Mathematica Pannonica
15/2 (2004), 283–288

ON A CONGRUENCE BY JÁNOS BOLYAI, CONNECTED WITH PSEUDOPRIMES

Elemér **Kiss**

Department of Mathematics and Computer Sciences, Sapientia University of Tg-Mureş, Tg-Mureş, Romania

József **Sándor**

Department of Mathematics and Computer Sciences, Babeş–Bolyai University of Cluj, Romania

Received: August 2004

MSC 2000: 11 A 07; 01 A 55

Keywords: Fermat's theorem, pseudoprimes, Fermat's quotient, congruences, János Bolyai's manuscripts.

Abstract: A congruence of János Bolyai, discovered recently in scattered manuscripts of Bolyai is analyzed, and its interesting connection with pseudoprimes and Fermat's quotients is studied.

1. Introduction

From Bolyai's manuscripts recently found in the Teleki–Bolyai Library of Tg-Mureş – Marosvásárhely (Romania) it is clear that the famous geometer János Bolyai (1802–1860) was deeply interested also in number theoretical problems. Specially, he tried to discover a general formula for the primes. Once he thought that this is provided by Fermat's "little" theorem: if p is a prime, and a a positive integer such that $(a, b) = 1$, then

E-mail addresses: elemer@ms.sapientia.ro, jjsandor@hotmail.com

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

On suggestions of his father, Farkas Bolyai (1775–1856), he investigated a search for a proof of the converse theorem. If this had been true, then the desired formula for primes would be obtained. After some experiences however he had realized that such a proof was impossible. He found that

$$2^{340} \equiv 1 \pmod{341},$$

although $341 = 11 \cdot 31$ is composite.

The composite numbers p satisfying relation (1) are now called as pseudoprimes (in base a). János Bolyai discovered the pseudoprime 341 (and many other pseudoprimes [5]) by proving previously the following theorem: If p and q are primes, a is a positive integer not divisible by p and q, further if $a^{p-1} \equiv 1 \pmod{q}$, $a^{q-1} \equiv 1 \pmod{p}$, then

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

This theorem corresponds exactly to the theorem of J. H. Jeans which he published in 1898, decades after the death of János Bolyai [4].

2. A new congruence

By letting $q = p$ in congruence (2), Bolyai deduced that

$$a^{p^2-1} \equiv 1 \pmod{p^2} \tag{3}$$

([3], 1265/33). We have not found results by him on this relation, though he noted the particular case $5^3 \equiv 1 \pmod{4}$.

In what follows, our aim will be to determine (or to reduce to known notions) all pairs (a, p) which satisfy relation (3).

By elementary arguments the following theorems can be proved:

Theorem 1. *If $p = 2$, then (3) is true iff*

$$a \equiv 1 \pmod{4}.$$

Theorem 2. *If $p = 3$, then (3) is true iff*

$$a \equiv \pm 1 \pmod{9}.$$

Theorem 3. *If $p = 5$, then (3) is true iff*

$$a \equiv \pm 1 \pmod{25} \text{ or } a \equiv \pm 7 \pmod{25}.$$

Theorem 4. *If $p = 7$, then (3) is true iff*

$$a \equiv \pm 1 \pmod{49} \text{ or } a \equiv \pm 18 \pmod{49}.$$

We will present here only the **proof of Th. 3**, the other results will follow on the same lines.

Let us consider therefore $p = 5$, i.e. the congruence

$$a^{24} \equiv 1 \pmod{25}. \tag{4}$$

Let us write the identity

$$\begin{aligned} a^{24} - 1 = (a-1)(a+1)(a^2 - a + 1)(a^2 + a + 1) \times \\ \times (a^2+1)(a^4+1)(a^4 - a^2 + 1)(a^8 - a^4 + 1). \end{aligned} \tag{5}$$

Clearly $a = 5k + r$ ($k \geq 0$, $r \in \{\pm 1, \pm 2\}$). If $a = 5k + 1$, then $a - 1 \equiv$ $\equiv 0 \pmod{5}$. Then no other term of (5) is divisible by 5. Indeed, it is immediate that $a+1 \equiv 2 \pmod{5}$, $a^2 - a + 1 \equiv 1 \pmod{5}$, $a^2 + a + 1 \equiv 3 \pmod{5}$, $a^2+1 \equiv 2 \pmod{5}$, $a^4+1 \equiv 2 \pmod{5}$, $a^4 - a^2 + 1 \equiv 1 \pmod{5}$, $a^8 - a^4 + 1 \equiv 1 \pmod{5}$. Therefore $a - 1 \equiv 0 \pmod{5}$, and from (4) it results $a - 1 \equiv 0 \pmod{25}$, i.e. $a \equiv 1 \pmod{25}$.

For the case $a = 5k-1$ we proceed similarly, but not only $a+1 \equiv 0 \pmod{5}$ is possible, and this yields as above that $a \equiv -1 \pmod{25}$.

Let now $a = 5k + 2$. Then from the terms of the right side of (5) only $a^2 + 1$ is divisible by 5. Since $a^2 + 1 = 25k^2 + 20k + 5 = 5(5k^2 + + 4k + 1)$, we must have that $5k^2 + 4k + 1$ is divisible by 5, so $4k + 1 \equiv 0 \pmod{5}$. From $4k + 1 = 5k - k + 1$ it remains $k - 1 \equiv 0 \pmod{5}$. Writing $k - 1 = 5u$, i.e. $a = 5k + 2 = 5(5u + 1) + 2 = 25u + 7$, we get $a \equiv 7 \pmod{25}$.

In the case $a = 5k - 2$ we obtain in an analogous way that $a \equiv -7 \pmod{25}$. $\Diamond$

We note that for the case $p = 7$ (Th. 4), the study of the above presented method is slightly more difficult since then a linear diophantine equation of type

$$5k + 1 = 7l$$

will appear so k has the form $k = 7t - 3$ etc.

Now, let us consider the most general case! We will prove the following result:

Theorem 5.

$$a^{p^2-1} \equiv 1 \pmod{p^2} \text{ iff } a^{p-1} \equiv 1 \pmod{p^2}. \tag{6}$$

Proof. Put $a^{p-1} = x$. Since $p^2 - 1 = (p-1)(p+1)$, one can write

$$(*) \qquad a^{p^2-1} - 1 = x^{p+1} - 1 = (x-1)(1 + x + \cdots + x^p).$$

If $a^{p-1} \equiv 1 \pmod{p^2}$, i.e. $p \mid x-1$, then by identity $(*)$ one has clearly also $a^{p^2-1} \equiv 1 \pmod{p^2}$, so a part of the theorem is proved.

Conversely, let us suppose that the left-side congruence (i.e. (3)) is true. Then a cannot be divisible by p, so $(a,p) = 1$. From Fermat's theorem (i.e. (1)) one has $p \mid x-1$.

Now we prove that

$$(7) \qquad p^2 \mid (1 + x + \cdots + x^p).$$

Indeed, since $1+x+\cdots+x^p = (x-1)+(x^2-1)+\cdots+(x^p-1)+(p+1)$, where each of $x-1, x^2-1, \ldots, x^p-1$ is divisible by p (on base of (1)), but $p+1$ cannot be divisible by p. Thus if (3) is valid, by (7), $x-1$ must be divisible not only by p, but by p^2, too. $\Diamond$

The following theorem generalizes Th. 5, and has a similar proof:

Theorem 6 *Let $k \geq 2$ be a fixed integer. Then*

$$a^{p^k-1} \equiv 1 \pmod{p^k} \quad \textit{iff } a^{p-1} \equiv 1 \pmod{p^2}.$$

The proof is based on the identity $a^{p^k-1} = x^{m+1} - 1 = (x-1)(1+ +x+\cdots+x^m)$, where x is defined as above, while $m = p+p^2+\cdots+p^{k-1}$. We omit the details. $\Diamond$

Finally, another generalization of Th. 5. is contained in the following:

Theorem 7.

$$a^{p^k-1} \equiv 1 \pmod{p^k} \quad \textit{iff } a^{p^{k-1}} \equiv 1 \pmod{p^k}.$$

Proof. First remark that, if one of the above congruences is true, then $(a,p) = 1$. Now, by Euler's divisibility theorem applied to $n = p^k$ gives

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

From the identity

$$a^{p^k-1} = a^{p^k-p^{k-i}} \cdot a^{p^{k-1}-1} = (1 + Mp^k) \cdot a^{p^{k-1}-1} \qquad (M \geq 1 \text{ integer})$$

we get that

$$a^{p^k-1} - 1 = a^{p^{k-1}-1} - 1 + M'p^k \quad (M' \geq 1 \text{ integer}).$$

Now this identity implies at once the result. $\Diamond$

Remark that for $k = 2$ Th. 7 implies (with a new proof) the result of Th. 5.

The following result can be proved similarly to Th. 7:

Theorem 8. *Let $n > 1$ be an arbitrary integer, and let p^k be the highest power of a prime p which divides n. Put $N = \frac{n}{p^k}$. Then*

$$a^m \equiv 1 \pmod{n} \text{ iff } a^s \equiv 1 \pmod{n},$$

where

$$m = p^k\ \varphi(N) \quad \text{and } s = p^{k-1}\ \varphi(N) \quad (\varphi(N) \text{ is Euler's function}).$$

For $n = p^k$, Th. 7 *is reobtained.*

We note that, by an extension of Euler's theorem, due to R. T. Hansen (see [7]):

$$a^{\varphi(n)+1} \equiv a(\mathrm{mod}\, n)$$

where $(a, n) = d$, and $(a, n/d) = 1$, we can slightly extend Th. 8 as follows (the notation is as above):

Theorem 9. *Let $(a, n) = d$, and suppose that $(a, n/d) = 1$. Then*

$$a^u \equiv a(\mathrm{mod}\, n) \quad \text{iff } a^v \equiv a(\mathrm{mod}\, n)$$

were

$$u = p^k\varphi(N) + 1 \quad \text{and} \quad v = p^{k-1}\varphi(N) + 1.$$

When $d = 1$, i.e. $(a, n) = 1$, Th. 8 *is reobtained.*

3. Remarks

1. Via Th. 5 a new proof can be offered for Ths. 1–4.

2. The history of mathematics attributes to Abel (1828) the question of examples for the congruence

$$a^{p-1} \equiv 1(\mathrm{mod}\, p^2) \quad (a \geq 2). \tag{8}$$

For $p \leq 37$ Jacobi found the following examples:

$$3^{10} \equiv 1 \pmod{11^2}, \quad 9^{10} \equiv 1 \pmod{11^2},$$
$$14^{28} \equiv 1 \pmod{29^2}, \quad 18^{36} \equiv 1(\mathrm{mod}\, 37^2).$$

For $a = 2$, (8) gives

$$2^{p-1} \equiv 1(\mathrm{mod}\, p^2) \tag{9}$$

Such primes p are called as Wieferich primes. In 1909 Wieferich gave a connection between the congruence (9) and Fermat's last (or "great") theorem. The numbers $p = 1093$ and $p = 3511$ satisfy relation (9), but the set of such primes seems to be very sporadic. These examples were found by Meissner and Beeger in 1913, resp. 1922. In 1985 Crandall,

Dilcher and Pomerance have shown that no other Wieferich primes do exist under $p < 4 \cdot 10^{12}$. Still, today it is believed that (9) (and generally, (8)) has infinitely many solutions. This seems to be very difficult (perhaps even unattackable at present) (see e.g. [6], [7]).

The quotient $q_p(a) = \frac{a^{p-1}-1}{p}$ is called also as the Fermat quotient (in base a). This quotient has many interesting properties. E.g. if p doesn't divide ab, then

$$q_p(ab) \equiv q_p(a) + q_p(b) \pmod{p}.$$

Other properties: $q_p(p-1) \equiv 1 \pmod{p}$, $q_p(p+1) \equiv -1 \pmod{p}$ etc.

For certain new properties and generalizations, with connections to other number theoretical results, see [1], [2], [7], where further references can be found.

References

[1] AGOH, T.: On Fermat and Wilson quotients, *Exp. Math.* **14** (1996), 145–170.

[2] AGOH, T., DILCHER, K. and SKULA, L.: Fermat's quotients for composite moduli, *J. Number Theory* **66** (1997), nr. 1, 29–50.

[3] BOLYAI, JÁNOS: Manuscripts, Târgu Mureş – Marosvásárhely, Teleki–Bolyai Library.

[4] JEANS, J. H.: The Converse of Fermat's Theorem, *Messenger of Mathematics* **27** (1897–1898), 174.

[5] KISS, E.: Fermat's theorem in János Bolyai's manuscripts, *Mathematica Pannonica* **6** (1995), no. 2, 237–242.

[6] RIBENBOIM, P.: *The new book of prime number records*, Springer-Verlag, 1996.

[7] SÁNDOR, J.: *Handbook of number theory II*, to appear, Kluwer Academic Publishers, The Netherlands.