«RECTANGLE» METHOD AND «MODULE REPLACEMENT» FOR UNKNOWN FIRST-ORDER COMPARISONS

Abstract: This work is one of the important factors of development of numbers theory, rectangular method and module replacement have been explained for comparisons $ax \equiv b \pmod{m}$ in depth, examples have been shown and new results have been proved. Methods have not been explained in textbooks and manuals. Therefore, new method of finding integer solutions of some Diophant’s equations was designated.

Key words: Comparison, discount module, unknown, equation number, matrix, solution.

Language: English

Citation: Usarov, B. O. (2019). «Rectangle» method and «Module replacement» for unknown first-order comparisons. ISJ Theoretical & Applied Science, 10 (78), 420-424.

Soi: http://s-o-i.org/1.1/TAS-10-78-78 DOI: https://dx.doi.org/10.15863/TAS.2019.10.78.78

Scopus ASCC: 2602.

Introduction
It is clear that, IF $a$ and $b$ are integers ,therefore, $m$ is natural number, and when $a$ devides to $m$ as well as $b$ devides to $m$, the resudes are equal to each other, then $a$ and $b$ are comparable numbers according to module $m$ and written as $a \equiv b \pmod{m}$. As well as, comparison $ax \equiv b \pmod{m}$ is called an unknown first-order comparison. Here $x$ is unknown number [1, 2, 4].

Analysis of Subject Matters
There are several methods of solving comparison like $ax \equiv b \pmod{m}$ and we will analyze each of them with examples.

1. Method choice. The essence of this method is that instead of $x$ in the $a \equiv b \pmod{m}$ comparison, all discounts in the complete system, $\{0,1,2,3, \ldots, m-1\}$ discount system on the module $m$ are consecutive. Which is the solution if any of them make the comparison right. However, when the module is much older the method becomes less efficient [1, 2, 3, 4, 8].

Exercise-1 $7x \equiv 2 \pmod{9}$ solve the comparison.

Solving. Because of $\left(\frac{7}{9}\right) = 1$ in comparison $7x \equiv 2 \pmod{9}$, the solution is unique.

There is a complete system of discounts on 9 modules $\{0,1,2,3,4,5,6,7,8\}$. We will sure that $x \equiv 8 \pmod{9}$ by checking directly.

Answer $x \equiv 8 \pmod{9}$.

2. Replacement coefficients method. The coefficients of the given comparison are adjusted until they are multiple exclusive and are resolved by the unknown by using the properties of comparisons [1, 2, 3, 8].

Exercise-2 $7x \equiv 5 \pmod{9}$ solve the comparison.

Solving. $7x \equiv 5 + 9 (\equiv 0) 7x \equiv 14 (\equiv 5)$ because of $\left(\frac{7}{14}\right) = 7$ and $\left(\frac{7}{9}\right) = 1$, solution $x \equiv 2 \pmod{9}$.

Answer: $x \equiv 2 \pmod{9}$.

Exercise-3. $17x \equiv 25 \pmod{28}$ solve the comparison.

Solving. $17x + 28x \equiv 25 \pmod{28}$ $45x \equiv 25 \pmod{28}$

From this $9x \equiv 5 \pmod{28}$ $9x \equiv 5 - 140 (\equiv -135) \equiv -135 \pmod{28}$ $x \equiv -15 \equiv 13 \pmod{28}$ the solution is found.

Answer: $x \equiv -15 \equiv 13 \pmod{28}$.

3. Method of using Euler’s theorem. It is clear that, if $a \equiv m = 1$, then $a^{\phi(m)} \equiv 1 \pmod{m}$ comparison is acceptable. From this, it might be
written comparison \( a^{\phi(m)} \cdot b \equiv b \mod m \). We will
sure that \( x \equiv a^{\phi(m)} \cdot b \mod (mod m) \) by comparing
the last comparison with comparison \( ax \equiv b \mod m \). When solving
expressions, expression \( x \equiv a^{\phi(m)} \cdot b \mod (mod m) \) should be come into
the smallest positive discount according to module \( m \) [1, 2, 3, 4, 5, 8].

Exercise-4. \( 3x \equiv 7 \mod(11) \) solve the comparison.

Solving. \( x \equiv 3^{\phi(11)-1} \cdot 7 \mod(11) \), because of
\( \phi(11) = 10 \cdot 3^2 \equiv 9 \mod(11) \)
\( 3^4 \equiv 4 \mod(11) \)
\( 3^5 \equiv 12 \equiv 1 \mod(11) \), \( x \equiv 3^9 \cdot 7 \equiv 28 \equiv 6 \mod(11) \)
solution is equal \( x \equiv 6 \mod(11) \).
Solution \( x \equiv 6 \mod(11) \).

4. Method of using uninterrupted fractions. \( ax \equiv b \mod m \) spread the \( m \) and \( a \mod m \) in the comparison to continued fractions, then define as
\( P_k = (k = 1; n) \). Because of \( q_{k} \) is irregular fraction
\( P_n = m \), \( q_n = a \). As a result, \( x \equiv (-1)^{n-1} \cdot b \cdot P_{n-1} \mod m \) comparison appeared. [1, 2, 3].

Exercise-5. \( 22x \equiv 34 \mod 38 \) solve the comparison.

Solving. \( 22,38 = 2 \), because of \( 34 : 2 \), we divide into \( 2 \) module and both two parts of comparison. Then appear this comparison
\( 11x \equiv 17 \mod(19) \).

now, we separate \( \frac{19}{11} \) to several accordant fractions.
\( \frac{19}{11} = 1 + \frac{8}{11} = 1 + \frac{1}{1 + \frac{2}{8}} = 1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{3}}} \)
\( = 1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{3}}} \)
\( = 1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{3}}} \)
\( = 1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{3}}} \)
\( = 1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{3}}} \)
\( q_1 = 1, q_2 = 1, q_3 = 2, q_4 = 1, q_5 = 2 \)
Then make a table for accordant fractions
\[
\begin{array}{c|ccccc}
q_k & 1 & 1 & 2 & 1 & 2 \\
p_k & 1 & 1 & 2 & 5 & 7 & 19 \\
\end{array}
\]
So, \( P_{5-1} = P_4 = 7 \). From this
\( x \equiv (-1)^4 \cdot 7 \cdot 17 \mod(19) \) or \( x \equiv 5(\mod 19) \).

In this case solutions of given comparison are:
\( x \equiv 5,24(\mod 38) \).
solution: \( x \equiv 5,24(\mod 38) \).

5. Method of using inverse class. In this method, we find the linear distribution of \( 1 \) to the numbers \( a \) and \( m \). \( 1 = au + mv \) number \( u \) is an opposite to number \( a \) for \( a \) module \( m \) in distribution. [2, 6].

We find solution for module \( m \) by multiplying both parts comparison to found unknown number.

Exercise-6. \( 5x \equiv 7 \mod(8) \) solve the comparison.

Solving. We find the linear expression of the largest common denominator of numbers 5 and 8 by using the Euclidean algorithm:
\( 8 = 5 \cdot 1 + 3 ; \quad 3 = 2 \cdot 3 + 1 \) \( 5 = 3 \\cdot 2 + 2 \) \( 2 = 3 \cdot 2 + 1 \) \( 1 = 2 \cdot 2 + 0 \).

From this \( 1 = 3 - 2 \cdot 1 = 3 - (5 - 3 \cdot 1) = 3 - 5 + 3 \cdot 1 = 3 - 2 - 5 = \) \( 8 = 2 \cdot 5 - 2 = 5 \) \( = 8 \cdot 2 - 5 - 2 = 5 \) \( = 8 - 2 - 5 - 2 = 5 \) \( = 8 - 2 - 5 - 2 = 5 \) \( = 5 - (3 - 5) + 8 \cdot 2 \)
Thus, \( 1 = 5 - (-3) + 8 \cdot 2 \) number 5 is opposite number to \(-3\) according to module 8 or \(-3 \equiv 5(\mod 8) \)
\( 5x \equiv 7 \mod(8) \) we find the solution by multiplying both parts of comparison 5 which is an opposite number for 5 according to module 8:
\( 5 \cdot 5x \equiv 5 \cdot 7 \mod(8) \) \( 25x \equiv 35 \mod(8) \)
\( x \equiv 3 \mod(8) \)
Answer: \( x \equiv 3 \mod(8) \).

Consequently, when it comes to the solution of the comparison \( ax \equiv b(\mod m) \), it is clear from the above statements that when the coefficients of the comparison are large enough, the application of these methods is not practical. In this regard, let's look at the most effective and also the most useful «Rectangle» method and «Module replacement».

Research Methodology

«Rectangle» method. The essence of this method is «Solving equations for given unknowns», «Replacement of class discounts by module \( m \) in comparison». The result of these comparisons, \( ax - m = mx + b \) is made using the equation to make comparisons much simpler, where the solutions are interrelated. The following theorem is relevant here. [7, 8, 9].

Theorem. IF
\( ax \equiv b(\mod m) \) (1)
is given, \( (a; m) = 1 \) va \( a > 0 \), then
\( ax - m = mx + b \) (2)

Proof. Based on the theorem about the linear form for comparison, and let us describe the form \( x \) and \( ax \pm m \) in the Descartes coordinate system as follows. (Graph 1).

In this graph \( x \) is base and \( m \) is height of rectangle placed inside to the second rectangle in which \( ax \) is height. \( S \) is the size of large right strangle while \( S' \) is size of small right strangle. [11].

Now we check \( S \) and \( S' \) that they are comparisons according to module \( m \):
\( S = ax \cdot x = ax^2 = (mq_1 + r) \cdot x \)
\( S' = (ax - m) \cdot x = (ax - m) \cdot x = (mq_2 + r) \cdot x \)
Here, it comes to \( S \) va \( S' \) are comparisons according to module \( m \). Then pay attention to ratio of \( S \) va \( S' \).

\[
S = \frac{ax^2}{(ax - m) \cdot x} = \frac{(mq_1 + r) \cdot x}{mq_1 + r} = \frac{mq_1 + r}{mq_2 + r}
\]

from this. We will have
\[
(ax - m = mq_2 + r). \quad \text{Thus, from first equation (1) we can write this equation}
\]

\[
\begin{align*}
S' &= \frac{ax^2}{(ax - m) \cdot x} = \frac{(mq_1 + r) \cdot x}{mq_2 + r} \\
\end{align*}
\]

Thus, \( ax - m = mq_2 + r \) as \( ax - m = mx_1 + b \). Theorem was proved.

From this theorem it comes to this conclusion:

By using (1) and (2) as well as this \( x = \frac{mx_1 + b + m}{mx_1 + b + m} \) equations, interchange module \( m \) to module \( a \) also, \( mx_1 + b + m \equiv 0 \bmod (mod a) \Rightarrow mx_1 \equiv -(b + m) \bmod (mod a) \). By continuing these replacements \( n \) times, we can make simpler comparison form of solutions of first equation (1) linking to each other:

\[
ax \equiv b(\text{mod } m), \quad ax - m = mx_1 + b \Rightarrow x = \frac{mx_1 + b + m}{m + at_1}
\]

\[
\begin{align*}
ax \equiv b(\text{mod } m), \quad ax - m &= mx_1 + b \Rightarrow x = \\
\end{align*}
\]

Exercise-7. 983x \( \equiv 991 \bmod (mod 997) \) solve the comparison.

Solving.

1). \( 983x \equiv 991 \bmod (mod 997) \), \( 983x - 991 = 997x_1 + 991, x = \frac{997}{997} \)

2). \( 997x_1 \equiv -1988 \bmod (mod 983) \), \( 14x_1 \equiv 961 \bmod (mod 983) \), \( 14x_1 - 983 = 983x_2 + 961 \), \( 983x_2 + 1944 \)

3). \( 983x_2 \equiv -1944 \bmod (mod 14) \), \( 3x_2 \equiv 2 \bmod (mod 14) \), \( 3x_2 - 14 = 14x_3 + 2, x_2 = \frac{14x_3 + 16}{3} \)

4). \( 14x_3 \equiv -16 \bmod (mod 3) \), \( 2x_3 \equiv 2 \bmod (mod 3) \), \( x_3 \equiv 1 \bmod (mod 3) \), \( x_4 \equiv 0 \).

\( x_4 = 0, x_3 = 1, x_2 = 10, x_1 = 841, x = 855 \)

Answer: \( x \equiv 855 \bmod (mod 997) \).

Thus, \( x \equiv 855 \bmod (mod 997) \) solution of given comparison.

Check: \( 983 \cdot 855 - 991 = 840465 - 991 = 839474 : 997 \).

The above properties of the surfaces of the module \( m \) are as follows:

\[
\begin{align*}
S &= ax \cdot x = ax^2 = (mq_1 + r) \cdot x \\
S' &= (ax - m) \cdot x = (ax - m) \cdot x = (mq_2 + r) \cdot x \\
\end{align*}
\]

Thus, it must be \( q_1 - q_2 = 1 \).

Now for the comparison (1) we will consider«Module replacement»:

Make a matrix for comparison \( ax \equiv b(\text{mod } m) \)

\[
\mathbb{M}(b) = (amb)
\]

Here, \( a \)-decisive module, \( m \)-main module, \( a \) and \( m \) interchangeable modules, \( b \)-residue (discount), \( (amb) \)-interchangeable matrix, signalize it as \( \mathbb{M}(b) \), \( (amb + m \cdot t_n) \)-decisive replacement of module, [9].

\[
ax \equiv b(\text{mod } m) \quad \text{-module replacement for comparison, } \mathbb{M}(b) = (amb)
\]

Replacing the module means the following replacements:

1). Reciprocal replacement of modules and change residual gesture in the matrix;

2). Multiply the main module to nonzero number and add to decisive module or residue;
3). In the matrix replace modules, switch to each other until the residual is found.

Exercise-8. $11x \equiv 13 (mod \ 17)$ solve the comparison.

Solving: Make a interchangeable matrix in order to replace module:

$$\frac{11}{17} M (13) = (111173)$$
$$\frac{16}{17} M (13) = (111173) - (111730) - (1711 - 30) - (6113) - (61114) - (116 - 14) - (564) - (5610) - (65 - 10) - (150)$$

Here: 11, 6, 5 – are decisive modules, 17, main module, 11 and 17, 6 and 11, 5 and 6 – are interchangeable modules, 13, 30, -3, 14, -14, 4, 10, -10, 5, 0 – residue (discounts), (111730), (61114), (5610). (150) - are decisive module replacements.

1). $(6 \cdot 0 + 10): 5 = 2$
2). $(11 \cdot 2 + 14): 6 = 6$
3). $(17 \cdot 6 + 30): 11 = 12$

So: $x = 12$

Check:

$$11 \cdot 12 - 13 = 132 - 13 = 119: 17$$

Answer: $x \equiv 12 (mod \ 17)$

Now we will do some exercises related to using of theorem that mentioned above.

**Analysis and results**

**Finding integer solutions of some Diofant equations**

It is well known that finding the whole solution of equations is one of the most important and interesting issues of mathematics, in particular, the theory of numbers, Mathematicians Pythagoras (VI century BC) and Diofant (II century BC) were engaged with simples of these types exercises. Therefore, such equations are called «Diophantine equations». Many scientists have always wondered how to find a complete and rational solution to all coefficients. The classical mathematicians P. Ferma, L. Euler, J. L. Lagrange, K. F. Gauss, P. L. Chebisev and others were employed. Especially in this regard Yu. V. Nesterenko's work deserves admiration. [5, 10].

It should be noted that the Diofant equations have a great theoretical and practical significance. Many problems of physics and technology, many practical and economic problems are solved using the Diofant equations. Therefore, in recent years, such equations and exercises that solved by them have been incorporated into the curriculum of special schools and in the Olympics. From this point of view, learning and teaching of Diofant equations is one of the most important and actual issues of today.

There is no common way to solve such equations. It is very interesting to solve equations in integers. Since ancient times, many ways to solve certain Diophantine equations have been accumulated, but there are no common ways to test them. It was appeared only in our century. In particular, Russian mathematician Yu. V. Nesterenko outlined to find and solve the whole solution of the unknown equation in the form $ax + by + cz = d$ in his book Theory of Numbers using matrix. [5].

Exercise-9. $17x + 13y + 8z = 89$ find the integer solutions of equation.

Solving. $17x + 13y + 8z = 89$ we solve equation related to $z$:

$$z = 89 - 17x - 13y \equiv 0 (mod \ 8)$$

1). $89 - 17x - 13y \equiv 0 (mod \ 8)$. $x + 5y \equiv 1 (mod \ 8)$, $x + 5y = 1$, $y = \frac{8k - x + 9}{5}$

2). $8k - x + 9 \equiv 0 (mod \ 5)$ $k \equiv 2x + 2 (mod \ 5)$

Then, we find integer value of $y$ and $z$:

1). $k = 2x + 2 \rightarrow y = \frac{8(2x + 2) - x + 9}{5} = 3x + 5$, $y = 3x + 5$

2). $y = 3x + 5 \rightarrow z = \frac{89 - 17x - 13(3x + 5)}{8} = 3 - 7x$, $z = 3 - 7x$

Answer: $x, y = 3x + 5$, $z = 3 - 7x$ $(x \in Z)$.

Check: $x = 1, y = 8, z = -4$.

$17 \cdot 1 + 13 \cdot 8 + 8 \cdot (-4) = 17 + 104 - 32 = 89$.

Exercise-10. $3x + 5y - 7z + 11d = 36$ find solutions in integers.

Solving. Do linear replacements:

$$3x + 5y - 7z + 11d = 36 \quad 3x + 3y + 2y + 4z - 11z + 11d = 36$$

$$3(x + y) + 2(y + 2z) - 11(z - d) = 36$$

$$x + y = x_1$$
$$y + 2z = x_2 \rightarrow 3x_1 + 2x_2 - 11x_3 = 36$$
$$x_3 = z - d = x_3$$

$$\frac{3x_1 + 2x_2 - 36}{3}$$

$$\frac{11}{3} x_1 + 2x_2 - 36 \equiv 0 (mod \ 11) \quad 3x_1 + 2x_2 \equiv 36 (mod \ 11)$$

$$3x_1 + 2x_2 \equiv 3 \cdot 11 \equiv 3$$

$$x_1 = 14 - 2x_2 \equiv 0 (mod \ 3)$$

$$2x_2 \equiv 14 (mod \ 3) \quad x_2 \equiv 7 (mod \ 3)$$

$$x_2 = 7 \rightarrow x_1 = \frac{14 - 2 \cdot 7}{3} = 0$$

$$x_3 = \frac{3 \cdot 0 + 2 \cdot 7 - 36}{3} = 14 - 36 = -22$$

$$x = y$$
$$y + 2z = 7 \rightarrow x_2 = 7$$
$$z - d = x_3 = -2$$

Answer: $x = 2z - 7, y = 7 - 2z, z, d = 2 + z$

Check:

$z = 1$ →
Exercise-11. Find solutions of linear system of equations in integers.
\[
\begin{align*}
3x_1 - 2x_2 + 2x_3 + 2x_4 &= 19, \\
5x_1 + 6x_2 - x_3 + 3x_4 &= 23
\end{align*}
\]
Solving. Find the equation that links equations in a given system:
\[
\begin{align*}
3x_1 - 2x_2 + 2x_3 + 2x_4 &= 19, \\
5x_1 + 6x_2 - x_3 + 3x_4 &= 23 \\
10x_1 + 12x_2 - 2x_3 + 3x_4 &= 46
\end{align*}
\]
\[
\Rightarrow 13x_1 + 10x_2 + 8x_4 = 65
\]

13x_1 + 10x_2 + 8x_4 = 65 Solve the equation related to unknown x_4:

\[
x_4 = \frac{65 - 13x_1 - 10x_2}{8}
\]

1. 65 - 13x_1 - 10x_2 \equiv 0 (mod 8), \quad 13x_1 + 10x_2 \equiv 1 (mod 8),
\[
x_1 = \frac{8k - 10x_2 + 9}{13}, \quad k \equiv -2x_2 - 6 (mod 13) \Rightarrow k \equiv -2x_2 - 6
\]
Then, find integer values of x_1, x_2, and x_4:
\[
1) \quad k = -2x_2 - 6 \rightarrow x_1 = \frac{8(-2x_2 - 6) - 10x_2 + 9}{13} = -2x_2 - 3, \quad x_1 = -2x_2 - 3;
\]
\[
2) \quad x_1 = -2x_2 - 3 \rightarrow x_4 = \frac{65 - 13(-2x_2 - 3) - 10x_2}{8} = 2x_2 + 13, \quad x_4 = 2x_2 + 13
\]
\[
3) \quad x_1 = -2x_2 - 3, \quad x_2, \quad x_3 = 2x_2 + 1, \quad x_4 = 2x_2 + 13 \quad (x_2 \in Z).
\]
Check: x_1 = -3, \quad x_2 = 0, \quad x_3 = 1, \quad x_4 = 13
\[
\begin{align*}
3 \cdot (-3) & - 2 \cdot 0 + 2 \cdot 1 + 2 \cdot 13 = 19 \\
5 \cdot (-3) + 6 \cdot 0 - 1 \cdot 1 + 3 \cdot 13 &= 23
\end{align*}
\]

References:

1. Nazarov, R. N., Tashpolatov, B. T., & Doumbetov, A. D. (1995). «Algebra and number theory». Section II. (p.57, 70-72), TASHKENT: «TEACHER».
2. Yunusov, A., & Yunusova, D. (2007). A series of examples and exercises based on the module «Algebra and Number Theory». (pp.237-243), TASHKENT.
3. Allakov, I., & Usarov, B. O. (2017). Educational-methodical complex on the theory of numbers. (pp.12-15), Termez.
4. Vinogradov, I. M. (1995). «Fundamentals of the theory of numbers». Translation from the sixth Russian edition. (pp.50-53), Tashkent: «TEACHER».
5. Nesterenko, Y. V. (2008). «Theory of numbers». (pp.18-29), Moscow: Publishing Center «Academy».
6. Malik, D. S., Mordeson, J. N., & Sen, M. K. (1997). «Fundamentals of abstract algebra». (pp.12-13).
7. Usarov, B. O’. (2018). «Actual challenges of modern science». Collection of scientific papers. Issue 5 (25), Part 2. (pp.107-111), Ukraine.
8. Usarov, B. O’. (2019). «Modern problems of mathematics and informatics». Materials of Republican scientific-practical conference. Section II. (pp.49-53), Fergana.
9. Usarov, B. O’. (2019). «Actual problems of analysis and their application». Proceedings of the scientific conference. (pp.314-316), Qarshi.
10. Kurbanov, N. H. (2008). «Special algebraic problems». Tutorial. «The National Encyclopedia of Uzbekistan». (pp.39-41), Tashkent: State Scientific Publishing House.
11. Pogorelov, A. V. (1990). «Geometry». Textbook for High School Year 7-11. Seventh edition of the Russian edition of the eighth edition. Translation. (pp.209-211), TASHKENT: «TEACHER».