Journal de Théorie des Nombres
de Bordeaux **14** (2002), 529–552

Polynomial cycles in certain rings of rationals

par Władysław NARKIEWICZ

To Professor Michel Mendès France on his 65^{th} birthday

Résumé. On montre que la méthode développée dans [HKN3] peut être appliquée pour l'étude des cycles polynomiaux dans certains anneaux, notamment les anneaux $\mathbf{Z}\left[\frac{1}{N}\right]$ pour lesquels nous décrivons les cycles polynomiaux lorsque N est impair ou le double d'un nombre premier.

Abstract. It is shown that the methods established in [HKN3] can be effectively used to study polynomial cycles in certain rings. We shall consider the rings $\mathbf{Z}\left[\frac{1}{N}\right]$ and shall describe polynomial cycles in the case when N is either odd or twice a prime.

0. Let R be an integral domain of zero characteristic. A sequence

$$\xi = (x_0, x_1, \dots, x_n)$$

of elements of R is called a *polynomial sequence* if there exists a polynomial $f \in R[X]$ such that $f(x_i) = x_{i+1}$ holds for $i = 0, 1, \dots, n-1$. A polynomial sequence ξ is called a *polynomial cycle* of length n (or an n-cycle for short) if the elements $x_0, x_1, \dots, x_{n-1}$ are distinct and $x_n = x_0$. It is well-known (see e.g. [HKN1]) that if R is finitely generated then the length of a polynomial cycle in R is bounded by a number depending only on the ring in question but not on the polynomial realizing it. In the case when R is the ring of integers in a $\mathfrak{p}$-adic field or an algebraic number field, such explicit bounds were given by T. Pezda ([Pe]).

Two cycles $\xi = (x_0, x_1, \dots, x_{n-1}, x_0)$ and $\eta = (y_0, y_1, \dots, y_{n-1}, y_0)$ of the same length are called equivalent, if for some $a \in R$ and u in the group $U(R)$ of invertible elements of R (which we shall call *units* of R) one has

$$y_j = a + u x_j \quad (j = 0, 1, \dots, n-1).$$

In such case, if $f \in R[X]$ is a polynomial realizing ξ, then

$$g(X) = u f\left(\frac{X-a}{u}\right) + a$$

Manuscrit reçu le 11 décembre 2000.

has its coefficients in R and realizes η. Obviously every cycle is equivalent to a cycle with $x_0 = 0$. A cycle ξ is called *normalized*, if $x_0 = 0$ and $x_1 = 1$. It is easy to show (see e.g. the proof of Lemma 12.7 (ii) in [N1]) that if $\xi = (x_0, x_1, \dots, x_{n-1}, x_0)$ is an n-cycle and we put $y_j = (x_j - x_0)/(x_1 - x_0)$ then $y_0, y_1, \dots$ all lie in R and $\eta = (y_0, y_1, \dots, y_{n-1}, y_0)$ is a normalized cycle. We shall call η the *normalization* of ξ. Note that if x_1 is not invertible then the cycles ξ and η are not equivalent.

A cycle is called *linear*, if it can be realized by a linear polynomial. It is a trivial task to describe all linear cycles. It has been shown in [HKN3] that in a finitely generated integral domain R of zero characteristic in which every non-zero element lies in only finitely many principal ideals there are only finitely many non-equivalent non-linear polynomial cycles.

The purpose of this note is to show that the arguments presented in [HKN3] can be used to obtain an explicit construction of all polynomial cycles in certain rings. We shall consider finitely generated subrings of the field of rational numbers, containing 1. Clearly every such ring has the form

$$Q^{(N)} = \mathbf{Z}\left[\frac{1}{N}\right],$$

where N is a positive square-free integer. Denote by $C(N)$ the set of lengths of polynomial cycles in $Q^{(N)}$. Our aim is to obtain some information about these sets and to compute them in the case when N is either odd or twice a prime.

The calculations were performed using Borland Pascal for Windows 7.0, PARI 1.38.62 [Ba] and KASH 1.9 [Da].

I am grateful to an anonymous referee, whose suggestions helped to improve the presentation.

1. We recall first certain simple facts about polynomial cycles:

Lemma 1. *Let R be a domain and denote by $U(R)$ its group of units.*

(i) ([N], Lemma 12.8) *If $(x_0, x_1, x_2, \dots, x_{n-1}, x_0)$ ($x_0 = 0, x_1 = 1$) is a normalized cycle in R of length n and we extend x_j by putting $x_j = x_{j-n}$ for $j > n$, then $x_{i+1} - x_i \in U(R)$ holds for $i = 1, 2, \dots$. Moreover for every i and $j \neq 0$ the elements $x_{i+j} - x_i$ and x_j are associated, which means that their ratio is a unit, and if $(j, n) = 1$ then x_j is a unit.*

(ii) ([N], Corollary 2 to Lemma 12.8) *If R contains an ideal I of finite norm $N = \#(R/I) > 1$, then prime divisors of cycle-lengths in R cannot exceed N.*

Corollary 1. *If in a domain R there is a polynomial cycle of odd length $n > 1$, then the equation $x + y = 1$ has a solution with $x, y \in U(R)$.*

Conversely, if units x, y satisfy this equation then $(0,1,x,0)$ is a cycle of length three, realized by the polynomial

$$f(t) = \frac{1-xy}{xy}t^2 + \frac{yx^2-1}{xy}t + 1.$$

Proof. Assertion (i) of the lemma shows that if $(0,1,x_2,\dots)$ is a normalized cycle of odd length n, then x_2 and $1-x_2$ are units. The polynomial f is the Lagrange interpolation polynomial realizing the cycle $(0,1,x,0)$. $\square$

Corollary 2. *If there is a normalized cycle $(0,1,x_2,\dots,x_{n-1},0)$ of length $n \geq 3$ in a ring R and I is an ideal in R of norm $N(I) = m < n$, then some non-zero element of that cycle lies in I.*

Proof. The residue classes $x_i \bmod I$ $(i = 0,1,2,\dots,n-1)$ cannot be all distinct, and if for some $i > j$ we have $x_i - x_j \in I$, then by Lemma 1 (i) the element x_{i-j} lies in I. $\square$

Lemma 2. *Let R be an integral domain.*

(i) ([HKN2], Lemma 5) *If $\alpha, \beta \in R$ then $\{0,1,\alpha,\beta,0)$ is a normalized cycle of length 4 for a polynomial in $R[X]$ if and only if the elements $\beta, 1-\alpha$, $\alpha-\beta$, $\alpha/(1-\beta)$ are units of R. If these conditions are satisfied then the Lagrange interpolation polynomial realizing the cycle equals*

$$1 + (\alpha-1)X + \gamma X(X-1) + \delta X(X-1)(X-\alpha),$$

where

$$\gamma = \frac{1-\beta}{\alpha(1-\alpha)} - 1, \quad \delta = \frac{1}{\beta(\beta-\alpha)} - \frac{\alpha}{(1-\beta)(\alpha-\beta)} + \frac{\gamma}{\alpha-\beta}.$$

(ii) ([NPe], Lemma 4) *If there is a polynomial cycle of length 4 in R then either R contains a root of the polynomial X^2+1 or there exist units u, v, w of R, distinct from 1, satisfying $u+v+w=1$.*

(iii) *Let $p \geq 3$ be a prime and denote by $L(R)$ the Lenstra constant of R. There exists a cycle of length p in R if and only if $p \leq L(R)$. If there is a polynomial cycle of length n in R then all prime divisors of n are bounded by $L(R)$.*

(Recall that $L(R)$ is defined as the maximal number n such that there exist elements $0,1,x_2,\dots,x_{n-1}$ of R whose all non-zero differences are units (see [Len], [LN]*).*

Proof of (iii). The necessity of the stated condition is implied by Lemma 1 (i) and its sufficiency follows from the observation that the Lagrange interpolation polynomial for the cycle $(0,1,x_2,\dots,x_{p-1},0)$ has its coefficients in R. The last part is a consequence of the trivial observation that if polynomial f has a cycle of length n and $d|n$ then the d-th iteration of f has a cycle of length n/d. $\square$

Corollary 1. *Let n be a positive integer and denote by $p(n)$ the minimal prime not dividing n. If there exists a polynomial cycle of length m in $Q^{(n)}$, then the prime factors of m cannot exceed $p(n)$.*

Proof. Follows from part (iii) of the lemma and the observation that the Lenstra constant of $Q^{(n)}$ equals $p(n)$. □

Corollary 2. *Let n be a positive integer. If a, b, c, d are non-zero integers such that all prime factors of the product $abcd$ divide n, $(a, b, c, d) = 1$, the equation*

$$a + b + c + d = 0 \tag{1}$$

is satisfied and moreover the ratio $(b + c)/(d + c)$ is a unit of $Q^{(n)}$ then

$$(0, 1, -\frac{b + c}{d}, -\frac{c}{d}, 0)$$

is a 4-cycle in the ring $Q^{(n)}$.

Conversely, every normalized 4-cycle in $Q^{(n)}$ leads to a solution of (1) satisfying the above conditions.

Proof. The first assertion is a consequence of (i). To prove the converse let $(0, 1, p_1/q, p_2/q, 0)$ $((p_1, p_2, q) = 1)$ be a 4-cycle in $Q^{(n)}$. Then (i) implies that the numbers p_2/q, $1 - p_1/q$, $(p_2 - p_1)/q$ and $p_1/(q - p_2)$ are all units of $Q^{(n)}$. Thus the numbers $a = q - p_1$, $b = p_1 - p_2$, $c = p_2$, $d = -q$ lie in $Q^{(n)}$, satisfy (1), $(b + c)/(d + c) = -p_1/(q - p_2)$ is a unit and $(a, b, c, d) = 1$ holds. □

Corollary 3. *If $Q^{(n)}$ contains two units $\neq -1, -2$ with difference 2, then $4 \in C(n)$.*

Proof. If $\lambda, \lambda + 2$ are units of $Q^{(n)}$ then the assertion results from part (i) of the lemma with $\alpha = 1 + \lambda$, $\beta = 2 + \lambda$. □

We shall utilize also a result of T. Pezda about cycles in p-adic rings:

Lemma 3 ([Pe, Theorem 2 (ii)]). *Let $\mathbf{Z}_p$ be the ring of integers of the p-adic field $\mathbf{Q}_p$ and put*

$$A_p = \{ab : \ 1 \leq a \leq p, \ b|p - 1\}.$$

The set of all lengths of polynomial cycles in $\mathbf{Z}_p$ equals A_p if $p \geq 5$ and $A_p \cup \{p^2\}$ if $p = 2, 3$.

Corollary. *If n has $r \geq 2$ distinct prime factors, then the length of a polynomial cycle in $Q^{(n)}$ is $O(r^2 \log^2 r)$.*

Proof. If p is the smallest prime not dividing n, then $p = O(r \log r)$ and it remains to observe that $Q^{(n)} \subset \mathbf{Z}_p$. □

The next lemma provides a method for constructing all non-equivalent non-linear (i.e.,, not realizable by a linear polynomial) n-cycles in a domain, provided one has a complete list of all normalized n-cycles. It is contained implicitly in the proof of Theorem 2 of [HKN3].

Lemma 4. *Let $\eta = (0, 1, y_2, \ldots, y_{n-1}, 0)$ be a normalized non-linear n-cycle in an integral domain R and let A be the leading term of the Lagrange interpolation polynomial (of degree M, with $2 \le M \le n-1$) realizing η. Let also $(0, x_1, x_2, \ldots, x_{n-1}, 0)$ be an n-cycle, whose normalization equals η. Then for $j = 1, 2, \ldots, n-1$ we have $x_j = y_j x_1$ and x_1^{M-1} divides A.*

Corollary. *If the Lagrange interpolation polynomials of all normalized non-linear n-cycles in a domain R have their leading coefficients invertible, then every non-linear n-cycle in R is equivalent to a normalized cycle.*

We shall also often use the easy fact (see e.g. [HKN2]) that if R is a domain and a polynomial cycle in R is realized by a polynomial with coefficients in R, then the Lagrange interpolation polynomial realizing that cycle has its coefficients in R.

3. Now we describe the sets $C(p)$ for prime p:

Theorem 1. *If p is a prime then*

$$C(p) = \begin{cases} \{1,2,3,4\} & \text{if } p = 2, \\ \{1,2,4\} & \text{if } p = 3, \\ \{1,2\} & \text{if } p \ge 5. \end{cases}$$

Proof. If $p \ge 3$ then $Q^{(p)} \subset \mathbf{Z_2}$ and it follows from Lemma 3 that $C(p) \subset \{1, 2, 4\}$. Since the polynomial $f(X) = -\frac{2}{3}X^3 + \frac{5}{3}X + 1$ has in $Q^{(3)}$ the cycle $(-1, 0, 1, 2, -1)$ it remains to show that in case $p \ge 5$ there are no cycles of length 4. If there would be such a cycle, then by Lemma 2 (ii) the equation $u + v + w = 1$ would have a solution in units u, v, w of $Q^{(p)}$ distinct from 1. Write $u = \epsilon_1 p^a$, $v = \epsilon_2 p^b$ and $w = \epsilon_2 p^c$, with suitable rational integers $a \ge b \ge c$ and $\epsilon_1, \epsilon_2, \epsilon_3 \in \{1, -1\}$. If $a < 0$ then $1 = u + v + w \le 3/5 < 1$, thus $a \ge 0$. This shows that $v + w$ must be a rational integer. The equality $v + w = 0$ would lead to $u = 1$, which is not possible thus $|v + w| \ge 1$, and hence, because of $p > 2$, we get $c \ge 0$. Since $c > 0$ implies $p|1$, we must have $c = 0$ and so finally

$$\epsilon_1 p^a + \epsilon_2 p^b = 2$$

with $b \ge 0$. In view of $p \ne 2$ we get $b = 0$ thus $p = 3$, which is a contradiction.

We are thus left with the case $p = 2$. Since $Q^{(2)} \subset \mathbf{Z_3} \cap \mathbf{Z_5}$, Lemma 3 implies $C(2) \subset \{1, 2, 3, 4, 6\}$.

Lemma 5. (i) *All solutions of the equations $u+v=1$ and $u+v=3$ in units of $Q^{(2)}$ are given by*

$$2+(-1)=\frac{1}{2}+\frac{1}{2}=1$$

and

$$2+1=4+(-1)=3,$$

respectively.

(ii) *There are three normalized cycles of length 3 in $Q^{(2)}$, namely*

$$(0,1,2,0), \quad (0,1,-1,0) \quad \text{and} \quad (0,1,1/2,0).$$

The corresponding Lagrange interpolation polynomials are

$$-\frac{3}{2}t^2+\frac{5}{2}t+1, \quad -\frac{3}{2}t^2-\frac{1}{2}t+1, \quad 3t^2-\frac{7}{2}t+1.$$

(iii) *Every cycle of length 3 in $Q^{(2)}$ is equivalent either to one of the cycles given in (ii) or to one of the cycles*

$$(0,3,6,0),\ (0,3,-3,0)\,(0,3,3/2,0).$$

The corresponding Lagrange interpolation polynomials are

$$-\frac{1}{2}t^2+\frac{5}{2}t+3, \quad -\frac{1}{2}t^2-\frac{1}{2}t+3, \quad t^2-\frac{7}{2}t+3.$$

Proof. Assertion (i) is immediate, (ii) follows from (i) and Corollary 1 to Lemma 1, whereas (iii) results from (ii) and Lemma 4. □

Corollary. *If there is a cycle $(0,1,x_2,\dots,x_5,0)$ of length 6 in $Q^{(2)}$, then there exist $\lambda,\mu\in\{1/2,-1,2\}$ such that $x_4=\lambda x_2$ and $x_5=1+\mu(x_3-1)$. Moreover x_2 is either a unit of $Q^{(2)}$ or is of the form 3ϵ with a unit ϵ and the same applies to x_3-1.*

Proof. The assumption implies that $(0,x_2,x_4,0)$ and $(0,x_3-1,x_5-1,0)$ are 3-cycles, hence it suffices to apply (iii). □

One can also easily list all 4-cycles in $Q^{(2)}$:

Lemma 6. (i) *All solutions of the equation $u+v+w=1$ in units of $Q^{(2)}$ distinct from 1 are given by*

$$1=\frac{1}{4}+\frac{1}{4}+\frac{1}{2}=2+(-\frac{1}{2})+(-\frac{1}{2})=4+(-2)+(-1).$$

(ii) *There are three normalized cycles of length 4 in $Q^{(2)}$, namely*

$$(0,1,\frac{3}{4},\frac{1}{4},0), \quad (0,1,\frac{3}{2},-\frac{1}{2},0), \quad (0,1,3,4,0)$$

and every 4-cycle in $Q^{(2)}$ is equivalent to one of them. The corresponding Lagrange interpolation polynomials are

$$-4t^3+10t^2-\frac{25}{4}t+1, \quad 8t^3-4t^2-\frac{7}{2}t+1, \quad -\frac{1}{4}t^3+\frac{1}{2}t^2+\frac{7}{4}t+1.$$

Proof. Write $u=\pm 2^a$, $v=\pm 2^b$ and $w=\pm 2^c$ with $a\geq b\geq c$. If u,v,w are integers then clearly $c=0$, $w=-1$ so $u+v=2$ and dividing by 2 and applying Lemma 5 (i) we arrive at the solution $u=4, v=-2, w=1$. If however w is not an integer, then $c<0$ hence all terms in $u2^{-c}+v2^{-c}\pm 1=2^{-c}$ are integers and moreover $v2^{-c}$ must equal ± 1. Thus $u2^{-c}+(-2^{-c})=\mp 2$ and dividing by ∓ 2 and using again Lemma 5 (i) we obtain the remaining two solutions. This settles (i).

To obtain (ii) observe first that Equation (1) does not have solutions a,b,c,d in $Q^{(2)}$ with $a+b=c+d=0$ such that $(b+c)/(d+c)$ is a unit of $Q^{(2)}$ and then use (i), Lemma 2 (i), (iii) and the corollary to Lemma 4. $\square$

Now we shall prove that there are no 6-cycles in $Q^{(2)}$. Assume thus that $(0,1,x_2,\ldots,x_5)$ is such a cycle. The corollary to Lemma 5 shows that with suitable units ϵ,η we have $x_2\in\{\epsilon,3\epsilon\}$ and $x_3\in\{1+\eta,1+3\eta\}$. Moreover $x_4=\lambda x_2$ and $x_5=1+\mu(x_3-1)$ with $\lambda,\mu\in\{-1,1/2,2\}$ and from Corollary 2 to Lemma 1 we infer that x_3 is divisible by 5. We have four case to consider:

(A) $x_2=\epsilon$, $x_3=1+\eta$; (B) $x_2=\epsilon$, $x_3=1+3\eta$;

(C) $x_2=3\epsilon$, $x_3=1+\eta$; (D) $x_2=3\epsilon$, $x_3=1+3\eta$.

In cases (A) and (B) the difference x_2-1 is a unit, hence Lemma 5 (i) shows that $x_2\in\{-1,1/2,2\}$ and we get

$$x_4\in\begin{cases}\{-1/2,2\} & \text{if } x_2=-1\\ \{-1/2,-1/4\} & \text{if } x_2=1/2\\ \{-2,4\} & \text{if } x_2=2.\end{cases}$$

Moreover in case (A) $x_3-x_2=1+\eta-\epsilon$ is a unit hence using Lemma 6 (i) we get

$$\eta\in\begin{cases}\{-4,2\} & \text{if } x_2=-1\\ \{-1/4\} & \text{if } x_2=1/2\\ \{1,-4\} & \text{if } x_2=-2\end{cases}$$

and we see that $x_3=1+\eta$ is not divisible by 5, contradiction. Thus case (A) cannot occur. The case (B) is also not possible, since $x_5-1=\mu(x_3-1)$ must be a unit, being associated to $x_4=\epsilon/\lambda$, and so $3\eta=x_3-1$ must be a unit. This contradiction shows that the case (B) is not possible.

The impossibility of case (C) follows from the observation that $x_3-1=\eta$ must be associated to $x_2=3\epsilon$.

It remains thus to deal with case (D). Here $\epsilon_1 = x_2 - 1 = 3\epsilon - 1$ is a unit and the equality

$$\frac{1}{\epsilon} + \frac{\epsilon_1}{\epsilon} = 3$$

leads, in view of Lemma 5 (i) to $\epsilon \in \{-1, 1, 1/4, 1/2\}$, thus

$$x_2 \in \{-3, 3, 3/4, 3/2\}.$$

Moreover $\epsilon_2 = x_3 - x_2$ is also a unit, and in view of $\epsilon_1 + \epsilon_2 = x_3 - 1 = 3\eta$ we get

$$\frac{\epsilon_1}{\eta} + \frac{\epsilon_2}{\eta} = 3$$

thus $\epsilon_1/\eta \in \{-1, 1, 2, 4\}$. Since $x_3 = 1 + 3\eta$ we get thus 16 possibilities for x_3, however only in the following five cases x_3 is divisible by 5:

$$\begin{aligned}
&x_2 = 3, x_3 \in \{-5, 5/2\};\\
&x_2 = -3, x_3 = -5;\\
&x_2 = 3/2, x_3 = 5/2;\\
&x_2 = 3/4, x_3 = 5/8.
\end{aligned}$$

So we are left with the following possible cycles:

$$\begin{aligned}
\alpha_1 &= (0, 1, 3, -5, 3\lambda, 1 - 6\mu, 0),\\
\alpha_2 &= (0, 1, 3, 5/2, 3\lambda, 1 + 3\mu/2, 0),\\
\alpha_3 &= (0, 1, -3, -5, -3\lambda, 1 - 6\mu, 0),\\
\alpha_4 &= (0, 1, 3/2, 5/2, 3\lambda/2, 1 + 3\mu/2, 0),\\
\alpha_5 &= (0, 1, 3/4, 5/8, 3\lambda/4, 1 - 3\mu/8, 0).
\end{aligned}$$

Using the fact that x_5 must be a unit and $\mu \in \{-1, 1/2, 2\}$ we see that in α_1 and α_3 one has $\mu = 1/2$, in a_2 and a_4 one has $\mu \in \{-1, 2\}$ and in α_5 one has $\mu = 2$. Furthermore $x_4 - x_3$ is a unit and thus in α_1 one has $\lambda = -1$, in α_2 one has $\lambda = 1/2$, in α_3, α_4 one has $\lambda \in \{-1, 2\}$, and in α_5 one has

$\lambda = -2$. This leaves us with the following ten cases:

$$\begin{aligned}
\beta_1 &= (0,1,3,-5,-3,-2,0),\\
\beta_2 &= (0,1,3,5/2,3/2,-1/2,0),\\
\beta_3 &= (0,1,3,5/2,3/2,4,0),\\
\beta_4 &= (0,1,-3,-5,3,-2,0),\\
\beta_5 &= (0,1,-3,-5,-6,-2,0),\\
\beta_6 &= (0,1,3/2,5/2,-3/2,-1/2,0),\\
\beta_7 &= (0,1,3/2,5/2,3,-1/2,0),\\
\beta_8 &= (0,1,3/2,5/2,-3/2,4,0),\\
\beta_9 &= (0,1,3/2,5/2,3,4,0),\\
\beta_{10} &= (0,1,3/4,5/8,-3/2,1/4,0).
\end{aligned}$$

Now a short computation shows that the leading coefficients of the corresponding Lagrange interpolation polynomials are equal to $1/40$, $-52/35$, $-4/5$, $-1/160$, $1/35$, $-2/5$, $-2/35$, $3/11$, $-2/5$ and $-417728/5355$ respectively, hence do not lie in $Q^{(2)}$. This establishes our claim. □

4. Now we consider the case of odd composite n.

Theorem 2. *If n is an odd composite number then either $C(n) = \{1,2\}$ or $C(n) = \{1,2,4\}$. The second possibility occurs if and only if Equation (1) has a non-trivial (i.e., without a vanishing subsum of the left-hand side) solution in coprime integers a,b,c,d whose all prime divisors divide n and moreover the ratio $(b+c)/(d+c)$ is a unit of $Q^{(n)}$.*

In particular one has $C(n) = \{1,2,4\}$ in the following cases:

(a) *n is divisible by 3,*

(b) *n is divisible by a product $u(u+2)$, where both u and $u+2$ are primes or prime powers,*

(c) *n is divisible by a product $u(2u \pm 1)$, where both u and $2u \pm 1$ are primes or prime powers.*

Proof. The first assertion is an immediate consequence of $Q^{(n)} \in \mathbf{Z_2}$ and Lemma 1 (iii). To prove the second we use Lemma 2 (iii) and the following simple lemma:

Lemma 7. *If n is odd, then no solution of the equation (1) with a vanishing subsum can lead to a 4-cycle in $Q^{(n)}$.*

Proof. Let a,b,c,d be non-zero integers in $Q^{(n)}$ satisfying $a+b+c+d = 0$ and with $(b+c)/(d+c)$ being a unit of $Q^{(n)}$. Assume also that $c = -a, d = -b$ and $(a,b) = 1$. Since a,b are both odd we may write

$$b - a = 2^r A, \quad b + a = 2^s B$$

with $r, s \geq 1$ and odd A, B. Our assumptions imply that $(b-a)/(b+a)$ is a unit of $Q^{(n)}$ and thus we must have $r = s$. But this implies

$$b = 2^{r-1}(A+B) \equiv 0 \pmod 2,$$

contradiction. □

Note that for even n this lemma fails, as the example $n = 30$ shows. In that case (1) has two trivial solutions, given by $2 + 3 + (-2) + (-3) = 3 + 5 + (-3) + (-5) = 0$ which satisfy the divisibility condition in Theorem 2 and thus lead to 4-cycles $(0, 1, 2/5, -3/5, 0)$ and $(0, 1, -1/3, -2/3, 0)$.

The last assertion of the theorem follows from the simple observation that $m|n$ implies $Q^{(m)} \subset Q^{(n)}$, thus $C(m) \subset C(n)$. In case (a) it is sufficient to recall that $4 \in C(3)$, as shown in Theorem 1. In case (b) our condition for the existence of a cycle of length 4 is satisfied with $a = -u - 2$, $b = d = 1$, $c = u$ and in case (c) that condition is satisfied with $a = -(2u \pm 1)$, $b = d = u$, $c = \pm 1$. □

A direct check shows that at least one of the conditions (a), (b), (c) is satisfied by every square-free composite odd number below 100 except $65 = 5 \cdot 13$, $77 = 7 \cdot 11$, $85 = 5 \cdot 17$ and $95 = 5 \cdot 19$. We shall now show that $C(77) = C(85) = C(95) = \{1, 2\}$ and $C(65) = \{1, 2, 4\}$. For this purpose we shall use the following result, which is an immediate corollary of the main results of [MDT]:

Lemma 8. *If $n \in \{65, 77, 85, 91\}$ then the only solutions, up to permutations, of Equation (1) in integers a, b, c, d composed of prime factors of n are given by $a = b = 13$, $c = -5^2$, $d = -1$ for $n = 65$ and $a = 5^2$, $b = -5$, $c = -1$, $d = -19$ for $n = 95$.*

One checks without difficulty that in case $n = 95$ the divisibility condition of Theorem 2 is violated, whereas in case $n = 65$ we have the cycle $(0, 1, 12/13, 25/13, 0)$ realized by the polynomial

$$\frac{338}{5^2}t^3 - 40t^2 + \frac{8581}{5^2 \cdot 13}t + 1.$$

It follows from known results about exponential diophantine equations that for any given n there are only finitely many non-trivial solutions of (1), i.e., solutions with no proper subsum of the left-hand side vanishing. Hence one can use the existing bounds (see [MDT], [Sk]) for non-trivial solutions of (1) to determine whether there is a 4-cycle in $Q^{(n)}$.

5. Our final example deals with $C(2p)$ with prime p. Here we prove the following result:

Theorem 3. *If $p \geq 3$ is a prime, then $C(2p) = \{1, 2, 3, 4, 5\}$ if $p = 3$, and for $p \geq 5$ one has either $C(2p) = \{1, 2, 3, 4\}$ or $C(2p) = \{1, 2, 3, 4, 6\}$.*

There exists an effective procedure to distinguish between these cases for any given prime p.

Proof. At first we shall assume $p \geq 5$ leaving for a while aside the case $p = 3$. Observe that $Q^{(2\cdot 5)} \subset \mathbf{Z}_3$ and for $p \geq 7$ we have $Q^{(2p)} \subset \mathbf{Z}_3 \cap \mathbf{Z}_5$. Lemma 1 (iii) implies thus $C(10) \subset \{1,2,3,4,6,9\}$ and for $p \geq 7$ we get $C(2p) \subset \{1,2,3,4,6\}$.

The following lemma contains an algorithm leading to a list of all non-equivalent cycles of length six and nine for a large class of domains. It is in certain cases simpler than the algorithm which can be deduced from [HKN3].

Lemma 9. *Let R be a finitely generated integral domain and assume that we have a complete list, say*

$$(0, \alpha_j, \beta_j, 0) \qquad (j = 1, 2, \ldots, N),$$

of pairwise non-equivalent cycles of length 3 in R. Without restriction we may assume, multiplying, if necessary, all elements of a cycle by a unit, that if α_j and α_k are associated then they are equal.

(i) *If*

$$\xi = (0, 1, x_2, x_3, x_4, x_5, 0)$$

is a normalized cycle of length 6 in R, then there exists j and k such that $\alpha_j = \alpha_k$ and

$$x_2 = \epsilon\alpha_j,\ x_3 = 1 + \eta\alpha_k,\ x_4 = \epsilon\beta_j,\ x_5 = 1 + \eta\beta_k,$$

where $\epsilon = 1/u$, $\eta = -1/z$, u is a solution of the unit equation $u + v = \alpha_j$, and z is a solution of the unit equation $z + w = \beta_k$.

(ii) *If*

$$\xi = (0, 1, x_2, x_3, \ldots, x_8, 0)$$

is a normalized cycle of length 9 in R, then there exist a unit e such that $1 - e$ is also a unit, and integers j, k, l such that $\alpha_j = \alpha_k = \alpha_l$ and

$$x_2 = e,\ x_3 = \epsilon_1\alpha_j,\ x_4 = \epsilon_2\alpha_j + 1,\ x_5 = \epsilon_3\alpha_j + e,$$
$$x_6 = \epsilon_1\beta_j,\ x_7 = \epsilon_2\beta_k + 1, x_8 = \epsilon_3\beta_l + e$$

where $\epsilon_1 = 1/u$, u is a solution of the equation $u + v = \alpha_j$, $\epsilon_2 = -1/w$, w is a solution of the equation $w + z = \alpha_j$, s is a solution of the equation $s + t = \beta_l$ and $\epsilon_3 = -e/s$.

Proof. (i) Assume that ξ is a normalized cycle of length 6 in R. Then $(0, x_2, x_4, 0)$ is a cycle of length 3. It is equivalent to one of the cycles in our list, hence with a suitable j and a unit ϵ we have $x_2 = \epsilon\alpha_j$ and $x_4 = \epsilon\beta_j$. Also $(1, x_3, x_5, 1)$ is a cycle of length 3,which is equivalent to the cycle $(0, x_3 - 1, x_5 - 1, 0)$, thus there exists k and a unit η such that

$x_3 = 1+\eta\alpha_k$ and $x_5 = 1+\eta\beta_k$. Lemma 1 (i) implies that $A = x_2-1 = \epsilon\alpha_j-1$ and $x_5 = 1+\eta\beta_k$ are both units, hence

$$\alpha_j = \frac{1}{\epsilon} + \frac{A}{\epsilon}$$

and

$$\beta_k = \frac{1}{\eta} + \frac{B}{\eta}.$$

It remains to establish the equality $\alpha_j = \alpha_k$. Since by Lemma 1 (i) the elements $x_3 - 1$ and x_2 are associated we obtain the equality

$$\eta\alpha_k = u\epsilon\alpha_j$$

with a certain unit u. This shows that α_j and α_k are associated and our assumption implies now $\alpha_j = \alpha_k$.

(ii) Assume that ξ is a normalized cycle of length 9 in R. Then $(0, x_3, x_6, 0)$ is a cycle of length 3, hence with a suitable j and a unit ϵ_1 we have $x_3 = \epsilon_1\alpha_j$ and $x_6 = \epsilon_1\beta_j$. Applying the same procedure to the 3-cycles $(1, x_4, x_7, 1)$ and (x_2, x_5, x_8, x_2) we obtain the existence of integers k, l and units ϵ_2, e_3 such that

$$x_4 = 1+\epsilon_2\alpha_k,\ x_7 = 1+\epsilon_2\beta_k,\ x_5 = \epsilon_3\alpha_l + x_2,\ x_8 = \epsilon_3\beta_l + x_2.$$

Lemma 1 (i) implies that x_2 and $1 - x_2$ are both units. Since x_8 is a unit, we get

$$\beta_l = \frac{x_8}{\epsilon_3} + \frac{-x_2}{\epsilon_3}$$

with both summands being units and since x_4 is also a unit we get

$$\alpha_k = \frac{x_4}{\epsilon_2} + \frac{-1}{\epsilon_2}$$

with unit summands. Finally $\epsilon_1\alpha_j = x_3 - 1 = \eta x_2$ with a unit η and hence

$$\alpha_j = \frac{1}{\epsilon_1} + \frac{\eta x_2}{\epsilon_1},$$

again with unit summands. To obtain the equality $\alpha_j = \alpha_k = \alpha_l$ it suffices to observe that Lemma 1(i) implies that the elements x_3, $x_4 - 1$ and $x_5 - x_2$ are associated and thus α_j, α_k and α_l are also associated. $\square$

The last assertion of the theorem follows immediately from the first part of the lemma and the observation that a complete family of non-equivalent 3-cycles in $Q^{(n)}$ can be determined using Corollary 1 to Lemma 1, Lemma 4 and an effective procedure of solving the equation $u + v = 1$ in units of any finitely generated number ring (see [Sch]).

Our argument for the non-existence of 9-cycles in $Q^{(2p)}$ did not cover the case $p = 5$, so we have now to address this case.

To obtain this we shall use the second part of the preceding lemma and to do that we have to find first a complete system of non-equivalent 3-cycles. This is done in a slightly greater generality in the following lemma:

Lemma 10. *Let p be an odd prime and $(0,1,\alpha,0)$ a normalized 3-cycle in $Q^{(2p)}$.*

(a) *If $p>3$ is a Fermat prime then*

$$\alpha \in \{-1, \frac{1}{2}, 2, p, 1-p, \frac{p-1}{p}, \frac{1}{p}, \frac{p}{p-1}, -\frac{1}{p-1}\}.$$

(b) *If p is a Mersenne prime then*

$$\alpha \in \{-1, \frac{1}{2}, 2, -p, p+1, \frac{p+1}{p}, p, -\frac{1}{p}, \frac{p}{p+1}, \frac{1}{p+1}\}.$$

(c) *If $p=3$ then*

$$\alpha \in \{-8,-3,-2,-1,-\frac{1}{2},-\frac{1}{3},-\frac{1}{8},\frac{1}{9},\frac{1}{3},\frac{1}{4},\frac{1}{2},\frac{2}{3},\frac{3}{4},\frac{8}{9},\frac{9}{8},\frac{4}{3},\frac{3}{2},2,3,4,9\}.$$

(d) *In all other cases $\alpha \in \{-1, \frac{1}{2}, 2\}$.*

In case (d) the Lagrange polynomials realizing normalized cycles of length 3 are those given in Lemma 5 (ii).

Proof. Lemma 2(i) shows that we have to determine all solutions of the equation $u+v=1$ in units of $Q^{(2p)}$. Multiplying this equation be the common denominator of u and v we get an equation of the form

$$\pm p^x \pm 2^y = 2^w p^z,$$

and one sees easily that apart from the trivial case $1+1=2$ this equation is reducible to

$$p^x - 2^y = \pm 1. \tag{7}$$

It is well-known (see e.g. [Si], [Wa]) that this is possible only if either $p = 2^y+1 > 3$ is a Fermat prime, or $p = 2^y-1$ is a Mersenne prime, or finally $p=3$ and the solutions are $3^2-2^3=1, 2^2-1=3, 3-2=1$. Now note that each solution of (7) leads to the following companion solutions of the unit equation $u+v=1$:

$$\frac{\pm 1}{p^x} + \frac{2^y}{p^x} = 1, \quad \frac{p^x}{2^y} + \frac{\mp 1}{2^y} = 1,$$

It remains to write down all units appearing in these equations. In particular in case (d) the only solutions of the unit equation are $1/2+1/2=1$ and $2+(-1)=1$, leading to $a=-1, 1/2$ and 2. □

Corollary 1. *If $p>3$ is neither a Fermat prime nor a Mersenne prime, then in $Q^{(2p)}$ we have the following non-equivalent cycles of length 3:*

$$(0,1,2,0),\ (0,1,-1,0),\ (0,1,\frac{1}{2},0), (0,3,6,0),\ (0,3,-3,0),\ (0,3,\frac{3}{2},0). \tag{8}$$

Proof. It follows from the lemma that the first three listed cycles form a complete set of normalized 3-cycles in $Q^{(2p)}$. Lemma 5 (ii) implies that the leading terms of the Lagrange interpolation polynomials are $3/2, 3/2$ and 3, respectively, hence they have, up to a unit factor, only 1 and 3 for divisors in $Q^{(2p)}$. The assertion follows now from Lemma 4. $\square$

The same approach leads to the following two assertions:

Corollary 2. *If $p = 2^{2^s}+1 > 3$ is a Fermat prime, then the list of all non-equivalent cycles of length 3 in $Q^{(2p)}$ consists of $(0,3,3\alpha,0)$ $(\alpha = -1, 1/2, 2)$ and all cycles of the form $(0,d,\alpha d,0)$ where α is a number listed in Lemma 10 (i) except $\alpha = -1, 1/2, 2$ and d is a divisor of p^2-p+1.*

Corollary 3. *If $p = 2^q-1$ is a Mersenne prime, then the list of all non-equivalent cycles of length 3 in $Q^{(2p)}$ consists of $(0,3,3\alpha,0)$ $(\alpha = -1, 1/2, 2)$ and all cycles of the form $(0,d,\alpha d,0)$ where α is a number listed in Lemma 10 (ii) except $\alpha = -1, 1/2, 2$ and d is a divisor of p^2+p+1.*

Now we can dispose of 9-cycles in $Q^{(10)}$. Corollary 2 to the last lemma shows that the set

$$\Big\{(0,d,\alpha d,0):\ d\in\{1,3,7,21\},\ \alpha\in\{-4,-\frac{1}{4},\frac{1}{5},\frac{4}{5},\frac{5}{4},5\}\Big\} \cup \Big\{(0,3,3\alpha):\ \alpha\in\{-1,\frac{1}{2},2\}\Big\} \tag{9}$$

forms a complete system of non-equivalent 3-cycles in $Q^{(10)}$.
Let $(0,1,x_2,\ldots,x_8,0)$ be a normalized cycle of length 9 in $Q^{(10)}$ and let $\alpha_j, u, v, \epsilon_1$ be defined as in Lemma 9 (ii), thus $\alpha_j \in \{1,3,7,21\}$.

Lemma 11. *One has $\alpha_j = 21$.*

Proof. Since x_2, x_4, x_5, x_7 and x_8 are units, hence by Corollary 2 to Lemma 1 we have $3\cdot 7 | x_3x_6$. Now $(0,x_3,x_6,0)$ is a 3-cycle which is equivalent to some cycle listed in (9). Thus with some unit ϵ and d,α listed in (9) we have $x_3 = \epsilon d$, $x_6 = \alpha\epsilon d$ and as α is a unit we must have $3\cdot 7 | d = \alpha_j$. $\square$

Lemma 12. *The equation*

$$x \pm y = 21z \tag{10}$$

has exactly three solutions in coprime positive integers x,y,z such that the product xyz has only 2 and 5 for its prime divisors. They are given by

$$2^4+5^1 = 5^2-2^2 = 2^2\cdot 5^1+1 = 21.$$

Proof. In view of $(x,y,z)=1$ at most one of the numbers x,y,z can be divisible by 2 resp. 5, thus at least one of them must equal 1. By symmetry we may assume $x > y$. Assume first $z = 1$. Then we have to solve the following four exponential equations:

$$2^X + 5^Y = 21, \quad 2^X 5^Y \pm 1 = 21, \quad 5^X - 2^Y = 21, \quad 2^X - 5^Y = 21.$$

The first has $X = 4, Y = 1$ for its only solution, leading to $2^4 + 5^1 = 21$ and the second has the solution $2^2 \cdot 5^1 + 1 = 21$. To solve the remaining two equations one uses Theorem 3 of [MDT] which shows that the summands in the left-hand sides of these equations do not exceed 29^4, so it suffices to perform a simple computer check. It shows that the obvious solution $5^2 - 2^2 = 21$ is the only one.

In the remaining case ($y = 1, z > 1$) we have to consider the following four equations:

$$2^X + 1 = 21 \cdot 5^Y, \quad 2^X - 1 = 21 \cdot 5^Y, \quad 5^X + 1 = 21 \cdot 2^Y, \quad 5^X - 1 = 21 \cdot 2^Y.$$

However it follows from the table given in [Le] that none of these equations has a solution. □

Corollary. *Numbers $u, v \in Q^{(10)}$ which are solutions of the unit equation $u + v = 21$ form the following set of six elements:*

$$\{-4, 1, 5, 16, 20, 25\}.$$

Proof. This follows from the observation that in every solution of (10) one has $z = 1$. □

Now we apply Lemma 9 (ii) which permits, with the use of the last two corollaries to establish a list of all 9-tuples of elements of $Q^{(10)}$ which may form normalized 9-cycles and a computer check shows that for all of them the necessary condition given in Lemma 1 (i) is violated. Since the polynomial

$$\frac{1}{20}(-t^5 + 10t^4 - 35t^3 + 50t^2 - 4t + 20)$$

realizes the 6-cycle $(0, 1, 2, 3, 4, 5, 0)$ in $Q^{(10)}$ one gets $C(10) = \{1, 2, 3, 4, 6\}$. □

6. It remains to consider the ring $Q^{(6)}$. Since it is contained in $\mathbf{Z}_5$ and $\mathbf{Z}_7$ hence it follows from Lemma 3 that the lengths of polynomial cycles in $Q^{(6)}$ lie in the set $\{1, 2, 3, 4, 5, 6, 8, 10, 12\}$. Because of $Q^{(2)} \subset Q^{(6)}$ Theorem 1 implies the existence of cycles of lengths 1,2,3 and 4. The existence of cycles of length 5 follows from the observation that the polynomial

$$f(x) = -\frac{5}{24}x^4 + \frac{5}{4}x^3 - \frac{55}{24}x^2 + \frac{9}{4}x + 1,$$

has the cycle $(0, 1, 2, 3, 4, 0)$.

We shall need certain simple results about unit equations.

Lemma 13. (i) *All solutions of* $x \pm y = 7z$ *in positive integers* x, y, z *having no prime divisor exceeding* 3 *and satisfying* $(x, y, z) = 1$ *are given by*

$$2 \cdot 3 + 1 = 2^3 - 1 = 2^2 + 3 = 3^2 - 2 = 2^4 - 3^2 = 7$$
$$2^6 - 1 = 7 \cdot 3^2, \quad 3^3 + 1 = 7 \cdot 2^2.$$

(ii) *All solutions of* $x \pm y = 13z$ *in positive integers* x, y, z *having no prime divisor exceeding* 3 *and satisfying* $(x, y, z) = 1$ *are given by*

$$2^4 - 3 = 2^8 - 3^5 = 2^2 + 3^2 = 13.$$

(iii) *All solutions of* $x \pm y = 73z$ *in positive integers* x, y, z *having no prime divisor exceeding* 3 *and satisfying* $(x, y, z) = 1$ *are given by*

$$3^4 - 2^3 = 2^6 + 3^2 = 2^3 \cdot 3^2 + 1 = 73.$$

Proof. We use standard methods. Our assumptions imply that in our equations $x \pm y = az$ $(a = 7, 13, 73)$ one of the numbers x, y, z must be equal to 1. Consider first the case $a \in \{7, 13\}$. If $z > 1$, thus $y = 1$ and a glimpse at the tables provided in [Le] shows that the only solutions are $2^6 - 1 = 7 \cdot 3^2$, $3^3 + 1 = 7 \cdot 2^2$ and $2^2 \cdot 3 + 1 = 13$. If $z = 1$ then we have to solve the exponential equations $|2^X + 3^Y| = 7$, $|2^X + 3^Y| = 13$, $|2^X - 3^Y| = 7$ and $|2^X - 3^Y| = 13$. The first two are trivial and the solution of the remaining two is accomplished with the use of the main result of [MDT] which implies that $\max\{2^X, 3^Y\} \le 29^4$, hence a short computer calculation suffices to complete the list of solutions in cases (i) and (ii).

If $a = 73$ then the case $z = 1$ is resolved in the same way as above, using the bound given in [MDT]. If $y = 1$ then we apply the standard procedure, going back to Störmer ([St]), of reducing exponential equations to Pell's equations. We have to solve the equations

$$|2^X - 73 \cdot 3^Y| = 1, \quad \text{and} \quad |3^X - 73 \cdot 2^Y| = 1. \tag{12}$$

Consider the first of them. If X, Y are both even, then putting $u = 2^{X/2}$ and $v = 3^{Y/2}$ we get

$$u^2 - 73v^2 = \pm 1 \tag{13}$$

Since the fundamental unit of the field $Q(\sqrt{73})$ equals $1068 - 125\sqrt{73}$ hence in every solution u, v of (13) the number v is divisible by 5, so $5|3$, contradiction.

If X is odd and Y is even then write $u = 2^{(X-1)/2}$ and $v = 3^{Y/2}$, thus $2u^2 - 73v^2 = \pm 1$ and $(2u)^2 - 146v^2 = \pm 2$. Since the fundamental unit of the field $Q(\sqrt{146})$ equals $\epsilon = 145 + 12\sqrt{146}$ and the only prime ideal of norm 2 of that field is principal and generated by $\xi = 12 - \sqrt{146}$ we get $2u + v\sqrt{146} = \pm\xi(145 \pm 12\sqrt{146})^N$ with $N = 0, 1, 2, \ldots$. For $N = 0$ we get $u = 6$, $v = 1$ which provides us with the solution $2^3 \cdot 3^2 + 1 = 73$ and one sees easily that for positive N we get $12|v$, thus v cannot be a power of 3.

If X is even and Y is odd, a similar procedure leads us to the equation $u^2 - 3 \cdot 73v^2 = \pm 1$ with v being a power of 3. However this is not possible as the fundamental unit of the field $Q(\sqrt{219})$ equals $74 + 5\sqrt{219}$ and this forces v to be divisible by 5.

Finally let both X and Y be odd. Then we are led to the equation $2u^2 - 3 \cdot 73v^2 = \pm 1$, thus $(2u)^2 - 438v^2 = \pm 2$, hence $2u + v\sqrt{438}$ is an integer of norm 2 or -2 in the field $Q(\sqrt{438})$. This is however not possible as the only ideal of norm 2 in this field is non-principal.

It remains to consider the second of the equations (14). If X, Y are both even then it reduces to Equation (15) with v being a power of 2 but we have seen already that any solution of (15) satisfies $5|v$. If X is odd and Y is even then we are led to $3u^2 - 73v^2 = \pm 1$, hence $(3u)^2 - 219u^2 = \pm 3$ but the only ideal of norm 3 in the field $Q(\sqrt{219})$ is non-principal, making the last equality impossible. If X is even and Y is even then we get $u^2 - 146v^2 = \pm 1$ with $v = 2^{(Y-1)/2}$. But the fundamental unit of $Q(\sqrt{146})$ equals $\epsilon = 145 + 12\sqrt{146}$, hence $3|v$, contradiction. Finally let both X and Y be odd. Then we get $3u^2 - 2 \cdot 73v^2 = \pm 1$ and $(3u)^2 - 438v^2 = \pm 3$. Since the fundamental unit of $Q(\sqrt{438})$ equals $293 + 14\sqrt{438}$ and the only ideal of norm 3 is generated by $\xi = 21 + \sqrt{438}$ we must have

$$3u + v\sqrt{438} = \pm\xi(293 \pm 14\sqrt{438})^N \qquad (N = 0, 1, 2, \dots).$$

Denote by P the unique prime ideal in the field $Q(\sqrt{438})$ dividing 73. Then $\sqrt{438} \equiv 0 \pmod{P}$ and $293 \equiv 1 \pmod{P}$ thus $3u \equiv \pm 21 \pmod{P}$, $3u \equiv \pm 21 \pmod{73}$ and $u \equiv \pm 7 \pmod{73}$. This is however not possible, as no power of 3 is congruent to $\pm 7 \bmod 73$. This concludes the proof of the lemma. □

Corollary. (i) *Numbers $u, v \in Q^{(6)}$ which are solutions of the unit equation $u + v = 7$ form the following set of* 14 *elements:*

$$\{-9, -2, -1, -\frac{1}{9}, \frac{1}{4}, 1, 3, 4, 6, \frac{27}{4}, \frac{64}{9}, 8, 9, 16\}.$$

(ii) *Numbers $u, v \in Q^{(6)}$ which are solutions of the unit equation $u + v =$* 13 *form the following set of six elements:*

$$\{-243, -3, 4, 9, 16, 256\}.$$

(iii) *Numbers $u, v \in Q^{(6)}$ which are solutions of the unit equation $u + v =$* 73 *form the following set of six elements:*

$$\{-8, 1, 9, 64, 72, 81\}.$$

Proof. Follows from the observation that $u = x/z$, $v = y/z$, where x, y, z are given in the corresponding part of the lemma. □

Lemma 14. *There are no cycles of length* 6 *or* 12 *in $Q^{(6)}$.*

Proof. Lemma 10 provides us with a list of all normalized cycles of length three and to deduce the list of all non-equivalent such cycles with the use of Lemma 4 we have to find the leading coefficients of polynomials realizing the normalized cycles. A simple application of Corollary 1 to Lemma shows that these coefficients form the set $\{1, 7, 13, 73\}$. This implies that a complete set of non-equivalent 3-cycles in $Q^{(6)}$ is given by

$$\{(0, d, \alpha d, 0) : \ d \in \{1, 7, 13, 73\}, \alpha \in \mathbf{A}\}, \tag{14}$$

where by $\mathbf{A}$ we denote the set of numbers listed in Lemma 10(c).

It suffices now to perform the algorithm given in Lemma 9 (i), all preliminary information being contained in the corollaries to the preceding lemma. This has been made by a Pascal program, which checked the 257 985 candidates for a 6-cycle and found that only six of them satisfy the necessary conditions given in Lemma 1 (i). However it turned out that their Lagrange interpolation polynomials do not have all coefficients in the ring $Q^{(6)}$, in fact, in each case at least one coefficient has its denominator divisible by seven. The non-existence of 6-cycles obviously implies the non-existence of cycles of length 12. □

We need to have a list of all solutions of the equation $a + b + c + d = 0$ in integers a, b, c, d whose prime divisors lie in $\{2, 3\}$ under the conditions

$$(a, b, c, d) = 1, \quad a + b \neq 0, \quad a + c \neq 0, \quad a + d \neq 0.$$

Since at most two of the numbers a, b, c, d can be divisible by 2 resp. 3 one sees easily that this task consists in finding all solutions in nonnegative integers of the eleven following equations:

$$2^x + 2^y = 3^z + 3^w, \tag{15}$$

$$2^x + 3^y = 2^z + 3^w, \tag{16}$$

$$2^x = 2^y + 3^z + 3^w, \tag{17}$$

$$3^x = 2^y + 2^z + 3^w, \tag{18}$$

$$2^x 3^y = 2^z 3^w + 1 + 1, \tag{19}$$

$$2^x 3^y + 2^z = 1 + 3^w, \tag{20}$$

$$2^x 3^y + 3^z = 2^w + 1, \tag{21}$$

$$2^x 3^y + 2^z + 1 = 3^w, \tag{22}$$

$$2^x 3^y + 3^z + 1 = 2^w, \tag{23}$$

$$2^x 3^y = 2^z + 3^w + 1, \tag{24}$$

$$2^x 3^y + 1 = 2^z + 3^w, \tag{25}$$

under the condition that no cancellation occurs. We shall call non-trivial every solution satisfying this condition.

Fortunately all solutions of these equations are known:

Lemma 15. (i) ([Pi]) *All non-trivial solutions of Equation (15) in non-negative integers are given by*

$$2+8=1+9, 4+8=3+9, 4+32=9+37.$$

(ii) ([Pi]) *All non-trivial solutions of Equation (16) in nonnegative integers are given by*

$$2+3=4+1, 2+9=8+3, 8+9=16+1,$$
$$8+27=32+3, 16+243=256+3.$$

(iii) ([Pi], [Wg], Theorem 2) *All non-trivial solutions of Equation (17) in nonnegative integers are given by*

$$4=2+1+1, 8=2+3+3, 8=4+1+3, 16=4+3+9,$$
$$32=2+3+27, 32=4+1+27, 256=4+9+243.$$

(iv) ([Pi], [Wg], Theorem 1) *All non-trivial solutions of Equation (18) in nonnegative integers are given by*

$$3=1+1+1, 9=1+4+4, 9=3+2+4, 27=3+8+16,$$
$$27=9+2+16, 81=1+16+64, 81=9+8+64.$$

(v) (Known essentially since medieval times, see e.g. [A1], Lemma 2.1)). *Equation (19) has*

$$4=2+1+1, 6=4+1+1, 8=6+1+1, 18=6+1+1$$

for its only solutions.

(vi) ([AF1], Lemma 3.2; [TW], Theorem 2) *All non-trivial solutions of Equation (20) in nonnegative integers are given by*

$$2+2=3+1, 2+8=9+1, 6+1=4+3, 18+64=81+1,$$
$$12+16=27+1, 8+2=9+1, 24+4=27+1.$$

(vii) ([A2], Lemma 2.3; [TW], Theorem 3) *All non-trivial solutions of Equation (21) in nonnegative integers are given by*

$$2+3=4+1, 6+3=8+1, 6+27=32+1, 486+27=512+1,$$
$$8+9=16+1, 24+9=32+1, 48+81=128+1, 432+81=512+1.$$

(viii) ([AF2],Theorem 1.A.1; [Wg], Theorem 3) *All non-trivial solutions of Equation (22) in nonnegative integers are given by*

$$1+1+1=3, 6+2+1=9, 18+8+1=27, 4+4+1=9,$$
$$24+2+1=27, 72+8+1=81, 216+512+1=729, 16+64+1=81,$$
$$48+32+1=81, 64+16+1=81.$$

(ix) ([AF2], Theorem 2.A.2; [Wg], Theorem 4) *All non-trivial solutions of Equation (23) in nonnegative integers are given by*

$$2+1+1=4, 4+3+1=8, 4+27+1=32, 6+1+1=8,$$
$$12+3+1=16, 12+243+1=256, 36+27+1=64,$$
$$1+9+6=16, 54+9+1=64.$$

(x) ([AF2], Theorem 2.A.3; [Wg], Theorem 5) *All non-trivial solutions of Equation (24) in nonnegative integers are given by*

$$3=1+1+1, 6=2+3+1, 6=4+1+1, 18=8+9+1,$$
$$18=16+1+1, 4=2+1+1, 12=2+9+1,$$
$$12=8+3+1, 36=8+27+1,$$
$$36=32+3+1, 8=4+3+1, 32=4+27+1.$$

(xi) ([TW], Theorem 1; [Sk], Theorem 3) *All non-trivial solutions of Equation (25) in nonnegative integers are given by*

$$6+1=4+3, 18+1=16+3, 4+1=2+3, 12+1=9+4,$$
$$24+1=16+9, 72+1=64+9, 16+1=9+8,$$
$$144+1=64+81, 96+1=16+81.$$

To obtain all possible normalized 4-cycles in $Q^{(6)}$ a computer test was made to check which solutions of the equation (1) implied by the preceding lemma satisfy the condition stated in Lemma 2 (iii). Finally the computer used Lemma 4 to obtain a complete set of pairwise non-equivalent 4-cycles. It turned out unexpectedly that all non-zero elements of normalized 4-cycles are units of $Q^{(6)}$. The calculations are summarized in the following lemma:

Lemma 16. (i) *There are* 114 *distinct normalized* 4*-cycles cycles in* $Q^{(6)}$. *All non-zero terms of these cycles are units of* $Q^{(6)}$, *the corresponding Lagrange polynomials are all of degree* 3 *and the ideals of* $Q^{(6)}$ *generated by the leading coefficients of these polynomials have the form* $aQ^{(6)}$ *with*

$$a \in \{1,5,11,13,17,19,23,25,29,31,43,53,59,107,109,115,149, 155,185,523,3187\}. \tag{26}$$

(ii) *There are* 8 *distinct non-normalized* 4*-cycles in* $Q^{(6)}$ *containing* 0.

Lemma 17. *There are no cycles of length* 8 *in* $Q^{(6)}$.

Proof. Assume that $(0,1,x_2,x_3,\ldots,x_7,0)$ is a cycle of length 8. According to Corollary 2 to Lemma 1 for some i x_i is divisible by 7. We shall now show that this implies $7|x_4$. Observe first that the sequence $(0,1,x_4/x_2,x_6/x_2,0)$ forms a normalized 4-cycle, thus by Lemma 2 (i) $\epsilon = x_6/x_2$ must be a unit and by Lemma 1 (i) the same applies to $\eta = x_4/(x_6-x_2)$. If thus x_2 is divisible by 7 then 7 divides $x_6 = \epsilon x_2$ and hence also $x_4 = \eta(x_6-x_2)$. If however x_2 is not divisible by 7 then 7 does not divide x_6 and hence it must divide x_4. Now note that $(0, x_2, x_4, x_6, 0)$ is also a 4-cycle and hence by Lemmas 4 and 16 we must have $x_4 = \xi u$, where ξ is a unit and u^2 divides the leading term of the Lagrange polynomial corresponding to one of the cycles determined in Lemma 16. That lemma shows that this can happen only if u is either a unit or is associated with 5, since 5^2 is the only non-squarefree number listed in (26). Thus x_4 cannot be divisible by 7, contradiction. □

It remains to exclude the possibility of a cycle of length 10 in $Q^{(6)}$.

Lemma 18. (i) *There are* 240 *normalized* 5*-cycles in* $Q^{(6)}$. *In five cases the corresponding Lagrange interpolation polynomials are cubic, in the remaining cases they are quartic.*

(ii) *Every non-normalized* 5*-cycle containing zero in* $Q^{(6)}$ *differs by a unit factor from one of the normalized* 5*-cycles.*

Proof. The first part is pure computing, based on Lemma 2 (ii). To prove the second one has to observe that the principal ideals in $Q^{(6)}$ generated by the leading terms of the quartic polynomials realizing 5-cycles do not have any non-trivial fourth power divisors, and the leading terms of cubic polynomials realizing 5-cycles are all units of $Q^{(6)}$. Thus (ii) follows from Lemma 4. □

It has been shown in [Mo] that no quadratic polynomial with rational coefficients can have a cycle of length four in the rational field and one could naively conjecture that a rational polynomial of degree N cannot have a cycle of length $N+2$ in the field of rationals. The five polynomials in the last lemma refute this hope. In particular the polynomial $3X^3 - \frac{9}{2}X^2 + \frac{1}{6}X + 1$ has the 5-cycle $(0, 1, -1/3, 1/3, 2/3, 0)$.

Corollary. *There are no cycles of length* 10 *in* $Q^{(6)}$.

Proof. Assume that $\xi = (0, x_1, x_2, x_3, \ldots, x_9, 0)$ is a 10-cycle in $Q^{(6)}$. Multiplying all elements of it by a suitable power of 2 and 3 we may assume that all x_i are integers. As $(0, x_2, x_4, x_6, x_8, 0)$ is a 5-cycle in $Q^{(6)}$, part (ii) of the lemma shows that it is equivalent to a normalized cycle, hence Lemma 2 (ii) implies that x_2, x_4, x_6, x_8 are all units of $Q^{(6)}$. By Corollary 2 to Lemma 1 some non-zero elements of ξ must be divisible by 5 and as x_3, x_7, x_9 are units, we get $5|x_5$ and similarly $7|x_5$, so finally $35|x_5$, so $x_5 = 35N$ with some integer N. Now observe that $(x_5, x_7, x_9, 1, x_3, x_5)$ is a 5-cycle, thus

$$\eta = (0, x_7 - x_5, x_9 - x_5, x_1 - x_5, x_3 - x_5, 0)$$

is a 5-cycle containing 0. Since all non-zero elements of a 5-cycle are units, the same applies to non-zero elements of η. Hence

$$35N = x_5 = x_i + \epsilon_i \quad (i = 1, 3, 7, 9) \tag{27}$$

holds with suitable units ϵ_i. Note that ϵ_i are integers.

Lemma 19. (i) *If a number in* $Q^{(6)}$ *has at least two distinct representations as a sum of two units then the principal ideal that it generates has the form* $NQ^{(6)}$ *with*

$$N \in \{5,7,11,13,17,19,23,25,31,35,37,41,43,47,49,55,61,\\ 65,73,85,97,217,431,485\}. \tag{28}$$

(ii) *The number* 35 *has three distinct representations as a sum of two units of* $Q^{(6)}$, *namely*

$$35 = 2^3 + 3^3 = 2^5 + 3^1 = 2^2 3^2 - 1.$$

Proof. (i) Let $0 < \alpha \in Q^{(6)}$ and assume that with suitable $\epsilon_i, \eta_i \in \{1,-1\}$ and integral x,y,z,w,s,t,r,q one has

$$\alpha = \epsilon_1 2^x 3^y + \eta_1 2^z 3^w = \epsilon_2 2^s 3^t + \eta_2 2^r 3^q.$$

Multiplying both sides by suitable powers of 2 and 3 we may assume that all exponents on the right-hand side are non-negative, the left-hand side α_1 is an integer, generating in $Q^{(6)}$ the same ideal as α and $\min\{x,z,s,r\} = 0$. Subtracting we get an equation of the form $a+b+c+d=0$ with integral $a,b,c,d \in Q^{(6)}$ satisfying $(a,b,c,d)=1$. This is an equation having one of the form considered in Lemma 15 hence that lemma provides us with a list of all solutions and now it is a trivial computer task to list all ideals which can be generated by α_1, hence also by α.

(ii) A simple computer calculation on basis of the list of solutions given in Lemma 15 shows that there are no other representations of 35 as a sum of two integers invertible in $Q^{(6)}$. It remains to show that there is no such a representation with non-integral summands. If there is such representation then it must have the form $35 = \pm a + \pm b$ with either $a = 2^x/3^k$, $b = 3^y/2^l$ or $a = 2^x/3^k$, $b = 1/2^l 3^m$ or finally $a = 3^x/2^k$, $b = 1/2^l 3^m$ (with x,y,k,l,m being non-negative integers). In the first case we get

$$35 \cdot 3^k 2^l = \pm 2^{x+l} \pm 3^{k+l}$$

which is possible only if $k = l = 0$. In the second case, if $k \le m$ then we get $35 \cdot 3^m = \pm 2^x 3^{m-k} \pm 1$ and if $k > m$ then $35 \cdot 3^k = \pm 2^x \pm 3^{k-m}$. This forces in both cases $k = m$ and thus $35 \cdot 3^k = \pm 2^x \pm 1$, but it follows from [Le] that this equation has no solutions. The third case can be handled similarly. □

Corollary. *If* $\alpha \in Q^{(6)}$ *is divisible by* 35 *and has at least two representations as a sum of two units then* $\alpha = 2^k 3^l \cdot 35$ *with integral* k,l.

Proof. It suffices to observe that 35 is the only element of the list (28) divisible by 35. □

If the representations given in (27) of $35N$ as a sum of two integers invertible in $Q^{(6)}$ all coincide, then, in view of $x_i \neq x_1$ $(i = 3, 7, 9)$, we must have $\epsilon_3 = \epsilon_7 = x_1$ thus $\epsilon_1 = x_3 = x_7$, which is clearly impossible. Hence there must be at least two distinct such representations and the corollary to Lemma 19 shows that N is a unit and using the equalities (27) and Lemma 19 (ii) we see that for $i = 1, 3, 5, 7$ one has $x_i \in \{-N, 3N, 8N, 27N, 32N, 36N\}$. However by Lemma 1(i) the differences $x_i - x_1$ are units for $i = 3, 5, 7$ but a direct calculation shows that this is not possible. This shows that there cannot be a polynomial cycle of length 10 in $Q^{(6)}$. □

References

[A1] L. J. Alex, *Diophantine equations related to finite groups.* Comm. Algebra **4** (1976), 77–100.

[A2] L. J. Alex, *On the diophantine equation* $1 + 2^a = 3^b5^c + 2^d3^e5^f$. Math. Comp. **44** (1985), 267–278.

[AF1] L. J. Alex, L. L. Foster, *On the diophantine equation* $1 + p^a = 2^b + 2^cp^d$. Rocky Mount. J. Math. **15** (1985), 739–761.

[AF2] L. J. Alex, L. L. Foster, *On the diophantine equation* $1 + x + y = z$. Rocky Mount. J. Math. **22** (1992), 11–62.

[Ba] C. Batut, D. Bernardi, H. Cohen, M. Olivier, *User's Guide to PARI-GP*, Bordeaux 1994.

[Ca] J. W. S. Cassels, *On the equation* $a^x - b^y = 1$. Amer. J. Math. **75** (1953), 159–162.

[Co] J. H. E. Cohn, *The Diophantine equation* $x^2 + 3 = y^n$. Glasgow Math. J. **35** (1993), 203–206.

[Da] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, M. Schörnig, K. Wildanger, *KANT V4*. J. Symbolic Comput. **24** (1997), 267–283.

[HKN1] F. Halter-Koch, W. Narkiewicz, *Polynomial cycles in finitely generated domains.* Monatsh. Math. **119** (1995), 275–279.

[HKN2] F. Halter-Koch, W. Narkiewicz, *Polynomial cycles and dynamical units.* Proc. Conf. Analytic and Elementary Number Theory, 70–80, Wien, 1996.

[HKN3] F. Halter-Koch, W. Narkiewicz, *Scarcity of finite polynomial orbits.* Publ. Math. Debrecen **56** (2000), 405–414.

[Le] D. H. Lehmer, *On a problem of Störmer.* Illinois J. Math. **8** (1964), 57–79.

[Len] H. W. Lenstra Jr., *Euclidean number fields of large degree.* Invent. Math. **38** (1977), 237–254.

[LN] A. Leutbecher, G. Niklasch, *On cliques of exceptional units and Lenstra's construction of Euclidean fields.* Number Theory, Lecture Notes in Math. **1380**, 150–178, Springer, 1989.

[MDT] D. Z. Mo, R. Tijdeman, *Exponential diophantine equations with four terms.* Indag. Math. (N.S.) **3** (1992), 47–57.

[Mo] P. Morton, *Arithmetic properties of periodic points of quadratic maps*, II. Acta Arith. **87** (1998), 89–102.

[N1] W. Narkiewicz, *Polynomial Mappings.* Lecture Notes in Math. **1600**, Springer, 1995.

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

[Pe] T. Pezda, *Polynomial cycles in certain local domains.* Acta Arith. **66** (1994), 11–22.

[Pi] S. S. Pillai, *On the equation* $2^x - 3^y = 2^X + 3^Y$. Bull. Calcutta Math. Soc. **37** (1945), 15–20.

[Sch] H. P. Schlickewei, *S-units equations over number fields.* Invent. Math. **102** (1990), 95–107.

[Sc] R. SCOTT, *On the equation* $p^x - b^y = c$ *and* $a^x + b^y = c^z$. J. Number Theory **44** (1993), 153–165.

[Si] W. SIERPIŃSKI, *Sur une question concernant le nombre de diviseurs premiers d'un nombre naturel.* Colloq. Math. **6** (1958), 209–210.

[Sk] C. M. SKINNER, *On the diophantine equation* $ap^x + bq^y = c + dp^z q^w$. J. Number Theory **35** (1990), 194–207.

[St] C. STÖRMER, *Quelques théorèmes sur l'équation de Pell* $x^2 - Dy^2 = \pm 1$ *et leurs applications.* Skr. Vidensk.-selsk. (Christiania) I, Mat. Naturv. Kl. (1897), no.2, 1–48.

[TW] R. TIJDEMAN, L. WANG, *Sums of products of powers of given prime numbers.* Pacific J. Math. **132** (1988), 177–193; corr. *ibidem* **135** (1988), 396–398.

[Wa] C. T. C. WALL, *A theorem on prime powers.* Eureka **19** (1957), 10–11.

[Wg] L. X. WANG, *Four terms equations.* Indag. Math. **51** (1989), 355–361.

Władysław NARKIEWICZ
Institute of Mathematics
Wrocław University
Plac Grunwaldzki 2-4
PL–50–384 Wrocław
Poland
E-mail : narkiew@math.uni.wroc.pl