A NOTE ON SHANKS'S CHAINS OF PRIMES

E. TESKE AND H. C. WILLIAMS

ABSTRACT. For integers a and b we define the Shanks chain $p_1, p_2, \dots, p_k$ of length k to be a sequence of k primes such that $p_{i+1} = ap_i{}^2 - b$ for $i = 1, 2, \dots, k-1$. While for Cunningham chains it is conjectured that infinitely long chains exist, this is, in general, not true for Shanks chains. In fact, with $s = ab$ we show that for all but 56 values of $s \le 1000$ any corresponding Shanks chain must have finite length. For this, we study certain properties of functional digraphs of quadratic functions over prime fields, both in theory and practice. We give efficient algorithms to investigate these properties and present a selection of our experimental results.

1. Introduction

Let $\epsilon \in \{+1, -1\}$ be fixed. A *Cunningham chain* $p_1, p_2, p_3, \dots, p_n$ of length k (see Guy [9], §A7) is a sequence of k primes such that

$$p_{i+1} = 2p_i + \epsilon \qquad (i = 1, 2, \dots, k-1) .$$

For example, if $\epsilon = 1$, we say that

$$2, 5, 11, 23, 47$$

is a Cunningham chain of length 5. The longest known chains of Cunningham primes have recently been determined by Forbes [8]. For $\epsilon = 1$ the longest chains have $k = 14$ (one of these has $p_1 = 23305436881717757909$), and for $\epsilon = -1$, the longest known chain has $k = 16$ ($p_1 = 3203000719597029781$). Indeed by Schinzel's [16] [17] Conjecture H one would expect for either value of ϵ and any given $k \ge 1$ the existence of an infinitude of Cunningham chains of length k. Consider now the quantitative version of Conjecture H, given by Bateman and Horn [4].

Hypothesis H. *Suppose $f_1, f_2, \dots, f_k$ are polynomials in one variable with all coefficients integral and leading coefficients positive, their degrees being $h_1, h_2, \dots, h_k$ respectively. Suppose each of these polynomials is irreducible over the field of rational numbers and no two of them are identical. Let $P(N)$ denote the number of positive integers n between 1 and N inclusive such that $f_1(n), f_2(n), \dots, f_k(n)$ are all (positive) primes. Then as $N \to +\infty$ we have*

$$P(N) = \frac{C(f_1, f_2, \dots, f_k)}{h_1 h_2 \cdots h_k} \int_2^N \frac{du}{(\log u)^k} + o\left(\int_2^N \frac{du}{(\log u)^k}\right) ,$$

Date: January 4, 2000.

1991 *Mathematics Subject Classification.* 11N13, 11N32, 11D41, 11Yxx.

Research of the second author supported by NSERC of Canada grant #A7649.

where

$$C(f_1, f_2, \dots, f_k) = \prod_q \left\{ \left(1 - \frac{1}{q}\right)^{-k} \left(1 - \frac{\omega(q)}{q}\right) \right\} ,$$

the product being extended over all primes and $\omega(q)$ being the number of solutions of the congruence

$$f_1(x) f_2(x) \cdots f_k(x) \equiv 0 \pmod{q} . \tag{1.1}$$

For the case of Cunningham chains of length k we have

$$f_1(x) = x,\ f_2(x) = 2x + \epsilon,\ f_3(x) = 4x + 3\epsilon, \dots , f_k(x) = 2^{k-1}x + (2^{k-1} - 1)\epsilon .$$

For any given odd prime q, let $\nu(q)$ denote the multiplicative order of 2 modulo q. We must have $\nu(q) \mid q - 1$ and

$$\omega(q) = \begin{cases} k & \text{when } k \le \nu(q) \\ \nu(q) & \text{otherwise .} \end{cases}$$

Thus, $\omega(q) \le q - 1 < q$ and $C(f_1, f_2, \dots , f_k)$ is positive. We can therefore assert under this conjecture that if $P(N)$ is the number of Cunningham chains of length k starting with some $p_1 < N$, then as $N \to \infty$, we have

$$P(N) \sim C(f_1, f_2, \dots , f_k) \int_2^N \frac{du}{(\log u)^k} .$$

Evidently, $P(N)$ goes to infinity as N does.

In 1963 Shanks [19] observed (under Hardy and Littlewood's [10] Conjecture F) that if

$$Q(n) = \#\{x \,:\, 0 \le x \le n, x^2 - 17 \text{ is prime } \} ,$$

then

$$Q(n) \sim 1.1803 \int_2^n \frac{dx}{\log x} .$$

Since the value of the constant 1.1803 exceeds 1, this caused him to write the following passage in a letter [18] to D.H. and Emma Lehmer in 1969.

> "$n^2 - 17$ has a higher prime density than n itself, even though it grows twice as fast....
> It follows that prime chains
>
> $$p_{i+1} = (2p_i)^2 - 17$$
>
> should be [a] little longer than
>
> $$p_{i+1} = 2p_i + 1$$
>
> even though they grow twice as fast. I never did run it though. Try it sometime."

There is no record of any response to this by the Lehmers, possibly because the doubly exponential growth rate for the p_i values rapidly produces numbers that certainly would have been too difficult to test for primality by the methods available at the time. In a short computer trial we discovered that if $p_1 = 3$, then p_1, p_2, p_3, p_4 are all primes and if $p_1 = 303593$, then p_1, p_2, p_3, p_4, p_5 are all primes. We were unable to find a sequence of 6 primes for any $p_1 < 6200000$.

For a given pair of integers a, b, we set $f(x) = ax^2 - b$ and define $f_1(x) = x$, $f_{i+1}(x) = f(f_i(x))$ $(i = 1, 2, \dots)$. We define the corresponding *Shanks chain* of length k to be a set of primes

$$p_1, p_2, p_3, \dots, p_k$$

such that $p_i = f_i(p_1)$ $(i = 1, 2, \dots, k)$. It seems that Shanks believed that when $a = 4$ and $b = 17$ one might be able to get somewhat longer chains of primes (starting with $p_1 < N$ for a given N) than the Cunningham chains. However, this is not the case. For consider the prime 59. It turns out that for any integer x one finds that

$$f_i(x) \equiv 0 \pmod{59}$$

for some $i \leq 17$. Thus, the maximum chain length possible for this Shanks chain is 16. That is, if $k \geq 17$, then the number of solutions of (1.1) is 59 when $q = 59$ or $w(59) = 59$. Hence, $C(f_1, f_2, \dots, f_k) = 0$ if $k \geq 17$. The question that now comes to mind is: how often does this phenomenon occur? To investigate this question we first note that

$$af_{i+1}(x) = (af_i(x))^2 - ab \ .$$

Thus, for an integer s we will define $g(x, s) = x^2 - s$, $g_0(x, s) = x$, $g_{i+1}(x, s) = g(g_i(x, s))$ $(i = 0, 1, 2, \dots)$. It follows that if $s = ab$, we get

$$f_i(x) = g_{i-1}(ax)/a \ , \tag{1.2}$$

and if $q \nmid a$, then (1.1) has just as many solutions as

$$\prod_{i=0}^{k-1} g_i(x, s) \equiv 0 \pmod{q} \ . \tag{1.3}$$

We now turn our attention to the problem of determining whether for a fixed integer s there exists some prime q and some minimal $\kappa(> 0) = \kappa(s)$ such that $q \nmid s$ and for any integer x

$$g_i(x, s) \equiv 0 \pmod{q} \tag{1.4}$$

for some $i \leq \kappa$. That is, when is $\omega(q) = q$ for $f_i(x)$ given by (1.2) and $k > \kappa$? We have already seen that if $s = 9$ $(\equiv 68 = 4 \cdot 17 \pmod{59})$, then this must be the case for $p = 59$ and $\kappa = 16$. In Table 1.1 we present for values of $q \leq 200$ those values of $s \pmod{q}$ and corresponding values of κ such that (1.4) must hold for some $i \leq \kappa$. Note that for these values of s the maximum possible chain length of a Shanks chains is $\kappa(s)$.

A glance at Table 1.1 reveals that for many values of s we would not expect to have arbitrarily long Shanks chains. The purpose of this paper is to examine when $\omega(q) = q$ for a particular value of s.

q	$s,\kappa(s)$	q	$s,\kappa(s)$	q	$s,\kappa(s)$
2		59	9,17; 25,11	137	87,27; 118,31
3	1,2	61	39,15; 45,11; 48,9	139	41,22; 107,21
5	4,3	67	62,16	149	96,32; 129,24
7	1,3; 4,3	71		151	94,35; 127,20; 137,27
11	5,5	73	61,22;	157	16,33; 100,32
13	9,6; 10,5	79	8,17	163	84,20; 135,29
17		83	37,21; 51,21	167	49,26
19	9,7; 17,7	89	10,18	173	151,40
23	1,9	97	54,18; 66,25	179	
29	5,8; 22,10; 25,11	101	54,25	181	136,25
31	16,8; 19,10	103	18,20	191	64,24; 104,24
37	33,13	107	102,22	193	4,39; 126,25
41	25,15; 39,13; 40,9	109	38,17; 82,27	197	
43	17,8	113		199	47,26; 98,32; 103,23
47		127	35,20; 74,30; 87,17		
53	44,14	131			

TABLE 1.1.

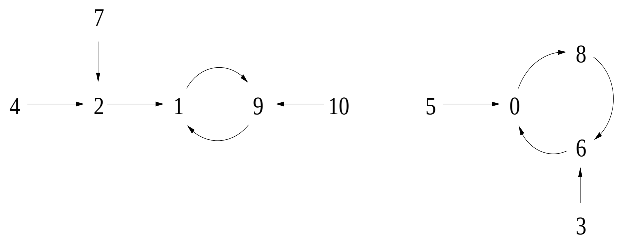
2. GENERATORS

Clearly, we are dealing here with a problem which involves iterating a nonlinear function modulo a prime; such problems, even for functions as simple as quadratic polynomials, are notoriously difficult. However, it is well known (and easy to prove) that for any integer x, there exist a least integer m and a least integer $n > m$ such that

$$g_m(x,s) \equiv g_n(x,s) \pmod{q}\ .$$

We denote this value of m by $\lambda = \lambda(x,s)$ and the value of $n-m$ by $\mu = \mu(x,s)$. λ is called the tail length, μ is called the cycle length and $\rho = \mu + \lambda = n$ is called the ρ-length of x with respect to $g(x,s)$ and q. Note that the values of $g_i(x,s)$ $(i = 0,1,2,\dots,\rho-1)$ are distinct modulo q, but that $g_\rho(x,s) \equiv g_\lambda(x,s) \pmod{q}$. Many probabilistic results are known concerning μ, λ, ρ for the iteration of random function (see Flajolet and Odlyzko [7] for several such results and references), and in [7] it is postulated that the properties of quadratic functions modulo an integer should be asymptotically the same as those of the class of all functions. Indeed, Bach [1] has proved that in initial stages, at least, quadratic functions do behave asymptotically like random functions. Thus, the expected values of μ, λ, ρ here should have values close to $\sqrt{\pi q/8}$, $\sqrt{\pi q/8}$ and $\sqrt{\pi q/2}$, respectively. Furthermore, the expected maximum values of μ, λ, ρ are respectively asymptotic to $c_1\sqrt{q}$, $c_2\sqrt{q}$, $c_3\sqrt{q}$, where $c_1 \approx .78248$, $c_2 \approx 1.73746$, $c_3 \approx 2.4149$. (See [7]).

Now consider the functional digraph of $g(x,s)$ over $\mathbb{F}_q$, the finite field of q elements. This is the directed graph whose nodes are the elements of $\mathbb{F}_q$ and whose edges are the ordered pairs $\langle x, g(x,s)\rangle$ for all $x \in \mathbb{F}_q$. For example, the functional digraph of $g(x,s)$ over $\mathbb{F}_{11}$ is



Each connected component of the functional digraph contains exactly one cycle. Thus, in the case of $g(x,9)$ over $\mathbb{F}_{59}$ the functional digraph has exactly one component with its cycle containing the node 0.

We say that s is a *generator* for a prime q if for any integer x, there must exist some minimal i (≥ 0) such that

$$g_i(x,s) = 0 \tag{2.1}$$

in $\mathbb{F}_q$. Thus, s is a generator for a prime q if and only if the functional digraph of $g(x,s)$ over $\mathbb{F}_q$ has a single connected component whose cycle contains the node 0. If s is a generator, we define $\kappa(=\kappa(s)) = \max\{i\}$ of all the values of i given by (2.1). Thus, if s is a generator, then any $x \in \mathbb{F}_q$ can be written as

$$x = \pm\sqrt{s \pm \sqrt{s \pm \sqrt{s \pm \sqrt{\dots}}}}$$

with no more than κ radicals. Since the expected number of connected components for the functional digraph (under the same caveats as those mentioned above) is $(\log q)/2$ (see [7]), we would not expect to find many generators for a given q and this is borne out by computations (see §4). Evidently, if $s = ab$ is a generator for some q, then $\omega(q) = q$ for $f(x) = ax^2 - b$ and $k > \kappa(s)$; the length of any corresponding Shanks chain can, therefore, not exceed $\kappa(s)$.

We now develop a technique for determining when s is a generator for a given q. Of course, this seems to be a very simple task because all we need do is start at some node $n_0 \in \mathbb{F}_q$ and by iterating g at this node compute the set $\mathcal{S}_{n_0}$ of all distinct nodes in its tail and cycle $\mathcal{C}_{n_0}$ over $\mathbb{F}_q$. If $\mathcal{S}_{n_0} = \mathbb{F}_q$, we are finished, but if $\mathcal{S}_{n_0} \neq \mathbb{F}_q$, we select $n_1 \notin \mathcal{S}_{n_0}$ and repeat the process. If for some h we get $\mathcal{C}_{n_0} = \mathcal{C}_{n_1} = \cdots = \mathcal{C}_{n_h}$ and $\cup_{i=0}^{h} \mathcal{S}_{n_i} = \mathbb{F}_q$, then s must be a generator; otherwise s is not. The difficulty with this very simple algorithm is that when it is implemented on a computer and q is large, the amount of memory management required during its run greatly degrades its performance.

We can develop an algorithm for proving that s is a generator for a given q which does not involve a great deal of memory management if we are willing to do some extra work. To this end we define the following subsets of $\mathbb{F}_q$. We put $\mathcal{R}_0 = \{0\}$ and define $\mathcal{R}_{i+1}$ recursively from $\mathcal{R}_i$ by

$$\mathcal{R}_{i+1} = \{t \,:\, t^2 = r + s, r \in \mathcal{R}_i, t \neq 0\}\ .$$

For example, if $q = 367$ and $s = 1$, we have $\mathcal{R}_0 = \{0\}$, $\mathcal{R}_1 = \{\pm 1\}$, $\mathcal{R}_2 = \{\pm 288\}$, $\mathcal{R}_3 = \{\pm 17\}$, $\mathcal{R}_4 = \{\pm 237\}$, $\mathcal{R}_5 = \emptyset$.

We next establish some very simple results concerning $\mathcal{R}_i$.

Lemma 2.1. *If $g(x,s) \in \mathcal{R}_i$ and $x \neq 0$, then $x \in \mathcal{R}_{i+1}$.*

Proof. We have $x^2 = g(x,s) + s$. Since $x \neq 0$, we must have $x \in \mathcal{R}_{i+1}$ because $g(x,s) \in \mathcal{R}_i$. □

Corollary. *If $g_j(x,s) = 0$ and $g_{j-i}(x,s) \neq 0$ $(0 \leq i \leq j)$, then $x \in \mathcal{R}_i$.*

Proof. Follows easily by induction on j. □

Lemma 2.2. *If $x \in \mathcal{R}_j$ $(j > 0)$, then $g(x,s) \in \mathcal{R}_{j-1}$.*

Corollary. *If $x \in \mathcal{R}_j$ $(j > 0)$, then $g_i(x,s) \in \mathcal{R}_{j-i}$ $(0 \leq i \leq j)$.*

Theorem 2.3. *If $i > 0$, then*

$$\mathcal{R}_i = \{x \,:\, g_i(x,s) = 0, g_j(x,s) \neq 0 \ (j = 0, 1, 2, \ldots, i-1)\} \ .$$

Proof. Follows easily from the corollaries of Lemmas 2.1 and 2.2. □

Corollary 2.3.1. *If $j > i$, then $\mathcal{R}_i \cap \mathcal{R}_j = \emptyset$.*

Proof. If $x \in \mathcal{R}_j$, then $g_i(x,s) \neq 0$ $(i < j)$, which means that $x \notin \mathcal{R}_i$. □

Corollary 2.3.2. *If*

$$\sum_{i=0}^{k} \#\mathcal{R}_i = q \ , \tag{2.2}$$

then s is a generator for q. Conversely, if s is a generator for q, then (2.2) *holds.*

Corollary 2.3.2 can be used by a computer to prove that s is a generator for q, and, as we can produce $\mathcal{R}_{i+1}$ from $\mathcal{R}_i$ only and the values of $\#\mathcal{R}_i$ tend to be small, the memory requirements are modest. Of course, we must compute roughly $\#\mathcal{R}_i/2$ square roots modulo q to produce $\mathcal{R}_{i+1}$, but in practice, the Tonelli-Shanks algorithm (see Bach and Shallit [2], pp. 155-157) for doing this is very efficient; moreover, we developed a method based on the continued fraction expansion to compute square roots modulo q that is by roughly a factor of two faster than the Tonelli-Shanks algorithm (see §4). That the values of $\#\mathcal{R}_i$ tend to be relatively small follows on noting that in the case that (2.2) holds k must exceed the maximum λ value and is likely close to the maximum ρ value. Since we expect that about half of the values of r in $\mathcal{R}_i$ are such that $((r+s)/q) = 1$, we expect that $\#\mathcal{R}_{i+1} \approx \#\mathcal{R}_i$. Thus, $k\#\mathcal{R}_i \approx q$ or $\#\mathcal{R}_i \approx q/k$ which will likely be less than $\sqrt{q}/c_3$. However, it turns out that in practice the average value of $\#\mathcal{R}_i$ tends to be much smaller than $\sqrt{q}/c_3$.

We can produce more useful necessary conditions for s to be a generator for q.

Theorem 2.4. *If s is a generator for q and $q > 2^j - 1$, then $\mathcal{R}_1, \mathcal{R}_2, \mathcal{R}_3, \ldots, \mathcal{R}_j \neq \emptyset$.*

Proof. Since the degree of $g_i(x,s)$ as a polynomial in x is 2^i, there can be at most $\sum_{i=0}^{j-1} 2^i = 2^j - 1$ values of x in $\mathbb{F}_q$ such that $g_i(x,s) = 0$ for $i \le j-1$. Since $2^j - 1 < q$, there must (if s is a generator for q) be some x such that $g_k(x,s) = 0$ $(k > j-1)$ and $g_i(s,x) \ne 0$ for all $0 \le i \le k-1$. Since $x \in \mathcal{R}_k$, we have $\mathcal{R}_k \ne \emptyset$ and therefore $\mathcal{R}_1, \mathcal{R}_2, \mathcal{R}_3, \dots, \mathcal{R}_j \ne \emptyset$. □

From this result we readily conclude that 1 cannot be a generator for 367 because $367 > 2^8 - 1$ and $\mathcal{R}_5 = \emptyset$. Furthermore, if $(s/q) = -1$, then $\mathcal{R}_1 = \emptyset$ which means that s cannot be a generator for q. Note that this theorem provides a possible technique for eliminating a given s as a possible generator for q. If $q > 2^j - 1$ for some conveniently selected value of j, we need only compute the sets $\mathcal{R}_1, \mathcal{R}_2, \mathcal{R}_3, \dots, \mathcal{R}_j$. If we find an empty one, then we know that s cannot be a generator for q. If we consider the special case of $s = 1$, we know that $\mathcal{R}_1 = \{\pm 1\}$ and $\mathcal{R}_2 = \{x : x^2 \equiv 2 \pmod{q}\}$. We get $\mathcal{R}_2 = \emptyset$ if $(2/q) = -1$.

If $(2/q) = 1$, then $\mathcal{R}_3 = \{x : x^2 = 1 + t, t^2 \equiv 2 \pmod{q}\}$. Now $(1-t)(1+t) = 1 - t^2 = -1$; hence, if $q \equiv 1 \pmod{8}$, then $((1-t)/q) = ((1+t)/q)$. Thus $\mathcal{R}_3 = \emptyset$ if $((1+t)/q) = -1$.

By a result of Barrucand and Cohn [3], we know this can only occur when q cannot be represented by the quadratic partition $a^2 + 32b^2$. We have the following theorem.

Theorem 2.5. *1 cannot be a generator for any prime q such that $q \equiv 3, 5 \pmod{8}$ or for any prime $q \equiv 1 \pmod{8}$ such that $q \ne a^2 + 32b^2$.*

3. Cycles

We mentioned earlier that it seems an unlikely event that any particular s will be a generator for a given q. Certainly, s will not be a generator if the functional digraph of $g(x,s)$ over $\mathbb{F}_q$ contains a cycle which does not have 0 as a node. In this section we will investigate the problem of the existence of small cycles. We will consider the cases of minimal $\mu = 1, 2, 3, 4$ only. For $\mu = 1$, we want to know whether there exists some x such that $g(x,s) = x$ in $\mathbb{F}_q$. Clearly, this will be the case if and only if $((4s+1)/q) = 0, 1$. Furthermore, this cycle is made up of the node x only when $(2x+1)^2 \equiv 4s + 1 \pmod{q}$. Since $x \not\equiv 0 \pmod{q}$ under this condition, we have proved the following simple result.

Theorem 3.1. *If $((4s+1)/q) = 0, 1$, then s is not a generator for q.*

We also have the following result.

Theorem 3.2. *If $s = t^2 - t$ $(\ne 0)$, then s can never be a generator for any prime q.*

For the case that $\mu = 2$, we must have $g_2(x,s) = x$ and $g_1(x,s) \ne x$ in $\mathbb{F}_q$. Now it is easy to see that

$$g_2(x,s) - x = (g_1(x,s) - x)(x^2 + x - s + 1) ;$$

thus, we have a cycle of length 2 if and only if $((4s-3)/q) = 0, 1$. However, since this cycle is made up of the nodes $\{x, -1-x\}$ when $(2x+1)^2 \equiv 4s - 3 \pmod{q}$, we see that 0 is not in the cycle only when $s \not\equiv 1 \pmod{q}$.

Theorem 3.3. *If $s \not\equiv 1 \pmod q$ and $((4s-3)/q) = 0, 1$, then s is not a generator for q.*

Also, if $s = t^2 + t + 1$, then s is not a generator for any q unless $s \equiv 1 \pmod q$ and 1 is a generator for q.

Theorem 3.4. *If $s = t^2 + t + 1$, $(t \le B)$, then s can never be a generator for any prime q if $t \not\equiv 0, -1 \pmod r$ for all primes $r \le B$ such that 1 is a generator for r.*

Now 1 is a generator for $r = 3, 7, 23$ and for no other prime ≤ 5000. Thus, if $s = t^2 + t + 1$ $(t \le 5000)$ and $t \not\equiv 0, -1 \pmod 3$, $t \not\equiv 0, -1 \pmod 7$ and $t \not\equiv 0, -1 \pmod{23}$, then s can never be a generator for any prime q.

Notice that for the forms of s given by Theorems 3.2 and 3.4 we can never have $\omega(q) = q$ when $s = ab$. Thus, we should (under Conjecture H) be able to find corresponding Shanks chains of arbitrary length. Also for these forms we have solutions in $\mathbb{Z}$ of $g_i(x, s) = x$. However, by a result of Narkiewicz ([14], Theorem 2), we know that there are no values of x in $\mathbb{Z}$ such that the least cycle length of $g(x, s)$ exceeds 2. This suggests (but certainly does not prove) that the only possible values of s which can never be a generator for any q are those given in Theorems 3.2 and 3.4.

We next consider the case of cycles of length 3 over $\mathbb{F}_q$. This has been examined for arbitrary fields of odd characteristic by Morton [12], but we will use a somewhat different and computationally more convenient approach here. We have

$$g_3(x, s) - x = (g_1(x, s) - x)c(x) ,$$

where

$$c(x) = x^6 + x^5 + (1-3s)x^4 + (1-2s)x^3 + (1-3s+2s^2)x^2 + (1-2s+s^2)x + 1 - s + 2s^2 - s^3 .$$

If we have a cycle of length 3 for $g(x, s)$ over $\mathbb{F}_q$, we must have three distinct zeros of $c(x)$, because if x is a zero of $c(x)$ in $\mathbb{F}_q$, then so also must be $g_1(x, s)$ and $g_2(x, s)$. That is, $x^2 - s$ and $(x-s)^2 - s$ must be zeros if x is. This follows from the simple observation that $g_{i+j}(x, s) = g_i(g_j(x, s), s)$. By an old result of Escott [6], we know that if $c(x)$ is to have a zero in $\mathbb{F}_q$, then $s = a^2 - a + 2$ for some $a \in \mathbb{F}_q$. When this happens, we get

$$c(x) = (x^3 + ax^2 + (a-s-1)x - (as-s+1))(x^3 + a'x^2 + (a'-s-1)x - (a's-s+1)) ,$$

where $a' = 1 - a$. Then, a necessary condition that there be a cycle of length 3 for $g(x, s)$ over $\mathbb{F}_q$ is that $((4s-7)/q) = 0, 1$. Now if $q \ne 3$ and $s = a^2 - a + 2$, we see that

$$p(x) = x^3 + ax^2 + (a-s-1)x - (as-s+1)$$

will have 3 zeros in $\mathbb{F}_q$ if and only if

$$h(x) = x^3 + 3(2a-1-4s)x - (16as + 2a - 20s + 13)$$

has 3 zeros in $\mathbb{F}_q$. Since

$$16as + 2a - 20s + 13 = (4a-3)(4s-2a+1) ,$$

it is a simple matter to evaluate the discriminant D of $h(x)$ as

$$D = -27(4s-2a+1)^2 .$$

If $4s-2a+1=0$ in $\mathbb{F}_q$, then $p(x)$ has the zero $-a/3$ with multiplicity 3; furthermore, if $x=-a/3$, then $g(x,s)=x$. Thus, we exclude this possibility and we find that $(D/q) = (-3/q) \equiv q \pmod 3$. By classical results concerning the solubility of cubic congruences modulo q (see Dickson [5], p. 256) we know that $h(x)$ can have 3 zeros in $\mathbb{F}_q$ if and only if $q \equiv (D/q) \pmod 3$ and

$$\alpha^{(q^2-1)/3} \equiv 1 \qquad \pmod q ,$$

where $\alpha = (A+\sqrt{D})/2$, $A = 16as+2a-20s+13$. We note that $\alpha = (4s-2a+1)\gamma$, where γ is a zero of $x^2-(4a-3)x+4s-2a+1$. If ζ is a primitive cube root of unity ($\zeta^2+\zeta+1=0$), then $\gamma = 2a+3\zeta$.

If $q \equiv -1 \pmod 3$, then $\alpha^{(q^2-1)/3} \equiv [\lambda/q] \pmod q$, where $[\lambda/q]$ is defined to be the value of ζ^i in $\mathbb{Z}[\zeta]$ such that $\gamma^{(q^2-1)/3} \equiv \zeta^i \pmod q$. If $q \equiv 1 \pmod 3$, then $\alpha^{(q^2-1)/3} = [\alpha/\pi]$, where π is a primary prime factor of q in $\mathbb{Z}[\zeta]$ and $[\alpha/\pi]$ is that value of ζ^i such that $\alpha^{(q^2-1)/3} \equiv \zeta^i \pmod \pi$. Thus, if $q \nmid 4s-2a+1$ and $q \neq 3$, then $p(x)$ has three zeros in $\mathbb{F}_q$ if and only if $[\gamma/q]=1$ when $q \equiv -1 \pmod 3$ or $[(4s-2a+1)\gamma/\pi] = 1$ when $q \equiv 1 \pmod 3$ and π is a primary prime factor of q. Also, if a cycle of length 3 exists for this s and a and $as-s+1 \neq 0$ in $\mathbb{F}_q$, then none of the zeros of $p(x)$ can be zero. We have proved the following theorem.

Theorem 3.5. *If q is a prime, $q \neq 3$, $q \nmid 4s-2a+1$ and $((4s-7)/q) = 0, 1$, then there is a cycle of length 3 for $g(x,s)$ over $\mathbb{F}_q$ if and only if $s \equiv a^2-a+2 \pmod q$, $\gamma = 2a+3\zeta$ and $[\gamma/q]=1$ when $q \equiv -1 \pmod 3$ or $[(4s-2a+1)\gamma/\pi]=1$ when $q \equiv 1 \pmod 3$ and π is a primary prime divisor of q. Furthermore, if a cycle of length 3 exists for this value of s and a, and $q \nmid as-s+1$, then s cannot be a generator for q.*

We remark here that the values of $[\xi/\psi]$ here can be obtained quite rapidly by making use of the idea of Jacobi (see Williams and Holte [21]).

If we consider the case of $s=1$, we see that we must have $(-3/q)=1$ in order to have $\mu = 3$. Thus, we require that $q \equiv 1 \pmod 3$ and we may put

$$4q = L^2 + 27M^2 \qquad (L \equiv 1 \pmod 3)$$

as an essentially unique (up to the sign of M) quadratic partition of $4q$. Since $a^2-a+1 \equiv 0 \pmod q$ is soluble for $a \in \mathbb{Z}$, we may put $q = \pi_1\pi_2$, where $\pi_1 \mid a+\zeta$, $\pi_2 \mid a-1-\zeta$ and π_1, π_2 are primary prime divisors of q in $\mathbb{Z}[\zeta]$. We have

$$(4s-2a+1)\gamma \equiv (5-2a)(2a+3\zeta) \equiv \zeta(5+2\zeta) \equiv 3\zeta - 2 \qquad \pmod{\pi_1} .$$

Also, $4s-2a+1 = 5-2a \neq 0$ if $q \neq 19$. Since $2-3\zeta$ is a primary prime divisor of 19, we get

$$\left[\frac{\gamma(4s-2a+1)}{\pi_1}\right] = \left[\frac{3\zeta-2}{\pi_1}\right] = \left[\frac{2-3\zeta}{\pi_1}\right] = \left[\frac{\pi_1}{2-3\zeta}\right]$$

by the law of cubic reciprocity. Now we select the sign of M such that $\pi_1 = (L+3M)/2+3M\zeta$ and note that $\zeta \equiv -12 \pmod{2-3\zeta}$; hence, $\pi_1 \equiv (L+3M)/2 - 36M \pmod{2-3\zeta}$. Thus, $[\pi_1/(2-3\rho)] = 1$ if and only if

$$((L+3M)/2-36M)^6 \equiv 1 \qquad \pmod{19} .$$

Since $2^{18} = 8^6 \equiv 1 \pmod{19}$, this is equivalent to $(4L+9M)^6 \equiv 1 \pmod{19}$ or $4L+9M \in \{\pm 1, \pm 7, \pm 8\} \pmod{19}$. We now have the following result for $s = 1$.

Theorem 3.6. *If $s = 1$ and $q \neq 3, 19$, there is a cycle of length 3 for $g(x,s)$ over $\mathbb{F}_q$ if and only if $q \equiv 1 \pmod 3$, $4q = L^2 + 27M^2$ and either $4L + 9M$ or $4L - 9M \in \{\pm 1, \pm 7, \pm 8\} \pmod{19}$. If both $4L+9M$ and $4L-9M \in \{\pm 1, \pm 7, \pm 8\} \pmod{19}$, then there are exactly two cycles of length 3. Also, 1 cannot be a generator for any q such that $g(x,s)$ over $\mathbb{F}_q$ has a cycle of length 3.*

If we consider the example of $q = 157$, we get $L = -14$, $M = \pm 4$. Since $4\cdot(-14)+9\cdot 4 \equiv -1$ and $4\cdot(-14) - 9 \cdot 4 \equiv 3 \bmod 19$, we see that there is a single cycle for $s = 1$; this is $\{92, 142, 67\}$. If $q = 151$, we get $L = 19$, $M = \pm 3$ and $4L \pm 9M \equiv \pm 8 \pmod{19}$. Thus, in this case we get two cycles, namely $\{19, 58, 41\}$ and $\{85, 127, 122\}$.

For the case of $\mu = 4$, it is convenient to use the techniques of Morton ([13], pp. 91-92). While they were employed with respect to $\mathbb{Q}$, they are very readily applicable to the case of $\mathbb{F}_q$. With some very simple manipulation of his formulas, it is easy to derive the following theorem.

Theorem 3.7. *If q is an odd prime and $q \nmid (4s-5)(16s^2+8s+5)$, there can be a cycle of length 4 for $g(x,s)$ over $\mathbb{F}_q$ if and only if there exists some solution $z \in \mathbb{Z}$ of*

$$z^3 + (3-4s)z + 4 \equiv 0 \pmod q$$

and a corresponding solution $w \in \mathbb{Z}$ of

$$w^2 - zw - 1 \equiv 0 \pmod q$$

such that

$$(z(zw+2)(z+2)/q) = 1 .$$

Furthermore, if such a cycle exists and $q \nmid z^6 + 2z^5 + 4z^4 + 6z^3 - 5z^2 - 8z - 16$, then s cannot be a generator for q.

As an example, we give $q = 23$ and $s = 40$. We find $z = 38$ and $w = 2$ and the corresponding cycle is $\{36, 15, 39, 21\}$.

4. Algorithms and computational results

We have already mentioned that one would not expect to find many generators s for a given prime q. In fact, by using a computer, we found all the generators for each prime $< 10^4$. Let $n(q)$ denote the number of generators for q and

$$N(x) = \#\{q : n(q) = x, q < 10^4\} .$$

In Table 4.1 we present some values of $N(x)$; note that $N(x) = 0$ if $n > 8$.

Thus, the average number of generators for each prime $q < 10^4$ is $\sum_0^8 iN(i)/\sum_0^8 N(i) \approx 1.14$. Incidentally, the value of q for which there are 8 generators is $q = 9767$ with generators $1051, 1937, 2217, 2301, 3478, 3697, 5471, 6803$.

x	$N(x)$	x	$N(x)$	x	$N(x)$
0	378	3	100	6	0
1	464	4	25	7	0
2	258	5	3	8	1

TABLE 4.1.

We used these generators to sieve out all the values of $s < 1000$ which must be a generator for some $q < 10^4$. The remaining values of s are presented in the tableau below.

2 3 6 12 20 21 30 42 56 72 90
105 108 110 111 128 132 156 182 195 198
206 210 213 215 240 251 272 273 287 290 293
303 306 311 338 342 356 380 381
420 437 462 471 483 495
506 525 545 548 552 570 591 593
600 612 623 630 642 650 651 656 657 675
702 713 723 726 735 740 752 755 756 768 770
800 812 821 840 857 861 870
908 912 930 936 957 965 987 992 993 996

Of these remaining numbers, we see that 2, 3, 6, 12, 20, 21, 30, 42, 56, 72, 90, 110, 111, 132, 156, 182, 210, 240, 272, 273, 306, 342, 380, 381, 420, 462, 506, 552, 600, 650, 651, 702, 756, 812, 870, 930, 992 and 993 are all of the forms given in Theorems 3.2 and 3.4; hence, these numbers can never be generators for any q. This leaves 54 numbers (< 1000) which may be generators for some prime $q > 10^4$. If, in fact, the only values of s which can never be generators for any q are those given by Theorems 3.2 and 3.4, we would expect to be able to eliminate all of these 54 remaining numbers by increasing our limit on q beyond 10^4. This means that we need to develop reasonably efficient algorithms for detecting when a particular s is a generator for a given q.

Such an algorithm is implicit in Corollary 2.3.2, but as we have seen earlier, it is most unlikely that a given s will be a generator for a given q; thus, it is best to develop an algorithm that will quickly determine that s is not a generator for q (when this is the case).

We note that since the average cycle length is expected to be $\sqrt{\pi q/8}$, the chance that it contains a zero node is $\sqrt{8/\pi q}$ which is very small. Indeed, if we examine all primes q such that $109 \le q < 10^5$ for $s = 108$ with the property that $(s/q) = 1$ and $(4s + 1/q) = -1$ and $(4s - 3/q) = -1$ and let $m(x) = \#\{q : x$ is the smallest number ≥ 0 such that the cycle in the component beginning with x does not contain a zero node$\}$, when $m(x) \neq 0$ we get Table 4.2.

Thus, to determine that s is not a generator for q we have the following algorithm: For $x = 0, 1, 2, \dots$ up to a certain bound B we check whether the cycle in the component beginning with x contains a zero node. For this, we compute the sequences $(g_i(0, s))_{i \ge 0}$ and $(g_{2i}(0, s))_{i \ge 0}$, and for each $i = 1, 2, \dots$ we check whether $g_i(0, s) \equiv g_{2i}(0, s) \pmod q$. This is

x	$m(x)$	x	$m(x)$
0	1185	5	1
1	11	7	1
2	4	9	1
4	2	45	1

TABLE 4.2.

expected to happen for $i \approx 1.0308\sqrt{q}$ (Floyd's method, see [15]). When this is the case, we know that $g_i(0,s)$ is in the cycle for that i, so that we compute $g_{i+1}(0,s)$, $g_{i+2}(0,s), \ldots$ until we find a minimal j such that $g_{i+j}(0,s) \equiv 0 \pmod{q}$ or $g_{i+j}(0,s) \equiv g_i(0,s) \pmod{q}$. If the latter happens first, we know that the zero node is not in the cycle, and s is not a generator for q. Otherwise, we compute for $x = 1, 2, \ldots$ the sequences $(g_i(x,s))_{i\geq 0}$ and $(g_{2i}(x,s))_{i\geq 0}$ and, while doing this, check whether $g_{2i-1} \equiv 0 \pmod{q}$ or $g_{2i}(x,s) \equiv 0 \pmod{q}$. As soon as this happens, we know that x belongs to the same component as the zero node, which is in the cycle. If $g_i(x,s) \equiv g_{2i}(x,s) \pmod{q}$ for some i and $g_j(x,s) \not\equiv 0 \pmod{q}$ for all $j \leq 2i$, we know that x belongs to a component different from the one with the zero node. As soon as this happens for some x, we know that s is not a generator for q. Otherwise, s may be a generator.

For example, for the 54 remaining values for s and the primes q between 10^4 and 10^5 for which $(s/q) = 1$ and $(4s+1/q) = -1$ and $(4s-3/q) = -1$, with $B = 100$ we find that altogether 40 pairs (s,q) pass this test. Among these 40 pairs, there are 15 cases where s indeed is a generator for q. When working with $B = 1000$, only 17 pairs (s,q) pass this test. Notice that, for given s, the test has to be applied only to about 12.5% of the 8363 primes between 10^4 and 10^5, since about 87.5% of the q are eliminated by checking the three Legendre symbols.

The running time for each $x = 0, 1, \ldots, B$ is proportional to the ρ-length and hence is expected to grow with $\sqrt{q}$. Given s, for larger values of q we therefore use the following, faster algorithm: First we choose parameters j_0 and B. Now, given a pair (s,q) such that $(s/q) = 1$ and $(4s+1/q) = -1$ and $(4s-3/q) = -1$, we check whether $\mathcal{R}_3$ is empty. If this is the case, s cannot be a generator for q. Otherwise, we apply the criteria provided by Theorems 3.5 and 3.7. If after that it is still possible that s is a generator for q, we compute $\mathcal{R}_4, \ldots, \mathcal{R}_{j_0}$. Only if $\mathcal{R}_j \neq \emptyset$ for all $k \leq j_0$ and if $\sum_{j=0}^{j_0} \#\mathcal{R}_j < q$, we check for $x = 0, 1, 2, \ldots, B$ whether the cycle in the component beginning with x contains a zero node. For $q \in [10^6, 10^{10}]$, a suitable choice for j_0 and B is $j_0 = 30$ and $B = 2000$. To illustrate the performance of this algorithm, for $s = 108, 840$ and $n = 4, 5, 6, 7, 8, 9$ we consider the least 10000 primes $\geq 10^n$ and let $k(n,s) = \#\{q : (s/q) \neq -1 \text{ or } (4s+1/q) \neq -1 \text{ or } (4s-3/q) \neq -1\}$. By $r_3(n,s)$ we denote the number of those primes q not included in $k(n,s)$ and for which $\mathcal{R}_3 = \emptyset$. By $c_3(n,s)$ we denote the number of those q among the primes not counted so far for which we can prove the existence of a cycle of length 3 using Theorem 3.5. Then, by $c_4(n,s)$ we denote the number of primes among the remaining values of q for which Theorem 3.7 establishes the existence of a cycle of length 4. By $r_{30}(n,s)$ we denote the number of those q that passed all tests so far and for which one of the $\mathcal{R}_4, \ldots, \mathcal{R}_{30}$ is empty and $\sum_{j=0}^{30} \#\mathcal{R}_j < q$. Then by $b_{2000}(n,s)$ we denote the number of those remaining q which do not pass the very last test that checks whether the component beginning with x ($x = 0, 1, \ldots, 2000$) contains a zero node. Our sample results are shown in Table 4.3. Here, the last column indicates how many primes q have passed all tests. These values of q are the only remaining candidates for which s can be a generator.

n	$k(n,s)$	$r_3(n,s)$	$c_3(n,s)$	$c_4(n,s)$	$r_{30}(n,s)$	$b_{2000}(n,s)$	survivors
			$s = 108$				
4	5019 + 2506 + 1224	516	208	103	342	82	0
5	4993 + 2456 + 1299	507	238	103	327	77	0
6	4983 + 2512 + 1230	524	192	119	345	95	0
7	5019 + 2488 + 1265	496	192	99	350	91	0
8	5015 + 2518 + 1216	489	192	122	366	82	0
9	5039 + 2497 + 1208	510	204	115	360	67	0
			$s = 840$				
4	4985 + 2534 + 1257	512	207	108	320	77	0
5	5042 + 2532 + 1211	452	214	112	360	77	1 ($q = 182101$)
6	4971 + 2517 + 1234	487	215	115	376	85	1 ($q = 1053583$)
7	5040 + 2525 + 1245	442	186	145	346	71	0
8	4990 + 2508 + 1245	488	214	112	354	89	0
9	4942 + 2558 + 1288	478	217	98	346	73	0

TABLE 4.3.

To process the values of q which remain in the end, we choose some larger bound B' and check for $x = 2001, \ldots, B'$ whether all components that begin with x end in a cycle that contains the zero node. For $q = 182101$ in Table 4.3 we find, for example, that the least positive number x that leads to a cycle that does not contain the zero node is $x = 3972$, while for $q = 1053583$ this is the case for $x = 80173$. Hence, $s = 840$ is not a generator for these values of q.

With the algorithm prescribed above we examined all primes q such that $100003 \leq q \leq 2 \cdot 10^8$ for all 54 remaining values of s. For 36 values of s we found a prime q such that s is a generator for q. In Table 4.4 we give the corresponding values of s and q. Notice that for each s, we only consider the least possible prime q for which s is a generator. In the third and sixth columns we also indicate the minimal value for k such that $\sum_{i=0}^{k} \#\mathcal{R}_i = q$, which also is the least k such that $\mathcal{R}_{k+1}$ is empty.

In summary of Table 4.4, Table 4.5 shows for various ranges of q the number of values of s such that q is the least prime for which s is a generator.

The remaining 18 values of s which are not a generator for any prime $q < 2 \cdot 10^8$ are $108, 128, 290, 338, 495, 525, 545, 623, 630, 656, 675, 723, 735, 755, 770, 800, 936, 987$. Extrapolating from the data in Table 4.5, we expect that in order to find appropriate values of q for all of these values of s, we would have to examine all values of q up to at least 10^{11}. This seems to be a hopeless task at present because we know of no algorithm that executes in fewer than constant times q steps for proving that s is a generator for a certain prime q.

s	q	k	s	q	k
105	97729	863	593	92802097	21661
195	1956979	2658	612	134639	833
198	820361	1682	642	1643779	3607
206	1746581	4191	657	23035711	11086
213	5994631	6548	713	275657	1242
215	25847	508	726	14087	286
251	89231	582	740	16691	374
293	56891	835	752	23059	444
287	8207041	6542	768	12441217	6044
303	29947	363	821	40682441	9916
311	631723	2063	840	10830383	6669
356	493853	1470	857	98947	888
437	34283	359	861	29947427	15438
471	20347	369	908	2060843	2695
483	31228199	17327	912	141184027	26912
548	58991	708	957	1686701	3379
570	493811	1757	965	39191	629
591	11369	204	996	35053	367

TABLE 4.4.

range for q	# generators
$[10^4, 10^5]$	15
$[10^5, 10^6]$	6
$[10^6, 10^7]$	7
$[10^7, 10^8]$	7
$[10^8, 2 \cdot 10^8]$	1

TABLE 4.5.

The largest value of q that appears in Table 4.4 is $q = 141184027$, which is the least prime for which $s = 912$ is a generator. Here, $\sum_{i=0}^{k} \#\mathcal{R}_i = q$ for $k = 26912$, with $\mathcal{R}_{26913}$ being the first set that is empty. The maximum value for $\#\mathcal{R}_i$ is 13198, while the average value for $\#\mathcal{R}_i$ is 5245. With an implementation using the computer algebra system LiDIA [11], the computation of the $\mathcal{R}_i$ took 4 hours, 6 minutes and 54 seconds on a SPARC Ultra-60. For this computation we used the Tonelli-Shanks algorithm to compute the square root of a modulo q.

We also devoloped another method to compute the square root of a modulo q that makes use of the continued fraction expansion of a/q. It works as follows. If $q \equiv 1 \pmod 4$, i.e., $(-1/q) = 1$, let λ such that $\lambda^2 \equiv -1 \pmod q$ and let n be a quadratic non-residue of q (which we can easily find by trial). If $q \equiv -1 \pmod 4$, let $\lambda = 1$ and $n = -1$. Now for $1 \leq x < \sqrt{q}$ we precompute tables of the Legendre symbols (x/q) and of the values $G(x)$

and $H(x)$, where

$$G(x) \equiv \begin{cases} \sqrt{x} & \text{if } (x/q) = 1 \\ \sqrt{nx} & \text{if } (x/q) = -1 \end{cases} \pmod{q}$$

and

$$H(x) \equiv \begin{cases} 1/\sqrt{x} & \text{if } (x/q) = 1 \\ 1/\sqrt{nx} & \text{if } (x/q) = -1 \end{cases} \pmod{q}\ ;$$

Here, $\sqrt{t}$ denotes either of the solutions, when they exist, of $y^2 \equiv t \pmod{q}$. To compute the square root of a modulo q when $(a/q) = 1$, we put $r_0 = q$, $r_1 = a$, $B_1 = 0$, and $B_2 = 1$. For $i \geq 2$ we let

$$\begin{aligned} r_i &= r_{i-2} \pmod{r_{i-1}}\ , \\ q_{i-1} &= r_{i-2} \ (\text{div } r_{i-1})\ , \\ B_{i+1} &= q_{i-1}B_i + B_{i-1}\ , \end{aligned}$$

until we find a minimal i such that $B_{i+1} > \sqrt{q}$. Then

$$(-1)^i r_{i-1} \equiv aB_i \pmod{q}$$

and

$$(a/q) = (B_i/q)(r_{i-1}/q)(-1/q)^i\ ,$$

where $B_i, r_{i-1} < \sqrt{q}$ (see [20]). It is now easy to verify that if $(a/q) = 1$, then

$$a \equiv \begin{cases} (G(r_{i-1})H(B_i))^2 \pmod{q} & \text{if } 2 \mid i \\ (\lambda G(r_{i-1})H(B_i))^2 \pmod{q} & \text{otherwise}\ . \end{cases}$$

Thus, once B_i and r_{i-1} have been found, (a/q) can be easily determined and, if $(a/q) = 1$, then $\sqrt{a} \pmod{q}$, can be computed simply by table look-ups and multiplication modulo q. It turns out that for large values of q, this method speeds up our algorithm by about a factor of 2. For example, to prove that $s = 912$ is a generator for $q = 141184027$ with the new method took only 2 hours, 6 minutes and 3 seconds, on the same machine as before.

We made a special effort to find values of q for which $s = 108$ and $s = 290$ are generators. This was without success – we only found that $s = 108$ and $s = 290$ are not generators for any prime $q < 10^{10}$. Moreover, because of Theorem 3.4 we also tried to find other values of q for which $s = 1$ is a generator. We found that 1 is a generator for $3, 7, 23, 19207$ and no other prime $< 2.1 \cdot 10^9$.

While for most of the primes q we can determine very rapidly that a given s is not a generator for q, once in a while we run into a value for q which requires much more effort. For example, for $s = 1$ and $q = 1523053897$, the least positive x such that the component beginning with x ends in a cycle that does not contain the zero node is $x = 2765848$; this component consists of 962 elements, and the corresponding cycle length is 26. On a SPARC Ultra-60, it took 14 days, 16 hours and 35 minutes to find this value of x. To determine that s is not a generator for q by considering the sets $\mathcal{R}_i$, we have to compute $\mathcal{R}_i$ up to $i = 121092$ (i.e., $\mathcal{R}_{121093}$ is the first set that is empty) until we find that the component that contains the zero node consists of only $1523052733 = q - 1164$ elements. This computation took 1 day, 9 hours and 56 minutes on a SPARC Ultra-60.

In Table 4.6, we list for $s = 1$, $s = 108$ and $s = 290$ those primes $q > 10^9$ ($q < 2 \cdot 10^9$ for $s = 1$, and $q < 10^{10}$ for $s = 108, 290$) that have passed all tests described prior to Table 4.3, and for which all $x = 0, 1, \ldots, 10000$ end in a cycle that contains the zero node. The respective cycle lengths are indicated in the second column of Table 4.6. However, for all these primes we eventually found a second component: in the third column we give the least x that ends in a cycle that does not contain the zero node, while the last column shows the corresponding cycle length.

q	μ	x	μ_x
$s = 1$			
1055114873	2	53870	70
1121788583	2	12934	278
1307586407	2	11064	41
1523053897	2	2765848	26
$s = 108$			
1361042663	35227	99379	7
3323409469	130529	130529	905
3570912959	28182	1574734	24
3945934931	79534	694699	13
5626917623	159574	47016	373
$s = 290$			
1492251769	78613	69682	123
2258948569	97638	18895	1198
2262261047	26405	62921	18
3870012343	153977	190103	24657
4696002397	19510	29918	350
5824284551	42637	37610	499
7865621479	98782	42567	379
8273290073	174261	1627204	44

TABLE 4.6.

Another exceptional pair (s, q) is given by $s = 545$ and $q = 16251619$: Here, we find that the component that ends in a cycle with the zero node consists of $q - 12$ elements, while there is a second component that consists of 12 elements and ends in a cycle of length 5. The least positive number x that belongs to that second component is $x = 4048245$.

REFERENCES

1. E. Bach, *Toward a theory of Pollard's rho method*, Information and Computation **90** (1991), 139–155.
2. E. Bach and J. O. Shallit, *Algorithmic number theory*, vol. Vol. 1, MIT Press, 1996.

3. P. Barrucand and H. Cohn, *A note on primes of type $x^2 + 32y^2$, class number and residuacity*, J. Reine Angew. Math. **238** (1969), 67–70.
4. P. T. Bateman and R. Horn, *Primes represented by irreducible polynomials in one variable*, Proc. Sympos. Pure Math., Vol VIII (Providence), AMS, 1965, pp. 119–132.
5. E. Dickson, *History of the theory of numbers*, vol. 1, Chelsea, New York, 1952.
6. E. B. Escott, *Cubic congruences with three real roots*, Annals of Math. **11** (1909-10), no. 2, 86–92.
7. P. Flajolet and A. M. Odlyzko, *Random mapping statistics*, Advances in Cryptology - EUROCRYPT '89, LNCS, vol. 434, 1990, pp. 329–354.
8. T. Forbes, *Prime clusters and Cunningham chains*, Math. Comp. **68** (1999), no. 228, 1739–1747.
9. R. K. Guy, *Unsolved problems in number theory*, second edition ed., Springer-Verlag, Berlin, 1994.
10. G. H. Hardy and J. E. Littlewood, *Some problems of partitio numerorum. III. On the expression of a number as a sum of primes*, Acta Math. **44** (1923), 1–70.
11. LiDIA Group, Technische Universität Darmstadt, Darmstadt, Germany, *LiDIA - a library for computational number theory, version 1.3*, 1997.
12. P. Morton, *Arithmetic properties of periodic points of quadratic maps*, Acta Arithmetica **62** (1992), 343–372.
13. ———, *Arithmetic properties of periodic points of quadratic maps II*, Acta Arithmetica **87** (1998), 89–102.
14. W. Narkiewicz, *Polynomial cycles in algebraic number fields*, Colloq. Math. **58** (1989), 151–155.
15. J. M. Pollard, *A Monte Carlo method for factorization*, BIT **15** (1975), no. 3, 331–335.
16. A. Schinzel and W. Sierpiński, *Sur certaines hypothèses concernant les nombres premiers*, Acta Arith. **4** (1958), 185–208.
17. ———, *Remarks on the paper "Sur certaines hypothèses concernant les nombres premiers"*, Acta Arith. **7** (1961), 1–8.
18. D. Shanks, Letter to D.H. and Emma Lehmer, June 10, 1969.
19. ———, *Supplemental data and remarks concerning a Hardy-Littlewood conjecture*, Math. Comp. **17** (1963), 188–193.
20. A. Stein and H. Williams, *An improved method of computing the regulator of a real quadratic function field*, Algorithmic Number Theory Seminar ANTS-III, Lecture Notes in Computer Science, vol. 1423, Springer-Verlag, 1998, pp. 607–620.
21. H. C. Williams and R. Holte, *Computation of the solution of $x^3 + dy^3 = 1$*, Math. Comp. **31** (1977), 778–785.

Dept. of Combinatorics and Optimization, University of Waterloo, Waterloo, ON N2L 3G1, Canada

Dept. of Computer Science, University of Manitoba, Winnipeg, MB R3T 2N2, Canada