analogy, the condition that $T_k(x)$, $k = N+1, \ldots, Nq-1$, has the "necessary" form gives

$$(23)\qquad \sum_{i=1}^{q-1}\sum_{j=1}^{N} F_{i,j}^{(k)} r_{i,j}^{(0)} = 0, \qquad k = N+1, \ldots, Nq-1,$$

where

$$F_{i,j}^{(k)} = DF_{i,j}^{(k-1)} + q(j-1)F_{i,j-1}^{(k-1)} + i\frac{df}{dx} f^{-1} F_{i,j}^{(k-1)},$$

$$i = 1, 2, \ldots, q-1;\ j = 1, 2, \ldots, N;\ k = N+1, \ldots, Nq-1.$$

Find a non-trivial solution of system (23) in polynomials $r_{i,j}^{(0)}$. It is easy to show by induction on k that $F_{i,j}^{(k)}$ are rational functions of type

$$(24)\qquad F_{i,j}^{(k)} = \frac{P_{i,j}^{(k)}}{f^{k-j+1}},$$

$$i = 1, 2, \ldots, q-1;\ j = 1, 2, \ldots, N;\ k = 1, 2, \ldots, Nq-1;\ j \leqslant k,$$

and that the degrees of polynomials $P_{i,j}^{(k)}$ do not exceed

$$(25)\qquad d_{i,j}^{(k)} = (k-j+1)(m-1).$$

It follows from (24) that system (23) is equivalent to the system

$$(26)\qquad \sum_{i=1}^{q-1}\sum_{j=1}^{N} \bar{F}_{i,j}^{(k)} r_{i,j}^{(0)} = 0, \qquad k = N+1, \ldots, Nq-1,$$

where

$$\bar{F}_{i,j}^{(k)} = f^{k-N} F_{i,j}^{(k)}.$$

We shall look for $r_{i,j}^{(0)}$ in the form

$$(27)\qquad r_{i,j}^{(0)} = f^{N-j+1}\bar{r}_{i,j}^{(0)}, \qquad i = 1, 2, \ldots, q-1;\ j = 1, 2, \ldots, N.$$

Then the system (26) turns into the system

$$(28)\qquad \sum_{i=1}^{q-1}\sum_{j=1}^{N} P_{i,j}^{(k)} \bar{r}_{i,j}^{(0)} = 0, \qquad k = N+1, \ldots, Nq-1,$$

with polynomial coefficients $P_{i,j}^{(k)}$. Let

$$P_{i,j}^{(k)} = \sum_{\mu=0}^{d_{i,j}^{(k)}} a_{i,j}^{(k,\mu)} x^{\mu},$$

$$i = 1, 2, \ldots, q-1;\ j = 1, 2, \ldots, N;\ k = N+1, \ldots, Nq-1.$$

We shall look for $\bar{r}_{i,j}^{(0)}$ in the form

$$\bar{r}_{i,j}^{(0)} = \sum_{\tau=0}^{e_{i,j}} b_{i,j}^{(\tau)} x^{\tau},$$

where $e_{i,j} = \big(N^2(q-1)^2 - N + j\big)(m-1)$.

Then system (28) is written in the form

$$\sum_{\varrho=0}^{d_{i,j}^{(k)}+e_{i,j}} \Big(\sum_{i=1}^{q-1}\sum_{j=1}^{N}\sum_{\mu+\tau=\varrho} a_{i,j}^{(k,\mu)} b_{i,j}^{(\tau)}\Big) x^{\varrho} = 0, \qquad k = N+1, \ldots, Nq-1.$$

Hence we have the equalities

$$(29)\qquad \sum_{i=1}^{q-1}\sum_{j=1}^{N}\sum_{\tau=0}^{e_{i,j}} a_{i,j}^{(k,\varrho-\tau)} b_{i,j}^{(\tau)} = 0,$$

$$k = N+1, \ldots, Nq-1;\ \varrho = 0, 1, \ldots, d_{i,j}^{(k)} + e_{i,j}.$$

In the last system there are

$$L = \sum_{i=1}^{q-1}\sum_{j=1}^{N} (e_{i,j}+1)$$

variables $b_{i,j}^{(\tau)}$ and

$$M \leqslant \sum_{k=N+1}^{Nq-1} (d_{i,j}^{(k)} + e_{i,j} + 1)$$

equations. We have by (25)

$$L = (m-1)(q-1)\sum_{j=1}^{N}\big(N^2(q-1)^2 - N + j\big) + (q-1)N$$

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

$$M \leqslant (m-1)\sum_{l=1}^{N(q-1)-1}\big(N^2(q-1)^2 + l + 1\big) + N(q-1)$$

$$\leqslant (m-1)(q-1)^3 N^3 - \frac{(m-1)(q-1)}{2} N^2 + \frac{(m+1)(q-1)}{2} N - m.$$

Thus $L - M \geqslant m$ and the system (29) has a non-trivial solution in elements $b_{i,j}^{(\tau)}$ of k_p. If follows from (22) and (27) that $t_j^{(0)}$, $j = 1, 2, \ldots, N$, are also polynomials. Since all the $T_k(x)$, $k = 0, 1, \ldots, Nq-1$, have the "necessary" form, all the derivatives of order up to $Nq-1$ inclusive of the polynomial $T_0(x)$ vanish at the points $a \in k_p$ for which $f(a) \neq 0$, and equation $y^n = f(a)$ is solvable in k_p.

An argument similar to that used in Lemma 1 proves that $T_0(x)$ is not identically equal to zero.

At last we estimate the degree of the polynomial $T_0(x)$. The degrees of the polynomials

$$\big(1 - f^{\frac{i(p-1)}{q}}\big) r_{i,j}^{(0)}(x)(x^p - x)^{j-1}, \qquad i = 1, 2, \ldots, q-1;\ j = 1, 2, \ldots, N,$$

do not exceed

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

and the degrees of the polynomials

$$t_j^{(0)}(x)(x^p-x)^j,\quad j=1,2,\ldots,N,$$

do not exceed

$$(m-1)(q-1)^2N^2+Np+m-1.$$

Hence the degree of the polynomial $T_0(x)$ is at most

$$\frac{(q-1)(p-1)}{q}m+(m-1)(q-1)^2N^2+Np+m.$$

Thus the proof of Lemma 2 is finished.

3. Let us prove the theorem. If $q=1$, then it is easy to see that $I_p=p$ and hence in this case the theorem is true.

Let $q\geqslant 2$. Since the number of roots of a polynomial does not exceed the degree of that polynomial, the inequality

$$\left(N+\left[\frac{N-1}{q-1}\right]+1\right)I_{-1}\leqslant\frac{(q-1)(p-1)}{q}m+Np+(m-1)N^2+m$$

follows from Lemma 1. Since

$$N+\left[\frac{N-1}{q-1}\right]+1\geqslant N+\frac{N}{q-1}$$

we get

$$\left(N+\frac{N}{q-1}\right)I_{-1}<Np+mp+(m-1)N^2$$

or

$$\left(N+\frac{N}{q-1}\right)\left(p-\frac{I_p-I_0}{q}-I_0\right)<Np+mp+(m-1)N^2.$$

But $I_0\leqslant m$. Hence

$$I_p>p-(q-1)m-\frac{(q-1)mp}{N}-(m-1)(q-1)N.$$

Take $N=\left[\sqrt{\frac{p}{2qm}}\right]$. Then

$$I_p>p-\sqrt{2qm}\,2qm\sqrt{p}.$$

By Lemma 2

$$NqI_{+1}\leqslant\frac{(q-1)(p-1)}{q}m+Np+(m-1)(q-1)^2N^2+m,$$

or

$$N(I_p-I_0)<Np+mp+(m-1)(q-1)^2N^2.$$

Hence

$$I_p<p+m+\frac{mp}{N}+(m-1)(q-1)^2N.$$

Take $N=\left[\frac{1}{q-1}\sqrt{\frac{p}{2qm}}\right]$. Then

$$I_p<p+\sqrt{2qm}\,2qm\sqrt{p}.$$

Therefore

$$|I_p-p|<\sqrt{2qm}\,2qm\sqrt{p},$$

and thus the theorem is fully proved.

References

[1] С. А. Степанов, *О числе точек гиперэллиптической кривой над простым конечным полем*, Изв. АН СССР, сер. мат., 33 (5) (1969), pp. 1171–1181.

[2] H. Hasse, *Abstrakte Begründung der komplexen Multiplikation und Riemannsche Vermutung in Funktionenkörpern*, Abh. Math. Sem., Hamburg, 10 (1934), pp. 325–348.

[3] Ю. И. Манин, *О сравнениях третьей степени по простому модулю*, Изв. АН СССР, сер. мат., 20 (1956), pp. 673–678.

[4] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Act. Sci. Ind. 1041, Paris 1948.

Received on 9. 7. 1969