Publ. Math. Debrecen
68/1-2 (2006), 15–23

On the solvability of some special equations over finite fields

By BÁLINT FELSZEGHY (Budapest)

Abstract. Let F be a polynomial over $\mathbb{F}_p$ with n variables and of degree d. Suppose that it is impossible to transform F by invertible homogeneous linear change of variables to a polynomial, which has less than n variables. Also suppose that the degree of F in each variable is less than p. Rédei conjectured that if $d \le n$ then $F = 0$ has at least one solution in $\mathbb{F}_p$. This was disproved in [5] by a collection of counterexamples, but the cases $\deg F = 3$ and $\deg F = 5$ remained open. We give a counterexample with $\deg F = 5$ over $\mathbb{F}_{11}$. On the positive side, we prove the statement for symmetric polynomials of degree 3.

Along a related line, consider polynomials of the form $F(x_1, \dots, x_n) = a_1x_1^k + \dots + a_nx_n^k + g(x_1, \dots, x_n)$, where $a_1a_2 \dots a_n \ne 0$, $g \in \mathbb{F}_p[x_1, \dots, x_n]$ and $\deg g < k$. We will show, that if $n \ge \left\lceil \frac{p-1}{\lfloor \frac{p-1}{k} \rfloor} \right\rceil$, then the equation $F(x_1, \dots, x_n) = 0$ is solvable in ${\mathbb{F}_p}^n$. This is a generalization of a result of Carlitz ([2]).

1. Introduction

In 1946 László Rédei formulated a conjecture (see [4]) about the solvability of polynomial equations over finite fields. Although it turned out that there are counterexamples, for some special polynomials the conjecture holds. We give first a brief overview of the related results.

Mathematics Subject Classification: 11T06, 11D79.
Key words and phrases: finite fields, equations, solvability.
Research supported in part by OTKA and NWO-OTKA grants, and the EU-COE Grant of MTA SZTAKI.

Let p be a prime, $\mathbb{F}_p$ be a field with p elements and $F(x_1, \dots, x_n) \in \mathbb{F}_p[x_1, \dots, x_n]$ be a polynomial, with n variables. We can assume that the degree of F in x_i is at most $p-1$ for $1 \le i \le n$, that is the polynomial is *reduced*. We denote the linear subspace (in the space of polynomials with n variables over $\mathbb{F}_p$) spanned by the partial derivates of F by V, so we put $V = \mathrm{Lin}\left\{\frac{\partial F}{\partial x_i} : 1 \le i \le n\right\}$. The *rank* of F is defined to be $\dim_{\mathbb{F}_p} V$.

We note that the original definition of rank in [4] is different. We will use that $\operatorname{rank} F$ is precisely the least positive integer r for which there exists an invertible homogeneous linear change of variables which carries F into a polynomial with r variables. The equivalence to the original notion can be found in [5]. With this notion of the rank, the conjecture is the following:

Rédei's Conjecture. *Let $F \in \mathbb{F}_p[x_1, \dots, x_n]$ be reduced, not constant and $\deg F \le \operatorname{rank} F$. Then $F(x_1, \dots, x_n) = 0$ is solvable.*

In [5] Rónyai disproved this by giving counterexamples. Let $c \in \mathbb{F}_p$ $(p \ge 5)$ be a quadratic nonresidue, and $F(x_1, \dots, x_n) = \left(\sum_{i=1}^n x_i^2\right)^2 - c$. It is clear, that $F = 0$ cannot be solvable in $\mathbb{F}_p$. In the case $n \ge 4$, F serves as a counterexample to the conjecture, as it is not difficult to see that $n = \operatorname{rank} F$. A similar polynomial can be constructed for $p = 3$. (The conjecture is true if $p = 2$.) There are counterexamples for every degree $d \ge 6$.

It is pointed out in [5] that the conjecture is valid for degrees 1 (this case is trivial) and 2. The remaining cases ($\deg F = 3$ or 5) are still open. In Section 2 we show a counterexample for $\deg F = 5$ and $p = 11$, and, as a positive result, we prove the conjecture for cubic symmetric polynomials. We note that the counterexample given above for $\deg F = 4$ is symmetric.

Rédei's conjecture holds also for some equations of diagonal type, see [5]. We prove the conjecture in Section 3 for a class of generalized diagonal polynomials.

2. The cases of degree 3 and 5

Proposition 1. *Let $n > 5$ be an integer, and let F be the polynomial over $\mathbb{F}_{11}$:*

$$F(x_1, \dots, x_n) = x_1^5 + \left(x_2^2 + x_3^2 + \cdots + x_n^2\right)^2 - 7.$$

Then $\deg F = 5$, $\operatorname{rank} F = n$, but $F(x_1, \dots, x_n) = 0$ has no solutions in $\mathbb{F}_{11}^n$, so Rédei's conjecture is not true for degree 5 in general.

Proof. Consider the polynomial $f(x, y) = x^5 + y^2 - 7$. Since in $\mathbb{F}_{11}$ $x^5 \in \{-1, 0, 1\}$ and $y^2 \in \{0, 1, 3, 4, 5, 9\}$, $x^5 + y^2$ never equals 7. So $f = 0$ has no solutions, and hence nor has $F = 0$.

It remains to show that $\operatorname{rank} F = n$, that is the partial derivates of F are linearly independent. Indeed, suppose that $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{F}_{11}$ and $0 = \sum_{i=1}^n \alpha_i \frac{\partial F}{\partial x_i}$. For a fixed j, we can regard $\sum_{i=1}^n \alpha_i \frac{\partial F}{\partial x_i}$ as a polynomial in x_j (over the extension field $\mathbb{F}_p(x_1, \dots, x_{j-1}, x_{j+1}, \dots, x_n)$), so it can be 0 for all x_j only if each coefficient of x_j^l is zero. Since

$$\sum_{i=1}^n \alpha_i \frac{\partial F}{\partial x_i} = 5\alpha_1 x_1^4 + 4\left(x_2^2 + x_3^2 + \cdots + x_n^2\right) \sum_{i=2}^n \alpha_i x_i,$$

the coefficient of x_1^4 is $5\alpha_1$, so $\alpha_1 = 0$. Thus we have

$$0 = 4\left(x_2^2 + x_3^2 + \cdots + x_n^2\right) \sum_{i=2}^n \alpha_i x_i$$

and $0 = \sum_{i=2}^n \alpha_i x_i$. This can happen only if $\alpha_i = 0$ $(2 \le i \le n)$, which means that $\operatorname{rank} F = n$. $\square$

On the positive side, we prove the conjecture for symmetric cubic polynomials. We are only interested in reduced polynomials, so for the remaining part of this section we suppose that $p \ge 5$. We denote the rth elementary symmetric function in variables $x_1, \dots, x_n$ by σ_r for $1 \le r \le n$.

Proposition 2. *If $F(x_1, \dots, x_n)$ is a symmetric polynomial of degree 3, then there exists a uniquely determined polynomial f in $\mathbb{F}_p[y_1, y_2, y_3]$ of the form*

$$f(y_1, y_2, y_3) = a y_3 + y_2(b y_1 + c) + g(y_1),$$

with a, b, $c \in \mathbb{F}_p$ and $g(y_1) \in \mathbb{F}_p[y_1]$, $\deg g \le 3$, such that $F(x_1, \dots, x_n) = f(\sigma_1, \sigma_2, \sigma_3)$.

Proof. The fundamental theorem of symmetric polynomials yields that there exists a uniquely determined $f_1(y_1,\dots,y_n) \in \mathbb{F}_p[y_1,\dots,y_n]$, such that $F(x_1,\dots,x_n) = f_1(\sigma_1,\dots,\sigma_n)$. The algebraic independence of σ_i implies that if $y_1^{k_1}y_2^{k_2}\dots y_n^{k_n}$ is a monomial of f_1 with nonzero coefficient, then F has nonzero terms, with degree $\sum_{i=1}^n ik_i$. It follows from $degF = 3$ that the only products with nonzero coefficients in f_1 can be y_3, y_2y_1, y_2, y_1^3, y_1^2, y_1, 1, thus $f(y_1,y_2,y_3) := f_1(y_1,\dots,y_n)$ completes the proof. □

The main part of the next statement is a corollary of Hasse's Theorem (see [6] or Hasse's original paper [3]) on elliptic curves over finite fields.

Proposition 3. *Let $p \geq 5$, and $h(x)$ be a polynomial in $\mathbb{F}_p[x]$, and suppose that $1 \leq \deg h \leq 3$. Then the equation $y^2 = h(x)$ is always solvable in ${\mathbb{F}_p}^2$.*

Proof. If $\deg h \leq 2$, then $y^2 - h(x)$ is a polynomial with rank 2, so it has a root in ${\mathbb{F}_p}^2$.

Suppose that $\deg h = 3$. If $x_0 \in \mathbb{F}_p$ is a root of h, then $(x_0, 0)$ is a solution of the above equation. If h has no roots in $\mathbb{F}_p$, then h is irreducible, and so h has three distinct roots (in $\mathbb{F}_{p^3}$), which means that $y^2 = h(x)$ is an equation of a (nonsingular) elliptic curve over $\mathbb{F}_p$. Hasse's Theorem yields that for the number E of the projective points of the curve the inequality $|E - (p+1)| \leq 2\sqrt{p}$ holds. Consequently $E \geq p+1-2\sqrt{p}$, which is greater than one, if p is greater than 4, and so the curve has at least 2 projective points. Since an elliptic curve with equation of type $y^2 = h(x)$ has exactly one point at infinity, this proves the statement. □

We apply the two propositions above to prove Rédei's conjecture for cubic symmetric polynomials.

Theorem 4. *Let $p \geq 5$, and $F(x_1,\dots,x_n)$ be a symmetric polynomial over $\mathbb{F}_p$ of degree 3 with $\operatorname{rank} F \geq 3$. Then $F(x_1,\dots,x_n) = 0$ has a solution in ${\mathbb{F}_p}^n$.*

Proof. It suffices to show the statement for $n = 3$. Using Proposition 2 we obtain that $F(x_1,x_2,x_3) = a\sigma_3 + \sigma_2(b\sigma_1 + c) + g(\sigma_1)$. Finding a root for F is equivalent to find a solution (in x_1, x_2, x_3, y_1, y_2, y_3) for the following system of equations:

$$ay_3 + y_2(by_1 + c) + g(y_1) = 0 \tag{1}$$
$$x_1 + x_2 + x_3 = y_1 \tag{2}$$
$$x_1x_2 + x_1x_3 + x_2x_3 = y_2 \tag{3}$$
$$x_1x_2x_3 = y_3. \tag{4}$$

By (2), we eliminate first x_1 from (3) and (4).

$$(y_1 - (x_2 + x_3))(x_2 + x_3) + x_2x_3 = y_2 \tag{3$'$}$$

$$(y_1 - (x_2 + x_3))x_2x_3 = y_3. \tag{4$'$}$$

From (1), ($3'$) and ($4'$) we infer

$$\begin{aligned} &a(y_1 - (x_2 + x_3))x_2x_3 \\ &\qquad + ((y_1 - (x_2 + x_3))(x_2 + x_3) + x_2x_3)\,(by_1 + c) + g(y_1) = 0. \end{aligned} \tag{5}$$

It is obvious that (5) is solvable iff the initial system of equations has a solution. Now let $u = x_2 + x_3$, $v = x_2x_3$ and $y = y_1$. With these variables (5) takes the form

$$a(y - u)v + ((y - u)u + v)(by + c) + g(y) = 0.$$

Thus we have

$$\frac{(y - u)u(by + c) + g(y)}{(a + b)y - au + c} = -v. \tag{6}$$

Since rank $F = 3$, at least one of a, b and c is nonzero, so $(a+b)y - au + c$ is not identically 0. If we can solve (6) then x_2 and x_3 have to be the two roots of the polynomial $x^2 - ux + v$. So precisely those solutions of (6) are satisfactory for which $\left(\frac{u}{2}\right)^2 - v = z^2$ is solvable. Together, we have the equation

$$\frac{(y - u)u(by + c) + g(y)}{(a + b)y - au + c} + \left(\frac{u}{2}\right)^2 = z^2. \tag{7}$$

to solve. Let $d \in \mathbb{F}_p$ be 1 or 2. If $a \neq 0$ then choose $u = \frac{1}{a}\left((a + b)y + c - d\right)$. If $a = 0$, but $b \neq 0$ then choose $y = \frac{1}{b}\left(d - c\right)$. In both cases the denominator of (6) becomes d, so the left hand side of (7) is a polynomial h in one indeterminate (y or u) of degree at most 3. It is clear, that for $d = 1$ or $d = 2$ h is not constant. If $a = b = 0$, then choose $u = 1$ or $u = 0$ according as g is constant or not, respectively.

So finally we have an equation of the form $z^2 = h(u)$, and application of Proposition 3 completes the proof. □

3. Generalized diagonal equations

In this section we give some more positive examples. We consider polynomials $F(x_1, \dots, x_n) \in \mathbb{F}_p[x_1, \dots, x_n]$ of form

$$F(x_1, \dots, x_n) = \sum_{i=1}^{n} a_i x_i^k + g(x_1, \dots, x_n),$$

where p is a prime, $\mathbb{F}_p$ is the field with p elements, $1 \leq k \leq p-1$, $a_1, \dots, a_n \in \mathbb{F}_p$, $a_1 a_2 \dots a_n \neq 0$ and $g(x_1, \dots, x_n) \in \mathbb{F}_p[x_1, \dots, x_n]$ is an arbitrary polynomial with $\deg g < k$. Then we call F a generalized diagonal polynomial. Our goal is to prove the following theorem.

Theorem 5. *Suppose that* $n \geq \left\lceil \frac{p-1}{\lfloor \frac{p-1}{k} \rfloor} \right\rceil$. *Then* $F(x_1, \dots, x_n) = \sum_{i=1}^{n} a_i x_i^k + g(x_1, \dots, x_n) = 0$ *is solvable in* ${\mathbb{F}_p}^n$.

To compare this to Rédei's conjecture, we observe that if $k = 1$ then $\operatorname{rank} F = 1$, otherwise we have $\operatorname{rank} F = n$. Indeed, put

$$F_i(x_1, \dots, x_n) := \frac{\partial F}{\partial x_i}(x_1, \dots, x_n) = k a_i x_i^{k-1} + \frac{\partial g}{\partial x_i}(x_1, \dots, x_n).$$

Suppose that there exist some α_i such that $\sum_{i=1}^{n} \alpha_i F_i(x_1, \dots, x_n) = 0$ holds for all $(x_1, \dots, x_n) \in {\mathbb{F}_p}^n$. Since $\deg \frac{\partial g}{\partial x_i} < k-1$, the coefficient of x_j^{k-1} is $\alpha_j k a_j$, hence $\alpha_j = 0$ for each j, which means that the F_i are linearly independent, and $\operatorname{rank} F = n$.

Rédei's conjecture predicts that there is a solution $(x_1, \dots, x_n) \in {\mathbb{F}_p}^n$ for $F(x_1, \dots, x_n) = 0$, in case $n \geq k$. We cannot prove this in general, but if $k | p-1$, then this is an immediate consequence of Theorem 5. Carlitz proved this special case in [2] in a way different from ours. It could happen that for a fixed p and k there would be polynomials $g_n(x_1, \dots, x_n)$, such that $F_n(x_1,\dots,x_n) = \sum_{i=1}^n a_{n,i}x_i^k + g_n(x_1,\dots,x_n)$ and none of the F_n-s have solution, however big n we would choose. Theorem 5 shows that it is impossible by presenting an upper bound $\le p-1$ for n.

Now recall a consequence of ALON's Combinatorial Nullstellensatz, that can be found in [1].

Theorem 6. *Let $G(x_1,\dots,x_n) \in \mathbb{F}_p[x_1,\dots,x_n]$ be a polynomial, assume that $\deg G = \sum_{i=1}^n t_i \ge 1$, the coefficient of $\prod_{i=1}^n x_i^{t_i}$ is not 0, and $0 \le t_i \le p-1$ for each i. Choose for all i an arbitrary $S_i \subseteq \mathbb{F}_p$ with $|S_i| = t_i + 1$. Then G cannot be constant on $S_1 \times S_2 \times \dots \times S_n$.*

Theorem 6 allows a simple proof of Theorem 5.

PROOF OF THEOREM 5. We can assume that $n = \left\lceil \frac{p-1}{\lfloor \frac{p-1}{k} \rfloor} \right\rceil$, because otherwise we can get a similar polynomial in $\left\lceil \frac{p-1}{\lfloor \frac{p-1}{k} \rfloor} \right\rceil$ variables by substituting zeros in place of some x_i. Let $G(x_1,\dots,x_n) = F(x_1,\dots,x_n)^{p-1}$. We intend to show, using Alon's Theorem, that G is not constant on $\mathbb{F}_p^{\,n}$. Since the value of $G(x_1,\dots,x_n)$ can be either 0 or 1, this will imply that there exists a root of G. Let

$$t_i = \left\lfloor \frac{p-1}{k} \right\rfloor k \quad \text{for } 1 \le i \le n-1 \quad \text{and}$$

$$t_n = (p-1)\,k - (n-1)\left\lfloor \frac{p-1}{k} \right\rfloor k.$$

It is obvious that $0 \le t_i \le p-1$ for all $1 \le i \le n-1$ and $\sum_{i=1}^n t_i = (p-1)k = \deg G$. The following simple calculation

$$t_n = (p-1)\,k - \left(\left\lceil \frac{p-1}{\left\lfloor \frac{p-1}{k} \right\rfloor} \right\rceil - 1 \right) \left\lfloor \frac{p-1}{k} \right\rfloor k$$

$$\le (p-1)\,k - \left(\frac{p-1}{\left\lfloor \frac{p-1}{k} \right\rfloor} - 1 \right) \left\lfloor \frac{p-1}{k} \right\rfloor k = \left\lfloor \frac{p-1}{k} \right\rfloor k \le p-1 \quad \text{and}$$

$$t_n > (p-1)\,k - \frac{p-1}{\left\lfloor \frac{p-1}{k} \right\rfloor} \left\lfloor \frac{p-1}{k} \right\rfloor k = 0$$

gives that t_n is also suitable.

In G there is a monomial $m = \prod_{i=1}^n x_i^{t_i}$ contributed by $\left(\sum_{i=1}^k a_i x_i^k\right)^{p-1}$, since $x_i^{t_i} = (x_i^k)^{\left\lfloor \frac{p-1}{k} \right\rfloor}$, and $x_n^{t_n} = (x_n^k)^{p-1-(n-1)\left\lfloor \frac{p-1}{k} \right\rfloor}$. The coefficient of m is

$$\frac{(p-1)!}{\prod_{i=1}^n \frac{t_i}{k}!} \prod_{i=1}^n a_i^{\frac{t_i}{k}} \neq 0.$$

The conditions of Theorem 6 are satisfied. G is not constant, hence there exists an $(x_1, \dots, x_n) \in \mathbb{F}_p{}^n$ such that $G(x_1, \dots, x_n) = 0$, and equivalently $F(x_1, \dots, x_n) = 0$. The theorem is proved. $\square$

If $k \mid p-1$ then the statement is also true in an arbitrary finite field.

Theorem 7. *Assume that $q = p^r$ is a prime power. If k divides $p-1$, $n \geq k$ and $F(x_1, \dots, x_n) = \sum_{i=1}^n x_i^k + g(x_1, \dots, x_n)$ then the equation $F(x_1, \dots, x_n) = 0$ is solvable in $\mathbb{F}_q{}^n$.*

Proof. In the preceding proof we used only once that p is a prime, namely when we stated that the corresponding coefficient is not zero. Using $k|p-1$ we can easily verify that $\frac{(q-1)!}{((q-1)/k)!^k} \neq 0$ in $\mathbb{F}_q$. The largest power of p which divides the numerator is

$$\sum_{i=1}^{\infty} \left\lfloor \frac{p^r - 1}{p^i} \right\rfloor = \sum_{i=1}^{r-1} \left\lfloor p^{r-i} - \frac{1}{p^i} \right\rfloor = \sum_{i=1}^{r-1} \left(p^{r-i} - 1\right).$$

This is the same for the denominator. Indeed

$$k \sum_{i=1}^{\infty} \left\lfloor \frac{\frac{p^r-1}{k}}{p^i} \right\rfloor = k \sum_{i=1}^{r-1} \left\lfloor \frac{p^{r-i} - 1}{k} + \frac{p^i - 1}{p^i k} \right\rfloor$$

$$= k \sum_{i=1}^{r-1} \frac{p^{r-i} - 1}{k} = \sum_{i=1}^{r-1} \left(p^{r-i} - 1\right).$$

The second to the last equality holds since $0 < \frac{p^i - 1}{p^i k} < 1$ and $k \mid p-1$ implies that $\frac{p^{r-i}-1}{k}$ is an integer. $\square$

References

[1] N. Alon, Combinatorial Nullstellensatz, *Combinatorics, Probability and Computing* **8** (1–2) (1999), 7–29.

[2] L. Carlitz, Solvabillity of certain equations in a finite field, *Quart. J. Math.* (2) **7** (1956), 3–4.

[3] H. Hasse, Zur Theorie der abstrakten elliptischen Funktionenkörper, *J. Reine Angew. Math.* **175** (1936), 55–62, 69–88, 193–208.

[4] L. Rédei, Zur Theorie der Gleichungen in endlichen Körpern, *Acta Univ. Szeged Sect. Sci. Math.* **11** (1946), 63–70.

[5] L. Rónyai, On a conjecture of László Rédei, *Acta Univ. Szeged Sect. Sci. Math.* (*to appear*).

[6] J. H. Silverman, The Arithmetic of Elliptic Curves, *Springer-Verlag*, 1986, 131.

BÁLINT FELSZEGHY
DEPARTMENT OF ALGEBRA
BUDAPEST UNIVERSITY OF TECHNOLOGY AND ECONOMY
H-1111 BUDAPEST, P.O. BOX 91
HUNGARY
AND
HUNGARIAN ACADEMY OF SCIENCES
COMPUTER AND AUTOMATION RESEARCH INSTITUTE
HUNGARY

E-mail: fbalint@math.bme.hu

(Received May 5, 2003; revised April 21, 2005)