Acta Mathematica et Informatica Universitatis Ostraviensis

Tadeusz Pezda

On cycles and orbits of polynomial mappings $\mathbb{Z}^2 \mapsto \mathbb{Z}^2$

Acta Mathematica et Informatica Universitatis Ostraviensis, Vol. 10 (2002), No. 1, 95--102

Persistent URL: `http://dml.cz/dmlcz/120574`

Terms of use:

© University of Ostrava, 2002

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.

This paper has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* `http://project.dml.cz`

On cycles and orbits of polynomial mappings $Z^2 \mapsto Z^2$

T. Pezda

1. Introduction

For a commutative ring R with unity and $\Phi = (\Phi^{(1)}, \dots, \Phi^{(N)})$, where $\Phi^{(i)} \in R[X_1, \dots, X_N]$ we define a cycle for Φ as a k-tuple $\bar{x}_0, \bar{x}_1, \dots, \bar{x}_{k-1}$ of different elements of R^N such that

$$\Phi(\bar{x}_0) = \bar{x}_1, \Phi(\bar{x}_1) = \bar{x}_2, \dots, \Phi(\bar{x}_{k-1}) = \bar{x}_0.$$

The number k is called the length of this cycle.

We denote $\mathcal{CYCL}(R, N)$ as the set of all possible cycle lengths for polynomial mappings in N variables with coefficients from R. We put $B(R, N)$ as the maximal element in $\mathcal{CYCL}(R, N)$ (if there is no such maximal element we put $B(R, N) = \infty$).

For $\bar{x} \in R^N$ and $\Phi : R^N \mapsto R^N$ we define the orbit

$$\mathcal{ORB}(\bar{x}, \Phi) = \{\bar{x}, \Phi(\bar{x}), \Phi^2(\bar{x}), \dots\}.$$

We call the orbit $\mathcal{ORB}(\bar{x}, \Phi)$ finite if it is a finite set.

Define $\mathcal{ORB}(R, N)$ as the maximal number of elements of **finite** orbits

$$\mathcal{ORB}(\bar{x}, \Phi)$$

with $\bar{x} \in R^N$, and $\Phi = (\Phi^{(1)}, \dots, \Phi^{(N)})$ with $\Phi^{(i)} \in R[X_1, \dots, X_N]$. If there is no such number we put $\mathcal{ORB}(R, N) = \infty$.

In 1998 W.Narkiewicz asked whether $B(Z, 2) \geq 7$. In this paper we shall give the positive answer to this question. Moreover, the set $\mathcal{CYCL}(Z, 2)$ will be completely determined.

As to orbits in [NP] it was shown that $\mathcal{ORB}(Z_K, 1) < \infty$ where Z_K is the ring of integers in a finite extension K of Q. Moreover, it was shown that $\mathcal{ORB}(Z, 1) = 4$.

Received: November 23, 2001.
2000 *Mathematics Subject Classification:* 11R04,11S05.

2. Results

Theorem 2.1. $\mathcal{CYCL}(Z,2) = \{24, 18, 16, 12, 9, 8, 6, 4, 3, 2, 1\}$.
So, in particular $B(Z,2) = 24$.

Theorem 2.2. $\mathcal{ORB}(Z,2) = \infty$. *So, it follows that* $\mathcal{ORB}(R,N) = \infty$ *for* R, *a ring of zero characteristic with unity and* $N \geq 2$ *(as* Z *can be embedded into* R*).*

3. Auxiliary results and some notations

3.1. The main auxiliary theorem

Proposition 3.1. *([Pe3]) Let* R *be a Dedekind domain. Let* $\mathcal{P}(R)$ *denote the set of all non-zero prime ideals of* R. *If* $N \geq 2$ *then*

$$\mathcal{CYCL}(R,N) = \bigcap_{\mathfrak{p}\in\mathcal{P}(R)} \mathcal{CYCL}(R_{\mathfrak{p}},N) = \bigcap_{\mathfrak{p}\in\mathcal{P}(R)} \mathcal{CYCL}(\widehat{R_{\mathfrak{p}}},N),$$

where $\widehat{R_{\mathfrak{p}}}$ *is the completion of* $R_{\mathfrak{p}}$ *with respect to the obvious valuation. In particular, it holds for the rings of integers in finite extensions of* Q.

3.2. Cycles in some local domains

Owing to the proposition 3.1 it is useful to recall some results concerning cycles in discrete valuation domains.

In this subsection let R be a discrete valuation domain of characteristic zero,P is the unique maximal ideal of R. We assume that the quotient field R/P is finite and has $N(P) = p^f$ elements (p is prime). Let π be a generator of the principal ideal P and let v be the norm of R, normalized so that $v(\pi) = \frac{1}{p}$. By w we denote the corresponding exponent, defined by $w(x) = -\frac{\log v(x)}{\log p}$ for $x \neq 0$ and $w(0) = \infty$.

We extend v and w to R^N by putting

$$v(\bar{x}) = v((x_1, \dots, x_N)) = \max\{v(x_i), i = 1, \dots, N\}$$

and

$$w(\bar{x}) = w((x_1, \dots, x_N)) = \min\{w(x_i), i = 1, \dots, N\}.$$

The congruence symbol $\bar{x} \equiv \bar{y} \pmod{P^d}$ will be used for vectors $\bar{x}, \bar{y}$ in R^N to indicate that corresponding components are congruent $\pmod{P^d}$, or equivalently $w(\bar{x} - \bar{y}) \geq d$.

Denote the image of some $\bar{x} \in R^N$ under the canonical mapping $R^N \to R^N/PR^N = (R/P)^N$ by $\bar{x} + PR^N$.

A cycle $\bar{x}_0, \dots, \bar{x}_{k-1}$ will be called a (*)-cycle if for all i, j one has $w(\bar{x}_i - \bar{x}_j) \geq 1$.

Definition 3.2. A (*)-cycle $\bar{x}_0, \dots, \bar{x}_{k-1}$ with $k \geq 2$ we call normalized provided $\bar{x}_0 = \bar{0}$ and $w(\bar{x}_1) = 1$.

Proposition 3.3. *If there is a (*)-cycle in* R^N *of length* $k \geq 2$ *then there exists a normalized (*)-cycle in* R^N *of the same length.*

Proof. Let a k-tuple $\bar{x}_0, \bar{x}_1, \ldots, \bar{x}_{k-1}$ be a (*)-cycle in R^N for a mapping Φ. Then the k-tuple $\bar{0}, \bar{x}_1 - \bar{x}_0, \ldots, \bar{x}_{k-1} - \bar{x}_0$ forms a (*)-cycle of length k for a mapping $\Psi(\bar{X}) = \Phi(\bar{X} + \bar{x}_0) - \bar{x}_0$, which is a polynomial mapping with coefficients from R.

So without any loss of generality we can assume that $\bar{x}_0 = \bar{0}$. Put $w(\bar{x}_1) = d \geq 1$. Then the vectors $\bar{0}, \pi^{-(d-1)}\bar{x}_1, \ldots, \pi^{-(d-1)}\bar{x}_{k-1}$ form a (*)-cycle of length k for $\Psi(\bar{X}) = \pi^{-(d-1)}\Phi(\pi^{d-1}\bar{X})$ which is a polynomial mapping with coefficients from R (as $\pi^{-(d-1)}\Phi(\bar{0}) = \pi^{-(d-1)}\bar{x}_1 \in R^N$). □

The cosets of elements of R^N (mod P) consist a linear space over R/P and $Lin(S)$ means a linear space spanned on a set S as a linear subspace of $(R/P)^N$.

For a cycle $\bar{x}_0, \ldots, \bar{x}_{k-1}$ we sometimes extend the indices by putting $\bar{x}_k = \bar{x}_0, \bar{x}_{k+1} = \bar{x}_1$, and so on.

Proposition 3.4. *([Pe3]) Let $\bar{0}, \bar{x}_1, \ldots, \bar{x}_{k-1}$ be a (*)-cycle in R^N (i.e. for a suitable polynomial mapping with coefficients from R). Then one has that $w(\bar{x}_m) \leq w(\bar{x}_n)$ for $m|n$(also for $m, n \geq k$).*

Proposition 3.5. *Let $\bar{0}, \bar{x}_1, \ldots, \bar{x}_{k-1}$ be a (*)-cycle in R^N for Φ. Put $\Phi'(\bar{0}) = A$. Write*

$\{w(\bar{x}_1), \ldots, w(\bar{x}_{k-1})\} = \{d_1 < d_2 < \cdots < d_r\}$ and $m_i = \min\{j : w(\bar{x}_j) = d_j\}$.

Then $1 = m_1|m_2|\ldots|m_r|k$ and

$\frac{m_{i+1}}{m_i} = \min\{j : (I + A^{m_i} + \cdots + A^{(j-1)m_i})\pi^{-d_i}\bar{x}_{m_i} \equiv \bar{0} \pmod P\}$ for $i = 1, 2, \ldots, r$, where we put $m_{r+1} = k$.

Moreover, for $i = 1, \ldots, r$ we have $\frac{m_{i+1}}{m_i} \leq p^{fN}$ and

$$(3.1) \quad (I + A^{m_i} + \cdots + A^{(\frac{m_{i+1}}{m_i} - 1)m_i})|_{Lin(\pi^{-d_i}\bar{x}_{m_i} + PR^N, A^{m_i}\pi^{-d_i}\bar{x}_{m_i} + PR^N, \ldots)} = 0$$

and

$$(3.2) \quad (I + A^{m_i} + \cdots + A^{(\frac{m_{i+1}}{m_i} - 1)m_i})|_{Lin(\pi^{-d_i}\bar{x}_{m_i} + PR^N, \pi^{-d_i}\bar{x}_{2m_i} + PR^N, \ldots)} = 0$$

So in particular

$(A^{m_{i+1}} - I)|_{Lin(\pi^{-d_i}\bar{x}_{m_i} + PR^N, A^{m_i}\pi^{-d_i}\bar{x}_{m_i} + PR^N, \ldots)} = 0$ and

$(A^{m_{i+1}} - I)|_{Lin(\pi^{-d_i}\bar{x}_{m_i} + PR^N, \pi^{-d_i}\bar{x}_{2m_i} + PR^N, \pi^{-d_i}\bar{x}_{3m_i} + PR^N, \ldots)} = 0.$

Proof. From the very definition of the numbers m_i we have that the cosets

$$\bar{0}, \pi^{-d_i}\bar{x}_{m_i} + PR^N, \ldots, \pi^{-d_i}\bar{x}_{(\frac{m_{i+1}}{m_i} - 1)m_i} + PR^N$$

are all different (mod P). So $\frac{m_{i+1}}{m_i} \leq p^{fN}$.

The formula (2) follows from (1) and the following formula(which could be derived from the Taylor's expansion)

$$\pi^{-d_i}\bar{x}_{(l+1)m_i} + PR^N = A^{m_i}\pi^{-d_i}\bar{x}_{lm_i} + \pi^{-d_i}\bar{x}_{m_i} + PR^N.$$

The rest was proved in [Pe3]. □

Proposition 3.6. *([Pe2]) Let $\Phi : R^N \mapsto R^N$ be a polynomial mapping with, as always, coefficients from R. Put $\Phi(\bar{0}) = \bar{x}, w(\bar{x}) = d, \Phi'(\bar{0}) = A$. Then $\Phi^s(\bar{0}) \equiv (A^{s-1} + A^{s-2} + \cdots + A + I)\bar{x} \pmod{P^{2d}}$.*

Let $\mathcal{G}(R/P, M)$ denotes the set of orders prime to p of cyclic subgroups of the linear group $GL_M(R/P)$ of invertible matrices $M \times M$ with coefficients from the field R/P.

Let $\mathcal{H}(R/P, M)$ denotes the set of orders prime to p of elements $A \in GL_M(R/P)$ such that for some $\bar{y} \in (R/P)^M$ the vectors $\bar{y}, A\bar{y}, A^2\bar{y}, \dots$ span the whole $(R/P)^M$.

Proposition 3.7. *([Pe3]) Let R be as above. Then*

(a) *the length of a polynomial cycle in R^N can be written in the form ab, where a is the length of a certain (*)-cycle in R^N and $b \le p^{fN}$. Conversely, every number of that form is a length of a suitable cycle in R^N. As 1-tuple $\bar{0}$ forms a (*)-cycle for zero mapping we have in particular:*

$$\{1, 2, \dots, p^{fN}\} \subset \mathcal{CYCL}(R, N);$$

(b) *the length of a (*)-cycle for a polynomial mapping in R^N is of the form:*

$$p^{\alpha} \prod_{i=1}^{t} h_i,$$

where $h_i \in \mathcal{H}(R/P, l_i), l_1 + \dots + l_t \le N$;

(c) *Let $\widehat{R}$ be the completion of the ring R with respect to the norm v. Then $\mathcal{CYCL}(R, N) = \mathcal{CYCL}(\widehat{R}, N)$.*

Remark 3.1. For every ring S we have that $k \in \mathcal{CYCL}(S, N)$ implies $l \in \mathcal{CYCL}(S, N)$ for every divisor l of k(it suffices to take a suitable iteration).

Proposition 3.8. *([Pe2]) If $\bar{x}_0, \dots, \bar{x}_{k-1}$ is a cycle in R^N then $w(\bar{x}_{i+j} - \bar{x}_i) = w(\bar{x}_{l+j} - \bar{x}_l)$ for every possible i, j, l, even bigger than k.*

4. Proof of Theorem 2.1

Owing to proposition 3.1 we have

$$\mathcal{CYCL}(Z, 2) = \bigcap_p \mathcal{CYCL}(Z_p, 2),$$

where Z_p is the p-adic ring.

In what follows we put $\bar{x}_k = \binom{x_k}{y_k}$. So x_k is the first coordinate of $\bar{x}_k$.

For $p = 2$ we try to find the shape of a (*)-cycles in Z_2^2. In this case we apply the results of subsection 3.2 to $R = Z_2, P = 2Z_2, \pi = 2$. Note that in this case $\mathcal{G}(R/P, 2) = \{1, 3\}$ and $\mathcal{G}(R/P, 1) = \{1\}$. This gives, by proposition 3.6 that (*)-cycles in Z_2^2 could have lengths only of the form $2^\alpha, 3 \cdot 2^\alpha$.

Note that a tuple $\binom{\pi}{0}, \binom{0}{\pi}, \binom{-\pi}{0}, \binom{0}{-\pi}$ is a (*)-cycle of length 4 for $\Phi(x, y) = (-y, x)$.

On the other hand a tuple $\binom{\pi}{0}, \binom{0}{\pi}, \binom{-\pi}{\pi}, \binom{-\pi}{0}, \binom{0}{-\pi}, \binom{\pi}{-\pi}$ is a (*)-cycle of lenght 6 for $\Phi(x, y) = (-y, x + y)$.

Note that two just mentioned (*)-cycles of length 4, 6 are suitable for every discrete valuation ring of characteristic zero with unity.

Lemma 4.1. *There are no (*)-cycles of length* 12 *in Z_2^2.*

Proof. Assume a contrary. By proposition 3.2 we then have a normalized (*)-cycle $\bar{0}, \bar{x}_1, \ldots, \bar{x}_{11}$ for a suitable Φ. Put $\Phi'(\bar{0}) = A$ and $\pi = 2$. Let $m_1, m_2, \ldots, m_r, d_1, \ldots, d_r, k$ be as in the proposition 3.4. So $k = 12, m_2 \leq 4$ and therefore $r \geq 2$.

1st case. $m_2 \in \{2, 4\}$. In this case $3 | \frac{k}{m_2} = \frac{m_3}{m_2} \cdot \ldots \cdot \frac{k}{m_r}$ and as all the quotients are ≤ 4 (by proposition 3.4) we have that there is unique $i \geq 2$ such that $3 = \frac{m_i+1}{m_i}$.

Again by proposition 3.4 we have
$(A^{2m_i} + A^{m_i} + I)\pi^{-d_i}\bar{x}_{m_i} \equiv \bar{0} \pmod P$ and $(A^{2m_i} + A^{m_i} + I)\pi^{-d_i}\bar{x}_{2m_i} \equiv \bar{0} \pmod P$.

But $\pi^{-d_i}\bar{x}_{m_i} + 2Z_2^2, \pi^{-d_i}\bar{x}_{2m_i} + 2Z_2^2$ are non-zero, distinct and hence linearly independent over $R/P = Z_2/2Z_2 = F_2$. Hence $A^{2m_i} + A^{m_i} + I \equiv 0 \pmod P$, i.e. it is a zero mapping, treated as a linear mapping of $(R/P)^2$.

By raising to the power 4, in view of the divisibility of suitable binomial coefficients by 2(which is an element of $P = 2Z_2$), we get that $A^{8m_i} + A^{4m_i} + I \equiv 0 \pmod P$.

By proposition 3.5, $(A^3 + A^2 + A + I)\bar{x}_1 \equiv \bar{x}_4 \equiv \bar{0} \pmod 4$ and hence $(A^4 - I)\frac{1}{2}\bar{x}_1 = (A - I)(A^3 + A^2 + A + I)\frac{1}{2}\bar{x}_1 \equiv \bar{0} \pmod 2$, whence $A^4\frac{1}{2}\bar{x}_1 \equiv \frac{1}{2}\bar{x}_1 \pmod 2$. Hence we obtain $(A^{8m_i} + A^{4m_i} + I)\frac{1}{2}\bar{x}_1 \equiv 3 \cdot \frac{1}{2}\bar{x}_1 \not\equiv \bar{0} \pmod 2$, a contradiction.

2nd case. $m_2 = 3$. In this case by proposition 3.4 $(A^2 + A + I)\frac{1}{2}\bar{x}_1 \equiv (A^2 + A + I)\frac{1}{2}\bar{x}_2 \equiv 0 \pmod P$. As $\frac{1}{2}\bar{x}_1 + PR^2, \frac{1}{2}\bar{x}_2 + PR^2$ are linearly independent over $R/P = F_2$ we have $A^2 + A + I \equiv 0 \pmod P$ and $A^3 \equiv I \pmod P$. This gives $(\Phi^3)'(\bar{0}) = \Phi'(\bar{x}_2) \circ \Phi'(\bar{x}_1) \circ \Phi'(\bar{0}) \equiv A^3 \equiv I \pmod P$(we used for instance $\bar{x}_1 \equiv \bar{0} \pmod P$, so $\Phi'(\bar{x}_1) \equiv \Phi'(\bar{0}) \pmod P$, where the congruence relation for matrices means that all corresponding components are congruent).

So we can write Φ^3 in the following form:

$\Phi^3(x, y) = (x_3 + (1 + 2a_1)x + 2b_1y + c_1x^2 + dxy + e_1y^2 + \ldots, y_3 + 2a_2x + (1 + 2b_2)y + c_2x^2 + Dxy + e_2y^2 + \ldots)$. Using such notation we silently assume that $a_1, a_2, b_1, \ldots$.. are from R.

As $w(\bar{x}_3) \geq 2$ we then have

$$(\Phi^6)'(\bar{0}) = (\Phi^3)'(\bar{x}_3) \circ (\Phi^3)'(\bar{0}) \equiv ((\Phi^3)'(\bar{0}))^2 = (\begin{pmatrix} 1 + 2a_1 & 2b_1 \\ 2a_2 & 1 + 2b_2 \end{pmatrix})^2 \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{P^2}.$$

Now by proposition 3.5 $\bar{0} = \bar{x}_{12} \equiv (I + (\Phi^6)'(\bar{0}))\bar{x}_6 \pmod{P^{2w(\bar{x}_6)}}$ and hence, as $w(\bar{x}_6) \geq 2$ we have $\bar{0} \equiv (I + (\Phi^6)'(\bar{0}))\bar{x}_6 \pmod{P^{w(\bar{x}_6)+2}}$.

So $\bar{0} \equiv 2\bar{x}_6 \pmod{P^{w(\bar{x}_6)+2}}$ what leads to contradiction as $w(2\bar{x}_6) = 1 + w(\bar{x}_6) < w(\bar{x}_6) + 2$. □

Notice that the remark 3.1 now gives that in Z_2^2 there are no (*)-cycles of length $24, 36, 48, \ldots$.

Lemma 4.2. *There are no (*)-cycles of length* 8 *in* Z_2^2.

Proof. Assume a contrary, i.e. we have a normalized (*)-cycle $\bar{0}, \bar{x}_1, \ldots, \bar{x}_7$ in Z_2^2 for a mapping Φ. Again we put $\Phi'(\bar{0}) = A$ and $\pi = 2$. Moreover, put $(\Phi^2)'(\bar{0}) = A_1, (\Phi^4)'(\bar{0}) = A_2$ and $\Phi(x, y) = (x_1 + \alpha x + \beta y + c_1x^2 + dxy + e_1y^2 + \ldots, y_1 + \gamma x +$

"'s

Sy -f C2X² + Dxy 4- e₂;y² + •••)• Furthermore mi,7712,... ,di,... are defined in the similar manner like in lemma 4.1.

As ra₂|8 and m₂ < 4 we háve ra₂ 6 {2,4}.

Ist čase. rn₂ = 4. Since in this čase ~x\ 4- PR?, \x₂ 4- PR² are Iineariy independent over R/P, the matrix 5 = {\xi,\x-2) with entries from R = Z₂ is invertible.

Then 0, B~ⁱž\,..., B~ⁱxy is a (*)~cycle for P⁻¹ o $ o B with coefficients from i?. Moreover, notě that w(B~~ⁱx) = w(x), so m₂ is preserved.

Hence we can asstime that X\ — („), x₂ — (₂) •

As |xj, |Ť2, ^3 are pairwise incongruent (mod P) we must háve \x₃ = (|) (mod P). So ž₃ = g) (mod P²).

From proposition 3.5 we háve (X2) = (/ + A.)(XI) (mod P²). This gives (°) =

(* + Q ! I s) © (mod P²) and a = 1 (mod P),

7 = 1 (mod P).

In the similar manner x₃ = (²) = (/ 4- A 4- -4²)(Q) (mod P²) and by easy calculation Í?E0 (mod P),6 ~ 1 (mod P).

So vl = (j J J (mod P).

If * = © Ě P** = 2X1 then #•(,,„ H (« + * f + *) [mod P²).

Now

(*⁴)'(0)

/ a + dy₃ 0 + dx₃ \ f <* + dy₂ 0 + dx₂ \
\ 7 + Dí/3 S 4- Dx₃) V 7 + Dy₂ 6 + Dx₂) '
{ a + dy₁ 0 + d x i \ / a 0 \
\ 7 + Dyi 6 + Dxₓ) \ 7 S) ~
a 0 V (dy₃ dx₃ \ (l Q\ (\ 0 \ / dy₂ dx₂
7 5) +\Dy₃ Dx₃ J{ 1 1) + ^ 1 1 yl ^ Zty₂ ,0^2
%i dii W 1 0 \ / 1 o \ / 2d 2d \ (1 0 \
Dyi ZJan ; 1 1 y - V 0 1) + { 2D 2D) \ 1 1 J +

(í ;) (s s)⁺(s 2S)(i ?) - (i ?)&-"')-

Hence, by proposition 3.5 and w(x₄) > 2 we háve

0 = x₈ = (/ + ($⁴)'(0))2ř₄ (mod P²ᵘ'(^)) and

0 S í d 1] (2ž₄) (mod p*»(*4)+2^ which gives a contradiction since W(2XA) < w(x₄) 4- 2 and (d 1 1 is invertible.

2nd čase. m₂ = 2 As in the čase m₂ = 4 we can assume that ži = Q) (more strictly in the reasoning from the čase m₂ = 4 we také P(J) = \x\ and we determine B(°) in such a way that P is invertible).

In view of $w(\bar{x}_2) \geq 2$ and proposition 3.5 we have $\bar{0} \equiv \bar{x}_2 \equiv (I + A)\binom{2}{0}$ (mod P^2) and $\alpha \equiv 1$ (mod P), $\gamma \equiv 0$ (mod P). Write $\alpha = 1 + 2a, \gamma = 2\Gamma$. Proposition 3.7 gives $\bar{x}_3 \equiv \bar{x}_1 \equiv \binom{2}{0}$ (mod P^2).

Taking this into account we get

$$(\Phi^4)'(\bar{0}) \equiv \Phi'(\bar{x}_3) \circ \Phi'(\bar{x}_2) \circ \Phi'(\bar{x}_1) \circ \Phi'(\bar{0}) \equiv (\Phi'(\bar{x}_1) \circ \Phi'(\bar{0}))^2 \equiv$$

$$(\begin{pmatrix} 1+2a & \beta+2d \\ 2\Gamma & \delta+2D \end{pmatrix}\begin{pmatrix} 1+2a & \beta \\ 2\Gamma & \delta \end{pmatrix})^2$$

$$\equiv \begin{pmatrix} 1+2\beta(1+\delta)^2\Gamma & (\beta+2a\beta+\beta\delta+2d\delta)(1+\delta^2+2D\delta) \\ 2\Gamma(1+\delta)(1+\delta^2) & 2\Gamma\beta(1+\delta)^2+\delta^4 \end{pmatrix} \pmod{P^2}.$$

From $w(\bar{x}_4) \geq w(\bar{x}_2) \geq 2$ and proposition 3.5 we have $\bar{0} = \bar{x}_8 \equiv (I+(\Phi^4)'(\bar{0}))\bar{x}_4$ (mod $P^{w(\bar{x}_4)+2}$). So, we then have

$$\begin{pmatrix} 2+2\beta(1+\delta)^2\Gamma & (\beta+2a\beta+\beta\delta+2d\delta)(1+\delta^2+2D\delta) \\ 2\Gamma(1+\delta)(1+\delta^2) & 2\Gamma\beta(1+\delta)^2+1+\delta^4 \end{pmatrix}\begin{pmatrix} x_4 \\ y_4 \end{pmatrix}$$

$$\equiv \bar{0} \pmod{P^{w(\bar{x}_4)+2}}. \tag{4.1}$$

If in (3) we take $\delta \equiv 1$ (mod P) then we get $2\bar{x}_4 \equiv \bar{0}$ (mod $P^{w(\bar{x}_4)+2}$), what leads to a contradiction.

If in (3) we take $y_4 \not\equiv \bar{0}$ (mod $P^{w(\bar{x}_4)+1}$) then from $x_4 \equiv 0$ (mod $P^{w(\bar{x}_4)}$) we get $1 + \delta^4 \equiv 0$ (mod P) and $\delta \equiv 1$ (mod P), what is impossible according to the previous reasoning.

So we must have $y_4 \equiv 0$ (mod $P^{w(\bar{x}_4)+1}$) and $\delta \equiv 0$ (mod P). Now (3) leads to $(2 + 2\beta\Gamma)x_4 + \beta y_4 \equiv 0$ (mod $P^{w(\bar{x}_4)+2}$), $2\Gamma x_4 + y_4 \equiv 0$ (mod $P^{w(\bar{x}_4)+2}$). If we subtract from the first congruence the second multiplied by β we get $2x_4 \equiv 0$ (mod $P^{w(\bar{x}_4)+2}$) and $x_4 \equiv 0$ (mod $P^{w(\bar{x}_4)+1}$). Hence $\bar{x}_4 \equiv \bar{0}$ (mod $P^{w(\bar{x}_4)+1}$), a contradiction. □

So we have obtained that a (*)-cycle of length k exists in Z_2^2 if and only if $k \in \{1, 2, 3, 4, 6\}$. Now proposition 3.6(i) gives that a cycle of length k exists in Z_2^2 if and only if $k \in \{1, 2, 3, 4, 6, 8, 9, 12, 16, 18, 24\}$.

To obtain the theorem 2.1 by remark 3.1 it suffices to show that for every prime $p \geq 3$ there are cycles of lengths 24, 18, 16 in Z_p^2. As $24 = 4 \cdot 6, 18 = 3 \cdot 6, 16 = 4 \cdot 4$ and there are (*)-cycles of lengths 6, 4 in Z_p^2(look at the examples just before lemma 4.1) we arrive at the statement as $3, 4 \leq p^2$.

5. Proof of Theorem 2.2

We start with an auxiliary lemma:

Lemma 5.1. *For every natural n there are polynomials $f, g \in Z[T, X]$ and non-zero $m \in Z[T]$ such that*

$$f(T,X)T^{2^{n+1}-1}\prod_{k=0}^{n-1}((XT)^{2^n-2^k}-1) + g(T,X)\prod_{k=0}^{n-1}(X^{2^n-2^k}-1) = m(T).$$

Proof. The polynomials $T^{2^{n+1}-1}\prod_{k=0}^{n-1}((XT)^{2^n-2^k}-1)$ and $\prod_{k=0}^{n-1}(X^{2^n-2^k}-1)$ are coprime when treated as polynomials of variable X over a field $Q(T)$. The rest is obvious. □

To finish the proof of theorem 2.2 take fixed s such that $m(s) \neq -1,0,1$ and $b = m(s)$. Now consider $\Phi(X,Y) = (X^2 - g(s,b)X(X-b)(X-b^2)\dots(X-b^{2^{n-1}}) - f(s,b)Y(Y-bs)(Y-b^2s^2)\dots(Y-b^{2^{n-1}}s^{2^{n-1}}), Y^2 - s^{2^{n+1}}g(s,b)X(X-b)\dots(X-b^{2^{n-1}}) - s^{2^{n+1}}f(s,b)Y(Y-bs)(Y-b^2s^2)\dots(Y-b^{2^{n-1}}s^{2^{n-1}}))$.

An easy calculation gives $\Phi^j(b,bs) = (b^{2^j}, b^{2^j}s^{2^j})$ for $j = 0,1,\dots,n$ and $\Phi^{n+1}(b,bs) = \Phi^{n+2}(b,bs) = \dots = (0,0)$. From this we have $\#\mathcal{ORB}((b,bs),\Phi) = n+2$, as $b \neq -1,0,1$. As n could be sufficiently large we arrive at the statement of the theorem.

References

[NP] Narkiewicz,W., Pezda,T. *Finite polynomial orbits in finitely generated domains* , Mh.Math. 124, 309-316 (1997).

[Pe1] Pezda,T. *Polynomial cycles in certain local domains* , Acta Arith., LXVI.1,1994, 11–22

[Pe2] Pezda,T. *Cycles of polynomial mappings in several variables* , Manuscr. Math.,83,1994,279-289.

[Pe3] Pezda,T. *Cycles of polynomial mappings in several variables over rings of integers in finite extensions of rationals* , Acta Arith., to appear.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF WROCLAW, PL.GRUNWALDZKI 2/4, 50-384 WROCLAW, POLAND

E-mail address: pezda@math.uni.wroc.pl