Exercises of division theory leading to brand new results

Zdeněk Polický
Dept. of Mathematics, Faculty of Education MU, Poříčí 31, 603 00 Brno, Czech Republic, *alize@seznam.cz*

The number theory is usually taught during one semester at the Faculties of Science in the programme for teachers of mathematics. After refreshing the elementary knowledge of mathematics from high schools (especially the properties of the division theory in integers), the students acquaint with the congruences. Students learn to work with linear congruences and congruences of higher degree - then they can solve equations in integers by using these congruences and their properties. Marginally, they also touch on the simplest types of diophantine equations. It is exactly the diophantine equations that can be one of the most practical topics and in the same time it could be used as a model for explanation of some theoretic problems.

The application of number theory at the Faculties of Education is usually quite marginal compared to the Faculties of Science. The creation of number fields and the division theory (which is taught as part of algebra) are emphasized. The division theory is closely connected with high school's topics. For assumption of elementary concepts, methods and assertions of number theory, it is convinient to acquaint students with the real problems of this part of mathematics in special seminars and lessons. Most of these problems could be defined in a simple way but there are some of them where we cannot answer the question of their solvability. Application of various methods on the arithmetical exercises can give a lot of new knowledge to students who can also verify the results of previous exercises by themselves.

A seminary based on similar methods of teaching would certainly achieve success in mathematical classes at the high schools. In the framework of one lesson; the teacher doesn't usually have enough time or opportunity to lead talented students individualy and he cannot use quality textbooks. The questions about existence and properties of Fermat's or Mersenne's numbers can be an interesting and suitable topic for students during the workshops of number theory.

Fermat primes are called primes of the form $2^{2^k}+1$, where $k \geq 0$. Only five Fermat primes are known these days. The Fermat primes are not only known in number theory but also in other parts of mathematics. One of the most interesting applications of these primes in geometry is their use for construction of regular polygon with *n* sides by ruler and compass. First, this assertion was proved by German mathematician Carl Fridrich Gauss at the beginning of the 19th century.

Proposition 1: There exist construction of the regular polygon with n sides by ruler and compass if and only if $n = 2^k F_{m_1} F_{m_2} \dots F_{m_j}$, where $n \geq 3, k \geq 0, j \geq 0$ and $F_{m_1} F_{m_2} \dots F_{m_j}$ are distinct Fermat primes.

You can find the prove of this proposition in [6].

Mersenne primes are all primes of the form $2^p - 1$, where *p* is prime. We can find very interesting use of Mersenne primes by trying if the examinated number is perfect or not. A number where the sum of its own divisors is equal to this number is called a perfect number. Today Mersenne primes are used especially for finding the biggest existing primes. (cf. [www1])

Although Fermat's and Mersenne's primes are already known for a couple of centuries and although the biggest mathematicians around the world were interested in these numbers and their properties, too, there remains a lot of still-open and unresolved problems until these days. The scientists often discovered new results that were applied widely in various parts of mathematics but they didn't solve the problem completely. The most interesting and still unresolved questions about Fermat's and Mersenne's numbers are pointed below (more in [6]):

Are there infinitely many Mersenne's primes? (39th Mersenne's prime was found very recently.)
Are the primes 3, 5, 17, 257, 65537 all the Fermat primes?
For which regular polygons does there exist a Euclidean construction?
Does there exist Fermat number divisible by the square of a prime number?
Are there infinitely many perfect numbers or does exist odd perfect number?

We can find another interesting results about Fermat's or Mersenne's numbers in solving some diophantine equation $\frac{q^n - 1}{q - 1} = y$ where *q* is power of prime number, $n \geq 3$, odd and

$\left|\left\{p,\ p\text{ - prime number}\ \wedge\ p \mid (y-1)\right\}\right| = 4$ that I tried to solve and that could be a suitable topic for a specialized seminar. The students could be introduced to this equation in a seminar where the teacher would show some of the solutions. For better imagination, the high schools students can study this equation as geometric progression with the first member $a_1 = 1$ and quotient $q = a^{\alpha}$, (a - prime, $\alpha \geq 0$, integer).

It is a special type of the equation $\frac{q^n - 1}{q - 1} = y^m$ where $m \geq 2$. W. Ljunggren solved this equation completely when m = 2 (in 1920) and Ljunggren with T. Nagell found solutions if $3 \mid n$ a $4 \mid n$ (in 1943). They found that in these cases there doesn´t exist any other solution except the following:

$$\frac{3^5 - 1}{3 - 1} = 11^2, \qquad \frac{7^4 - 1}{7 - 1} = 20^2, \qquad \frac{18^3 - 1}{18 - 1} = 7^3.$$

Later French mathematicians Y. Bugeaud, M. Mignotte and Y. Roy found solutions for cases when *q* is power of a prime, assign him *p* and *p* divides (y-1) (in 1999) or *m* is a prime and every prime divisor of *q* also divides (y –1) (in 2000). (see [5])

The article of Iranian mathematicians A. a B. Khosravi (who solved this diophantine equation exactly for three prime divisors of (y-1)) became my first motivation for solving this equation. My aim was to continue in their work by trying to solve the equation for four prime divisors of (y-1). So we denote $y = a^{\alpha} b^{\beta} c^{\chi} d^{\delta} + 1$ where a, b, c, d, are primes and $\alpha, \beta, \chi, \delta \geq 1$, integers.

When solved, it is convinient to denote y-1 = A, so A has just four prime divisors, then

$$\frac{q^n - 1}{q - 1} - 1 = \frac{q\left(q^{n-1} - 1\right)}{q - 1} = \frac{q\left(q^{(n-1)/2} - 1\right)\left(q^{(n-1)/2} + 1\right)}{q - 1} = A.$$

Because $\left(q^{(n-1)/2} - 1, q^{(n-1)/2} + 1\right) \mid 2$ and $(q-1) \mid \left(q^{(n-1)/2} - 1\right)$ then holds $\left(q^{(n-1)/2} + 1\right) \mid A$. So $q = a^{\alpha} \vee b^{\beta} \vee c^{\chi} \vee d^{\delta}$. Denote $q = a^{\alpha}$, then $a^{\alpha(n-1)/2} + 1 = b^{\beta}$ or $a^{\alpha(n-1)/2} + 1 = b^{\beta} c^{\chi}$ or $a^{\alpha(n-1)/2} + 1 = b^{\beta} c^{\chi} d^{\delta}$ which means that one of the primes must be even. Fixed a = 2 then $y = 2^{\alpha} b^{\beta} c^{\chi} d^{\delta} + 1$. Now the solutions of the equation could be divided on two parts if *q* is an odd prime or an even prime. For the case that *q* is an odd prime we can divide the solution to nine various types by using $\left(b^{\beta(n-1)/2} - 1, b^{\beta(n-1)/2} + 1\right) = 2$. Four of them are leading immediately to contradiction with the assumption. For remaining types we can find 16 particular solutions.

As a demonstration of the methods used to solve this equation we will explain the case when $q = b^{\beta}$, b is also an odd prime and equation in question is divided in three parts: $b^{\beta(n-1)/4} + 1 = 2c^{\chi}$, $\frac{b^{\beta(n-1)/4} - 1}{b^{\beta} - 1} = 1$, so n = 5 and $b^{\beta(n-1)/2} + 1 = 2^{\alpha - 1} d^{\delta}$. First consider the case when χ=1 (see [2] and [7]), then there exist the solution for $\beta = 1, \delta = 2$. We find two equations: $b + 1 = 2c$ and $b^2 + 1 = 2d^2$. Express *b* from the first equation and substitute to the other equation, then holds $2c^2 - 2c + 1 = d^2$, so $c^2 + (c-1)^2 = d^2 \Rightarrow c^2 = d^2 - (c-1)^2 \Rightarrow c^2 = (d - c + 1)(d + c - 1)$. The prime decomposition in integers is uniquely determined, so one of these possibilities must be correct:

$d - c + 1 = 1 \ \wedge\ d + c - 1 = c^2$, so d = c and then $c^2 - 2c + 1 = (c-1)^2 = 0 \Rightarrow c = 1$, contradiction!

$d - c + 1 = c^2 \ \wedge\ d + c - 1 = 1$, so d = 2- c, but *c* and *d* are primes, contradiction!

$d + c - 1 = c \ \wedge\ d - c + 1 = c \Rightarrow d = 2c - 1 \wedge d = 1$, contradiction!

So any solution doesn't exist in this case.

The solutions when q is even prime number are listed in table.1.

q	**n**	**y**	**conditions**
2	**9**	**2*3*5*17 + 1**	
2^{α}	**9**	$2^{\alpha}*\left(2^{\alpha}+1\right)*\left(2^{2\alpha}+1\right)*\left(2^{4\alpha}+1\right)+1$	$2^{\alpha}+1$, $2^{2\alpha}+1$, $2^{4\alpha}+1$ **are Fermat's primes.**
2^{3}	**5**	$2^{3}*3^{2}$ ***5*13 + 1**	
2^{α}	**5**	$2^{\alpha}*\left(2^{\alpha}+1\right)*\left(2^{2\alpha}+1\right)+1$	$2^{\alpha}+1=$ **d is Fermat's prime and** $2^{2\alpha}+1=\mathrm{b}^{\beta}\mathrm{c}^{\chi}$**.**
2^{α}	**3**	$2^{\alpha}*\left(2^{\alpha}+1\right)+1$	$2^{\alpha}+1=\mathrm{b}^{\beta}\mathrm{c}^{\chi}\mathrm{d}^{\delta}$
2	**2p+1**	**2*** $\left(2^{\mathrm{p}}-1\right)*\left(2^{\mathrm{p}}+1\right)+1$	$2^{\mathrm{p}}-1=$ **d is Mersenne's prime and** $2^{\mathrm{p}}+1=3^{\beta}\mathrm{c}^{\chi}$**, p is prime.**
2^{α}	**4k+3** $\mathbf{k\geq 1}$	$2^{\alpha}*\left(2^{\alpha}+1\right)*\left(\frac{2^{\alpha(\mathrm{n}-1)/2}-1}{2^{\alpha}-1}\right)+1$	$2^{\alpha(\mathrm{n}-1)/2}+1=3^{\beta}\mathrm{c}^{\chi}$ **and** $2^{\alpha(\mathrm{n}-1)/2}-1=\mathrm{d}^{\delta}*\left(2^{\alpha}+1\right)$

Tab. 1: The solutions of the equation $\left(\mathrm{q}^{\mathrm{n}}-1\right)/\left(\mathrm{q}-1\right)=\mathrm{y}$ if $\mathrm{q}=2^{\alpha}$.

Especially the 4th row of the table seems to be very interesting because the only possible solution satisfies the conditions of the equation. If we rewrite the assumptions and the conditions in notation of Fermat's numbers we can say that F_m must be Fermat's prime and in the same time F_{m+1} isn't Fermat's prime. The only one known couple of consecutive Fermat's numbers with the property that the first one is a prime and the second one is a composite number are F_5, F_6. Untill now we are not sure if there exists any other solution or if the number of solutions is infinite.

To simplify the finding or verifying solutions of students' exercises from almost all parts of mathematics (and also for solving the congruences) you can use the computer program PARI (GP/PARI CALCULATOR). This program solves high levels of number theory exercises but it can also help to students at high schools or even elementary schools. (see [8]).

References

Y. BUGEAUD, M. MIGNOTTE, Y. ROY, *On the diophantine equation* $\left(x^{n}-1\right)/\left(x-1\right)=y^{q}$, Pacific Journal of Math., 193 (2) (2000), pp. 257-268.

P. CRESCENZO, *A diophantine equation arises in the theory of finite groups,* Advances in mathematics, 17 (1975), pp. 25-29.

J. HERMAN, R. KUČERA, J. ŠIMŠA, Metody řešení matematických úloh I.(Methods of solving exercises in mathematics), Masaryk University, Brno, 1996, 278 pages.

P. HORÁK, Algebra a teoretická aritmetika I. (Algebra and theoretical aritmetic I.), Masaryk University, Brno, 1994, 196 pages.

A. KHOSRAVI, B. KHOSRAVI, *On the diophantine equation* $\left(q^{n}-1\right)/\left(q-1\right)=y,$ to appear.

M. KŘÍŽEK, F. LUCA, L. SOMER, *17 Lectures on Fermat Numbers: From Number Theory to Geometry,* Springer-Verlag New York, 2001, 257 pages.

Z. POLICKÝ, *Osvojení teorie dělitelnosti pomocí jedné diofantické rovnice* (*Assumption of division theory by using one diophantine equation),* Collection of works from XXI. Intenational Colloquium on the Acquisition Process Management aimed at current issues in science, education and creative thinking development, May 2003, Vyškov, CD-ROM.

B. RŮŽIČKOVÁ, *Upevňování a procvičování učiva o dělitelnosti přirozených čísel pomocí PARI SYSTÉMU (Memorising and practising of natural number's division by using PARI system),* Matematika-fyzika-informatika, 12 (2002/2003), pp. 423-429.

I. M. VINOGRADOV, *Základy theorie čísel (Elementary number theory)*, Nakladatelství ČAV, Praha, 1953, 257 pages.

Web Sites Resources [www1] http:// www.mersenne.org