COMPONENT GROWTH OF ITERATION GRAPHS UNDER THE SQUARING MAP MODULO p^k

Walter Carlip

Department of Mathematics, Franklin & Marshall College, Lancaster, Pennsylvania 17603
e-mail: c3ar@zaphod.uchicago.edu

Martina Mincheva

Department of Mathematics, Franklin & Marshall College, Lancaster, Pennsylvania 17603

(Submitted December 2005-Final Revision May 2006)

ABSTRACT

We derive a formula for the number of components of the iteration graph $G(p^k)$ of the squaring function on the ring $\mathbf{Z}/p^k\mathbf{Z}$. In particular, if p is not a Wieferich prime, then the number of components is linear in k, and if p is a Wieferich prime, then the number of components is eventually linear in k.

1. INTRODUCTION

If R is any set, a mapping $f: R \to R$ induces a directed graph on R whose vertices are the elements of R and whose directed edges connect each $x \in R$ with its image $f(x) \in R$. This graph, which we denote $G(R)$, is called the iteration graph of the map f. When R is the ring $\mathbf{Z}/n\mathbf{Z}$, we use the abbreviated notation $G(n)$ for the iteration graph.

Iteration graphs provide a nice tool for studying properties of R that respect the mapping f, and arise in several fields, including number theory (see, e.g., [14] and [4]), group theory (see, e.g., [3]), and dynamical systems (see, e.g., [7]). In the last decade, a number of people have studied the iteration graphs arising from homomorphisms of finite abelian groups, in particular the power maps $x \mapsto x^n$ (see, e.g., [9], [17], and[5]) and quadratic polynomials on finite fields (see, e.g., [15] and [12]). Particular attention has been paid to the squaring map on the prime fields $\mathbf{F}_p$ (see, e.g., [15] and [13]) and, more generally, the squaring map on the rings $\mathbf{Z}/n\mathbf{Z}$ (see, e.g., [2] and [14]). The iteration graphs of the squaring map on the rings $\mathbf{Z}/n\mathbf{Z}$ are intimately connected to questions in number theory and are the focus of our interest here. In particular, we study the decomposition of the iteration graph of the squaring map on $\mathbf{Z}/n\mathbf{Z}$ when $n = p^k$ is the power of a prime. We show that if p is not a Wieferich prime, then the number of components of $G(p^k)$ increases linearly as a function of k. In the exceptional cases, when p is a Wieferich prime, the number of components is linear in k when k is sufficiently large.

2. PRELIMINARIES

Definition: For each n and a with $(a, n) = 1$, denote by $\operatorname{ord}(a, n)$ the order of a modulo n, i.e., the least integer ℓ such that $a^\ell \equiv 1 \pmod{n}$. Since a generates a cyclic subgroup $\langle a\rangle$ of order $\operatorname{ord}(a, n)$ in the abelian group $G = (\mathbf{Z}/n\mathbf{Z})^*$, which has order $\phi(n)$, the fraction $\phi(n)/\operatorname{ord}(a, n)$ is equal to the index of the subgroup $\langle a\rangle$ in G. We will write $\operatorname{ind}(a, n) = \phi(n)/\operatorname{ord}(a, n)$.

The following theorem about orders of integers modulo powers of a prime p is well known (see, e.g., Theorem 3.6 of [11]).

Theorem 2.1: *Suppose that p is an odd prime and $a > 1$ a positive integer relatively prime to p. Let $d = \text{ord}(a,p)$. If $p^t \parallel a^d - 1$, then $\text{ord}(a,p^k) = \text{ord}(a,p)$ when $k \le t$ and $\text{ord}(a,p^k) = p^{k-t}\text{ord}(a,p)$ when $k \ge t$.*

In particular, the sequence of orders $\{\text{ord}(a,p^k)\}_{k=1}^{\infty}$ increases geometrically with ratio p after an initial constant segment. The case that $a = 2$ has recieved special attention. Since $\text{ord}(2,p) \mid p-1$ and $(p,p-1) = 1$, it follows that $\text{ord}(2,p) = \text{ord}(2,p^2)$ if and only if $2^{p-1} \equiv 1 \pmod{p^2}$. Primes p for which these conditions are true are called *Wieferich primes*, after Arthur Wieferich, who proved in 1909 that any prime exponent p that is a counterexample to the first case of Fermat's last theorem satisfies this property [16]. To date, there are only two known Wieferich primes, 1093 and 3511, discovered by W. Meissner [10] and N. G. W. H. Beeger [1], respectively. It has been verified computationally that there are no other Wieferich primes less than 1.25×10^{15} [8]. For primes that are not Wieferich primes Theorem 2.1 [8] can be simplified.

Corollary 2.2: *If p is an odd prime that is not a Wieferich prime, then $\text{ord}(2,p^k) = p^{k-1}\text{ord}(2,p)$ for all $k \ge 1$.*

3. COUNTING COMPONENTS

Definition: For each positive integer n, let $G(n)$ denote the directed graph whose vertices correspond to elements of $\mathbf{Z}/n\mathbf{Z}$ and whose edges consist of the ordered pairs $\{(a,a^2) \mid a \in \mathbf{Z}/n\mathbf{Z}\}$ and let $N(n)$ denote the number of connected components of $G(n)$.

By a straight-forward graph theoretic argument, it is easy to see that every connected component of $G(n)$ has exactly one cycle, so $N(n)$ also represents the number of cycles in $G(n)$.

The following theorem about cycles under the squaring map on a finite group G is known in special cases, see, e.g., Theorem 15 of [9] when $G = (\mathbf{Z}/p\mathbf{Z})^*$ and Lemma 3 of [17] when $G = (\mathbf{Z}/n\mathbf{Z})^*$, but applies equally well to any finite group G.

Theorem 3.1: *If G is any finite group, then an element $g \in G$ lies in a cycle under the squaring map if and only if g has odd order. If g has odd order d, then every element in the cycle containing g has order d and the length of the cycle containing g is $\text{ord}(2,d)$.*

Proof: If $g \in G$, then $\text{ord}(g^2) = \text{ord}(g)/2$ when g has even order and $\text{ord}(g^2) = \text{ord}(g)$ when g has odd order. If g lies in a cycle, then $g^{2^k} = g$, for some k, and hence g must have odd order. Conversely, if g has odd order d, then g^{2^k} has order d for all k, and since G is finite $g^{2^k} = g^{2^\ell}$ for some $\ell < k$. Choose k minimal with this property. Then $1 = g^{2^k - 2^\ell} = g^{2^\ell(2^{k-\ell}-1)}$. Since g^{2^ℓ} also has order d, it follows that $g^{(2^{k-\ell}-1)} = 1$, and $g^{2^{k-\ell}} = g$. By minimality of k, we see that $k = k - \ell$, and $g^{2^k} = g$. Thus g lies in a cycle of length k. The cycle length is the smallest integer k such that $g^{2^k-1} = 1$, and hence the smallest k such that $d \mid 2^k - 1$. Thus $k = \text{ord}(2,d)$.

For reference below we make the following definition.

Definition: Let $G = (\mathbf{Z}/n\mathbf{Z})^*$ be the unit group of the ring $\mathbf{Z}/n\mathbf{Z}$ and define $\mathcal{O}(n)$ to be the set of odd divisors of $\phi(n)$. In particular, $\mathcal{O}(p^k)$ is the set of odd divisors of $p^{k-1}(p-1)$.

Our main goal is to generalize to prime powers $n = p^k$ the following well-known theorem for primes $n = p$ (see, e.g., [15]).

Theorem 3.2: *Suppose that $n = p$. Then the iteration graph $G(n)$ contains $\phi(d)/\mathrm{ord}(2,d)$ cycles of length* $\mathrm{ord}(2,d)$ *and one additional cycle of length* 1. *In particular,*

$$N(p) = 1 + \sum_{d \in \mathcal{O}(p)} \frac{\phi(d)}{\mathrm{ord}(2,d)} = 1 + \sum_{d \in \mathcal{O}(p)} \mathrm{ind}(2,d).$$

Proof: Clearly, the point 0 is a fixed point of $G(n)$ and the component of 0 contains every element of $\mathbf{Z}/p\mathbf{Z}$ that is divisible by p. The remaining elements lie in the unit group G. Since G is cyclic of order $p-1$, G contains exactly $\phi(d)$ elements of order d, for each $d \in \mathcal{O}(p)$. Each element of order d lies in a cycle of length $\mathrm{ord}(2,d)$ consisting of distinct elements of order d, and it follows that $G(n)$ has exactly $\phi(d)/\mathrm{ord}(2,d)$ such cycles. The formula for $N(p)$ follows immediately. □

To generalize 3.2, we make the following definition.

Definition: Define the constant $\epsilon(p)$ by

$$\epsilon(p) = \sum_{d \in \mathcal{O}(p)} \mathrm{ind}(2,p)\mathrm{ind}(2,d)(\mathrm{ord}(2,p), \mathrm{ord}(2,d)).$$

Theorem 3.3: *Suppose that $n = p^k$, where p is an odd prime. If p is not a Wieferich prime, then the number of cycles in the iteration graph $G(n)$ is*

$$N(p^k) = 1 + \sum_{d \in \mathcal{O}(p)} \mathrm{ind}(2,d) + (k-1)\epsilon(p) = N(p) + (k-1)\epsilon(p).$$

Proof: As in the proof of Theorem 3.2, the point 0 is a fixed point of $G(n)$, and the remaining cycles lie in the unit group G. By Theorem 3.1 each element $g \in G$ of odd order d lies in a cycle of length $\mathrm{ord}(2,d)$.

Since p is an odd prime, $G = (\mathbf{Z}/p^k\mathbf{Z})^*$ is cyclic of order $\phi(p^k) = p^{k-1}(p-1)$. Clearly $\mathcal{O}(p^k) = \{p^t d \mid d \in \mathcal{O}(p) \text{ and } 0 \le t \le k-1\}$. Since G is cyclic, G contains $\phi(p^t d)$ elements of order $p^t d$, each of which lies in a cycle of length $\mathrm{ord}(2, p^t d)$. It follows that the number of cycles in $G(n)$ is

$$N(p^k) = 1 + \sum_{d \in \mathcal{O}(p)} \sum_{t=0}^{k-1} \frac{\phi(p^t d)}{\mathrm{ord}(2, p^t d)} = 1 + \sum_{d \in \mathcal{O}(p)} \sum_{t=0}^{k-1} \mathrm{ind}(2, p^t d). \tag{1}$$

Suppose that $d \in \mathcal{O}(p)$. Since $d \mid p-1$, we know that $(p,d) = 1$, and therefore $\phi(p^t d) = \phi(p^t)\phi(d)$. On the other hand, $\mathrm{ord}(2,p^t d) = \mathrm{lcm}(\mathrm{ord}(2,p^t), \mathrm{ord}(2,d)) = \mathrm{ord}(2,p^t)\mathrm{ord}(2,d)/(\mathrm{ord}(2,p^t), \mathrm{ord}(2,d))$. Since p is not a Wieferich prime, $\mathrm{ord}(2,p^t) = p^{t-1}\mathrm{ord}(2,p)$ when $t \ge 1$. Thus, if $t \ge 1$,

$$\begin{aligned} \mathrm{ind}(2,p^t d) = \frac{\phi(p^t d)}{\mathrm{ord}(2,p^t d)} &= \frac{p^{t-1}\phi(p)\phi(d)}{p^{t-1}\mathrm{ord}(2,p)\mathrm{ord}(2,d)} \cdot (p^{t-1}\mathrm{ord}(2,p), \mathrm{ord}(2,d)) \\ &= \mathrm{ind}(2,p)\mathrm{ind}(2,d)(\mathrm{ord}(2,p), \mathrm{ord}(2,d)). \end{aligned} \tag{2}$$

It follows that the number of cycles in $G(n)$ is

$$\begin{aligned} N(p^k) &= 1+\sum_{d\in\mathcal{O}(p)}\sum_{t=0}^{k-1}\operatorname{ind}(2,p^td) = 1+\sum_{d\in\mathcal{O}(p)}\operatorname{ind}(2,d)+\sum_{d\in\mathcal{O}(p)}\sum_{t=1}^{k-1}\operatorname{ind}(2,p^td) \\ &= N(p)+\sum_{t=1}^{k-1}\sum_{d\in\mathcal{O}(p)}\operatorname{ind}(2,p)\operatorname{ind}(2,d)(\operatorname{ord}(2,p),\operatorname{ord}(2,d)) \\ &= N(p)+(k-1)\epsilon(p), \end{aligned} \tag{3}$$

as desired. □

The method of proof of Theorem 3.3 can be modified to yield the following result for Wieferich primes p.

Theorem 3.4: *Suppose that $n = p^k$, where p is a Wieferich prime. Choose e minimal such that* $\operatorname{ord}(2,p^{e+1}) = p\operatorname{ord}(2,p^e)$. *Then the number of cycles in the iteration graph $G(p^k)$ for $k \geq e$ is*

$$N(p^k) = N(p^e) + (k-e)p^{e-1}\epsilon(p).$$

Note: Observe that Theorem 3.4 reduces to Theorem 3.3 when $e = 1$.

Proof: As in Theorem 3.3, (1) can be used to compute $N(p^k)$, however we must modify (2). For $1 \leq t < e$ we obtain $\operatorname{ord}(2,p^t) = \operatorname{ord}(2,p)$ and for $t \geq e$ we obtain $\operatorname{ord}(2,p^t) = p^{t-e}\operatorname{ord}(2,p)$, and therefore

$$\operatorname{ind}(2,p^td) = \begin{cases} p^{t-1}(\operatorname{ord}(2,p),\operatorname{ord}(2,d))\operatorname{ind}(2,p)\operatorname{ind}(2,d) & \text{if } 1\leq t<e, \text{ and} \\ p^{e-1}(\operatorname{ord}(2,p),\operatorname{ord}(2,d))\operatorname{ind}(2,p)\operatorname{ind}(2,d) & \text{if } t\geq e. \end{cases}$$

As in (3), we have

$$\begin{aligned} N(p^k) &= 1+\sum_{d\in\mathcal{O}(p)}\sum_{t=0}^{k-1}\operatorname{ind}(2,(p^td)) = 1+\sum_{t=0}^{e-1}\sum_{d\in\mathcal{O}(p)}\operatorname{ind}(2,(p^td))+\sum_{t=e}^{k-1}\sum_{d\in\mathcal{O}(p)}\operatorname{ind}(2,(p^td)) \\ &= N(p^e)+\sum_{t=e}^{k-1}\sum_{d\in\mathcal{O}(p)}p^{e-1}\operatorname{ind}(2,p)\operatorname{ind}(2,d)(\operatorname{ord}(2,p),\operatorname{ord}(2,d)) \\ &= N(p^e)+(k-e)p^{e-1}\epsilon(p), \end{aligned}$$

as desired. □

Corollary 3.5: *If p is not a Wieferich prime, then $N(p^k)$ increases linearly as a function of k. If p is a Wieferich prime, $N(p^k)$ is linear for k sufficiently large.*

4. COMPUTATIONS

In this final section we offer several examples of Theorem 3.3 and Theorem 3.4 at work. In particular, we compute $N(3^k)$ and $N(19^k)$ using Theorem 3.3 and $N(1093^k)$ and $N(3511^k)$ using Theorem 3.4. Since 1093 and 3511 are the only known Wieferich primes, these are the only cases for which Theorem 3.4 is known to be required. We conclude the paper with a table of $N(p^k)$ for all primes $p < 1000$. The distribution of the values of $N(p)$ and $\epsilon(p)$ is interesting and merits further study. Some of the computations in this section were performed using the discrete mathematics computation package Gap [6].

Example 1: If $n = 3^k$, then $N(n) = k + 1$.

Proof: Observe that $\mathcal{O}(3) = \{1\}$. Thus, the number of cycles in $G(3)$ is simply

$$1 + \operatorname{ind}(2,1) = 1 + \frac{\phi(1)}{\operatorname{ord}(2,1)} = 2.$$

Since $\epsilon(3) = \sum_{d\in\mathcal{O}(3)} (\operatorname{ord}(2,p), \operatorname{ord}(2,d))\operatorname{ind}(2,p)\operatorname{ind}(2,d) = 1$, Theorem 3.3 implies that $G(3^k)$ has $2 + (k-1) = k+1$ cycles. □

Example 2: If $n = 19^k$, then $N(n) = 9k - 5$.

Proof: Observe that $\mathcal{O}(19) = \{1,3,9\}$. Thus, the number of cycles in $G(19)$ is

$$1 + \operatorname{ind}(2,1) + \operatorname{ind}(2,3) + \operatorname{ind}(2,9) = 1 + \frac{\phi(1)}{\operatorname{ord}(2,1)} + \frac{\phi(3)}{\operatorname{ord}(2,3)} + \frac{\phi(9)}{\operatorname{ord}(2,9)} = 4.$$

Moreover $\epsilon(19) = \sum_{d\in\mathcal{O}(19)} (\operatorname{ord}(2,p), \operatorname{ord}(2,d))\operatorname{ind}(2,p)\operatorname{ind}(2,d) = 1 + 2 + 6 = 9$. It now follows from Theorem 3.3 that $G(19^k)$ has $4 + (k-1)\cdot 9 = 9k - 5$ cycles. □

The next two examples give $N(p^n)$ for each of the two known Wieferich primes $p = 1093$ and $p = 3511$.

Example 3: If $n = 1093^k$, then $N(n) = 307 + 304947(k-2)$, for $k \geq 2$.

Proof: Since $\operatorname{ord}(2,1093) = \operatorname{ord}(2,1093^2) = 364$, while $\operatorname{ord}(2,1093^3) = 397852 = 1093 \cdot 364$, we know that $e = 2$. Since $1092 = 2^2 \cdot 3 \cdot 7 \cdot 13$, we obtain $\mathcal{O}(1093) = \{1,3,7,13,21,39,91,273\}$, and therefore

$$\begin{aligned}\epsilon(1093) &= \sum_{d\in\mathcal{O}(1093)} \operatorname{ind}(2,1093)\operatorname{ind}(2,d)(\operatorname{ord}(2,1093), \operatorname{ord}(2,d)) \\ &= 3\cdot 1\cdot(364,1) + 3\cdot 1\cdot(364,2) + 3\cdot 2\cdot(364,3) + 3\cdot 1\cdot(364,12) \\ &\quad + 3\cdot 2\cdot(364,6) + 3\cdot 2\cdot(364,12) + 3\cdot 6\cdot(364,12) + 3\cdot 12\cdot(364,12) \\ &= 3 + 6 + 6 + 12 + 12 + 24 + 72 + 144 = 279.\end{aligned}$$

By (1):

$$\begin{aligned} N(1093^2) &= 1 + \sum_{d \in \mathcal{O}(1093)} \text{ind}(2,d) + \sum_{d \in \mathcal{O}(1093)} \text{ind}(2,1093d) \\ &= 1 + \sum_{d \in \mathcal{O}(1093)} \text{ind}(2,d) + \sum_{d \in \mathcal{O}(1093)} \text{ind}(2,1093)\text{ind}(2,d)(\text{ord}(2,1093), \text{ord}(2,d)) \\ &= 1 + 27 + \epsilon(1093) = 307. \end{aligned}$$

Finally, by Theorem 3.4,

$$N(1093^k) = \begin{cases} 28 & \text{if } k = 1; \\ 307 + 304947(k-2) & \text{if } k \geq 2, \end{cases}$$

as desired. □

Example 4: If $n = 3511^k$, then $N(n) = 892 + 3131812(k-2)$, for $k \geq 2$.

Proof: Since $\text{ord}(2,3511) = \text{ord}(2,3511^2) = 1755$, while $\text{ord}(2,3511^3) = 6161805 = 3511 \cdot 1755$, we obtain $e = 2$. Since $3510 = 2 \cdot 3^3 \cdot 5 \cdot 13$, we find $\mathcal{O}(3511) = \{1,3,5,9,13,15,27,39,45,65,117,135,195,351,585,1755\}$, and therefore

$$\begin{aligned} \epsilon(3511) &= \sum_{d \in \mathcal{O}(3511)} \text{ind}(2,3511)\text{ind}(2,d)(\text{ord}(2,3511), \text{ord}(2,d)) \\ &= 2 \cdot 1 \cdot (1755,1) + 2 \cdot 1 \cdot (1755,2) + 2 \cdot 1 \cdot (1755,4) + 2 \cdot 1 \cdot (1755,6) + 2 \cdot 1 \cdot (1755,12) \\ &\quad + 2 \cdot 2 \cdot (1755,4) + 2 \cdot 1 \cdot (1755,18) + 2 \cdot 2 \cdot (1755,12) + 2 \cdot 2 \cdot (1755,12) \\ &\quad + 2 \cdot 4 \cdot (1755,12) + 2 \cdot 6 \cdot (1755,12) + 2 \cdot 2 \cdot (1755,36) + 2 \cdot 8 \cdot (1755,12) \\ &\quad + 2 \cdot 6 \cdot (1755,36) + 2 \cdot 24 \cdot (1755,12) + 2 \cdot 24 \cdot (1755,36) \\ &= 2 + 2 + 2 + 6 + 6 + 4 + 18 + 12 + 12 + 24 + 36 + 36 + 48 + 108 + 144 + 432 \\ &= 892. \end{aligned}$$

By (1):

$$\begin{aligned} N(3511^2) &= 1 + \sum_{d \in \mathcal{O}(3511)} \text{ind}(2,d) + \sum_{d \in \mathcal{O}(3511)} \text{ind}(2,3511d) \\ &= 1 + \sum_{d \in \mathcal{O}(3511)} \text{ind}(2,d) + \sum_{d \in \mathcal{O}(3511)} \text{ind}(2,3511)\text{ind}(2,d)(\text{ord}(2,3511), \text{ord}(2,d)) \\ &= 1 + 86 + \epsilon(3511) = 979. \end{aligned}$$

Finally, by Theorem 3.4,

$$N(3511^k) = \begin{cases} 87 & \text{if } k = 1; \\ 979 + 3131812(k-2) & \text{if } k \geq 2, \end{cases}$$

as desired. □

p	$N(p^k)$	p	$N(p^k)$	p	$N(p^k)$	p	$N(p^k)$	p	$N(p^k)$
3	$k+1$	149	$5k-2$	347	$3k$	557	$3k$	769	$6k-3$
5	$k+1$	151	$200k-191$	349	$15k-9$	563	$9k-3$	773	$9k-5$
7	$4k-1$	157	$45k-39$	353	$12k-9$	569	$6k-2$	787	$9k-3$
11	$3k$	163	$81k-75$	359	$4k-1$	571	$315k-300$	797	$3k+1$
13	$3k$	167	$4k-1$	367	$22k-16$	577	$36k-32$	809	$10k-7$
17	$2k$	173	$7k-2$	373	$21k-6$	587	$3k$	811	$729k-714$
19	$9k-5$	179	$9k+1$	379	$189k-168$	593	$20k-17$	821	$205k-192$
23	$4k-1$	181	$45k-36$	383	$6k-2$	599	$12k-5$	823	$16k-7$
29	$3k+1$	191	$10k-4$	389	$9k-5$	601	$480k-471$	827	$9k-2$
31	$30k-24$	193	$6k-3$	397	$135k-126$	607	$10k-4$	829	$27k-17$
37	$9k-5$	197	$17k-11$	401	$50k-46$	613	$81k-67$	839	$4k-1$
41	$10k-7$	199	$28k-19$	409	$54k-45$	619	$21k-14$	853	$9k-2$
43	$27k-20$	211	$63k-47$	419	$9k-3$	631	$1372k-1335$	857	$6k-3$
47	$6k-2$	223	$30k-24$	421	$105k-89$	641	$50k-47$	859	$63k-48$
53	$5k-2$	227	$9k-3$	431	$110k-98$	643	$27k-21$	863	$22k-10$
59	$3k$	229	$27k-21$	433	$162k-157$	647	$16k-7$	877	$75k-56$
61	$15k-9$	233	$16k-13$	439	$108k-89$	653	$3k$	881	$272k-266$
67	$9k-3$	239	$18k-8$	443	$23k-10$	659	$9k+1$	883	$441k-417$
71	$12k-5$	241	$150k-144$	449	$6k-2$	661	$165k-150$	887	$4k-1$
73	$40k-36$	251	$315k-310$	457	$54k-48$	673	$294k-287$	907	$93k-70$
79	$22k-16$	257	$16k-14$	461	$15k-8$	677	$57k-53$	911	$410k-368$
83	$5k-1$	263	$4k-1$	463	$70k-54$	683	$2139k-2100$	919	$408k-389$
89	$16k-13$	271	$82k-70$	467	$9k+1$	691	$81k-65$	929	$10k-7$
97	$6k-3$	277	$27k-20$	479	$6k-2$	701	$75k-65$	937	$256k-243$
101	$25k-21$	281	$36k-29$	487	$244k-237$	709	$9k-3$	941	$15k-8$
103	$16k-7$	283	$27k-20$	491	$51k-40$	719	$6k-2$	947	$21k-9$
107	$3k$	293	$9k+1$	499	$27k-21$	727	$228k-219$	953	$378k-368$
109	$81k-76$	307	$135k-121$	503	$12k-5$	733	$45k-39$	967	$84k-65$
113	$12k-8$	311	$124k-109$	509	$19k+1$	739	$135k-121$	971	$115k-102$
127	$234k-220$	313	$78k-72$	521	$50k-42$	743	$12k-5$	977	$10k-7$
131	$13k-5$	317	$3k+1$	523	$27k-18$	751	$190k-178$	983	$4k-1$
137	$18k-14$	331	$1089k-1074$	541	$135k-123$	757	$189k-168$	991	$298k-274$
139	$9k-2$	337	$224k-217$	547	$147k-119$	761	$30k-24$	997	$27k-21$

Table 1. Values of $N(p^k)$ for primes $p < 1000$.

REFERENCES

[1] N. G. W. H. Beeger. "On a New Case of the Congruence $2^{p-1} = 1(p^2)$." *Messenger of Math* **51** (1922): 149-150.

[2] Earle L. Blanton, Jr., Spencer P. Hurd, and Judson S. McCranie. "On a Digraph Defined by Squaring Modulo n." *Fibonacci Quart.* **30.4** (1992): 322-334.

[3] Steven Bryant. "Groups, Graphs, and Fermat's Last Theorem." *Amer. Math. Monthly* **74** (1967): 152-156.

[4] Guy Chassé. "Combinatorial Cycles of a Polynomial Map Over a Commutative Field." *Discrete Math.* **61.1** (1986): 21-26.

[5] Wun-Seng Chou and Igor E. Shparlinski. "On the Cycle Structure of Repeated Exponentiation Modulo a Prime." *J. Number Theory* **107.2** (2004): 345-356.

[6] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.4*, 2005, (http://www.gap-system.org).

[7] Andrei Khrennikov and Marcus Nilsson. "On the Number of Cycles of p-adic Dynamical Systems." *J. Number Theory* **90.2** (2001): 255-264.

[8] Joshua Knauer and Jörg Richstein. "The Continuing Search for Wieferich Primes." *Math. Comp.* **75** (2005): 1559-1563.

[9] Caroline Lucheta, Eli Miller, and Clifford Reiter. "Digraphs from Powers Modulo p." *Fibonacci Quart.* **34.3** (1996): 226-239.

[10] W. Meissner. "Über die Teilbarkeit von $2^p - 2$ durch das Quadrat der Primzahl $p = 1093$" *Sitzungsber. Akad. d. Wiss. Berlin* **51** (1913): 663-667.

[11] Melvyn B. Nathanson. *Elementary Methods in Number Theory*, Graduate Texts in Mathematics, vol. 195, Springer-Verlag, New York, 2000.

[12] A. Peinado, F. Montoya, J. Muñoz, and A. J. Yuste. *Maximal Periods of $x^2 + c$ in $\mathbb{F}_q$*, Applied algebra, algebraic algorithms and error-correcting codes (Melbourne, 2001), Lecture Notes in Comput. Sci., vol. 2227, Springer, Berlin, 2001, pp. 219–228.

[13] Thomas D. Rogers. "The Graph of the Square Mapping on the Prime Fields." *Discrete Math.* **148.1-3** (1996): 317-324.

[14] Lawrence Somer and Michal Křížek. "On a Connection of Number Theory With Graph Theory." *Czechoslovak Math. J.* **54(129).2** (2004): 465-485.

[15] Troy Vasiga and Jeffrey Shallit. "On the Iteration of Certain Quadratic Maps Over $GF(p)$." *Discrete Math.* **277.1-3** (2004): 219-240.

[16] A. Wieferich. "Zum letzten Fermat'schen Theorem." *J. Reine Angew. Math.* **136** (1909): 293–302.

[17] Brad Wilson. "Power Digraphs Modulo n." *Fibonacci Quart.* **36.3** (1998): 229-239.

AMS Classification Numbers: 05C20, 05C75, 11A07, 11T99