Czechoslovak Mathematical Journal

Walter Carlip; Martina Mincheva

Symmetry of iteration graphs

Czechoslovak Mathematical Journal, Vol. 58 (2008), No. 1, 131–145

Persistent URL: http://dml.cz/dmlcz/128250

Czechoslovak Mathematical Journal, 58 (133) (2008), 131–145

SYMMETRY OF ITERATION GRAPHS

Walter Carlip, Martina Mincheva, Lancaster

(Received January 10, 2006)

Abstract. We examine iteration graphs of the squaring function on the rings $\mathbb{Z}/n\mathbb{Z}$ when $n = 2^k p$, for p a Fermat prime. We describe several invariants associated to these graphs and use them to prove that the graphs are not symmetric when $k = 3$ and when $k \geqslant 5$ and are symmetric when $k = 4$.

Keywords: digraph, iteration digraph, quadratic map, tree, cycle

MSC 2000: 05C20, 11T99

1. Introduction

If R is any set, a mapping $f\colon R \to R$ induces a directed graph on R, called the *iteration digraph* of f, whose vertices are the elements of R and whose directed edges connect each $x \in R$ with its image $f(x) \in R$. The iteration graphs of the squaring function $f(x) = x^2$ on the rings $R = \mathbb{Z}/n\mathbb{Z}$ have interesting connections to number theory (see, e.g., [6] and [2]) and have been extensively studied (see, e.g., [5], [8], [1], and [6]), yet interesting questions about them remain unanswered. For each positive integer n, we denote the iteration graph of the squaring function on the ring $\mathbb{Z}/n\mathbb{Z}$ by $G(n)$.

In [6], the authors call an iteration graph *symmetric* if its connected components can be partitioned into isomorphic pairs. They offer a theorem, which they attribute to László Szalay [7], that the iteration diagraph of $G(n)$ is symmetric if $n \equiv 2 \pmod 4$ or $n \equiv 4 \pmod 8$. In this paper we prove that the generalization to higher powers of 2 is false. In particular, we show that if p is a Fermat prime, and $n = 2^k p$, then $G(n)$ is not symmetric when $k = 3$ and when $k \geqslant 5$, but it is symmetric when $k = 4$. We are currently working on a generalization of this work to $G(n)$ for arbitrary n.

2. Preliminaries

Theorem 2.1. *If $n = \prod_{i=1}^{t} p_i^{\alpha_i}$, then $G(n)$ has exactly $2^{\omega(n)} = 2^t$ fixed points.*

Proof. It is easy to see that 0 and 1 are the only fixed points modulo p^α for any prime p. If a is a fixed point modulo n, then certainly a is a fixed point modulo $p_i^{\alpha_i}$ for each i, so for each i we know that $a \equiv 0 \pmod{p_i^{\alpha_i}}$ or $a \equiv 1 \pmod{p_i^{\alpha_i}}$. Conversely, by the Chinese Remainder Theorem, for each choice $\varepsilon_i \in \{0, 1\}$ there is a unique a such that $a \equiv \varepsilon_i \pmod{p_i^{\alpha_i}}$, and clearly, a is a fixed point modulo n. Since there are 2^t distinct ways to choose the ε_i, $G(n)$ has exactly 2^t fixed points. □

Theorem 2.2. *Suppose that $n = 2^k p$, where $p = 2^l + 1$ is a Fermat prime and $k \geqslant 1$. Let α be the smallest even integer such that $\alpha l \geqslant k$ and β the smallest odd integer such that $\beta l \geqslant k$. Then the four fixed points of $G(n)$ are*

$$0, \quad 1, \quad 2^{\alpha l}, \quad \text{and} \quad 2^{\beta l} + 1. \tag{1}$$

Proof. By the proof of Theorem 2.1, it suffices to show that each listed point is equivalent to 0 or 1 modulo 2^k and to 0 or 1 modulo p. This is obvious for the points 0 and 1.

Since $\alpha l \geqslant k$, it is clear that $2^{\alpha l} \equiv 0 \pmod{2^k}$. On the other hand, since $2^l \equiv -1 \pmod{p}$ and α is even, $2^{\alpha l} \equiv (-1)^\alpha \equiv 1 \pmod{p}$.

Similarly, since $\beta l \geqslant k$, we see that $2^{\beta l} + 1 \equiv 1 \pmod{2^k}$. Since $2^l \equiv -1 \pmod{p}$ and β is odd, $2^{\beta l} + 1 \equiv 0 \pmod{p}$. □

We can also express the fixed points of $G(n)$ in terms of k and l as follows.

Theorem 2.3. *Suppose that $n = 2^k p$, where $p = 2^l + 1$ is a Fermat prime and $k \geqslant 1$. Suppose that $k \equiv t \pmod{2l}$ with $0 < t \leqslant 2l$. Then the four fixed points of $G(n)$ are*

$$0, \quad 1, \quad 2^{k+2l-t}, \quad \text{and} \quad 2^{k+3l-t} + 1.$$

Proof. Again it suffices to show that each listed point is equivalent to 0 or 1 modulo 2^k and to 0 or 1 modulo p, and this is obvious for 0 and 1.

Clearly, $k+2l-t \geqslant k$ and $k+3l-t \geqslant k$, so $2^{k+2l-t} \equiv 0 \pmod{2^k}$ and $2^{k+3l-t}+1 \equiv 1 \pmod{2^k}$.

On the other hand, since $k \equiv t \pmod{2l}$, we can write $k - t = 2la$ for some integer a and therefore $2^{k+2l-t} = 2^{2l(a+1)} \equiv 1^{a+1} \equiv 1 \pmod{p}$ and $2^{k+3l-t} + 1 = 2^{2la+3l} + 1 = 2^{2la}2^{3l} + 1 \equiv -1 + 1 \equiv 0 \pmod{p}$. □

In the table below we list the fixed points for $G(n)$ for $p = 3$ and $p = 5$.

p	n	k	Fixed Points			
3	$3 \cdot 2^k$	$k \equiv 0 \pmod 2$	0	1	2^k	$2^{k+1} + 1$
3	$3 \cdot 2^k$	$k \equiv 1 \pmod 2$	0	1	2^{k+1}	$2^k + 1$
5	$5 \cdot 2^k$	$k \equiv 0 \pmod 4$	0	1	2^k	$2^{k+2} + 1$
5	$5 \cdot 2^k$	$k \equiv 1 \pmod 4$	0	1	2^{k+3}	$2^{k+1} + 1$
5	$5 \cdot 2^k$	$k \equiv 2 \pmod 4$	0	1	2^{k+2}	$2^k + 1$
5	$5 \cdot 2^k$	$k \equiv 3 \pmod 4$	0	1	2^{k+1}	$2^{k+3} + 1$

Theorem 2.4. *If $n = 2^k p$, where $p = 2^l + 1$ is a Fermat prime, then $G(n)$ has exactly four components.*

P r o o f. By a straight-forward graph theoretic argument, each component of $G(n)$ has exactly one cycle. Therefore it suffices to show that $G(n)$ has no cycles of length greater than one.

To this end, suppose that a lies in a cycle. We will show that a is one of the four fixed points of $G(n)$. By the argument of Theorem 2.1 once again, it suffices to show that a is congruent to 0 or 1 modulo 2^k and to 0 or 1 modulo p.

Since a lies in a cycle, there is a smallest positive integer t such that $a^{2^t} \equiv a \pmod n$. But then $a(a^{2^t-1} - 1) \equiv a^{2^t} - a \equiv 0 \pmod n$.

Now a and $a^{2^t-1} - 1$ are relatively prime, so one or the other, but not both, is divisible by 2^k, and one or the other, but not both, is divisible by p. Thus there are four cases corresponding to which of them is divisible by p and by 2^k.

Obviously if a is divisible by 2^k or by p then $a \equiv 0 \pmod{2^k}$ or $a \equiv 0 \pmod p$, respectively.

If $a^{2^t-1} - 1$ is divisible by p, then $a^{2^t-1} \equiv 1 \pmod p$, and a has odd order dividing $2^t - 1$ in the unit group $(\mathbb{Z}/p\mathbb{Z})^*$. Since $|(\mathbb{Z}/p\mathbb{Z})^*| = p - 1 = 2^l$, the only element of odd order in $(\mathbb{Z}/p\mathbb{Z})^*$ is the identity, and it follows that $a \equiv 1 \pmod p$.

Similarly, if $a^{2^t-1} - 1$ is divisible by 2^k, then $a^{2^t-1} \equiv 1 \pmod{2^k}$. Again, this implies that a has odd order in the unit group $(\mathbb{Z}/2^k\mathbb{Z})^*$, which has order 2^{k-1}. The only element of odd order in $(\mathbb{Z}/2^k\mathbb{Z})^*$ is the identity, so $a \equiv 1 \pmod{2^k}$.

Thus, in all four cases a is congruent to 0 or 1 modulo p and to 0 or 1 modulo 2^k, and hence a is one of the fixed points of $G(n)$. □

3. Component heights

Definition 3.1. For $a \in \mathbb{Z}/n\mathbb{Z}$, denote by $\mathrm{Comp}(a)$ the connected component of a in the graph $G(n)$.

Definition 3.2. For any component $\mathrm{Comp}(a)$, denote by $\mathrm{Height}(\mathrm{Comp}(a))$ the greatest distance of any point in $\mathrm{Comp}(a)$ to the unique cycle of $\mathrm{Comp}(a)$.

Theorem 3.3. *If $n = 2^k p$, then $\mathrm{Height}(\mathrm{Comp}(0)) = m$, where m is the smallest positive integer such that $2^m \geqslant k$, i.e., $m = \lceil \log_2(k) \rceil$.*

Proof. Suppose that $a \in \mathrm{Comp}(0)$. Then $a^{2^t} \equiv 0 \pmod{n}$ for some t, and obviously a is divisible by $2p$. Since all powers of a will be divisible by p, the distance of a to 0 is the smallest t such that $2^k \mid a^{2^t}$, and this is maximized when $2 \parallel a$. But then t is the smallest positive integer such that $2^t \geqslant k$, i.e., $t = m$, as desired. □

Note that for $k = 1, 2, 3, \ldots$ the corresponding sequence of heights of $\mathrm{Comp}(0)$ is $0, 1, 2, 2, 3, 3, 3, 3, 4, 4, 4, 4, 4, 4, 4, 4, \ldots$, and the heights grow logarithmically as a function of k.

Theorem 3.4. *If $n = 2^k p$, where $p = 2^l + 1$ is a Fermat prime, then* $\mathrm{Height}(\mathrm{Comp}(1)) = \max(k-2, l)$.

Proof. If $a \in \mathrm{Comp}(1)$, then $a^{2^t} \equiv 1 \pmod{n}$ for some positive integer t. It follows that a is invertible modulo n, so $a \in (\mathbb{Z}/n\mathbb{Z})^*$, and that the order of a divides 2^t. Conversely, any element $a \in (\mathbb{Z}/n\mathbb{Z})^*$ whose order is 2^t lies in the component of 1 and is a distance t from 1.

It follows that an element farthest from 1 in $\mathrm{Comp}(1)$ is an element of greatest two-power order in $(\mathbb{Z}/n\mathbb{Z})^*$.

By the (extended) Chinese Remainder Theorem,

$$(\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}/2^k\mathbb{Z})^* \times (\mathbb{Z}/p\mathbb{Z})^*, \tag{2}$$

and by the structure theorem for unit groups,

$$(\mathbb{Z}/n\mathbb{Z})^* \cong \begin{cases} Z_{2^l} & \text{when } k = 1, \\ Z_2 \times Z_{2^l} & \text{when } k = 2, \\ Z_{2^{k-2}} \times Z_2 \times Z_{2^l} & \text{when } k \geqslant 3. \end{cases} \tag{3}$$

It follows that the element of greatest two-power order in $(\mathbb{Z}/n\mathbb{Z})^*$ lies a distance l from 1 when $k - 2 \leqslant l$, and a distance $k - 2$ from 1 when $k - 2 > l$, as desired. □

Note that for $k = 1, 2, 3, \ldots$ the corresponding sequence of heights of Comp(1) is

$$\underbrace{l, l, \ldots, l,}_{l+2 \text{ times}} l+1, l+2, l+3, l+4, l+5, \ldots,$$

and, after an initial constant segment, the heights grow linearly as a function of k.

Theorem 3.5. *Suppose $n = 2^k p$, where $p = 2^l + 1$ is a Fermat prime, and set $m = \lceil \log_2(k) \rceil$. Then, using the notation of Theorem* 2.2, $\mathrm{Height}(\mathrm{Comp}(2^{\alpha l})) = \max(m, l)$.

P r o o f. Suppose that $a \in \mathrm{Comp}(2^{\alpha l})$. Then for some t, $a^{2^t} - 2^{\alpha l} \equiv 0 \pmod{n}$, and it follows that a is even. Since a is even and $2^m \geqslant k$, we know that $a^{2^{\max(m,l)}} \equiv 2^{\alpha l} \equiv 0 \pmod{2^k}$. On the other hand, $a^{2^t} \equiv 2^{\alpha l} \equiv 1 \pmod{p}$, so $a \in (\mathbb{Z}/p\mathbb{Z})^*$. Since $|(\mathbb{Z}/p\mathbb{Z})^*| = 2^l$, we know that $a^{2^l} \equiv 1 \pmod{p}$. Thus $a^{2^{\max(m,l)}} \equiv 1 \pmod{p}$. Since $a^{2^{\max(m,l)}} \equiv 2^{\alpha l} \pmod{2^k}$ and $a^{2^{\max(m,l)}} \equiv 2^{\alpha l} \pmod{p}$, we know that $a^{2^{\max(m,l)}} \equiv 2^{\alpha l} \pmod{n}$. Therefore $\mathrm{Height}(\mathrm{Comp}(2^{\alpha l})) \leqslant \max(m, l)$.

To show that $\mathrm{Height}(\mathrm{Comp}(2^{\alpha l})) = \max(m, l)$, it now suffices to find $a \in \mathrm{Comp}(2^{\alpha l})$ whose distance to $2^{\alpha l}$ is at least $\max(m, l)$. We claim that this maximal distance is attained by $a = 6$ when $l > 2$ and by $a = 2$ when $l \leqslant 2$.

By definition of m, we have $2^{m-1} < k \leqslant 2^m$. Consequently, $6^{2^m} \equiv 0 \pmod{2^k}$, while $6^{2^{m-1}} \not\equiv 0 \pmod{2^k}$. It follows that the distance from 6 to $2^{\alpha l}$ at least m.

On the other hand, if $l > 1$, we claim that 3 is a generator of the cyclic unit group $(\mathbb{Z}/p\mathbb{Z})^*$. Since $|(\mathbb{Z}/p\mathbb{Z})^*| = p - 1 = 2^l$, $(\mathbb{Z}/p\mathbb{Z})^*$ is a cyclic two group. The generators of $(\mathbb{Z}/p\mathbb{Z})^*$ are exactly those elements that are not quadratic residues modulo p. However, since p is a Fermat prime, l is a power of 2, so if $l > 1$, then $p \equiv 2^l + 1 \equiv (-1)^l + 1 \equiv 2 \pmod{3}$. Since 2 is not a quadratic residue modulo 3, quadratic reciprocity yields

$$(-1)\Big(\frac{3}{p}\Big) = \Big(\frac{p}{3}\Big)\Big(\frac{3}{p}\Big) = (-1)^{\frac{p-1}{2}\frac{3-1}{2}} = 1,$$

so $(\frac{3}{p}) = -1$. Thus 3 is not a quadratic residue modulo p, and hence 3 generates $(\mathbb{Z}/p\mathbb{Z})^*$. In particular, $3^{2^l} \equiv 1 \pmod{p}$, while $3^{2^{l-1}} \not\equiv 1 \pmod{p}$.

Now if $l > 2$, since l is a power of 2, we know $2l \mid 2^{l-1}$. It follows that $2^{2^{l-1}} \equiv 2^{2l} \equiv 1 \pmod{p}$. Therefore $6^{2^l} \equiv 1 \pmod{p}$, while $6^{2^{l-1}} \not\equiv 1 \pmod{p}$. In this case, it follows that the distance from 6 to $2^{\alpha l}$ is at least l.

We now know that the distance of 6 to $2^{\alpha l}$ is at least $\max(m, l)$ when $l > 2$.

If $l = 2$, so $p = 5$, it is easy to check that $2^{2^{l-1}} = 4 \not\equiv 1 \pmod{5}$, while $2^{2^l} \equiv 1 \pmod{5}$. Obviously, $2^{2^{m-1}} \not\equiv 0 \pmod{2^k}$, while $2^{2^m} \equiv 0 \pmod{2^k}$. Therefore 2 is a distance at least $\max(m, l)$ to $2^{\alpha l}$.

Finally, if $l = 1$, then $p = 3$ and $2^{2^{l-1}} \equiv 2 \not\equiv 0 \pmod 3$, while $2^{2^l} \equiv 4 \equiv 1 \pmod 3$. Again, $2^{2^{m-1}} \not\equiv 0 \pmod{2^k}$, while $2^{2^m} \equiv 0 \pmod{2^k}$. Therefore 2 is a distance at least $\max(m, l)$ to $2^{\alpha l}$.

Having found the desired element a, we now conclude that $\mathrm{Height}(\mathrm{Comp}(2^{\alpha l})) = \max(m, l)$. □

Corollary 3.6. *If $n = 2^k p$, where $p = 2^l + 1$ is a Fermat prime, then*

$$\mathrm{Height}(\mathrm{Comp}(2^{\alpha l})) = \mathrm{Height}(\mathrm{Comp}(0)) \quad \textit{exactly when } m \geqslant l.$$

In particular,

$$\mathrm{Height}(\mathrm{Comp}(2^{\alpha l})) = \mathrm{Height}(\mathrm{Comp}(0)) \quad \textit{when } k > 2^{l-1} = (p-1)/2.$$

P r o o f. The first statement follows immediately from Theorem 3.3 and Theorem 3.5. Clearly, if $k > 2^{l-1}$, then $2^m \geqslant k > 2^{l-1}$, so $m \geqslant l$. Conversely, if $m \geqslant l$, then $m - 1 \geqslant l - 1$. Since $k > 2^{m-1}$, it follows that $k > 2^{l-1}$, as desired. □

Theorem 3.7. *Suppose $n = 2^k p$, where $p = 2^l + 1$ is a Fermat prime. Then, using the notation of Theorem 2.2,*

$$\mathrm{Height}(\mathrm{Comp}(2^{\beta l} + 1)) = \begin{cases} 0 & \textit{if } k = 1, \\ 1 & \textit{if } k = 2, \textit{ and} \\ k - 2 & \textit{if } k > 2. \end{cases}$$

P r o o f. Suppose that $a \in \mathrm{Comp}(2^{\beta l} + 1)$. Then for some t, $a^{2^t} \equiv 2^{\beta l} + 1 \equiv 1 \pmod{2^k}$ and $a^{2^t} \equiv 2^{\beta l} + 1 \equiv 0 \pmod p$. Clearly a is divisible by p and a is invertible modulo 2^k. Since 2^0, 2^1, and 2^{k-2} are, respectively, the greatest order of an element of $(\mathbb{Z}/2^k\mathbb{Z})^*$ when $k = 1$, 2, and $k > 2$, it follows that $a^1 \equiv 2^{\beta l} + 1 \pmod n$ when $k = 1$, $a^{2^2} \equiv 2^{\beta l} + 1 \pmod n$ when $k = 2$, and $a^{2^{k-2}} \equiv 2^{\beta l} + 1 \pmod n$ when $k > 2$. It follows that $\mathrm{Height}(\mathrm{Comp}(2^{\beta l+1})) \leqslant 1$, 2, and $k - 2$, respectively, when $k = 1$, 2, and $k > 2$.

It remains to identify elements $a \in \mathrm{Comp}(2^{\beta l+1})$ that attain the maximal distance to $2^{\beta l} + 1$.

Choose any s of maximal order t in $(\mathbb{Z}/2^k\mathbb{Z})^*$. Thus $t = 2^0$, 2^1, or 2^{k-2}, respectively, as $k = 1$, $k = 2$, or $k > 2$. By the Chinese Remainder Theorem, there is a unique a modulo n such that $a \equiv s \pmod{2^k}$ and $a \equiv 0 \pmod p$. Clearly a has the desired maximal order t modulo 2^k, so $a^t \equiv 1 \pmod{2^k}$ and, since a is divisible by p, $a^t \equiv 0 \pmod p$. It follows that $a^t \equiv 2^{\beta l} + 1 \pmod n$ and $a \in \mathrm{Comp}(2^{\beta l} + 1)$, a distance at most t from $2^{\beta l} + 1$. On the other hand, $a^{t-1} \not\equiv 1 \pmod{2^k}$, so the distance from a to $2^{\beta l} + 1$ is exactly t, as desired. □

Corollary 3.8. *If $n = 2^k p$, where $p = 2^l + 1$ is a Fermat prime, then*

$$\text{Height}(\text{Comp}(2^{\beta l} + 1)) = \text{Height}(\text{Comp}(1)) \quad \textit{when } k - 2 \geqslant l,$$

and also when $p = 3$ and $k = 2$.

P r o o f. The result follows immediately from Theorem 3.4 and Theorem 3.7. □

4. Weak symmetry

Definition 4.1. The graph $G(n)$ is said to be *symmetric* if the connected components can be partitioned into isomorphic pairs.

In order to study symmetry, we define a weaker notion, which we call *weak symmetry*.

Definition 4.2. The graph $G(n)$ is said to be *weakly symmetric* if the connected components can be partitioned into pairs such that there is a bijection of the form $\tau(a) = a + \varepsilon$, between paired components. When there exists such a bijection between components $\text{Comp}(a)$ and $\text{Comp}(b)$ we write $\text{Comp}(a) \sim \text{Comp}(b)$.

It is a consequence of weak symmetry that paired components have the same cardinality, but they may fail to have the same graph topology.

Theorem 4.3. *If $n = 2^k p$, where $p = 2^l + 1$ is a Fermat prime, then $G(n)$ is weakly symmetric. In particular, using the notation of Theorem* 2.2*,*

$$\text{Comp}(0) \sim \text{Comp}(2^{\beta l} + 1) \quad \textit{and} \quad \text{Comp}(1) \sim \text{Comp}(2^{\alpha l}).$$

P r o o f. First, to show that $\text{Comp}(0) \sim \text{Comp}(2^{\beta l} + 1)$, define $\tau(a) = a + 2^{\beta l} + 1$. To prove that τ is the desired bijection, we will show that $\tau(a) \in \text{Comp}(2^{\beta l} + 1)$ if and only if $a \in \text{Comp}(0)$.

Suppose that $a \in \text{Comp}(0)$. Then by Theorem 3.3, $a^{2^m} \equiv 0 \pmod{n}$, where as usual $m = \lceil \log_2(k) \rceil$. In particular, $a \equiv 0 \pmod{p}$. Since $2^{\beta l} + 1 \equiv 0 \pmod{p}$ as well, $\tau(a) \equiv 0 \pmod{p}$. We also note that a is even. Since $\beta l \geqslant k$,

$$\tau(a)^{2^{k-1}} = (a + 2^{\beta l} + 1)^{2^{k-1}} \equiv (a + 1)^{2^{k-1}} \pmod{2^k}.$$

A simple induction starting with $(a+1) \equiv 1 \pmod{2}$ yields $(a+1)^{2^{k-1}} \equiv 1 \pmod{2^k}$, and hence

$$\tau(a)^{2^{k-1}} \equiv 1 \pmod{2^k}.$$

Since $\tau(a)^{2^{k-1}} \equiv 2^{\beta l}+1 \equiv 0 \pmod{p}$ and $\tau(a)^{2^{k-1}} \equiv 2^{\beta l}+1 \equiv 1 \pmod{2^k}$, it follows that $\tau(a)^{2^{k-1}} \equiv 2^{\beta l}+1 \pmod{n}$, and therefore $\tau(a) \in \mathrm{Comp}(2^{\beta l}+1)$, as desired.

Conversely, suppose that $\tau(a) \in \mathrm{Comp}(2^{\beta l}+1)$. Then, by Theorem 3.7, $(a+2^{\beta l}+1)^{2^{k-1}} \equiv 2^{\beta l}+1 \pmod{n}$. In particular, $(a+2^{\beta l}+1)^{2^{k-1}} \equiv 2^{\beta l}+1 \equiv 0 \pmod{p}$. Since $2^{\beta l}+1 \equiv 0 \pmod{p}$, it follows that $a^{2^{k-1}} \equiv 0 \pmod{p}$, and hence $a \equiv 0 \pmod{p}$. Similarly, $(a+2^{\beta l}+1)^{2^{k-1}} \equiv 1 \pmod{2^k}$. Since $2^{\beta l}+1 \equiv 1 \pmod{2^k}$, we conclude that $(a+1)^{2^{k-1}} \equiv 1 \pmod{2^k}$. It follows that a is even, and hence $a^{2^m} \equiv 0 \pmod{2^k}$. But now $a^{2^m} \equiv 0 \pmod{n}$ and $a \in \mathrm{Comp}(0)$, as desired. This proves that $\mathrm{Comp}(0) \sim \mathrm{Comp}(2^{\beta l}+1)$.

Next, to show that $\mathrm{Comp}(1) \sim \mathrm{Comp}(2^{\alpha l})$, define $\tau(a) = a + 2^{\alpha l} - 1$. Suppose that $a \in \mathrm{Comp}(1)$. Then $a^{2^t} \equiv 1 \pmod{n}$ for some t. Therefore $a^{2^t} \equiv 1 \pmod{p}$ and $a^{2^t} \equiv 1 \pmod{2^k}$. Since $a^{2^t} \equiv 1 \pmod{p}$, we know that a is not divisible by p. But $2^{\alpha l} - 1 \equiv 0 \pmod{p}$, so $\tau(a) = a + 2^{\alpha l} - 1$ is not divisible by p. It follows that $\tau(a) \in (\mathbb{Z}/p\mathbb{Z})^*$, and hence $(\tau(a))^{2^l} \equiv 1 \pmod{p}$. On the other hand, since $a^{2^t} \equiv 1 \pmod{2^k}$, we know that a is odd. Therefore $\tau(a) = a + 2^{\alpha l} - 1$ is even. Consequently $(\tau(a))^{2^k} \equiv 0 \pmod{2^k}$. We now conclude that $(\tau(a))^{\max(2^l,2^k)} \equiv 2^{\alpha l} \pmod{n}$, and hence $\tau(a) \in \mathrm{Comp}(2^{\alpha l})$.

Conversely, suppose that $\tau(a) \in \mathrm{Comp}(2^{\alpha l})$. Then $(\tau(a))^{2^t} \equiv 2^{\alpha l} \pmod{n}$, for some t. It follows that $(\tau(a))^{2^t} \equiv 1 \pmod{p}$ and $(\tau(a))^{2^t} \equiv 0 \pmod{2^k}$. The first of these congruences implies that $\tau(a)$ is not divisible by p. Since $\tau(a) = a + 2^{\alpha l} - 1$ and $2^{\alpha l} - 1 \equiv 0 \pmod{p}$, it follows that a is not divisible by p. Therefore $a \in (\mathbb{Z}/p\mathbb{Z})^*$ and $a^{2^l} \equiv 1 \pmod{p}$. The second congruence implies that $\tau(a)$ is even. But then a is odd. Consequently $a \in (\mathbb{Z}/2^k\mathbb{Z})^*$, so $a^{2^k} \equiv 1 \pmod{2^k}$. It follows that $a^{\max(2^l,2^k)} \equiv 1 \pmod{n}$, so $a \in \mathrm{Comp}(1)$, as desired. □

Theorem 4.4. *If $n = 2^k p$, where $p = 2^l + 1$ is a Fermat prime, then, using the notation of Theorem* 2.2,

$$|\mathrm{Comp}(0)| = |\mathrm{Comp}(2^{\beta l}+1)| = 2^{k-1}$$

and

$$|\mathrm{Comp}(1)| = |\mathrm{Comp}(2^{\alpha l})| = 2^{k-1}(p-1).$$

P r o o f. It is easy to see that $a \in \mathrm{Comp}(0)$ if and only if a is even and divisible by p. Clearly $\mathbb{Z}/n\mathbb{Z}$ contains 2^k multiples of p, of which 2^{k-1} are even. Therefore $|\mathrm{Comp}(0)| = 2^{k-1}$. By Theorem 4.3, $\mathrm{Comp}(0) \sim \mathrm{Comp}(2^{\beta l}+1)$, which implies that $|\mathrm{Comp}(0)| = |\mathrm{Comp}(2^{\beta l}+1)|$.

Similarly, the elements of $\mathrm{Comp}(1)$ are invertible elements of $\mathbb{Z}/n\mathbb{Z}$ that have 2-power order. Thus the elements of $\mathrm{Comp}(1)$ are just those integers belonging

to the Sylow 2-subgroup of the unit group $(\mathbb{Z}/n\mathbb{Z})^*$. Since p is a Fermat prime, $|(\mathbb{Z}/p\mathbb{Z})^*| = p - 1 = 2^l$ is a power of two, and we conclude that $|\mathrm{Comp}(1)| = |(\mathbb{Z}/n\mathbb{Z})^*|_2 = 2^{k-1}(p-1)$. Since Theorem 4.3 implies that $\mathrm{Comp}(1) \sim \mathrm{Comp}(2^{\alpha l})$, we conclude that $|\mathrm{Comp}(1)| = |\mathrm{Comp}(2^{\alpha l})|$, as desired. □

5. Symmetry

It is known [6] that the iteration graph $G(n)$ is symmetric when $n \equiv 2 \pmod 4$ and when $n \equiv 4 \pmod 8$. However, beyond these two infinite families of graphs, symmetry seems to be quite rare. In this section we offer a characterization of the symmetry of the graphs $G(n)$ for $n = 2^k p$, where p is a Fermat prime, by applying the invariants described in the previous sections. In particular, we show that for each Fermat prime p, the graphs $G(n)$ fail to be symmetric when $k = 3$ and when $k > 5$. Thus, each Fermat prime contributes an infinite family of nonsymmetric iteration graphs.

Our argument is motivated by the observation that the heights of two components, $\mathrm{Comp}(0)$ and $\mathrm{Comp}(2^{\alpha l})$ increase logarithmically, while the heights of the other two components $\mathrm{Comp}(1)$ and $\mathrm{Comp}(2^{\beta l} + 1)$ increase linearly as a function of k. Thus, for large k the heights must differ, and components from the two groups cannot be isomorphic. However, within the two groups, the cardinalities differ, again preventing isomorphism. Our asymptotic argument works for all $k \geqslant 6$, and specific comparison of component heights also provides a proof when $k = 3$. When $k = 5$, all components may have the same height, and an *ad hoc* argument must be applied.

As remarked above, it is known that $G(n)$ is symmetric when $k = 1$ and when $k = 2$. To this list we add the case $k = 4$. Thus, each Fermat prime p, contributes an iteration graph $G(n) = G(16p)$ that is symmetric. We offer no opinion as to whether this provides an infinite family of symmetric graphs. We suspect, however, that the methods we apply here may be modified to work for integers n that are not of the from $2^k p$. In a future paper we intend to investigate conditions under which graphs $G(n)$ for which $n \equiv 16 \pmod{32}$ are symmetric.

Theorem 5.1. *Suppose $n = 2^k p$, where $p = 2^l + 1$ is a Fermat prime. Then the iteration graph $G(n)$ is not symmetric when $k = 3$ and when $k \geqslant 6$.*

Proof. If $G(n)$ is symmetric, $\mathrm{Comp}(0)$ must be isomorphic to one of the other three components. Since isomorphic components have the same cardinality, and $2^{k-1} \neq 2^{k-1}(p-1)$, Theorem 4.4 implies that $\mathrm{Comp}(0)$ is not isomorphic to $\mathrm{Comp}(1)$ or to $\mathrm{Comp}(2^{\alpha l})$. However, isomorphic components must also have the same height. By Theorem 3.3, $\mathrm{Height}(\mathrm{Comp}(0)) = m = \lceil \log_2(k) \rceil$ and, by Theorem 3.7,

Height(Comp($2^{\beta l}+1$) $= k-2$ when $k > 2$. It is an easy exercise in calculus to verify that $k-2 > m$ when $k \geqslant 6$. Furthermore, when $k = 3$ we obtain $k-2 = 1 \neq 2 = \lceil \log_2(3) \rceil$. It follows that Comp(0) is not isomorphic to Comp($2^{\beta l}+1$) when $k = 3$ and when $k \geqslant 6$. We conclude that Comp(0) is not isomorphic to any of the other three components, and therefore $G(n)$ is not symmetric, when $k = 3$ and when $k \geqslant 6$. □

Since it is known that $G(n)$ is symmetric when $k = 1$ and $k = 2$, Theorem 5.1 leaves open two cases: $k = 4$ and $k = 5$. In our last two theorems we show that $G(n)$ is symmetric when $k = 4$ and is not symmetric when $k = 5$.

Theorem 5.2. *Suppose $n = 2^k p$, where $p = 2^l + 1$ is a Fermat prime. Then the iteration graph $G(n)$ is not symmetric when $k = 5$.*

P r o o f. As in the proof of Theorem 5.1, Comp(0) cannot be isomorphic to Comp(1) or to Comp($2^{\alpha l}$), so it suffices to show that Comp(0) is also not isomorphic to Comp($2^{\beta l}+1$).

By Theorem 3.3 and Theorem 3.7, we see that Height(Comp(0)) $= m = 3$ and Height(Comp($2^{\beta l}+1$)) $= k-2 = 3$, so both components have height 3. Let $A \subset$ Comp(0) be the set of elements whose distance from 0 is equal to 3 and $B \subset$ Comp($2^{\beta l}+1$) the set of elements whose distance from $2^{\beta l}+1$ is 3. An isomorphism between Comp(0) and Comp($2^{\beta l}+1$) must induce a bijection between A and B.

Clearly, if $a \in A$, then $a^8 \equiv 0 \pmod{n}$ while $a^4 \not\equiv 0 \pmod{n}$. It follows that $a = 2ps$ for some odd s. Now, if $2ps$ and $2pt$ are two elements of A, then we claim that $(2ps)^2 \equiv (2pt)^2 \pmod{n}$. Clearly, $(2pt)^2 - (2ps)^2 = 4(t^2-s^2)p^2 \equiv 0 \pmod{p}$. Moreover, $t^2 - s^2 \equiv 0 \pmod{8}$, because 1 is the only square of an odd integer modulo 8, so $4(t^2-s^2)p^2 \equiv 0 \pmod{32}$. Thus $(2ps)^2 \equiv (2pt)^2 \pmod{n}$, as desired. It follows that any two elements of A connect to the same element of $G(n)$.

By the Chinese Remainder Theorem, for each integer s of order 8 in the unit group $(\mathbb{Z}/32\mathbb{Z})^*$ there is a unique $b \in \mathbb{Z}/n\mathbb{Z}$ such that $b \equiv 0 \pmod{p}$ and $b \equiv s \pmod{32}$. Clearly each b chosen in this way belongs to B. Since 3 and 5 have order 8 modulo 32, we can find a and $b \in B$ with $a \equiv 3 \pmod{32}$ and $b \equiv 5 \pmod{32}$. But then $b^2 - a^2 \equiv 25 - 9 \equiv 16 \pmod{32}$. Consequently, $a^2 \not\equiv b^2 \pmod{n}$, and hence a and b connect to distinct elements of $G(n)$.

It now follows that no bijection from Comp(0) to Comp($2^{\beta l}+1$) can preserve the graph topology of $G(n)$. Therefore Comp(0) is not isomorphic to Comp($2^{\beta l}+1$), and the graph $G(n)$ is not symmetric. □

Theorem 5.3. *Suppose $n = 2^k p$, where $p = 2^l + 1$ is a Fermat prime. Then the iteration graph $G(n)$ is symmetric when $k = 4$.*

P r o o f. To show that $G(n)$ is symmetric, we prove that $\mathrm{Comp}(0) \cong \mathrm{Comp}(2^{\beta l} + 1)$ and $\mathrm{Comp}(1) \cong \mathrm{Comp}(2^{\alpha l})$.

By Theorem 4.4, $|\mathrm{Comp}(0)| = |\mathrm{Comp}(2^{\beta l} + 1)| = 8$ and, by Theorem 3.3 and Theorem 3.7, $\mathrm{Height}(\mathrm{Comp}(0)) = \mathrm{Height}(\mathrm{Comp}(2^{\beta l} + 1)) = 2$. As in the proof of Theorem 5.2, the elements of $\mathrm{Comp}(0)$ that lie a maximal distance from 0 have the form $2ps$ for odd s. In particular, there are four such elements: $2p$, $6p$, $10p$, and $14p$. Each of these elements satisfies $(2ps)^2 = 4p^2s^2 \equiv 0 \pmod p$ and $(2ps)^2 = 4p^2s^2 \equiv 4p^2 \pmod{16}$, so in $G(n)$ they connect to the same element $4p^2$. The elements a distance one from 0 have the form $4p^2s$ or $8p^2s$ for odd s. There are exactly three of them: $4p^2$, $8p^2$, and $12p^2$.

Also as in the proof of Theorem 3.7, the elements of $\mathrm{Comp}(2^{\beta l} + 1)$ that lie a maximal distance from $2^{\beta l} + 1$ are divisible by p and congruent to an element of maximal order 4 in $(\mathbb{Z}/16\mathbb{Z})^*$. Since $(\mathbb{Z}/16\mathbb{Z})^*$ has four elements of order 4, namely 3, 5, 11, and 13, exactly four elements lie a distance two from $2^{\beta l} + 1$. In particular, since $p = 2^l + 1$ with $l \geqslant 1$, it follows that $p^4 = (2^l+1)^4 = 2^{4l} + 4{\cdot}2^{3l} + 6{\cdot}2^{2l} + 4{\cdot}2^l + 1 \equiv 1 \pmod{16}$, so we can write these four elements as $3p^4$, $5p^4$, $11p^4$, and $13p^4$. Since each of these elements has square congruent to 9 modulo 16 and 0 modulo p, they all connect to the same element in $G(n)$. In particular, they all connect to $9p^4$. The elements a distance one from $2^{\beta l} + 1$ are divisible by p and congruent to an element of order 2 in $(\mathbb{Z}/16\mathbb{Z})^*$. The elements of order two in $(\mathbb{Z}/16\mathbb{Z})^*$ are 7, 9, and 15, so the elements a distance one from $2^{\beta l} + 1$ are $7p^4$, $9p^4$, and $15p^4$. Note that $2^{\beta l} + 1 \equiv 1 \pmod{16}$ and $2^{\beta l} + 1 \equiv 0 \pmod p$, so $2^{\beta l} + 1 \equiv p^4 \pmod n$.

It follows that the map $\tau\colon \mathrm{Comp}(0) \to \mathrm{Comp}(2^{\beta l} + 1)$ defined by

$$2p \mapsto 3p^4 \quad 6p \mapsto 5p^4, \quad 10p \mapsto 11p^4, \quad 14p \mapsto 13p^4,$$
$$4p^2 \mapsto 9p^4, \quad 8p^2 \mapsto 7p^4, \quad 12p^2 \mapsto 15p^4, \quad 0 \mapsto p^4$$

is an isomorphism.

Next we consider the structure of $\mathrm{Comp}(1)$ and $\mathrm{Comp}(2^{\alpha l})$. As noted in the proof of Theorem 3.4, the elements of $\mathrm{Comp}(1)$ belong to the Sylow 2-subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$, which is isomorphic to $Z_4 \times Z_2 \times Z_{2^l}$.

From the analysis in Theorem 3.5 it is evident that the elements of $\mathrm{Comp}(2^{\alpha l})$ are congruent to 0 (mod 2) and are relatively prime to p. Under the natural multiplication in $\mathbb{Z}/n\mathbb{Z}$, the elements of $\mathrm{Comp}(2^{\alpha l})$ do not form a group. We will introduce a new operation $*$ on $\mathrm{Comp}(2^{\alpha l})$ which coincides with squaring in $\mathbb{Z}/n\mathbb{Z}$ and under which $\mathrm{Comp}(2^{\alpha l})$ forms a group isomorphic to $Z_4 \times Z_2 \times Z_{2^l}$. It will then follow that $\mathrm{Comp}(2^{\alpha l}) \cong \mathrm{Comp}(1)$, as desired.

To begin, we identify each of the eight even integers $\hat{a} \in \{0, 2, 4, 6, 8, 10, 12, 14\}$ with a corresponding element $\sigma(\hat{a}) \in \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ as follows:

$$\begin{array}{cccc} \sigma(0) = (0,0), & \sigma(2) = (1,0), & \sigma(4) = (2,0), & \sigma(6) = (3,0), \\ \sigma(8) = (0,1), & \sigma(10) = (1,1), & \sigma(12) = (2,1), & \sigma(14) = (3,1). \end{array}$$

We now associate each element $a \in \mathrm{Comp}(2^{\alpha l})$ with an element $\tau(a) \in Z_4 \times Z_2 \times Z_{2^l}$ by setting $\tau(a) = (\sigma(\hat{a}), \bar{a})$, where $\hat{a}$ is the natural image of a in $\mathbb{Z}/16\mathbb{Z}$ and $\bar{a}$ is the natural image of a in $(\mathbb{Z}/p\mathbb{Z})^* \cong Z_{2^l}$. Note that we have written the first two components of $Z_4 \times Z_2 \times Z_{2^l}$ additively and the third component multiplicatively, so $\tau(a)\tau(b) = (\sigma(\hat{a}) + \sigma(\hat{b}), \bar{a}\bar{b})$.

The map τ is easily seen to be a bijection. By the Chinese Remainder Theorem, each element of $\mathrm{Comp}(2^{\alpha l})$ is uniquely determined by its residues modulo 16 and p. Conversely, via the identification τ, each element of $Z_4 \times Z_2 \times Z_{2^l}$ corresponds to a unique residue modulo n that is even and relatively prime to p.

Since τ is a bijection, we can use τ to induce a multiplication $*$ on $\mathrm{Comp}(2^{\alpha l})$ by setting $a * b = \tau^{-1}(\tau(a)\tau(b))$, and it is immediate that under this induced multiplication $\mathrm{Comp}(2^{\alpha l})$ is isomorphic as a group to $Z_4 \times Z_2 \times Z_{2^l}$.

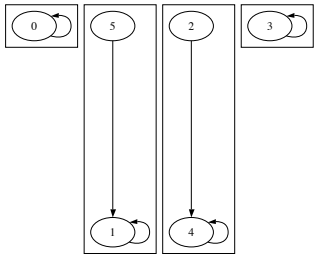
It remains to show that squaring under the induced multiplication $*$ coincides with the standard squaring operation in $\mathrm{Comp}(2^{\alpha l})$. Clearly, if $a, b \in \mathrm{Comp}(2^{\alpha l})$, $\bar{a}\bar{b} = \overline{ab}$, so $\bar{a}^2 = \overline{a^2}$. On the other hand, note that $\sigma(\hat{a}) + \sigma(\hat{a}) = (0,0)$ when $\hat{a} \in \{0, 4, 8, 12\}$, i.e., when $a \equiv 0 \pmod 4$ and $\sigma(\hat{a}) + \sigma(\hat{a}) = (2,0)$ when $\hat{a} \in \{2, 6, 10, 14\}$, i.e., when $a \equiv 2 \pmod 4$. However, if $a \in \mathrm{Comp}(2^{\alpha l})$ and $a \equiv 0 \pmod 4$, then certainly $a^2 \equiv 0 \pmod{16}$, so $\sigma(\widehat{a^2}) = (0,0) = \sigma(\hat{a}) + \sigma(\hat{a})$ and if $a \equiv 2 \bmod 4$, then $a^2 \equiv 4 \pmod{16}$, so $\sigma(\widehat{a^2}) = (2,0) = \sigma(\hat{a}) + \sigma(\hat{a})$.

It now follows that the graphs $\mathrm{Comp}(1)$ and $\mathrm{Comp}(2^{\alpha l})$ are both isomorphic to the graph of the group $Z_4 \times Z_2 \times Z_{2^l}$, and are hence isomorphic to each other.

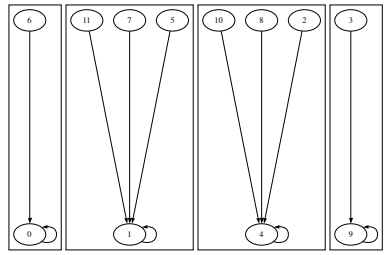
We have now shown that $\mathrm{Comp}(0) \cong \mathrm{Comp}(2^{\beta l} + 1)$ and $\mathrm{Comp}(1) \cong \mathrm{Comp}(2^{\alpha l})$, and hence $G(n)$ is symmetric. □

6. Diagrams

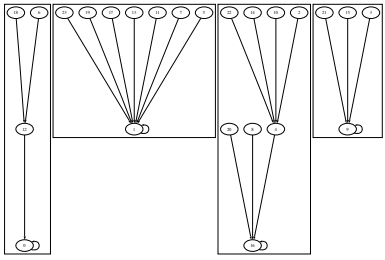
The following twelve diagrams, constructed with the aid of the computational mathematics package Gap [4] and displayed using the Graphviz visualization tool [3] display the iteration graphs $G(3 \cdot 2^k)$ and $G(5 \cdot 2^k)$ for $1 \leqslant k \leqslant 6$.



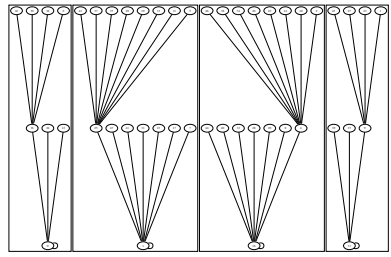
$G(6)$



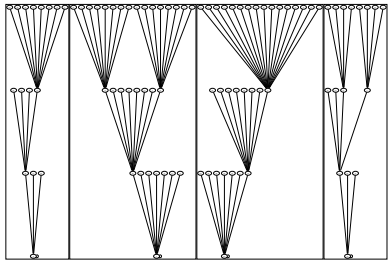
$G(12)$



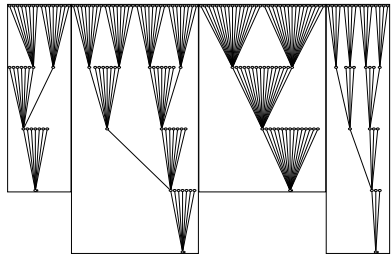
$G(24)$



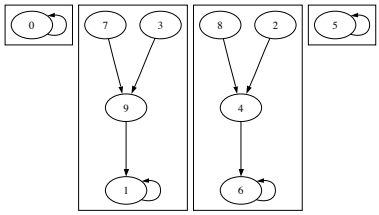
$G(48)$



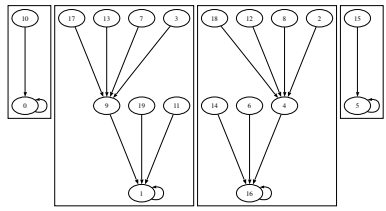
$G(96)$



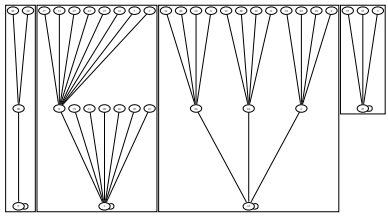
$G(192)$



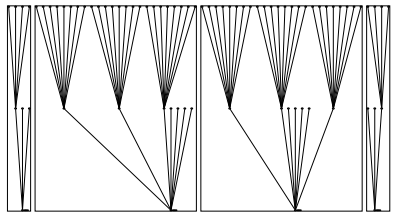
$G(10)$



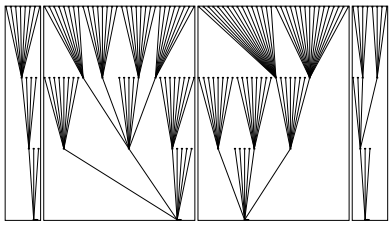
$G(20)$



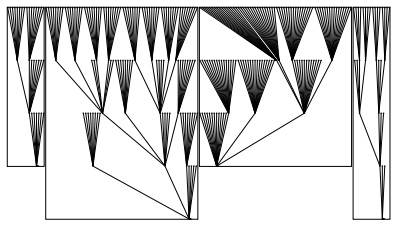
$G(40)$



$G(80)$



$G(160)$



$G(320)$

References

[1] *Earle L. Blanton, Jr., Spencer P. Hurd and Judson S. McCranie*: On a digraph defined by squaring modulo n. Fibonacci Quart. *30* (1992), 322–334. zbl

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

[3] *John Ellson, Emden Gansner, Lefteris Koutsofios, Stephen C. North and Gordon Woodhull*: Graphviz-open source graph drawing tools. Graph drawing (Petra Mutzel, Michael Jünger, and Sebastian Leipert, eds.), Lecture Notes in Computer Science, vol. 2265, Springer-Verlag, Berlin, 2002, Selected papers from the 9th International Symposium (GD 2001) held in Vienna, September 23–26, 2001, pp. 483–484. (In English.) zbl

[4] The GAP Group, Gap-groups, algorithms, and programming, version 4.4, 2005, (http://www.gap-system.org).
[5] *Thomas D. Rogers*: The graph of the square mapping on the prime fields. Discrete Math. *148* (1996), 317–324. zbl
[6] *Lawrence Somer and Michal Křížek*: On a connection of number theory with graph theory. Czechoslovak Math. J. *54* (2004), 465–485. zbl
[7] *L. Szalay*: A discrete iteration in number theory. BDTF Tud. Közl. *8* (1992), 71–91. zbl
[8] *Troy Vasiga and Jeffrey Shallit*: On the iteration of certain quadratic maps over GF(p). Discrete Math. *277* (2004), 219–240. zbl

Authors' addresses: Walter Carlip, Department of Mathematics, Franklin & Marshall College, Lancaster, Pennsylvania 17604, USA, e-mail: c3ar@math.uchicago.edu; Martina Mincheva, Department of Mathematics, Franklin & Marshall College, Lancaster, Pennsylvania 17604, USA.