education sciences

MDPI

Article

Teaching Congruences in Connection with Diophantine Equations

Ďuriš Viliam [1], Gonda Dalibor [2,*], Tirpáková Anna [1,3] and Gabriela Pavlovičová [1]

[1] Department of Mathematics, Faculty of Natural Sciences, Constantine The Philosopher University in Nitra, Tr. A. Hlinku 1, 94901 Nitra, Slovakia; vduris@ukf.sk (Ď.V.); atirpakova@gmail.com (T.A.); gpavlovicova@ukf.sk (G.P.)

[2] Department of Mathematical Methods and Operations Research, Faculty of Management Science and Informatics, University of Žilina, Univerzitná 1, 01001 Žilina, Slovakia

[3] Department of School Education, Faculty of Humanities, Tomas Bata University in Zlín, Štefánikova 5670, 760 00 Zlín, Czech Republic

* Correspondence: dalibor.gonda@fri.uniza.sk; Tel.: +421-911-720-507

Abstract: The presented paper is devoted to the new teaching model of congruences of computer science students within the subject of discrete mathematics at universities. The main goal was to create a new model of teaching congruences on the basis of their connection with Diophantine equations and subsequently to verify the effectiveness and efficiency of the proposed model experimentally. The teaching of congruences was realized in two phases: acquisition of procedural knowledge and use of Diophantine equations to obtain conceptual knowledge of congruences. Experiments confirmed that conceptual understanding of congruences is positively related to increasing the procedural fluidity of congruence resolution. Research also demonstrated the suitability of using Diophantine equations to link congruences and equations. Among other things, the presented research has confirmed the justification of teaching mathematics in computer-oriented study programs.

Keywords: congruences; residual classes; cryptography; relational algebra; prime numbers; discrete mathematics; survey

check for updates

Citation: Viliam, Ď.; Dalibor, G.; Anna, T.; Pavlovičová, G. Teaching Congruences in Connection with Diophantine Equations. *Educ. Sci.* **2021**, *11*, 538. https://doi.org/10.3390/educsci11090538

Academic Editor: Miklos Hoffmann

Received: 30 July 2021
Accepted: 10 September 2021
Published: 14 September 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Society is currently being intensively digitized, and the ongoing COVID-19 pandemic has increased that need. With the transfer of work activities to the online space, the requirements for the security of virtual space are also increasing, which should also be ensured by high-quality encryption of the content of messages transmitted within the Internet networks. It is a challenge also for the field of education, which often faces criticism from the employers of school graduates themselves. Various employers claim that schools do not pay enough attention to understanding and developing the skills that graduates need to succeed outside school [1]. The World Economic Forum (2016) identified, among other things, the skills that students should have after completing their university studies. These are, for example, the ability to solve problems comprehensively, the ability to think critically, the ability to creatively use already acquired knowledge in various contexts and cognitive flexibility enabling insight into the problem to be solved from different perspectives. For these reasons, too, we consider it necessary to explore the possibilities of teaching mathematics with regard to the understanding and interconnection of individual knowledge. At the same time, it is necessary for students to gain experience in the diverse use of mathematics from the teaching of mathematics. According to Prawat [2], the assignment of diverse tasks is beneficial for the student, as necessary knowledge and skills are built up when the student has to deal with rich information and by resolving cognitive conflicts, instead of using ready-made algorithms to solve standard tasks. Applying knowledge in a variety of situations is a convenient way to combine the process of remembering and understanding. According to Marton et al. [3], it is necessary to combine these two processes in the

teaching mathematics. Research also suggested that practitioners draw on interdisciplinary knowledge in problem solving ([4–6]). Given the difficulty and complexity of the problems that need to be addressed today, interdisciplinary knowledge is a natural requirement for school leavers. The accelerated development of scientific knowledge creates a natural requirement and a precondition to manage the teaching process through interdisciplinary relationships [7]. For example, regarding machine learning, in addition to programming skills the solver of a real problem needs a relatively broad knowledge of various areas of mathematics.

The above-mentioned need for cyber security requires quality computer experts and computer scientists. Informatics and mathematics have really strong ties and a common history [8]. Mathematics provides a theoretical basis for many sub-areas of computer science. It also provides important analytical tools that computer scientists apply to specific computational problems. For example, the study of ciphers and the search for possibilities to break them has an incredibly large amount of synergy with mathematics [9]. This link between mathematics and computer science and practice could serve as a strong motivating factor for students to acquire the mathematical knowledge needed to understand the nature of encryption. The basic precondition for mastering the problem of encryption is the acquisition of knowledge in the field of congruences. When teaching students how to solve linear congruences, it might be useful to consider these congruences as analogous to equations [10]. To achieve this goal, Diophantine equations, which can also be solved using congruences, prove to be a suitable tool. According to [11] the development of quality procedural lessons in order to create basic procedural knowledge in conjunction with pointing out the basic concepts is a prerequisite for later improvement of procedural knowledge and gaining the necessary conceptual knowledge. The search for ways to combine the isolated requirements of professional subjects with a conceptual understanding of mathematical concepts or procedures could contribute to the streamlining of mathematical courses in non-mathematical study fields of universities. To understand professional problems, computer science students to a large extent need a conceptual understanding of the mathematical background of a given issue. On the basis of the above research objectives, the aim was to find out whether the connection of knowledge about congruences with the solution of Diophantine equations will increase the success of students in solving problems related to congruences. At the same time, we experimentally verified the assumption that improving procedural knowledge of congruences can support the improvement of conceptual knowledge of congruences.

2. Cryptography and Congruences

The problem of encrypting a message so that the enemy does not understand it and the ally can decrypt it again has been important since ancient times. It is known that Gaius Julius Caesar already used a simple code in which each letter was replaced by a different one found in the Latin alphabet "three places further", i.e., $A \to D$, $B \to E$, $C \to F$, etc. Important mathematicians took part in solving codes. For example, François Viète (1540–1603) deciphered the code used by Spanish troops in France. During World War II, the Germans used an encryption machine called ENIGMA. The breaking of this code by a group of British correspondents led by Alan Turing [12] was essential for the Allied victory in the North Atlantic, where German submarines threatened the convoys of Allied ships. In the Pacific, the decipherment of the Japanese code before the Battle of Midway Roundtable brought the Americans a great advantage when they managed to sink four Japanese aircraft carriers and lost only one themselves.

It can be said that until the early 1970s, cryptography was more or less a military matter and not much was published about the theory of coding. However, the civilian, commercial and banking sphere began to make more and more use of wireless data transmission, which could also be "sensitive". Therefore, there arose the need to find a simple cryptographic algorithm used for secure and fast data transmission. In November 1976, it was formally adopted in the USA as a federal standard called DES (Digital Encryption Standard) [13]. It

was a cryptographic system with a secret key, where any two users had to exchange this key before they could exchange encrypted messages. The encrypted message was very difficult to decipher for those who did not know the key.

In 1976, Diffie and Hellman proposed a fundamentally new method using the so-called public key for encryption systems. However, the system also has a secret key, and only those who know it are able to easily decrypt the text encrypted with the public key. The implementation of this system was proposed by Rivest, Shamir and Adleman (a so-called RSA system) [14]. This method is related to the issue of electronic signatures or trading on the Internet. It is based on the mathematical apparatus (factorization) of natural numbers into powers of prime numbers. It is an encryption in which each of its principles is known and is public, but no one decrypts the encrypted information, because the public key only (i.e., knowledge of the encryption principle) is not enough. To decipher the cipher and read the message, it is necessary to obtain prime number elements of prime factorization that can only be obtained by the recipient of the message who also knows the private key (that is, some necessary information on how the product originated). One of the first standards was RSA-768 [15], which represents a 232-digit number. The standard has been broken by scientists by bringing together hundreds of computers that have been working for a period representing 2000 years of one computers work. Later, the RSA-1024, RSA-2048 or RSA-4096 standards have been developed which are used today. The use of linear congruences for coding problems stems from knowledge from the 18th century, which has started to be used practically now in the 20th century.

Thus, we can easily algorithmically decompose only numbers of a certain "small" size into the product of prime numbers and this fact is the basis of virtual security. If we take two very large prime numbers, where both the first and the second represent some information, it is easy to multiply them with each other, giving a very large composite number practically decomposable (unless we know the so-called private key, i.e., some necessary information how the large number came up). Algorithms that would look for the factors of a product by "brute force", i.e., by trying all possibilities, would have a tremendous time complexity [16]. The principle of coding a given message x using the RSA method is that we take two large primes p and q, which mutually different such that $x < p{\cdot}q$ and $p \nmid x$, $q \nmid x$. We create their product $p{\cdot}q$, which is publicly accessible. However, only one who knows both primes p and q can easily calculate the value of the Euler function $\varphi(p{\cdot}q) = (p-1)(q-1)$. For those who do not know from which primes the product originated, it is very difficult to calculate the value of $\varphi(p{\cdot}q)$ because the decomposition of the large number which originated as a product of prime numbers is demanding. Now we choose any number e, incommensurable with $\varphi(p{\cdot}q)$, except $e = 1$ and $e = (p-1)(q-1) - 1$. This number, a so-called encryption exponent, shall also be disclosed. Anyone who knows the numbers $p{\cdot}q$ and e can encrypt their message by calculating the number y for which $y \equiv x^e (\text{mod } p{\cdot}q)$ holds true. The author of the message must calculate the so-called decoding exponent f, presented by a private key. It can be found as a solution of the congruence $e{\cdot}f \equiv 1(\text{mod } \varphi(p{\cdot}q))$. It holds true that $(e, \varphi(p{\cdot}q)) = 1$ and the search for the number f is performed by Euclid's algorithm [17], so there exist integers f, h such that $e{\cdot}f + \varphi(p{\cdot}q){\cdot}h = 1$. Then, $e{\cdot}f = 1 - \varphi(p{\cdot}q){\cdot}h$ and thus $e{\cdot}f - 1$ is divisible by $\varphi(p{\cdot}q)$ and $e{\cdot}f \equiv 1(\text{mod } \varphi(p{\cdot}q))$. The decryption of the encoded word y consists of the following steps. We know that $e{\cdot}f = 1 - \varphi(p{\cdot}q){\cdot}h$. Let $k = -h$, then $e{\cdot}f = 1 + \varphi(p{\cdot}q){\cdot}k$. As $(x, p{\cdot}q) = 1$, then according to Euler's theorem [18],

$$x^{\varphi(p\cdot q)} \equiv 1(\text{mod } p{\cdot}q), \tag{1}$$

and also

$$x^{k\cdot\varphi(p\cdot q)} = \left(x^{\varphi(p\cdot q)}\right)^k \equiv 1(\text{mod } p{\cdot}q), \tag{2}$$

then

$$y^f = x^{e\cdot f} = x{\cdot}x^{k\cdot\varphi(p\cdot q)} \equiv x(\text{mod } p{\cdot}q). \tag{3}$$

The last relation describes that in order to decrypt the encoded word y, it is sufficient to calculate the smallest non-negative remainder by dividing the power y^f by the number $p{\cdot}q$, which is an easily solvable task. The RSA method is the simplest one and it shows how modular arithmetic has a practical application. The RSA method has become very widespread in e-banking, online shopping, electronic signatures, etc. [19].

We will show the RSA encryption principle using the congruences on a specific example. We will encrypt (and decrypt) the name (message) "REX" by RSA method using prime numbers $p = 7$, $q = 11$. We will work with the letters of English alphabet, A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, and Z, assigning each letter a numeric two-digit number, sequentially to letter A—01, to letter B—02 etc. to letter Z—26.

Then the word "REX" in numeric form will presented by number $x = 180524$. Now, we will encrypt letter by letter. The product $p{\cdot}q = 77$, hence $\varphi(p{\cdot}q) = \varphi(77) = 77{\cdot}\left(1-\frac{1}{7}\right){\cdot}\left(1-\frac{1}{11}\right) = 77{\cdot}\frac{6}{7}{\cdot}\frac{10}{11} = 6{\cdot}10 = 60$ [20]. Let us choose, e.g., $e = 43$ as the encryption exponent so that $\gcd(60, 43) = 1$. Now we have to calculate the number f that $e{\cdot}f \equiv 1(\text{mod } 60)$. Using the Euclidean algorithm, we get $60 = 43{\cdot}1 + 17$, $43 = 17{\cdot}2 + 9$, $17 = 9{\cdot}1 + 8$ a $9 = 8{\cdot}1 + 1$. Next $\gcd(60, 43) = 1 = 9 - 8 = 9 - (17 - 9) = 17{\cdot}(-1) + 9{\cdot}2 = 17{\cdot}(-1) + (43 - 17{\cdot}2){\cdot}2 = 43{\cdot}2 + 17{\cdot}(-5) = 43{\cdot}2 + (60 - 43){\cdot}(-5) = 60{\cdot}(-5) + 43{\cdot}7$. From that we see $43{\cdot}7 = 1 + 60{\cdot}5$, and therefore $43{\cdot}7 \equiv 1(\text{mod } 60)$. Then the decryption exponent is $f = 7$.

As we encrypt letter by letter, we now have to calculate the numbers y such that $y \equiv a^{43}(\text{mod } 77)$ (resp. we solve the Diophantine equation $-77x + y = a^{43}$, because $77|y - a^{43} \Rightarrow y - a^{43} = 77x$) sequentially for $a = 18,\ 5,\ 24$. Now we calculate $y \equiv 18^{43}$ $(\text{mod } 77)$, so we're searching such y that belong to the same residual class as the number 18^{43} modulo 77. It holds $18^{43} = 18{\cdot}18^{42} = 18{\cdot}\left(18^6\right)^7 \equiv 18{\cdot}15^7 = 270{\cdot}15^6 = 270{\cdot}\left(15^3\right)^2 \equiv 270{\cdot}64^2 \equiv 46(\text{mod } 77)$. Analogously from congruences $y \equiv 5^{43}(\text{mod } 77)$ and $y \equiv 24^{43}(\text{mod } 77)$ we get the remaining values 26 and 52 for y. To decrypt the message back with the private key $f = 7$ letter by letter, we first calculate the congruence $x \equiv 46^7(\text{mod } 77)$ and we get $x = 18$, which represents the letter R. The same way we calculate the remaining two congruences $x \equiv 26^7(\text{mod } 77)$ and $x \equiv 52^7(\text{mod } 77)$. The results obtained are shown in Table 1.

Table 1. RSA encryption principle.

Message from Sender	x	y Encrypted Message	Decrypted Message	Message at the Recipient
R	18	**46**	18	**R**
E	5	**26**	5	**E**
X	24	**52**	24	**X**

More information on RSA cryptosystems using congruences can be found, e.g., in [21].

3. Results

Consider $a, b, m \in \mathbb{Z}$, while $m > 1$. Then we say that number a is congruent with number b by module m (or we call it modulo m), if $m|(a - b)$. Additionally, we note

$$a \equiv b(\text{mod } m). \tag{4}$$

The number a is called the left side, the number b the right side of congruence. The notation $ab(\text{mod } m)$ means that the number a is not congruent with number b by module m., i.e., $m \nmid (a - b)$ [22].

The relation of congruence is:

1. reflex: $a \equiv a(\text{mod } m)$
2. symmetric: $a \equiv b(\text{mod } m) \Rightarrow b \equiv a(\text{mod } m)$

3. transitive: $a \equiv b(\text{mod } m) \wedge b \equiv c(\text{mod } m) \Rightarrow a \equiv c(\text{mod } m)$

Now we show that if $a + b \equiv c(\text{mod } m)$ and $a \equiv d(\text{mod } m)$, then $d + b \equiv c(\text{mod } m)$. From $a + b \equiv c(\text{mod } m)$ it applies $m|a + b - c$ and from $a \equiv d(\text{mod } m)$ it applies $m|a - d$. Then $a + b - c = k_1 m$ and $a - d = k_2 m$, thus $d - a = -k_2 m$. Then $a + b - c + d - a = k_1 m - k_2 m$, and therefore $d + b - c = (k_1 - k_2)m$. Out of previous $d + b \equiv c(\text{mod } m)$.

Furthermore, if $a \equiv b(\text{mod } m)$ and c is any integer, then:

$$a + c \equiv b + c(\text{mod } m). \tag{5}$$

Because if $a \equiv b(\text{mod } m)$, then $m|(a - b)$. As $(a + c) - (b + c) = a - b$, then $m|[(a + c) - (b + c)]$, out of which $a + c \equiv b + c(\text{mod } m)$.

Now consider the congruence system:

$$(\text{mod } m)a_2 \equiv b_2(\text{mod } m) \cdots a_k \equiv b_k(\text{mod } m) \tag{6}$$

Then $a_1 a_2 \ldots a_k \equiv b_1 b_2 \ldots b_k(\text{mod } m)$. The formula can be proved by mathematical induction. First let $k = 2$. Then we must show that $a_1 a_2 \equiv b_1 b_2(\text{mod } m)$. Let us denote $M = a_1 a_2 - b_1 b_2 = a_1 a_2 - a_1 b_2 + a_1 b_2 - b_1 b_2 = a_1(a_2 - b_2) + b_2(a_1 - b_1)$. From the assumptions of the first and second congruence the following applies $m|(a_1 - b_1)$ and $m|(a_2 - b_2)$, and thus $m|M$. The second step is analogous.

From the last statement we can deduce the result that if $a \equiv b(\text{mod } m)$ and c is any integer, then:

$$ac \equiv bc(\text{mod } m). \tag{7}$$

Next, let $a \equiv b(\text{mod } m)$. Let d be an integer with properties $d|a$, $d|b$, $(d, m) = 1$. Then:

$$\frac{a}{d} \equiv \frac{b}{d}(\text{mod } m). \tag{8}$$

To prove the validity of this formula, let us denote $a = a_1 d$, $b = b_1 d$. Based on the assumption $m|(a - b)$, it is valid that $m|d(a_1 - b_1)$. As $(d, m) = 1$, it is valid that $m|(a_1 - b_1)$. Then $a_1 \equiv b_1(\text{mod } m)$, thus $\frac{a}{d} \equiv \frac{b}{d}(\text{mod } m)$.

Again, let $a \equiv b(\text{mod } m)$ and $d > 0$ be a common divisor of numbers a, b, m. Then:

$$\frac{a}{d} \equiv \frac{b}{d}\left(\text{mod } \frac{m}{d}\right). \tag{9}$$

If it is true that $a \equiv b(\text{mod } m)$, then there is such an integer c, that $a - b = mc$. After dividing by number d we get $\frac{a}{d} - \frac{b}{d} = \frac{m}{d}c$, which means that $\frac{m}{d}\left|\left(\frac{a}{d} - \frac{b}{d}\right)\right.$, and thus $\frac{a}{d} \equiv \frac{b}{d}(\text{mod } \frac{m}{d})$.

Next consider any natural number $m > 1$. According to the division with remainder theorem [23], we can write every integer n in the form:

$$n = m{\cdot}q + r,\ 0 \leq r < m \tag{10}$$

While the number r is called the remainder of division of the number n by number m. Now let us decompose the set $\mathbb{Z}$ to subsets $R_0(m)$, $R_1(m), \ldots, R_{m-1}(m)$ in such a way that R_i is the set of all those integers whose remainder after dividing by a number m is i.

Then the sets $R_i(m)$ are called the residual classes according to a module (or we talk about modulo) m. The residual classes are disjoint by pairs and each integer belongs to one of them. At the same time the set $R_i(m)$ is a set of all integers x, to which it applies that $x \equiv i(\text{mod } m)$. If modulo is known, we simply refer R_i instead of $R_i(m)$.

Integers a and b belong to the same modulo class m if and only if $a \equiv b$ (mod m). We can prove the validity of the statement from both sides.

I. Let us express the numbers $a,\ b \in\ R_i$ in the form:

$$a = m{\cdot}q + i,\ b = m \cdot p + i. \tag{11}$$

Then $a - b = m(q - p)$, i.e., $m|a - b$, and then $a \equiv b(\text{mod } m)$.

II. Now let $a \equiv b \ (\text{mod } m)$ and $a = mq + i$, $b = mp + j$ $(0 \leq i,\ j < m)$. Suppose for example that $i > j$. As $a \equiv b \ (\text{mod } m)$, then $m|a - b$. However, then $m|(a - b) = [m(q - p) + (i - j)]$, out of which $m|(i - j)$, but that is a contradiction because $0 < i - j < m$. Similarly, a contradiction arises from the assumption $i < j$. It must therefore apply $i = j$, and then numbers a a b belong to the same residual class.

The m-tuple of numbers $x_0, \ldots, x_{m-1}$ is called a complete residual modulo system m, if $x_i \in R_i$ for $i = 0, \ldots, m - 1$. We say that the residual class R_i by module m is reduced if $(i,\ m) = 1$. For example, the residual class R_2 is reduced modulo 7, because $(2,\ 7) = 1$. The class R_0 it is not reduced by any module.

If R_i is a reduced residual class modulo m, then for any $x \in R_i$ it applies $(x, m) = 1$. Because it is valid that $x \equiv i(\text{mod } m)$, thus $m|(x - i)$, and therefore there exists such an integer c that $x - i = mc$, thus $x - mc = i$. Then every common divisor of numbers x and m would also be a divisor of number i, and thus the common divisor of i and m. However, as $(i,\ m) = 1$, it is valid that $(x, m) = 1$.

There exist $\varphi(m)$ reduced residual classes of modulo m [23]. We say that $\varphi(m)$-tuple of numbers $y_1, \ldots, y_{\varphi(m)}$ forms a reduced residual modulo system m if numbers y_i are selected one by one from the reduced residual classes. The elements of the reduced system are coprime with m. The reduced residual system can be obtained by omitting numbers that are commensurable with the module, from the complete. E.g., if $m = 8$. The complete residual system consists e.g., of numbers $0,\ 1,\ 2,\ 3,\ 4,\ 5, 6, 7$. We will choose $0,\ 2,\ 4\ 6$ from those because they are commensurable with m, so we get a reduced residual system of 1,3,5,7. It is valid that $\varphi(8) = 8\left(1 - \frac{1}{2}\right) = 4$.

Generally, all non-negative numbers less than m coprime with m form the smallest non-negative reduced residual system.

If $y_1, \ldots, y_{\varphi(m)}$ is a reduced residual system modulo m and $(m,\ c) = 1$, then $cy_1, \ldots, cy_{\varphi(m)}$ is a reduced residual system too, by module m. Numbers $y_1, \ldots, y_{\varphi(m)}$ belong to different residual classes and the same can be said of numbers $cy_1, \ldots, cy_{\varphi(m)}$ because of congruence $cy_i \equiv cy_j(\text{mod } m)$ under the condition $(m, c) = 1$ the following results:

$$y_i \equiv y_j(\text{mod } m). \tag{12}$$

The count of numbers cy_i is $\varphi(m)$ while $(cy_i,\ m) = 1$. It means the numbers cy_i are selected one by one out of the reduced residual classes.

Let $x_1, \ldots, x_{\varphi(m)}$ and $y_1, \ldots, y_{\varphi(m)}$ are any reduced residual systems modulo m. Then

$$x_1 \ldots x_{\varphi(m)} \equiv y_1 \ldots y_{\varphi(m)} \ (\text{mod } m). \tag{13}$$

Each x_i is congruent with just one y_j because both groups are selected one by one from the reduced classes. Additionally, the evidence then results directly from the properties of the congruences, while if:

$$a_1 \equiv b_1(\text{mod } m) a_2 \equiv b_2(\text{mod } m) \cdots a_k \equiv b_k(\text{mod } m) \tag{14}$$

then $a_1 a_2 \ldots a_k \equiv b_1 b_2 \ldots b_k(\text{mod } m)$.

A linear congruence with one unknown is a congruence in the form:

$$ax \equiv b \ (\text{mod } m). \tag{15}$$

The solution of linear congruence is such a residual class $R_i(m)$ that $m|(ax - b)$ applies. A congruence is called solvable if it has at least one solution.

Congruence $ax \equiv b \ (\text{mod } m)$ can also be written in the form:

$$ax = b + my, \tag{16}$$

which actually gives a linear Diophantine equation with two unknowns [17].

A linear congruence $ax \equiv b \pmod{m}$ is solvable if and only if $(a, m)|b$. If module m and coefficient a are coprime, then linear congruence is always solvable and the elements of one residual class are the solution.

Let $y \in \mathbb{Z}$ is a solution to congruence $ax \equiv b \pmod{m}$ and let $y \in R_i(m)$. Then all the elements of the set R_i are a solution to congruence $ax \equiv b \pmod{m}$. Thus, a solvable linear congruence has infinitely many solutions. This follows directly from the basic properties of congruences and residual classes. If $z \in R_i$, then $z \equiv y(\text{mod } m)$ and $az \equiv ay \equiv b(\text{mod } m)$.

If $(a, m)|b$, then congruence $ax \equiv b \pmod{m}$ has just (a, m) mutually non-congruent (or we talk about incongruent) solutions. Let us denote $d = (a, m)$, $z = \frac{m}{d}$. Let y is such a congruence solution $ax \equiv b \pmod{m}$ to which it applies $0 \leq y < m$. Additionally, let us examine numbers that are in the form:

$$y + zs, \text{ where } s = 0, 1, \ldots, d - 1. \tag{17}$$

These numbers are congruent $ax \equiv b \pmod{m}$ because it is true that $a(y + zs) = ay + a\frac{m}{d}s \equiv b(\text{mod } m)$ because $\frac{a}{d}s$ is an integer, and thus $a\frac{m}{d}s$ is a multiple of the number m. Now we indirectly prove that the numbers $y + zs$ are non-congruent with each other according to modulo m. Suppose:

$$y + zs_1 \equiv y + zs_2(\text{mod } m). \tag{18}$$

From this, based on common congruence simplifications, we get:

$$s_1 \equiv s_2(\text{mod } m), \tag{19}$$

which is not possible, because $s_1 \neq s_2$ while $0 \leq s_1,\ s_2 < m$. Vice versa, if u and v are different solutions to congruence $x \equiv b \pmod{m}$, then the following applies:

$$au \equiv av(\text{mod } m). \tag{20}$$

Then:

$$\frac{a}{d}u \equiv \frac{a}{d}v\left(\text{mod}\frac{m}{d}\right).$$

As $\left(\frac{a}{d}, \frac{m}{d}\right) = 1$, it is valid that:

$$u \equiv v\left(\text{mod } \frac{m}{d}\right). \tag{21}$$

So, all solutions of congruence $ax \equiv b \pmod{m}$ that belong to the interval $\langle 0,\ m - 1\rangle$ are congruent with y by module $\frac{m}{d}$ and are in form of $ax \equiv b \pmod{m}$ and all remaining solutions are congruent with some of the solutions.

A linear congruence can also be solved using Euler's theorem [18]. If we have a congruence $ax \equiv b \pmod{m}$ where $(a,\ m) = 1$, then the number

$$a^{\varphi(m)-1}b \tag{22}$$

is one of its solutions. Because it is true that $a\left(a^{\varphi(m)-1}b\right) = a^{\varphi(m)}b \equiv b(\text{mod } m)$.

4. Research Methodology

The research was carried out at a selected university in the Slovak Republic with the knowledge and consent of the faculty management. Before the start of the research, all students of the 1st year of bachelor's study in computer science study fields were addressed. A total of 38 students volunteered for the research. All participants in the research were informed about the anonymity of the obtained data. The methodological research is based on the claims of Dahlin and Watkins [24], according to which the connecting point between memorization and comprehension is meaningful repetition. Meaningful repetition creates

a deep impression, which leads to memorization and can also lead to the "discovery of a new meaning", which leads to understanding [25]. Therefore, we divided the teaching of congruences into two phases (Figure 1):

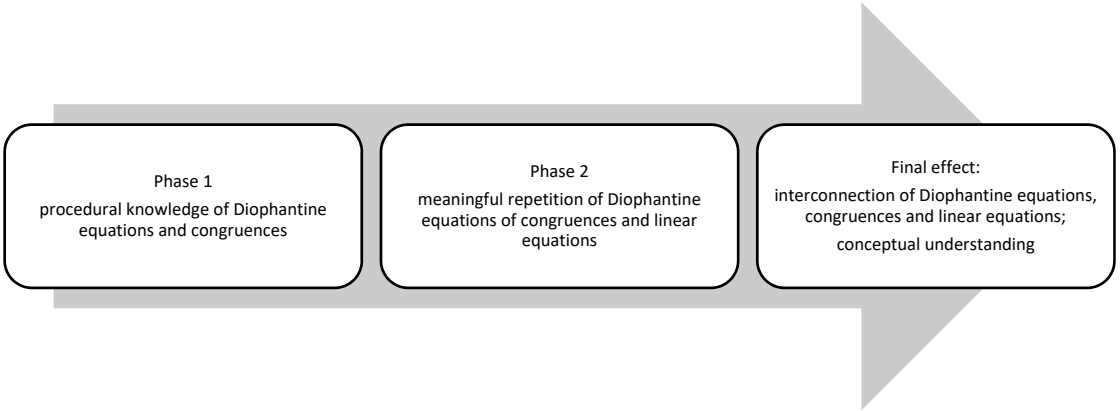

Figure 1. Scheme of teaching congruences.

Phase 1—teaching congruences with a focus on the development of procedural knowledge about congruences, Phase 2—"meaningful repetition" of congruences in order to create a conceptual understanding of the concept of congruence in students. This division is theoretically based on the finding that improving procedural knowledge can support the improvement of conceptual knowledge. Evidence comes from studies of carefully constructed practical problems [26–29]. We used the solution of Diophantine equations in the second phase as a "tool" to connect between congruences and linear equations. According to [30], this connection is very important for the successful solution of congruences.

In the first phase of the research, students completed a seminar on mathematics consisting of two parts: (a) solving Diophantine equations, and (b) congruences. The seminar was realized in the form of full-time teaching. In this phase, students became acquainted with the basic algorithm for solving Diophantine equations. We solved linear Diophantine equations with two unknowns in the form $ax + by = c$, $a,\ b \neq 0$, while explaining the algorithmic solution procedure. As the solution procedure required knowledge of the Euclidean algorithm, this was taken over separately [31]. Subsequently, they adopted the concept of "congruence" and their basic properties. Then simple congruences (equations on the set Z_n) were solved. Within the curriculum of congruences, we first took over the basic properties of congruences and the basic theorems for working with congruences. We have separately explained the residual classes and definitions as a complete or reduced residual system. We have defined a linear congruence with one unknown in the form $ax \equiv b \pmod{m}$ and showed an algorithm for its solution. We explained conditions for solvable congruence and what congruent and incongruent solutions mean (Section 3, part Equations (15)–(22)). The same time was devoted to both parts of the seminar. After completing the seminar, a pre-test was carried out, in which tasks from both parts of the seminar were equally represented (two tasks from each thematic area). Students had 60 min to solve the four tasks. We asked students to measure the real time they needed to solve each task in addition to solving the given tasks. In the second phase of the research, after passing the pre-test, the same students completed another part of the mathematics seminar, where attention was paid to the connection between congruences and Diophantine equations. In this part of the seminar, students were introduced to the method of using congruences to solve Diophantine equations (Section 3, Equation (16)). This can be considered a meaningful repetition in order to link the solution of congruences with the solution of equations. Thus, students can use already acquired algebraic knowledge and skills in solving congruences. After the second part of the mathematics seminar, students completed a post-test, which included two problems to be solved by Diophantine equations

and two problems for congruences (as in the pre-test). In addition to solving the problems, they also recorded the time needed for solving.

We sought answers to the following research hypotheses by content analysis of respondents work and statistical analysis of respondents success in pre-test and post-test:

Hypothesis (H1): *Linking congruences with the solution of Diophantine equations and linear equations will increase the success of students in solving congruences.*

Hypothesis (H2): *Conceptual understanding of congruences will reduce students' time to solve congruent problems.*

5. Research Results

5.1. Analysis of the Success of Respondents in Solving Tasks

The results (number of points) that the students achieved in the pre-test and in the post-test are shown in Figure 2.

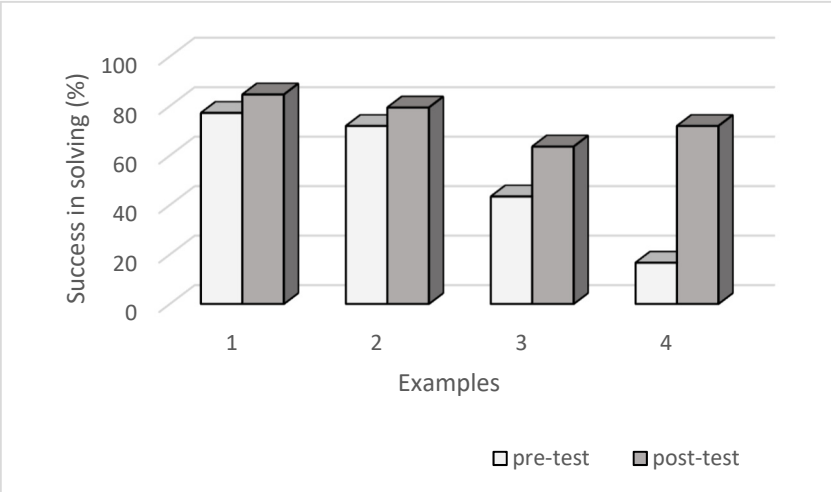

Figure 2. Success of solving assigned tasks in pre-test and post-test (number of points).

In Figure 2 we can see that the students in the pre-test and in the post-test achieved different results (number of points). We wondered if these differences were also statistically significant. A parametric paired t-test can be used to verify the statistical significance of the differences between the two tests in the results obtained. A prerequisite for its correct use is the fulfillment of the assumption of a normal distribution of the observed feature. In our case, we verified the assumption of a normal distribution of both sets by the Shapiro–Wilk test.

As the assumption of a normal distribution of observed traits is not substantiated, we used the nonparametric Wilcoxon signed rank test, which is a nonparametric analogy of a paired parametric t-test, to verify the statistical significance of differences in the level of observed traits.

In our case, the observed characters were X, Y, where X is the number of points that students gained in the pre-test and Y is the number of points that students gained in the post-test. Because we assume that students received higher scores in the post-test, in this case we will use the one-sided Wilcoxon test. We tested hypothesis H_0: the medians X, Y are equal to the one-sided alternative hypothesis H_1 that the median Y is greater. We implemented the test in the STATISTICA program. After entering the input data, we got the following results into the output set of the computer: the value of the test criterion of the one-sample Wilcoxon test (Z = 5.373) and the value of the probability p (p = 0.000). We evaluated the test using the value of p (p is the probability of an error we make when we reject the tested hypothesis). If the calculated value of the probability p is sufficiently small

($p < 0.05$ or $p < 0.01$), we reject the tested hypothesis (at the significance level 0.05 or 0.01). As the calculated value of the probability $p < 0.01$, at the level of significance $\alpha = 0.01$ we reject the tested hypothesis H_0. This means that by taking over or by supplementing the curriculum focused on the relationship between Diophantine equations and congruences in the optional seed, the level of students' knowledge in the field of congruences increased statistically significantly.

Subsequently, we were interested in whether knowledge in solving problems in the field of congruences statistically significantly improved, and also whether it improved for Diophantine equations. For this reason, we verified the statistical significance of the differences in the success of solving each of the four pre-test and post-test tasks by using the Wilcoxon one-sample test. The obtained results are clearly recorded in Table 2.

Table 2. Wilcoxon signed rank test (success in pre-test and post-test).

Problem	*Z*	*p*-Value
1	2.950	0.003 *
2	2.094	0.036 *
3	4.372	0.000 *
4	5.232	0.000 *

Note. Statistically significant values are marked with an asterisk in the table.

The results of the test showed that in all four tasks, students achieved a statistically significantly higher success rate in the post-test than in the pre-test. This confirmed the validity of the research Hypothesis (H1).

5.2. Analysis of the Length of Time Required to Solve Tasks

Average number of minutes that the students needed in the pre-test and in the post-test are shown in Figure 3.

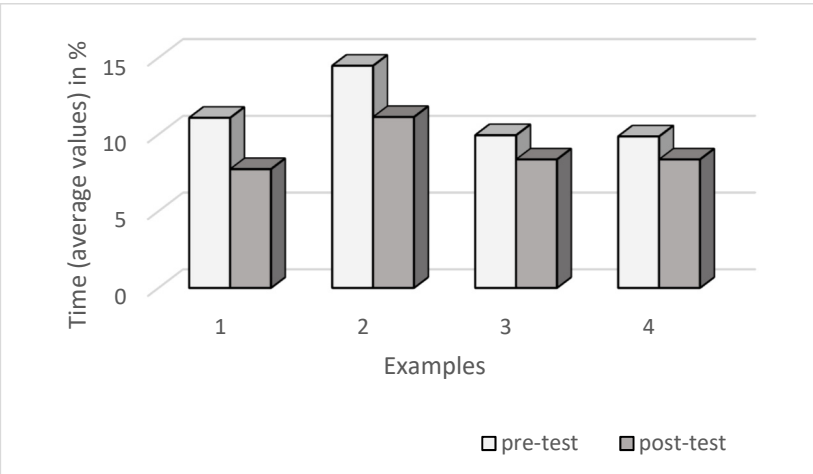

Figure 3. Average time of solving assigned problems in pre-test and post-test (in minutes).

In Figure 3 we can see that there are differences between the average time that students needed to solve the problems in pre-test in post-test. We also verified whether these differences are statistically significant in the case of using the Wilcoxon signed rank test. We proceeded analogously as in the previous case—when analyzing the success of solving problems in the pre-test and post-test. We calculated the value of the single-sample Wilcoxon test criterion ($Z = 4.839$) and the probability value p ($p = 0.000$). We also evaluated the test when using the value of the probability p. As the calculated value of the probability $p < 0.01$, at the level of significance $\alpha = 0.01$ we reject the tested hypothesis H_0. This means that by teaching the curriculum focused on the relationship between Diophantine equations

and congruences in the selective seminar, the time that students needed in the post-test to solve problems was statistically significantly reduced.

Subsequently, we were interested in whether time decreased statistically significantly not only in solving problems in the field of congruences but also Diophantine equations. For this reason, we used the Wilcoxon single-sample test to verify the statistical significance of the differences in time that students needed to solve each of the 4 pre-test and post-test problems. The obtained results are clearly recorded in Table 3.

Table 3. Wilcoxon signed rank test (time required to solve pre-test and post-test tasks).

Problem	*Z*	*p*-Value
1	4.022	0.000 *
2	3.456	0.001 *
3	2.187	0.029 *
4	2.113	0.035 *

Note. Statistically significant values are marked with an asterisk in the table.

The results of the test showed that in all four problems, students achieved a statistically significantly shorter time in the post-test than in the pre-test. In other words, the difference between the time that students needed to solve a given problem (each) in the post-test is statistically significantly shorter than the students needed to solve an adequate problem in the pre-test. This confirmed the validity of the research Hypothesis (H2).

6. Discussion

In the pre-test, which followed the first phase of teaching congruences, students recorded very low success in solving problems focused on congruences (success rate was 43% or 17%). Congruences were a new concept for them and, according to students, it was an isolated concept for them (72% of students). Isolated knowledge leads to the acquisition of skills without understanding [32]. The solution of congruences was for them a "branched" algorithm, the memory of which caused them problems. This was evidenced by the large number of unresolved problems. Our findings confirmed the fact that learning new concepts is difficult for students if there is no network of previously learned concepts and skills with which to combine a new topic [33]. Despite sufficient time to solve the pre-test, the students were unable to reconstruct the insufficiently memorized algorithm. This indicates their focus on acquiring procedural skills without understanding the individual steps of the algorithm [34]. However, a conceptual understanding of a new concept is also necessary for the successful solution of problems, and this requires the connection of new knowledge with already acquired knowledge [35]. In our case.

There is a need to link the concept of "congruence" with knowledge of equations and their solutions. Based on the results of the pre-test, students did not find this connection. The same conclusion was found out by [36], according to who university students in the USA, future teachers of mathematics did not find linear congruences analogous to equations. The high success of students in the pre-test in solving Diophantine equations was probably conditioned by the existing connection with the term "equation" and students learned a new algorithm for solving another type of equation. It is also evidenced by the fact that some students solved Diophantine equations by choosing one unknown as a parameter and then expressing the other unknown depending on the value of the parameter. In rare cases, we also recorded a solution by trial and error. When solving Diophantine equations, students showed faith in their own ability to solve the equation, because they could use their already acquired knowledge and skills in solving equations. In solving the congruences, the students relied on the limited possibilities of the memorized "branched" algorithm. In the post-test, the students were divided into two groups for Diophantine equations. One group of students (mainly those students who successfully solved both problems on Diophantine equations in the pre-test) did not use congruence to

solve a simpler problem. They preferred the already "proven" way of solving Diophantine equations. This approach of students corresponds to the knowledge that when students learn a new, more effective procedure, they do not always abandon the old procedure. Instead, they use either the old procedure or the new one, depending on the situation. Only with time and practice they stop using fewer effective methods [37,38]. In the second (more complex) problem, they considered a method of solution—to use or not to use congruences. According to their own statements, they considered which of the procedures would lead to the result in a shorter way. In determining how to use as few computational steps as possible, students analyzed the problem, demonstrating the ability to think of higher order [39]. These students mastered the solution of congruences at a higher level of knowledge, such as understanding, because they were able to evaluate the suitability of using congruences to solve a given problem [40]. The second group (most students) solved Diophantine equations using congruences, i.e., they evaluated the use of congruences as a more efficient way of solving Diophantine equations. Replacing learned practices with new more effective solutions are part of the development of strategic skills [33]. This group of students was also more successful in solving congruences. Overall, in the post-test, the success of students in solving congruences increased significantly, mainly due to their connection with the solution of equations. The number of unresolved tasks decreased significantly.

In the post-test, there was also a statistically significant decrease in the time that students needed to solve particular problems, which indicates an increase in the procedural fluency of the use of learned algorithms. Procedural fluency is the ability to flexibly, accurately, and efficiently perform learned problem-solving procedures (mostly algorithms) in conjunction with the ability to assess the appropriateness of using a given procedure [33]. Students will acquire procedural fluency in the use of their strategic abilities to choose between effective procedures. This finding indicates an increase in the conceptual understanding of the concept of "congruence" and also an understanding of the algorithm for solving congruences. According to [41], experience in solving diverse problems using developed procedural fluency in conjunction with experience in solving problems help students gain new conceptual knowledge. The flexibility of procedural knowledge is positively related to conceptual knowledge [42].

7. Conclusions

To understand professional problems, computer science students need a conceptual understanding of the mathematical background of a given issue. This mathematical knowledge is often far removed from the mathematical knowledge that students acquired in previous mathematical education. In such a case, the teacher faces the problem of how to present the new subject to students, because conceptual understanding requires the connection of new knowledge with already acquired knowledge. Based on the results of our research, one of the possible ways is to divide teaching into two phases. First, to create an isolated island of procedural skills related to the subject matter and then, by "meaningful" repetition, to create a link between the new and the already acquired, thus ensuring the necessary conceptual understanding. In teaching congruences, we confirmed that Diophantine equations are a suitable tool to support the development of conceptual understanding of congruences. A certain degree of acquisition of procedural skills in solving congruences, which students acquired in the first phase of the seminar, was a suitable springboard for the use of congruences in solving equations. The search for similar possibilities to connect the isolated requirements of professional subjects for the conceptual understanding of mathematical concepts or procedures could contribute to the streamlining of mathematical courses in non-mathematical study fields of universities.

Author Contributions: Conceptualization, Ď.V. and G.D.; methodology, G.P.; software, Ď.V.; validation, T.A.; formal analysis, T.A.; investigation, G.P.; resources, G.D.; data curation, Ď.V.; writing—original draft preparation, Ď.V.; writing—review and editing, G.D.; visualization, Ď.V.; supervision, T.A.; project administration, T.A.; funding acquisition, Ď.V. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. English, L.D. Promoting interdisciplinarity through mathematical modelling. *ZDM* **2009**, *41*, 161–181. [CrossRef]
2. Prawat, R.S. Current self-regulation views of learning and motivation viewed through a Deweyan lens: The problems with dualism. *Am. Educ. Res. J.* **1998**, *351*, 99–224. [CrossRef]
3. Marton, F.; Watkins, D.; Tang, C. Discontinuities and continuities in the experience of learning: An interview study of high-school students in Hong Kong. *Learn. Instr.* **1997**, *7*, 21–48. [CrossRef]
4. Gainsburg, J. The mathematical modeling of structural engineers. *Math. Think. Learn.* **2006**, *8*, 3–36. [CrossRef]
5. Noss, R.; Hoyles, C.; Pozzi, S. Abstraction in expertise: A study of nurses'conceptions of concentration. *J. Res. Math. Educ.33(3)* **2002**, 204–229. [CrossRef]
6. Zawojewski, J.S.; McCarthy, L. Numeracy in Practice. *Princ. Leadersh.* **2007**, *7*, 32–37.
7. Metlenkov, N. Dynamics of architectural education. *Astra Salvensis* **2018**, *1*, 657–667.
8. Modeste, S. Impact of informatics on mathematics and its teaching. In *International Conference on the History and Philosophy of Computing*; Springer: Cham, Switzerland, 2015; pp. 243–255.
9. Hauser, U.; Komm, D. Interdisciplinary education in mathematics and informatics at Swiss high schools. *Bull. EATCS* **2018**, *3*, 67–78.
10. Zaykis, R.; Campbell, S.R. *Number Theory in Mathematics Education: Perspectives and Prospects*; Routledge: London, UK, 2011.
11. Rittle-Johnson, B.; Schneider, M. Developing conceptual and procedural knowledge of mathematics. In *Oxford Handbook of Numerical Cognition*; Oxford University Press: Oxford, UK, 2015; pp. 1118–1134.
12. Nixon, J. Methods for Understanding Turing Machine Computations. *Math. Aeterna* **2013**, *3*, 709–738.
13. Mushtaq, M.F.; Jamel, S.; Disina, A.H.; Pindar, Z.A.; Shakir, N.S.A.; Deris, M.M. A Survey on the Cryptographic Encryption Algorithms. *Int. J. Adv. Comput. Sci. Appl.* **2017**, *8*, 333–344.
14. Coutinho, S.C. *The Mathematics of Ciphers: Number Theory and RSA Cryptography*, 1st ed.; A. K. Peters: Natick, MA, USA, 1999; p. 198. ISBN 9781568810829.
15. Kleinjung, T.; Aoki, K.; Franke, J.; Lenstra, A.K.; Thomé, E.; Bos, J.W.; Gaudry, P.; Kruppa, A.; Montgomery, P.L.; Osvik, D.A.; et al. Factorization of a 768-Bit RSA Modulus. In *Advances in Cryptology—CRYPTO 2010. Lecture Notes in Computer Science*; Springer: Berlin/Heidelberg, Germany, 2010; Volume 6223. [CrossRef]
16. Garey, M.R.; Johnson, D.S. *Computers and Intractability—A Guide to the Theory of NP-Completeness*; W. H. Freeman & Co.: New York, NY, USA, 1990; ISBN 0716710455.
17. Pommersheim, J.E.; Marks, T.K.; Flapan, E.L. *Number Theory*; Wiley: Hoboken, NY, USA, 2010; p. 753. ISBN 978-0-470-42413-1.
18. Koshy, T. *Elementary Number Theory with Applications*, 1st ed.; Academic Press: Cambridge, MA, USA, 2001; ISBN 9780124211711.
19. Kodl, J.; Trojan, V. E-signature. Signatures in the electronic environment of communication networks. *Vesmír* **2000**, *79*, 611–613.
20. Ďuriš, V. *Notes on Number Theory*, 1st ed.; Verbum: Prague, Czech Republic, 2020; p. 141. ISBN 978-80-87800-63-8.
21. Riesel, H. *Prime Numbers and Computer Methods for Factorization*, 2nd ed.; Springer: New York, NY, USA, 2012; p. 482. ISBN 978-0-8176-8298-9. [CrossRef]
22. Jones, G.A.; Jones, J.M. *Elementary Number Theory*; Springer: London, UK, 1998; ISBN 9783540761976.
23. Znám, Š. *Number Theory*; SPN: Bratislava, Slovak Republic, 1975.
24. Dahlin, B.; Watkins, D. The role of repetition in the processes of memorizing and understanding: A comparison of the views of German and Chinese secondary school students in Hong Kong. *Br. J. Educ. Psychol.* **2000**, *70*, 65–84. [CrossRef]
25. Li, S. Does practice make perfect? *Learn. Math.* **1999**, *19*, 33–35.
26. Canobi, K.H. Concept-procedure interactions in children's addition and subtraction. *J. Exp. Child Psychol.* **2009**, *102*, 131–149. [CrossRef]
27. McNeil, N.M.; Fyfe, E.R.; Petersen, L.A.; Dunwiddie, A.E.; Brletic-Shipley, H. Benefits of practicing 4=2+2: Nontraditional problem formats facilitate children's understanding of mathematical equivalence. *Child Dev.* **2001**, *82*, 1620–1633. [CrossRef]
28. McNeil, N.M.; Chesney, D.L.; Matthews, P.G.; Fyfe, E.R.; Petersen, L.A.; Dunwiddie, A.E.; Wheeler, M.C. It pays to be organized: Organizing arithmetic practice around equivalent values facilitates understanding of math equivalence. *J. Educ. Psychol.* **2012**, *104*, 1109. [CrossRef]

29. McNeil, N.M.; Fyfe, E.R.; Dunwiddie, A.E. Arithmetic practice can be modified to promote understanding of mathematical equivalence. *J. Educ. Psychol.* **2015**, *107*, 423. [CrossRef]
30. Cuarto, P.M. Algebraic Algorithm for Solving Linear Congruences: Its Application to Cryptography. *Asia Pac. J. Educ. Arts Sci.* **2014**, *1*, 34–37.
31. Ďuriš, V. Solving Some Special Task for Arithmetic Functions and Perfect Numbers. In Proceedings of the 19th Conference on Applied Mathematics, Bratislava, Slovakia, 6–24 February 2020; pp. 374–383.
32. Nunes, T. Ethnomathematics and everyday cognition. In *Handbook of Research on Mathematics Teaching and Learning*; Grouws, D.A., Ed.; Macmillan: New York, NY, USA, 1992; pp. 557–574.
33. Kilpatrick, J.; Swafford, J.; Findell, B. *Adding It Up: Helping Children Learn Mathematics*; National Research Council, Ed.; National Academy Press: Washington, DC, USA, 2001; Volume 2101.
34. Fan, L.; Bokhove, C. Rethinking the role of algorithms in school mathematics: A conceptual model with focus on cognitive development. *ZDM* **2014**, *46*, 481–492. [CrossRef]
35. Hiebert, J.; Carpenter, T.P. Learning and teaching with understanding. In *Handbook of Research on Mathematics Teaching and Learning*; Grouws, D.A., Ed.; Macmillan: New York, NY, USA, 1992; pp. 65–97.
36. Smith, J.C. Connecting undergraduate number theory to high school algebra: A study of a course for prospective teachers. In Proceedings of the 2nd International Conference on the Teaching of Mathematics, Crete, Greece, 1–6 July 2002; John Wiley & Sons Inc.: Hoboken, NJ, USA, 2002; pp. 1–8.
37. Alibali, M.W. How children change their minds: Strategy change can be gradual or abrupt. *Dev. Psychol.* **1999**, *35*, 127–145. [CrossRef]
38. Lemaire, P.; Siegler, R.S. Four aspects of strategic change: Contributions to children's learning of multiplication. *J. Exp. Psychol. Gen.* **1995**, *124*, 83–97. [CrossRef] [PubMed]
39. Popat, S.; Starkey, L. Learning to code or coding to learn? A systematic review. *Comp. Educ.* **2019**, *128*, 365–376. [CrossRef]
40. Rittle-Johnson, B.; Star, J.R.; Durkin, K. Developing procedural flexibility: Are novices prepared to learn from comparing procedures? *Br. J. Educ. Psychol.* **2012**, *82*, 436–455. [CrossRef] [PubMed]
41. Silver, E.A.; Alacaci, C.; Stylianou, D.A. Students' performance on extended constructed-response tasks. In *Results from the Seventh Mathematics Assessment of the National Assessment of Educational Progress*; Silver, E.A., Kenney, P.A., Eds.; National Council of Teachers of Mathematics: Reston, VA, USA, 2000; pp. 301–341.
42. Schneider, M.; Rittle-Johnson, B.; Star, J.R. Relations between conceptual knowledge, procedural knowledge, and procedural flexibility in two samples differing in prior knowledge. *Dev. Psychol.* **2011**, *47*, 1525–1538. [CrossRef] [PubMed]