ACTA ARITHMETICA
LXVI.1 (1994)

Polynomial cycles in certain local domains

by

T. Pezda (Wrocław)

1. Let R be a domain and $f \in R[X]$ a polynomial. A k-tuple $x_0, x_1, \ldots \ldots, x_{k-1}$ of distinct elements of R is called a *cycle* of f if

$$f(x_i) = x_{i+1} \quad \text{for } i = 0, 1, \ldots, k-2 \quad \text{and} \quad f(x_{k-1}) = x_0\,.$$

The number k is called the *length* of the cycle. A tuple is a cycle in R if it is a cycle for some $f \in R[X]$.

It has been shown in [1] that if R is the ring of all algebraic integers in a finite extension K of the rationals, then the possible lengths of cycles of R-polynomials are bounded by the number $7^{7\cdot 2^N}$, depending only on the degree N of K. In this note we consider the case when R is a discrete valuation domain of zero characteristic with finite residue field.

We shall obtain an upper bound for the possible lengths of cycles in R and in the particular case $R = \mathbb{Z}_p$ (the ring of p-adic integers) we describe all possible cycle lengths. As a corollary we get an upper bound for cycle lengths in the ring of integers in an algebraic number field, which improves the bound given in [1].

The author is grateful to the referee for his suggestions, which essentially simplified the proof in Subsection 6 and improved the bound for $C(p)$ in Theorem 1 in the case $p = 2, 3$.

2. Let R be a discrete valuation domain of zero characteristic with finite residue field having cardinality $N(P) = p^f$. Fix a generator π of the prime ideal P of R and denote by v the norm (multiplicative valuation) of R, normalized so that $v(\pi) = 1/p$. Moreover, put $v(p) = p^{-\operatorname{ord} p}$. A cycle $x_0, x_1, \ldots, x_{k-1}$ will be called a $(*)$-*cycle* if $v(x_i - x_j) < 1$ for $i \ne j$.

We shall prove the following results:

Supported by the KBN grant 2 1037 91 01.

Theorem 1. (i) *The length of a* $(*)$*-cycle in* R *does not exceed* $(N(P)-1)p^{C(p)}$, *where*

$$C(p) = 1 + \frac{\log(\operatorname{ord} p)}{\log 2}\,.$$

(ii) *The length of a cycle in* R *does not exceed* $N(P)(N(P)-1)p^{C(p)}$, *where* $C(p)$ *is given in* (i).

In case of $R = \mathbb{Z}_p$ we can be more precise:

Theorem 2. (i) *A* $(*)$*-cycle of length* n *exists in* $\mathbb{Z}_p$ *if and only if* n *is a divisor of* $p-1$ *except for* $p = 2, 3$ *in which case* n *can be any integer not exceeding* p.

(ii) *If* $p > 3$ *then a cycle of length* n *exists in* $\mathbb{Z}_p$ *if and only if* $n = ab$, *where* a *is a divisor of* $p-1$ *and* $b \le p$. *The set of possible cycle lengths in* $\mathbb{Z}_2$ *is* $\{1,2,4\}$, *and in* $\mathbb{Z}_3$ *it is* $\{1,2,3,4,6,9\}$.

Corollary 1. *Let* R *be the ring of all integers in an algebraic number field of degree* N *over the rationals. The cycle lengths in* R *are bounded by* $(2^N-1)2^{N+1}$.

Corollary 2. *If* k *is the length of a cycle in* R *then*

$$k \le \min(N(P_1)(N(P_1)-1)N(P_2)(N(P_2)-1))\,,$$

the minimum being taken over all pairs P_1, P_2 *of prime ideals with*

$$\operatorname{char}(R/P_1) \ne \operatorname{char}(R/P_2)\,.$$

For cyclotomic fields K the bound given in Corollary 1 can be essentially improved:

Corollary 3. *Let* K_M *be the* M*-th cyclotomic field and* R *its ring of integers. The cycle lengths in* R *do not exceed* $c_4(\varepsilon)M^{2L+\varepsilon}$ *for every* $\varepsilon > 0$, *where* L *denotes the Linnik constant.*

Note that $N = [K_M : Q] = \varphi(M) \gg M/\log\log M$, and thus the cycle lengths in this case do not exceed $c_5(\varepsilon)N^{2L+\varepsilon}$ for every $\varepsilon > 0$, which is a much better bound than that resulting from Corollary 1.

3. We list first certain simple properties of cycles in arbitrary domains. We use the following convention: if $x_0, x_1, \ldots, x_{k-1}$ is a cycle, then for $n \equiv r \pmod{k}$, $0 \le r < k \le n$ we put $x_n = x_r$. For $a, b \in R$ we write $a \sim b$ if a, b are associated, i.e. differ by an invertible factor.

Lemma 1. *Let* R *be a domain and let* $x_0, \ldots, x_{k-1}$ *be a cycle in* R *for the polynomial* $F(X) = a_nX^n + \ldots + a_1X + a_0$. *Then*

(i) *this cycle is a cycle for some polynomial* G *of degree not exceeding* $k-1$,

(ii) *if* $a, b \in R$, *a is a unit in* R *and* $y_i = ax_i + b$ $(i = 0, \ldots, k-1)$, *then* $y_0, \ldots, y_{k-1}$ *is a cycle for some polynomial over* R,

(iii) *if* $k = rs$ *then* $x_0, x_{1\cdot r}, \ldots, x_{(s-1)r}$ *is a cycle for some polynomial*,

(iv) *for* $0 < r < k$ *one has* $(x_{i+r} - x_i) \sim (x_{j+r} - x_j)$,

(v) *if* $(i - j, k) = 1$ *then* $(x_i - x_j) \sim (x_1 - x_0)$,

(vi) *if* $x_i = ay_i$, $a, y_i \in R$, *then* $y_0, \ldots, y_{k-1}$ *is a cycle for some polynomial.*

Proof. (i) Take for G the remainder of the division of F by $(X - x_0)\ldots$ $\ldots(X - x_{k-1})$.

(ii) The polynomial $G(X) = aF((X - b)a^{-1}) + b \in R[X]$ will do.

(iii) The sequence $x_0, x_r, \ldots, x_{(s-1)r}$ is a cycle for the rth iteration of F.

(iv) Notice that

$$\frac{F(X) - F(Y)}{X - Y} = a_n(X^{n-1} + \ldots + Y^{n-1}) + \ldots + a_2(X + Y) + a_1 \in R[X, Y]$$

and thus $x_r - x_0 \mid x_{r+1} - x_1 \mid \ldots \mid x_{k+r-1} - x_{k-1} \mid x_r - x_0$.

(v) In view of (iv) it suffices to deal with the case $j = 0$. If $t > 0$ is defined by $t \cdot i \equiv 1 \pmod{k}$ then $x_i - x_0 \mid x_{2i} - x_i \mid \ldots \mid x_{ti} - x_{(t-1)i}$, hence $x_i - x_0 \mid (x_i - x_0) + (x_{2i} - x_i) + \ldots + (x_{ti} - x_{(t-1)i}) = x_{ti} - x_0 = x_1 - x_0$, but of course $x_1 - x_0 \mid (x_1 - x_0) + \ldots + (x_i - x_{i-1}) = x_i - x_0$.

(vi) The y_i's form a cycle for $G(X) = a^{-1}F(aX) \in R[X]$. ∎

PROOF OF THEOREM 1

4. From now on we assume that R satisfies the conditions stated at the beginning of Subsection 2.

Lemma 2. *The length of any cycle in* R *is a product of primes not exceeding* $N(P)$.

Proof. In view of Lemma 1(iii) it suffices to show that if q is a prime exceeding $N(P)$ then there cannot be a cycle of length q in R. Let $x_0, \ldots, x_{q-1}$ be such a cycle. In view of Lemma 1(v) one has $v(x_i - x_j) = v(x_1 - x_0) = p^{-r}$ for $x_i \neq x_j$. Thus we can write $x_i = x_0 + \pi^r w_i$ $(1 \le i < q)$ where $w_i \notin P$ and $w_i - w_j \notin P$ for $1 \le i < j < q$, a contradiction. ∎

Lemma 3. *If* k *is a cycle length in* R *then* $k = ab$, *where* a *is the length of some* $(*)$-*cycle in* R *and* $b \le N(P)$.

Proof. Let $x_0, \ldots, x_{k-1}$ be a cycle. Assume first that for some $i > 0$ we have $v(x_i - x_0) < 1$, and denote by b the smallest integer with this property. Then $b \mid k$. In fact, if $k = qb + r$, $0 < r < b$, then by Lemma 1(iv)

$$v(x_{b-r} - x_0) = v(x_{(q+1)b} - x_0) \le \max\{v(x_{(q+1)b} - x_{qb}), \ldots, v(x_b - x_0)\} < 1\,,$$

contradicting the choice of b.

It is obvious that either there exists a pair $1 \le r < s < b$ with $x_r - x_0 \equiv x_s - x_0 \pmod{P}$, and then $v(x_{s-r} - x_0) = v(x_s - x_r) < 1$, which is impossible, or all differences $x_r - x_0$ $(r = 1, \ldots, b-1)$ are distinct $\pmod{P}$ and since they cannot lie in P we get $b \le N(P)$, as asserted. The numbers $x_0, x_b, \ldots, x_{(a-1)b}$ form a $(*)$-cycle. ∎

5. Now we shall consider the lengths of $(*)$-cycles.

LEMMA 4. *Let $y_0, y_1, \ldots, y_{q-1}$ be a $(*)$-cycle of $F(X) = a_n X^n + \ldots + a_1 X + a_0$, q prime, $y_0 = 0$. Then either $q \mid N(P) - 1$, or $q = p$ and $a_1 \equiv 1 \pmod{P}$.*

Proof. Clearly

$$\begin{aligned}\frac{y_{k+2} - y_{k+1}}{y_{k+1} - y_k} &= \frac{F(y_{k+1}) - F(y_k)}{y_{k+1} - y_k}\\ &= a_n(y_{k+1}^{n-1} + \ldots + y_k^{n-1}) + \ldots + a_2(y_{k+1} + y_k) + a_1\\ &\equiv a_1 \pmod{P},\end{aligned}$$

and thus

$$1 = \prod_{k=1}^{q} \frac{y_{k+2} - y_{k+1}}{y_{k+1} - y_k} \equiv a_1^q \pmod{P}.$$

This implies

$$a_1^{(q, N(P)-1)} \equiv 1 \pmod{P}$$

and hence $q \mid N(P) - 1$ or $a_1 \equiv 1 \pmod{P}$.

Consider $a_1 \equiv 1 \pmod{P}$ and write $v(y_1 - y_0) = p^{-d}$. Then

$$\frac{y_2 - y_1}{y_1 - y_0} \equiv F'(0) \equiv 1 \pmod{P},$$

whence $y_2 - y_1 \equiv y_1 - y_0 \pmod{P^{d+1}}$, and similarly we get $y_{k+2} - y_{k+1} \equiv y_{k+1} - y_k \equiv \ldots \equiv y_1 - y_0 \pmod{P^{d+1}}$. But then

$$0 = \sum_{k=1}^{q} (y_{k+1} - y_k) \equiv q(y_1 - y_0) \pmod{P^{d+1}}$$

and $q = p$ follows. ∎

LEMMA 5. *Let $F \in R[X]$, $g = F'(0)$ and $a_k = F^k(0)$ with $v(a_1) = p^{-d}$, $d > 0$. Then*

$$a_k \equiv (1 + g + \ldots + g^{k-1}) a_1 \pmod{P^{2d}}.$$

Proof. Easy recurrence. ∎

LEMMA 6. *If m is the length of a $(*)$-cycle in R and $p \nmid m$, then $m \mid N(P) - 1$.*

Proof. Let $y_0, \ldots, y_{m-1}$ be such a cycle realized by F. In view of Lemma 1(ii), (vi) we can assume without loss of generality that $y_0 = 0$ and $y_1 = \pi$. If we put $g = (y_2 - y_1)/(y_1 - y_0)$, then

$$\frac{y_{k+1} - y_k}{y_k - y_{k-1}} \equiv g \pmod{P}$$

and by Lemma 5,

$$y_k \equiv (1 + g + \ldots + g^{k-1})\pi \pmod{P^2}. \tag{1}$$

Suppose that for some $0 < r < m$ we have

$$y_r \in P^2 \tag{2}$$

and let M be the smallest such r. Then $g^M \equiv 1 \pmod{P}$ and $M \mid m$ since $y_m = 0 \in P^2$. Let $v(y_M) = p^{-d}$ $(d \geq 2)$ and write

$$\underbrace{F \circ \ldots \circ F}_{M \text{ times}}(X) = F^M(X) = b_t X^t + \ldots + b_1 X + b_0 .$$

Since

$$b_1 \equiv F'(0)^M \equiv g^M \equiv 1 \pmod{P}$$

we get

$$y_{(k+2)M} - y_{(k+1)M} \equiv y_{(k+1)M} - y_{kM} \pmod{P^{d+1}}$$

and

$$0 = \sum_{k=1}^{m/M} (y_{(k+1)M} - y_{kM}) \equiv \frac{m}{M}(y_M - y_0) \pmod{P^{d+1}}$$

gives a contradiction.

Thus (2) does not hold and $y_1, \ldots, y_{m-1} \notin P^2$. If $m \nmid N(P) - 1$, then $g^m \equiv 1 \pmod{P}$, $g^{N(P)-1} \equiv 1 \pmod{P}$, $g^{(m, N(P)-1)} \equiv 1 \pmod{P}$ and using (1) and remembering that $g \not\equiv 1 \pmod{P}$ we get $y_{(m,N(P)-1)} \in P^2$, which contradicts the last statement. ∎

6. By Lemmas 3 and 6 it remains to consider $(*)$-cycles of lengths p^α.

Proposition. *If there is a $(*)$-cycle of length p^α, then $\alpha \leq C(p)$, where $C(p)$ is defined in Theorem* 1.

Proof. Let $x_0, x_1, \ldots, x_{p^\alpha - 1}$ be a $(*)$-cycle. By Lemma 1 we can assume that $x_0 = 0$ and $v(x_1) = p^{-1}$. For $0 \leq k \leq \alpha - 1$, put $v(x_{p^k}) = p^{-d_k}$ (so in particular $d_0 = 1$), and $\lambda_k = (F^{p^k})'(0)$. So for $k \leq \alpha - 1$ one has

$$1 = \prod_{l=1}^{p^{\alpha-k}} \frac{x_{(l+1)p^k} - x_{l \cdot p^k}}{x_{l \cdot p^k} - x_{(l-1)p^k}} \equiv (\lambda_k)^{p^{\alpha-k}} \pmod{P} \quad \text{and} \quad \lambda_k \equiv 1 \pmod{P}.$$

Write $\lambda_k = 1 + u_k \pi^{w_k}$, where $u_k \notin P$, $w_k \geq 1$, putting $w_k = \infty$ in case $\lambda_k = 1$.

Lemma 5 gives

$$x_{p\cdot p^k} \equiv (1+\lambda_k+\ldots+\lambda_k^{p-1})x_{p^k} \pmod{P^{2d_k}}.$$

If $\lambda_k = 1$ then for $d_{k+1} < 2d_k$ one has $d_{k+1} = d_k + \operatorname{ord} p$, and if $\lambda_k \neq 1$ then

$$x_{p\cdot p^k} \equiv \frac{(1+u_k\pi^{w_k})^p - 1}{u_k\pi^{w_k}} x_{p^k} \pmod{P^{2d_k}},$$

leading to

$$x_{p\cdot p^k} \equiv \left(p + \binom{p}{2} u_k\pi^{w_k} + \ldots \right.$$
$$\left. \ldots + \binom{p}{p-1}(u_k\pi^{w_k})^{p-2} + (u_k\pi^{w_k})^{p-1}\right) x_{p^k} \pmod{P^{2d_k}}.$$

Hence if $d_{k+1} < 2d_k$ then $d_{k+1} \geq \min(d_k + \operatorname{ord} p,\, d_k + (p-1)w_k)$ and we arrive at

(3) $$d_{k+1} \geq \min(2d_k, d_k + \operatorname{ord} p, d_k + (p-1)w_k).$$

By putting $k = \alpha - 1$ we get

$$p + \binom{p}{2}(u_{\alpha-1}\pi^{w_{\alpha-1}}) + \ldots + \binom{p}{p-1}(u_{\alpha-1}\pi^{w_{\alpha-1}})^{p-2}$$
$$+ (u_{\alpha-1}\pi^{w_{\alpha-1}})^{p-1} \in P^{d_{\alpha-1}}.$$

If $w_{\alpha-1}(p-1) \neq \operatorname{ord} p$ then

(4) $$d_{\alpha-1} \leq \operatorname{ord} p.$$

Otherwise

(5) $$w_{\alpha-1}(p-1) = \operatorname{ord} p.$$

For $k \leq \alpha - 2$ one has

$$\lambda_{k+1} = (F^{p^{k+1}})'(0) = \prod_{j=0}^{p-1} (F^{p^k})'(x_{j\cdot p^k}) \equiv \lambda_k^p \pmod{P^{d_k}},$$

and thus we obtain

(6) $$w_{k+1} \geq \min(d_k, w_k + \operatorname{ord} p, pw_k).$$

In the case $p = 2$ we need stronger inequalities. Since

$$\lambda_{k+1} \equiv \lambda_k(\lambda_k + (F^{p^k})''(0)x_{p^k}) \pmod{P^{2d_k}},$$

and $2 \mid (F^{p^k})''(0)$ the inequality

(7) $$w_{k+1} \geq \min(2d_k, w_k + \operatorname{ord} 2, 2w_k, d_k + \operatorname{ord} 2)$$

results.

Lemma 7. *For $k = 0, 1, \ldots, \alpha - 1$ one has* $\min(d_k, w_k) \leq \operatorname{ord} p$.

Proof. If the assertion failed for some k, then (3) and (6) would imply

$$w_{\alpha-1}, d_{\alpha-1} > \operatorname{ord} p\,,$$

contradicting (4) and (5). ∎

LEMMA 8. *For every prime p and for $k = 0, 1, \ldots, \alpha - 1$ one has*

(i) $d_k \geq 2^k$ *in case* $d_k \leq \operatorname{ord} p$,
(ii) $w_k \geq 2^{k-1}$ *if p is odd*,
(iii) $w_k \geq 2^k$ *if* $p = 2$.

Proof. First consider the case of $p \neq 2$. For $k = 0$ the assertion is obvious, and if it holds for some k, and $d_k \leq \operatorname{ord} p$, then by (3) and (6) we obtain $d_{k+1} \geq 2^{k+1}$ and $w_{k+1} \geq 2^k$, and if $d_k > \operatorname{ord} p$, then the preceding lemma implies $w_{k+1} \leq \operatorname{ord} p$ and (6) gives $w_{k+1} \geq 3 \cdot 2^{k-1} > 2^k$.

In case $p = 2$ the argument is the same, except that one uses (7) instead of (6). ∎

Using (4), (5) and Lemma 8 one immediately obtains the assertion of the Proposition. ∎

By the Proposition, Lemma 3 and Lemma 6 we get Theorem 1. ∎

7. Proof of Corollary 1. Let P be a prime ideal over $2\mathbb{Z}_K$, let f be its degree, e its ramification index, and $R = (\mathbb{Z}_K)_P$ the corresponding localization. Clearly the cycle lengths in $\mathbb{Z}_K$ cannot exceed the maximal cycle length in R. So in particular $N(P) = 2^f$, $\operatorname{ord} 2 = e$ and $f \cdot e \leq N = [K : Q]$. By using Theorem 1(i) one deduces $\alpha \leq e$; and as $e \leq N$ we conclude that the cycle lengths are bounded by

$$2^f(2^f - 1)2^e \leq 2^{N/e}(2^{N/e} - 1)2^e \leq 2^{N+1}(2^N - 1)\,. \ ∎$$

8. Proof of Corollary 2. As we have seen in the proof of Theorem 1 we can write $k = a_1 b_1 c_1 = a_2 b_2 c_2$ where $a_i \leq N(P_i)$, $b_i \mid (N(P_i) - 1)$, and c_i is a power of $p_i = \operatorname{char} R/P_i$. So

$$c_1 \mid a_2 b_2 c_2 \Rightarrow c_1 \mid a_2 b_2 \Rightarrow k \leq a_1 b_1 a_2 b_2\,. \ ∎$$

PROOF OF THEOREM 2

9. We start with the non-existence assertion.

LEMMA 9. (i) *If $y_0, \ldots, y_{p-1}$ is a $(*)$-cycle in $\mathbb{Z}_p$, and $v(y_1 - y_0) = p^{-d}$ then $(p-2)d \leq 1$.*

(ii) *If $p > 3$ then there are no $(*)$-cycles of length p in $\mathbb{Z}_p$. In $\mathbb{Z}_3$ there are no $(*)$-cycles of length 9 and in $\mathbb{Z}_2$ there are no $(*)$-cycles of length 4.*

Proof. (i) Let $y_0, y_1, \ldots, y_{p-1}$ be a $(*)$-cycle for $F(X) = a_{p-1} X^{p-1} + \ldots + a_0$ and $v(y_1 - y_0) = p^{-d}$, $d \geq 1$. In view of Lemma 1(ii) one can assume $y_i = p^d z_i$ for $i = 0, 1, \ldots, p-1$, with $z_0 = 0$, $z_1 = 1$.

Consider the linear system

$$(S) = \begin{cases} a_0 + a_1 y_0 + \ldots + a_{p-1} y_0^{p-1} = y_1, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_0 + a_1 y_{p-1} + \ldots + a_{p-1} y_{p-1}^{p-1} = y_0 . \end{cases}$$

If δ denotes its determinant, then $v(\delta) = p^{-dp(p-1)/2}$ by Lemma 1(v) and we get

$$p^{dp(p-1)/2} \mid \begin{vmatrix} 1 & y_0 & \ldots & y_0^{p-2} & y_1 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & y_{p-1} & \ldots & y_{p-1}^{p-2} & y_0 \end{vmatrix} \quad \text{and}$$

$$p^{d(p-2)} \mid \begin{vmatrix} 1 & z_0 & \ldots & z_0^{p-2} & z_1 - z_0 - 1 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & z_{p-1} & \ldots & z_{p-1}^{p-2} & z_0 - z_{p-1} - 1 \end{vmatrix} = \Delta, \quad \text{say}.$$

Since by Lemma 4, $F'(0) \equiv 1 \pmod p$, Lemma 5 gives $z_i \equiv i \pmod p$ $(i = 0, 1, \ldots)$ and thus

$$\Delta_k = \begin{vmatrix} 1 & z_0 & \ldots & z_0^{p-2} \\ \ldots & \ldots & \ldots & \ldots \\ 1 & z_{k-1} & \ldots & z_{k-1}^{p-2} \\ 1 & z_{k+1} & \ldots & z_{k+1}^{p-2} \\ \ldots & \ldots & \ldots & \ldots \\ 1 & z_{p-1} & \ldots & z_{p-1}^{p-2} \end{vmatrix} \equiv (-1)^k c \pmod p$$

with

$$c = \frac{1}{(p-1)!} \prod_{0 \leq i < j \leq p-1} (j - i) \not\equiv 0 \pmod p .$$

If we had $(p-2)d \geq 2$ then $p^2 \mid \Delta$. But

$$\Delta = \sum_{k=0}^{p-1} (-1)^k (z_{k+1} - z_k - 1) \Delta_k ,$$

and since $\Delta_k = (-1)^k c + p\alpha_k$ with a suitable $\alpha_k \in \mathbb{Z}_p$ we get

$$\begin{aligned} \Delta &= c \sum_{k=0}^{p-1} (z_{k+1} - z_k - 1) + p \sum_{k=0}^{p-1} (-1)^k (z_{k+1} - z_k - 1) \alpha_k \\ &\equiv -pc \not\equiv 0 \pmod{p^2} , \end{aligned}$$

since $z_{k+1} - z_k - 1 \equiv 0 \pmod p$ for $k = 0, 1, \ldots, p-1$, and this is a contradiction.

(ii) In case $p = 2, 3$ the assertion results from Theorem 1 and for $p > 3$ it is an immediate consequence of (i). ∎

LEMMA 10. *There are no* $(*)$-*cycles of length* 6 *in* $\mathbb{Z}_3$.

Proof. The preceding lemma shows that if 0, z_1, z_2 is a $(*)$-cycle in $\mathbb{Z}_3$, then $v(z_1) = 1/3$. Let $0, y_1, \ldots, y_5$ be a $(*)$-cycle of length 6 in $\mathbb{Z}_3$ realized by the polynomial $F(X) = a_5X^5 + \ldots + a_0$. Lemma 9(i) implies $v(y_2) = v(y_4) = 1/3$. This implies $v(y_1) = 1/3$ and $v(y_3) < 1/3$ since there are only three residue classes $\bmod 3$. Now Lemma 1 shows that it suffices to consider the cycle

$$0, 3, 6 + 9c, 9 \cdot 3^D u, 3 + 9 \cdot 3^D v, 6 + 9c + 3^D w\,,$$

with $D \ge 0$ and $3 \nmid uvw$.

Considering again the system (S) with determinant δ we get $v(\delta) = 3^{-18-3D}$. Put $\mathbf{A} = 2 + 3c + 3^{1+D}w$, $\mathbf{B} = 2 + 3c$. Observe that $a_2 \in \mathbb{Z}_3$ implies the divisibility of the determinant

$$\begin{vmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 2+3c & 1 & 1 & 1 \\ 1 & 2+3c & 3^{1+D}u & (2+3c)^3 & (2+3c)^4 & (2+3c)^5 \\ 0 & 3^{1+D}u & 3^{1+D}v & (3^{1+D}u)^3 & (3^{1+D}u)^4 & (3^{1+D}u)^5 \\ 0 & 3^{1+D}v & 3^{1+D}w & (1+3^{1+D}v)^3-1 & (1+3^{1+D}v)^4-1 & (1+3^{1+D}v)^5-1 \\ 0 & 3^{1+D}w & -3^{1+D}u & \mathbf{A}^3-\mathbf{B}^3 & \mathbf{A}^4-\mathbf{B}^4 & \mathbf{A}^5-\mathbf{B}^5 \end{vmatrix}$$

by 3^{4+3D}. All elements of the last three lines of this determinant are divisible by 3^{1+D}, hence

$$3 \,\Big|\, \begin{vmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 2 & 1 & 1 & 1 \\ 1 & 2 & 0 & 2 & 1 & 2 \\ 0 & u & v & 0 & 0 & 0 \\ 0 & v & w & 0 & v & 2v \\ 0 & w & -u & 0 & 2w & 2w \end{vmatrix}, \qquad 3 \mid vu + w^2 \quad \text{and} \quad 3 \mid uv + 1\,.$$

Now $a_3 \in \mathbb{Z}_3$ implies

$$3^{5+3D} \,\Big|\, \begin{vmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 2+3c & 1 & 1 \\ 1 & 2+3c & (2+3c)^2 & 3^{1+D}u & (2+3c)^4 & (2+3c)^5 \\ 0 & 3^{1+D}u & (3^{1+D}u)^2 & 3^{1+D}v & (3^{1+D}u)^4 & (3^{1+D}u)^5 \\ 0 & 3^{1+D}v & (1+3^{1+D}v)^2-1 & 3^{1+D}w & (1+3^{1+D}v)^4-1 & (1+3^{1+D}v)^5-1 \\ 0 & 3^{1+D}w & \mathbf{A}^2-\mathbf{B}^2 & -3^{1+D}u & \mathbf{A}^4-\mathbf{B}^4 & \mathbf{A}^5-\mathbf{B}^5 \end{vmatrix}$$

and here again all elements of the last three rows are divisible by 3^{1+D}, hence

$$3\,|\begin{vmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 2 & 1 & 1 \\ 1 & 2 & 1 & 0 & 1 & 2 \\ 0 & u & 0 & v & 0 & 0 \\ 0 & v & 2v & w & v & 2v \\ 0 & w & w & -u & 2w & 2w \end{vmatrix},$$

$$3\,|\,u(w^2 - v(u+w)) - v\cdot v\cdot w\,,$$

and

$$3\,|\,u - v - w(1+uv)$$

but since $3\,|\,uv+1$ we get $u \equiv v \pmod 3$, and $3\,|\,u^2+1$, a contradiction. ∎

10. Now we construct cycles with lengths listed in Theorem 2 and start with $(*)$-cycles. Obviously for any p the polynomial $-X+p$ realizes the $(*)$-cycle $0, p$ of length 2 in $\mathbb{Z}_p$, and the polynomial $-\frac{1}{2}X(X-3)+X+3$ realizes the $(*)$-cycle $0, 3, 6$ of length 3 in $\mathbb{Z}_3$, and this settles the exceptional cases in Theorem 2(i). The remaining cases of (i) are covered by the following lemma, which gives slightly more than needed:

LEMMA 11. *If R is a complete discrete valuation domain of zero characteristic with prime ideal $P = \pi R$ and finite residue field of $N(P)$ elements, then there exists a $(*)$-cycle of any length dividing $N(P)-1$.*

P r o o f. In view of Lemma 1(iii) it suffices to find a cycle of length $N(P)-1$. Clearly we may assume $N(P) > 2$. Denote by g_0 any primitive root $\bmod P$ and put

$$W(X) = 1 + X + X^2 + \ldots + X^{N(P)-2}\,. \tag{8}$$

Clearly $W(g_0) \equiv 0 \pmod P$, and Hensel's lemma shows the existence of a root $g \in R$ of W. The polynomial $gX + \pi$ realizes the cycle

$$0, \pi, (1+g)\pi, \ldots, (1+g+g^2+\ldots+g^{N(P)-3})\pi$$

of length $N(P)-1$. ∎

The proof of part (ii) of Theorem 2 in the exceptional cases $p = 2, 3$ follows from the following examples of cycles:

(a) $F(X) = -\frac{2}{3}X(X-1)(X-2)+X+1$ has the cycle 0, 1, 2, 3 of 4 elements in $\mathbb{Z}_2$,

(b) $F(X) = -\frac{1}{4}X^3 + \frac{1}{2}X^2 + \frac{7}{4}X + 1$ has the cycle 0, 1, 3, 4 of 4 elements in $\mathbb{Z}_3$,

(c) $F(X) = -\frac{1}{20}X(X-1)(X-2)(X-3)(X-4)+X+1$ has the cycle 0, 1, 2, 3, 4, 5 of 6 elements in $\mathbb{Z}_3$,

(d) $F(X) = -\frac{9}{8!}X(X-1)(X-2)(X-3)(X-4)(X-5)(X-6)(X-7) + X + 1$ has the cycle 0, 1, 2, 3, 4, 5, 6, 7, 8 of 9 elements in $\mathbb{Z}_3$.

In the remaining cases the assertion (ii) is a consequence of the following lemma:

LEMMA 12. *If R is a complete discrete valuation domain of zero characteristic with prime ideal $P = \pi R$ and finite residue field of $N(P)$ elements, and there exists in R a $(*)$-cycle of length m, then for each $r = 0, 1, \ldots, N(P)-1$ there exists in R a cycle of length $(1+r)m$.*

Proof. Let $M = (1+r)m$ and let $a_0 = 0, a_1, \ldots, a_r$ be elements of R lying in different cosets $\pmod P$. Moreover, let $y_0 = 0$, $y_1, \ldots, y_{m-1}$ be a $(*)$-cycle realized by a polynomial F. For $n = 1, 2, \ldots$ put

$$W_n(X) = (1-(X-a_r)^{N(P)^n(N(P)-1)})F(X-a_r) + \sum_{j=0}^{r-1}((1-(X-a_j)^{N(P)^n(N(P)-1)})(X+a_{j+1}-a_j)).$$

Thus $W_n^{l(1+r)+j}(y_0) \equiv y_l + a_j \pmod{P^{n+1}}$ for $j = 0, 1, \ldots, r$.

Let

$$L_n(X) = \sum_{i=0}^{M-1} a_i^{(n)} X^i$$

be the remainder of the division of $W_n(X)$ by the polynomial

$$X \prod_{j=1}^{M-1} (X - W_n^j(0)).$$

A simple recurrence argument gives $L_n^j(0) = W_n^j(0)$ $(j = 1, 2, \ldots, M)$. Choose now a subsequence $n_1, n_2, \ldots$ so that the limits

$$c_i = \lim_{k\to\infty} a_i^{(n_k)}$$

exist for each $i = 0, 1, \ldots, M$, and put

$$L(X) = \sum_{i=0}^{M-1} c_i X^i.$$

Then

$$L^{l(1+r)+j}(y_0) = \lim_{k\to\infty} L_{n_k}^{l(1+r)+j}(y_0) = \lim_{k\to\infty} W_{n_k}^{l(1+r)+j}(y_0) = y_l + a_j$$

and thus the polynomial L realizes a cycle of M elements. ∎

Note that the assertions of Lemmas 11 and 12 remain true also if R is not complete. Indeed, let S be the completion of R and $x_0, x_1, \ldots, x_{m-1}$ a cycle in S. Choose a sequence $y_0, y_1, \ldots, y_{m-1}$ with $v(y_i - x_i)$ sufficiently small for all i. It follows from the Lagrange interpolation formula that the unique polynomial F of degree not exceeding $m-1$ which satisfies $F(y_i) = y_{i+1}$ for $i = 0, 1, \ldots, m-2$ and $F(y_{m-1}) = y_0$ has its coefficients in R.

11. Proof of Corollary 3. It suffices to observe that every prime congruent to $1 \pmod{M}$ splits in the Mth cyclotomic field and apply Theorem 2. ∎

Reference

[1] W. Narkiewicz, *Polynomial cycles in algebraic number fields*, Colloq. Math. 58 (1989), 151–155.

MATHEMATICAL INSTITUTE
UNIVERSITY OF WROCŁAW
PL. GRUNWALDZKI 2/4
50-384 WROCŁAW, POLAND

Received on 25.9.1992
and in revised form on 9.8.1993 (2307)