Apsny Sciences

POWER RESIDUES EXPANDABILITY
AND
THE THEOREM OF PIERRE DE FERMAT

RASIM A. KAMLIYA

BILINGUA
in association with
the Academy of Sciences of Abkhazia

R.A. Kamliya. ***Power Residues Expandability and the Theorem of Pierre de Fermat. Monograph. "Apsny Sciences" series. – Moscow, BILINGUA, 2011.***

The monograph is dedicated to the theorem of Fermat. It considers various properties and relations of numbers to satisfy Fermat's equation, problems of power residues expansion into the sum of two power residues, properties of Pythagorean numbers, and a series of novel theorems to exclusively prove Fermat's theorem by techniques of elementary theory of numbers.

For those interested in the theory of numbers.

ISBN 978-5-902868-08-8

Contents

Note

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

This monograph is the first book in the "Apsny Sciences" series.

Preface

Since 1670 mathematics has known a dispute whether Pierre de Fermat managed to discover an original proof of his theorem.

Subsequent approaches have brought some positive results though not all of them may be used to prove the famous theorem. However, all those might be of interest in their own right to mathematics.

Yet, there has been certain reason to believe that while analysing the expandability of power residues Fermat conjectured his famous theorem. It is adduced in P. Ribenboim's book *Fermat's Last Theorem* as follows: *"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"*.

In the present study the theorem is proved by way of power residues expansion into the sum of two power residues. If a power residue is expandable modulo a prime, any power residue is expandable. Yet, this in no way means that a sum of two power residues is a power residue.

Here the expandability of quadratic residues shows that any Pythagorean triple includes a number divisible by three, and a number divisible by five.

Special properties and relations of numbers consistent with Fermat's equation, in case it has a solution, are described in Chapter 1.

Noted properties of Euler's and Fermat's comparisons are presented in Chapter 2.

Certain properties of power residues obtained by using a residue matrix are revealed in Chapter 3.

Power residue properties and expansion into the sum of two power residues are presented in Chapter 4 and Chapter 5.

The proof of Fermat's theorem by two non-contradictory ways is demonstrated in Chapter 6.

This monograph being the result of a long research and thorough development, its author looks forward to seeing that it will serve a contribution to the theory of numbers.

The author expresses his many thanks to those who assisted this publication: the Academy of Sciences of Abkhazia, colleagues and official readers, translators, publisher.

Chapter 1. Fundamental Theorems and Relations

1.1 Theorem 1

Theorem 1. *Let p be a prime, b and c be coprimes incongruous modulo* ***p****. Then in the equation* $c^p - b^p = (c-b)(c^{p-1} + \ldots + b^{p-1})$ *the right part factors* $a_1 = c-b$ *and* $a_2 = c^{p-1} + \ldots + b^{p-1}$ *do not have a common divisor.*

Proof. Let $\mathbf{p}_1$ be a prime, a divisor of $\mathbf{a}_1$. Then $a_1 \equiv 0 (mod p_1)$ or $c-b \equiv 0 (mod\ p_1)$ or $c \equiv b (mod\ p_1)$.

The latter implies that $c = p_1 q + r$, $b = p_1 q_1 + r$,

$0 < r < p_1$,

where **q**, $\mathbf{q}_1$, **r** are integers. Hence,

$$a_1 = c - b = p_1 q + r - p_1 q_1 - r = p_1 (q-q_1) \qquad (1)$$

$$a_2 = (p_1 q + r)^{p-1} + \ldots + (p_1 q_1 + r)^{p-1} = k p_1 + p r^{p-1}, \qquad (2)$$

where ***k*** is an integer.

Since ***c*** and ***b*** under the hypothesis of the theorem are incongruous *modulo* ***p***, any number $\boldsymbol{p}_1$, to the modulus of which ***c*** and ***b*** are congruous, is not equal to ***p***.

(1) implies that the number $\boldsymbol{p}_1$ divides $\boldsymbol{a_1}$, but does not divide $\boldsymbol{a}_2$, as in this case $\boldsymbol{p}_1$ has to divide the second summand in (2), i.e. $\boldsymbol{p r^{p-1}}$**.** This is impossible as ***p*** is a prime number, and $\boldsymbol{r < p_1}$, where $\boldsymbol{p}_1$ is a prime number. For $\boldsymbol{p}_1$ we can take any prime divisor of $\boldsymbol{a}_1$ greater than 1. If any prime divisor of $\boldsymbol{a_1}$ does not divide $\boldsymbol{a}_2$, then $\boldsymbol{a_1}$ and $\boldsymbol{a}_2$ are coprimes. *This completes the proof of Theorem 1.*

1.2. Theorem 1A

Theorem 1A. *Let* **p** *be a prime,* **b** *and* **c** *be coprimes, while* **c+b** *is not a multiple of* **p.** *Then in the equation* $c^p + b^p = (c+b)(c^{p-1} - c^{p-2}b + \cdots + b^{p-1})$ *the right part factors* $a_1 = c+b$ *and* $a_2 = c^{p-1} - \cdots + b^{p-1}$ *do not have a common divisor.*

Proof. Let **m** be a prime which divides $\mathbf{a}_1$. Then $a_1 \equiv 0 (\mathrm{mod}\, m)$ or $c+b \equiv 0 (\mathrm{mod}\, m)$. This implies that $c = mq + r$, $b = mq_1 - r$, where q_1, q, r are integers.

$$a_1 = c + b = mq + r + q_1 m - r = m(q_1 + q) \qquad (1)$$

$$a_2 = (mq + r)^{p-1} - \cdots + (mq_1 - r)^{p-1} = km + pr^{p-1}, \qquad (2)$$

where **k** is an integer.

The number $\boldsymbol{a_1}$ under the hypothesis of the theorem is not a multiple of ***p***, but building on (1) it is a multiple of ***m***. Hence, ***m*** is not equal to ***p*** and is not a multiple of ***p*** as ***m*** is a prime number.

The number $\boldsymbol{a_2}$ is not a multiple of ***m*** as in (2) the second summand $p r^{p-1}$ is not a multiple of ***m***, where ***p*** is a prime and unequal to ***m*** and ***r*** < prime ***m***. Likewise goes the proof for any prime divisor of $\boldsymbol{a}_1$. If this condition is satisfiable for all prime divisors of $\boldsymbol{a}_1$ then $\boldsymbol{a}_1$ and ***a***2 are coprimes. *This completes the proof of Theorem 1A.*

It is theoretically possible that proofs for the above given theorems may exist elsewhere, yet they have failed to be found.

The use of Theorem 1 and Theorem 1A gives the popular Abel's formulae. Those will be adduced hereinafter with the following notations:

$$c\text{-}b=a_1^p \tag{3}$$

$$c\text{-}a = b_1^p \tag{4}$$

$$a+b= c_1^p , \tag{5}$$

where $\boldsymbol{a}_1$, $\boldsymbol{b}_1$, $\boldsymbol{c}_1$ are divisors of $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$, respectively.

1.3. Theorem 2

Theorem 2. *If the equation* $a^p + b^p = c^p$ *has a solution at a prime* p *and pairwise coprime* a, b, c, *which are not divisible by* p, *then the equation* $a + b \equiv c \pmod{p^2}$ *is true.*

This theorem determines for the first case of Fermat's theorem more stringent ties among the numbers a, b, c than in the known relation:

$$a + b = c \pmod{p} \tag{1}$$

Proof. Introduce the parameter e = a + b – c. Carry c in the left part of the formula (1) and have:

$$e= 0 \pmod{p} \tag{2}$$

Using Abel's formulae (3), (4), (5) of 1.2 and taking into consideration that $\boldsymbol{e = a + b - c}$, the following can be written:

$$\begin{aligned} e &= a - a_1^p \\ e &= b - b_1^p \\ e &= c_1^p - c \end{aligned} \tag{3}$$

or

$$\begin{aligned} a &= e + a_1^p \\ b &= e+ b_1^p \\ c &= c_1^p - e \end{aligned} \tag{4}$$

With the help of the latter equalities, the equation $a^p + b^p = c^p$ can be written as:

$$(e + a_1^p)^p + (e + b_1^p)^p = (c_1^p - e)^p \qquad (5)$$

If the latter equality is possible to implement, its left and right parts are congruous modulo any number, modulo $\boldsymbol{p}^2$ in particular. Then

$$(e + a_1^p)^p + (e + b_1^p)^p = (c_1^p - e)^p \ (mod\ p^2) \qquad (6)$$

Raise to power and discard the terms multiple of $\boldsymbol{p}^2$, with regard for (2) obtain:

$$(a_1^p)^p + (b_1^p)^p \equiv (c_1^p)^p \ (\mathrm{mod}\ p^2) \qquad (7)$$

$$\text{or } (a_1^{p-1})^p a_1^p + (b_1^{p-1})^p b_1^p \equiv (c_1^{p-1})^p c_1^p \ (\mathrm{mod}\ p^2) \qquad (8)$$

In terms of Fermat's little theorem $a_1^{p-1} \equiv 1(\mathrm{mod}\ p)$, $b_1^{p-1} \equiv 1(\mathrm{mod}\ p)$, $c_1^{p-1} \equiv 1(\mathrm{mod}\ p)$. Hence, $(a_1^{p-1})^p \equiv 1(\mathrm{mod}\ p^2)$, $(b_1^{p-1})^p \equiv 1(\mathrm{mod}\ p^2)$, $(c_1^{p-1})^p \equiv 1(\mathrm{mod}\ p^2)$. With regard for the latter comparisons obtain of (8):

$$a_1^p + b_1^p \equiv c_1^p (mod\ p^2) \qquad (9)$$

Let us add together the two latter equalities of (3):

$$2e = c_1^p - c + b - b_1^p$$

$$or\ \ 2e = c_1^p - a_1^p - b_1^p \qquad (10)$$

With regard for (9) the latter equality can be written as:

$$2e \equiv 0\ (mod\ p^2)$$

As $\boldsymbol{p}^2$ is an odd number, let's cancel out 2 in the latter comparison. Hence,

$$e \equiv 0 (\text{mod } p^2) \tag{11}$$

Set the value of ***e*** in (11) and obtain $a+b-c \equiv 0 (mod\ p^2)$

$$\text{or} \quad a+b \equiv c\ (mod\ p^2) \tag{12}$$

This concludes the proof of the theorem.

An intriguing form of Fermat's equation for the first case can be obtained through several easy transformations.

Building on (10),

$$\boldsymbol{e} = \frac{c_1^p - a_1^p - b_1^p}{2} \tag{13}$$

Substitute the obtained value of ***e*** in the left part of the equation (5), Fermat's equation can be written as:

$$(e+ a_1^p)^p + (e+ b_1^p)^p = (e + a_1^p + b_1^p)^p \tag{14}$$

The function $f(x) = (e + x)^p$ being introduced, this equation can have another form. Namely:

$$f(x_1) + f(x_2) = f(x_1 + x_2), \tag{15}$$

where $x_1 = a_1^p$; $x_2 = b_1^p$.

This equation is easy to write as:

$$f(x_1 + x_2) = f(x_1) + f(x_2) \tag{16}$$

1.4. Properties of Numbers in Fermat's equation

Performing the congruence modulo various numbers of the left and the right part of Fermat's equation, different properties

and relations of the numbers satisfying Fermat's equation can be defined, if it generally has a solution for some prime powers ***p***.

The relation $c \equiv a+b \pmod{p}$ is known to appear from the congruence modulo ***p*** of the left and the right part of the equation [2]. The relation $c \equiv a+b \pmod{3}$ appears likewise, since for any odd ***p*** the comparisons $a^p \equiv a \pmod{3}$, $b^p \equiv b \pmod{3}$, $c^p \equiv c \pmod{3}$ are satisfiable for any ***a***, ***b***, ***c***, including the case when one of those is divisible by ***p*** or 3.

If the comparisons $c \equiv a+b \pmod{p}$ и $c \equiv a+b \pmod{3}$ are satisfiable, the comparison modulo product of moduli is true: $c \equiv a+b \pmod{3p}$.

The comparisons $a^p \equiv a \pmod{2}$, $b^p \equiv b \pmod{2}$, $c^p \equiv c \pmod{2}$ taken into consideration,

$$c \equiv a+b \pmod{6p} \qquad (1)$$

As a rule, proofs to Fermat's theorem are partitioned into two cases. In the first case none of the numbers ***a***, ***b***, ***c*** is divisible by ***p***. In the second case one of the numbers is divisible by ***p***. Two of the numbers cannot be divisible by ***p***, for in this case the third number has to be also divisible by ***p*** and we can cancel out p^p in the equation

Now, consider properties of the numbers ***a***, ***b***, ***c*** irrespective of case 1 or case 2.

If a number is divisible of ***p***, it is either the number ***c***, ***a*** or ***b***. To be definite, assume that ***a*** is not divisible of ***p***.

Further relations are true irrespective of whether either ***b*** or ***c*** is divisible by ***p*** or none of them is divisible by ***p***. Building on the properties to be found in the process of analysis, consider the numbers ***a*** and ***b*** predetermined, while the number ***c*** unknown:

$$c^p = b^p + a^p \qquad (2)$$

Carry $\boldsymbol{b}^p$ in the left part to factorize:

$$(c-b)(c^{p-1}+\ldots+b^{p-1}) = a^p \qquad (3)$$

Building on Abel's formulae one of the left part factors can be presented as:

$$c\text{-}b=a_1^p, \tag{4}$$

This relation is true irrespective of whether either ***c*** or ***b*** is multiple of ***p***, and ***a*** as suggested above is not a multiple of ***p***. The number a_1 is a divisor of ***a.*** The second left part multiple (3) is evidently greater than 1. Therefore, ***a*** besides a_1 includes at least one more divisor greater than 1. At that by Theorem 1 the latter has no common divisor with a_1.

Denote as a_2 one of the prime divisors of ***a***, which is not a divisor of a_1. If the equation (2) has an integer solution, its left and right parts are congruous modulo any number, modulo a_2 in particular.

Consider comparison of the left and the right parts (2) modulo a_2.

$$c^p \equiv b^p + a^p \ (mod\ a_2) \tag{5}$$

Since a_2 divides ***a***, the latter comparison can be written as:

$$c^p \equiv b^p \ (mod\ a_2) \tag{6}$$

The number of solutions for comparison of this form, if it is true, is known to equal $d=(p,\varphi(a_2))$, while the right part index has to be a multiple of ***d*** ([2], Гл. IV, §5).

Since ***p*** is a prime number, the number of solutions is defined by the value $\varphi(a_2)$. If $\varphi(a_2)$ is a multiple of ***p***, then $d=p$, if not $d=1$. The index in the right part of (6) is a multiple of ***p***, hence, in any case it is multiple of ***d***. Then the comparison (6) has solutions.

Consider 2 cases for ***d***.

Case 1. Let d=1. Then the comparison (6) has a single solution, which is easy to find by factorizing (6):

$$p \cdot ind\ c \equiv p \cdot ind\ b\ (mod\ \varphi(a_2))$$

Divide this comparison by $\boldsymbol{p}$ and obtain:

$$ind\ c \equiv ind\ b\ (mod\ \varphi(a_2))$$

The single solution is:

$$c \equiv b\ (mod\ a_2)$$

$$\text{or}\quad c-b \equiv 0\ (mod\ a_2) \tag{8}$$

With regard for the known relation (4) the comparison (8) takes the form:

$$a_1^p = 0\ (mod\ a_2) \tag{9}$$

Since $\boldsymbol{a}_1$ is not a multiple of $\boldsymbol{a}_2$, the latter comparison is not workable. Hence, the comparison (6) for the case $\boldsymbol{d=1}$ has no solution. Then the equation (2) has no solution either.

Case 2. Let $\boldsymbol{d = p}$. Then the comparison (6) has $\boldsymbol{p}$ solutions.

Obtain them using the popular techniques by Vinogradov ([2],Гл.IV,§5). Factorize the comparison (6):

$$p \cdot ind\ c \equiv p \cdot ind\ b\ (mod\ \varphi(a_2)) \tag{10}$$

Cancel out $\boldsymbol{p}$ in (10) taking into consideration that $\varphi(a_2)$ is multiple of $\boldsymbol{p}$. Then:

$$ind\ c \equiv ind\ b\ \left(mod\ \frac{\varphi(a_2)}{p}\right) \tag{11}$$

Find $\boldsymbol{p}$ various values of $\boldsymbol{ind\ c}$ as follows:

$$indc \equiv indb + \frac{\varphi(a_2)}{p} k, \qquad (12)$$

where k = 0, 1,…, p-1**.**

Suppose $\alpha = \frac{\varphi(a_2)}{p}$. Then (12) takes the form:

$$indc \equiv indb + \alpha k \ (mod \ \tfrac{\varphi(a_2)}{p}) \qquad (13)$$

or $$indc \equiv indb + indg^{\alpha k} \ (mod \tfrac{\varphi(a_2)}{p}), \qquad (14)$$

where ***g*** is a generator modulo $\boldsymbol{a}_2$.

Solutions for ***c*** in the general view can be written as follows:

$$c \equiv bg^{\alpha k} \ (mod \ a_2) \qquad (15)$$

At various values of ***k*** obtain ***p*** numbers incongruous modulo $\boldsymbol{a}_2$. Solutions for ***c*** are ***p*** classes of numbers, each having numbers congruous modulo $\boldsymbol{a}_2$.

If $\boldsymbol{a}_2$ is not a prime, all divisors of $\boldsymbol{a}_2$ have the form *kp+1*. If not, having considered the comparison (6) modulo this number, *d=1* would have been obtained, i.e. Case 1, which has no solution.

Chapter 2. Further Properties of Euler's and Fermat's Comparisons

Euler's certain theorem notes that at ***m>1*** and ***(a, m)=1*** the following comparison is true:

$$a^{\varphi(m)} = 1 \ (mod\ m) \qquad (1)$$

In this case modulus ***m*** can be written as modulus ***3m*** at the same $\varphi(m)$ and the condition that ***a*** is not a multiple of 3, i.e. (a,3)=1. This substitution is possible as $a^2 \equiv 1 \pmod 3$ at (a,3)=1. Since $\varphi(m)$ is always an even number at ***m***>2, the comparison (1) can be presented in the following form:

$$(a^2)^{\frac{\varphi(m)}{2}} \equiv 1 \pmod m \qquad (2)$$

$$\text{or} \quad (3k+1)^{\frac{\varphi(m)}{2}} \equiv 1 \pmod m$$

The latter formula implies that the left part is congruent to 1 modulo 3, and in this case the comparison modulo product of moduli is true:

$$a^{\varphi(m)} \equiv 1 \pmod{3m} \qquad (3)$$

Determine other numbers modulo which the comparison (1) is true. This depends on the divisors of $\varphi(m)$. Suppose $\varphi(m) = p_1 \cdot p_2 \cdots p_n$. If the product of any divisors of $\varphi(m)$ (any combination) + 1 is a prime, then the comparison (1) modulo this prime is satisfiable on condition that ***a*** is not multiple of this prime number.

Give a numerical example. Suppose ***m***=41. Then $\varphi(41) = 2 \cdot 2 \cdot 2 \cdot 5$. At various combinations of the multipliers of the latter we can obtain the divisors of $\varphi(41)$ 2, 4, 10, which equal

$2 = \varphi(3),\ \ 4 = \varphi(5),\ \ 10 = \varphi(11)$. Therefore, the comparison (1) is satisfiable modulo product $3 \cdot 5 \cdot 11 \cdot 41 = 6765$ at (***a***,6765)=1.

At ***m=p*** Fermat's theorem can be written as follows:

$$a^{p-1} \equiv 1 (\text{mod p}) \tag{4}$$

In [2] it has a more general view:

$$a^{p} \equiv a (\text{mod p}) \tag{5}$$

The numbers ***a*** and $\boldsymbol{a^p}$ coinside in evenness. Hence, the latter comparison is satisfiable modulo 2.

Besides, if $a \equiv 0 (\text{mod}\, 3)$, then $a^p \equiv 0 (\text{mod}\, 3)$, and if $a \equiv \pm 1 (\text{mod}\, 3)$, then $a^p \equiv \pm 1 (\text{mod}\, 3)$. Thus, the comparison is satisfiable modulo 3.

If the comparison is satisfiable modulo 2, 3, ***p***, it is satisfiable modulo product of these moduli. Hence, still within the general approach the comparison can be written as:

$$a^{p} \equiv a (\text{mod}\, 6p) \tag{6}$$

Chapter 3. Residues Matrix and Residues Properties

To clarify the properties of comparisons and power residues it seems reasonable to consider the matrix of power ***p*** residues modulo a prime ***m*** of the form ***k****p*+1.

To build the matrix consider the comparison $K^p = 1 (\text{mod}\, m)$.

Solution to this comparison can be found by way of indexing and it can be written as:

$$K_i = g^{\alpha_i},$$

where $\alpha_i = \frac{\varphi(m)}{p} i$

i= 0,1,2,….,p-1.

This solution is likewise (15), Ch. 1, 1.4 at ***b=1***.

Dispose all these solutions as elements of the matrix zero column ascent to ***i***. The first column of the matrix is the product K_i g= $g^{\frac{\varphi(m)}{p}i+1}$. An entry in the ***j-th*** column and ***i-th*** row can be written as $a_{i,j} = K_i\, g^j = g^{\frac{\varphi(m)}{P}i+j}$. The second column is a product of zero column entries by $\boldsymbol{g^2}$ etc. The lowermost row is the row of the least positive residues of power ***p***, i.e. $a_j = g^{jp} \pmod m$. Now, depict the matrix itself:

$$K_{p-1} \quad a_{p-1,1} \quad a_{p-1,2} \ldots a_{p-1,j} \ldots a_{p-1,\alpha}$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$K_i \quad a_{i,1} \quad a_{i,2} \ldots a_{i,j} \ldots a_{i,\alpha}$$

$$K_{i-1} \quad a_{i-1,1} \quad a_{i-1,2} \ldots a_{i-1,j} \ldots a_{i-1,\alpha}$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\mathrm{K}_1 \quad a_{1,1} \quad a_{1,2} \ldots a_{1,j} \ldots a_{1,\alpha}$$

$$1 \quad a_{0,1} \quad a_{0,2} \ldots a_{0,j} \ldots a_{0,\alpha}$$

$$1 \quad a_1 \quad a_2 \quad a_j \quad a_\alpha$$

All the entries in each column raised to power ***p*** are congruous modulo ***m***. This property becomes evident if we in general view raise any entry to the power ***p:***

$$a_j = (g^{\frac{\varphi(m)}{p}i+j})^p = g^{\varphi(m)i+jp} = g^{\varphi(m)i}\ g^{jp} = (km+1)^i\ g^{jp}$$

Now, find residue modulo ***m*** as:

$$a_j \equiv (km+1)^i\ g^{jp} \pmod{m}$$

$$a_j \equiv g^{jp} \pmod{m}$$

It is seen that a_j is independent of ***i*** , i.e. of which entry in the column is raised to the power ***p***, since $g^{\varphi(m)} = 1 \pmod{m}$. If take another entry which belongs to another column, the value will be different.

For any ***n*** ranging from 1 to $\varphi(m)$ all g^n are incongruous modulo ***m***. Hence, g^n runs over the complete residue system modulo ***m*** when ***n*** runs over values from 1 to $\varphi(m)$. This stipulates the choice of the number ***g***, which is the generator modulo ***m***, as the base of the exponential function.

If $a = g^n \pmod{m}$, to determine attachment to the row and column it is sufficient to represent ***n*** as

$$n = \frac{\varphi(m)}{p} i + j ,$$

where $j < \frac{\varphi(m)}{p}$.

The obtained ***i*** and ***j*** determine the row and the column this entry belongs to.

Corollary. Since the entries in the same column give one the least positive residue, these satisfy the comparison of the form $c^p \equiv b^p \pmod{m}$. Each column contains ***p*** entries and any combination of them is a solution to the comparison. Hence, for

each column there are $\boldsymbol{p}^2$ couples of entries which satisfy the latter comparison. Since there are $\frac{\varphi(m)}{p}$ columns, there will be $\varphi(m)\boldsymbol{p}$ couples of entries which satisfy the comparison.

If Fermat's equation $c^n = b^n + a^n$ has a solution, its left and right parts have to be congruous modulo any number ***m***. Then the left part will have the power ***n*** residue, and the right part will have a sum of two power ***n*** residues. This means that for the selected modulus ***m*** the power residue must be expandable into the sum of two power residues, moreover not each sum of power residues is a power residue.

Problems of power residues expandability will be considered below in Chapter 5.

Demonstrate several matrices for various primes and various powers ***n***. For each matrix note the possibility to expand a power residue into a sum of two power residues as well as the existence of adjacent residues, which is indicative of power residues expandability. The correspondent theorem on power residues expandability will be proven below in Chapter 5.

Assume *m*=41, *p*=5. For ***m***=41 the generator g=6.

37	17	20	38	23	15	8	7
16	14	21	2	31	22	9	13
18	26	33	34	40	35	5	30
10	19	32	28	4	24	21	3
1	6	36	11	25	27	39	29

1	27	32	3	40	14	9	38

As seen from the bottom row of power residues, there are no adjacent residues and the sum of any two residues is not a residue.

Set up a matrix of residues for $\boldsymbol{m}$=13, $\boldsymbol{n}$=2, 3, 4,.

	12	11	9	5	10	7
	1	2	4	8	3	6
x^2	1	4	3	12	9	10
x^4	1		3		9	

As seen from the row of residues for the square, there are adjacent residues 3, 4 and 9, 10. For the power 4 there are no adjacent residues. There are only three residues for the power 4 and none of the residues is congruent to the sum of the other two modulo $\boldsymbol{m}$.

For the power 3 the matrix of residues modulo 13 has the following form:

	9	5	10	7
	3	6	12	11
	1	2	4	8
x^3	1	8	12	5

Here there are no adjacent power residues either, while the absence of expandability of power residues is easy to check.

Further on represent the matrix of residues for the prime $\boldsymbol{m}$=31 and the powers 2, 4, 3, 5.

	30	28	22	4	12	5	15	14	11	2	6	18	23	7	21
	1	3	9	27	19	26	16	17	20	29	25	13	8	24	10

x^2	1	9	19	16	20	25	8	10	28	4	5	14	2	18	7
x^4	1		19		20		8		28		5		2		7

As seen from the matrix, there are adjacent residues for the power 4: 19, 20 and 7, 8. All these power residues are expandable into the sum of two power residues.

The matrix of cubic residues modulo ***m***=31 has the following form:

	5	15	14	11	2	6	18	23	7	21
	25	13	8	24	10	30	28	22	4	12
	1	3	9	27	19	26	16	17	20	29
x^3	1	27	16	29	8	30	4	15	2	23

All cubic residues modulo 31 are expandable into the sum of two residues.

The matrix of residues of the power 5 modulo ***m***=31 is as follows:

	2	6	18	23	7	21
	4	12	5	15	14	11
	8	24	10	30	28	22
	16	17	20	29	25	13
	1	3	9	27	19	26
x^5	1	26	25	30	5	6

All the residues of the power 5 modulo 31 are also expandable.

3.1. Theorem 3

Theorem 3. *If* $\frac{\varphi(m)}{p}$ *is not identically equal to zero modulo* ***p****, at the prime* ***m*** *and the prime* ***p****, any residue of the power* ***p*** *is a residue of the power* $\boldsymbol{p^2}$.

Proof. To prove the theorem consider the matrix of residues modulo the prime $m = kp + 1$, where ***p*** is a prime.

As stated above in this chapter the residues of the complete residue system in the matrix column are bound by the relation:

$$V_2 = V_1 \cdot g^{\frac{\varphi(m)}{p} i} \pmod{m}, \qquad (1)$$

where ***i*** is the difference between the numbers of the rows which include the residues V_2 and V_1.

Let both residues be power residues.

Multiply the comparison (1) by V_1', such that $V_1 \cdot V_1' \equiv 1 \pmod{m}$. Such a residue exists by Property 2 of power residues. Then obtain:

$$V_2 \cdot V_1' \equiv g^{\frac{\varphi(m)}{p} i} \pmod{m} \qquad (2)$$

In the left part we have a product of the two power residues, which is also a power residue by Property 1 of power residues.

Under the hypothesis of the theorem $\frac{\varphi(m)}{p}$ is not identically equal to zero modulo ***p***, while $i < p$, hence, ***i*** is not a multiple of ***p***. As ***g*** is a generator, the right part of the formula can be a residue of power ***p*** only at $i \equiv 0 \pmod{p}$, i.e. $i = 0$. This means that V_1 and V_2 belong to the same row and it is one and the same residue.

If any column cannot have two residues of the power ***p***, while the number of columns and the number of power residues

equal $\frac{\varphi(m)}{p}$, into each column gets one and only one residue of the power p.

As follows from the above (Ch. 3) each column includes p entries, which are solutions to the comparison of the form:

$$x^p \equiv V(\mathrm{mod}\, m), \tag{3}$$

where V is a residue of the power p.

If as stated above one of these solutions in the same column is a power p residue, there exists $x_i \equiv a^p(\mathrm{mod}\, m)$. Then of (3) obtain:

$$(a^p)^P \equiv V(\mathrm{mod}\, m)$$

$$\text{or} \quad a^{p^2} \equiv V(\mathrm{mod}\, m) \tag{4}$$

Thus, a number a satisfying the latter comparison exists. Therefore, V is a residue of the power p^2. This completes the proof of the theorem.

3.2. Quadratic Residues

In the complete residue system modulo m one half, i.e. $\frac{\varphi(m)}{2}$, represents quadratic residues [2], while the other half represents quadratic nonresidues. As denoted above, any residue, quadratic in this particular case, can be written as:

$$\mathrm{V}= g^{\frac{\varphi(m)}{2}i+j}(\mathrm{mod}\, m), \tag{1}$$

where g is a generator.

For the quadratic residue i can have the two following values: i=0 and i=1.

Consider two residues of the same column of the quadratic residues matrix. They correspond to some value of j and two different values of i:

$$V_1 = g^j \pmod m \tag{2}$$

$$V_2 = g^{\frac{\varphi(m)}{2}+j} \pmod m \tag{3}$$

Assume ***j*** is an even number. Then V_1 is a quadratic residue. Hence, V_2 is also a quadratic residue at $\frac{\varphi(m)}{2} \equiv 0 \pmod 2$.

Solving simultaneously (2) and (3), can obtain:

$$V_1 \equiv -V_2 \pmod m$$

$$\text{or} \quad V_1 + V_2 \equiv 0 \pmod m$$

Thus, in the case $\frac{\varphi(m)}{2} \equiv 0 \pmod 2$ the matrix column includes two quadratic residues the sum of which equals ***m***, while for the odd ***j*** the column includes two quadratic nonresidues.

Consider the case $\frac{\varphi(m)}{2} \equiv 1 \pmod 2$. Here, at the even ***j*** the residue V_1 will be a quadratic residue, and V_2 will be a quadratic nonresidue, their sum being equal to ***m.***

In the case when ***j*** is an odd number, the residue V_2 will be a quadratic residue, and V_1 will be a quadratic nonresidue, their sum being equal to ***m***, too.

Thus, all the columns of the residues matrix include one quadratic residue and one quadratic nonresidue. Examples of quadratic matrices are given above in 3.1.

3.3. Generators

Describe several properties of generators.

If ***g*** is a generator modulo ***m***, then at $\varphi(m)$ identically unequal to zero modulo ***n***, the number $g_1 \equiv g^n \pmod m$ is also a generator.

Assume the number $g_1 \equiv g^n (\mathrm{mod}\, m)$ is not a generator. Then it belongs to the power $\alpha < \varphi(m)$ modulo ***m*** , i.e.

$$(g^n)^\alpha \equiv 1 (\mathrm{mod}\, m) \quad (1)$$

$$\text{or } (g^\alpha)^n \equiv 1 (\mathrm{mod}\, m) \quad (2)$$

The latter comparison has $d = (n, \varphi(m))$ solutions. As $\varphi(m)$ is identically unequal to zero modulo ***n***, the number of solutions is d=1. This single solution is $g^\alpha \equiv 1 (\mathrm{mod}\, m)$. Hence, $\alpha \equiv 0 (\mathrm{mod}\ \varphi(m))$. Our conjecture that $\alpha < \varphi(m)$ is wrong. The number $g_1 \equiv g^n (\mathrm{mod}\, m)$ is one of the generators.

Consider the general formula to represent the residues of the complete residue system modulo ***m***:

$$a \equiv g^{\frac{\varphi(m)}{p} i + j} (\mathrm{mod}\, m) \quad (3)$$

Suppose ***j*** divides $\varphi(m)$ and perform a simple transformation

$$g^{\frac{\varphi(m)}{p} i + j} \equiv (g^{\frac{\varphi(m)}{j \cdot p} i + 1})^j \equiv b (\mathrm{mod}\, m)$$

The obtained number is not a generator for it belongs to the power $\frac{\varphi(m)}{j}$ modulo ***m***.

Thus, each column the number of which is not dividing $\varphi(m)$ includes ***p*-1** generators, while one of the residues as ascertained within the proof of Theorem 3 is a power ***p*** residue.

3.4. Composite Modulus Case

To prove Fermat's theorem it is essential to consider the expandability of power residues modulo any numbers, composite including. To represent any power residue modulo a prime as a power function, the function base must be a generator.

In this connection consider the possibility of search of a number with a prime generator properties.

Let g_1 be the prime m_1 generator and g_2 be the generator modulo m_2.

The number denoted as a generator modulo m_1 and m_2 obtain as follows:

$$g = m_2\, m_2'\, g_1 + m_1\, m_1'\, g_2 \pmod{m_1\, m_2}, \qquad (1)$$

where $m_2\, m_2' \equiv 1 \pmod{m_1}$,

$m_1\, m_1' \equiv 1 \pmod{m_2}$.

The search of this number can be spread to the case of a bigger amount of composite number prime divisors, as it is done in [2].

The number g is generator modulo m_1 and a generator modulo m_2. irrespective of whether g is the least among all generators.

Note that the generator obtained in (1) is not a generator modulo product of moduli. The proof will be given below in 4.5 (Theorem 4).

3.5. Inverse Numbers Modulo a Composite

Two numbers are called mutually inverse modulo m if their product is congruent to 1 modulo m. Comparisons of the form

$$ax \equiv b \pmod{m} \qquad (1)$$

are considered in [2, Ch. 4, § 2]. The comparison (1) always has a solution if $(a, m)=d=1$ and this solution is unique.

If $d>1$, the comparison has d solutions in case b is divisible by d. Otherwise the comparison has no solution.

To obtain the number x inverse of the given number a modulo m, equate b in the comparison (1) to 1. Then

$$a \cdot x \equiv 1 \pmod{m} \qquad (2)$$

The solution to the latter comparison exists at $(a, m)=d=1$ only. If $d>1$, the number $b=1$ is not divisible by d and the comparison will have no solution.

In fact, if a and m are divisible by a number m_1, the comparison (2) has no solution, as in the case it has a solution there has to be a solution for the comparison modulo m_1, the latter being a devisor of m and a. But in this case come to a wrong comparison:

$$0 \equiv 1 (mod\ m_1).$$

Thus, for the number x inverse of a modulo m to exist the numbers a and m have to be coprime.

If take modulus $m!$, for any $a<m$ there exits no inverse number modulo $m!$.

Chapter 4. Power Residues

4.1. Properties of Power Residues

Describe several properties of power residues which will be used below.

Property 1. A product of power residues is a power residue.

This affirmation follows from the notion that a product of power functions is a power function:

$$x^n \cdot y^n = (xy)^n \qquad (1)$$

The left and right parts of the latter equality having been considered congruous modulo m, obtain

$$V_x \cdot V_y \equiv V_{xy} (\mathrm{mod}\, m), \qquad (2)$$

where $V_x \equiv x^n (\mathrm{mod}\, m)$, $V_y \equiv y^n (\mathrm{mod}\, m)$, $V_{xy} \equiv (xy)^n (\mathrm{mod}\, m)$ are power residues.

Property 2. For any power residue V modulo the prime m there has to exist inverse modulo m power residue $V^{/}$.

Let the power residue $V \equiv x^p (\mathrm{mod}\, m)$. For any x, as 3.3 implies, there exists the number $x^{/}$ which is inverse of it modulo

m, such that $x \cdot x^{/} \equiv 1(\mathrm{mod}\, m)$. Then $x^p \cdot x'^p = (x \cdot x')^p \equiv 1(\mathrm{mod}\, m)$. Hence, there exists $V^{/} \equiv (x^{/})^p (\mathrm{mod}\, m)$ such that $V \cdot V^{/} \equiv 1(\mathrm{mod}\, m)$.

Property 3. For any power p residue of an odd prime number there has to exist a negative residue of the like power and of the like absolute value. This convention is built on the notion that if the comparison $x^p \equiv V(\mathrm{mod}\, m)$ has a solution, the comparison $(m-x)^p \equiv -V(\mathrm{mod}\, m)$ is also true. Therefore, for any ***V*** there exists another power residue ***m*-V**.

Property 4. Any power residue ***V*** modulo the prime ***m*** can be written as a product of any other power residue V_1 by the corresponding third power residue V_2 such that

$$V_1 \cdot V_2 \equiv V(\mathrm{mod}\, m) \qquad (1)$$

Demonstrate the existence of such power residue by multiplication of the latter comparison by $V_1^{'}$ inverse modulo ***m*** of the power residue V_1 . Then of (1) obtain:

$$V_2 \equiv V \cdot V_1^{/} (\mathrm{mod}\, m)$$

The right part, as Property 1 implies, is a power residue as the product of power residues. Hence, there exists the power residue V_2.

Property 5. If it is possible to expand at least one power residue into a sum of two power residues, any power residue has to be expandable into a sum of two power residues.

Assume that one of the power residues is expandable into the sum of two power residues:

$$u_3 \equiv u_1 + u_2 (\mathrm{mod}\, m) \qquad (1)$$

Multiply the comparison by $u_3^{/}$, inverse of u_3 modulo ***m***. Then

$$1 \equiv u_1 \cdot u_3^{/} + u_2 \cdot u_3^{/} (\mathrm{mod}\, m) \qquad (2)$$

In the right part of the formula each product of the residues is a power residue by Property 1. Let $u_4 \equiv u_1 \cdot u_3^{/} (\mathrm{mod}\, m)$ and $u_5 \equiv u_2 \cdot u_3^{/} (\mathrm{mod}\, m)$. From (2) obtain:

$$1 \equiv u_4 + u_5 (\mathrm{mod}\, m) \qquad (3)$$

The power residue 1 is separated into a sum of two power residues u_4 and u_5. Thus, the multiplication of the comparison (3) by any power residue gives its expansion into a sum of two power residues.

Property 6. A product of a power residue by a power nonresidue is a power nonresidue.

Assume the opposite:

$$u_1 \cdot u \equiv u_2 (\mathrm{mod}\, m), \qquad (1)$$

where u_1, u_2 are power residues,

u is a power nonresidue.

u_2 cannot be a residue, as multiplication of the comparison (1) by $u_1^{/}$, at which $u_1 \cdot u_1^{\cdot} \equiv 1 (\mathrm{mod}\, m)$, results in the impossible comparison:

$$u \equiv u_2 \cdot u_1^{/} (\mathrm{mod}\, m) \qquad (2)$$

The right part of this comparison is a product of two power residues, which is a power residue, while the left part is a nonresidue by the above definition. Hence, u_2 is a nonresidue.

4.2. Comparison Modulo a Composite

Comparisons of the form $x^n \equiv a (\mathrm{mod}\, m)$ are considered in [2] in full detail. The number of solutions for any such comparison equals $d = (n, \varphi(m))$. The solutions exist if ***a*** is a power residue and ***ind a*** is a multiple of ***d***. These cases were considered for $m = p^{\alpha}$ or $m = 2 \cdot p^{\alpha}$.

Herein, consider the comparisons modulo product of two primes. Suppose the following is given:

$$x^p \equiv V(\mathrm{mod}\, m_1 \cdot m_2), \quad (1)$$

where $\boldsymbol{p}$ is an odd prime,

$\boldsymbol{m}_1$, $\boldsymbol{m}_2$ are primes.

The number V $< m_1 \cdot m_2$ is the power $\boldsymbol{p}$ residue modulo $m_1 \cdot m_2$.

If the comparison (1) has a solution modulo product of the moduli $m_1 \cdot m_2$, then the comparisons modulo $\boldsymbol{m}_1$ and modulo $\boldsymbol{m}_2$ also have solutions:

$$x^p \equiv V(\mathrm{mod}\, m_1) \quad (2)$$

$$x^p \equiv V(\mathrm{mod}\, m_2) \quad (3)$$

Consider each of these comparisons separately. If $\varphi(m_1)$ is identically unequal to zero modulo p, the number of solutions to the comparison (2) equals $d = (n, \varphi(m_1))$=1. $\boldsymbol{V}$ is a power residue. The class of numbers which are residues modulo $\boldsymbol{m}_1$ can be written as:

$$V \equiv V_1 + k_1 \cdot m_1, \quad (4)$$

where V_1 is the least positive power residue,

k_1 is an integer.

Consider the existence of solutions for different values of V_1. Let in the comparison

$$(g^i)^p \equiv V_i(\mathrm{mod}\, m_1), \quad (5)$$

where g is a generator modulo m_1, V_i be the least positive power residue.

The integer $\boldsymbol{i}$ varies from 1 to $\varphi(m_1)$. Then g^i runs over the complete residue system modulo $\boldsymbol{m}_1$.

As the comparison under consideration has only one solution modulo $\boldsymbol{m}_1$, no two values g^i and g^j will give one power residue V_i. Hence, each of $\varphi(m_1)$ different values of g^i will give different

values of V_i, therefore, the number of power residues will also equal $\varphi(m_1)$.

Thus, V_i runs over the complete residue system modulo m_1, like g^i but in a different sequence. Hence, for any $V_i < m_1$ there is a solution and it is unique.

The comparison (3) also has a unique solution at any ***V***.

The residue ***V*** modulo m_2 can be written as

$$V = V_2 + k_2 \cdot m_2, \tag{6}$$

where $V_2 < m_2$ is the least positive power residue modulo m_2,

k_2 is an integer.

The equations (4), (6) give the classes of numbers modulo m_1 and m_2 which are power residues modulo m_1 and m_2. Hence, the comparisons (2), (3) can be written as:

$$x^p \equiv V_1 (\mathrm{mod}\, m_1) \tag{7}$$

$$x^p \equiv V_2 (\mathrm{mod}\, m_2) \tag{8}$$

Thus, by the determination of the residue ***V*** modulo $m_1 \cdot m_2$, the least positive residues V_1 and V_2 modulo m_1 and m_2 respectively are obtained. The popular technique [2] allows the reverse transformation:

$$V \equiv m_2 \cdot m_2^{/} \cdot V_1 + m_1 \cdot m_1^{/} \cdot V_2 (\mathrm{mod}\, m_1 \cdot m_2), \tag{9}$$

where $m_2 \cdot m_2^{/} \equiv 1 (\mathrm{mod}\, m_1)$, $m_1 \cdot m_1^{/} \equiv 1 (\mathrm{mod}\, m_2)$

After such a transformation of the comparisons (7), (8) consider the comparisons (2), (3).

If the comparisons (7), (8) have one solution each, the comparisons (2),(3) also have one solution each.

Let the solutions for (2) and (3) respectively be:

$$x = x_1 (\mathrm{mod}\, m_1) \tag{10}$$

$$x = x_2 (\mathrm{mod}\, m_2) \tag{11}$$

The simultaneous solving of the two latter comparisons gives the following result:

$$x \equiv m_2 \cdot m_2^{/} \cdot x_1 + m_1 \cdot m_1^{/} \cdot x_2 (\mathrm{mod}\, m_1 \cdot m_2) \qquad (12)$$

The obtained solution for the comparison is the solution modulo $m_1 \cdot m_2$.

The set of solutions modulo m_1 represents a class of numbers modulo m_1:

$$x = x_1 + k_1 \cdot m_1, \qquad (13)$$

while modulo m_2 it is:

$$x = x_2 + k_2 \cdot m_2 \qquad (14)$$

The solution modulo $m_1 \cdot m_2$ is possible when the right parts of (13), (14) are congruous modulo $m_1 \cdot m_2$

$$x_1 + k_1 \cdot m_1 \equiv x_2 + k_2 \cdot m_2 (\mathrm{mod}\, m_1 \cdot m_2) \qquad (15)$$

The solutions x_1 and x_2 are unique modulo m_1 and m_2 respectively. The solution for the comparison (1) is also unique, which is evident from (12) and (15). Since the solutions x_1 and x_2 exist, there also exists a solution for (1).

4.3. Power Residues Modulo 3m

Consider the comparison:

$$g^{ip} \equiv u \,(\mathrm{mod}\ \mathrm{m}), \qquad (1)$$

where ***g*** is a generator,

u is the least positive residue,

i is an integer,

p is a prime,

m=kp+1 is a prime.

If ***i*** runs over all values from 0 to $\frac{\varphi(m)}{p}$, then g^{ip} runs over all power ***p*** residues modulo ***m***. If ***u*** is the least power residue

modulo ***m***, the least power residue modulo ***3m*** will be one of the three following values: ***u, m+u,*** or ***2m+u***. The form of the power residue modulo 3*m* is dependable of the modulus ***m*** and of the number the residue ***u*** is congruent to modulo 3.

Introduce notations with subscripts for the least power residues, the subscript pointing to which of the numbers 0, 1, or 2 the power residue modulo 3 is congruent to. Thus, $u_0 \equiv 0(\mathrm{mod}\,3)$, $u_1 \equiv 1(\mathrm{mod}\,3)$, $u_2 \equiv 2(\mathrm{mod}\,3)$.

The search methodology is as follows. If in the comparison (1) $u = u_1 \equiv 1(\mathrm{mod}\,m)$, then this comparison modulo 3***m*** for $g \equiv 0\,(\mathrm{mod}\ 3)$ and ***m***=2(mod 3) will take the form:

$$g^{ip} \equiv m + u_1\,(\mathrm{mod}\ 3\boldsymbol{m}) \qquad (2)$$

The comparison is true since its left part is always congruent to zero modulo 3 as $g \equiv 0\,(\mathrm{mod}3)$, while its right part is also congruent to zero modulo 3 as $u_1 \equiv 1\,(\mathrm{mod}3)$, $m \equiv 2\,(\mathrm{mod}3)$. Hence, $m + u_1 \equiv 0\,(\mathrm{mod}3)$. If the comparison is possible modulo 3 and modulo ***m***, it is also possible modulo their product ***3m*** [2].

If in (1) $u = u_0 \equiv 0\,(\mathrm{mod}3)$, the comparison (1) will take the form:

$$g^{ip} \equiv u_0\,(\mathrm{mod}3\mathrm{m}) \qquad (3)$$

The third variant is possible at $u = u_2 \equiv 2\ (\mathrm{mod}3)$:

$$g^{ip} \equiv 2m + u_2\,(\mathrm{mod}3\mathrm{m}) \qquad (4)$$

Thus, having the least positive power residue modulo ***m***, we can unambiguously obtain the least positive power residue modulo ***3m***. Using this technique, find power residues modulo ***3m*** at various ***g*** and ***m***. Tabulate all these variants for $\mathrm{m} \equiv 2(\mathrm{mod}3)$ and $\mathrm{m} \equiv 1(\mathrm{mod}3)$.

Table 3

	$m \equiv 2 (\text{mod} 3)$		
$g \equiv 0 (\text{mod} 3)$	V_0	$m+V_1$	$2m+V_2$
$g \equiv 1 (\text{mod} 3)$	V_1	$m+V_2$	$2m+V_0$
$g \equiv 2 (\text{mod} 3)$	V_2	$m+V_0$	$2m+V_1$
odd power			

Table 4

	$m \equiv 1 (\text{mod} 3)$		
$g \equiv 0 \ (\text{mod} 3)$	V_0	$m+V_1$	$2m+V_2$
$g \equiv 1 (\text{mod} 3)$	V_1	$m+V_2$	$2m+V_0$
$g \equiv 2 (\text{mod} 3)$	V_2	$m+V_0$	$2m+V_1$
odd power			

Even powers for $g \equiv 2 (\text{mod} 3)$ conform to the case $g \equiv 1 (\text{mod} 3)$, as at $g \equiv 2 (\text{mod} 3)$ $g^{2i} \equiv 1 \ (\text{mod} 3)$.

Corollary. The obtained result implies that the difference between any two adjacent modulo ***m*** power residues modulo 3m is congruent to zero modulo 3. For the case $m \equiv 2 (\text{mod} 3)$ the difference between the adjacent ***m*** residues equals m+1, while for the case $m \equiv 1 (\text{mod} 3)$ the difference equals 2m+1. The power functions having the same base, the difference in both cases is a multiple of 3. However, this means that the powers have to be of the same evenness at $g \equiv 2 (\text{mod} 3)$.

4.4. Amount of Power Residues Modulo a Composite

Consider the problem of the amount of power residues modulo product of the two primes m_1, m_2.

As shown in Ch. 3, 3.4, find the number which is a generator modulo m_1 and modulo m_2.

This generator might not be the least among the generators. Its principle characteristic lies in its belonging to the power $\varphi(m_1)$ modulo m_1 and the power $\varphi(m_2)$ modulo m_2. To be definite, assume that $m_1 < m_2$.

The power function g^j runs over the complete residue system modulo m_2 and modulo m_1 if ***j*** ranges from 1 to $\varphi(m_2)$, as m_2 and m_1 are primes, while $\varphi(m_2) > \varphi(m_1)$.

Put the question if there exists such a value of ***j*** that

$$g^j \equiv 1 (\mathrm{mod}\, m_1 m_2) ? \qquad (1)$$

Moreover, g^j must run over all the residues of the complete residue system modulo m_1, and all the residues of the complete residue system modulo m_2.

To fulfill the condition (1) at the least value of ***j***, consider the same comparison modulo m_1 and m_2.

$$g^j \equiv 1 (\mathrm{mod}\, m_1) \qquad (2)$$

$$g^j \equiv 1 (\mathrm{mod}\, m_2) \qquad (3)$$

To perform the comparison (2) it is essential that

$$j \equiv 0 (\mathrm{mod}\, \varphi(m_1)) \qquad (4)$$

To perform the comparison (3) it is essential that

$$j \equiv 0 (\mathrm{mod}\, \varphi(m_2)) \qquad (5)$$

The conditions (4) and (5) are possible when ***j*** is a multiple of any divisor of $\varphi(m_1)$ and a multiple of any divisor of $\varphi(m_2)$. Such a number is the least common multiple (LCM) of the two numbers $\varphi(m_1)$ and $\varphi(m_2)$. Thus, j= LCM $(\varphi(m_1), \varphi(m_2))$. Denote α = LCM $(\varphi(m_1), \varphi(m_2))$. Then:

$$g^\alpha \equiv 1 (\mathrm{mod}\, m_1 m_2) \qquad (6)$$

The latter comparison is true by Euler's comparison property (Ch. 2).

Come to the problem of the amount of the power residue modulo a composite number. For this consider the comparison:

$$x^p \equiv V \ (\mathrm{mod}\, m_1\ m_2) \tag{7}$$

If this comparison has solutions, the comparisons modulo m_1 and m_2 have solutions, too.

$$x^p \equiv V_1 (\mathrm{mod}\, m_1) \tag{8}$$

$$x^p \equiv V_2 (\mathrm{mod}\, m_2) \tag{9}$$

The power residue $\boldsymbol{V}$ in (7) can be written as:

$$\mathrm{V} = V_1 + k_1\ m_1 = V_2 + k_2\ m_2 .$$

For the comparisons (8), (9) the number of the solutions respectively equals $d_1 =$ (p, $\varphi(m_1)$), $d_2 =$ (p, $\varphi(m_2)$). The amount of the power residues modulo m_1 and modulo m_2 is respectively $n_1 = \dfrac{\varphi(m_1)}{d_1}$, $n_2 = \dfrac{\varphi(m_2)}{d_2}$. It depends on the divisibility of $\varphi(m_1)$ and $\varphi(m_2)$ by $\boldsymbol{p}$. On this the values d_1 and d_2 also depend.

Using the comparisons (8), (9) and the formula (9) of 4.2, the power residue $\boldsymbol{V}$ modulo $m_1 \cdot m_2$ can be defined as follows:

$$V = m_2 m_2' \cdot V_1 + m_1 m_1' \cdot V_2 (\mathrm{mod}\, m_1 m_2) \tag{10}$$

The combination of any power residue V_1 modulo m_1 with any power residue V_2 modulo m_2 gives the power residue modulo $m_1 \cdot m_2$.

Any number multiple of m_1 or m_2 taken to the power $\boldsymbol{p}$ gives a power residue modulo $m_1 \cdot m_2$. Consider the comparison:

$$(km_1)^p \equiv V \ (\mathrm{mod}\, m_1 \cdot m_2) \tag{11}$$

Its left part is congruent to zero modulo m_1, therefore, the right part is also congruent to zero modulo m_1. The comparison modulo m_1 is always satisfiable.

If $\boldsymbol{V}$ is a power residue, there also exists a solution modulo m_2. The number of the solutions for the comparison $(km_1)^p \equiv V \pmod{m_2}$, by [2], can be written as $d_2 = (p, \varphi(m_2))$, while the number of the power residues can be written as $\frac{\varphi(m_2)}{d_2}$.

Likewise is defined the amount of the power residues for a series of numbers multiple of m_2 and less than $m_1 \cdot m_2$.

By the above, find the total amount of the power residues modulo $m_1 \cdot m_2$ from the formula:

$$n = \frac{\varphi(m_1)}{d_1} \cdot \frac{\varphi(m_2)}{d_2} + \frac{\varphi(m_1)}{d_1} + \frac{\varphi(m_2)}{d_2} \qquad (12)$$

4.5. Theorem 4

Theorem 4. *There is no generator modulo an add composite number.*

Proof. Let be given two odd primes m_1 and m_2. The number which is a generator modulo m_1 and modulo m_2 can be obtained by the formula (9) of 4.2:

$$g = m_2 m_2' \cdot g_1 + m_1 m_1' \cdot g_2 \pmod{m_1 m_2}, \qquad (1)$$

where g_1 is a generator modulo m_1,

g_2 is a generator modulo m_2,

$m_2 m_2' \equiv 1 \pmod{m_1}$

$m_1 m_1' \equiv 1 \pmod{m_2}$

Any combination of the generators modulo m_1 and modulo m_2 gives the number simultaneously being a generator modulo m_1 and a generator modulo m_2.

Introduce the notations $\varphi(m_1)=\mathrm{n}\,k_1$, $\varphi(m_2)=\mathrm{n}\,k_2$, where ***n*** is the greatest common divisor (GCD) of $\varphi(m_1)$ and $\varphi(m_2)$.

All common divisors belonging to ***n***, the numbers k_1 and k_2 are coprimes. Hence, $\mathrm{n}\,k_1\,k_2 = \mathrm{LCM}\,(\varphi(m_1),\varphi(m_2))$. The product of $\varphi(m_1)$ and $\varphi(m_2)$ can be written as:

$$\varphi(m_1)\,\varphi(m_2)=\mathrm{GCD}\,(\varphi(m_1),\varphi(m_2))\cdot\mathrm{LCM}\,(\varphi(m_1),\varphi(m_2))=\beta\cdot\alpha \quad (2)$$

Now, refer to the sequence g^j at ***j*** ranging from 1 to $\alpha=\mathrm{LCM}(\varphi(m_1),\varphi(m_2))$. At that g^j runs over the power ***p*** residues numbering $\frac{\alpha}{p}$. ***j*** ranges from 1 to α, as $g^{\alpha}\equiv 1(\mathrm{mod}\,m_1m_2)$. At further changes of ***j*** obtain the repetition of the power residues. This convention is true since the two numbers g^{j_1} and g^{j_2} are congruous modulo $m_1\cdot m_2$ if $g^{j_1-j_2}\equiv 1(\mathrm{mod}\,m_1\cdot m_2)$, the latter being possible at $j_1\equiv j_2(\mathrm{mod}\,\alpha)$.

The amount of the power residues by the above is defined by the formula:

$$\mathrm{n}=\frac{\varphi(m_1)}{d_1}\cdot\frac{\varphi(m_2)}{d_2}+\frac{\varphi(m_1)}{d_1}+\frac{\varphi(m_2)}{d_2}.$$

The number $\frac{\alpha}{d_2}$ is the number of the power ***p*** residues run over by g^j irrespective of the selected value of **g**, as for any ***g*** the comparison $g^{\alpha}\equiv 1(\mathrm{mod}\,\alpha)$ is possible.

If the power function base is another number, which is also a generator modulo m_1 and m_2, then g^j also runs over $\frac{\alpha}{p}$ power residues. However, this amount is always less than the total amount of power residues since for any prime m_1 the value $\frac{\varphi(m_1)}{d_1} \geq 2$. The latter assertion is true since for any $m_1 \geq 3$, GCD of $\varphi(m_1)$ and $\varphi(m_2)$ always includes the number 2.

Thus, regardless of the number taken for the power function base, g^j doesn't run over all the power residues. Therefore, no generator modulo $m_1 \cdot m_2$ exists. This concludes the proof of the theorem.

Chapter 5. Expandability of Power Residues

5.1. Expandability of Power Residues Modulo a Prime

The power residue modulo ***m*** is considered expandable into the sum of two like power residues if the following comparison is true:

$$U_1 \equiv U_2 + U_3 \pmod{m}, \quad (1)$$

where U_1, U_2, U_3 are power residues.

The expandability of a power residue into a sum of two power residues respective of Fermat's equation $c^p = b^p + a^p$ being considered, $U_1 \equiv c^p \pmod{m}$, $U_2 \equiv e^p \pmod{m}$, $U_3 \equiv a^p \pmod{m}$.

The expandability of power residues into a sum of two like power residues is closely connected with the proof of Fermat's equation.

There is every reason to suppose that analysing expandability of power residues modulo various numbers Pierre de Fermat came to a certain conclusion and posed the following 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 [4].

If Fermat's equation

$$c^p = b^p + a^p \qquad (2)$$

has integer solutions, its left and right parts have to be equally residual at division by any number, including either of the numbers ***a, b, c*** or their divisors. In other words, the left and the right parts (2) have to be congruous modulo any number.

There are prime numbers modulo which for the prime ***m*** power ***p*** residues cannot be expanded into a sum of two like power residues. The prime 13 serves an example modulo which the numbers 1, 5, 8, 12 are power 3 residues, and none of them can be presented as the sum of the other two numbers.

For Fermat's equation to have a solution at $p=3$, one of the numbers ***a, b, c*** has to be a multiple of 13. Then it is possible to obtain a solution for the equation:

$$c^n \equiv b^n + a^n \ (mod 13) \qquad (3)$$

If there is no expandability modulo ***m***, one of the numbers ***a, b, c*** has to be a multiple of ***m***.

For the power 2 such numbers are 3 and 5, hence, any Pythagorean triple includes numbers divisible by 3 and 5.

Attempts to prove Fermat's theorem suppose comparisons modulo ***p***, for the relation $a^p \equiv a (mod\ p)$ is known, and this is why the proof is generally separated into two cases.

Consider in general the comparison (1) modulo the prime ***m*** of the form $kp+1$. If the comparison (1) has been produced from Fermat's equation (2) and one of the numbers ***a, b,*** **c** is divisible by ***m***, this will be a particular case of the general one, when one of the numbers U_1, U_2, U_3 equals zero, i.e. it will be the expansion with one zero solution modulo ***m***.

To study certain properties and relations of expandable power residues, perform some transposition of the comparison (1), where $U_1>0, U_2>0, U_3>0$.

By Property 2 of power residues (Ch. 4, 4.1) there is a power residue U_1', such that $U_1 \cdot U_1' \equiv 1 \pmod{m}$.

By Property 1 a product of power residues is a power residue.

By Property 3 of power residues there are negative power residues since ***p*** is an odd number.

Introduce the following notations:

$$V_1 \equiv U_3 \cdot U_1' (\mathrm{mod}\, m) \tag{4}$$

$$V_3' \equiv U_2 \cdot U_1' (\mathrm{mod}\, m) \tag{5}$$

Multiply the comparison (1) by U_1' and carry all its terms into its left part, using the above notations obtain:

$$V_3' + V_1 + 1 \equiv 0 (\mathrm{mod}\, m) \tag{6}$$

Multiply the latter comparison by V_1' such that $V_1 \cdot V_1' \equiv 1 (\mathrm{mod}\, m)$ and obtain:

$$V_1' + V_3' \cdot V_1' + 1 \equiv 0 (\mathrm{mod}\, m) \tag{7}$$

Further multiply the comparison (6) by V_3 such that $V_3 \cdot V_3' \equiv 1 (\mathrm{mod}\, m)$. Then:

$$V_1 \cdot V_3 + V_3 + 1 \equiv 0 (\mathrm{mod}\, m) \tag{8}$$

The comparisons (7), (8) include mutually inverse modulo ***m*** power residues $V_3' \cdot V_1'$ and $V_1 \cdot V_3$ which are a product of power residues.

Denote $V_2 \equiv V_3' \cdot V_1' (\mathrm{mod}\, m)$.

Then the inverse of V_2 power residue can be written as $V_2' \equiv V_1 \cdot V_3 (\mathrm{mod}\, m)$. The comparison is possible since $(V_1 \cdot V_3) \cdot (V_1' \cdot V_3') \equiv (V_1 \cdot V_1') \cdot (V_3 \cdot V_3') \equiv 1 \cdot 1 \equiv 1 (\mathrm{mod}\, m)$.

With regard for the above taken notations transform the comparisons (6), (7), (8) into the following:

$$V_3' + V_1 + 1 \equiv 0 (\mathrm{mod}\, m) \tag{9}$$

$$V_1' + V_2 + 1 \equiv 0 (\mathrm{mod}\, m) \tag{10}$$

$$V_2' + V_3 + 1 \equiv 0 (\mathrm{mod}\, m) \tag{11}$$

In (9), (10), (11) the primed residues are inverse modulo ***m*** of the correspondent unprimed power residues. The relations of the residues are as follows:

$$\begin{aligned} V_1' &= V_2 \cdot V_3 (\mathrm{mod}\, m) \\ V_2' &= V_1 \cdot V_3 (\mathrm{mod}\, m) \\ V_3' &= V_1 \cdot V_2 (\mathrm{mod}\, m) \end{aligned} \qquad (12)$$

The comparisons (9), (10), (11) imply that any of the six power residues has an adjacent power residue, e.g.: $V_1 + 1 = -V_3' (\mathrm{mod}\, m)$ or $V_3' + 1 = -V_1' (\mathrm{mod}\, m)$. Since ***p*** is an odd number, $-V_3'$ and $-V_1$ are also power residues.

Power residues are easy to present by one base functions. For the congruence modulo modulo a prime it is convenient to use a generator as the base, since g^j runs over the complete residue system modulo ***m*** if ***j*** runs over the values from 1 to $\varphi(m)$. Therefore, any residue can be written as a power function. Present the power residues as power functions and continue the analysis.

$$\begin{aligned} V_1 &\equiv g^{j_1 p} (\mathrm{mod}\, m) \\ V_1^{'} &\equiv g^{j_1^{'} p} (\mathrm{mod}\, m) \\ V_2 &\equiv g^{j_2 p} (\mathrm{mod}\, m) \\ V_2^{'} &\equiv g^{j_2^{'} p} (\mathrm{mod}\, m) \\ V_3 &\equiv g^{j_3 p} (\mathrm{mod}\, m) \\ V_3^{'} &\equiv g^{j_3^{'} p} (\mathrm{mod}\, m), \end{aligned} \qquad (13)$$

where g is a generator modulo ***m***.

The sum of power functions powers correspondent to the mutually inverse residues is congruent to 0 modulo $\varphi(m)$:

$$\begin{aligned} j_1^{'} p + j_1 p &\equiv 0 (\mathrm{mod}\, \varphi(m)) \\ j_2^{'} p + j_2 p &\equiv 0 (\mathrm{mod}\, \varphi(m)) \\ j_3^{'} p + j_3 p &\equiv 0 (\mathrm{mod}\, \varphi(m)) \end{aligned} \qquad (14)$$

As the relations (13) and (14) are considered modulo ***m***, and $g^{\varphi(m)\cdot k} \equiv 1(\mathrm{mod}\, m)$, the powers multiple of $\varphi(m)$ can be discarded, i.e. take the powers to the values less than $\varphi(m)$. Thereupon suppose that $j_1 p < \varphi(m)$, $j_2 p < \varphi(m)$, $j_3 p < \varphi(m)$, $j_1^{'} p < \varphi(m)$, $j_2^{'} p < \varphi(m)$, $j_3^{'} p < \varphi(m)$.

Then from (14) can come to the equalities:

$$\begin{aligned} j_1^{'} p + j_1 p &= \varphi(m) \\ j_2^{'} p + j_2 p &= \varphi(m) \\ j_3^{'} p + j_3 p &= \varphi(m) \end{aligned} \qquad (15)$$

(15) can be written as:

$$\begin{aligned} j_1^{'} p &= \varphi(m) - j_1 p \\ j_2^{'} p &= \varphi(m) - j_3 p \\ j_3^{'} p &= \varphi(m) - j_3 p \end{aligned} \qquad (16)$$

Set the corresponding power functions in (12)

$$\begin{aligned} g^{\varphi(m)-j_3 p} &\equiv g^{j_1 p} \cdot g^{j_2 p} (\mathrm{mod}\, m) \\ g^{\varphi(m)-j_2 p} &\equiv g^{j_1 p} \cdot g^{j_3 p} (\mathrm{mod}\, m) \\ g^{\varphi(m)-j_1 p} &\equiv g^{j_2 p} \cdot g^{j_3 p} (\mathrm{mod}\, m) \end{aligned}$$

Set congruous the powers of any of the latter comparisons and obtain:

$$j_1 p + j_2 p + j_3 p \equiv 0(\mathrm{mod}\, \varphi(m)) \qquad (17)$$

Add together the left and the right parts of the equation (16). Then:

$$j_1^{'} p + j_2^{'} p + j_3^{'} p = 3\varphi(m) - j_1 p - j_2 p - j_3 p \qquad (18)$$

Each summand in (17) is less than $\varphi(m)$ so the sum is less than $3\varphi(m)$. Therefore, this sum equals either $\varphi(m)$ or $2\varphi(m)$. If the sum in (17) equals $2\varphi(m)$, the other sum of the primed powers equals $\varphi(m)$. The comparisons (9), (10), (11) are seen to include

the power residues V_1, V_2, V_3 and three inverse of them power residues V_1', V_2', V_3'.

To be definite suppose that

$$j_1 p + j_2 p + j_3 p = \varphi(m) \tag{19}$$
$$j_1' p + j_2' p + j_3' p = 2\varphi(m)$$

From the two latter equations obtain the relation:

$$2(j_1 p + j_2 p + j_3 p) = j_1' p + j_2' p + j_3' p \tag{20}$$

To be definite suppose that $j_1 p < j_2 p < j_3 p$, since there are no like powers by virtue of incongruency of the residues V_1, V_2, V_3 modulo ***m***. Then (20) implies that $j_3' < j_2' < j_1'$.

Thus, the search of the class of prime numbers, modulo which power residues are inexpendable into a sum of two power residues, has given no positive result.

5.2 Criteria of Power Residues Expandability

Criterion 1. *Existence of adjacent power residues*.

The condition of power residues expandability implies:

$$u_1 \equiv u_2 + u_3 (\mathrm{mod}\, m), \tag{1}$$

where ***m*** is a prime number.

The inverse power residue exists by virtue of Property 2.

Multiply the comparison by u_3' inverse modulo ***m*** of the power residue u_3 and obtain:

$$u_1 \cdot u_3' \equiv u_2 \cdot u_3' + 1 (\mathrm{mod}\, m) \tag{2}$$

A product of power residues is a power residue (Property 1). Hence:

$$u_4 \equiv u_5 + 1 (\mathrm{mod}\, m), \tag{3}$$

where $u_4 \equiv u_1 \cdot u_3' (\mathrm{mod}\, m)$, $u_5 \equiv u_2 \cdot u_3' (\mathrm{mod}\, m)$.

As seen from the latter comparison the power residues u_4 and u_5 are adjacent. Thus, at the expandability of at least one power residue u_1 there must exist two adjacent power residues, which is a criterion of power residues expandability.

The existence of adjacent power residues is an obligatory condition of power residues expandability, their absence pointing to impossibility to expand any power residue.

Fermat's equation can exist if and only if one of the numbers ***a***, ***b***, ***c*** is a multiple of ***m***. Then the comparison $c^n \equiv b^n + a^n (\mathrm{mod}\, m)$ is possible.

As will be shown below quadratic residues modulo 3 and modulo 5 are inexpandable, therefore, any Pythagorean triple includes a number multiple of 3 and a number multiple of 5.

Criterion 2. *If there exist two power residues such that their product is congruent to their own sum modulo* ***m****, the power residues modulo* ***m*** *are expandable modulo* ***m****.*

Assume $V_1 \cdot V_2 \equiv V_1 + V_2 (\mathrm{mod}\, m)$. Carry V_1 to the left and factor it out and obtain: $V_1 (V_2 - 1) \equiv V_2 (\mathrm{mod\ m})$.

If V_1 and V_2 are power residues, (V_2-1) is also a power residue otherwise in the latter comparison V_2 would have been a power nonresidue by Property 6. Therefore, V_2 has an adjacent power residue (V_2-1). Similar actions with the residue V_1, will give: $V_2 (V_1 - 1) \equiv V_1 (\mathrm{mod\ m})$. From the latter comparison comes out the following conclusion: the residue V_1 also has an adjacent power residue.

Consider the equations (9), (10) of 5.1. The two power residues have the adjacent power residues $(V_1 + 1)$ and $(V_1' + 1)$, while their product is congruent to their own sum modulo ***m***:

$(V_1 + 1) \cdot (V_1' + 1) \equiv 1 + V_1 + V_1' + 1$ (modm).

Thus, criteria of expandability 1 and 2 are closely connected and mutually inverse.

Criterion 3. *The power* ***p*** *residues modulo* ***m*** *at* $\varphi(m)$ *which is not a multiple of* ***p*** *are expandable into a sum of two power residues*.

If $\varphi(m)$ is not a multiple of ***p***, the comparison of the form $x^p \equiv V(\mathrm{mod}\, m)$ has a unique solution ([2], Ch. 6, §5). Any ***p*** power number gives some power residue. As the above comparison has a unique solution, any residue of the complete residue system is a power of a number of this complete residue system, i.e. is a power residue.

Thus, residues of power ***p*** modulo ***m*** at $\varphi(m)$ which is not a multiple of ***p*** are expandable into a sum of two power residues.

5.3. Particular Cases of Power Residues Expandability

Criterion 1 of power residues expandability implies that to expand quadratic residues into a sum of two quadratic residues it is essential and sufficient for at least two of all the quadratic residues to be adjacent.

Proceeding from this postulate consider the expandability of quadratic residues modulo some primes.

5.3.1. Modulus 3. Modulo 3 there is only one number to be a quadratic residue, which is 1. There is no expandability of the quadratic residue into a sum of two quadratic residues.

5.3.2. Modulus 5. There are two quadratic residues modulo 5. These are the numbers 1, 4 and they are not adjacent. There is no expandability of the quadratic residues modulo 5 either.

Since the quadratic residues modulo 3 and modulo 5 are not expandable into a sum of two quadratic residues, any Pythagorean triple can be asserted to include a multiple of three and a multiple of 5. Illustrate this by the formulae to obtain Pythagorean triples: m^2+n^2, m^2-n^2, $2mn$, where ***m*** and ***n*** are coprimes. Examples of Pythagorean triples: 5, 4, 3 and 13, 12, 5.

5.3.3. Modulus 2p+1. If the number 2p+1 is a prime, there are only two residues of the power ***p***, namely 1 and m-1. Each of them is inexpandable into a sum of two power residues at $p \geq 3$ modulo 2p+1.

5.3.4 Modulus 4p+1. If the number 4p+1 is a prime, the amount of the power ***p*** residues equals $\frac{\varphi(m)}{p} = \frac{4p}{p} = 4$. Two of the power residues are certain and independent of the odd prime ***p*** value. These are 1 and -1, or ***m***-1. The sum of the other two power residues also equals ***m***. Denote them as V and ***m***-V.

Come to the problem of expandability of power residues into a sum of two power residues.

Criterion 1 of power residues expandability implies that expandability exists if there are at least two adjacent power residues.

To be definite V<***m***-V. For the residue V to be adjacent to 1, it has to equal 2. In this case the number $2 \cdot 2 = 4$, being a product of power residues, must also be a power residue. The number 4p=m-1 is a power residue, hence, ***p*** is a power residue too, as 4 and ***m***-1 are power residues. Being a product of two power residues the number ***2p*** is also a power residue.

Thus, there are over four power residues, which is impossible. Hence, the number 2 cannot be a power residue modulo m=4p+1. If 1 has no adjacent power residue, (m-1) has no adjacent power residue either.

So, for the power residues expandability to exist, we have to suppose that V and m–V, the sum of which equals ***m***, are adjacent power residues. Then:

$$m-V=V+1$$

$$\text{or} \quad m-1=2V.$$

The left part of the latter equality is a power residue, while the right part is a product of the power residue V by the number 2, which has to be a power residue, too (Properties 1, 4). However, the number 2, as stated above, is not a power residue, hence,

adjacent power residues modulo ***m=4p+1*** are impossible. This convention implies the following conclusion: power residues modulo m=4p+1 are inexpendable into a sum of two power residues.

5.4. Expandability of Quadratic Residues

Theorem 5. *Quadratic residues modulo any prime **m>5** are expandable into a sum of two quadratic residues.*

Proof. The amount of quadratic residues modulo a prime equals $\frac{\varphi(m)}{2}$, there are as many quadratic nonresidues [2].

To prove this hypothesis the two following cases should be considered:

1. $\frac{\varphi(m)}{2} \equiv 1(\mathrm{mod}2)$

2. $\frac{\varphi(m)}{2} \equiv 0(\mathrm{mod}2)$

In the first case ***m***-1 is not a quadratic residue. By condition of expandability of at least one quadratic residue, have $u \equiv u_1 + u_2(\mathrm{mod}\, m)$. Properties 1, 2 and Criterion 1 of expandability of power residues are fully applicable to quadratic residues.

Illustrate the existence of adjacent quadratic residues in each of the cases.

Case 1. Let $\frac{\varphi(m)}{2} \equiv 1(\mathrm{mod}2)$. Consider a set of numbers of the complete residue system from 1 to m-1.

Building on Chapter 3, any residue of the complete residue system can be written as $\boldsymbol{a} \equiv g^{\frac{\varphi(m)}{P} i+j} \pmod{m}$,

where $\boldsymbol{g}$ is a generator.

Then the number which complements $\boldsymbol{a}$ to $\boldsymbol{m}$ equals

$$m\text{-}a \equiv g^{\frac{\varphi(m)}{P} i+j+\frac{\varphi(m)}{2}} \ (mod\ m)$$

In the right part of the two latter comparisons the powers $\boldsymbol{g}$ have different evenness as their difference is congruent to 1 modulo 2:

$$\frac{\varphi(m)}{2} i + j + \frac{\varphi(m)}{2} - (\frac{\varphi(m)}{2} i + j) \equiv 1 (\mathrm{mod}\, 2)$$

Hence, one of the numbers $\boldsymbol{a}$ or $\boldsymbol{m}$-$\boldsymbol{a}$ is a quadratic residue, while the other is a quadratic nonresidue.

Now, consider a set of numbers of the complete residue system modulo $\boldsymbol{m}$. The numbers 1 and 4 are quadratic residues. If the number 2 or 3 is a quadratic residue, then the adjacent 1 and 2 or the adjacent 3 and 4 will also be quadratic residues. If 2 and 3 are quadratic nonresidues, their complements to $\boldsymbol{m}$, i.e $\boldsymbol{m}$-2 and $\boldsymbol{m}$-3 are adjacent quadratic residues.

Thus, in Case 1 adjacent quadratic residues always exist. Hence, quadratic residues are expandable into a sum of two power residues.

Case 2. Let $\frac{\varphi(m)}{2} \equiv 0 (\mathrm{mod}\, 2)$. Both the numbers $a \equiv g^{\frac{\varphi(m)}{2} i+j} (\mathrm{mod}\, m)$ and $m - a \equiv g^{\frac{\varphi(m)}{2} i+j+\frac{\varphi(m)}{2}} (\mathrm{mod}\, m)$ belong to the same column of the residue matrix. Like in the above case, consider the set of numbers of the complete residue system

modulo ***m*** from 1 to $\frac{m-1}{2}$ and the other set of numbers which complement the former set of numbers to ***m***.

Write the residues modulo ***m*** in the form of a power function the base of which equals the generator ***g***. If a residue ***a*** of the former set can be written as

$$a \equiv g^{\frac{\varphi(m)}{2}i+j} (\mathrm{mod}\, m), \qquad (1)$$

then its complement to ***m*** is written as

$$m-a \equiv g^{\frac{\varphi(m)}{2}i+j+\frac{\varphi(m)}{2}} (\mathrm{mod}\, m) \qquad (2)$$

The powers in the right part of the two latter comparisons differ, as they should, in $\frac{\varphi(m)}{2}$. If the difference of the powers equals $\frac{\varphi(m)}{2}$, while $\frac{\varphi(m)}{2} \equiv 0(\mathrm{mod}\, 2)$ in the case under consideration, the powers have like evenness. This means that irrespective of the number ***a*** selected from the set, the numbers ***a*** and (***m-a***) are both either quadratic residues or quadratic nonresidues.

Reveal the convention by a specific example.

The first set numbers 1 and 4 are quadratic residues. Assume the worst, that the numbers 2, 3, 5 are quadratic nonresidues and there exists no pair of quadratic residues until 5.

As has already been said, the amount of quadratic residues and nonresidues in the complete residue system modulo a prime ***m*** equal $\frac{\varphi(m)}{2}$ each, as ***a*** and (***m-a***) can both be either quadratic residues or quadratic nonresidues. The former and the latter sets include an equal amount of quadratic residues and quadratic nonresidues. Hence, each of the amounts equals one half of the whole. In this case, the total amount of quadratic residues equals

the total amount of quadratic nonresidues when in each set the amounts of quadratic residues and quadratic nonresidues are equal.

Of the numbers less than 5 there are two quadratic residues and two quadratic nonresidues. To continue the discussion it is essential to answer the question if for all numbers greater than 5 quadratic residues and quadratic nonresidues can alternate, adjacent quadratic residues being absent.

If such alternation of quadratic residues and quadratic nonresidues is possible, while the number 5 is a quadratic nonresidue, then all even numbers including $\frac{m-1}{2}=\frac{\varphi(m)}{2}$ will be quadratic residues. Then as follows from 3.2 of Chapter 3, its complement to ***m*** being equal to $m-\frac{m-1}{2}=\frac{m+1}{2}$ is also a quadratic residue. The latter is always adjacent to $\frac{m+1}{2}$, as their difference equals $\frac{m+1}{2}-\frac{m-1}{2}=1$

Thus, in the worst distribution of quadratic residues there is always at least one pair of adjacent quadratic residues. Hence, quadratic residues modulo any prime m>5 are expandable into a sum of two quadratic residues. This completes the proof of the theorem.

5.5 Expandability of Power Residues Modulo a Composite

Wherever speaking about the expandability of power residues, in case it is not specially treated, the expandability of the odd prime ***p*** power residue into a sum of two like power residues is meant. The above analysis of expandability of power residues modulo a prime (Ch. 1, 1.4) stated that at least one power residue

being expandable, including the power residue 1, all power residues are expandable.

The residue 1, being a power residue modulo any number, is easy for mathematical operations: having its expansion, multiplication of the comparison by the power residue under consideration gives its expansion, as in the right part by Property 1 (Ch. 4, 4.1) a product of power residues is a power residue.

In case there are several variants of the residue 1 expansion, the multiplication of each variant by this power residue can give all the variants of its expansion.

There are primes modulo which power residues are inexpendable. Examples of such numbers are the primes of the form **2p+1** and ***4p+1*** for the power ***p***, the primes 13, 7 for the power ***p=3***, the prime 41 for the power ***p=5*** etc.

If the power ***p*** residues modulo ***m*** are inexpendable, Fermat's equation can have a solution only in case one of the equation numbers is a multiple of ***m***. In this case find solutions for the comparison of the type $x^p \equiv a^p \pmod{m}$, just as in 1.4 of Chapter 1, and obtain the expansion of power residues with one zero solution modulo ***m***. As shown in 5.3, quadratic residues modulo 3 and modulo 5 are inexpandable into a sum of two quadratic residues, hence, any Pythagorean triple includes a number multiple of 3, a number multiple of 5, and one possible number multiple of 15.

Prove the hypothesis of the power residues expandability into a sum of two like power residues modulo a composite number.

Theorem 6. *Power residues modulo any composite number are expandable into a sum of two like power residues.*

Proof. Consider expansions of the power residue 1 into a sum of two power residues modulo a composite number $m_1 \cdot m_2 \cdots m_n = M$

$$\begin{aligned} 1 &\equiv V_1 + V_2 \ (mod m_1) \\ 1 &\equiv V_3 + V_4 \ (mod m_2) \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ 1 &\equiv V_{2n-1} + V_{2n} \pmod{m_n} \end{aligned} \qquad (1)$$

If the power residue 1 is expandable modulo some number m_i, then in the right part of the comparison both power residues are greater than 1.

If there is no expandability of a power residue, one of the right part power residues modulo ***m*** equals zero, i.e. a zero solution, while the other equals 1. To be definite, suppose that in the right parts of the comparisons with inexpandable power residues (1) the power residue with an even subscript equals zero and the other one equals 1.

It is essential to obtain expansion of the power residue 1 into a sum of two power residues modulo product of moduluses $m_1 \cdot m_2 \cdots m_n = M$.

$$1 \equiv U_1 + U_2 (\mathrm{mod}\, M) \qquad (2)$$

It is also essential to demonstrate that there exists at least one such expansion of the power residue 1 into a sum of two power residues at $U_1 > 1$ and $U_2 > 1$.

To find the power residues U_1 and U_2, use the popular technique by Vinogradov ([2], Ch. IV, §3). Determine the numbers M_i and M_i' by the condition $M_i \cdot M_i' \equiv 1 (\mathrm{mod} m_i)$, where $M_i = \frac{M}{m_i}$.

$$U_1 \equiv M_1 \cdot M_1' \cdot V_1 + M_2 \cdot M_2' \cdot V_3 + \cdots + M_n \cdot M_n' \cdot V_{2n-1} (\mathrm{mod\ M}) \quad (3)$$

$$U_2 \equiv M_1 \cdot M_1' \cdot V_2 + M_2 \cdot M_2' \cdot V_4 + \cdots + M_n \cdot M_n' \cdot V_{2n} \ (\mathrm{mod\ M}) \quad (4)$$

If the found values U_1 and U_2 set in the comparison (2), obtain the expansion of the residue 1 into a sum of two power residues modulo M. It is easy to verify that the comparison (2) is implemented modulo each divisor of M, hence, the comparison is implemented modulo their product. Note that (3) includes all power residues with odd subscripts, while (4) includes the ones with even subscripts. Any pair of residues being swapped in any comparison of (1), find another variant of the expansion of 1 in (2), which can be obtained from (3), (4). E.g. in (3), (4) relevant to the first comparison

in (1) V_1 and V_2 can be swapped. The number of various variants of expandability is easy to determine if the amount of the comparisons in (1) equals ***n***. This number equals 2^n.

Note another fact. If modulo some m_i there exist several variants of the residue 1 expansion, only one of these variants should be included in the system (1). The other variants will give still more variants of the residue 1 expansion modulo M.

To demonstrate the existence of at least one expansion of 1 modulo product of moduluses, assume the worst that modulo any prime m_i the power residues are inexpendable. Then, for the comparison to be possible in the expansions (1) in each comparison one of the residues equals zero, while the other equals 1. To be definite assume that all power residues with subscripts equal 0. In this case in (4) $U_2 \equiv 0(\mathrm{mod}\, m)$, the expansion (2) with a nonzero solution is impossible.

For U_1 and U_2 in (2) to be greater than 1 it is sufficient to swap places any pairwise V_1, V_2 or V_3, V_4 residues in the comparisons (3), (4) etc. Then U_2 will not equal 0 as V_1 or V_3 do not equal 0.

If $m \geq 2$, the right part of any comparison of (1) includes a power residue equal to 1, even for the modulus to which there is no expansion. Hence, in (3), (4) for each comparison at $m \geq 2$ there is at least one power residue, therefore, the expansion (2) with a nonzero solution is always possible.

If n=1, the power residues modulo m_1 are likely to be inexpendable, while one of the right part summands in (2) will equal 0. Therefore, the power residue expansion is impossible to obtain by multiplication of this comparison by power residues.

Thus, the expansion of power residues modulo a number exists if and only if the modulus is a composite number, i.e. it has at least two divisors. In this case power residues are always expandable into a sum of two power residues. This completes the proof of the theorem.

At n=2 the comparisons (1) have the forms:

$$1 \equiv 1 + 0 (\mathrm{mod}\, m_1)$$

$$1 \equiv 0 + 1 (\mathrm{mod}\, m)$$

Their simultaneous solving will result in:

$$1 \equiv m_2 \cdot m_2' + m_1 \cdot m_1' (\mathrm{mod}\, m_1 \cdot m_2),$$

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

Thus, obtained the power residue 1 expansion into a sum of two power residues modulo product m_1 and m_2, when modulo each number the power residues are inexpendable. Therefore, all power residues modulo $m_1 \cdot m_2$ are expendable since the multiplication of the obtained expansion by any power residue modulo $m_1 \cdot m_2$ will result in power residues as product of power residues both in the left and the right part of the comparison.

For example. Cubic residues modulo 7 and modulo 13 are inexpandable into a sum of two cubic residues. Then the expansions of 1 will have the form:

$1 \equiv 1+0 \ (mod 7)$

$1 \equiv 1+0 \ (mod 13)$

The simultaineous solving results in: $1 \equiv 78+14 \ (mod 91)$

Theorem 7. *Expansion of any power odd prime* ***p*** *residue modulo* ***m*** *into a sum of two like power residues is a product of this power residue by the expansion the power residue 1 into a sum of two power residues, and the corresponding expansion of 1 into a sum of two like power residues exists.*

Proof. To begin with, find all possible variants to expand all the residues of the complete residue system modulo **m** into a sum of two other residues of the complete residue system modulo **m**.

Write the residue ***v*** of the complete residue system modulo **m** as the following sum:

$$v=(m-u)+(u+v) \ (mod\ m), \qquad (1)$$

where ***m*** is a composite number,

u, v are residues of the complete residue system modulo **m**.

The latter comparison is easy to see true if we remove the brackets in the right part of the comparison.

Determine the amount of possible extensions.

The amount of the residues modulo ***m*** equals *(m–1),* each being differently expandable into a sum of two power residues. The variant of expansion is determined by the value of ***u*** in (1). Of all (m–1) residues ***u*** can take (*m–2*) values except for $u \equiv -v(\mathrm{mod}\, m)$, as in this case $u + v \equiv 0(\mathrm{mod}\, m)$ and one of the comparison (1) summands will equal 0, but we are not interested in the zero solution variant. Therefore, the total amount of possible expansions is defined by the formula:

$$N=(m-1)(m-2) \qquad (2)$$

Now, in the comparison (1) equal the residue ***v*** to 1 and obtain one of the variants to expand 1 into a sum of two residues at a given **u**:

$$1 \equiv (m-u)+(u+1)(\mathrm{mod}\, m) \qquad (3)$$

Changing ***u*** from 1 to *m–2*, obtain *m–2* variants of expansion. Change the value of ***u*** until *m–2*, as at *u=m–1* the second summand equals 0, obtain a zero solution, which we are not interested in:

$$u+1=m-1+1=m \equiv 0(\mathrm{mod}\, m)$$

Further multiply *m–1* various residues by *m–2* variants of expansion of 1 and obtain the like amount of possible expansions of residues: *N=(m–1)(m–2).*

Thus, both ways of expansion produce the full amount of possible expansions.

In fact, the maximum amount of pairwise residues from *m–1* equals *(m–1)(m–2),* as each of the *m–1* residues works in combination with *m–2* residues except the variant when the sum of two residues is congruent to zero modulo ***m.***

Thus, the maximum amount of residue expansions can be obtained by multiplication of all the variants of the expansion of 1 by the residue of our interest. Therefore, for any expansion of any

residue there exist a corresponding expansion of residue 1 which is to be multiplied by the residue of our interest.

To continue, of all residue expansions of the complete residue system select the expansions which always exist by virtue of Theorem 6. Namely those of which the residues in the left part and both residues in the right part are power ***p*** residues modulo ***m***.

The expansions of the residue 1 into a sum of two residues which produce expansions of the power residues into a sum of two power residues also represent the expansion of the power residue 1 into a sum of two power residues. Otherwise, at the multiplication of the expansion of 1 by a power residue there would have appeared power nonresidues in the right part of the comparison (Property 2 of power residues). The expansion of 1 has been proven to exist.

All the variants of power residues expansion have been exhausted, each of them has been obtained by multiplication of this power residue by the expansion of the residue 1, the existence of which has also been proven. This completes the proof of the theorem.

Chapter 6. Proof of Fermat's Theorem

The present chapter is dedicated to the key problem of the monograph. Before we proceed to it, draw the reader's attention to the fact that solving the comparisons in the above proofs of Theorem 6 and Theorem 7 within the study of power residues expandability modulo a number was not supposed.

Now, write Fermat's equation for the prime ***p*** in the following form:

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

Suppose it has an integer nonzero solution at coprimes ***a, b, c***.

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

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

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

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

If the numbers ***a, b, c*** are coprimes and none of them is divisible of ***m***, while there are solutions to the comparisons (2), (3), the power ***p*** residues can be separated into a sum of two power ***p*** residues modulo ***m.***

If some number in (2), for example ***a***, is divisible by some prime number m_1, obtain the comparison $c^3 \equiv b^p \,(\text{mod}\, m_1)$, which as stated above in 1.4 has solutions. The second summand in the comparison equals 0 modulo m_1.

There are primes modulo which for some prime powers ***p*** power residues are inexpandable into a sum of two power residues. For example, the power 3 residues modulo 13, the power 5 residues modulo 41.

Since the comparison (2) must be satisfiable modulo any number, and there are numbers modulo which the power ***p*** residues are inexpandable into a sum of two power ***p*** residues, one of the numbers ***a, b, c*** must be a multiple of this number but not equal to 0. This secures the possibility of the comparison (2) modulo this number.

This reasoning also refers to the power 2. Modulo 3 and modulo 5 quadratic residues are inexpandable into a sum of two quadratic residues (Ch.5, 5.3). Therefore, any Pythagorean triple includes a multiple of 3 and a multiple of 5.

To analyse the possibility of Fermat's equation, consider the comparison (2) modulo various numbers.

Select any finite number ***m*** satisfying the inequality $c \le m < c^p$, at which, as assumed above, there is a solution to Fermat's equation.

The comparison (2) must be satisfiable both modulo ***m*** and modulo any number $m_i \le m$. Hence, the comparison (2) is satisfiable modulo product of these moduluses. Select the modulus $M = m!$.

As follows from Theorem 6, power residues modulo a composite number can be expanded into a sum of two power residues:

$$V_c \equiv V_b + V_a (\mathrm{mod}\, M) \tag{4}$$

As follows from Theorem 7, power residue expansion can be written as a product of the residue V_c by the residue 1 expansion into a sum of two power residues, and such residue 1 expansion exists. As there may be several expansions of the kind there exist different variants to expand the residue V_c.

Let one of the variants to expand 1 applicable for Fermat's equation be as follows:

$$1 \equiv u_1 + u_2 \,(mod\ M), \tag{5}$$

where u_1, u_2 are power ***p*** residues modulo M.

Further, multiply the latter comparison by V_c:

$$V_c \equiv u_1 \cdot V_c + u_2 \cdot V_c \ (mod\ \mathrm{M}) \tag{6}$$

The products of the power residues $u_1 \cdot V_c$ and $u_2 \cdot V_c$ are power residues (Property 1).

If among all the residue 1 expansion variants there is an expansion applicable for Fermat's equation and it is the one that was selected in the course of our discussion, then there will be obtained $u_1 \cdot V_c \equiv V_b\,(mod\ \mathrm{M})$, $u_2 \cdot V_c \equiv V_a\,(mod\ \mathrm{M})$, i.e. the comparison (3).

Proceed to the problem of finding solutions to the comparisons and Fermat's equation. Suppose $u_1 \equiv x^p (\mathrm{mod}\, M)$, $u_2 \equiv y^p (\mathrm{mod}\, M)$. Set these values in (5):

$$1 \equiv x^3 + y^3 (\mathrm{mod}\, M) \quad (7)$$

To obtain Fermat's equation it is essential to write each of the power residues (6) as the powers of some numbers. As V_c, u_1, u_2 are power residues, such numbers exist.

In general, the equation of the form

$$x^p \equiv V (\mathrm{mod}\, m) \quad (8)$$

can have a non-unique solution. In this connection the transfer from the comparison (6), which figures power residues modulo M=m!, to the powers of numbers must be thoroughly performed. Thus, to conclude there is no solution to Fermat's equation, it is essential to study all possible combinations of the numbers ***a, b, c*** at ***a<m, b<m, c<m.***

For the comparison (6) to be satisfiable any possible solutions may be used, while to obtain Fermat's equation it is essential to select proper solutions for the comparison $c^p \equiv V_c (\mathrm{mod}\, M)$.

The selected solutions ***x*** and ***y*** in (7) may be greater than ***m***, but less than ***m!***. The number ***c*** satisfying the equation (1) is less than ***m***. Meaning these very characteristics, discuss finding solutions for the following comparison:

$$c^p \equiv V_c (\mathrm{mod}\, M) \quad (9)$$

The number ***c*** is one of its solutions, which is also a hypothetical solution for Fermat's equation. Try and separate it into a sum of the other two powers.

The point is that in the expansions of the power residue V_c in (6) this residue also occurs in the right part of the comparison.

At the present moment of the research there is no reason to believe that the like solution for ***c*** in the left part can be used in the right part. There may be one power residue while solutions may be

various, and at some other solutions the values of ***a*** and ***b*** modulo ***M*** can be obtained. Which means it is possible to obtain not only a true comparison but also an equality.

Suppose the comparison (9) have some more solutions besides ***c<m*** known by the definition

$$c_i^{\,p} \equiv V_c (\mathrm{mod}\, M) \tag{10}$$

The right parts of (9) and (10) are the same, therefore, the left parts are congruous modulo ***M***

$$c_i^{\,p} \equiv c^p (\mathrm{mod}\, M) \tag{11}$$

The number ***c*** is dividing M=m!. Hence, the comparison is possible modulo ***c***. Then:

$$c_i^{\,p} \equiv 0 (\mathrm{mod}\, c) \tag{12}$$

The latter obviously implies that $c_i \equiv 0 (\mathrm{mod}\, c)$, while the solutions for ***c*** have the form $c_i \equiv k_i \cdot c$.

The number ***c*** satisfies Fermat's equation, and any $c_i^{\,p}$ produces the like power residue V_c, if such solutions exist for some ***p*** and ***m*** in general.

The problem of the amount of the solutions is the subject of other works for it is unessential for the proof of Fermat's theorem. It is essential that all the solutions are multiples of ***c***, while the coefficient of multiplicity $k_i \equiv 1$ at the unique solution and greater than 1 at the non-unique solution.

The solutions being generally defined, replace in (6) all the power residues by the powers ***p*** of the obtained general solutions:

$$c^p \equiv x^p \cdot (k_i \cdot c)^p + y^p (k_j \cdot c)^p (\mathrm{mod}\, M), \tag{13}$$

where k_i, k_j are integers.

The latter comparison is always possible, irrespective of the solution set for c_i in (10).

In the left part leave c^p, as by the primary hypothesis it is expandable into a sum of two other powers b^p and a^p.

Thus, the comparison (13) has to give Fermat's equation, if it has a solution in general and k_i, k_j, the variant of the expansion of 1, as well as the solutions ***x*** and ***y*** have been correctly selected.

The multiplication gives:

$$c^p \equiv (x \cdot k_i \cdot c)^p + (y \cdot k_j \cdot c)^p (\mathrm{mod} M) \tag{14}$$

From the latter the following is possible:

$$b \equiv x \cdot k_i \cdot c (\mathrm{mod} M) \tag{15}$$

$$a \equiv y \cdot k_j \cdot c (\mathrm{mod} M) \tag{16}$$

Irrespective of whether the comparison (10) has a unique solution for which $k_i = 1$, $k_j = 1$ or non-unique for which $k_i \geq 1$, $k_j \geq 1$, the latter comparisons are possible modulo any divisor ***M***, modulo ***c*** in particular:

$$b \equiv 0 (\mathrm{mod} c) \tag{17}$$

$$a \equiv 0 (\mathrm{mod} c) \tag{18}$$

Thus, irrespective of ***x, y,*** k_i, k_j, the numbers ***b*** and ***a*** are multiples of ***c***.

Let $b = k_1 \cdot c$, $a = k_2 \cdot c$.

Set the obtained solutions in Fermat's equations (1):

$$c^p = (k_1 \cdot c)^p + (k_2 \cdot c)^p \tag{19}$$

Cancel c^p and obtain the impossible at $k_1 \geq 1$, and $k_2 \geq 1$ equality:

$$1 = {k_1}^p + {k_2}^p \tag{20}$$

There is no solution for Fermat's equation. Fermat's theorem for odd prime powers is true.

It seems expedient to analyse yet another approach. If there is a solution for Fermat's equation at coprimes ***a, b, c***, its left and right parts have to be congruous modulo any number, modulo m! including, where ***m*** is greater than or equal to ***c***, such that a solution for equation exists. Then there also is a power residue expansion into a sum of two power residues modulo any number.

As follows from Theorem 7, the power residue c^p expansion can be written as a product of c^p by the expansion of the power residue 1 into a sum of two power residues modulo ***m!***.

Try and find the corresponding separation of the power residue 1 into a sum of two power residues of Fermat's equation, as such separation exists (Theorem 7).

Proceeding from the fact that c>b, c>*a*, it is impossible to divide each term of Fermat's equation by c^p even modulo m!, since representing b^p as

$$b^p \equiv (b + k \cdot m!)^p \,(\mathrm{mod}\, m!) \qquad (21)$$

$$\text{or } b^p \equiv b^p + k \cdot m! \,(\mathrm{mod}\, m!), \qquad (22)$$

it becomes evident that at any ***k*** the number ***c*** is dividing ***km***!, as $c \le m$ and is dividing ***m***!, while b^p is not divisible by ***c*** or all the more so by c^p.

To obtain the expansion of 1 satisfying Fermat's equation (1) , like in (5) try and find the number to multiply the comparison $c^p \equiv b^p + a^p \,(\mathrm{mod}\, m!)$.

This number has to be of the ***p-th*** power so that after the multiplication in the right part there also appear the ***p-th*** powers of some numbers:

$$c^p \cdot c'^p \equiv (b \cdot c')^p + (a \cdot c')^p \,(\mathrm{mod\ m!})$$

If Fermat's equation has a solution, then there is the power residues expansion, hence, by Theorem 7 there is the expansion of 1 into a sum of two power residues. However, there is no number c' which might give a solution to the comparison

$c^p \cdot c'^p \equiv 1(\mathrm{mod}\, m!)$ at $\boldsymbol{c \le m}$. This is easy to see if consider the latter comparison modulo $\boldsymbol{c}$ which is dividing $\boldsymbol{m!}$:

$$0 \equiv 1(\mathrm{mod}\, c) \tag{23}$$

The obtained comparison is impossible.

Thus, is failing the search for the power residue 1 expansion into a sum of two power residues modulo $\boldsymbol{m!}$ at $c \le m$ and solvability of Fermat's equation, though such expansion of the power residue 1 into a sum of two power residues by Theorem 7 has to be. Hence, Fermat's equation has no solution. Fermat's theorem for odd prime powers is true.

Continue the discussion. If in Fermat's equation the power is a composite number, the proof should be divided into the following two cases:

1. The power has the form 2^i.
2. The power is a multiple of some odd prime.

Analyse each case separately.

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

In this connection assume that $i_1 > 0$. Write Fermat's equation as follows:

$$(c^{2^{i_1}})^4 = (b^{2^{i_1}})^4 + (a^{2^{i_1}})^4 \tag{24}$$

The latter equation being considered Fermat's equation for the power 4, it has no solution as Fermat proved himself, to say nothing of these solutions being some powers of numbers. Hence, Fermat's equation has no solutions for any powers $n = 2^i$ at $\boldsymbol{i}$>1.

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

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

The latter equation being considered Fermat's equation for an odd prime power $\boldsymbol{p}$, then as proven above it has no solution for any odd primes $\boldsymbol{p}$, to say nothing of these solutions being some powers

of the numbers ***a, b, c***. This implies that Fermat's equation has no solutions for any $n = n_1 \cdot p$ at $n_1 > 0$.

The two above discussed cases have exhausted the numbers n>2. Hence, true is the following statement: Fermat's equation has no solutions for any powers greater than 2.

This completes the proof of Fermat's theorem.

References

1. Ribenboim, P. Fermat's Last Theorem for Amateurs. NY: Springer. First edition, 1999.
2. Davenport H. Multiplicative Number Theory. NY: Springer. Third Edition, 2000.
3. Виноградов И.М. Основы теории чисел. Государственное издательство технико-теоретической литературы, Москва, 1953г.
4. Постников М.М. Введение в теорию алгебраических чисел. М, Наука, 1992г.

Задник

КАМЛИЯ РАСИМ АРКАДЬЕВИЧ

ТЕОРЕМА ФЕРМА
И РАЗЛОЖИМОСТЬ СТЕПЕННЫХ ВЫЧЕТОВ

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.