Apsny Sciences

FERMAT'S THEOREM: ANOTHER PROOF

RASIM A. KAMLIYA

BILINGUA
in association with
the Academy of Sciences of Abkhazia

R.A. Kamliya. ***Fermat's Theorem: Another Proof.*** *Monograph. "Apsny Sciences" series. – Sukhum-Moscow: BILINGUA, 2011.*

This Monograph presents an elementary proof of Fermat's theorem which is built upon certain properties of power residues.

For those interested in the theory of numbers.

"Apsny" is an ancient name of Abkhazia, a small Caucasian country where sciences have been paid much attention to.

This short monograph is the second book in the "Apsny Sciences" series.

ISBN 978-5-902868-10-1

CONTENTS

Preface

Over four centuries ago Pierre de Fermat put forward his famous hypothesis: "*It is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general, any power higher than the second into two like powers*" [2]. Ever after many number theorists tried to prove the theorem, each suggesting his own way.

The approach by R.A. Kamliya demonstrated in this short publication is the result of a long research and thorough development. His previous study [1] unambiguously proved that the power residues modulo a prime can be unexpandable into a sum of two power residues. However, if at least one power residue is expandable, all the power residues are expandable modulo the selected number.

The present theory includes an essential preliminary theorem on expandability and the following original proof of Fermat's theorem. The references are at the end of the book.

1. EXPANSION OF POWER RESIDUES

To prove Fermat's Theorem preliminary prove the following.

Theorem. If one of the residues of the odd prime ***p*** power modulo prime ***m*** is expandable into a sum of two like power residues modulo ***m***, then an expansion of any power ***p*** residue is a product of this power ***p*** residue and the expansion of 1 into the sum of two like power residues modulo m, and the corresponding expansion of 1 into the sum of two power ***p*** residues exists.

Proof. By the hypothesis there exists an expansion of a power residue into a sum of two power residues.

$$v \equiv v_1 + v_2 (\mathrm{mod}\, m) \qquad (1)$$

If at least one odd prime ***p*** power residue is expandable into a sum of two power residues, then as follows from 5.5 [1] all the power residues are expandable, moreover, various variants of expandability are possible.The criterion of expandability is the presence of adjacent power residues [1].

If we have a couple of the adjacent power residues ***u*** and *(u+1)*, the expansion of 1 into the sum of two power residues is easy to find:

$$1 \equiv (m-u) + (u+1) (\mathrm{mod}\, m) \qquad (2)$$

The number *(m-u)* is a power residue as the power ***p*** is an odd prime. The multiplication of the latter comparison by any power residue produces its expansion into a sum of two power residues, as in the right part the power residues product gives a power residue (Property 1of power residues, [1]).

Thus, if we have a couple of adjacent power residues, we can find the expansion of any power residue. For each couple there is one particular variant of expandability of 1 and, therefore, of any power residue.

Now, we have to demonstrate that for any expansion of a power residue there exists a corresponding expansion of 1 into a sum of two power residues which will give the initial expansion of the power residue (1) at its multiplication by ***v***.

Multiply the initial expansion (1) by the number v' inverse of ***v*** modulo ***m***, i.e. satisfying the comparison:

$$v \cdot v' \equiv 1 (\mathrm{mod}\, m) \qquad (3)$$

After the multiplication have

$$1 \equiv v_1 \cdot v' + v_2 \cdot v' (\mathrm{mod}\, m) \qquad (4)$$

Such a number v' exists, as the number ***m*** is a prime and for any number inverse of the modulus there exists an inverse number.

This number v' is a power residue, as otherwise the product of the power residue ***v*** by v' would have given a power nonresidue (Property 6 of power residues [1]), but 1 is a power residue.

The right part of the latter comparison has two products of the power residues, each of them being a power residue (Property 1 of power residues [1]). Therefore, the comparison (4) is the expansion of 1 into a sum of two power residues.

The multiplication of the comparison (4) by v' gives the initial comparison (1), which convinces us in the discovery of the corresponding expansion of 1 into a sum of two power residues. Likewise we can unambiguously obtain the expansion of 1 into a sum of two power residues which satisfies any variant of expansion of any power residue. The variant is determined by the couple of the adjacent power residues. This completes the proof of the theorem.

2. PROOF OF FERMAT'S THEOREM

Write Fermat's equation for the prime power ***p*** as

$$c^p = b^p + a^p \quad (1)$$

And suppose that it has an integer nonzero solution in the finite numbers at pairwise coprimes ***a***, ***b***, ***c***.

If the equation has a solution, then its left and right parts are congruous modulo any number ***m***.

$$c^p \equiv b^p + a^p (\text{mod m}) \quad (2)$$

If the notations $V_c \equiv c^p (\text{mod m})$, $V_b \equiv b^p (\text{mod m})$, $V_a \equiv a^p (\text{mod m})$ are introduced, the comparison (2) takes the following form:

$$V_c \equiv V_b + V_a (\text{mod m}) \quad (3)$$

If solutions to the comparison (3) exist, the expandability of power ***p*** residues into a sum of two power ***p*** residues modulo ***m*** is said to exist.

If the equation of Fermat (1) has a solution, then the comparison (2) has to be satisfiable modulo any number.

Take two prime moduli $m_1 > c^p$ and $m_2 > c^p$, $m_1 < m_2$.

Assume that the power ***p*** residues modulo m_1 and m_2 are expandable into a sum of two power residues. If not, the comparison (3) would not have had a nontrivial solution, therefore, there only remains a trivial solution when one of the numbers ***a***, ***b***, ***c*** is congruent to 0 modulo m_1 or m_2. The latter means that our assumption of the solution existence in (1) is wrong, as we selected $m_1 > c^p$, $m_2 > c^p$. To prove Fermat's theorem Fermat's equation has to be considered in view of expandability of the powers of numbers, following the hypothesis of the theorem [2].

As follows from the above proven theorem any expansion of power residues can be written as a product of this power residue and the expansion of 1 into a sum of two power residues. Therefore, there exists the expansion of 1

$$1 \equiv u_{1,1} + u_{2,1} (\text{mod} m_1) \quad (4)$$

such that its multiplication by V_c will produce the comparison

$$V_c \equiv u_{1,1} \cdot V_c + u_{2,1} \cdot V_c (\text{mod} m_1) \quad (5)$$

i.e. the comparison (3),

where $V_b \equiv u_{1,1} \cdot V_c (\text{mod} m_1)$, $V_a \equiv u_{2,1} \cdot V_c (\text{mod} m_1)$.

If the comparison (3) has to be also satisfiable modulo the prime m_2, there has to exist the expansion of 1 modulo m_2

$$1 \equiv u_{1,2} + u_{2,2} (\text{mod} m_2) \quad (6)$$

which also has to produce the comparison (3) after its multiplication by V_c

$$V_c \equiv u_{1,2} \cdot V_c + u_{2,2} \cdot V_c (\text{mod} m_2) , \quad (7)$$

where $V_b \equiv u_{1,2} \cdot V_c (\text{mod} m_2)$, $V_a \equiv u_{2,2} \cdot V_c (\text{mod} m_2)$.

If the comparison (3) is possible modulo m_1 and modulo m_2, it has to be possible modulo the product of moduli $m_1 \cdot m_2$.

Now, obtain the expansion of V_c modulo $m_1 \cdot m_2$. For this find the expansion of 1 into a sum of two power residues modulo $m_1 \cdot m_2$ by simultaneously solving the comparisons (4), (6) [1]. The expansions (4) and (6) are different, as $m_1 \neq m_2$.

Find the right part summands as follows:

$$u_1 \equiv m_2 \cdot m_1' \cdot u_{1,1} + m_1 \cdot m_2' \cdot u_{1,2} (\text{mod} m_1 \cdot m_2) \quad (8)$$

$$u_1 \equiv m_2 \cdot m_1' \cdot u_{2,1} + m_1 \cdot m_2' \cdot u_{2,2} (\text{mod} m_1 \cdot m_2) , \quad (9)$$

where $m_2 \cdot m_1' \equiv 1 (\text{mod} m_1)$, $m_1 \cdot m_2' \equiv 1 (\text{mod} m_2)$.

Now, can write the expansion of 1 into a sum of two power residues modulo $m_1 \cdot m_2$

$$1 \equiv u_1 + u_2 (\text{mod} m_1 \cdot m_2) \quad (10)$$

as well as the expansion of V_c modulo $m_1 \cdot m_2$

$$V_c \equiv u_1 \cdot V_c + u_2 \cdot V_c (\text{mod} m_1 \cdot m_2) \quad (11)$$

The truth of the latter comparison modulo $m_1 \cdot m_2$ can be justified by its check modulo m_1 and modulo m_2. Now, go over to the solutions for (10), (11). The residues u_1 and u_2 in (10) are power residues modulo $m_1 \cdot m_2$. They have some solutions

$$1 \equiv k_1^{\,p} + k_2^{\,p} (nod m_1 \cdot m_2) \qquad (12)$$

The power residue $V_c \equiv c^p (\mathrm{mod}\, m_1 \cdot m_2)$. The number c^p is the least positive power residue modulo $m_1 \cdot m_2$ by the determined above $m_1 > c^p$, $m_2 > c^p$. Set these notations of the power residues in (11):

$$c^{\,p} \equiv k_1^{\,p} \cdot c^p + k_2^{\,p} \cdot c^p (\mathrm{mod}\, m_1 \cdot m_2) \qquad (13)$$

Obviously, $k_1^{\,p} \cdot c^p > m_1 \cdot m_2$, $k_2^{\,p} \cdot c^p > m_1 \cdot m_2$. If not, c^p could have been cancelled out in (13), which means that Fermat's equation would have been impossible to obtain.

In the course of proving the theorem we have to answer the question if the equation (1) is possible to obtain from (13). Had this been possible, the comparison (2) would have been possible modulo $m_3 > m_2$. However, the expansion of 1 modulo m_3 differs from (4), (6), (10). This is why we have to find the expansion of 1 modulo m_3 and further on solve this comparison simultaneously with (10) and obtain the expansion of 1 into a sum of two power residues modulo $m_1 \cdot m_2 \cdot m_3$. In the obtained solution modulo $m_1 \cdot m_2 \cdot m_3$ the right part summands have to be greater than $m_1 \cdot m_2 \cdot m_3$.

Thus, the process of the search of the solutions for the comparison (3) modulo $m_1 \cdot m_2 \cdot m_3$ has been reduced to the search of the expansion of 1 modulo m_3, if in general there is the expandability of power residues modulo m_3, and its simultaneous solving with (10), as well as multiplication by c^p. For each next prime modulus the above described process must be repeated. The amount of primes is infinite, therefore, it is impossible to find the solution to Fermat's equation in finite numbers.

Fermat's theorem for odd prime powers is true.

Now, if in Fermat's equation the power is a composite number, the proof should be partitioned into the two cases:

1. The power has the form 2^i.

2. The power is a multiple of some odd prime number.

Consider each case separately.

Case 1. If the power has the form 2^i, write it as $n = 4 \cdot 2^{i_1}$. If $i_1 = 0$, then n=4 and the theorem for this power was proven by Fermat himself. Hence, suppose $i_1 > 0$.

Write Fermat's equation as

$$(c^{2^{i_1}})^4 = (b^{2^{i_1}})^4 + (a^{2^{i_1}})^4 \qquad (14)$$

If consider the latter equation as Fermat's equation power 4, then it has no solution as was proven by Fermat, not to mention that these solutions have to be some powers of the numbers. Hence, Fermat's equation has no solution for any powers $n = 2^i$ at i>1.

Case 2. Let the power be a multiple of some odd prime ***p***, i.e. $n = n_1 \cdot p$. Then Fermat's equation can be written as follows:

$$(c^{n_1})^p = (b^{n_1})^p + (a^{n_1})^p \qquad (25)$$

If consider the latter equation as Fermat's equation for the odd prime power ***p***, then it has no solution as proven above for any odd prime ***p***, not to mention that these solutions have to be some powers of the numbers *a, b, c*. Hence, Fermat's equation has no solutions for any $n = n_1 \cdot p$ at $n_1 > 0$.

The two cases considered above exhaust all the powers greater than 2.

This completes the proof of Fermat's theorem.

References

1. Kamliya, R.A. Power Residues Expandability and the Theorem of Pierre de Fermat / Monograph. “Apsny Sciences” series. – Moscow: Bilingua, 2011.
2. Ribenboim, P. Fermat's Last Theorem for Amateurs. NY: Springer. First edition, 1999.

Задник

КАМЛИЯ РАСИМ АРКАДЬЕВИЧ

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ ФЕРМА

Монография

Русская редакция, перевод, английская редакция, набор и оригинал-макет выполнены в научно-образовательном центре «Билингва»

www.bilingua.ru

e-mail: bilingua@bilingua.ru

Тел: +7 985 210 74 25

+7 495 210 74 25

+7 495 785 24 99

2011 г.

Тираж 500 экз.