Michal Křížek; Lawrence Somer

Sophie Germain little suns

Mathematica Slovaca, Vol. 54 (2004), No. 5, 433--442

Persistent URL: http://dml.cz/dmlcz/129574

Mathematica Slovaca
© 2004
Mathematical Institute
Slovak Academy of Sciences

Math. Slovaca, **54** (2004), No. 5, 433–442

SOPHIE GERMAIN LITTLE SUNS

MICHAL KŘÍŽEK* — LAWRENCE SOMER**

(*Communicated by Stanislav Jakubec*)

ABSTRACT. We assign to each positive integer n a digraph whose set of vertices is $H = \{0, 1, \ldots, n-1\}$ and for which there is a directed edge from $a \in H$ to $b \in H$ if $a^2 \equiv b \pmod{n}$. We show that this digraph has an interesting structure for $n = 2p+1$, where p is a Sophie Germain prime. Namely, in this case its nontrivial components look like little suns. Making use of the Carmichael function, we prove that the number of little suns is equal to $(p-1)/s$, where s is the multiplicative order of 2 modulo p. We also present a new relationship between Mersenne and Sophie Germain primes.

1. Introduction

In 1819, a French mathematician Sophie Germain demonstrated that if p and $2p+1$ are both prime, then the so-called first case of Fermat's Last Theorem holds for the exponent p. Odd primes p for which $2p+1$ is also a prime are thus called *Sophie Germain primes*. These primes have a number of interesting properties. For instance, in [8] we observe that all quadratic nonresidues are primitive roots modulo $2p+1$, where p is a Sophie Germain prime, except for exactly one number $2p$, which is a quadratic nonresidue, but not a primitive root.

Another well-known property can be stated as follows. Let p be a prime such that $p \equiv 3 \pmod 4$. Then $2p+1$ divides the Mersenne number $2^p - 1$ if and only if $2p+1$ is prime (see, e.g., [7; p. 214]). It is not known whether the number of Sophie Germain primes is finite or infinite. However, if there would be infinitely many Sophie Germain primes for which $p \equiv 3 \pmod 4$, then there would be also infinitely many composite Mersenne numbers, since $2p+1$ divides $2^p - 1$.

2000 Mathematics Subject Classification: Primary 11A07, 05C20, 20K01.
Keywords: Sophie Germain prime, Fermat prime, Mersenne prime, Chinese remainder theorem, primality, digraph.

This paper was supported by grant A 1019201 of the Grant Agency of the Academy of Sciences of the Czech Republic.

Conjecturally, for large x the number of integers $n \leq x$ such that both n and $(n-1)/2$ are primes is $\big(1+o(1)\big)Dx/\log^2 x$, where $D \cong 0.6601618\ldots$. An upper bound of this order of magnitude is known by B r u n 's work (see [6] and also [2]). If this is true, then by the recent paper [1] there exists a sixth-degree polynomial deterministic algorithm for testing the primality of a given integer number.

Here, for each positive integer n, we construct a directed graph (digraph) $G(n)$ whose vertices are $0, 1, 2, \ldots, n-1$. In particular, we will see that when p is a Sophie Germain prime, then $G(2p+1)$ has a particularly beautiful structure.

For $n \geq 1$ let

$$H = \{0, 1, \ldots, n-1\}$$

and let f be a map of H into itself. The *iteration digraph* of f is a directed graph whose vertices are elements of H and such that there exists exactly one directed edge from x to $f(x)$ for all $x \in H$. For each $x \in H$ let $f(x)$ be the remainder of x^2 modulo n, i.e.,

$$f(x) \in H \qquad \text{and} \qquad x^2 \equiv f(x) \pmod{n}. \tag{1.1}$$

From here on, whenever we refer to the iteration digraph of f, we assume that the mapping f is as given in (1.1). (A connection of Sophie Germain primes with more general polynomial mappings is given in [9; p. 235].)

Each natural number has a specific iteration digraph corresponding to it. For instance, S z a l a y in [13] investigated properties of iteration digraphs corresponding to Fermat primes, i.e., the primes of the form $n = 2^{2^m} + 1$ for $m = 0, 1, \ldots$. He showed that the associated digraphs have always a special binary structure (cf. Figure 1). This result was independently discovered in [11]. Further connections between number theory and graph theory are also examined in [3] [5], [7] [12].

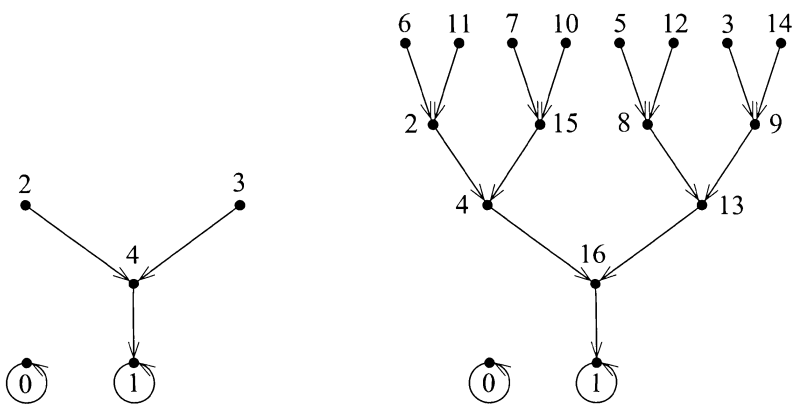

FIGURE 1. Iteration digraphs corresponding to the Fermat primes $n = 5$ and $n = 17$.

In this paper, we shall see that iteration digraphs corresponding to $n = 2p+1$, where p is a Sophie Germain prime, have particular structural characteristics. Namely, we prove that their "nontrivial" components are identical and resemble little suns (or ship wheels according to [11; p. 323]), compare with Figures 2, 3, and 4.

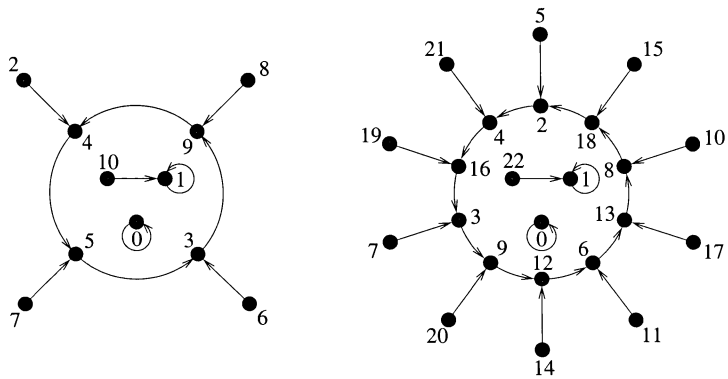

FIGURE 2. Iteration digraphs corresponding to $n = 11$ and $n = 23$.

2. Discrete iteration

Starting with an arbitrary element x_0 from H, we define the sequence of successive elements of H by

$$x_{j+1} = f(x_j), \qquad j = 0, 1, \ldots,$$

where f is given by (1.1). This iteration scheme is called a *discrete iteration*. Since H is finite, the sequence $\{x_j\}$ has to be cyclic starting from some element x_k. If $x_k, x_{k+1}, \ldots, x_\ell$ are pairwise distinct and

$$\begin{aligned} x_{k+1} &= f(x_k), \\ &\vdots \\ x_\ell &= f(x_{\ell-1}), \\ x_k &= f(x_\ell), \end{aligned}$$

then the elements $x_k, x_{k+1}, \ldots, x_\ell$ constitute a *cycle* of length $\ell - k + 1$. Let us call a cycle of length 1 a *fixed point*. The cycles of length t are called *t-cycles*. Cycles are assumed to be oriented counterclockwise (see Figures 2 and 3).

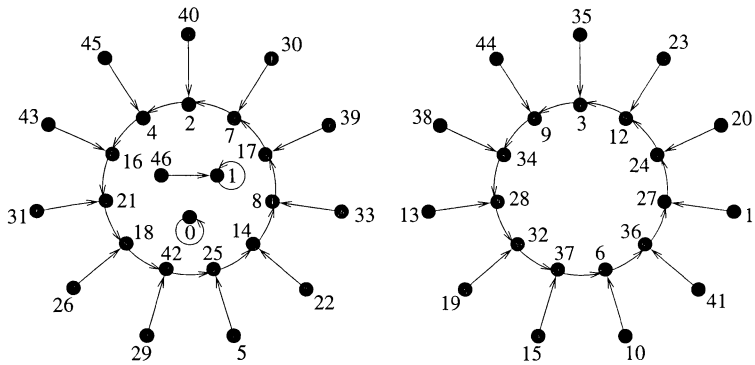

FIGURE 3. Iteration digraph corresponding to $n = 47$.

We identify the vertex a of H with residues modulo n. For brevity we will make statements such as $\gcd(a, n) = 1$, treating the vertex a as a number. Moreover, when we refer, for instance, to the vertex a^2, we identify it with the remainder $f(a)$ given by (1.1).

For a particular value of n, we denote the iteration digraph of f by $G(n)$. We investigate the structure of $G(n)$ in [12]. Also R o g e r s [11] describes completely the structure of each component of $G(n)$ when n is prime.

Let $\omega(n)$ stand for the number of distinct primes dividing n. By [13] the number of fixed points of $G(n)$ is equal to $2^{\omega(n)}$. This leads to the following corollary (cf. Figures 1 and 2).

COROLLARY 2.1. *If n is prime, then there exist exactly two fixed points, namely 0 and 1.*

3. Structure of iteration digraphs

A *component* of the iteration digraph is a subdiagraph which is a maximal connected subgraph of the symmetrization of this digraph (i.e., the associated nondirected graph). In [12], we showed that each component has exactly one cycle (which is a general property of the iteration graph of any mapping $f\colon H \to H$). Therefore, the number of components of $G(n)$ is equal to the number of its cycles.

Before proceeding further, we need to review some properties of the C a r m i c h a e l lambda-function $\lambda(n)$, which was first defined in [3]. It modifies the Euler totient function $\phi(n)$ in that it can be used in an analogue of the Euler-Fermat theorem (see Theorem 3.2 below).

DEFINITION 3.1. Let n be a positive integer. Then the *Carmichael lambda-function* $\lambda(n)$ is defined as follows:

$$\begin{aligned}
\lambda(1) &= 1 = \phi(1)\,,\\
\lambda(2) &= 1 = \phi(2)\,,\\
\lambda(4) &= 2 = \phi(4)\,,\\
\lambda(2^k) &= 2^{k-2} = \tfrac{1}{2}\phi\big(2^k\big) \qquad \text{for} \quad k \geq 3\,,\\
\lambda(p^k) &= (p-1)p^{k-1} = \phi\big(p^k\big) \qquad \text{for any odd prime } p \text{ and } k \geq 1\,,\\
\lambda\big(p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}\big) &= \operatorname{lcm}\big[\lambda(p_1^{k_1}), \lambda(p_2^{k_2}), \ldots, \lambda(p_r^{k_r})\big]\,,
\end{aligned}$$

where $p_1, p_2, \ldots, p_r$ are distinct primes and $k_i \geq 1$ for all $i \in \{1, \ldots, r\}$.

It immediately follows from Definition 3.1 that $\lambda(n) \mid \phi(n)$ for all n. The following theorem generalizes the well-known Euler-Fermat theorem. It shows that $\lambda(n)$ is a universal order modulo n.

THEOREM 3.2 (CARMICHAEL). *Let* $a, n \in \mathbb{N}$. *Then*

$$a^{\lambda(n)} \equiv 1 \pmod{n} \tag{3.1}$$

if and only if $\gcd(a, n) = 1$. *Moreover, there exists an integer* g *such that*

$$\operatorname{ord}_n g = \lambda(n)\,, \tag{3.2}$$

where $\operatorname{ord}_n g$ *denotes the multiplicative order of* g *modulo* n.

For the proof see [3] or [7; p. 21].

THEOREM 3.3. *There exists a cycle of length* t *in* $G(n)$ *if and only if* $t = \operatorname{ord}_d 2$ *for some odd positive divisor* d *of* $\lambda(n)$.

P r o o f . Suppose that a is a vertex of a t-cycle in $G(n)$. Then t is the least positive integer such that

$$a^{2^t} \equiv a \pmod{n}\,,$$

which implies that t is the least positive integer for which

$$a^{2^t} - a \equiv a\big(a^{2^t-1} - 1\big) \equiv 0 \pmod{n}\,. \tag{3.3}$$

Since $\gcd\big(a, a^{2^t-1}-1\big) = 1$, it follows from (3.3) that if $n_1 = \gcd(a, n)$ and $n_2 = n/n_1$, then t is the least positive integer such that

$$\begin{aligned}
a &\equiv 0 \pmod{n_1}\,,\\
a^{2^t-1} &\equiv 1 \pmod{n_2}\,,
\end{aligned} \tag{3.4}$$

and therefore, $\gcd(n_1, n_2) = 1$. Hence, by the Chinese remainder theorem, there exists an integer b such that

$$\begin{aligned} b &\equiv 1 \pmod{n_1}, \\ b &\equiv a \pmod{n_2}. \end{aligned} \tag{3.5}$$

It follows from (3.4) and (3.5) that t is the least positive integer such that

$$b^{2^t-1} \equiv 1 \pmod{n}. \tag{3.6}$$

Let $d = \operatorname{ord}_n b$. Then $d \mid 2^t - 1$. Since, by (3.6), t is the least positive integer for which $d \mid 2^t - 1$, we see that $t = \operatorname{ord}_d 2$. Clearly, d is odd as $d \mid 2^t - 1$. Moreover, $d \mid \lambda(n)$ by (3.1), since $\gcd(b, n) = 1$ due to (3.6).

Conversely, suppose that d is an odd positive divisor of $\lambda(n)$ and let $t = \operatorname{ord}_d 2$. By Carmichael's Theorem 3.2, there exists a residue g modulo n such that $\operatorname{ord}_n g = \lambda(n)$. Let $h = g^{\lambda(n)/d}$. Then $\operatorname{ord}_n h = d$. Since $d \mid 2^t - 1$ but $d \nmid 2^k - 1$ whenever $1 \le k < t$, we see that t is the least positive integer for which

$$h^{2^t-1} \equiv 1 \pmod{n}. \tag{3.7}$$

Since, by (3.7),

$$h \cdot h^{2^t-1} = h^{2^t} \equiv h \pmod{n},$$

if follows that h is a vertex in a t-cycle of $G(n)$. □

THEOREM 3.4. *Let p be a Sophie Germain prime. Then $G(2p+1)$ has two trivial components: the isolated fixed point 0 and the component $\{1, 2p\}$ having the fixed point 1. Each of the other components has $2t$ vertices and contains a t-cycle, where $t = \operatorname{ord}_p 2$. The number of directed edges coming into a vertex of a t-cycle is exactly 2.*

Proof. Since $n = 2p + 1$ is prime, by Definition 3.1 we get

$$\lambda(2p+1) = 2p.$$

The only odd positive divisors of $2p$ are 1 and p. Setting $d = 1$ in Theorem 3.3, we find by Corollary 2.1 that there are exactly two fixed points: 0 and 1. Clearly, 0 is the only solution to the congruence $x^2 \equiv 0 \pmod{n}$, and so 0 is an isolated fixed point. Moreover, $x = 1$ and $x = 2p$ are the only solutions of the congruence $x^2 \equiv 1 \pmod{n}$, since n is prime. We have to show that the associated component containing $\{1, 2p\}$ does not contain any other vertices. Since p and n are odd numbers, we find that $n \equiv 3 \pmod{4}$. Consequently, $2p$ is a quadratic nonresidue modulo n, which means that the congruence $x^2 \equiv 2p \pmod{n}$ has no solution.

Now set $d = p$ in Theorem 3.3. Hence, each of the other components of $G(2p+1)$ contains a cycle of length $t = \operatorname{ord}_p 2$ with $t > 1$. If a vertex a belongs

to this t-cycle, then the congruence $x^2 \equiv a \pmod{n}$ has a solution, and hence, a is a quadratic residue modulo n. Since n is an odd prime, the congruence has exactly two solutions, c and $-c$. One of them lies on the t-cycle and the other outside. As $n = 2p + 1 \equiv 3 \pmod{4}$, one of the two residues c or $-c$ has to be a quadratic residue and the other a quadratic nonresidue modulo n.

Suppose that c is the quadratic nonresidue modulo n. Then c lies outside the t-cycle and the directed edge going out of c enters a. Since c is a quadratic nonresidue modulo n, there is no edge going into c. Thus, the associated component has exactly $2t$ vertices. □

In Theorem 3.10 we give a converse of Theorem 3.4.

DEFINITION 3.5. If p is a Sophie Germain prime, then all components of $G(2p + 1)$ which do not contain vertices 0 and 1 are called *Sophie Germain little suns.*

COROLLARY 3.6. *Let p be a Sophie Germain prime. Then the number of Sophie Germain little suns of $G(2p + 1)$ is equal to*

$$\frac{p-1}{\operatorname{ord}_p 2}. \tag{3.8}$$

Proof. According to Theorem 3.4, the number of vertices of $G(2p + 1)$ that are outside the two trivial components is equal to $2p - 2$. By Theorem 3.4 we also know that each Sophie Germain little sun has $2\operatorname{ord}_p 2$ vertices, which leads to the corollary. □

Remark 3.7. If $2p + 1$ is prime with $p > 1$, then $2p - 2$ is not divisible by 3. Consequently, by (3.8), the number of Sophie Germain little suns is never divisible by 3 and the length of each of the associated t-cycles is also not divisible by 3.

We can prove a more general statement, namely that $G(2p+1)$ never contains a q-cycle for $q = 3, 5, 7, 13, 17, 19, \ldots$, which are the exponents of all Mersenne primes $M_q = 2^q - 1$ with $q > 2$. (Notice that $G(7)$ contains a 2-cycle.)

THEOREM 3.8. *Let M_q be a Mersenne prime with $q > 2$. Then there does not exist a Sophie Germain prime p such that $G(2p + 1)$ contains a q-cycle.*

Proof. Assume to the contrary that there exist a Sophie Germain prime p and a Mersenne prime M_q with $q > 2$ such that $G(2p + 1)$ contains a q-cycle. Then by Theorem 3.4, $q = \operatorname{ord}_p 2$ and thus $p = 2^q - 1$. However, the number

$$2p + 1 = 2^{q+1} - 1 = \left(2^{(q+1)/2} + 1\right)\left(2^{(q+1)/2} - 1\right)$$

is composite for $q > 2$ prime, which is a contradiction. □

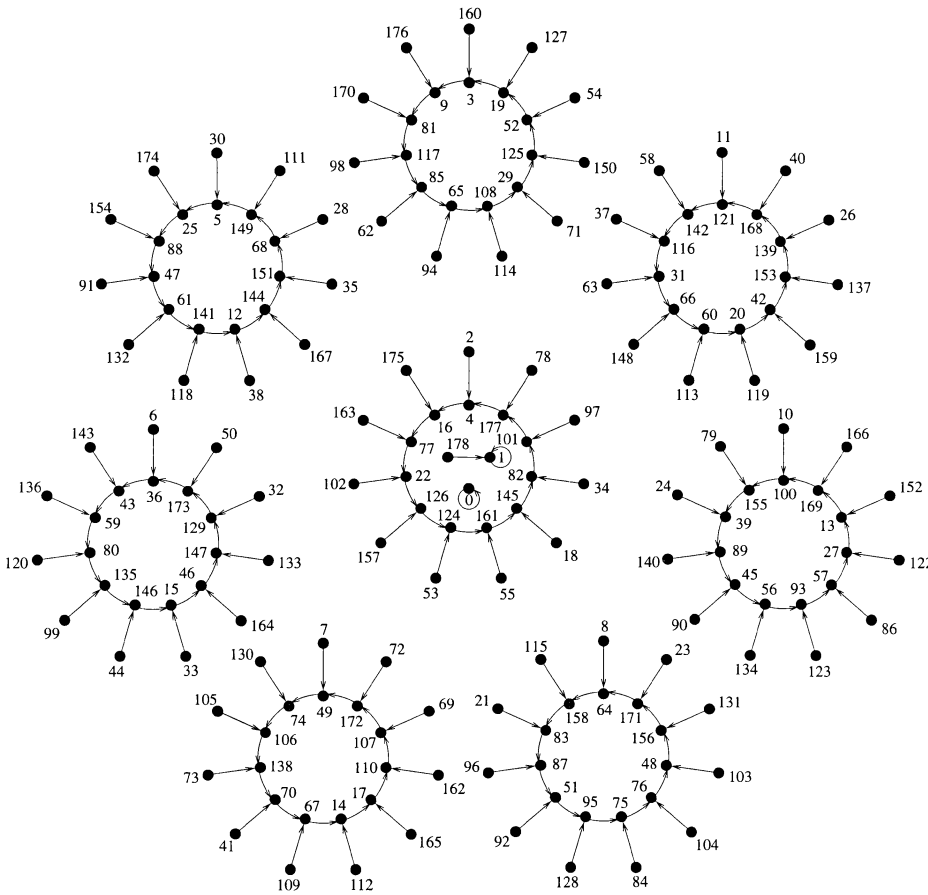

FIGURE 4. Iteration digraph corresponding to $n = 179$.

EXAMPLE 3.9. Let $p = 89$. Since $2^{11} \equiv 1 \pmod{89}$, we see that $\operatorname{ord}_{89} 2 = 11$. Hence, by Corollary 3.6, the number of Sophie Germain little suns of $G(179)$ is $88/11 = 8$ (see Figure 4).

THEOREM 3.10. *Let n be a positive integer. Suppose that $G(n)$ has exactly two trivial components: the isolated fixed point 0 and the component $\{1, n-1\}$ having the fixed point 1. Suppose further that $G(n)$ has a positive number of other components, each of which has $2t$ vertices and contains a t-cycle, where $t > 1$ is a fixed integer. Then n is a prime of the form $2m + 1$, where $m \geq 3$ is odd, and $\operatorname{ord}_p 2 = \operatorname{ord}_q 2 = t$ for any primes p and q dividing m, and $\operatorname{ord}_p 2 = \operatorname{ord}_{p^k} 2$ whenever $p^k \parallel m$.*

P r o o f . We first observe that $n \geq 7$, since the two trivial components of $G(n)$ contain 3 vertices and each of the other components has at least $2t$ vertices, where $t \geq 2$. Moreover, by the discussion preceding Corollary 2.1, we see that if n has two or more distinct prime divisors, then there exist at least four fixed points, contrary to the hypothesis that $G(n)$ has exactly two fixed points. Furthermore, $n \neq p^k$, where p is a prime and $k \geq 2$, since then the component of $G(n)$ containing the vertex 0 also contains the vertex p^{k-1}, contradicting the assumption that 0 is an isolated fixed point. Thus, n is an odd prime.

We now claim $4 \nmid \lambda(n)$. If $4 \mid \lambda(n)$, then by (3.2), it follows that there exists an integer $1 < c < n$ such that $\operatorname{ord}_n c = 4$. Then the component of $G(n)$ containing the vertex 1 has at least three vertices, namely 1, $n-1$, and c, contrary to the hypothesis. Since $\lambda(n) = n - 1$, we find that n is of the form $2m + 1$, where $m \geq 3$ is odd.

By Theorem 3.3, $\operatorname{ord}_d 2 = t$ for every odd divisor d of m such that $d > 1$. We further note that if $\operatorname{ord}_p 2 = \operatorname{ord}_{p^k} 2$, where p is an odd prime and $k \geq 2$, then $\operatorname{ord}_p 2 = \operatorname{ord}_{p^e} 2$ for $1 \leq e \leq k$. We also observe that if $\gcd(r, s) = 1$ and $\operatorname{ord}_r 2 = \operatorname{ord}_s 2 = t$, then $\operatorname{ord}_{rs} 2 = t$. The result now follows. □

Remark 3.11. To fulfil the assumptions of Theorem 3.10, we can choose, e.g., $p = 499$, $q = 2657$ and $t = \operatorname{ord}_p 2 = \operatorname{ord}_q 2 = 166$. Then p, q and $n = 2pq+1 = 2\,651\,687$ are primes. Note in Theorem 3.10 that when n is a prime of the form $2m + 1$ and m is itself an odd prime, then m is a Sophie Germain prime.

Acknowledgement.

The authors are indebted to László Szalay for fruitful discussions and Pavel Křížek for his assistance in preparation of figures.

REFERENCES

[1] AGRAWAL, M.—KAYAL, N.—SAXENA, N.: *Primes is in P.* Preprint 2002.

[2] BRUN, V.: *Sur les nombres premiers de la forme* $ap+b$, Archiv for Mathematik (Christiania) **14** (1917), 1 9.

[3] CARMICHAEL, R. D.: *Note on a new number theory function*, Bull. Amer. Math. Soc. **16** (1910), 232 238.

[4] CHASSÉ, G.: *Applications d'un corps fini dans lui-même.* Dissertation, Univ. de Rennes I, 1984.

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

[6] HARDY, G. H.—LITTLEWOOD, J. E.: *Some problems of 'partitio numerorum' III: On the expression of a number as a sum of primes*, Acta. Math. **44** (1923), 1–70.
In: Collected Papers of G. H. Hardy, Vol. I, Clarendon Press, Oxford, 1966, pp. 561 630.

[7] KŘÍŽEK, M.—LUCA, F.—SOMER, L.: *17 Lectures on Fermat Numbers. From Number Theory to Geometry*, Springer-Verlag, New York, 2001.

[8] KŘÍŽEK, M.—SOMER, L.: *A necessary and sufficient condition for the primality of Fermat numbers*, Math. Bohem. **126** (2001), 541–549.

[9] LUCHETA, C.—MILLER, E.—REITER, C.: *Digraphs from powers modulo p*, Fibonacci Quart. **34** (1996), 226–239.

[10] ROBERT, F.: *Discrete Iterations*. Springer Ser. Comput. Math. 6, Springer, New York, 1986.

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

[12] SOMER, L.—KŘÍŽEK, M.: *On a connection of number theory with graph theory*, Czechoslovak Math. J. **54** (2004), 465–485.

[13] SZALAY, L.: *A discrete iteration in number theory*, BDTF Tud. Közl. 8. Természettudományok 3, Szombathely, (1992), 71–91. (Hungarian)

Received October 10, 2003
Revised December 02, 2003

* *Mathematical Institute*
Academy of Sciences
Žitná 25
CZ–115 67 Prague 1
CZECH REPUBLIC
E-mail: krizek@math.cas.cz

** *Department of Mathematics*
Catholic University of America
Washington, D.C. 20064
U.S.A.
E-mail: somer@cua.edu