Annales Mathematicae et Informaticae
55 (2022) pp. 196–207
DOI: https://doi.org/10.33039/ami.2022.02.002
URL: https://ami.uni-eszterhazy.hu

Solving selected problems on the Chinese remainder theorem

Viliam Ďuriš[a], Veronika Bojdová[a], Timotej Šumný[b]

[a]Department of Mathematics, Faculty of Natural Sciences, Constantine The Philosopher University in Nitra, Tr. A. Hlinku 1, Nitra, Slovakia
vduris@ukf.sk, vbojdova@ukf.sk

[b]Štefan Moyses Primary School, Školská 608, Tesárske Mlyňany, Slovakia
sumnyt@gmail.com

Abstract. The Chinese remainder theorem provides the solvability conditions for the system of linear congruences. In section 2 we present the construction of the solution of such a system. Focusing on the Chinese remainder theorem usage in the field of number theory, we looked for some problems. The main contribution is in section 3, consisting of Problems 3.1, 3.2 and 3.3 from number theory leading to the Chinese remainder theorem. Finally, we present a different view of the solution of the system of linear congruences by its geometric interpretation, applying lattice points.

Keywords: Chinese remainder theorem, proof, construction of a solution, geometric interpretation

AMS Subject Classification: 11A07, 01A99

1. Introduction

One of the first systematic knowledge of the discipline we now call number theory came from ancient China [10, 11], where queries leading to linear indeterminate equations and systems of linear congruences occurred. Indeterminate linear equations of two unknowns occurred mainly in commercial tasks, e.g. by selling several kinds of goods at integer prices. Apart from mathematics (e.g. in astronomy) appeared more complicated problems leading to systems of linear indeterminate equations with multiple unknowns, which we classify within the congruence domain nowadays. A very significant knowledge from this period, in particular, is the so-called Chinese remainder theorem, which determines the necessary and sufficient

Submitted: November 16, 2021
Accepted: February 16, 2022
Published online: February 17, 2022

conditions for the solvability of a system of linear congruences. In the mathematical treatise, which comes from the ancient Chinese mathematician Sun-c' (4^{th} century AD), we can find this problem [7]: "An unknown number of things is given. If they are counted by three, two remain, if they are counted by five, three remain, if they are counted by seven, there remain two. Determine the number of these things."

Solving this problem is easy. The least common multiple of the numbers 3, 5, and 7 is 105, so one solution of the problem will occur in the set $\{1, 2, \dots, 105\}$. From the second condition, it follows, that the solution is a number in the form $5n+3$ from the given set. Therefore it suffices to check the numbers $3, 8, 13, \dots, 103$, if the remainder after division by three (resp. seven) meets the problem conditions. The smallest suitable solution is $x = 23$. There are still other solutions, which are "repeated by 105", and are in the form $y \equiv 23 \mod 105$. The problem of the Chinese mathematician Sun-c' reached both India and Europe [6], and especially in the 18^{th} and 19^{th} centuries engaged the attention of mathematicians L. Euler and C. F. Gauss. The Chinese used a lunar calendar, in which small and large months changed by 29 and 30 days, so the year had 354 days. However, such a calendar brought problems, because due to the different length of the solar year, which the Chinese set at $365\frac{1}{4}$ days, it happened that the beginnings of the years were not in fixed dates. The Chinese inserted after 19 lunar years another 7 lunar months (around 600 BC) [2]. At the end of the first millennium AD, Chinese mathematicians and astronomers devoted great effort to calculate the so-called Great period, i.e. the question in how many years the three periods will meet – the tropical year with $365\frac{1}{4}$ days, the lunar month with $29\frac{499}{940}$ days and a sixty-day cycle [13]. The problem led to a system of congruences with large numbers. The Chinese mathematician Qin Jiushao [12] came up with a solution to the system of congruences $x \equiv 193440 \pmod{1014000}$, $x \equiv 16377 \pmod{499067}$, where $x = 6172608n$, (n is the number of years elapsed since the Great Period) [8].

There are several ways to formulate the Chinese remainder theorem.

Theorem 1.1. *Let there be a system of solvable linear congruences*

$$\begin{aligned} a_1 x &\equiv b_1 \pmod{m_1} \\ a_2 x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ a_k x &\equiv b_k \pmod{m_k}, \end{aligned} \tag{1.1}$$

where $a_i, b_i, m_i (i = 1, 2, \dots, k)$ are given integers. If m_i are pairwise coprime, then the system is solvable; or more precisely, elements of the congruence class modulo $m = m_1 m_2 \cdots m_k$ satisfy all given congruences. This statement is called the Chinese remainder theorem [9].

Proof. By mathematical induction. First, consider a system with two congruences:

$$\begin{aligned} a_1 x &\equiv b_1 \pmod{m_1} \\ a_2 x &\equiv b_2 \pmod{m_2}. \end{aligned}$$

The first congruence is solvable from assumption, hence there exists $x \equiv c_1($ $\pmod{m_1})$ which satisfies the first congruence. Substitute this solution $x = c_1 + tm_1, t \in Z$, into the second congruence:

$$a_2(c_1 + m_1 t) \equiv b_2 \pmod{m_2}$$
$$(a_2 m_1)t \equiv (b_2 - a_2 c_1) \pmod{m_2}.$$

Since m_1 and m_2 are coprime, then $\gcd(a_2 m_1, m_2) = \gcd(a_2, m_2)$. From the theorem assumptions the second congruence is solvable too, therefore $\gcd(a_2, m_2) \mid b_2$. However, this already results in $\gcd(a_2 m_1, m_2) \mid b_2$, which is the condition for solvability of the congruence $(a_2 m_1)t \equiv (b_2 - a_2 c_1) \pmod{m_2}$. So we have $t \equiv c_2 \pmod{m_2}$, which satisfies the second congruence. Then we can rewrite x as:

$$x = c_1 + m_1(c_2 + sm_2) = (c_1 + c_2 m_1) + s(m_1 m_2),$$

where $c_1, c_2, s \in Z$. Thus, the solution of the system of the two linear congruences is the whole congruence class

$$x \equiv e_1 \pmod{m_1 m_2},$$

where $e_1 = c_1 + c_2 m_1$.

Now suppose the statement holds true for $k = \nu$. Consider the system of $\nu + 1$ solvable linear congruences with pairwise coprime moduli $m_1, m_2, \ldots, m_{\nu+1}$. The system of first ν congruences is solvable from the induction assumption, so we have

$$x \equiv e_\nu \pmod{m_1 m_2 \ldots m_\nu}$$

satisfying the first ν congruences. We have to find out if any element of this congruence class is also the solution of the last congruence. We solve the system of congruences:

$$x \equiv e_\nu \pmod{m_1 m_2 \ldots m_\nu}$$
$$a_{\nu+1} x \equiv b_{\nu+1} \pmod{m_{\nu+1}}.$$

Since $\gcd(m_{\nu+1}, m_1, \ldots, m_\nu) = 1$, then there exists the solution of this system of two congruences (by analogy to the first step of the proof). $\square$

The Chinese remainder theorem says nothing about a case of the congruence system (1.1) with non-coprime moduli. In this case, the system can be unsolvable, although individual congruences are solvable. But the system also can be solvable.

2. The construction of a solution of a system of linear congruences

First, we present the applicable construction method for a solution of the system (1.1). We show, that u in the following form is a solution of the system (1.1).

Theorem 2.1. *Consider the solvable system of linear congruences (1.1). Then*

$$u = \sum_{i=1}^{k} \frac{m}{m_i} c_i r^{(i)} = \frac{m}{m_1} c_1 r^{(1)} + \dots + \frac{m}{m_k} c_k r^{(k)}$$

is a common solution of given system, where $r^{(i)}$ is a solution of $a_i x \equiv b_i \pmod{m_i}$ and c_i is a solution of

$$\frac{m}{m_i} y \equiv 1 \pmod{m_i}, \quad m = m_1 m_2 \dots m_k,\ i = 1, \dots, k, \quad \gcd\left(\frac{m}{m_i}, m_i\right) = 1.$$

Proof. First, let us solve the congruences

$$\frac{m}{m_i} y \equiv 1 \pmod{m_i}, \quad i = 1, \dots, k, \quad \gcd\left(\frac{m}{m_i}, m_i\right) = 1,$$

where c_i is the appropriate solution. Let $r^{(i)}$ be a solution satisfying

$$a_i x \equiv b_i \pmod{m_i}, \quad i = 1, \dots, k.$$

We show that

$$u = \sum_{i=1}^{k} \frac{m}{m_i} c_i r^{(i)} = \frac{m}{m_1} c_1 r^{(1)} + \dots + \frac{m}{m_k} c_k r^{(k)}$$

satisfies any of the congruences $a_i x \equiv b_i \pmod{m_i}$.

We express

$$a_i x = a_i u = a_i \sum_{i=1}^{k} \frac{m}{m_i} c_i r^{(i)} = a_i \left(\frac{m}{m_1} c_1 r^{(1)} + \dots + \frac{m}{m_i} c_i r^{(i)} + \dots + \frac{m}{m_k} c_k r^{(k)} \right).$$

Since all members $\frac{m}{m_1}, \dots, \frac{m}{m_k}$ except member $\frac{m}{m_i}$ are divisible by the number m_i, we get

$$a_i u \equiv a_i \frac{m}{m_i} c_i r^{(i)} \pmod{m_i}.$$

Since c_i is a solution of $\frac{m}{m_i} y \equiv 1 \pmod{m_i}$, then $\frac{m}{m_i} c_i \equiv 1 \pmod{m_i}$, and thus

$$a_i u \equiv a_i r^{(i)} \pmod{m_i}.$$

And finally from $a_i r^{(i)} \equiv b_i \pmod{m_i}$ we have $a_i u \equiv b_i \pmod{m_i}$.

Now we show that any $x = u + tm, t \in Z$ satisfies the congruence $a_i x \equiv b_i \pmod{m_i}$. We have

$$a_i(u + tm) = a_i u + a_i tm,$$

where $a_i u \equiv b_i \pmod{m_i}$ and $a_i tm \equiv 0 \pmod{m_i}$, while $\exists h \in Z : m = h m_i$. Then

$$a_i(u + tm) \equiv b_i \pmod{m_i}.$$

If the congruence $a_i x \equiv b_i \pmod{m_i}$ has n_i incongruent solutions $r^{(i)}$, then we have together $n_1 n_2 \cdots n_k$ incongruent solutions $u = \frac{m}{m_1} c_1 r^{(1)} + \cdots + \frac{m}{m_i} c_i r^{(i)} + \cdots + \frac{m}{m_k} c_k r^{(k)}$ of the system (1.1). We show, that all are incongruent by modulo m.

If we changed any of the solutions $r^{(i)}$ of the congruence $a_i x \equiv b_i \pmod{m_i}$ of the common solution u of the system to an incongruent one by modulo m_i, we would get an incongruent solution u. Let's change, e.g., h solutions $r^{(i)}$ $(h \leq k)$ to incongruent ones by modulo m_i and arrange the expressions $\frac{m}{m_i} c_i r^{(i)}$ in u by placing forward those, which contain an incongruent solution $r^{(i)}$. Then, after re-indexing members in u and re-denoting incongruent solutions, we can write

$$u_2 = \frac{m}{m_1} c_1 r_2^{(1)} + \cdots + \frac{m}{m_i} c_i r_2^{(i)} + \cdots + \frac{m}{m_h} c_h r_2^{(h)} + \frac{m}{m_{h+1}} c_{h+1} r^{(h+1)} + \cdots + \frac{m}{m_k} c_k r^{(k)}.$$

We show, that u_2 is not congruent with u by modulo m. By contradiction, if $u \equiv u_2 \pmod{m}$, then $m \mid u - u_2 \wedge m_i \mid m \Rightarrow m_i \mid u - u_2$, hence $u \equiv u_2 \pmod{m_i}$. Then

$$\frac{m}{m_1} c_1 r^{(1)} + \cdots + \frac{m}{m_i} c_i r^{(i)} + \cdots + \frac{m}{m_h} c_h r^{(h)} - \left(\frac{m}{m_1} c_1 r_2^{(1)} + \cdots \right.$$
$$\left. + \frac{m}{m_i} c_i r_2^{(i)} + \cdots + \frac{m}{m_h} c_h r_2^{(h)} \right) \equiv 0 \pmod{m_i}.$$

From the last congruence we have

$$\frac{m}{m_i} c_i r^{(i)} - \frac{m}{m_i} c_i r_2^{(i)} \equiv 0 \pmod{m_i} \quad \Leftrightarrow \quad \frac{m}{m_i} c_i r^{(i)} \equiv \frac{m}{m_i} c_i r_2^{(i)} \pmod{m_i}.$$

Since $\frac{m}{m_i} c_i \equiv 1 \pmod{m_i}$, then $r^{(i)} \equiv r_2^{(i)} \pmod{m_i}$, what is a contradiction. Hence solution u_2 can not be congruent with u by modulo m. This means we have incongruent solutions u and u_2. □

3. Selected problems from number theory leading to use of Chinese remainder theorem

Focusing on the use of the Chinese remainder theorem, we present the proofs of selected problems from number theory. We also present simple codes in R language to demonstrate the solutions to these problems.

Problem 3.1. There are at most two n-digit numbers with the property $x^2 = k10^n + x$. Such numbers x, whose squares end in themselves, are called 1-automorphic numbers (see e.g. [5]).

Solution. We are searching for natural numbers x, among n-digit numbers $0 \leq x < 10^n$, with the property:

$$x^2 = k10^n + x.$$

Hence

$$x^2 - x = k10^n = k2^n5^n,$$

which leads to congruence $x^2 \equiv x \pmod{10^n}$, or

$$x^2 - x = x(x-1) \equiv 0 \pmod{10^n}. \tag{3.1}$$

Since $x \in N$, then it is true that if x is even then $x-1$ is odd, or if x is odd then $x-1$ is even. Then from (3.1) we get, that x satisfies either system of congruences

$$\begin{aligned} x &\equiv 0 \pmod{2^n} \\ x-1 &\equiv 0 \pmod{5^n} \quad \Leftrightarrow \quad x \equiv 1 \pmod{5^n} \end{aligned} \tag{3.2}$$

or system of congruences

$$\begin{aligned} x &\equiv 0 \pmod{5^n} \\ x-1 &\equiv 0 \pmod{2^n} \quad \Leftrightarrow \quad x \equiv 1 \pmod{2^n}. \end{aligned} \tag{3.3}$$

Since $\gcd(2^n, 5^n) = 1$ and $0 \equiv 1 \pmod{1}$ holds true, then the system (3.2) and also the system (3.3) has a unique solution modulo 2^n5^n. Consequently there are at most two n-digit numbers with the property $x^2 = k10^n + x$.

We present a code in R language to demonstrate solutions for $n \in \{1, \ldots, 8\}$:

```
library(numbers)
n=8
a1=c(1,0)
a2=c(0,1)
for (i in 1:n) {
 m=c(2^i, 5^i)
  print(chinese(a1,m))
  print(chinese(a2,m)) }
> 5
  6
  25
  76
  625
  376
  9376
  90625
  890625
  109376
  2890625
  7109376
  12890625
  87109376
```

Problem 3.2 (inspired by [1]). For every positive integer n, there exist n consecutive positive integers such that none of them is a power of a prime.

Solution. We show that for any n there exists $x \in N$ such that none of the numbers $x+1, x+2, \ldots, x+n \in N$ is a power of a prime. The number $x+i$ $(i = 1, 2, \ldots, n)$ is not a power of a prime if there are two different primes p, q, that divide $x + i$.

Let $n \in N$, $i = 1, 2, \ldots, n$, and let all $p_1, p_2, \ldots, p_n, q_1, q_2, \ldots, q_n$ be distinct primes. We look for $x \in N$, which satisfies $p_i q_i \mid x + i$ for each $i = 1, 2, \ldots, n$. Written as the system of congruences we have

$$x + i \equiv 0 \pmod{p_i q_i},$$

or

$$x \equiv p_i q_i - i \pmod{p_i q_i} \tag{3.4}$$

for $i = 1, 2, \ldots, n$.

Since p_i, q_i $(i = 1, 2, \ldots, n)$ were distinct, then $\gcd(p_i q_i, p_j q_j) = 1$. Hence there exists one solution x of the system (3.4). Thus, for any $n \in N$ we found (constructed) $x \in N$ such that numbers $x + 1, x + 2, \ldots, x + n \in N$ have two different prime divisors.

A simple code in R language allows us to demonstrate the solution for $n = 3$: the three consecutive integers are 18458, 18459 and 18460. With help of prime factorization it's easy to see, that none of them is a power of a prime.

```
library(numbers)
n = 3
p = c(11,7,5)
q = c(2,3,13)
i = 1:n
x = chinese(p*q-i,p*q)
print(x)
> 18457

library(gmp)
factorize(x+1)
> 2   11  839

factorize(x+2)
> 3   3   7   293

factorize(x+3)
> 2  2  5  13 71
```

Problem 3.3 (inspired by [1]). There exists a set S of three positive integers such that for any two distinct $a, b \in S$ $a - b$ divides a and b but none of the other elements of S.

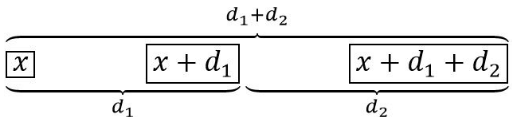

Figure 1. Elements of S.

Solution. Denote three positive integers from S by $x, x+d_1, x+d_1+d_2$, where d_1, d_2 denote the differences between consecutive elements of S (Figure 1).
We have 3 pairs of distinct elements and we write down the divisibility conditions for the first element x:

$$\begin{aligned} d_1 \mid x \quad &\Leftrightarrow \quad x \equiv 0 \pmod{d_1} \\ d_1+d_2 \mid x \quad &\Leftrightarrow \quad x \equiv 0 \pmod{d_1+d_2} \\ d_2 \nmid x \quad &\Leftrightarrow \quad x \equiv a_1 \pmod{d_2}, \end{aligned} \tag{3.5}$$

where $a_1 \in \{1, 2, \ldots, d_2-1\}$ is the non-zero remainder. We show, that it suffices to choose any coprime positive integers $d_1, d_2, d_1 < d_2$, and then the existence of x follows from the Chinese remainder theorem.

Let $d_1, d_2, d_1 < d_2$, be any coprime positive integers, hence also d_1, d_2, d_1+d_2 are pairwise coprime. Remainder $a_1 \in \{1, 2, \ldots, d_2-1\}$ depends on the choice of d_1, d_2 following way. From the condition $x + d_1 \equiv 0 \pmod{d_2}$ we have $x \equiv -d_1 \pmod{d_2}$, which together with congruence

$$x \equiv a_1 \pmod{d_2}$$

gives the result for a_1: $a_1 \equiv -d_1 \pmod{d_2}$, so we can put $a_1 = d_2 - d_1$ (since $d_1 < d_2$). Since d_1, d_2, d_1+d_2 are pairwise coprime moduli, then there is a unique solution of the system (3.5):

$$\begin{aligned} x &\equiv 0 \pmod{d_1} \\ x &\equiv 0 \pmod{d_1+d_2} \\ x &\equiv d_2 - d_1 \pmod{d_2}. \end{aligned}$$

We can get some solutions of this example by using the following code in R language:

```
library(numbers)
d1 = 8
d2 = 15
a = c(0,0,d2-d1)
m = c(d1,d1+d2,d2)
x = chinese(a,m)
print(c(x,x+d1,x+d1+d2))
```

Table 1. Some solutions.

d_1	d_2	x	$x+d_1$	$x+d_1+d_2$
2	3	10	12	15
2	7	54	56	63
8	15	2392	2400	2415

4. Geometric interpretation of the solution of system of linear congruences

Finally, we present a different view of the solution of the system of linear congruences by its geometric interpretation, applying lattice points. For some basic knowledge of the lattice points, see, e.g. [4].

Consider a congruence $ax \equiv b \pmod{m}, a, b, x, m \in Z, m > 1$. There is a direct connection between this congruence relation and the Diophantine equation [3], while $ax - b = ym, y \in Z$, represents the linear Diophantine equation

$$ax - my = b$$

(where $x, y \in Z$ are the unknowns and $a, b, m \in Z, a, b \neq 0$, are given constants).

On the other hand, the equation

$$ax - my - b = 0 \tag{4.1}$$

represents a straight line (in Euclidean plane). So for given $a, b, m \in Z$ the solution of the congruence $ax \equiv b \pmod{m}$ geometrically represents all intersection points $[x_0, y_0], x_0, y_0 \in Z$, of the straight line (4.1) and the lattice of integral coordinates.

Example 4.1. Consider system of congruences

$$\begin{aligned} 3x &\equiv 4 \pmod{8} \\ 4x &\equiv 2 \pmod{5}. \end{aligned}$$

Both congruences are solvable ($\gcd(3,8) = 1 \mid 4$ and $\gcd(4,5) = 1 \mid 2$). The solution of the second congruence $4x \equiv 2 \pmod{5}$ is $x \equiv 3 \pmod{5}$. Substitute $x = 3 + 5t,\ t \in Z$ into the first congruence, then

$$3(3 + 5t) \equiv 4 \pmod{8},$$

hence

$$15t \equiv -5 \pmod{8}$$

with a solution $t \equiv 5 \pmod{8}$. Finally, after substitution $t = 5 + 8y,\ y \in Z$ into x:

$$x = 3 + 5(5 + 8y) = 28 + 40y,$$

we get the solution $x \equiv 28 \pmod{40}$ of the system.

Figure 2 shows the geometric representation of the congruence $x \equiv 28 \pmod{40}$. That means, there are infinitely many points $[x_0, y_0]$ with integer coordinates on the green straight line $x - 28 - 40y = 0$. See, that e.g. the lattice point $[68, 1]$ is one of the solution points.

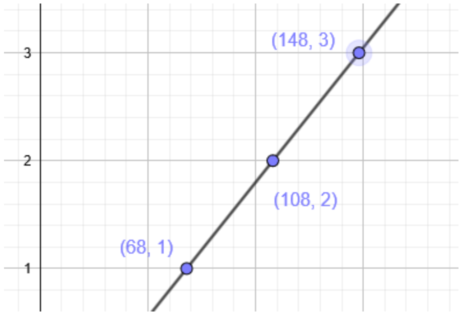

Figure 2. Example of the intersection of straight line and a lattice of the integer coordinates.

In our geometric interpretation of the Diophantine equation, we consider the solvability conditions based on the lattice points, through which the line represented by equation (4.1) passes.

Now consider a system of linear congruences (1.1), where $\gcd(m_i, m_j) = 1$ for all $i, j,\ i \neq j,\ i, j = 1, \ldots, k$. Such a system of congruences can be converted to Diophantine equations with the same consideration as mentioned above. Since we are looking for a common solution for these Diophantine equations, geometrically this means that we are looking for a line that passes through all the lattice, which is characteristic for concrete Diophantine equations. The solution of such a system of equations is a congruence

$$x \equiv u \pmod{\prod m_i},$$

which we can interpret as a straight line in the form

$$x - u - y \prod m_i = 0.$$

In other words, considered congruences give us information about a line in various specific scales, and we're looking for its formula. For an illustration of this representation, an example follows.

Example 4.2. Consider system of congruences

$$\begin{aligned} 2x - 4 &\equiv 0 \pmod{8} \\ 2x - 1 &\equiv 0 \pmod{3} \\ 13x - 4 &\equiv 0 \pmod{5}. \end{aligned} \tag{4.2}$$

We will construct the solution of the system of congruences according to the Theorem 2.1. We see, that $\gcd(8,3) = \gcd(3,5) = \gcd(8,5) = 1$, so we can apply the Chinese remainder theorem. Denote $m = 2^3 \cdot 3 \cdot 5 = 120$. Then the number of system solutions is $n = n_1 n_2 n_3 = 2 \cdot 1 \cdot 1 = 2$.

Congruence $2x - 4 \equiv 0 \pmod 8$ has solutions $r_1^{(1)} = 2, r_2^{(1)} = 6$, congruence $2x - 1 \equiv 0 \pmod 3$ has a solution of $r^{(2)} = 2$ and congruence $13x - 4 \equiv 0 \pmod 5$ has a solution of $r^{(3)} = 3$.

Solutions of congruences $\frac{120}{8} y \equiv 1 \pmod 8$, $\frac{120}{3} y \equiv 1 \pmod 3$ and $\frac{120}{5} y \equiv 1 \pmod 5$ are $c_1 = 7, c_2 = 1$ and $c_3 = 4$, respectively.

Finally $u = 15 \cdot 7r^{(1)} + 40 \cdot 1r^{(2)} + 24 \cdot 4r^{(3)} = 105r^{(1)} + 40r^{(2)} + 96r^{(3)}$.

Table 2. Summary of the resulting two solutions.

	$r^{(1)}$	$r^{(2)}$	$r^{(3)}$	u
1.	2	2	3	$578 \equiv 98 \pmod{120}$
2.	6	2	3	$998 \equiv 38 \pmod{120}$

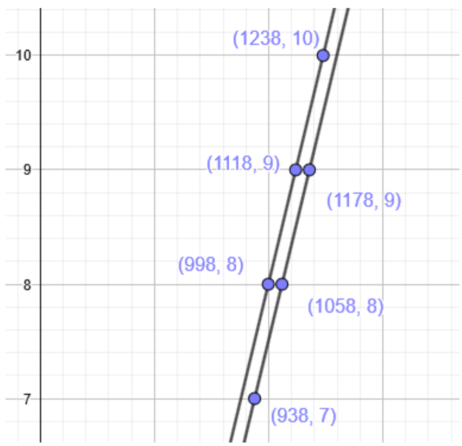

Figure 3. Geometric interpretation of the solution.

The solutions from Table 2 are represented in the Figure 3 by straight lines with equations

$$x - 120y - 98 = 0,$$
$$x - 120y - 38 = 0.$$

Finally we mention, that there exists one residue class containing all solutions in form $x \equiv 38 \pmod{60}$, represented by a straight line with equation $x - 60y - 38 = 0$.

5. Conclusion

The paper introduces the historical background of the Chinese remainder theorem, focusing on one of its proofs. Section 2 presents the construction of a solution of a system of linear congruences, which gives the applicable solving method of the system (1.1). The main contribution is in section 3, consisting of three problems from number theory, leading to the Chinese remainder theorem. The article also deals with the geometric interpretation of the solution of the system of linear congruences. It introduces a different perspective of the solution, applying lattice points and the relationship between the congruence and the Diophantine equation. Illustrating examples supplement all of the theoretical results.

References

[1] E. Chen: *The Chinese Remainder Theorem, February 3, 2015, article for olympiad students*, 2015.

[2] C. Cullen: *Astronomy and Mathematics in Ancient China: The 'Zhou Bi Suan Jing'*, UK: Cambridge University Press, 2007.

[3] V. Ďuriš, D. Gonda, A. Tirpáková, G. Pavlovičová: *Teaching Congruences in Connection with Diophantine Equations*, Education Sciences 11.9 (2021), pp. 1–14, doi: https://doi.org/10.3390/educsci11090538.

[4] V. Ďuriš, T. Šumný: *Diophantine Geometry in Space E2 and E3*, TEM Journal 8.1 (2019), pp. 78–81, doi: https://doi.org/10.18421/TEM81-10.

[5] V. de Guerre, R. A. Fairbairn: *Automorphic Numbers*, J. Recr. Math. 1 (1968), pp. 173–179.

[6] A. P. Juškevič: *History of mathematics in the Middle Ages*, Prague: Academia, 1977.

[7] S. Kangsheng: *Historical Development of the Chinese Remainder Theorem*, Arch. Hist. Exact Sci. 38.4 (1988), pp. 285–305, doi: https://doi.org/10.1007/bf00357063.

[8] J. C. Martzloff: *Astronomy and Calendars – The Other Chinese Mathematics, 1st ed.* Switzerland: Springer Nature, 2016.

[9] P. Ribenboim: *The Little Book of Bigger Primes, 2nd ed.* New York: Springer-Verlag, 2004.

[10] D. E. Smith: *History of Mathematics*, vol. I, US: Dover Publications, 1958.

[11] D. E. Smith: *History of Mathematics*, vol. II, US: Dover Publications, 1958.

[12] C. Smoryński: *Logical Number Theory I*, Germany: Springer Verlag Berlin Heidelberg, 1991.

[13] D. Yinke: *Ancient Chinese Inventions*, China: China Intercontinental Press, 2005.