On a conjecture of László Rédei

Lajos Rónyai
Computer and Automation Institute
Hungarian Academy of Sciences
H-1111 Budapest, Lágymányosi u. 11.
lajos@csillag.sztaki.hu
and
Budapest University of Technology and Economics

April 30, 2003

Abstract

Let p be a prime, and $F(x_1, x_2, \ldots, x_n) \in \mathbb{F}_p[x_1, \ldots, x_n]$ be a non-constant polynomial such that the degree of F in each variable x_i is at most $p-1$. The *rank* of F is the least integer r for which there exists an invertible homogeneous linear change of variables which carries F into a polynomial with precisely r variables. In [6] Rédei proposed the following conjecture: if the rank of F is at least $\deg F$, then the equation (congruence) $F(x_1, \ldots, x_n) = 0$ has a solution in ${\mathbb{F}_p}^n$.

We disprove the conjecture by giving counterexamples. On the other hand, we show that it holds for some important special cases, including generalized diagonal equations.

Keywords. Finite fields, equations, solvability.

AMS Subject Classification (2000): 11T06, 11D79.

---

[0]Research supported in part by OTKA and NWO-OTKA grants, and the EU-COE Grant of MTA SZTAKI.

1 Introduction

At the memorial conference held on the 100th anniversary of László Rédei's birth (Szeged, November 17-19, 2000) Laci Márki gave a memorable lecture on Rédei's rich, colorful and momentous work on rings and polynomials. There he discussed the following problem related to polynomial equations, which appeared in [6].

Let $\mathbb{F}_p$ be a finite prime field and $F(x_1, x_2, \ldots, x_n) \in \mathbb{F}_p[x_1, \ldots, x_n]$ be a polynomial. We assume that F is *reduced* in the sense that the degree of F in each variable x_i is at most $p-1$. The *rank* of F is the least integer r for which there exists an invertible homogeneous linear change of variables carrying F into a polynomial with precisely r variables. We assume that the coefficients of the substitutions (linear forms) are from the the algebraic closure $\mathbb{F}$ of $\mathbb{F}_p$. (For reduced polynomials the rank over $\mathbb{F}$ is the same as the rank over $\mathbb{F}_p$, see Proposition 2.1 below.)

In [6] the following conjecture is formulated.

Let $F(x_1, x_2, \ldots, x_n) \in \mathbb{F}_p[x_1, \ldots, x_n]$ be a nonconstant reduced polynomial of rank r and with $\deg F \leq r$. Then the equation

$$F(x_1, \ldots, x_n) = 0 \tag{1}$$

has a solution $(a_1, \ldots, a_n)$ in ${\mathbb{F}_p}^n$.

In this note we give a counterexample to the conjecture. For every prime $p > 2$ and integer $r > 0$ we give a reduced polynomial $F \in \mathbb{F}_p[x_1, \ldots, x_n]$ with degree 4 and rank r such that (1) has no solution with coordinates from $\mathbb{F}_p$.

Reading [6] gives the impression that Rédei formulated the conjecture on the basis of considerations involving diagonal equations, i.e., when F is of the form $c + \sum a_i x_i^{d_i}$, with $c, a_i \in \mathbb{F}_p$ and positive integers d_i. On the affirmative side, we prove the conjecture for generalized diagonal equations and for smooth cubic surfaces.

2 Examples

First we give a characterization of the rank in terms of the partial derivatives of F.

Proposition 2.1 *Let p be a prime, $F(x_1, \ldots, x_n) \in \mathbb{F}_p[x_1, \ldots, x_n]$ be a reduced polynomial. Then the rank of F (over any field containing $\mathbb{F}_p$) is the dimension of the $\mathbb{F}_p$-space spanned by the partial derivatives*

$$F_i := \frac{\partial F}{\partial x_i} \quad (1 \leq i \leq n).$$

Proof. Let $\mathbb{K} \supseteq \mathbb{F}_p$ be a field and

$$l_i = a_{i1}y_1 + a_{i2}y_2 + \cdots + a_{in}y_n \in \mathbb{K}[y_1, \ldots, y_n] \quad (1 \leq i \leq n)$$

be homogeneous linear forms such that $\det(a_{ij}) \neq 0$. The reducedness of F implies that

$$F(l_1, l_2, \ldots, l_n) \in \mathbb{K}[y_{k+1}, y_{k+2}, \ldots, y_n]$$

if and only if

$$\frac{\partial F(l_1, \ldots, l_n)}{\partial y_j} = 0, \text{ as polynomials, for } 1 \leq j \leq k. \tag{2}$$

By the chain rule we have

$$\frac{\partial F(l_1, \ldots, l_n)}{\partial y_j} = \sum_{i=1}^{n} F_i(l_1, \ldots, l_n) \frac{\partial l_i}{\partial y_j} = \sum_{i=1}^{n} F_i(l_1, \ldots, l_n) a_{ij}.$$

Thus the rank of F over $\mathbb{K}$ is at most $n - k$ iff there exists a nonsingular n by n matrix (a_{ij}) over $\mathbb{K}$ such that

$$\sum_{i=1}^{n} F_i(l_1, \ldots, l_n) a_{ij} = 0 \text{ for } 1 \leq j \leq k. \tag{3}$$

The polynomials $l_1, \ldots, l_n$ are algebraically independent over $\mathbb{K}$, hence the solvability of (3) for a_{ij} is equivalent to the likewise solvability of

$$\sum_{i=1}^{n} F_i(x_1, \ldots, x_n) a_{ij} = 0 \text{ for } 1 \leq j \leq k. \tag{4}$$

Taking into consideration that the matrix (a_{ij}) is nonsingular, the solvability of (4) is equivalent to the fact that the subspace spanned by the F_i is of dimension at most $n - k$ over $\mathbb{K}$. This proves the statement. $\square$

We proceed now to give a counterexample. Assume first that $p \geq 5$ and write

$$H(x_1, \dots, x_r) := \left(x_1^2 + x_2^2 + \cdots + x_r^2\right)^2. \tag{5}$$

Let $c \in \mathbb{F}_p$ be a quadratic nonresidue, and put

$$F(x_1, \dots, x_r) := H(x_1, \dots, x_r) - c. \tag{6}$$

It is immediate that $F \in \mathbb{F}_p[x_1, \dots, x_r]$ is reduced, $\deg F = 4$. Equation (1) has no solutions in $\mathbb{F}_p$, because the values of H are quadratic residues.

Finally we verify that the rank of F is r. We use Proposition 2.1. The partial derivatives

$$\frac{\partial F}{\partial x_i} = 4\left(x_1^2 + x_2^2 + \cdots + x_r^2\right) x_i \quad 1 \leq i \leq r$$

are linearly independent over $\mathbb{F}_p$, because $x_1, \dots, x_r$ are. We conclude, that the polynomial F from (6) is a counterexample whenever $r \geq 4$.

For $p = 2$ the conjecture is obviously true. If F is reduced and (1) has no solutions over $\mathbb{F}_2$, then F is the constant 1 polynomial.

For $p = 3$ a slight modification of the general construction works. Note that in this case the polynomial H from (5) is not reduced. We use instead the reduced version of H, in which x_i^4 is replaced by x_i^2:

$$H^*(x_1, \dots, x_r) := \left(x_1^2 + x_2^2 + \cdots + x_r^2\right)^2 - (x_1^4 + \cdots + x_r^4) + (x_1^2 + x_2^2 + \cdots + x_r^2).$$

One can put $F := H^* + 1$. Again, this F is reduced, $\deg F = 4$ and (1) has no solutions in ${\mathbb{F}_3}^r$.

One can check that the rank of F is r. We have

$$\frac{\partial F}{\partial x_j} = 4\left(\sum_{i=1}^{r} x_i^2\right) x_j - 4x_j^3 + 2x_j \text{ for } 1 \leq j \leq r.$$

By inspecting the homogeneous linear parts, we see that they are linearly independent, and Proposition 2.1 gives the claim.

Our constructions provide counterexamples with $\deg F = 4$, for all ranks $r \geq 4$. In fact, there are counterexamples for all degrees $d > 3$, $d \neq 5$. This follows readily from the next Lemma.

Lemma 2.2 *Let $f(x_1) \in \mathbb{F}_p[x_1]$ be a nonconstant polynomial, and $g(x_2, \ldots, x_r) \in \mathbb{F}_p[x_2, \ldots, x_r]$ be a polynomial with rank $r-1>0$. Assume that both f and g are reduced. Then the rank of $h = f(x_1)g(x_2, \ldots, x_r) \in \mathbb{F}_p[x_1, \ldots, x_r]$ is r.*

Proof. Clearly we have $h_1 := \frac{\partial h}{\partial x_1} = f'(x_1)g(x_2, \ldots, x_n)$ and $h_i := \frac{\partial h}{\partial x_i} = f(x_1)g_i$ for $i = 2, \ldots, r$, where $g_i = \frac{\partial g(x_2, \ldots, x_r)}{\partial x_i}$.

Suppose that $\sum_{i=1}^r a_i h_i = 0$ for some $a_i \in \mathbb{F}_p$. Let d be the degree of f. By collecting the terms divisible by x_1^d we obtain that $\sum_{i=2}^r a_i g_i = 0$. From the assumption on the rank of g Proposition 2.1 implies that $a_2 = \ldots = a_r = 0$. But $h_1 \neq 0$, hence $a_1 = 0$. The h_i are linearly independent over $\mathbb{F}_p$, and Proposition 2.1 gives the statement. □

Let $p > 2$ and $d > 5$ be a prescribed degree. By the preceding discussion there exists a polynomial $g(x_2, \ldots, x_d) \in \mathbb{F}_p[x_2, \ldots, x_d]$ such that the rank of g is $d-1$, $\deg g = 4$ and $g = 0$ has no solutions in ${\mathbb{F}_p}^{d-1}$. Let $f(x_1) \in \mathbb{F}_p[x_1]$ be an irreducible polynomial with $\deg f = d-4$. Note that $\deg f \geq 2$, hence f has no roots in $\mathbb{F}_p$. The polynomial

$$h(x_1, \ldots, x_d) := f(x_1)g(x_2, \ldots, x_d)$$

ha no zeroes over $\mathbb{F}_p$. Moreover, we have $\deg h = d$ and the rank of h is also d by Lemma 2.2.

3 Positive results

For $\deg F = 1$ the conjecture is obviously valid, as a nonconstant linear equation is always solvable in the ground field.

The conjecture holds also for $\deg F = 2$. Indeed, let $q > 2$ be an odd prime power and let $F(x_1, \ldots, x_n) \in \mathbb{F}_q[x_1, \ldots, x_n]$ be a quadratic polynomial. We may assume that n is minimal in the sense that F can not be written (via an invertible homogeneous linear change of variables) as a polynomial in less than n variables. Then, by the assumption on the rank of F we have $n \geq 2$. After a suitable diagonalization of the quadratic part of F over $\mathbb{F}_q$ (see Remark 6.28 in [4]) we may assume that

$$F = a_1x_1^2 + a_2x_2^2 + \cdots + a_kx_k^2 + b_1x_1 + \cdots + b_nx_n + c, \tag{7}$$

where $k \leq n$, $a_i, b_j, c \in \mathbb{F}_q$, and $a_1a_2 \cdots a_k \neq 0$. If $k < n$, then $b_n \neq 0$ by the minimality of n. In this case the number of solutions of $F = 0$ in $\mathbb{F}_q$ is

q^{n-1}, because any substitution for $x_1, \ldots, x_{n-1}$ can be extended uniquely to a solution by a suitable value for x_n.

If $k = n$, then the substitutions $x_i = y_i - \frac{b_i}{2a_i}$ (completing the square) transform (7) into

$$a_1 y_1^2 + a_2 y_2^2 + \cdots + a_n y_n^2 = d$$

for a suitable $d \in \mathbb{F}_q$, while preserving the number of solutions. V. A. Lebesgue's formulae (Theorems 6.26 and 6.27 in [4]) show that the latter equation is always solvable if $n \geq 2$. Solvability for q prime follows also from Theorem 3.2 below.

The cases $\deg F = 3$ or 5 remain open. We note, however, an affirmative fact in this direction. Let $\mathbb{F}$ denote the algebraic closure of $\mathbb{F}_q$.

Proposition 3.1 *Let $q \geq 7$ be a prime power, and $F(x, y, z) \in \mathbb{F}_q[x, y, z]$ be a cubic polynomial such that the (projective) surface $X \subset \mathbf{P}^3(\mathbb{F})$ defined by $F = 0$ is smooth. Then the equation*

$$F(x, y, z) = 0$$

has a solution in ${\mathbb{F}_q}^3$.

We remark that this includes the diagonal equations with $F = ax^3 + by^3 + cz^3 + d$, where a, b, c, d are nonzero elements of $\mathbb{F}_q$.

Proof. Manin [3] and Swinnerton-Dyer [8] determined the possible zeta functions of smooth cubic surfaces over finite fields. It turns out (see Table 1 in [8]) that X has at least $q^2 - 2q + 1$ points in $\mathbf{P}^3(\mathbb{F}_q)$. Let $\Pi \subset \mathbf{P}^3(\mathbb{F}_q)$ denote the plane at infinity.

It is known (cf. [7], [2]) that X contains exactly 27 lines. Also, as X is defined by a cubic equation, any line that contains four points of X belongs entirely to X. These imply, that $\Pi \not\subset X$, for otherwise X would contain at least 57 lines.

If $\Pi \cap X = \emptyset$, then by $q^2 - 2q + 1 > 0$ the surface X must have an affine point over $\mathbb{F}_q$. Otherwise, let $P \in \Pi \cap X$ be a point and consider the $q + 1$ lines $\ell_1, \ldots, \ell_{q+1}$ of Π adjacent to P. Out of these at most 3 can belong entirely to X. Otherwise any line of Π not passing through P would contain at least 4 points of X, implying that $\Pi \subset X$. We have

$$|\Pi \cap X| = 1 + \sum_{i=1}^{q+1} |(\ell_i \setminus \{P\}) \cap X| \leq 1 + 3q + 2(q-2) = 5q - 3.$$

Finally, $5q-3 < q^2-2q+1$ for $q \geq 7$, hence X must have a point in $\mathbf{P}^3(\mathbb{F}_q) \setminus \Pi$. This completes the proof. $\square$

In [6] Rédei considered mostly diagonal equations. Here we verify the conjecture for a more general class of polynomials. Let $f_i(x_i) \in \mathbb{F}_p[x_i]$ be polynomials for $1 \leq i \leq s$ with $1 \leq \deg f_i \leq p-1$. Put

$$k := \max\{\deg f_i : \ i = 1, \ldots, s\},$$

and consider the generalized diagonal equation

$$f_1(x_1) + f_2(x_2) + \cdots + f_s(x_s) = 0 \tag{8}$$

over $\mathbb{F}_p$.

Theorem 3.2 *If $k \leq s$ then (8) is solvable in ${\mathbb{F}_p}^s$.*

By Proposition 2.1 it is clear that the rank of $\sum f_i(x_i)$ in (8) is s, provided that $\deg f_i > 1$ holds with at most one exception, Thus, Theorem 3.2, a contribution to the generalized Waring problem over $\mathbb{F}_p$, states that Rédei's conjecture holds for equations of the form (8). We remark also, that the condition $k \leq s$ is necessary even for diagonal equations, see the examples in [6].

For a polynomial $f(x) \in \mathbb{F}_p[x]$ we denote by $V(f)$ its value set:

$$V(f) := \{f(a) : \ a \in \mathbb{F}_p\}.$$

It is immediate that for a nonconstant f we have

$$|V(f)| \geq \left\lceil \frac{p}{\deg f} \right\rceil = \left\lfloor \frac{p-1}{\deg f} \right\rfloor + 1. \tag{9}$$

In the proof of Theorem 3.2 the following results of of Carlitz, Lewis, Mills, and Straus [1] will be useful. In fact, part (a) of the Theorem covers most of the cases to be considered.

Theorem 3.3 *(a) Equation (8) is solvable in $\mathbb{F}_p$, if*

$$\sum_{i=1}^{s} \left\lfloor \frac{p-1}{\deg f_i} \right\rfloor + t > p,$$

where t is the number of f_i which are neither of degree $p-1$ nor of the form $a(x-b)^e + c$, with $a, b, c \in \mathbb{F}_p$ and $e = \frac{p-1}{2}$.
(b) Let $f(x) \in \mathbb{F}_p[x]$ be reduced with $|V(f)| = 2$. Then $\deg f = p-1$.

Also, we need the Cauchy-Davenport Theorem [5] from additive number theory. Let $A, B \subseteq \mathbb{F}_p$ nonempty sets. Recall that

$$A + B := \{a + b : \ a \in A, \ b \in B\}.$$

The Cauchy-Davenport Theorem states that $|A+B| \geq \min\{|A|+|B|-1, p\}$.

Proof of Theorem 3.2.

Suppose first that $k = p-1$. Then $s \geq p-1$. Clearly we have $|V(f_i)| \geq 2$, and then obvious induction involving the Cauchy-Davenport Theorem gives that

$$|V(f_1) + V(f_2) + \cdots + V(f_i)| \geq \min\{i + 1, p\},$$

and in particular

$$V(f_1) + \cdots + V(f_{p-1}) = \mathbb{F}_p.$$

This proves the claim for the case $k = p - 1$. From now on we may assume that $k < p - 1$.

If there is an f_i of degree $\frac{p-1}{2}$ then $s \geq \frac{p-1}{2}$. Also, by Theorem 3.3 (b) we have $|V(f_i)| \geq 3$ for $1 \leq i \leq s$. Now an inductive application of the Cauchy-Davenport Theorem shows that

$$|V(f_1) + V(f_2) + \cdots + V(f_i)| \geq \min\{2i + 1, p\},$$

hence

$$V(f_1) + \cdots + V(f_{\frac{p-1}{2}}) = \mathbb{F}_p.$$

We may additionally assume that $\deg f_i > 1$ for every i. Indeed, if say f_1 is a linear polynomial, then we may give arbitrary values to $x_2, \ldots, x_s$ from $\mathbb{F}_p$. This reduces (8) to a linear equation which is solvable for x_1. We may therefore suppose that no f_i has degree 1, $\frac{p-1}{2}$ or $p - 1$. In view of Theorem 3.3 (a) it suffices to verify that

$$s + \sum_{i=1}^{s} \left\lfloor \frac{p-1}{\deg f_i} \right\rfloor > p.$$

In fact, division with remainder gives that

$$p - 1 = \deg f_i \left\lfloor \frac{p-1}{\deg f_i} \right\rfloor + m_i$$

with $0 \leq m_i \leq \deg f_i - 2$, because p is a prime and $\deg f_i > 1$. We infer that

$$1 + \left\lfloor \frac{p-1}{\deg f_i} \right\rfloor \geq \frac{p-1}{\deg f_i} + \frac{2}{\deg f_i} = \frac{p+1}{\deg f_i},$$

and hence

$$s + \sum_{i=1}^{s} \left\lfloor \frac{p-1}{\deg f_i} \right\rfloor \geq \sum_{i=1}^{s} \frac{p+1}{\deg f_i} \geq \frac{s(p+1)}{k} \geq p+1.$$

This finishes the proof of the Theorem. $\square$

Acknowledgment I thank the referee and Bálint Felszeghy for their valuable remarks.

References

[1] L. Carlitz, D. J. Lewis, W. H. Mills, E. G. Straus, Polynomials over finite fields with minimal value sets; *Mathematika, 8(1961), 121–130.*

[2] R. Hartshorne, *Algebraic Geometry;* GTM 52, Springer-Verlag 1977.

[3] Ju. I. Manin, On the arithmetic of rational surfaces (in Russian); *Dokl. Akad. Nauk SSSR, 152(1963), 46–49.*

[4] R. Lidl, H. Niederreiter, *Finite Fields;* Addison-Wesley Publishing Co. 1983.

[5] M. B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets;* GTM 165, Springer-Verlag 1996.

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

[7] B. Segre, *The Non-Singular Cubic Surfaces;* Oxford University Press 1942.

[8] H. P. F. Swinnerton-Dyer, The zeta function of a cubic surface over a finite field; *Proc. Cambridge Philos. Soc. 63(1967), 55–71.*