Anisotropic forms modulo $p^2$

by

Lekbir Chakri (Rabat) and
El Mostafa Hanine (Mohammadia)

1. Introduction. A form (i.e., a homogeneous polynomial) defined over a field $K$ is said to be anisotropic if it has only the trivial zero in $K$. In the 1930’s E. Artin [3] conjectured that for every prime $p$ and any $d \geq 1$, an anisotropic form, with coefficients in the field of $p$-adic numbers $\mathbb{Q}_p$, of degree $d$ has at most $d^2$ variables. Terjanian [15] disproved the conjecture by exhibiting a 2-adic quartic form in 18 variables with no nontrivial 2-adic zero; subsequently, he [16] gave such an example with 20 variables. Generalizing Terjanian’s construction, Browkin [5] gave counterexamples for each prime $p$, but always in fewer than $d^3$ variables. Later investigations concerning a problem of Hilbert and Kamke allow Arkhipov and Karatsuba [1, 2] to prove that for each prime $p$, there are infinitely many natural numbers $d$ such that the number of variables required to guarantee the existence of a nontrivial $p$-adic zero for a form of degree $d$ may need to be exponentially large in terms of $d$. The latter result was slightly sharpened independently by Brownawell [7], and by Lewis and Montgomery [13] via the introduction of a more efficient principle of $p$-adic interpolation. Note that we currently possess no counterexample of odd degree. Thus Artin’s conjecture is still open in particular for prime degrees.

It is still of interest to know precisely when the conjecture is true. It has been verified in case $d = 2$ (see [11] for short proof), in case $d = 3$ [9, 12] and in case $d = 5$ [11] provided the residue class field has at least 47 elements. But, it is impressive that Ax and Kochen [4], by employing methods from Mathematical Logic, were able to show that Artin’s conjecture is very nearly true in general. They proved that there exists a function $p_0(d)$ such that the conjecture is true for all $p > p_0(d)$. In [10], there is an analogous result which states that to each natural number $d \geq 2$, there corresponds a function $p(d)$ such that, if $p$ is a prime number $> p(d)$ and $f \in \mathbb{Z}_p[X_1, \ldots, X_{2d+1}]$ is a form of degree $d$, then the congruence $f(X_1, \ldots, X_{2d+1}) \equiv 0 \pmod{p^2}$ has
a primitive zero (an element \((x_1, \ldots, x_n) \in \mathbb{Z}_p^n\) is primitive if there exists \(i \in \{1, \ldots, n\}\) such that \(p\) does not divide \(x_i\)). The argument used to derive this result does not enable one to calculate explicit estimates for \(p(d)\). But there is in principle no barrier to providing such (see [8], where it is shown that \(p(4) \leq 37\)).

In this paper we give an explicit upper bound for the quantity \(p(d)\) and construct, in a similar manner analyzed in [6] and described in [16], for each prime \(p > 3\) other counterexamples to Artin’s conjecture of degree \(D\), where \(D\) is any multiple of \(p^2 - p\).

2. Constructions. It is well known that a form \(f\), with coefficients in a ring of \(p\)-adic integers \(\mathbb{Z}_p\), in \(n\) variables is anisotropic if and only if there exists a natural number \(k \geq 1\) such that if \(f(x_1, \ldots, x_n) \equiv 0 \pmod{p^k}\), then \(x_1 \equiv \ldots \equiv x_n \equiv 0 \pmod{p}\). When this holds we say that \(f\) is anisotropic modulo \(p^k\).

Whenever \(r\) and \(s\) are natural numbers with \(0 \leq r \leq s\), and \(f\) is a polynomial involving the variables \(X_r, \ldots, X_s\), we denote by \(f^{(m)}\), where \(m \geq 0\), the polynomial \(f(X_{m+r}, \ldots, X_{m+s})\).

If \(p\) is a prime number and \(d \geq 1\) an integer, \(n_d\) denotes a normic form, with coefficients in the ring of \(p\)-adic integers \(\mathbb{Z}_p\), of degree \(d\) in \(d\) variables that is anisotropic modulo \(p\).

Let \(p\) be a prime number \(> 3\). Let \(k\) be a natural number with \(2 \leq k \leq p - 2\).

The form \(v \in \mathbb{Z}_p[X_1, X_2]\) of degree \(p^2 - p\) defined by

\[
v(X_1, X_2) = X_1^{(p-1)(p-k)}(X_1^{p-1} - X_2^{p-1})^k + X_2^{p^2-p}
\]

satisfies

\[
v(x_1, x_2) \equiv 1 \pmod{p^2}
\]

for every primitive \((x_1, x_2) \in \mathbb{Z}_p^2\).

Let \(d\) be a natural number with \(d \geq 1\). Consider the form \(f(X) \in \mathbb{Z}_p[X_1, \ldots, X_{2d}]\) of degree \(D = d(p^2 - p)\), defined by

\[
f = v(n_d, n_d^{(d)}).
\]

Then

\[
f(x_1, \ldots, x_{2d}) \equiv 1 \pmod{p^2}
\]

whenever \(x_1, \ldots, x_{2d}\) are not all congruent to 0 modulo \(p\).

Put now

\[
g = \sum_{i=0}^{p^2-2} f(2di).
\]
It is clear that \( g \) is a form, with coefficients in \( \mathbb{Z}_p \), of degree \( D \) in \( 2d(p^2 - 1) \) variables that satisfies

\[
g(x) \equiv r \pmod{p^2}
\]

with \( 1 \leq r \leq p^2 - 1 \) for every primitive \( x \).

Put \( N = dD(p^2 - 1) \). We define an element \( h \) of \( \mathbb{Z}_p[\{X_1, \ldots, X_N\}] \) by

\[
h = \sum_{i=0}^{p-1} p^{2i} g(2di(p^2-1)).
\]

\( h \) is a counterexample of degree \( D \) to Artin’s conjecture since \( h \) is anisotropic modulo \( p^D \) and \( N > D^2 \).

3. Homogeneous diophantine equations modulo \( p^2 \). We remark that in order to get a counterexample of degree \( d \) to Artin’s conjecture, it suffices to construct a form, with coefficients in a ring \( \mathbb{Z}_p \), of degree \( d \) in \( 2d + 1 \) variables that is anisotropic modulo \( p^2 \).

Indeed, let \( p \) be a prime number and \( f \in \mathbb{Z}_p[\{X_1, \ldots, X_{2d+1}\}] \) be a form of degree \( d \) that is anisotropic modulo \( p^2 \).

If \( d \) is even, put

\[
f_1 = \sum_{i=0}^{d-2} p^i f(\frac{i}{2}(2d+1)) \quad \text{with } i \text{ even.}
\]

If \( d \) is odd, put

\[
f_2 = \sum_{i=0}^{d-1} p^i f(\frac{i}{2}(2d+1)) \quad \text{with } i \text{ even.}
\]

It is easy to see that both \( f_1 \) and \( f_2 \) are anisotropic modulo \( p^d \).

We now give an explicit upper bound for the quantity \( p(d) \) mentioned in the introduction.

**Theorem 3.1.** Let \( f \in \mathbb{Z}_p[X_1, \ldots, X_{2d+1}] \) be a form of degree \( d \). Assume that \( p > 250d^5 \) and \( d(d-1)^2 + (2pd^5)^{1/2} + 2d\phi \leq p \), where \( \phi = 2dk^2 \), with \( k = \left( \frac{d+1}{2} \right) \). Then the congruence

\[
f(X_1, \ldots, X_{2d+1}) \equiv 0 \pmod{p^2}
\]

has a primitive zero.

**Proof.** Let \( F = \bar{f} \) denote the reduction of \( f \) modulo \( p \).

**First case.** If \( F = 0 \), then it follows from Chevalley’s theorem that (1) has a primitive zero.

**Second case.** If \( F \) is reducible, then \( F = F_1 F_2 \). Let \( f_1, f_2 \) be two forms such that \( \bar{F_1} = \bar{f_1} \) and \( \bar{F_2} = \bar{f_2} \). We then write \( f = f_1 f_2 + ph \) for some form
The system of congruences

\[
\begin{align*}
    f_1(X_1, \ldots, X_{2d+1}) &\equiv 0 \pmod{p}, \\
    f_2(X_1, \ldots, X_{2d+1}) &\equiv 0 \pmod{p}, \\
    h(X_1, \ldots, X_{2d+1}) &\equiv 0 \pmod{p}
\end{align*}
\]

satisfies the hypotheses of Chevalley’s theorem. So it has a primitive zero that satisfies (1).

**Third case.** Assume that \( F \) is irreducible but not absolutely. Let \( F_1 \) be an irreducible factor of \( F \) over the algebraic closure \( \overline{\mathbb{F}}_p \) of \( \mathbb{F}_p \). We normalize \( F_1 \) by requiring that the leading coefficient (in some lexicographic ordering of the monomials) is 1. Let \( K \) be the field obtained from \( \mathbb{F}_p \) by adjoining the coefficients of \( F_1 \). Write \( m = [K : \mathbb{F}_p] \). There are then \( m \) \( \mathbb{F}_p \)-homomorphisms, denoted \( \sigma_i \), \( i = 1, \ldots, m \), from \( K \) into \( \overline{\mathbb{F}}_p \). For each \( i \in \{1, \ldots, m\} \), \( \sigma_i(F_1) \) is irreducible over \( \overline{\mathbb{F}}_p \) and divides \( F \). For \( i \neq j \), we have \( (\sigma_i(F_1), \sigma_j(F_1)) = 1 \). So, since \( \overline{\mathbb{F}}_p[X_1, \ldots, X_{2d+1}] \) is UFD, the product \( \prod_{i=1}^m \sigma_i(F_1) \) divides \( F \). But this product has coefficients which are invariant under conjugation. Hence, it has coefficients in \( \mathbb{F}_p \). Since \( F \) is irreducible over \( \mathbb{F}_p \), there exists a constant \( c \in \mathbb{F}_p \) such that \( F = c \prod_{i=1}^m \sigma_i(F_1) \). Each factor \( \sigma_i(F_1) \) has degree exactly \( d/m \).

Let now \( \{e_1, \ldots, e_m\} \) be a basis of \( K \), considered as an \( \mathbb{F}_p \)-vector space, and \( G_1, \ldots, G_m \in \mathbb{F}_p[X_1, \ldots, X_{2d+1}] \) be forms such that \( F_1 = \sum_{i=1}^m G_i e_i \). Then

\[
F = c \prod_{i=1}^m \left( \sum_{j=1}^m G_j \sigma_i(e_j) \right) = G(G_1, \ldots, G_m),
\]

where \( G \) is a form, with coefficients in \( \mathbb{F}_p \), of degree \( d \). Thus, if \( G = \overline{g} \) and \( G_i = \overline{g}_i \) for \( i \in \{1, \ldots, m\} \), we may write \( f = g(g_1, \ldots, g_m) + ph \) for some form \( h \in \mathbb{Z}_p[X_1, \ldots, X_{2d+1}] \). By Chevalley’s theorem, the system

\[
\begin{align*}
    g_1(X_1, \ldots, X_{2d+1}) &\equiv 0 \pmod{p}, \\
    \cdots \\
    g_m(X_1, \ldots, X_{2d+1}) &\equiv 0 \pmod{p}, \\
    h(X_1, \ldots, X_{2d+1}) &\equiv 0 \pmod{p}
\end{align*}
\]

has a primitive zero that satisfies (1).

**Fourth case.** Now assume that \( F \) is absolutely irreducible. It then follows from [14, p. 210, Theorem 5A] that the number \( N \) of zeros of \( F \) in \( \mathbb{F}^{2d+1}_p \) satisfies

\[
|N - p^{2d}| < p^{2d-1}((2pd^5)^{1/2} + 2d\phi).
\]

Since \( \deg(F) < p \), there exists \( i_0 \in \{1, \ldots, 2d + 1\} \) such that \( \partial F/\partial X_{i_0} \neq 0 \). Hence, \( F \) and \( \partial F/\partial X_{i_0} \) have no common factor of degree \( \geq 1 \) since \( F \) is irreducible. By [14, p. 152, Lemma 3C], the number \( N' \) of common zeros of \( F \) and \( \partial F/\partial X_{i_0} \) satisfies

\[
N' \leq p^{2d-1}(d - 1)^2 d.
\]
So, if \( d(d - 1)^2 + (2pd^5)^{1/2} + 2d\phi \leq p \), then \( F \) has a nonsingular \( \mathbb{F}_p \)-rational zero. Therefore (1) has a primitive zero by Hensel’s lemma. This completes the proof of the theorem.

References


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

Department of Mathematics
Faculty of Sciences and Technology
P.O. Box 146
Mohammadia, Morocco
E-mail: hanine@uh2m.ac.ma

Received on 8.12.2001 and in revised form on 8.4.2002