Lawrence Somer

My twelve years of collaboration with Michal Křížek on number theory

In: Jan Brandts and J. Chleboun and Sergej Korotov and Karel Segeth and J. Šístek and Tomáš Vejchodský (eds.): Applications of Mathematics 2012, In honor of the 60th birthday of Michal Křížek, Proceedings. Prague, May 2-5, 2012. Institute of Mathematics AS CR, Prague, 2012. pp. 267–277.

Persistent URL: http://dml.cz/dmlcz/702912

Conference Applications of Mathematics 2012
in honor of the 60th birthday of Michal Křížek.
Institute of Mathematics AS CR, Prague 2012

MY TWELVE YEARS OF COLLABORATION WITH MICHAL KŘÍŽEK ON NUMBER THEORY

Lawrence Somer
Department of Mathematics, Catholic University of America
Washington, D.C. 20064, U.S.A.
Somer@cua.edu

Abstract

We give a survey of the joint papers of Lawrence Somer and Michal Křížek and discuss the beginning of this collaboration.

1. Introduction

In the fall of 1999, I was in Prague on a one-year sabbatical from The Catholic University of America in Washington, D.C., and was teaching a course entitled *"Primality Testing and Its Application to Cryptography"* at the Faculty of Mathematics and Physics of Charles University. At the same time I met Florian Luca in Prague, whom I knew from the Fibonacci Conferences. He was preparing with Michal Křížek the book, *17 Lectures on Fermat Numbers*. Michal had been interested in the topic of Fermat numbers since he wrote a paper with Jan Chleboun for Mathematica Bohemica in 1994 on Fermat numbers. In November 1998, Florian Luca also submitted a paper related to Fermat numbers to Mathematica Bohemica for which Michal was the referee. Subsequently Michal invited Florian to visit the Institute of Mathematics in Prague in 1999–2000. While visiting Florian at the Institute, he introduced me to Michal, and soon after this, both asked me if I wanted to be a third coauthor of this book. After some thought, I agreed. Thus began my fruitful 12-year collaboration with Michal that has resulted in 30 joint papers and 2 books, primarily in the fields of number theory and combinatorics (see [1]–[32]).

Our papers were written in four languages – English, Czech, Spanish, and Chinese. As far as I know, Michal has also published papers in the six additional languages of Russian, German, Finnish, Dutch, Slovak, Serbo-Croatian.

2. Some of our most notable results

2.1. Euclidean primes

Euclid's theorem on the infinitude of primes is usually proved by a contradiction argument. It is assumed that there are only finitely many primes $p_1, p_2, \ldots, p_n$ and then it is shown that

$$m = p_1 p_2 \cdots p_n + 1 \tag{1}$$

is a new prime or m has a new prime factor different from $p_1, p_2, \ldots, p_n$, which is a contradiction.

Therefore, primes of the form (1) are called *Euclidean primes.* For instance,

$$2+1=3,\ 2\cdot3+1=7,\ 2\cdot3\cdot5+1=31,\ 2\cdot3\cdot5\cdot7+1=211,\ 2\cdot3\cdot5\cdot7\cdot11+1=2311$$

are Euclidean primes, but the next term

$$2\cdot3\cdot5\cdot7\cdot11\cdot13+1=59\cdot509$$

is composite.

Let p be a prime and let a be a natural number coprime to p. Then by Fermat's little theorem

$$a^{p-1} \equiv 1 \pmod{p}.$$

We call the integer $a \not\equiv 0 \pmod{p}$ a *primitive root modulo* p if

$$a^k \not\equiv 1 \pmod{p}$$

for all $k \in \{1, 2, \ldots, p-2\}$. For example, 3 is a primitive root modulo 5, since $3^k \not\equiv 1 \pmod{5}$ for all $k = 1, \ldots, 3$ (and $3^4 \equiv 1 \pmod{5}$ by Fermat's little theorem).

Denote by $A(p)$ the number of primitive roots modulo the prime p. In [20] we proved that Euclidean primes have the minimum possible number of primitive roots.

Theorem 1. *If p is a Euclidean prime, then for all primes $q < p$ we have*

$$\frac{A(q)}{q} > \frac{A(p)}{p}.$$

2.2. Fermat primes

Recall that

$$F_m = 2^{2^m} + 1 \quad \text{for } m = 0,\ 1,\ 2, \ldots \tag{2}$$

are called *Fermat numbers.* If F_m is prime it is termed a *Fermat prime.* For instance,

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537, \tag{3}$$

are Fermat primes, but F_5 is composite.

As contrasted to Euclidean primes which have the minimum possible number of primitive roots, it is well known that Fermat primes have the maximum possible number of primitive roots, namely $(F_m - 1)/2$ (for a proof of this results see [16] or [3, p. 51]).

Leonhard Euler proved that any divisor of F_m is of the form $k2^{m+1} + 1$. Édouard Lucas refined this result by showing that each divisor of $F_m > 5$ is of the form $k2^{m+2} + 1$. In [3], we proved the following result.

Theorem 2. *If $k2^{m+2} + 1$ is a prime divisor of a composite Fermat number F_m, where $k = 3, 5$ or 6, then F_m has no prime divisor of the form $\ell 2^{m+2} + 1$, where $1 \leq \ell < k$, and $k2^{m+2} + 1$ is the smallest prime divisor of F_m.*

2.3. Mersenne and Sophie Germain primes

In [19] we provided a relationship between Mersenne and Sophie Germain primes (see Theorem 3 below). Recall that the number $M_p = 2^p - 1$, where p is prime, is termed a *Mersenne number.* If $2^p - 1$ itself is prime, then it is called a *Mersenne prime.* In particular, if

$$p = 2,\ 3,\ 5,\ 7,\ 13,\ 17,\ 19,\ 31,\ 61,\ 89, \ldots$$

we get a Mersenne prime.

In 1819, the 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.* For example 5, 11, and 23 are Sophie Germain primes.

Furthermore, we examine some connections of number theory with graph theory. We assign to each pair of positive integers $k \geq 2$ and n a digraph $G(n, k)$ whose set of vertices is $H = \{0, 1, \ldots, n - 1\}$ and for which there exists a directed edge from $a \in H$ to $b \in H$ if $a^k \equiv b \pmod{n}$. The cycles of length q are said to be *q-cycles.* All cycles are assumed to be oriented counterclockwise (see Figure 1 for $n = 47$).

In [19] we proved the following relatively simple statements.

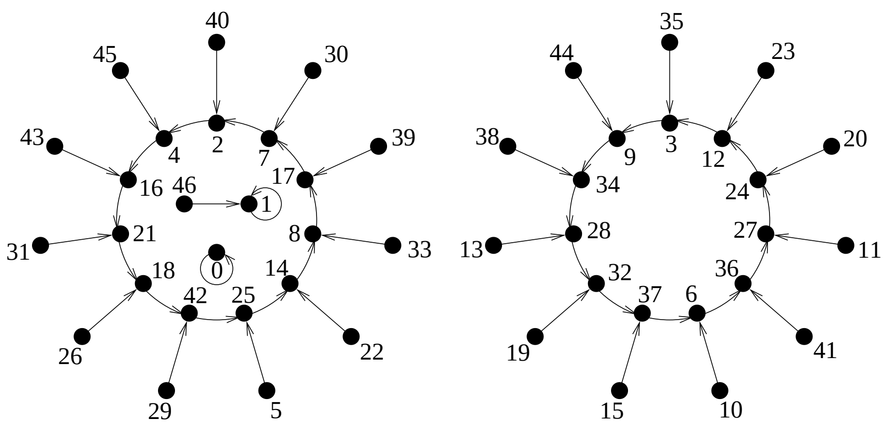

Figure 1: Iteration digraph corresponding to $n = 47$.

Theorem 3. *Let M_q be a Mersenne prime with $q > 2$. Then there does not exist a Sophie Germain prime p such that $G(2p+1, 2)$ contains a q-cycle.*

We proved the following characterization of Sophie Germain primes.

Theorem 4. *Let p be a Sophie Germain prime. Then $G(2p+1, 2)$ 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. The number of directed edges coming into a vertex of a t-cycle is exactly 2.*

See Figure 1 for the iteration digraph $G(2p+1, 2)$, where $p = 23$ is a Sophie Germain prime.

If the quadratic congruence

$$x^2 \equiv a \pmod{p}$$

has no solution x then a is said to be *a quadratic nonresidue modulo p*.

Theorem 5. *Let p be a Sophie Germain prime. Then all quadratic nonresidues are primitive roots modulo $2p+1$, except for exactly one number $2p$, which is a quadratic nonresidue, but not a primitive root.*

2.4. Semiregular iteration digraphs modulo n

The *indegree* of a vertex $a \in H$ of $G(n, k)$ is the number of directed edges coming into a. The digraph $G(n, k)$ is said to be *semiregular* if there exists a positive integer d such that each vertex of the digraph has indegree d or 0.

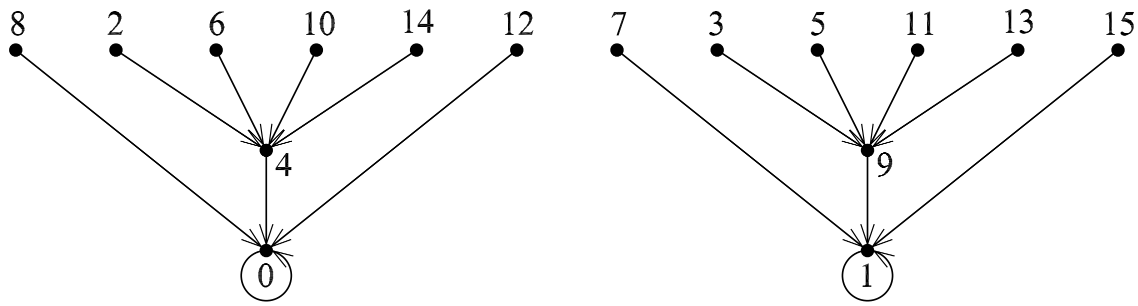

Figure 2: The semiregular iteration digraph $G(16, 2)$.

By Figure 2 we see that $G(16, 2)$ is semiregular. In Theorem 6 which was proved in [30], we characterize the structure all semiregular digraphs $G(n, k)$.

We use the notation $\prod_{i=1}^{0} a_i$ to denote that the corresponding product is empty and set equal to 1 by convention.

Theorem 6. *Let $k \geq 2$ be a fixed integer with the factorization*

$$k = Q \prod_{i=1}^{\ell} p_i^{\alpha_i},$$

where each p_i is a prime such that $\gcd(p_i - 1, k) = 1$ and in addition, $\ell \geq 1$, $\alpha_i \geq 1$, and $\gcd(q-1, k) > 1$ for each prime q dividing Q. Let $n \geq 2$ have the prime power factorization

$$n = S \prod_{i=1}^{\ell} p_i^{\beta_i} \prod_{i=1}^{m} q_i^{\gamma_i},$$

where $\beta_i \geq 0$, $m \geq 0$, $\gamma_i \geq 1$, $\gcd(q_i(q_i - 1), k) = 1$ for $i = 1, 2, \ldots, m$, and $\gcd(t-1, k) > 1$ for each prime t dividing S.

Then $G(n,k)$ is semiregular if and only if one of the following conditions holds:

(a) $n = \prod_{i=1}^{\ell} p_i^{\beta_i} \prod_{i=1}^{m} q_i$ *for* $0 \leq \beta_i \leq \alpha_i + 1$ *and* $m \geq 0$ *when* p_i *is odd for each* $i \in \{1, 2, \ldots, \ell\}$,

(b) $n = 2^{\beta_1}$ *for* $\beta_1 \in \{1, 2, 4\}$ *when* $k = 2$,

(c) $n = 2^{\beta_1}$ *for* $1 \leq \beta_1 \leq 5$ *when* $k = 2^2$,

(d) $n = 2^{\beta_1}$ *for* $1 \leq \beta_1 \leq \alpha_1 + 2$ *when* $p_1 = 2$ *and* $k \geq 6$.

2.5. Symmetric iteration digraphs modulo n

A *component* of the iteration digraph is a subdigraph which is a maximal connected subgraph of the associated nondirected graph. The digraph $G(n,k)$ is symmetric of order M if its set of components can be partitioned into disjoint subsets, each containing exactly M isomorphic components.

By Figure 3, the digraph $G(39,3)$ is symmetric of order 3. Before proceeding further, we need to define the Carmichael lambda-function $\lambda(n)$.

Definition 1. Let n be a positive integer. Then the *Carmichael lambda-function* $\lambda(n)$ is defined as follows:

$$\lambda(1) = \lambda(2) = 1,$$
$$\lambda(4) = 2,$$

$$\lambda(2^k) = 2^{k-2} \text{ for } k \geq 3,$$
$$\lambda(p^k) = (p-1)p^{k-1} \text{ for any odd prime } p \text{ and } k \geq 1,$$
$$\lambda(p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}) = \operatorname{lcm}[\lambda(p_1^{k_1}),\ \lambda(p_2^{k_2}), \ldots,\ \lambda(p_r^{k_r})],$$

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

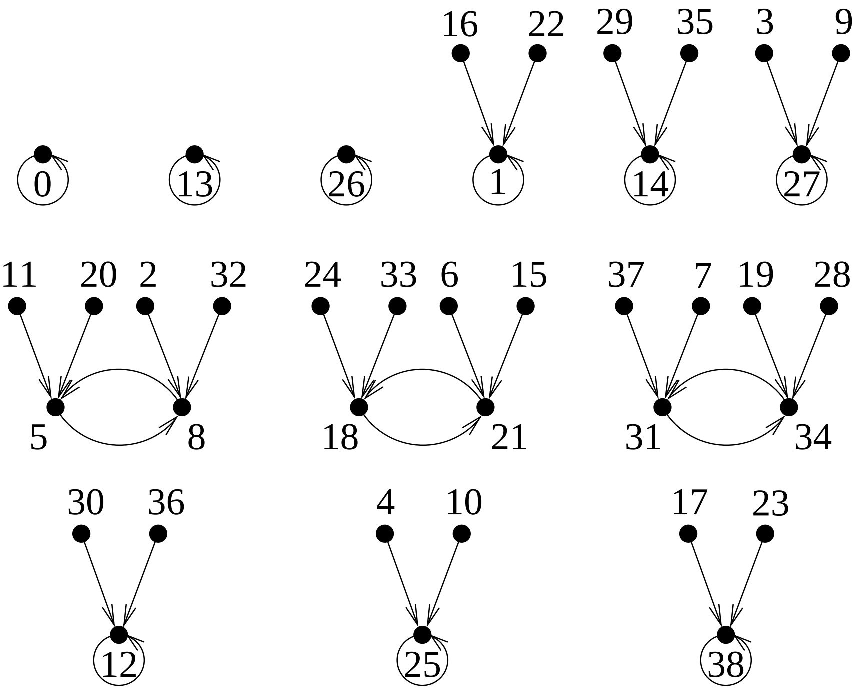

Figure 3: The symmetric iteration digraph $G(39, 3)$ of order 3.

In Theorem 7 which was proved in [31], we give several sufficient conditions for a digraph $G(n, k)$ to be symmetric of order $M \geq 2$.

Theorem 7. *Let $n = n_1 n_2$, where $n_1 > 1$, $n_2 \geq 1$, and $\gcd(n_1, n_2) = 1$.*

(i) Suppose that $n_1 = p^\alpha$, where p is an odd prime and $\alpha \geq 1$. Suppose further that $k \equiv 1 \pmod{p-1}$ and $p^{\alpha-1} \mid k$. Then $G(n, k)$ is symmetric of order p.

(ii) Suppose that $n_1 = 2^\alpha$, where $\alpha \geq 1$. Then $G(n, k)$ is symmetric of order 2 if one of the following conditions holds:

(a) $\alpha \leq 2$, $k \geq 2$, and $2^{\alpha-1} \mid k$,
(b) $\alpha \geq 3$, $k > 2$, and $2^{\alpha-2} \mid k$,
(c) $\alpha = 4$ and $k = 2$.

(iii) Suppose that $n_1 = q_1 q_2 \cdots q_s$, where the q_i's are distinct primes, not necessarily odd, and $s \geq 2$. Suppose that $k \equiv 1 \pmod{\lambda(n_1)}$. Then $G(n, k)$ is symmetric of order n_1.

(iv) Suppose that $n_1 = p^\alpha q_1 q_2 \cdots q_s$, where p is an odd prime, $\alpha \geq 2$, $s \geq 1$, and the q_i's are distinct primes such that $p \neq q_i$ and $p \nmid q_i - 1$ for $i = 1, 2, \ldots, s$. Suppose further that $k \equiv 1 \pmod{\lambda(p q_1 q_2 \cdots q_s)}$ and $p^{\alpha-1} \mid k$. Then $G(n, k)$ is symmetric of order $p q_1 q_2 \cdots q_s$.

2.6. Elite primes

Motivated by a generalization of the Pepin primality test (see [3, pp. 42–43]) for Fermat numbers (2), Aigner introduced the notion of *elite primes* which are the primes p such that F_m is a quadratic nonresidue modulo p for all but finitely many m. For example, 3, 5, 7, and 41 are elite primes. Denoting by E the set of all elite primes, the following statement holds (see [4]):

Theorem 8. *The series*

$$\sum_{p \in E} \frac{1}{p}$$

is convergent.

Note that $\sum_{p \in P} \frac{1}{p}$ over the set P of all primes is divergent.

Since the sequence of Fermat numbers is eventually periodic modulo any prime p with at most p distinct elements in the image, the period length t_p is bounded by p and the number of arithmetic operations modulo p to test p for being elite is bounded by $O(p \log p)$. In [2] (published in *Journal of Integer Sequences*) we showed that $t_p = O(p^{3/4})$, in particular improving the estimate $t_p \leq (p+1)/4$ of Müller and Reinhart in 2008. The same order of magnitude $O(p^{3/4})$ is also derived for the so-called *anti-elite primes* which are introduced in [2]. This paper generalizes some of our previous paper [4] published in *Journal of Number Theory*.

2.7. Šindel sequences

In [10] we found that there is a remarkable relationship between the triangular numbers $T_k = 1 + 2 + \cdots + k$ and the bellworks of the astronomical clock (horologe) of Prague.

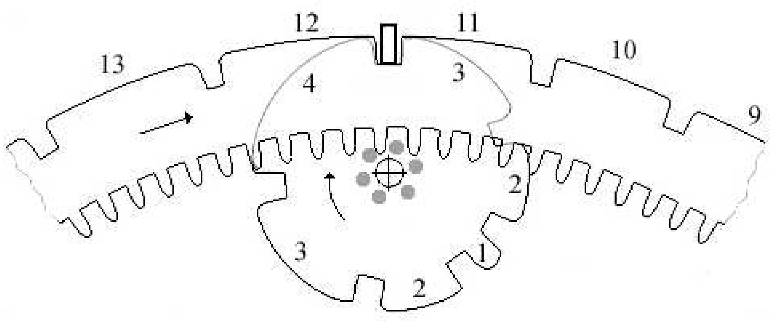

Figure 4: The number of bell strokes is denoted by the numbers ..., 9, 10, 11, 12, 13, ... along the large gear. The small gear placed behind it is divided by slots into segments of arc lengths 1, 2, 3, 4, 3, 2.

When the small gear of the bellworks revolves (see Figure 4) it generates by means of its slots a periodic sequence whose particular sums correspond to the number of strokes of the bell at each hour:

$$1\ 2\ 3\ 4\ \underbrace{3\ 2}_{5}\ \ \underbrace{1\ 2\ 3}_{6}\ \ \underbrace{4\ 3}_{7}$$

$$\underbrace{2\ 1\ 2\ 3}_{8}\ \ \underbrace{4\ 3\ 2}_{9}\ \ \underbrace{1\ 2\ 3\ 4}_{10}\ \ \underbrace{3\ 2\ 1\ 2\ 3}_{11}\ \ \underbrace{4\ 3\ 2\ 1\ 2}_{12}$$

$$\underbrace{3\ 4\ 3\ 2\ 1}_{13}\ \ \underbrace{2\ 3\ 4\ 3\ 2}_{14}\ \ \underbrace{1\ 2\ 3\ 4\ 3\ 2}_{15}\ \dots \tag{4}$$

The mathematical model of the astronomical clock of Prague was probably invented by Jan Šindel around 1410. In honor of this great achievement we introduced in [10] a new term, the *Šindel sequence* $\{a_i\} \subset \mathbb{N}$ of natural numbers as such a periodic sequence with period p that satisfies the following condition: for any $k \in \mathbb{N}$ there exists $n \in \mathbb{N}$ such that

$$T_k = a_1 + \cdots + a_n. \tag{5}$$

This condition guarantees a functioning of the bellworks, which is controlled by the horologe (for details see [10]). In [10] we made a systematic investigation of Šindel sequences.

In the next theorem from [10] we show that we could continue in (4) indefinitely in this way. Let

$$s = \sum_{i=1}^{p} a_i.$$

Theorem 9. *A periodic sequence $\{a_i\}$ for s odd is a Šindel sequence if* (5) *holds for* $k = 1, 2, \dots, (s-1)/2$.

In [10] we, moreover, give a necessary and sufficient condition for a periodic sequence to be a Šindel sequence. We also present an algorithm which produces the so-called primitive Šindel sequence, which is uniquely determined for a given $s = a_1 + \cdots + a_p$.

3. Our monographs

In 2001, Michal, Florian Luca, and I published the book *17 Lectures on Fermat numbers* [3] in honor of the 400th anniversary of Fermat's birth. The book had 3 authors, took 5 years to prepare, consisted of 17 lectures, had 257 pages, and hopefully will make USD 65 537 in royalties (compare with (3)). This book contains a lot of known results, but some theorems are also ours. Its second edition appeared in 2011.

In 2009, Michal, Alena Šolcová, and I published another book *Kouzlo čísel* [26] (Magic of numbers). This book won the Josef Hlávka Prize for the best scientific book published in the Czech Republic in 2009 in the category of the science of inanimate nature. The second edition of this book appeared in 2011.

Finally, let us mention one interesting result from [26]. Magic squares consisting solely of primes have been of considerable interest. Based on the Green-Tao theorem, which states that there are arithmetic progressions of arbitrary length containing only primes, we proved the following statement.

Theorem 10. *For any natural number n there exists a magic square of order n containing only primes.*

This theorem can be easily generalized to any set that contains arithmetic progressions of arbitrary length.

4. Closing remark

It has been a fruitful twelve years of collaboration with Michal and I look forward to many more years of joint research.

References

[1] Katrnoška, F., Křížek, M., and Somer, L.: Magické čtverce a sudoku. Pokroky Mat. Fyz. Astronom. **53** (2008), 113–124.

[2] Křížek, M., Luca, F., Shparlinski, I., and Somer, L.: On the complexity of testing elite primes. J. Integer Seq. **14** (2011), Article 11.1.2, 1–5.

[3] Křížek, M., Luca, F., and Somer, L.: *17 lectures on Fermat numbers: From number theory to geometry.* CMS Books in Mathematics, vol. 9, Springer-Verlag New York, 2001, second edition 2011.

[4] Křížek, M., Luca, F., and Somer, L.: On the convergence of series of reciprocals of primes related to the Fermat numbers. J. Number Theory **97** (2002), 95–112.

[5] Křížek, M., Luca, F., and Somer, L.: Aritmetické vlastnosti Fibonacciových čísel. Pokroky Mat. Fyz. Astronom. **50** (2005), 127–140.

[6] Křížek, M., Luca, F., and Somer, L.: From Fermat numbers to geometry. Math. Spectrum **38** (2005/2006), 56–63.

[7] Křížek, M., Luca, F., and Somer, L.: Arithmetic properties of Fibonacci numbers. In: J. Přívratská, J. Příhonská, and Z. Andres(Eds.) *Proc. Internat. Conf. Presentation of Mathematics '06*, pp. 7–18. Tech. Univ. of Liberec, 2006.

[8] Křížek, M., Luca, F., and L. Somer: Desde los números de Fermat hasta la geometría. Gac. R. Soc. Mat. Esp. **10** (2007), 471–483.

[9] Křížek, M., Šolcová, A., and Somer, L.: Šindel sequences and the Prague horologe. In: J. Chleboun, K. Segeth, and T. Vejchodský (Eds.), *Proc. PANM 13 dedicated to the 80th birthday of Professor Ivo Babuška*, pp. 156–164. Math. Inst. Prague, 2006.

[10] Křížek, M., Šolcová, A., and Somer, L.: Construction of Šindel sequences. Comment. Math. Univ. Carolin. **48** (2007), 373–388.

[11] Křížek, M., Šolcová, A., and Somer, L.: Ten theorems on the astronomical clock of Prague In: J. Příhonská, K. Segeth, D. Andrejsová (Eds.), *Proc. Internat. Conf. Presentation of Mathematics '07*, pp. 53–62. Tech. Univ. of Liberec, 2007.

[12] Křížek, M., Šolcová, A., and Somer, L.: What mathematics is hidden behind the astronomical clock of Prague? Highlights of Astronomy **14**. In: R. M. Ros and J. M. Pasachoff (Eds.), *SPS2 - Innovation in Teaching and Learning Astronomy, Proc. of the IAU XXVIth General Assembly in Prague, August 2006* , p.575. Cambridge Univ. Press, 2007. Also in: J. M. Pasachoff, R. M. Ros, and N. Pasachoff: *Innovation in astronomy education*. Cambridge Univ. Press, 2008, 142–143.

[13] Křížek, M., Šolcová, A., and Somer, L.: The astronomical clock of Prague and triangular numbers. In: *Proc. Conf. Matematika a současná společnost*. Tech. Univ. Liberec, 2008, 41–50.

[14] Křížek, M., Šolcová, A., Somer, L.: The mathematics behind Prague's horologe (in Chinese and English). Math. Culture **1** (2) (2010), 69–77.

[15] Křížek, M., Šolcová, A., Somer, L.: 600 years of Prague's horologe and the mathematics behind it. Math. Spectrum **44** (2011/2012), 28–33.

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

[17] Křížek, M. and Somer, L.: 17 necessary and sufficient conditions for the primality of Fermat numbers. Acta Math. Inf. Univ. Ostraviensis **11** (2003), 73–79.

[18] Křížek, M. and Somer, L.: Pseudoprvočísla. Pokroky Mat. Fyz. Astronom. **48** (2003), 143–151.

[19] Křížek, M. and Somer, L.: Sophie Germain little suns. Math. Slovaca **54** (2004), 433–442.

[20] Křížek, M. and Somer, L.: Euclidean primes have the minimum number of primitive roots. JP J. Algebra Number Theory Appl. **12** (2008), 121–127.

[21] Křížek, M. and Somer, L.: Abelova cena v roce 2008 udělena za objevy v teorii neabelovských grup. Pokroky Mat. Fyz. Astronom. **53** (2008), 177–187.

[22] Křížek, M. and Somer, L.: On peculiar Šindel sequences. JP J. Algebra Number Theory Appl. **17** (2010), 129–140.

[23] Křížek, M. and Somer, L.: Architects of symmetry in finite nonabelian groups. Symmetry: Culture and Science **21** (2010), 333–344.

[24] Křížek, M. and Somer, L.: John Tate získal Abelovu cenu za rok 2010. Pokroky Mat. Fyz. Astronom. **55** (2010), 89–96.

[25] Křížek, M., Somer, L., and Šolcová, A.: Jaká matematika se ukrývá v pražském orloji? Matematika-fyzika-informatika **16** (2006), 129–137.

[26] Křížek, M., Somer, L., and Šolcová, A.: *Kouzlo čísel: Od velkých objevů k aplikacím*. Edice Galileo, sv. 39, Academia, Praha, 2009, 365 + VIII pp. Second edition, 2011.

[27] Křížek, M., Somer, L., and Šolcová, A.: Deset matematických vět o pražském orloji. Pokroky Mat. Fyz. Astronom. **54** (2009), 281–300.

[28] Somer, L. and Křížek, M.: On a connection of number theory with graph theory. Czechoslovak Math. J. **54** (2004), 465–485.

[29] Somer, L. and Křížek, M.: Structure of digraphs associated with quadratic congruences with composite moduli. Discrete Math. **306** (2006), 2174–2185.

[30] Somer, L. and Křížek, M.: On semiregular digraphs of the congruence $x^k \equiv y \pmod{n}$. Comment. Math. Univ. Carolin. **48** (2007), 41–58.

[31] Somer, L. and Křížek, M.: On symmetric digraphs of the congruence $x^k \equiv y \pmod{n}$. Discrete Math. **309** (2009), 1999–2009.

[32] Somer, L. and Křížek, M.: The structure of digraphs associated with the congruence $x^k \equiv y \pmod{n}$. Czechoslovak Math. J. **61** (2011), 337–358.