Mathematica Pannonica
6/2 (1995), 237 – 242

FERMAT'S THEOREM IN JÁNOS BOLYAI'S MANUSCRIPTS

Elemér **Kiss**

Department of Mathematics, Technical University of Tg-Mureş, str. N. Iorga 1, 4300 Tg-Mureş, Romania

Dedicated to Prof. Hans Vogler on the occasion of his 60^{th} birthday

Received October 1994

MSC 1991: 01 A 55, 01 A 70, 11 A 07, 11 A 51

Keywords: Congruence, Fermat's theorem, pseudo-prime numbers, absolute pseudo-prime numbers, Carmichael numbers.

Abstract: The paper relates some number theoretic researches of János Bolyai, on the basis of his manuscripts unknown before.

It is known that if a and m are integer numbers, a is not divisible by m and

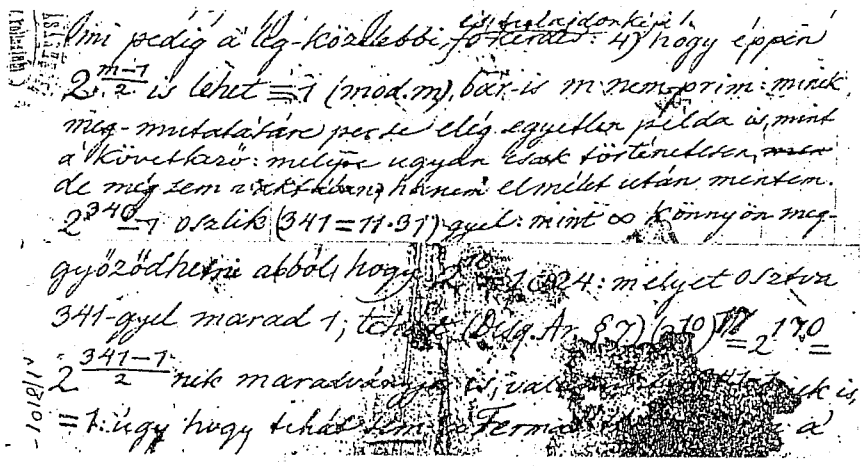
$$a^{m-1} \equiv 1 \pmod{m} \tag{1}$$

for any such a, then m is not necessary prime. We can record as a remarkable event of the history of mathematics, that János Bolyai was among the firsts mathematicians who investigated this question, and who found three such composite numbers m, for which the congruence (1) holds. This statement may appear as unexpected, for all the authors of Bolyai's monographs agree with the opinion that the creator of the non-euclidean geometry hadn't ever been dealing with number theoretic problems.

Most of the manuscripts of János Bolyai (1802–1860) are located in the Teleki–Bolyai Library in Târgu-Mureş. Among these is to be found a letter dated from May 1855, in which he communicates to his father, that the number $2^{(341-1)/2} - 1$ and consequently the number $2^{340} - 1$ too, is divisible by 341. In this letter it is mentioned that he guessed the above example using his own theory, and according to this example, the converse of the Fermat's theorem is not valid even in the case of $a = 2$. Furthermore, the conjecture that the congruence

$2^{(p-1)/2} \equiv 1 \pmod{p}$ is a criterion for the primality of p, fails as well ([1], 1018/1 and 1018/1^v).

Here is a passage of this letter, written in Hungarian:



The text of the manuscript is:

"mi pedig a leg-közelebbi és tulajdonképi fő-kérdés: 4) hogy éppen $2^{m-1/2}$ is lehet $\equiv 1 \pmod{m}$, bár is m nem-prim: minek megmutatására persze elég egyetlen példa is, mint a következő: melyre ugyan csak történetesen de még sem vaktában, hanem elmélet után mentem. 2^{340} - 1 oszlik $(341 = 11 \cdot 31)$gyel: mint végtelen könnyön meggyőződhetni abból, hogy $2^{10} = 1024$: melyet osztva 341-gyel marad 1, tehát (Disq. Ar. & 7.) $(2^{10})^{17} = 2^{170} = 2^{\frac{341-1}{2}}$ nek maradványja is, valamint 2^{341-1} nek is, $= 1$: úgy hogy tehát sem a Fermat theoréma sem a ... "

We can decipher Bolyai's "theory" from the manuscript pages 1265/33 and 1265/33^v. He is concerned here with the conditions on which the congruence

$$a^{pq-1} \equiv 1 \pmod{pq} \tag{2}$$

holds, where p and q are prime numbers and a is an integer nondivisible by p and q. He noticed that due to the congruence

$$a^{(p-1)(q-1)} \equiv 1 \pmod{pq},$$

(2) is true, provided that the congruence

$$a^{p-1}a^{q-1} \equiv 1 \pmod{pq}$$

is true as well. (We mention that a similar reasoning is used by Pál Erdős in 1949 in [4].) But $a^{p-1} \equiv 1 \pmod{p}$ and $a^{q-1} \equiv 1 \pmod{q}$, so there exist such h and k, integers that

$$a^{p-1} = 1 + hp \quad \text{and} \quad a^{q-1} = 1 + kq$$

that is the condition of validity of (2) is

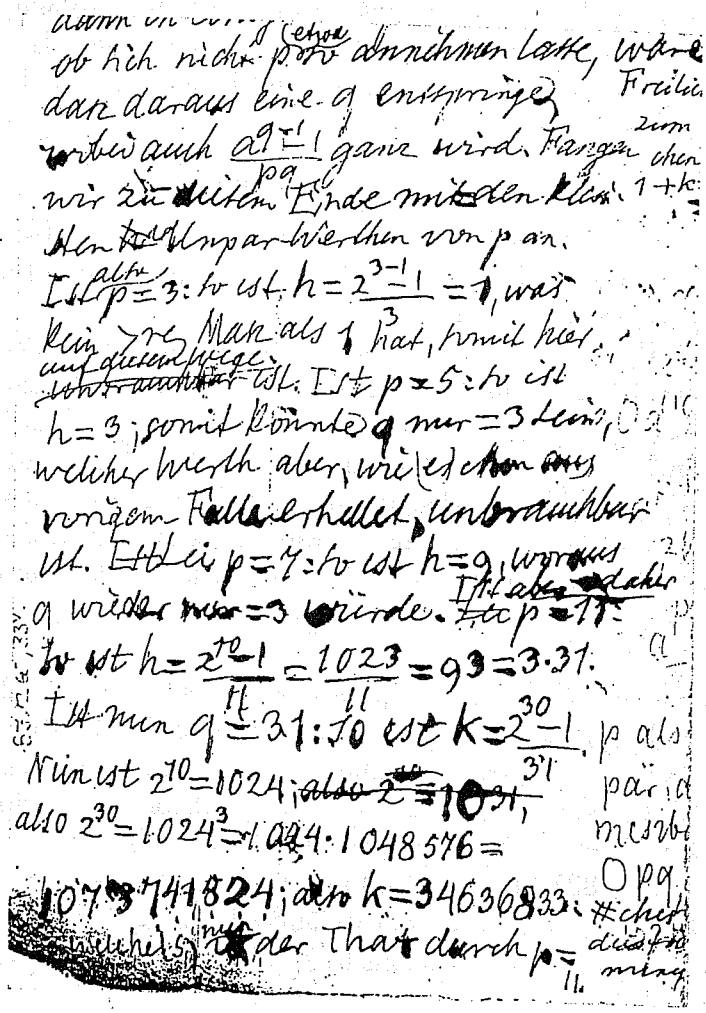
$$hp + kq = (a^{p-1} - 1) + (a^{q-1} - 1) \equiv 0 \pmod{pq}. \tag{3}$$

Now if p divides k and q divides h, then (3) holds. This means, Bolyai says, that (2) is valid for such prime numbers, for which

$$\frac{a^{p-1} - 1}{pq} \quad \text{and} \quad \frac{a^{q-1} - 1}{pq} \quad \text{are both integers.} \tag{4}$$

In the simplest case of $a = 2$ Bolyai checked one by one $p = 3, 5, 7, 11$ and he had been looking for an appropriate value of the prime q. By this way, finally he was led to $p = 11$ and $q = 31$.

We give a part of his computations in manuscript, which is in German:



The text of the manuscript is:

"ob sich nicht p etwa so annehmen lasse, dasz daraus eine q entspringe wobei auch $\frac{a^{q-1}-1}{pq}$ ganz wird. Fangen wir zu diesem Ende mit den kleisten Unpar-Werten von p an. Ist also $p = 3$: so ist $h = \frac{2^{3-1}-1}{3} = 1$ was kein >... Masz als 1 hat, somit hier auf diesem Wege unbrauchbar ist. Ist $p = 5$: so ist $h = 3$; somit könnte q nur $= 3$ sein, welcher Wert aber, wie (es) schon aus vorigen Falle erhellet, unbrauchbar ist. Sei $p = 7$: so ist $h = 9$, woraus q wieder nur $= 3$ würde. Ist aber daher $p = 11$: so ist $h = \frac{2^{10}-1}{11} = \frac{1023}{11} = 93 = 3 \cdot 31$. Ist nun $q = 31$: so ist $k = \frac{2^{30}-1}{31}$. Nun ist $2^{10} = 1024$ also $2^{30} = 1024^3 = 1024 \cdot 1048576 = 1073741824$; also $k = 34636833$: welches nun der That durch $p = 11$ meszbar ist: ... "

János Bolyai — just like many others — had been searching a formula of all primes, as well [6]. Indeed, this was the stimulus for his investigations concerning Fermat's theorem. This goal is expressed even in the above quoted letter. The "nice conjecture" was broken up by the counter example found by him. He was doubtlessly deeply concerned with this problem, for he also built up the formula $4^{14} \equiv 1 \pmod{15}$ (see [1], $1265/39^v$), and moreover, he wrote

$$2^{2^{32}} \equiv 1 \pmod{2^{32}+1}, \tag{5}$$

as we can see in [1], 1550/1. Here is the way followed by János Bolyai: he started from the obvious $2^{32} \equiv -1 \pmod{2^{32}+1}$ and performed the appropriate number of squaring.

One of the examples of János Bolyai, namely the congruence $2^{340} \equiv 1 \pmod{341}$, was found first by F. Sarrus in 1820 and also by an unknown author in 1830, as L. E. Dickson relates in [3]. Bolyai, who lived and worked isolated from the scientific community, had no possibility to know these works. He attained his achievements independently and pursuing his own original way. This is backed up certainly also by the fact, that congruences like (5) in which arise the numbers

$$m = F_k = 2^{2^k} + 1$$

appear only much later in the papers of M. Cipolla (1903) and A. Cunnigham (1904). It is maybe of some interest to mention that the researches for the composite numbers m from the congruence (1) — these became the so called pseudo-prime and absolute pseudo-prime or Carmichael numbers — were started only in 1876 (E. Lucas) and were broadened since 1897 (J. H. Jeans) and later in this century (by R. D. Carmichael, M. Cipolla, E. B. Escott and others [3]).

These are not the only reasons to appreciate the Bolyai's attempts.

Let us take in (4) $a = 2$ to obtain

$$2^{p-1} \equiv 1 \pmod{q} \quad \text{and} \quad 2^{q-1} \equiv 1 \pmod{p}. \tag{6}$$

In other words, Bolyai says if the conditions (6) hold, then it follows

$$2^{pq-1} \equiv 1 \pmod{pq}.$$

This is precisely a well known theorem of J. H. Jeans, published in 1897 [3]. Therefore Bolyai preceded Jeans by more than 40 years.

Using Bolyai's method we can discover other composite numbers m of (1), too. Unfortunately, this method can be applied only for those m, which are products of exactly two prime numbers. Nevertheless the method extends with no difficulty for the case of products of arbitrary number of primes. The sequence of ideas of Bolyai leads to the following generalization of Jeans's theorem, which probably is nothing but a "folk-theorem" of the Number Theory.

Theorem 1. *Let $p_1, p_2, \dots p_n$ be prime numbers ($n \geq 1$), and let a be a number non-divisible by any one of these numbers. If*

$$\begin{aligned} a^{p_1 p_2 \cdots p_{n-1}-1} &\equiv 1 \pmod{p_n} \\ a^{p_1 \cdots p_{n-2} p_n - 1} &\equiv 1 \pmod{p_{n-1}} \\ &\dots \\ a^{p_2 p_3 \cdots p_n - 1} &\equiv 1 \pmod{p_1} \end{aligned}$$

then

$$a^{p_1 p_2 \cdots p_n - 1} \equiv 1 \pmod{p_1 p_2 \cdots p_n}\,. \tag{7}$$

Proof. From $a^{p_1 p_2 \cdots p_{n-1}-1} \equiv 1 \pmod{p_n}$ we deduce $a^{p_1 p_2 \cdots p_n - p_n} \equiv 1 \pmod{p_n}$ and from this using $a^{p_n - 1} \equiv 1 \pmod{p_n}$ it follows

$$a^{p_1 p_2 \cdots p_n - 1} \equiv 1 \pmod{p_n}.$$

By an analogous way we have also

$$\begin{aligned} a^{p_1 p_2 \cdots p_n - 1} &\equiv 1 \pmod{p_{n-1}} \\ &\dots \\ a^{p_1 p_2 \cdots p_n - 1} &\equiv 1 \pmod{p_1}. \end{aligned}$$

Taking the product of these congruences we get (7). $\Diamond$

It can be shown easy now, applying this theorem, that, for instance, $561 = 3 \cdot 11 \cdot 17$ is a Carmichael number. This was found by him in 1909, [2]. Indeed, elementary computations prove that for all the numbers a non-divisible by anyone of 3, 11 and 17, we have $a^{3 \cdot 11 - 1} \equiv 1$

(mod 17), $a^{11\cdot 17-1} \equiv 1 \pmod 3$, and $a^{17\cdot 3-1} \equiv 1 \pmod{11}$. We get therefore

$$a^{3\cdot 11\cdot 17-1} \equiv 1 \pmod{3\cdot 11\cdot 17}.$$

It can be checked similarly that (1) is true for $m = 13\cdot 37\cdot 73\cdot 457$ and for all a, non-divisible by the prime numbers 13, 37, 73 and 457 (Carmichael 1912, [3]).

Literatur

[1] JÁNOS BOLYAI: Manuscripts, Târgu-Mureş, Teleki–Bolyai Library.

[2] CARMICHAEL, R. D.: Note on a new number theory function, *Bull. Am. Soc.* **16** (1909–1910), 232–238.

[3] DICKSON, L. E.: History of the Theory of Numbers, (Chap. III.), Chelsea, New York, 1952.

[4] ERDŐS, P.: On the Converse of Fermat's Theorem, *Am. Math. Monthly* **56** (1949), 623–624.

[5] SIERPINSKI, W.: Elementary Theory of Numbers, Warszawa, 1964.

[6] STÄCKEL, P.: Bolyai Farkas és Bolyai János geometriai vizsgálatai I, Budapest, 1914.