ACTA ARITHMETICA
C.4 (2001)

Correction of "Polynômes singuliers à plusieurs variables sur un corps fini et congruences modulo p^2"

(Acta Arith. 68 (1994), 1–10)

by

LEKBIR CHAKRI (Rabat and Mahammadia) and
EL MOSTAFA HANINE (Mahammadia)

1. Introduction. We say that a field K has the *property* $c_i(d)$ if every form defined over K of degree d in more than d^i variables has a nontrivial zero.

E. Artin [1] has conjectured that p-adic fields have the property $c_2(d)$. However G. Terjanian [5] exhibited an example establishing that $\mathbb{Q}_2$ does not have the property $c_2(4)$, thus disproving Artin's conjecture. J. Ax and S. Kochen [2] showed the following result: For each integer $d \geq 1$, there exists a number $p_0(d)$ such that whenever $p > p_0(d)$, every polynomial defined over $\mathbb{Q}_p$ of degree d in more than d^2 variables and without constant term, has a nontrivial zero. E. M. Hanine [3] has obtained the analogous result which states that for each integer $d \geq 1$, there exists $p(d)$ such that whenever $p > p(d)$, the congruence

$$f(x_1, \ldots, x_{2d+1}) \equiv 0 \pmod{p^2}$$

has a primitive solution for every polynomial $f \in \mathbb{Z}_p[X_1, \ldots, X_{2d+1}]$ of degree d and without constant term.

The object of this paper is to determine explicitly an upper bound for $p(4)$.

In order to do this Hensel's Lemma permits us to study only singular polynomials of degree 4 over finite fields. We obtain the following result:

Let $F \in \mathbb{F}_q[X_1, \ldots, X_n]$ be a singular polynomial of degree 4 without constant term and in at least 9 variables over $\mathbb{F}_q$ with $q > 36$ odd. Then F is one of the following:

2000 *Mathematics Subject Classification*: 12E20, 12E05, 11D88, 11D79, 11D72.

(i) $F=\varepsilon(g_1^2-vg_2^2)$, *where* $\varepsilon\in\{-1,1\}$, v *is a nonsquare element of* $\mathbb{F}_q$ *and* g_1 *and* g_2 *are of degrees* ≤ 2 *defined over* $\mathbb{F}_q$ *and without constant term*;

(ii) $F=G(L_1,\ldots,L_k)$, *where* G *is an anisotropic polynomial of degree* 4 *defined over* $\mathbb{F}_q$ *and* L_i, $1\le i\le k$, *is a linear form and* $k\le 4$.

This result permits us to show that the congruence

$$f(x_1,\ldots,x_9)\equiv 0 \pmod{p^2},$$

where f is a polynomial of degree 4 with coefficients in $\mathbb{Z}_p$ and without constant term, has a primitive solution whenever $p>36$.

These results were already stated in [4] but the proofs were incorrect.

We say that $(x_1,\ldots,x_n)\in\mathbb{Z}_p^n$ is *primitive* if there exists $i\in\{1,\ldots,n\}$ such that p does not divide x_i.

A nonzero polynomial F is said to be *singular* if every nontrivial zero of F is singular, i.e. all the partial derivatives of F vanish there. A nonzero polynomial F is said to be *nonsingular* if it has a nonsingular zero, i.e. a zero at which not all the partial derivatives of F vanish.

2. Singular polynomials of degree 4 in many variables. In this section we consider singular polynomials of degree 4. First we need to show the following lemma for quartic forms.

LEMMA 2.1. *Let* F *be a quartic form in at least two variables over a field* K. *Assume that* F *has two singular projective* K*-rational zeros* u *and* v. *Let* $\langle u,v\rangle$ *denote the projective line in* $P^n(K)$ *through* u *and* v. *Then at least one of the following possibilities occurs*:

(i) u *and* v *are the only zeros of* F *in* $\langle u,v\rangle$.

(ii) *The restriction of* F *to* $\langle u,v\rangle$ *is the zero polynomial.*

Proof. By a k-rational change of variables we may assume $u=(1,0,\ldots,0)$ and $v=(0,1,0,\ldots,0)$. Then $F(x_0,x_1,0,\ldots,0)=ax_0^2x_1^2$.

If $a\neq 0$, we have case (i). If $a=0$, we have case (ii).

REMARK 1. The proof of Lemma 3.2 of [4] is completely incorrect by Lemma 2.1 above since for a quartic form and for any two K-rational projective zeros the quartic form could vanish identically on the line joining them. Hence in this way we cannot find a plane section that contains just two singular points. So the transformation to the K-rational affine zeros in the proof of Lemma 3.2 of [4] is not justified. In addition the proof of Theorem 3.1 is wrong mainly due to its use of Lemma 3.2.

Now let $F\in\mathbb{F}_q[X_1,\ldots,X_n]$ be a singular polynomial of degree 4, without constant term and in at least 9 variables over $\mathbb{F}_q$ with q odd.

Lemma 3.2 of [4] should be modified to the following lemma:

LEMMA 2.2. *If* $q > 3$, *then either* (i) *or* (ii) *below can occur*:

(i) *There exists an invertible homogeneous linear transformation* $X_i = L_i(Y_1, \dots, Y_n)$ *such that*

$$F = G(Y_1, \dots, Y_n) = Y_1^2 Q(Y_2, \dots, Y_n) + 2Y_1 C(Y_2, \dots, Y_n) + U(Y_2, \dots, Y_n),$$

where G, Q, C *and* U *are defined over* $\mathbb{F}_q$ *and have the following properties*: G *depends on* Y_1, Q *is a quadratic form*, C *and* U *are of degrees respectively* ≤ 3 *and* ≤ 4 *and without homogeneous term of degree* ≤ 1.

(ii) *There exists an anisotropic polynomial* $G \in \mathbb{F}_q[X_1, \dots, X_k]$ *of degree* 4 *such that* $F = G(L_1, \dots, L_k)$, *where* L_i, $1 \leq i \leq k$, *with* $k \leq 4$ *is a linear form defined over* $\mathbb{F}_q$.

Proof. Since F is singular, $F = F_4 + F_3 + F_2$, where F_i is the homogeneous term of degree i of F. It then follows from the Chevalley–Warning Theorem that there exists $x \in \mathbb{F}_q^n$, $x \neq 0$, such that $F_4(x) = 0$ and $(F_3 + F_2)(x) = 0$. Thus there exists an invertible homogeneous linear transformation $X_i = L_i(Y_1, \dots, Y_n)$ that transforms x into $(1, 0, \dots, 0)$. We may then write

$$\begin{aligned} F &= G(Y_1, \dots, Y_n) \\ &= aY_1^4 + bY_1^3 + cY_1^2 + Y_1^3(a_2Y_2 + \dots + a_nY_n) \\ &\quad + Y_1^2(Q(Y_2, \dots, Y_n) + b_2Y_2 + \dots + b_nY_n) \\ &\quad + Y_1(C^*(Y_2, \dots, Y_n) + c_2Y_2 + \dots + c_nY_n) + U(Y_2, \dots, Y_n), \end{aligned}$$

where G, Q, C^* and U are defined over $\mathbb{F}_q$ and have the following properties: G is singular, Q is a quadratic form, C^* and U are of degrees respectively ≤ 3 and ≤ 4 and without homogeneous term of degree ≤ 1.

From the above, the homogeneous term of degree 4 of G satisfies $G_4(1, 0, \dots, 0) = 0$, hence $a = 0$. Moreover, we have the following relations:

$$G(1, 0, \dots, 0) = b + c = 0, \tag{1}$$

$$\frac{\partial G}{\partial Y_i}(1, 0, \dots, 0) = 3b + 2c = 0. \tag{2}$$

The relation (2) follows from the fact that G is singular. We then deduce from (1) and (2) that $b = c = 0$.

Hence, $G(x, 0, \dots, 0) = 0$ for all $x \in \mathbb{F}_q$; and since G is singular, we have

$$\frac{\partial G}{\partial Y_i}(x, 0, \dots, 0) = a_i x^3 + b_i x^2 + c_i x = 0 \quad \text{for all } i \in \{2, \dots, n\}.$$

We then conclude that $a_i = b_i = c_i = 0$ for all $i \in \{2, \dots, n\}$ since $q > 3$.

If G depends on Y_1, we have case (i) by putting $C^*(Y_2, \dots, Y_n) = 2C(Y_2, \dots, Y_n)$.

If G does not depend on Y_1, we repeat the same process whenever the polynomial obtained by a linear change of variables has a nontrivial zero in $\mathbb{F}_q^m$, where m is the number of variables occurring in this polynomial.

This implies that after a finite number of changes of variables we have either case (i) or $F = G(L_1, \ldots, L_k)$, where G is an anisotropic polynomial of degree 4 and L_i, $1 \leq i \leq k$, with $k \leq 4$ is a linear form defined over $\mathbb{F}_q$. This completes the proof of the lemma.

By this lemma, Theorem 3.1 of [4] should be modified as follows:

THEOREM 2.1. *Let $F \in \mathbb{F}_q[X_1, \ldots, X_n]$ be a singular polynomial of degree* 4, *without constant term and in at least* 9 *variables over $\mathbb{F}_q$ with $q > 36$ odd. Then F is one of the following*:

(i) $F = \varepsilon(g_1^2 - vg_2^2)$, *with $\varepsilon \in \{-1, +1\}$, v is a nonsquare element in $\mathbb{F}_q$ and g_1 and g_2 are of degrees ≤ 2 defined over $\mathbb{F}_q$ and without constant term.*

(ii) $F = G(L_1, \ldots, L_k)$, *where G is an anisotropic polynomial of degree* 4 *and L_i, $1 \leq i \leq k$, with $k \leq 4$ is a linear form defined over $\mathbb{F}_q$.*

Proof. It follows from Lemma 2.2 that either we have case (ii) of the theorem or there exists an invertible homogeneous linear transformation $X_i = L_i(Y_1, \ldots, Y_n)$ such that $F = G(Y_1, \ldots, Y_n) = Y_1^2 Q(Y_2, \ldots, Y_n) + 2Y_1 C(Y_2, \ldots, Y_n) + U(Y_2, \ldots, Y_n)$, where G, Q, C and U are defined over $\mathbb{F}_q$ and have the following properties: G depends on Y_1, Q is a quadratic form, C and U are of degrees respectively ≤ 3 and ≤ 4 and without homogeneous term of degree ≤ 1. In this case by making use of the same argument of case 1 and case 2 of the proof of Theorem 3.1 of [4], we have case (i) of the theorem. This completes the proof.

3. Diophantine equations of degree 4 modulo p^2. In this section we make use of the main result from Section 2.

THEOREM 3.1. *Let p be a prime number > 36. Then for every polynomial $f \in \mathbb{Z}_p[X_1, \ldots, X_9]$ of degree* 4 *and without constant term*, *the congruence*

$$f(x_1, \ldots, x_9) \equiv 0 \pmod{p^2}$$

has a primitive solution.

Proof. Consider $F = \bar{f} \in \mathbb{F}_p[X_1, \ldots, X_9]$, where $\bar{f}$ denotes the reduction of f modulo p.

First case. If F is the zero polynomial, then there exists $h \in \mathbb{Z}_p[X_1, \ldots, X_9]$ such that $f = ph$. Thus it follows from the Chevalley–Warning Theorem that the congruence $h \equiv 0 \pmod{p}$ has a primitive solution $(x_1, \ldots, x_9)$ which satisfies

$$f(x_1, \ldots, x_9) \equiv 0 \pmod{p^2}.$$

Second case. If F is nonsingular, then there exist $(x_1, \dots, x_9) \in \mathbb{F}_p^9$ and $1 \le i_0 \le 9$ such that

$$F(x_1, \dots, x_9) = 0 \quad \text{and} \quad \frac{\partial F}{\partial X_{i_0}}(x_1, \dots, x_9) \neq 0.$$

Thus it follows from Hensel's Lemma that there exists $(y_1, \dots, y_9) \in \mathbb{Z}_p^9$ such that $(y_1, \dots, y_9)$ is primitive and

$$f(y_1, \dots, y_9) = 0,$$

which implies that

$$f(y_1, \dots, y_9) \equiv 0 \pmod{p^2}.$$

Third case. If F is singular of degree 4, then there are two subcases to consider.

Assume that $F = \varepsilon(G_1^2 - vG_2^2)$, where $G_1, G_2 \in \mathbb{F}_q[X_1, \dots, X_9]$ are of degrees ≤ 2 and without constant term. In this case let $g_1, g_2 \in \mathbb{Z}_p[X_1, \dots, X_9]$ be of degrees ≤ 2 and without constant term such that $\overline{g}_1 = G_1$ and $\overline{g}_2 = G_2$. Consider $h \in \mathbb{Z}_p[X_1, \dots, X_9]$ such that $f = \varepsilon(g_1^2 - vg_2^2) + ph$.

The system of congruences

$$\begin{cases} g_1(x_1, \dots, x_9) \equiv 0 \pmod{p}, \\ g_2(x_1, \dots, x_9) \equiv 0 \pmod{p}, \\ h(x_1, \dots, x_9) \equiv 0 \pmod{p} \end{cases}$$

satisfies the hypotheses of the Chevalley–Warning Theorem. So it has a primitive solution $(x_1, \dots, x_9) \in \mathbb{Z}_p^9$ that satisfies

$$f(x_1, \dots, x_9) \equiv 0 \pmod{p^2}.$$

Assume now that $F = G(L_1, \dots, L_k)$, where G is anisotropic, L_i is a linear form and $k \le 4$. Let $g \in \mathbb{Z}_p[X_1, \dots, X_k]$ be a polynomial such that $\overline{g} = G$ and let $l_i \in \mathbb{Z}_p[X_1, \dots, X_9]$ with $1 \le i \le k$ be a linear form such that $\bar{l}_i = L_i$. Consider now the polynomial $h \in \mathbb{Z}_p[X_1, \dots, X_9]$ such that $f = g(l_1, \dots, l_k) + ph$.

The system of congruences

$$\begin{cases} l_1(x_1, \dots, x_9) \equiv 0 \pmod{p}, \\ \dots \\ l_k(x_1, \dots, x_9) \equiv 0 \pmod{p}, \\ h(x_1, \dots, x_9) \equiv 0 \pmod{p} \end{cases}$$

satisfies the hypotheses of the Chevalley–Warning Theorem. So it has a primitive solution $(x_1, \dots, x_9) \in \mathbb{Z}_p^9$ that satisfies

$$f(x_1, \dots, x_9) \equiv 0 \pmod{p^2}.$$

Fourth case. If F is singular of degree ≤ 3, then Lemmas 3.2 and 4.1 of [3] permit us to show the theorem. This completes the proof.

References

[1] E. Artin, *The Collected Papers*, Addison–Wesley, Reading, MA, 1965.
[2] J. Ax and S. Kochen, *Diophantine problems over local fields*: *III. Decidable fields*, Ann. of Math. 83 (1966), 437–456.
[3] E. M. Hanine, *Équations diophantiennes modulo* p^2, Colloq. Math. 64 (1993), 275–286.
[4] —, *Polynômes singuliers à plusieurs variables sur un corps fini et congruences modulo* p^2, Acta Arith. 68 (1994), 1–10.
[5] G. Terjanian, *Un contre exemple à une conjecture d'Artin*, C. R. Acad. Sci. Paris 262 (1966), 612.

Department of Mathematics
Faculty of Sciences
P.O. Box 1014
Rabat, Morocco
E-mail: lchakri@hotmail.com

Department of Mathematics
Faculty of Sciences and Technics
P.O. Box 146
Mahammadia, Morocco
E-mail: hanine@uh2.ac.ma

Received on 17.03.2000
and in revised form on 2.02.2001 (3780)