On the iteration of certain quadratic maps over $GF(p)$

Troy Vasiga,Jeffrey Shallit [1]

School of Computer Science, University of Waterloo, Waterloo, ON, N2L 3G1, Canada

Abstract

We consider the properties of certain graphs based on iteration of the quadratic maps $x \to x^2$ and $x \to x^2 - 2$ over a finite field $GF(p)$.

Key words: Discrete iteration; Quadratic map; Finite field; Mersenne prime; Fermat prime; functional digraph.

1 Introduction

Let S be a finite set, and let $f : S \to S$ be a function. We can iterate f as follows: define $f^0(x) = x$ and $f^i(x) = f(f^{i-1}(x))$ for $i \geq 1$. We now define a directed graph $G_f = (\mathcal{V}, \mathcal{E})$ whose vertices are given by the elements of S and whose directed edges are $(x, f(x))$ for each $x \in S$. (The graph G_f is sometimes called a *functional digraph.*) A natural question is the following: what is the topology of G_f?

We may also pick a particular $x \in S$ and focus on the *orbit* of x (the directed path in G_f beginning at x). Since S is finite, for each x there exists a least positive integer $s = s(x)$ such that $f^s(x) \in \{f^0(x), f^1(x), \ldots, f^{s-1}(x)\}$. Let $t = t(x)$ be the least non-negative integer such that $f^s(x) = f^t(x)$. Setting $c = c(x) = s(x) - t(x)$, we have $f^t(x) = f^{t+c}(x)$. We call the list of elements $x, f(x), f^2(x), \ldots, f^{t-1}(x)$ the *tail* and $f^t(x), \ldots, f^{t+c-1}(x)$ the *cycle*. See Figure 1.

Email addresses: `tmjvasiga@cs.uwaterloo.ca` (Troy Vasiga), `shallit@graceland.uwaterloo.ca` (Jeffrey Shallit).
URLs: `http://www.cs.uwaterloo.ca/~tmjvasiga` (Troy Vasiga), `http://www.math.uwaterloo.ca/~shallit` (Jeffrey Shallit).

[1] Research supported in part by a grant from NSERC.

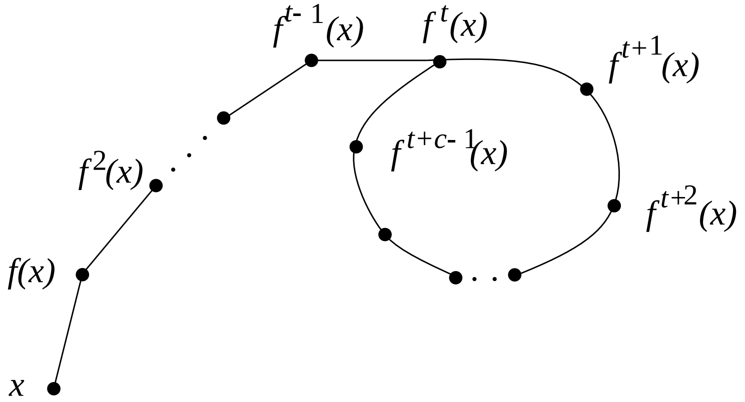

Fig. 1. The tail and cycle of an iteration

Other natural questions are as follows: what are the average values of $t(x)$ and $c(x)$ over all elements $x \in S$? How many distinct cycles are there? What is their average size? What is the average tail length?

In this paper, we discuss these questions where p is an odd prime number, $S = GF(p)$ (the finite field with p elements), and f is a quadratic map of the form $x \to x^2 + a$, $a \in \{0, -2\}$. Motivation for studying this case comes, in part, from four areas of algorithmic number theory.

First, the properties of the iteration $h : x \to x^2 - 2$ form the basis for the Lucas-Lehmer test for primality of Mersenne numbers, that is, numbers of the form $M_q := 2^q - 1$, where q is a prime [17,14]. As is well known, if q is an odd prime then $2^q - 1$ is prime if and only if $h^{q-2}(4) \equiv 0 \pmod{2^q - 1}$. Similarly, the properties of the iteration $g : x \to x^2$ form the basis of Pepin's test for primality of Fermat numbers (numbers of the form $F_k := 2^{2^k} + 1$) [21]: F_k is a prime iff $g^{2^k-1}(5) \equiv -1 \pmod{F_k}$. (Actually, any non-residue, such as 3, would work in place of 5.)

Second, Pollard's integer factoring algorithm is based on the iteration $f : x \to x^2 + a$ for a randomly-chosen a [22,6]. Pollard cautions "x^2 and $x^2 - 2$ should not be used (whatever the starting value x_0), the latter for reasons connected with its appearance in the Lucas-Lehmer test for primality of the Mersenne numbers". Our analysis gives a quantitative interpretation of Pollard's warning; see Section 4.

Third, the topology of the functional digraph of quadratic maps is related to Shanks' chains of primes, as recently investigated by Teske and Williams [24].

Finally, the iteration $x \to x^2$ modulo composite numbers is an integral part of modern pseudo-random bit generation, as discussed, for example, in Blum, Blum, and Shub [4].

2 The iteration $x \to x^2 \pmod p$

Although our main results concern the iteration $x \to x^2 - 2 \pmod p$, we start by reviewing the somewhat simpler case $x \to x^2 \pmod p$. Although our techniques are not new, the results of Theorems 6 (e), 9 and 10, for example, do appear to be new.

We use the following notation. If H is a multiplicative group and $x \in H$, then by $\text{ord}_H\ x$ we mean the least positive integer i such that $x^i = 1$. In the case that $H = (\mathbb{Z}/(n))^*$, the group of invertible elements modulo n, we write $\text{ord}_n\ x$.

If p is a prime, and n is an integer, then by $\nu_p(n)$ we mean the exponent of the largest power of p which divides n. We define $\nu_p(0) = +\infty$. One identity we will make use of frequently is $\sum_{d\,|\,n} \varphi(d) = n$, where φ is the Euler-φ function.

We will be dealing with certain directed graphs. A *complete binary tree of height* h, denoted B_h, is a directed graph with 2^i nodes at depth i, for $0 \le i \le h$, with the property that every non-leaf node has exactly two children. The graph B_h contains $2^{h+1} - 1$ nodes in total. If $G = (\mathcal{V}, \mathcal{E})$ is a directed graph, then by G^R we mean the graph $(\mathcal{V}, \mathcal{E}^R)$, where

$$\mathcal{E}^R := \{(x, y) \ : \ (y, x) \in \mathcal{E}\}.$$

We call G^R the *reversed graph.*

Theorem 1 *Let p be an odd prime, and let $S = GF(p)^*$ and $g : x \to x^2$. If $t(x)$ is the length of the tail for the element x, and $c(x)$ is the length of the cycle for x, as defined above, then $t(x) = \nu_2(\text{ord}_p\ x)$ and $c(x) = \text{ord}_l\ 2$, where $\text{ord}_p\ x = 2^e \cdot l$ and e, l are non-negative integers with l odd.*

Proof. If $g^t(x) = g^{t+c}(x)$, then we have $x^{2^t} \equiv x^{2^{t+c}} \pmod p$. Hence for $x \neq 0$ we have $x^{2^t(2^c-1)} \equiv 1 \pmod p$. Suppose $\text{ord}_p\ x = 2^e \cdot l$, where e, l are non-negative integers with l odd. Then we have $2^e \cdot l \,|\, 2^t(2^c - 1)$. By the definition of c and t it now follows that $e = t = \nu_2(\text{ord}_p\ x)$, and furthermore that c is the least positive integer such that $2^c \equiv 1 \pmod l$. In other words, $c = \text{ord}_l\ 2$.

We can characterize the tails of elements in terms of primitive roots, as follows:

Theorem 2 *Let p be an odd prime, and let γ be a primitive root mod p. Then*

(a) $\{a \in GF(p)^* \ : \ t(a) = 0\} = \{\gamma^i \ : \ 0 \le i < p$ *and* $\nu_2(i) \ge \nu_2(p-1)\}$;

(b) For $1 \leq k \leq \nu_2(p-1)$ we have

$$\{a \in GF(p)^* \ : \ t(a) = k\} = \{\gamma^i \ : \ 0 \leq i < p \text{ and } \nu_2(i) = \nu_2(p-1) - k\}.$$

Proof. Suppose $a = \gamma^i$ and $p - 1 = 2^\tau \cdot \rho$, where ρ is odd.

(a) We have $t(a) = 0$ iff there exists $l > 0$ such that $a = a^{2^l}$. But $a = a^{2^l}$ iff $a^{2^l - 1} = 1$, iff $\gamma^{i(2^l-1)} = 1$, iff $p - 1 \,|\, i(2^l - 1)$, iff $\nu_2(i) \geq \tau$ and $\rho \,|\, i(2^l - 1)$. Thus $t(a) = 0$ iff $\nu_2(i) \geq \nu_2(p-1)$ and there exists $l \geq 1$ such that $\rho \,|\, i(2^l - 1)$. But for all odd $\rho \geq 1$ there exists an $l \geq 1$ with $\rho \,|\, 2^l - 1$: we may take $l = \mathrm{ord}_p\, 2$. Since $\tau = \nu_2(p-1)$, the result follows.

(b) We have $t(a) = k$, $k \geq 1$, iff there exists $l > 0$ such that $a^{2^k} = a^{2^{k+l}}$ and $a^{2^{k-1}} \neq a^{2^{k+l-1}}$. As above, the last two relations hold iff $\gamma^{i2^k(2^l-1)} = 1$ and $\gamma^{i2^{k-1}(2^l-1)} \neq 1$, iff $p-1 \,|\, i2^k(2^l-1)$ and $p-1 \nmid i2^{k-1}(2^l-1)$, iff $2^\tau \,|\, i2^k$, $2^\tau \nmid i2^{k-1}$, and $\rho \,|\, i(2^l - 1)$. It follows that $t(a) = k$ iff $\nu_2(\tau) = \nu_2(i2^k)$, and the desired result follows.

It follows that, in general, the topology of the functional digraph $G_{x \to x^2}$ can be described as follows:

Corollary 3 *Let p be an odd prime with $p-1 = 2^\tau \cdot \rho$, ρ odd. For each positive integer divisor d of ρ, $G_{x\to x^2}$ contains $\varphi(d)/(\mathrm{ord}_d\, 2)$ cycles of length $\mathrm{ord}_d\, 2$. There are ρ elements in all these cycles, and off each element in these cycles there hang reversed complete binary trees of height $\tau - 1$ containing $2^\tau - 1$ elements.*

Proof. Let γ be a primitive root, mod p. The elements x in the cycles are precisely those for which $t(x) = 0$, and by Theorem 2 they are of the form $\gamma^{j \cdot 2^\tau}$, $0 \leq j < \rho$. Hence there are ρ elements in all cycles. These elements form a cyclic group of order ρ, and hence there are $\varphi(d)$ elements of order d for each divisor d of ρ. The elements of order d are given by $\gamma^{j2^\tau\rho/d}$ for $0 \leq j < d$, $\gcd(j, d) = 1$. The length of the cycle for $\gamma^{j2^\tau\rho/d}$ is the least c for which $\frac{j}{d}(2^c - 1)$ is an integer; in other words, $\mathrm{ord}_d\, 2$. It follows that there are $\varphi(d)/(\mathrm{ord}_d\, 2)$ cycles corresponding to these elements.

Finally, the elements with tail size 1 whose square gives $\gamma^{j\cdot 2^\tau}$ are those of the form $\gamma^{j \cdot 2^{\tau-1}}$. In general, if γ^i is an element with tail size $1 \leq t < \tau$, the corresponding elements with tail size $t+1$ are $\gamma^{i/2}$ and $\gamma^{(i+p-1)/2}$. These are distinct since $\gamma^{(p-1)/2} = -1$.

As an example, let us consider the case $p = 29$, where $\tau = 2$ and $\rho = 7$. See Figure 2.

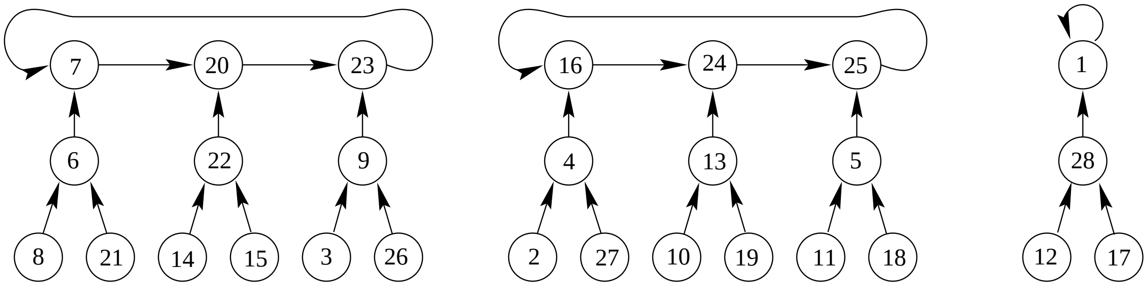

Fig. 2. The topology of $G_{x\to x^2}$ for $p=29$

We can enumerate the number of elements in $GF(p)^*$ that have a given cycle structure, as follows: for each divisor d of $p-1$ there are exactly $\varphi(d)$ elements of $GF(p)^*$ of order d. From above, the tail length for each such element is $t=\nu_2(d)$ and the cycle length is of size $\mathrm{ord}_{d/2^{\nu_2(d)}}\,2$. For example, for $p=29$ we have the data in Table 1.

d	$\varphi(d)$	elements of order d	$t=\nu_2(d)$	$l=d/2^t$	$c=\mathrm{ord}_l\ 2$
1	1	$\{1\}$	0	1	1
2	1	$\{28\}$	1	1	1
4	2	$\{12,17\}$	2	1	1
7	6	$\{7,16,20,23,24,25\}$	0	7	3
14	6	$\{4,5,6,9,13,22\}$	1	7	3
28	12	$\{2,3,8,10,11,14,15,18,19,21,26,27\}$	2	7	3

Table 1: The structure of $G_{x\to x^2}$ for $p=29$.

There are two special cases where we can give more details about the structure and properties of $G_{x\to x^2}$. The first is when $p=2^{2^k}+1$, a Fermat prime.

Theorem 4 *The structure of the digraph $G_{x\to x^2}$ for prime p when $p=2^{2^k}+1$, a Fermat prime, is a reversed complete binary tree of height 2^k-1 with root -1, attached to a cycle of length 1 on the integer 1. The elements x with $t(x)=a$ for $0\le a\le 2^k$ are given by $3^{e\cdot 2^{2^k-a}}$, $0\le e<2^a$, e odd.*

Proof. We use Theorem 2 and Corollary 3. The only odd divisor of $p-1$ is 1, and it is well-known and easily proved that 3 is a primitive root of $p=2^{2^k}+1$ when p is prime and $k\ge 1$.

Figure 3 illustrates this construction when $k = 2$, $p = 17$.

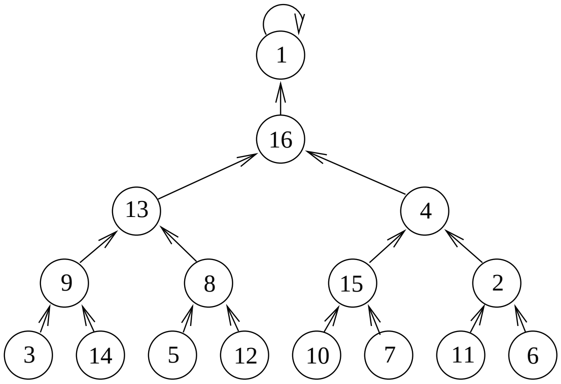

Fig. 3. The topology of $G_{x\rightarrow x^2}$ for $p = 17$

The second case where we can give a more complete description is when $p = 2^q - 1$, a Mersenne prime.

Theorem 5 *When $p = 2^q - 1$, a Mersenne prime, the digraph $G_{x\rightarrow x^2}$ consists of cycles whose length divides $q - 1$. Off each element in these cycles there hangs a single element with tail length* 1*.*

Proof. We have $p - 1 = 2(2^{q-1} - 1)$, so $\tau = 1$ and $\rho = 2^{q-1} - 1$. It follows that the divisors of $p - 1$ are of the form $2^f j$, where $j \mid 2^{q-1} - 1$ and $f \in \{0, 1\}$. The cycle length for any element is therefore given by $\operatorname{ord}_j 2$ for some j a divisor of $2^{q-1} - 1$. Now $\operatorname{ord}_j 2 \mid q - 1$, and so the cycle length for every element is a divisor of $q - 1 \approx \log_2 p$.

The result of Theorem 5 can be contrasted with the average cycle length of $\approx \sqrt{p}$ in the case of a random map [12].

Figure 4 illustrates Theorem 5 in the case where $q = 5$, $p = 31$.

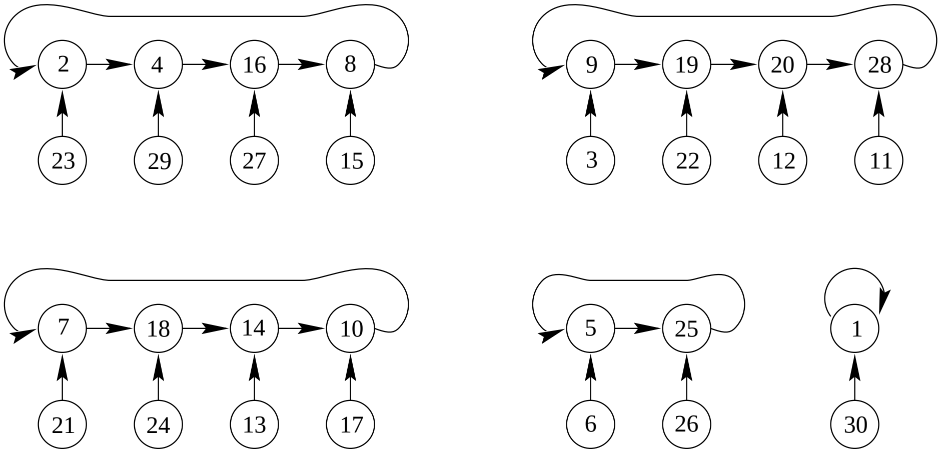

Fig. 4. The topology of $G_{x \to x^2}$ for $p = 31$

We now consider some statistics about the tail and cycle lengths for a given prime p. We write $t_p(x)$ for the length of the tail in the orbit of x under this iteration, and $c_p(x)$ for the length of the cycle in the orbit of x.

Definitions.

With respect to the iteration $x \to x^2 \pmod{p}$, we define:

- $TC(p) :=$ total number of cycles;
- $T_0(p) :=$ total number of elements in all cycles, i.e., the number of $a \in GF(p)^*$ with $t(a) = 0$;
- $AC(p) :=$ average length of a cycle;
- $C(p) :=$ average value of $c_p(a)$ over all $a \in GF(p)^*$;
- $T(p) :=$ average value of $t_p(a)$ over all $a \in GF(p)^*$.

For example, $TC(29) = 3$, $T_0(29) = 7$, $AC(29) = 7/3$, $C(29) = 19/7$, and $T(29) = 5/4$. The following theorem gives formulas for these quantities.

Theorem 6 *Let $p - 1 = 2^\tau \cdot \rho$ with ρ odd. With respect to the iteration $x \to x^2 \pmod{p}$ we have*

(a) $TC(p) = \sum_{d \,|\, \rho} \frac{\varphi(d)}{\mathrm{ord}_d\ 2}$*;*
(b) $T_0(p) = \rho$*;*
(c) $AC(p) = \frac{\rho}{TC(p)}$*;*
(d) $C(p) = \frac{1}{\rho} \sum_{d \,|\, \rho} \varphi(d) \mathrm{ord}_d\ 2$*;*
(e) $T(p) = \frac{1}{p-1} \sum_{d \,|\, p-1} \varphi(d) \nu_2(d) = \tau - 1 + 2^{-\tau}$*.*

Proof. Parts (a)-(d) follow directly from Corollary 3. For part (e) we have

$$
\begin{aligned}
T(p) &= \frac{1}{p-1}\sum_{1\le a\le p-1} t_p(a)\\
&= \frac{1}{p-1}\sum_{d\,|\,p-1} \varphi(d)\nu_2(d)\\
&= \frac{1}{p-1}\sum_{d\,|\,\rho}\sum_{0\le i\le\tau} \varphi(d\cdot 2^i)\nu_2(d\cdot 2^i)\\
&= \frac{1}{p-1}\sum_{d\,|\,\rho}\varphi(d)\sum_{1\le i\le\tau} \varphi(2^i)\cdot i\\
&= \frac{1}{p-1}\sum_{d\,|\,\rho}\varphi(d)\sum_{1\le i\le\tau} i\cdot 2^{i-1}\\
&= \frac{1}{p-1}\sum_{d\,|\,\rho}\varphi(d)((\tau-1)2^\tau+1)\\
&= \frac{1}{p-1}\rho((\tau-1)2^\tau+1)\\
&= \tau-1+2^{-\tau}.
\end{aligned}
$$

We now examine the average behavior of some of these quantities over all odd primes $p \le N$.

Definitions.

With respect to the iteration $x \to x^2 \pmod p$, we define

- $ST_0(N) := \sum_{2<p\le N} T_0(p)$;
- $ST(N) := \sum_{2<p\le N}\sum_{1\le a<p} t_p(a)$.

We can obtain good asymptotic estimates for these quantities, assuming the Extended Riemann Hypothesis (ERH).

First some basic definitions. Let $\pi(x,l,k)$ denote the number of primes $\le x$ which are congruent to $k \pmod l$. We define asymptotic bounds on functions in the standard way: see, for example Lewis and Denenberg [15]. Let f, g be functions from non-negative real numbers to non-negative real numbers. We say $f = O(g)$ if there exist constants $c > 0$ and $n_0 \ge 0$ such that $f(n) \le cg(n)$ for all $n \ge n_0$. For lower bounds, we use the notation $f = \Omega(g)$ to indicate that there exist constants $c > 0$ and $n_0 \ge 0$ such that $f(n) \ge cg(n)$ for all $n \ge n_0$. We say that $f = \Theta(g)$ if $f = O(g)$ and $f = \Omega(g)$.

Next, we need the following lemmas.

Lemma 7 *Assume the ERH. Then, if the logarithmic integral* $\mathrm{li}(x)$ *is defined* *by* $\mathrm{li}(x) = \int_2^x \frac{1}{\log t} dt$ *and if* $\gcd(k,l) = 1$ *then*

$$\pi(x,l,k) = \frac{\mathrm{li}(x)}{\varphi(l)} + O(\sqrt{x}(\log x + 2\log l)).$$

Proof. See, for example, [1, pp. 217, 235].

It should be noted that without the assumption of the ERH, we would not have a polynomial bound on the O term. Specifically, without the ERH, we would have (using results from [1, p. 215]) that there is a constant $c > 0$ such that if $\gcd(k,l) = 1$ then

$$\pi(x,l,k) = \frac{\mathrm{li}(x)}{\varphi(l)} + O(xe^{-c(\log x)^{3/5}(\log\log x)^{-1/5}}).$$

This bound is not strong enough for our purposes. Therefore, we assume the ERH and use the tighter bound in our analysis.

Lemma 8 *Assume the ERH. Let* k, l *be integers with* $\gcd(k,l) = 1$*. Then*

$$\sum_{\substack{p \le x \\ p \equiv k \pmod{l}}} p = \frac{1}{\varphi(l)} \left(\frac{x^2}{2\log x}\right) \left(1 + O(\frac{1}{\log x})\right) + O(x^{3/2}(\log x + 2\log l)).$$

Proof. By Lemma 7 we have

$$\pi(x,l,k) = \frac{\mathrm{li}(x)}{\varphi(l)} + O(\sqrt{x}(\log x + 2\log l)).$$

Now, by Stieltjes integration (see, e.g., [1, pp. 28-29]), we have

$$\sum_{\substack{p \le x \\ p \equiv k \pmod{l}}} p = \frac{1}{\varphi(l)} \int_2^x \frac{t}{\log t} dt + O(x^{3/2}(\log x + 2\log l)). \tag{1}$$

On the other hand, by asymptotic integration (see, e.g., [1, pp. 27-28]), we have

$$\int_2^x \frac{t}{\log t} dt = \frac{x^2}{2\log x} + O\left(\frac{x^2}{(\log x)^2}\right). \tag{2}$$

The result comes from combining Eqs. (1) and (2).

Now we are ready to estimate $ST_0(N)$.

Theorem 9 *Assume the ERH. Then* $ST_0(N) \sim \frac{N^2}{6\log N}$.

Proof. We have, using Lemma 8, that

$$\begin{aligned}\sum_{p\leq N}\frac{p-1}{2^{\nu_2(p-1)}} &= \sum_{1\leq i\leq\log_2 N}\ \sum_{\substack{p\leq N\\ p\equiv 2^i+1 \pmod{2^{i+1}}}}\frac{p-1}{2^i}\\ &= \frac{N^2}{2\log N}(1+O(\frac{1}{\log N}))\sum_{1\leq i\leq\log_2 N}\frac{1}{4^i}\\ &= \frac{N^2}{2\log N}(1+O(\frac{1}{\log N}))\frac{1}{3}(1+O(\frac{1}{N})).\end{aligned}$$

We now turn to $ST(N)$.

Theorem 10 *Assume the ERH. Then*

$$ST(N) \sim \frac{2}{3}\cdot\frac{N^2}{\log N}.$$

Proof. We have

$$\begin{aligned}\sum_{p\leq N}\sum_{1\leq x\leq p-1}t_p(x) &= \sum_{p\leq N}(p-1)(\nu_2(p-1)-1+2^{-\nu_2(p-1)})\\ &= \sum_{p\leq N}\nu_2(p-1)p-\sum_{p\leq N}\nu_2(p-1)-\sum_{p\leq N}p+\sum_{p\leq N}1+\sum_{p\leq N}\frac{p-1}{2^{\nu_2(p-1)}}.\end{aligned}$$

We start by evaluating $\sum_{p\leq N}\nu_2(p-1)p$. We have

$$\begin{aligned}\sum_{p\leq N}\nu_2(p-1)p &= \sum_{1\leq i\leq\log_2 N}\ \sum_{\substack{p\leq N\\ p\equiv 1 \pmod{2^i}}}p\\ &= \frac{N^2}{\log N}\left(1+O(\frac{1}{\log N})\right)\left(1+O(\frac{1}{N})\right),\end{aligned}$$

where we have used Lemma 8.

Next we have, using Lemma 7, that

$$\begin{aligned}\sum_{p\leq N} \nu_2(p-1) &= \sum_{1\leq i\leq \log_2 N} \pi(N, 2^i, 1)\\ &= \sum_{1\leq i\leq \log_2 N} \left(\frac{\mathrm{li}(N)}{2^{i-1}} + O(\sqrt{N}\log N)\right)\\ &= \mathrm{li}(N)(2 + O(\frac{1}{N})) + O(\sqrt{N}(\log N)^2),\end{aligned}$$

It is well known that $\sum_{p\leq N} p \sim \frac{N^2}{2\log N}$; see, for example, [1, p. 28-29].

By the prime number theorem, $\sum_{p\leq N} 1 \sim \frac{N}{\log N}$.

Putting all these estimates together with Theorem 9, and the well-known estimate $\mathrm{li}(x) = \frac{x}{\log x}(1 + O(\frac{1}{\log x}))$, we obtain the desired result.

We now compare the estimates in Theorem 9 and 10 with empirical data:

N	$ST_0(N)$	$N^2/(6\log N)$	$ST(N)$	$2N^2/(3\log N)$
10	5	7.24	9	28.95
10^2	342	361.91	1366	1447.65
10^3	25875	24127.47	99383	96509.88
10^4	1922532	1809560.34	7481452	7238241.36
10^5	151468221	144764827.30	605859857	579059309.20
10^6	12531875547	12063735608.42	49994218943	48254942433.69

Table 2: Comparing $ST_0(N)$ and $ST(N)$ to asymptotic estimates

It is harder to estimate the average behavior of $c_p(x)$. A reasonable conjecture is that there are infinitely many primes p such that (a) $p' := (p-1)/2$ is also prime and (b) 2 is a primitive root (mod p'). The first few such primes are

$$7, 11, 23, 59, 107, 167, 263, 347, 359, 587, 839, 887, 983, 1019, 1307, 1319, 2039, 2459,$$
$$2903, 2999, 3467, 3803, 3863, 3947, 4139, 4283, 4679, \cdots$$

For these primes p we have

$$\sum_{1\leq a<p} c_p(a) = 2\sum_{d\,|\,(p-1)/2} \varphi(d)\mathrm{ord}_d\, 2 = 2(1 + (p'-1)(p'-1)) = \Omega(p^2).$$

If p is a Fermat prime, then $p-1 = 2^{2^k}$ for some k. Using Theorem 6, we have

$\rho = 1$ and so

$$\sum_{1 \leq a < p} c_p(a) = \frac{p-1}{\rho} \sum_{d \mid \rho} \varphi(d) \text{ord}_d\ 2 = 2^{2^k} = p - 1.$$

However, few believe there are infinitely many Fermat primes.

If p is a Mersenne prime, say $p = 2^q - 1$, then

$$\sum_{1 \leq a < p} c_p(a) \leq (q-1)(2^{q-1} - 1) = O(p \log p).$$

Most people believe there are infinitely many Mersenne primes, but of course no proof currently exists.

Assuming a conjecture of Wagstaff [25] on the distribution of the least prime in an arithmetic progression, we now show there are infinitely many primes p for which

$$\sum_{1 \leq a < p} c_p(a) = O(p (\log p)^2).$$

To observe this, for each integer $\tau \geq 1$ consider the least prime p with $p \equiv 1 \pmod{2^\tau}$. Now write

$$p - 1 = 2^{\tau + c} \cdot \rho \tag{3}$$

for some non-negative integer c and odd integer ρ. Then $\varphi(p) = p - 1 = 2^{\tau+c} \cdot \rho$. Wagstaff's conjecture states that the least prime $p \equiv a \pmod{n}$, when $\gcd(a, n) = 1$, is $O(\varphi(n)(\log n)(\log \varphi(n)))$. Letting $n = 2^\tau$, we find

$$\begin{aligned} p &= O(\varphi(2^\tau)(\log 2^\tau)(\log \varphi(2^\tau))) \\ &= O(2^{\tau-1}\tau(\log 2)(\tau - 1)(\log 2)) \\ &= O(\tau^2 2^\tau). \end{aligned}$$

Dividing this last result by (3), we get $\rho = O(\tau^2)$. Also, $p = O(\tau^2 2^\tau)$ gives $\tau = \Theta(\log p)$.

Using Theorem 6, we have

$$\begin{aligned} \sum_{1 \leq a < p} c_p(a) &= \frac{p-1}{\rho} \sum_{d \mid \rho} \varphi(d) \text{ord}_d\ 2 \\ &= 2^{\tau+c} \sum_{d \mid \rho} \varphi(d) \text{ord}_d\ 2 \\ &\leq 2^{\tau+c} \cdot \rho \sum_{d \mid \rho} \varphi(d) \\ &= 2^{\tau+c} \cdot \rho^2 \\ &= O(\rho p). \end{aligned}$$

Combining this result with the previous fact that $\rho = O(\tau^2) = O((\log p)^2)$, we have

$$\sum_{1 \le a < p} c_p(a) = O(p(\log p)^2),$$

as desired.

The properties of the iteration $x \to x^2 \pmod{p}$ have received some previous attention. Chassé [7–9] proved some basic results regarding the cycle length of iterations of the form $x \to x^2 + d$. Blanton, Hurd, and McCranie [2,3] also investigated this iteration. They proved our Theorem 1, Corollary 3, and Theorem 6 (a). Rogers [23] independently discussed this iteration and obtained Corollary 3 and Theorem 6 (a). Flores [10], in a brief expository paper, observed Theorem 4.

Lucheta, Miller, and Reiter [18] performed a similar analysis for the iteration $x \to x^k$ modulo a prime, and Wilson [26] and Brennan and Geist [5] discussed this iteration modulo an arbitrary integer. The iteration $x \to x^k$ over the p-adic numbers was discussed by Khrennikov and Nilsson [13].

3 The iteration $x \to x^2 - 2 \pmod{p}$

Rogers [23] stated,

> "The family of nonlinear maps given by $f(x) = x^2 + c,\ c \in \mathbb{F}_p$, for nonzero values of the parameter $c \in \mathbb{F}_p$, produces graphs whose tree structure (graphically, the transients leading down to the cycles) seems beyond description; in general the trees attached to the cycles are of variable height, and even those trees attached to the same cycle vary."

However, as we will see in this section, Rogers' statement is not true for $c = -2$, whose special character was previously recognized by Pollard [22].

In this section we determine the properties of the iteration $h : x \to x^2 - 2 \pmod{p}$.

It is worth noting that Dickson polynomials (see Lidl, Mullen and Turnwald [16]) can be used to describe this iteration. In particular, Dickson polynomials (of the first kind) can be defined recursively as follows:

$$\begin{aligned} D_0(x,a) &= 2, \\ D_1(x,a) &= x, \\ D_n(x,a) &= xD_{n-1}(x,a) - aD_{n-2}(x,a), \qquad \text{for } n \ge 2. \end{aligned}$$

where x is an indeterminate and a is an element from a commutative ring. From this, one can derive that $h^n(x) = D_{2^n}(x, 1)$. Moreover, Dickson polynomials with $a = 1$ have been studied to some depth [19], but, as Lidl, Mullen and Turnwald [16, p. 90] point out,

> The computations and arguments for determining the fixed point formulas for the cases $a = 1$ and $a = -1$ are quite detailed and lengthy (some twenty pages for each case)...

Our techniques can be used to obtain these results for the case of prime moduli. Furthermore, we obtain much more detailed results (e.g., Theorem 14 and Corollary 15).

More recently, Peinado, Montoya, Munõz and Yuste [20] have proven upper bounds on the cycle lengths for $x \to x^2 + c$ over $\mathbb{F}_q$, where q is a prime power. Additionally, Gilbert, Kolesar, Reiter, and Storey [11] obtained similar results, but in an ad hoc manner. One of our contributions is a general algebraic framework for understanding the iteration $x \to x^2 - 2$, which shows that it is quite analogous to the (well-understood) map $x \to x^2$.

Given $a \in GF(p)$, let us define the polynomial $u(X) = X^2 - aX + 1$. Let α and β be the roots of u in $GF(p^2)$. Note that $\alpha + \beta = a$ and $\alpha\beta = 1$.

Proposition 11 *We have $h^n(a) = \alpha^{2^n} + \beta^{2^n}$ for $n \geq 0$.*

Proof. By induction on n. For $n = 0$ we have $h^0(a) = a = \alpha + \beta$. Now assume the result is true for n; we prove it for $n + 1$. We have

$$\alpha^{2^{n+1}} + \beta^{2^{n+1}} = (\alpha^{2^n} + \beta^{2^n})^2 - 2\alpha^{2^n}\beta^{2^n} = h^n(a)^2 - 2.$$

Theorem 12 *Let $a \in GF(p)$, and suppose that iterating h, starting with a, results in a tail of length $t = t(a)$ and a cycle of length $c = c(a)$. Then t and c can be computed as follows. Let α and β be the roots of $u(X) = X^2 - aX + 1$ over $GF(p^2)$. Let $\operatorname{ord}_{GF(p^2)^*} \alpha = 2^e \cdot l$, where l is odd. Then $e = t$ and c is the least integer $i \geq 1$ such that $2^i \equiv \pm 1 \pmod{l}$.*

Proof. We have $h^{t+c}(a) = h^t(a)$ and $t \geq 0$, $c \geq 1$ are as small as possible. Then by Proposition 11 this is equivalent to

$$\alpha^{2^{t+c}} + \alpha^{-2^{t+c}} = \alpha^{2^t} + \alpha^{-2^t}.$$

This holds iff

$$\alpha^{2^{t+c+1}} + 1 = \alpha^{2^{t+c}+2^t} + \alpha^{2^{t+c}-2^t}$$

iff

$$(\alpha^{2^{t+c}} - \alpha^{2^t})(\alpha^{2^{t+c}} - \alpha^{-2^t}) = 0$$

iff $\alpha^{2^{t+c}} = \alpha^{2^t}$ or $\alpha^{2^{t+c}} = \alpha^{-2^t}$ iff $\alpha^{2^t(2^c-1)} = 1$ or $\alpha^{2^t(2^c+1)} = 1$. If $\mathrm{ord}_{GF(p^2)^*}\ \alpha = 2^e \cdot l$, where l is odd, then $2^e \cdot l \mid 2^t(2^c-1)$ or $2^e \cdot l \mid 2^t(2^c+1)$. The desired result now follows.

It follows that $c = \mathrm{ord}_l\ 2$ or $(\mathrm{ord}_l\ 2)/2$.

From the previous result we see that $t(a)$ and $c(a)$ depend on $\mathrm{ord}_{GF(p^2)^*}\ \alpha$, where α, β are the roots of $X^2 - aX + 1 = 0$. (Note that $\mathrm{ord}_{GF(p^2)^*}\ \alpha = \mathrm{ord}_{GF(p^2)^*}\ \beta$.) The following theorem characterizes these orders.

Theorem 13*(a) For each divisor d of $p-1$, $d \neq 1, 2$ there are $\varphi(d)/2$ elements $a \in GF(p)$ for which the corresponding α has* $\mathrm{ord}_{GF(p^2)^*}\ \alpha = d$*;*

(b) For each divisor d' of $p+1$, $d' \neq 1, 2$ there are $\varphi(d')/2$ elements $a \in GF(p)$ for which the corresponding α has $\mathrm{ord}_{GF(p^2)^*}\ \alpha = d'$*;*

(c) For $a = 2$ we have $\alpha = \beta = 1$ and $\mathrm{ord}_{GF(p^2)^*}\ \alpha = 1$*;*

(d) For $a = -2$ we have $\alpha = \beta = -1$ and $\mathrm{ord}_{GF(p^2)^*}\ \alpha = 2$.

Proof. Consider the polynomial $u(X) = X^2 - aX + 1$ over $GF(p)$. This polynomial is reducible if and only if it can be written in the form $(X - b)(X - b^{-1})$ where $a = b + b^{-1}$. By symmetry, this occurs for $(p+1)/2$ distinct values of a. The roots b, b^{-1} are identical iff $b^2 = 1$, that is, if $b = \pm 1$. For the remaining $(p-3)/2$ values of a the roots are distinct. This proves parts (a), (c), and (d).

Otherwise the polynomial $u(X)$ is irreducible over $GF(p)$ with distinct zeroes α, β. We claim that the equation

$$\theta^{p+1} = 1 \tag{4}$$

has $p+1$ roots in $GF(p^2)$: namely 1, -1, and the $p-1$ roots α, β of the irreducible $u(X)$. To see this, note that $\alpha^{p+1} = \alpha \cdot \alpha^p = \alpha\beta = 1$. Since the roots of Eq. (4) form a cyclic group, for each $d' \mid p+1$ there are $\varphi(d')$ roots of order d'. Now each a corresponding to an irreducible u has two roots, so there are $\varphi(d')/2$ different a's corresponding to α of order d'.

We now prove the analogue of Theorem 2.

Theorem 14 *Let p be an odd prime. Let δ be a generator for $GF(p^2)^*$ and define $\theta = \delta^{p-1}$, so that θ is a generator of the subgroup of $(p+1)$'th roots of unity in $GF(p^2)$. Let $\gamma = \delta^{p+1}$, so that γ generates $GF(p)^*$.*

If $p \equiv 1 \pmod 4$ then

(a)

$$\{a \in GF(p) \ : \ t(a) = 0\} = \{\theta^i + \theta^{-i} \ : \ 1 \le i \le (p-1)/2 \textit{ and } \nu_2(i) \ge \nu_2(p+1)\} \cup \{\gamma^j + \gamma^{-j} \ : \ 0 \le j \le (p-1)/2 \textit{ and } \nu_2(j) \ge \nu_2(p-1)\}; \quad (5)$$

(b) For $1 \le k \le \nu_2(p-1)$ *we have*

$$\{a \in GF(p) \ : \ t(a) = k\} = \{\theta^i + \theta^{-i} \ : \ 1 \le i \le (p-1)/2 \textit{ and } \nu_2(i) = \nu_2(p+1) - k\} \cup \{\gamma^j + \gamma^{-j} \ : \ 0 \le j \le (p-1)/2 \textit{ and } \nu_2(j) = \nu_2(p-1) - k\}. \quad (6)$$

If $p \equiv 3 \pmod 4$ *then*

(c)

$$\{a \in GF(p) \ : \ t(a) = 0\} = \{\theta^i + \theta^{-i} \ : \ 0 \le i \le (p+1)/2 \textit{ and } \nu_2(i) \ge \nu_2(p+1)\} \cup \{\gamma^j + \gamma^{-j} \ : \ 1 \le j \le (p-3)/2 \textit{ and } \nu_2(j) \ge \nu_2(p-1)\}; \quad (7)$$

(d) For $1 \le k \le \nu_2(p+1)$ *we have*

$$\{a \in GF(p) \ : \ t(a) = k\} = \{\theta^i + \theta^{-i} \ : \ 0 \le i \le (p+1)/2 \textit{ and } \nu_2(i) = \nu_2(p+1) - k\} \cup \{\gamma^j + \gamma^{-j} \ : \ 1 \le j \le (p-3)/2 \textit{ and } \nu_2(j) = \nu_2(p-1) - k\}. \quad (8)$$

Furthermore, all these unions are distinct.

Proof. We begin by proving case (a) and (b). For case (a), assume $p \equiv 1 \pmod 4$. Write $p + 1 = 2^{\tau'} \cdot \rho'$, where ρ' is odd. Note that $\tau' = 1$ since $p + 1 \equiv 2 \pmod 4$.

By Theorem 12 we have that

$$t(a) = 0 \text{ iff there exists } c \ge 1 \text{ such that } \alpha^{2^c - 1} = 1 \text{ or } \alpha^{2^c + 1} = 1, \quad (9)$$

where α is a zero of $u(X) = X^2 - aX + 1$. (Note: $a = \alpha + \alpha^{-1}$.) There are two cases to consider: (i) u is irreducible over $GF(p)$ or (ii) u is reducible.

(i) If u is irreducible, then $\alpha = \theta^i$ for some i with $1 \le i \le p$, $i \ne (p+1)/2$. (Note that $\theta^0 = \theta^{p+1} = 1$ and therefore $\theta^{(p+1)/2} = -1$.) Restating (9), we have $t(a) = 0$ iff there exists $c \ge 1$ such that $\theta^{i(2^c-1)} = 1$ or $\theta^{i(2^c+1)} = 1$, iff there exists $c \ge 1$ with $p + 1 \,|\, i(2^c - 1)$ or $p + 1 \,|\, i(2^c + 1)$, iff there exists $c \ge 1$ with $\nu_2(i) \ge \tau'$ and $\rho' \,|\, 2^c - 1$, or $\nu_2(i) \ge \tau'$ and $\rho' \,|\, 2^c + 1$. We know there does exist a c which satisfies the condition $\rho' \,|\, 2^c - 1$: that is, pick $c = \mathrm{ord}_{\rho'} 2$. Therefore, $t(a) = 0$ iff $a = \theta^i + \theta^{-i}$ for some i with $1 \le i \le p$, $i \ne (p+1)/2$, $\nu_2(i) \ge \tau'$. But $\theta^{p+1} = 1$, so $\theta^i + \theta^{-i} = \theta^{p+1-i} + \theta^{-(p+1-i)}$, so we may eliminate duplicates by dividing our range for i by one-half. To summarize this case, we have $t(a) = 0$ iff $a = \theta^i + \theta^{-i}$ with $1 \le i \le (p-1)/2$ and $\nu_2(i) \ge \nu_2(p+1)$.

(ii) If u is reducible, then $\alpha = \gamma^j$ for some j with $0 \leq j \leq p-2$. Write $p-1 = 2^\tau \cdot \rho$. From the proof of Theorem 12 we have $t(a) = 0$ iff there exists a $c \geq 1$ such that $\alpha^{2^c-1} = 1$ or $\alpha^{2^c+1} = 1$, iff $\gamma^{j(2^c-1)} = 1$ or $\gamma^{j(2^c+1)} = 1$, iff $2^\tau \cdot \rho \,|\, j(2^c-1)$ or $2^\tau \cdot \rho \,|\, j(2^c+1)$. That is, $t(a) = 0$ iff $\tau \leq \nu_2(j)$ and either $\rho \,|\, j(2^c-1)$ or $\rho \,|\, j(2^c+1)$. Again, as in the earlier case, we picking $c = \text{ord}_\rho\, 2$ yields $\rho \,|\, (2^c-1)$. As well, notice that $\gamma^{p-1} = 1$, so $\gamma^j + \gamma^{-j} = \gamma^{p-1-j} + \gamma^{-(p-1-j)}$, so we need only consider one-half of the range of possible values for j. Thus, $t(a) = 0$ iff $a = \gamma^j + \gamma^{-j}$ with $0 \leq j \leq (p-1)/2$ and $\nu_2(j) \geq \nu_2(p-1)$.

We now show that the quantities $\theta^i + \theta^{-i}$, $1 \leq i \leq (p-1)/2$ and $\gamma^j + \gamma^{-j}$, $0 \leq j \leq (p-1)/2$ are all distinct.

If $\theta^i + \theta^{-i} = \theta^{i'} + \theta^{-i'}$ for $1 \leq i, i' \leq (p-1)/2$ then it follows by simple algebra that $(\theta^{i+i'} - 1)(\theta^{i-i'} - 1) = 0$. Hence $\theta^{i+i'} = 1$ or $\theta^{i-i'} = 1$. Since $\text{ord}_{GF(p^2)^*}\, \theta = p+1$, it follows that $p+1 \,|\, (i+i')$ or $p+1 \,|\, (i-i')$. But $2 \leq i+i' \leq p-1$, so the first is impossible, while the second implies $i = i'$.

A similar argument applies if $\gamma^j + \gamma^{-j} = \gamma^{j'} + \gamma^{-j'}$.

Finally, suppose $\theta^i + \theta^{-i} = \gamma^j + \gamma^{-j}$ where $1 \leq i \leq (p-1)/2$ and $0 \leq j \leq (p-1)/2$. Now $\theta = \delta^{p-1}$ and $\gamma = \delta^{p+1}$, where δ is a generator for $GF(p^2)^*$. Hence it follows that

$$\delta^{(p-1)i} + \delta^{-(p-1)i} = \delta^{(p+1)j} + \delta^{-(p+1)j}.$$

Hence by simple algebra $(\delta^{(p-1)i+(p+1)j} - 1)(\delta^{(p-1)i-(p+1)j} - 1) = 0$. Hence $\delta^{(p-1)i+(p+1)j} = 1$ or $\delta^{(p-1)i-(p+1)j} = 1$. Since $\text{ord}_{GF(p^2)^*}\, \delta = p^2 - 1$, it follows that $p^2 - 1 \,|\, (p-1)i + (p+1)j$ or $p^2 - 1 \,|\, (p-1)i - (p+1)j$. Hence, since p is odd, we get that there exists k such that either

$$\frac{p-1}{2} i = -\frac{p+1}{2} j + k\frac{p^2-1}{2} \tag{10}$$

or

$$\frac{p-1}{2} i = \frac{p+1}{2} j + k\frac{p^2-1}{2}. \tag{11}$$

In both cases, $\frac{p+1}{2}$ divides both terms of the right-hand side, and hence must divide the left-hand side. But $\gcd(\frac{p-1}{2}, \frac{p+1}{2}) = 1$, so $\frac{p+1}{2} \,|\, i$, a contradiction. This concludes the proof of case (a).

Now let us look at case (b). By Theorem 12 we have

$$t(a) = k \text{ iff } \text{ord}_{GF(p^2)}\, \alpha = 2^k \cdot l, \tag{12}$$

where l is odd and α is a zero of $u(X) = X^2 - aX + 1$. Once again we break up the argument into two cases: (i) u is irreducible and (ii) u is reducible.

(i) If u is irreducible, then $\alpha = \theta^i$, for some i with $1 \leq i \leq p$, $i \neq (p+1)/k$. Restating (12), we have $t(a) = k$ iff $\theta^{i2^k l} = 1$ and $\theta^{i2^{k-1}l} \neq 1$, iff $p+1 \mid i2^k l$ and $p+1 \not| \, i2^{k-1}l$, iff $\nu_2(p+1) = \nu_2(i) + k$.

Case (ii) is similar and is left to the reader.

We now indicate the minor changes needed to prove (c) and (d). We need only remark that the different ranges for the exponents arise because of two reasons: first, the polynomial $X^2 + 1$ is irreducible if $p \equiv 3 \pmod 4$ and reducible if $p \equiv 1 \pmod 4$. Second, $t(-2) = 1$ and must be treated as a special case depending on $p \pmod 4$.

For l odd define $\mathrm{ord}'_l\, 2$ to be the least e such that $2^e \equiv \pm 1 \pmod l$.

Corollary 15 *Let p be an odd prime with $p-1 = 2^\tau \cdot \rho$, $p+1 = 2^{\tau'} \cdot \rho'$, and ρ, ρ' odd. For each divisor $d > 1$ of ρ, $G = G_{x \to x^2-2}$ contains $\varphi(d)/(2\ \mathrm{ord}'_d\, 2)$ cycles of length $\mathrm{ord}'_d\, 2$. There are ρ elements in all these cycles, and off each element in these cycles there hang reversed complete binary trees of height $\tau - 1$ containing $2^\tau - 1$ elements.*

Similarly, for each divisor $d' > 1$ of ρ' there exists $\varphi(d')/(2\ \mathrm{ord}'_{d'}\, 2)$ cycles of length $\mathrm{ord}'_{d'}\, 2$, and off each element in these cycles there hang reversed complete binary trees of height $\tau' - 1$ containing $2^{\tau'} - 1$ elements.

Finally, the element 0 is the root of a complete binary tree of height $\tau - 2$ (respectively $\tau' - 2$) when $p \equiv 1 \pmod 4$ (respectively $p \equiv 3 \pmod 4$), and G also contains the directed edges $(0, -2)$, $(-2, 2)$, $(2, 2)$.

Proof. Exactly like that in Corollary 3.

For $p = 29$ we have the structure in Figure 5 and the data in Table 3.

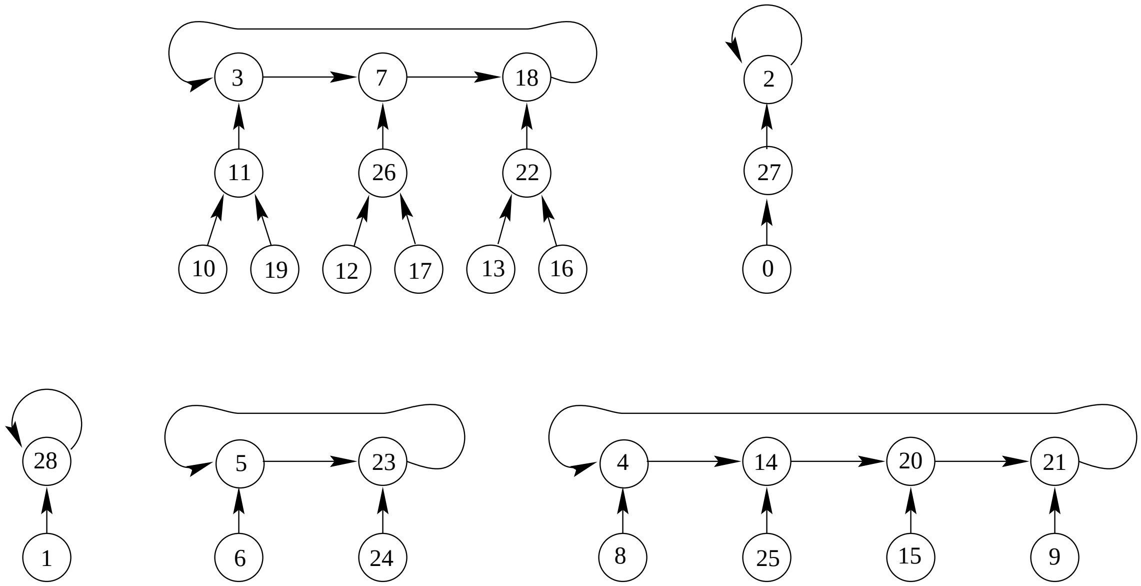

Fig. 5. The topology of $G_{x\to x^2-2}$ for $p = 29$

d	$\varphi(d)$	a with α of order d	$t = \nu_2(d)$	$l = d/2^t$	$c = \text{ord}'_l\ 2$
1	1	$\{2\}$	0	1	1
2	1	$\{27\}$	1	1	1
4	2	$\{0\}$	2	1	1
7	6	$\{3, 7, 18\}$	0	7	3
14	6	$\{11, 22, 26\}$	1	7	3
28	12	$\{10, 12, 13, 16, 17, 19\}$	2	7	3
3	2	$\{28\}$	0	3	1
5	4	$\{5, 23\}$	0	5	2
6	2	$\{1\}$	1	3	1
10	4	$\{6, 24\}$	1	5	2
15	8	$\{4, 14, 20, 21\}$	0	15	4
30	8	$\{8, 9, 15, 25\}$	1	15	4

Table 3: The structure of $G_{x\to x^2-2}$ for $p = 29$

There are two special cases where we can give more detailed information about $G_{x\to x^2-2}$. The first is when $p = 2^{2^k} + 1$, a Fermat prime.

Theorem 16 *The structure of the digraph $G_{x\to x^2-2}$ when $p = 2^{2^k}+1$, a Fermat prime is as follows:*

(i) A reversed complete binary tree of height 2^k-2 with root 0, attached to the node -2, attached to the node 2 with a cycle of length 1 on this node. The elements in this component are of the form 3^j+3^{-j} for $0 \le j \le 2^{2^k-1}$.

(ii) A set of cycles of length dividing 2^k-1. Off each element in these cycles there hangs a single element with tail length 1.

Proof. Part (i) follows immediately from Theorem 14 and the fact that 3 is a primitive root (mod p).

Part (ii) follows from the fact that $p+1 = 2(2^{2^k-1}+1)$.

For $p = 2^{2^2}+1 = 17$ we have the structure in Figure 6.

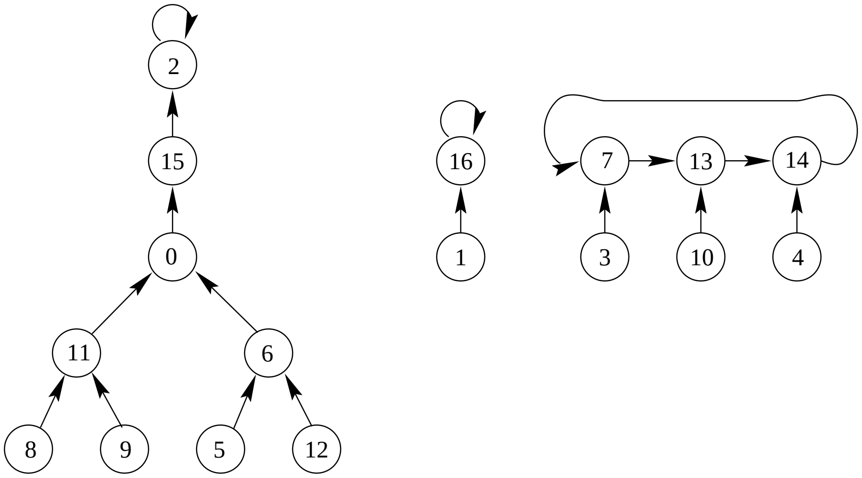

Fig. 6. The topology of $G_{x\to x^2-2}$ for $p = 17$

The second case where we can describe $G_{x\to x^2-2}$ more precisely is when $p = 2^q-1$, a Mersenne prime. Here q is an odd prime.

Theorem 17 *When $p = 2^q-1$, a Mersenne prime, the digraph $G_{x\to x^2-2}$ consists of*

(i) A reversed complete binary tree of height $q-1$ with root 0, attached to the node -2, which is attached to the node 2 with a cycle of length 1 on this node. The nodes in this tree are given by $\theta^n+\theta^{-n}$, $0 \le n \le 2^{q-1}$, where θ is a zero of X^2-4X+1.

(ii) A set of cycles of length dividing $q-1$. Off each element in these cycles there hangs a single element with tail length 1. The nodes in these cycles are given by 3^n+3^{-n}, $1 \le n \le 2^{q-1}-2$.

Proof. Use Corollary 15.

For $p = 2^5 - 1 = 31$ we have the structure in Figure 7.

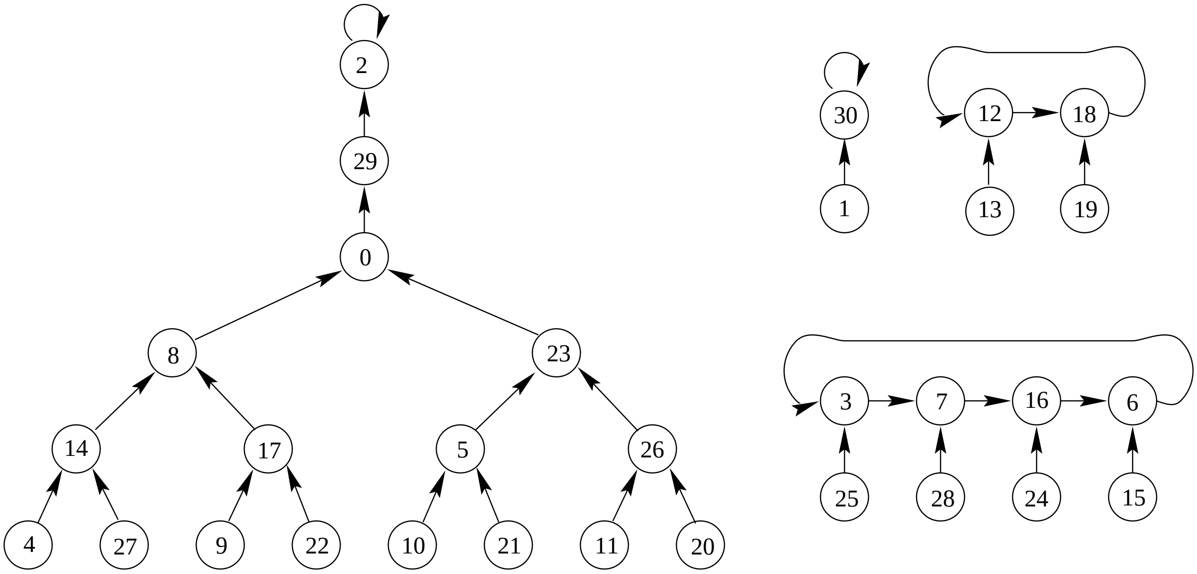

Fig. 7. The topology of $G_{x \to x^2 - 2}$ for $p = 31$

We now define quantities similar to that given in Section 2.

Definitions.

With respect to the iteration $x \to x^2 - 2 \pmod{p}$, we define:

- $TC'(p) :=$ total number of cycles;
- $T'_0(p) :=$ total number of elements in all cycles, i.e., the number of $a \in GF(p)$ with $t(a) = 0$;
- $AC'(p) :=$ average length of a cycle;
- $C'(p) :=$ average value of $c_p(a)$ over all $a \in GF(p)$;
- $T'(p) :=$ average value of $t_p(a)$ over all $a \in GF(p)$.

Corollary 18 *Let p be prime. Let $p - 1 = 2^\tau \cdot \rho$ and $p + 1 = 2^{\tau'} \cdot \rho'$ with ρ, ρ' odd. With respect to the iteration $x \to x^2 - 2 \pmod{p}$, we have*

(a) $TC'(p) = \frac{1}{2}\left(\sum_{d\,|\,\rho} \frac{\varphi(d)}{\mathrm{ord}'_d\ 2} \;+\; \sum_{d'\,|\,\rho'} \frac{\varphi(d')}{\mathrm{ord}'_{d'}\ 2}\right)$;
(b) $T'_0(p) = (\rho + \rho')/2$;
(c) $AC'(p) = T'_0(p)/TC'(p)$;
(d) $C'(p) = \frac{1}{2p}\left(2^\tau \sum_{d\,|\,\rho} \varphi(d)\mathrm{ord}'_d\ 2 \;+\; 2^{\tau'} \sum_{d'\,|\,\rho'} \varphi(d')\mathrm{ord}'_{d'}\ 2\right)$;

(e) $T'(p) = \frac{1}{2p}\left(\sum_{d\,|\,p-1}\varphi(d)\nu_2(d) \ + \ \sum_{d'\,|\,p+1}\varphi(d')\nu_2(d')\right) = \frac{\tau+\tau'}{2}+\frac{\tau'-\tau+\rho+\rho'}{2p}-1.$

Proof. Again, only (e) requires explanation. We have

$$\begin{aligned}
T'(p) &= \frac{1}{2p}\left(\sum_{d\,|\,p-1}\varphi(d)\nu_2(d) \ + \ \sum_{d'\,|\,p+1}\varphi(d')\nu_2(d')\right)\\
&= \frac{1}{2p}\left(\sum_{d\,|\,\rho}\varphi(d)((\tau-1)2^{\tau}+1) \ + \ \sum_{d'\,|\,\rho'}\varphi(d')((\tau'-1)2^{\tau'}+1)\right)\\
&= \frac{1}{2p}\left(\rho((\tau-1)2^{\tau}+1) \ + \ \rho'((\tau'-1)2^{\tau'}+1)\right)\\
&= \frac{1}{2p}\left((\tau-1)(p-1)+\rho+(\tau'-1)(p+1)+\rho'\right)\\
&= \frac{\tau+\tau'}{2}+\frac{\tau'-\tau+\rho+\rho'}{2p}-1.
\end{aligned}$$

Definitions.

With respect to the iteration $x \to x^2-2 \pmod p$, we define

- $ST_0'(N) := \sum_{2<p\le N} T_0'(p)$;
- $ST'(N) := \sum_{2<p\le N}\sum_{0\le a<p} t_p(a)$.

For example, we have $TC'(29) = 5$; $T_0'(29) = 11$; $AC'(29) = 11/5$; $C'(29) = 81/29$; and $T'(29) = 25/29$.

We now give a result analogous to Theorem 9.

Theorem 19 *Assume the ERH. Then, with respect to the iteration $x \to x^2-2$ (mod p) we have $ST_0'(N) \sim \frac{N^2}{6\log N}$.*

Proof. Exactly like that for Theorem 9.

It is interesting to note that we can obtain a slightly weaker result without any unproved hypotheses. Indeed, since

$$\frac{p+1}{2} \le \rho+\rho' \le \frac{3p+1}{4}$$

we immediately obtain $T_0'(p) = \Theta(p)$ and hence $ST_0'(N) = \Theta(N^2/(\log N))$.

Next, we prove a result analogous to Theorem 10.

Theorem 20 *Assume the ERH. Then, with respect to the iteration $x \to x^2-2 \pmod p$ we have $ST'(N) \sim \frac{2}{3} \cdot \frac{N^2}{\log N}$.*

Proof. By Theorem 18 (e) we have

$$\begin{aligned} ST'(N) &= \sum_{2<p\leq N} p\left(\frac{\nu_2(p-1)+\nu_2(p+1)}{2} + \frac{\tau'-\tau+\rho+\rho'}{2p} - 1\right) \\ &= \frac{1}{2}\sum_{2<p\leq N} \nu_2(p-1)(p-1) + \frac{1}{2}\sum_{2<p\leq N} \nu_2(p+1)(p+1) + \frac{1}{2}\sum_{2<p\leq N} \frac{p-1}{\nu_2(p-1)} \\ &\quad + \frac{1}{2}\sum_{2<p\leq N} \frac{p+1}{\nu_2(p+1)} - \sum_{2<p\leq N} p. \end{aligned}$$

Using exactly the same techniques as in the proof of Theorem 10, we obtain the desired result.

Table 4 compares the asymptotic estimates to empirical data.

N	$ST'_0(N)$	$N^2/(6\log N)$	$ST'(N)$	$2N^2/(3\log N)$
10	5	7.24	17	28.95
10^2	350	361.91	1368	1447.65
10^3	25484	24127.47	98718	96509.88
10^4	1918051	1809560.34	7548493	7238241.36
10^5	151494654	144764827.30	605787238	579059309.20
10^6	12516198017	12063735608.42	50108219545	48254942433.69

Table 4: Comparing $ST'_0(N)$ and $ST'(N)$ to asymptotic estimates

4 Pollard's factoring method

Pollard's factoring method is based on the fact that iterating a random quadratic map, modulo p, seems to produce tails and cycles that average $O(\sqrt{p})$ in size. Is this true for the iteration $x \to x^2-2$? As we have seen in Theorem 20,

$$\sum_{2<p\leq N} \sum_{0\leq a<p} t_p(a) \sim \frac{2}{3} \cdot \frac{N^2}{\log N},$$

while

$$\sum_{2<p\leq N}\sum_{0\leq a<p} 1 \sim \frac{N^2}{2\log N}.$$

One way to interpret this is to say that, on average, iterating the map $x \to x^2-2$ produces a tail of size $4/3$ — which is quite short.

However, we do not know any good asymptotic estimate for

$$SC'(N) := \sum_{2<p\leq N}\sum_{0\leq a<p} c_p(a).$$

If p is a Mersenne prime, say $p = 2^q - 1$, then

$$\begin{aligned}\sum_{0\leq a<p} c_p(a) &= \frac{2^\tau \sum_{d\,|\,\rho} \varphi(d)\mathrm{ord}'_d\ 2 \ + \ 2^{\tau'} \sum_{d'\,|\,\rho'} \varphi(d')\mathrm{ord}'_{d'}\ 2}{2} \\ &\leq \frac{2(2^{q-1}-1)(q-1)+2^q}{2} = O(p\log p).\end{aligned}$$

However, for certain primes p, such as those for which (a) $p' := (p-1)/2$ is prime and (b) 2 is a primitive root (mod p'), we have

$$\begin{aligned}\sum_{0\leq a<p} c_p(a) &= \frac{2^\tau \sum_{d\,|\,\rho} \varphi(d)\mathrm{ord}'_d\ 2 \ + \ 2^{\tau'} \sum_{d'\,|\,\rho'} \varphi(d')\mathrm{ord}'_{d'}\ 2}{2} \\ &\geq (p'-1)\frac{p'-1}{2} = \Omega(p^2).\end{aligned}$$

We expect there to be infinitely many such primes; indeed, heuristics such as Artin's conjecture on primitive roots suggest there are about $cN/(\log N)^2$ such primes $\leq N$. This suggests that $SC'(N)$ might well be $\Omega(N^3/(\log N)^2)$ and hence the "average" element will have cycle length at least $c'N/(\log N)^2$. This suggests it is indeed wise to avoid the iteration $x \to x^2 - 2$, as Pollard suggested.

We did some computations on this question, which are summarized in Table 5.

N	$SC'(N)$
10	15
10^2	6106
10^3	3292717
10^4	1896148462
10^5	1269905340415
10^6	902615197142485

Table 5: Some selected values of $SC'(N)$

These computations suggest that perhaps $SC'(N) \sim c'' \frac{N^3}{(\log N)^2}$, where $c'' \doteq .17$.

Acknowledgements

We would like to thank the referees, whose careful reading and suggestions helped us improve the paper. We also thank Eric Bach and Alberto Peinado for their comments.

References

[1] E. Bach and J. Shallit. *Algorithmic Number Theory.* MIT Press, 1996.

[2] E. L. Blanton, Jr., S. P. Hurd, and J. S. McCranie. On the digraph defined by squaring mod m, when m has primitive roots. *Congr. Numer.* **82** (1991), 167–177.

[3] E. L. Blanton, Jr., S. P. Hurd, and J. S. McCranie. On a digraph defined by squaring modulo n. *Fibonacci Quart.* **30** (1992), 322–333.

[4] L. Blum, M. Blum, and M. Shub. A simple unpredictable pseudo-random number generator. *SIAM J. Comput.* **15** (1986), 364–381.

[5] J. J. Brennan and B. Geist. Analysis of iterated modular exponentiation: the orbits of x^α mod N. *Designs, Codes and Cryptography* **13** (1998), 229–245.

[6] A. Z. Broder. *Weighted random mappings; properties and applications.* PhD thesis, Department of Computer Science, Stanford University, May 1985. Technical Report STAN-CS-85-1054.

[7] G. Chassé. *Applications d'un corps fini dans lui-même*, Vol. 149. Université de Rennes I U.E.R. de Mathématiques et Informatique, Rennes, 1984. Dissertation, Université de Rennes I, Rennes, 1984.

[8] G. Chassé. Applications d'un corps fini dans lui-même. In *Algebra Colloquium (Rennes, 1985)*, pp. 207–219. Univ. Rennes I, Rennes, 1985.

[9] G. Chassé. Combinatorial cycles of a polynomial map over a commutative field. *Discrete Math.* **61** (1986), 21–26.

[10] A. Flores. Geometry of numeric iterations. *PRIMUS* **4**(1) (1994), 29–38.

[11] C. L. Gilbert, J. D. Kolesar, C. A. Reiter, and J. D. Storey. Function digraphs of quadratic maps modulo p. *Fibonacci Quart.* **39** (2001), 32–49.

[12] B. Harris. Probability distributions related to random mappings. *Ann. Math. Stat.* **31** (1960), 1045–1062.

[13] A. Khrennikov and M. Nilsson. On the number of cycles of p-adic dynamical systems. *J. Number Theory* **90** (2001), 255–264.

[14] D. H. Lehmer. An extended theory of Lucas' functions. *Ann. Math.* **31** (1930), 419–448.

[15] H. R. Lewis and L. Denenberg. *Data Structures & Their Algorithms.* HarperCollins, 1991.

[16] G. L. Mullen R. Lidl and G. Turnwald. *Dickson Polynomials.* Pitman Monographs and Surveys in Pure and Applied Mathematics, Vol. 65, Longman Scientific, Essex, England, 1993.

[17] E. Lucas. Théorie des fonctions numériques simplement périodiques. *Amer. J. Math.* **1** (1878), 184–240; 289–321.

[18] C. Lucheta, E. Miller, and C. Reiter. Digraphs from powers modulo p. *Fibonacci Quart.* **34** (1996), 226–239.

[19] W. Nöbauer. Über die Fixpunte der Dickson-Permutationen. *Österreich. Akad. Wiss. Math.-Natur. Kl. Sitzungsber. II* **193** (1984), 115–133.

[20] A. Peinado, F. Montoya, J. Muñoz, and A. J. Yuste. Maximal periods of x^2+c in $\mathbb{F}_q$. In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (Melbourne, 2001)*, Vol. 2227 of *Lecture Notes in Comput. Sci.*, pp. 219–228. Springer, 2001.

[21] T. Pepin. Sur la formule $2^{2^n}+1$. *C. R. Acad. Sci. Paris* **85** (1877), 329–331.

[22] J. M. Pollard. A Monte Carlo method for factorization. *BIT* **15** (1975), 331–334.

[23] T. D. Rogers. The graph of the square mapping on the prime fields. *Discrete Math.* **148** (1996), 317–324.

[24] E. Teske and H. C. Williams. A note on Shanks' chains of primes. In W. Bosma, editor, *Proceedings of ANTS IV*, Vol. 1838 of *Lecture Notes in Computer Science*, pp. 563–580. Springer-Verlag, 2000.

[25] S. S. Wagstaff, Jr. Greatest of the least primes in arithmetic progressions having a given modulus. *Math. Comp.* **33** (1979), 1073–1080.

[26] B. Wilson. Power digraphs modulo n. *Fibonacci Quart.* **36** (1998), 229–239.