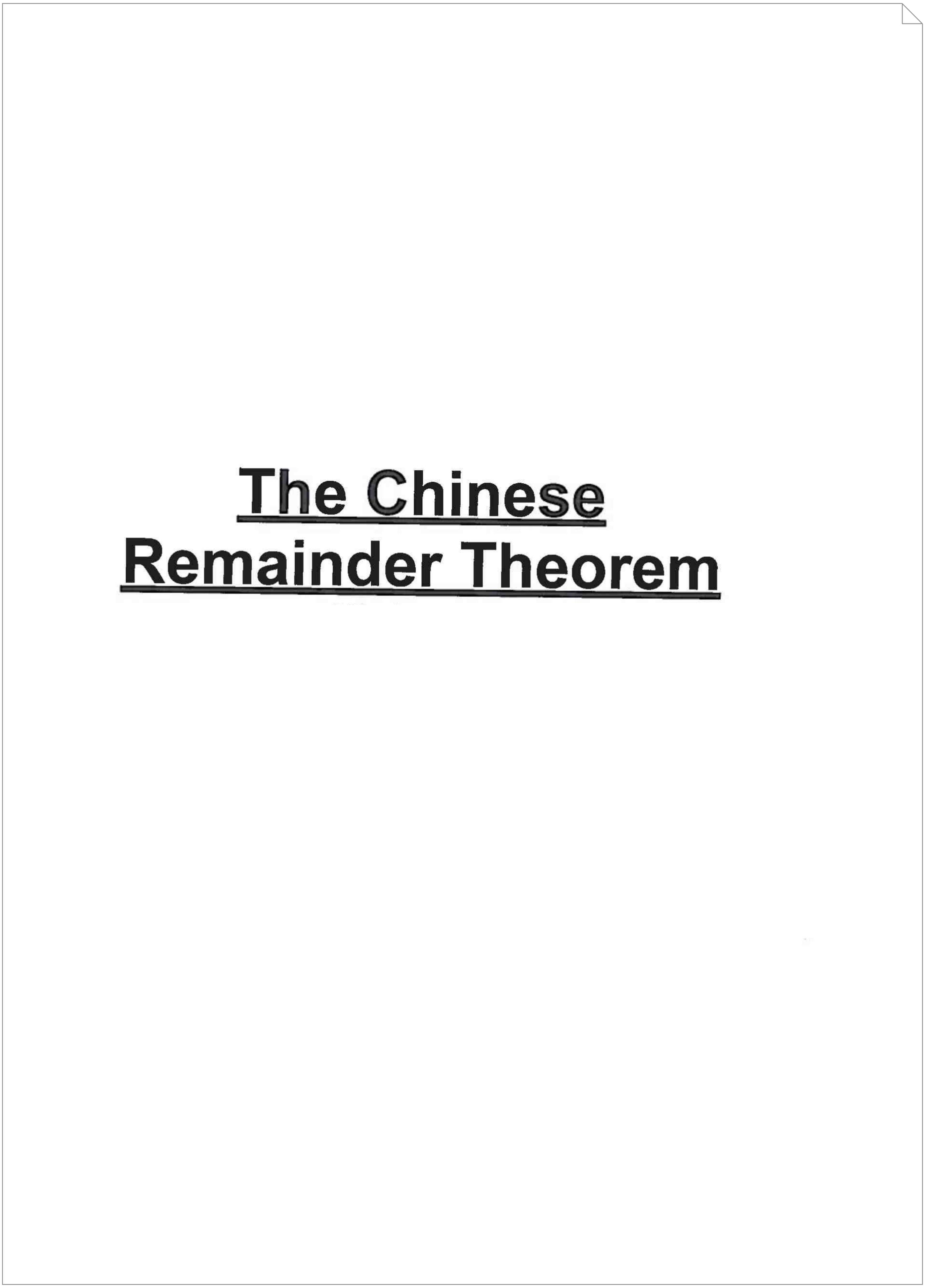
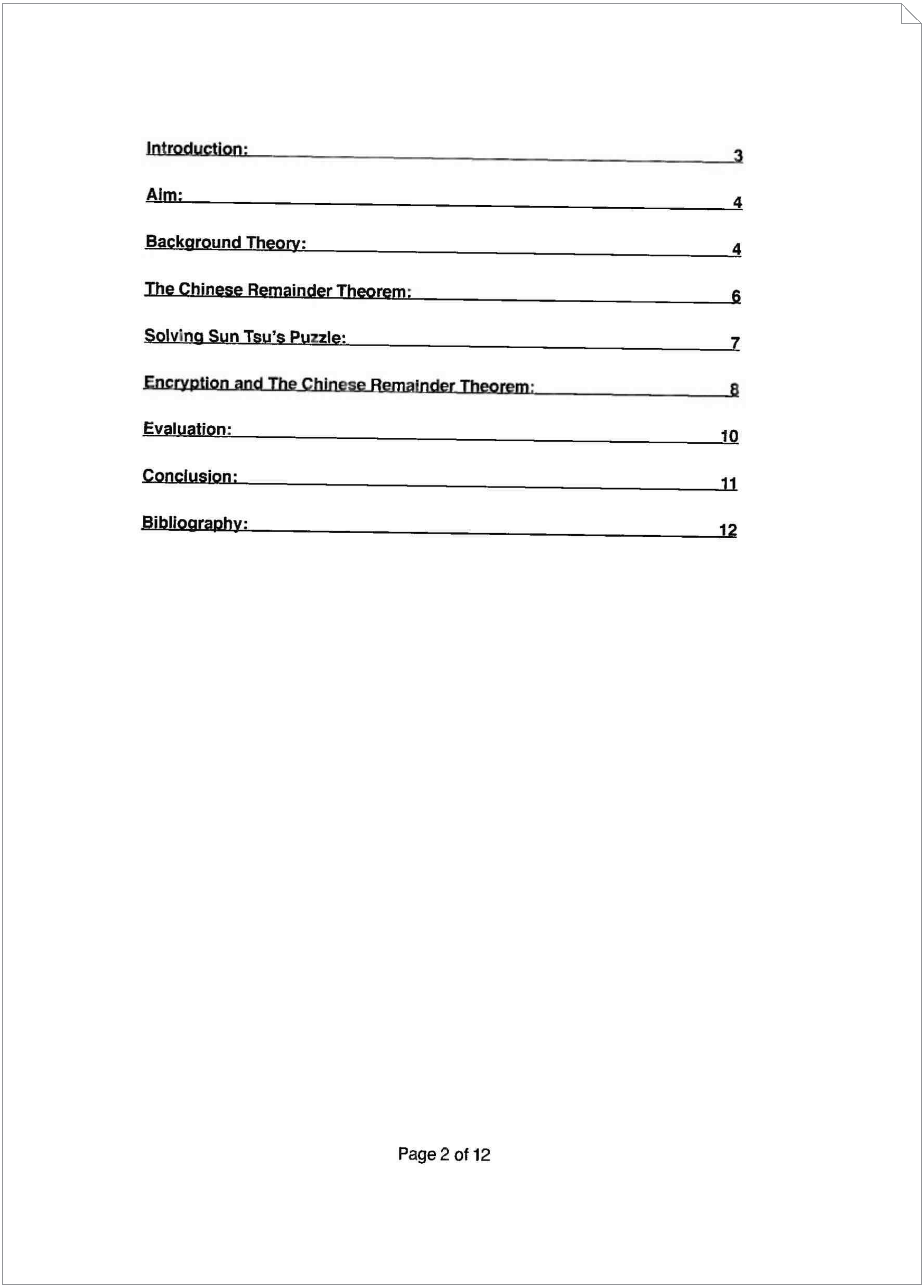
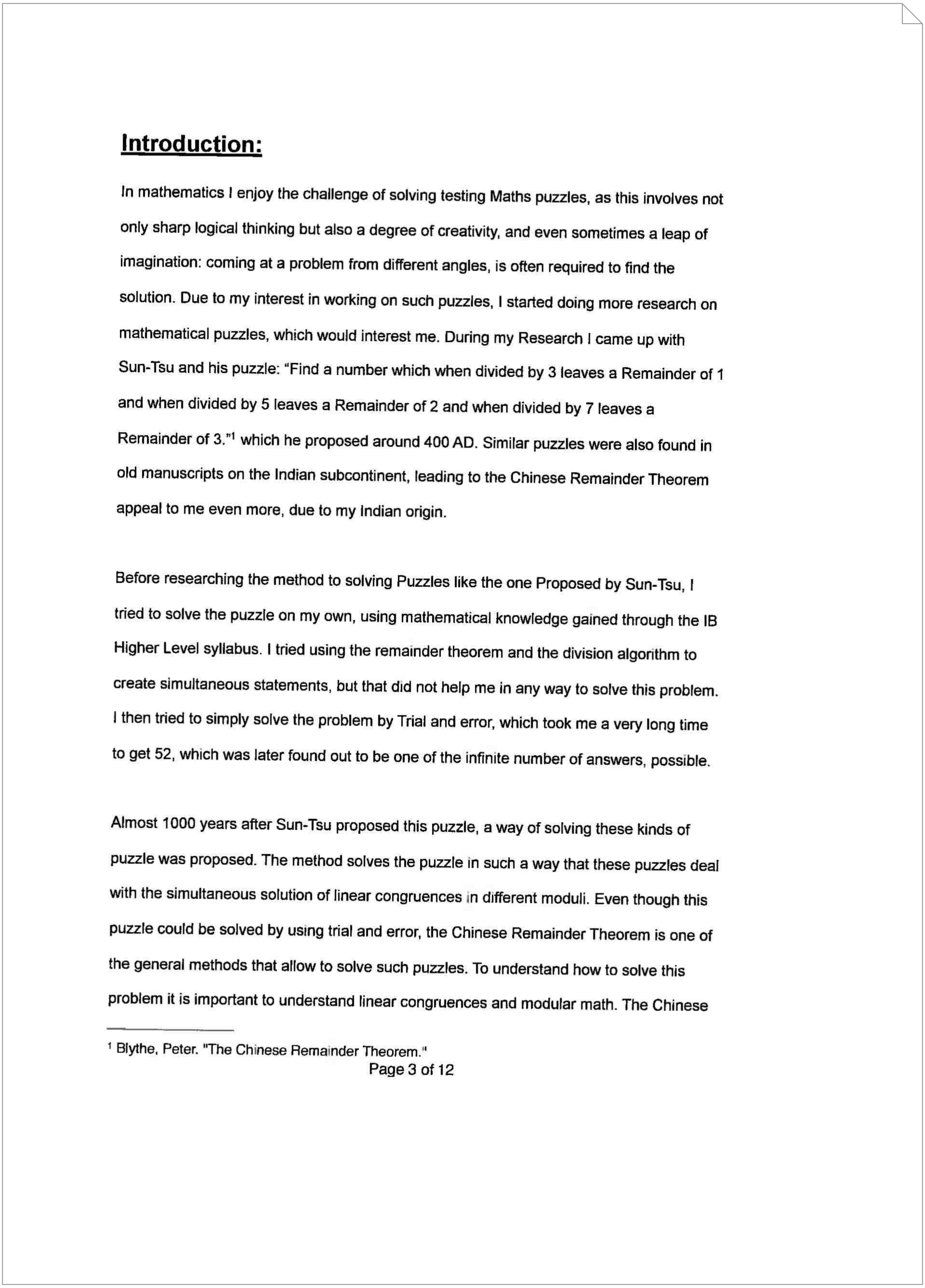


The Chinese Remainder Theorem





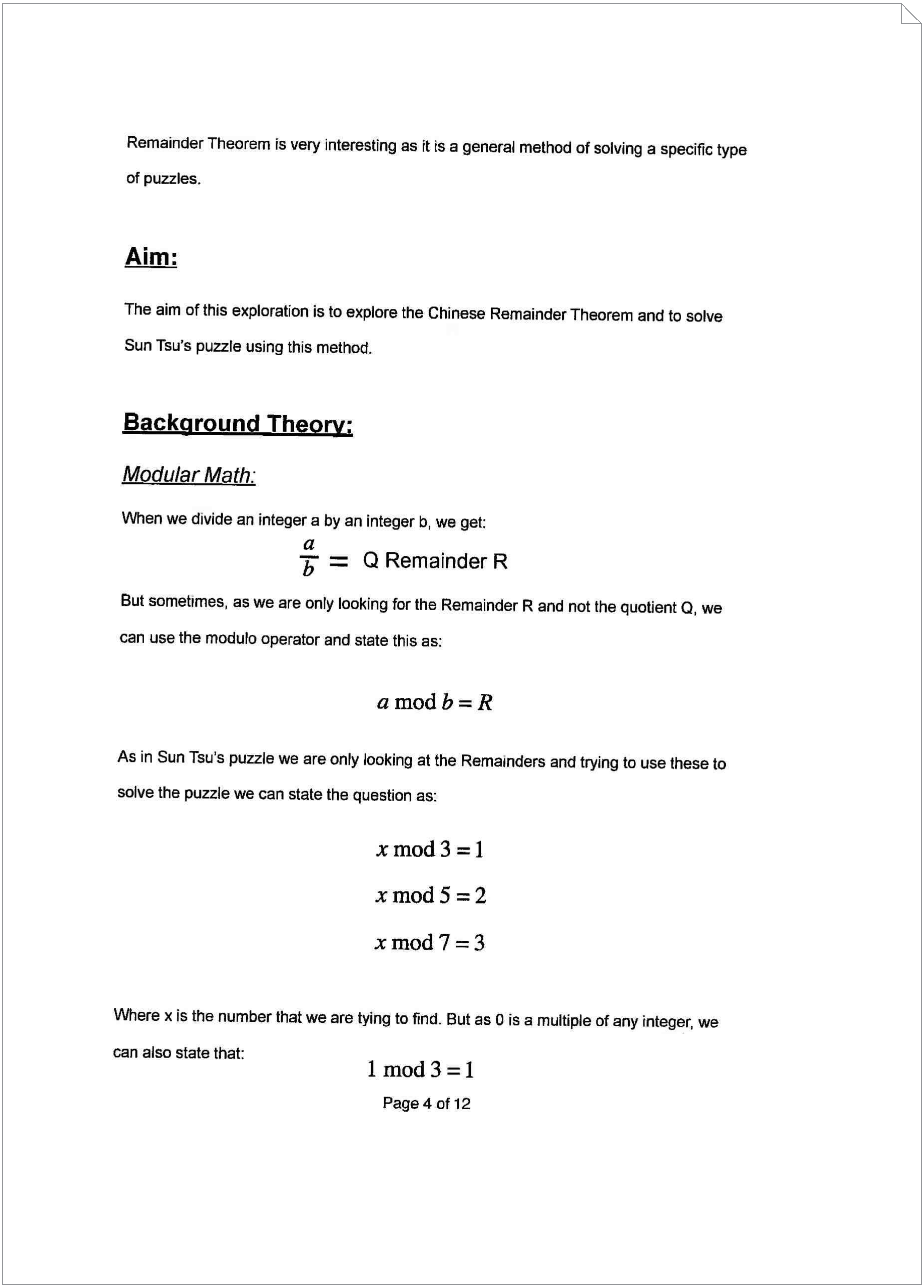
Introduction:

In mathematics I enjoy the challenge of solving testing Maths puzzles, as this involves not only sharp logical thinking but also a degree of creativity, and even sometimes a leap of imagination: coming at a problem from different angles, is often required to find the solution. Due to my interest in working on such puzzles, I started doing more research on mathematical puzzles, which would interest me. During my Research I came up with Sun-Tsu and his puzzle: "Find a number which when divided by 3 leaves a Remainder of 1 and when divided by 5 leaves a Remainder of 2 and when divided by 7 leaves a Remainder of 3."[1] which he proposed around 400 AD. Similar puzzles were also found in old manuscripts on the Indian subcontinent, leading to the Chinese Remainder Theorem appeal to me even more, due to my Indian origin.

Before researching the method to solving Puzzles like the one Proposed by Sun-Tsu, I tried to solve the puzzle on my own, using mathematical knowledge gained through the IB Higher Level syllabus. I tried using the remainder theorem and the division algorithm to create simultaneous statements, but that did not help me in any way to solve this problem. I then tried to simply solve the problem by Trial and error, which took me a very long time to get 52, which was later found out to be one of the infinite number of answers, possible.

Almost 1000 years after Sun-Tsu proposed this puzzle, a way of solving these kinds of puzzle was proposed. The method solves the puzzle in such a way that these puzzles deal with the simultaneous solution of linear congruences in different moduli. Even though this puzzle could be solved by using trial and error, the Chinese Remainder Theorem is one of the general methods that allow to solve such puzzles. To understand how to solve this problem it is important to understand linear congruences and modular math. The Chinese

[1] Blythe, Peter. "The Chinese Remainder Theorem."



Remainder Theorem is very interesting as it is a general method of solving a specific type of puzzles.

Aim:

The aim of this exploration is to explore the Chinese Remainder Theorem and to solve Sun Tsu's puzzle using this method.

Background Theory:

Modular Math:

When we divide an integer a by an integer b, we get:

$$\frac{a}{b} = \text{Q Remainder R}$$

But sometimes, as we are only looking for the Remainder R and not the quotient Q, we can use the modulo operator and state this as:

$$a \bmod b = R$$

As in Sun Tsu's puzzle we are only looking at the Remainders and trying to use these to solve the puzzle we can state the question as:

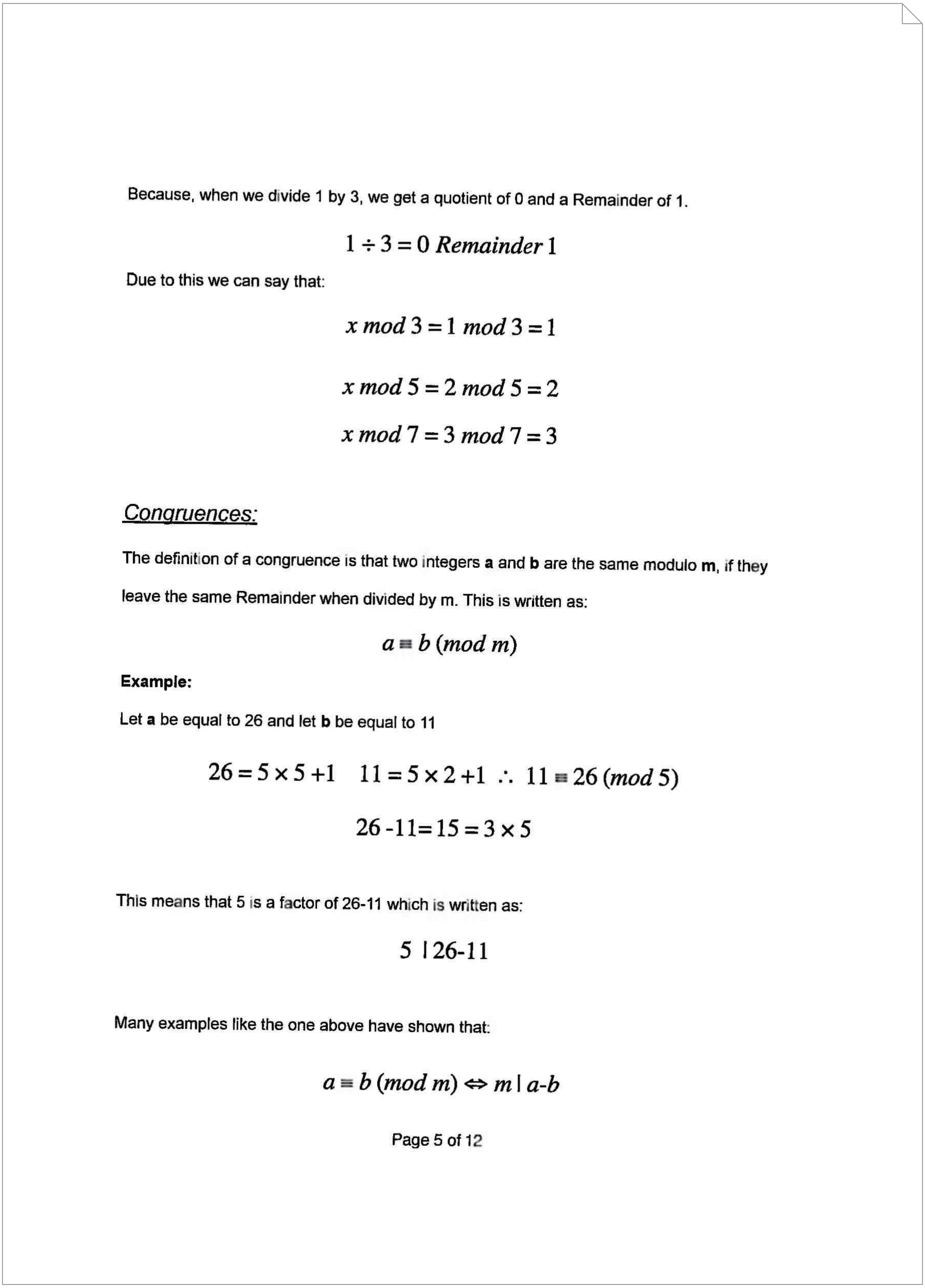
$$x \bmod 3 = 1$$

$$x \bmod 5 = 2$$

$$x \bmod 7 = 3$$

Where x is the number that we are tying to find. But as 0 is a multiple of any integer, we can also state that:

$$1 \bmod 3 = 1$$



Because, when we divide 1 by 3, we get a quotient of 0 and a Remainder of 1.

$$1 \div 3 = 0 \; Remainder \; 1$$

Due to this we can say that:

$$x \; mod \; 3 = 1 \; mod \; 3 = 1$$

$$x \; mod \; 5 = 2 \; mod \; 5 = 2$$

$$x \; mod \; 7 = 3 \; mod \; 7 = 3$$

Congruences:

The definition of a congruence is that two integers **a** and **b** are the same modulo **m**, if they leave the same Remainder when divided by m. This is written as:

$$a \equiv b \; (mod \; m)$$

Example:

Let **a** be equal to 26 and let **b** be equal to 11

$$26 = 5 \times 5 + 1 \quad 11 = 5 \times 2 + 1 \;\; \therefore \;\; 11 \equiv 26 \; (mod \; 5)$$

$$26 - 11 = 15 = 3 \times 5$$

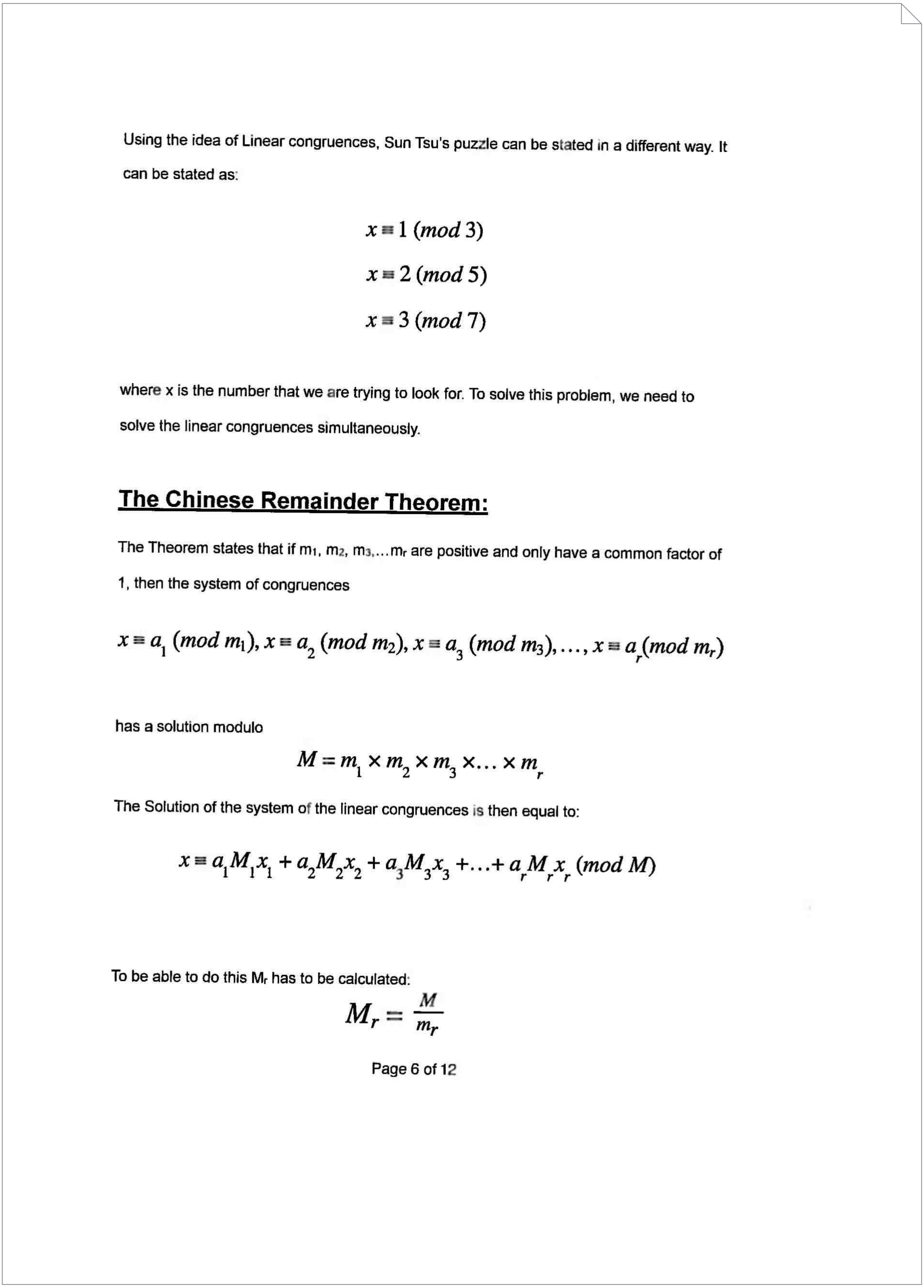
This means that 5 is a factor of 26-11 which is written as:

$$5 \mid 26\text{-}11$$

Many examples like the one above have shown that:

$$a \equiv b \; (mod \; m) \Leftrightarrow m \mid a\text{-}b$$

Page 5 of 12



Using the idea of Linear congruences, Sun Tsu's puzzle can be stated in a different way. It can be stated as:

$$x \equiv 1\ (mod\ 3)$$

$$x \equiv 2\ (mod\ 5)$$

$$x \equiv 3\ (mod\ 7)$$

where x is the number that we are trying to look for. To solve this problem, we need to solve the linear congruences simultaneously.

The Chinese Remainder Theorem:

The Theorem states that if m_1, m_2, m_3,…m_r are positive and only have a common factor of 1, then the system of congruences

$$x \equiv a_1\ (mod\ m_1), x \equiv a_2\ (mod\ m_2), x \equiv a_3\ (mod\ m_3), \ldots, x \equiv a_r (mod\ m_r)$$

has a solution modulo

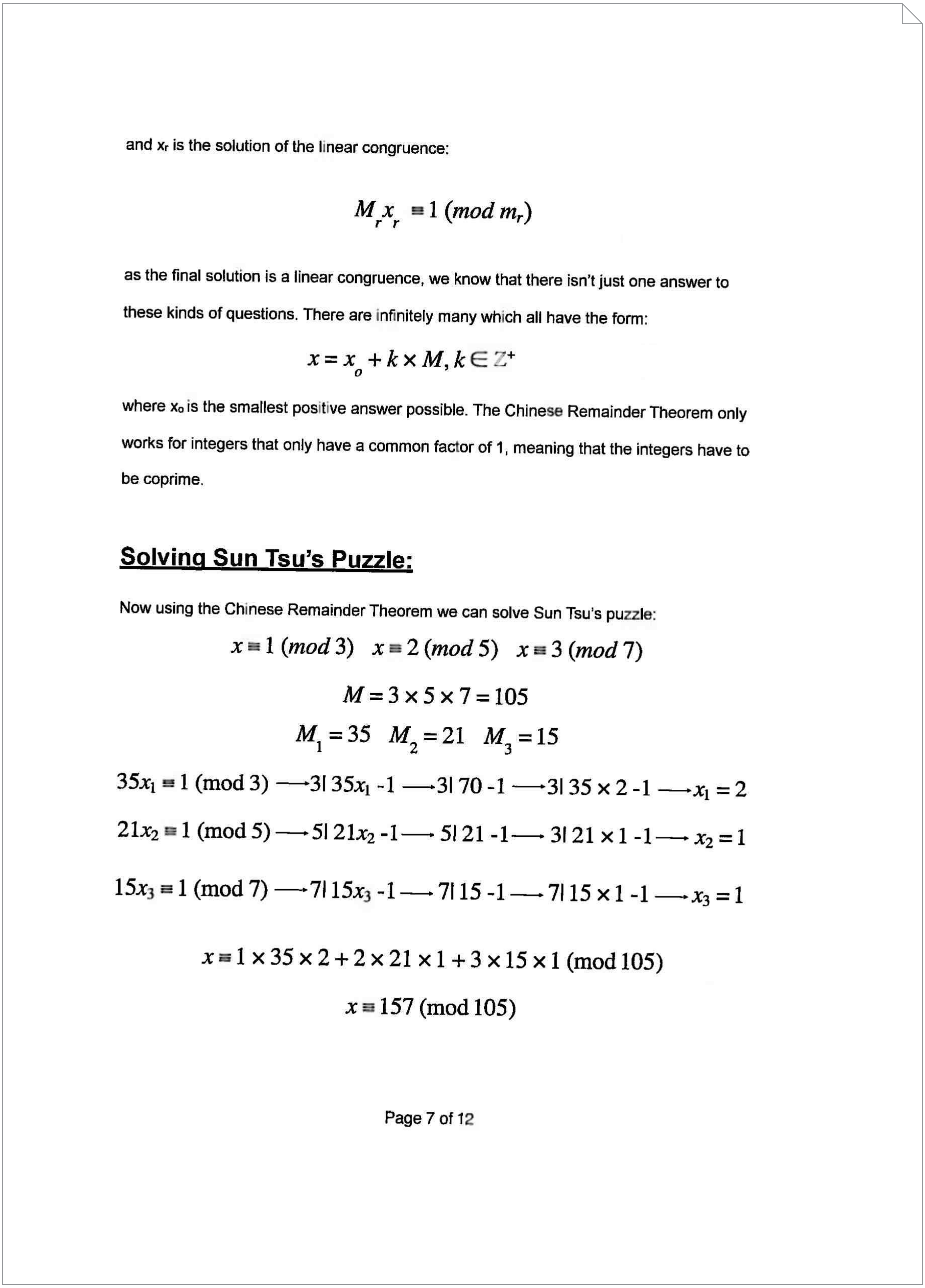
$$M = m_1 \times m_2 \times m_3 \times \ldots \times m_r$$

The Solution of the system of the linear congruences is then equal to:

$$x \equiv a_1 M_1 x_1 + a_2 M_2 x_2 + a_3 M_3 x_3 + \ldots + a_r M_r x_r\ (mod\ M)$$

To be able to do this M_r has to be calculated:

$$M_r = \frac{M}{m_r}$$



and x_r is the solution of the linear congruence:

$$M_r x_r \equiv 1 \ (mod \ m_r)$$

as the final solution is a linear congruence, we know that there isn't just one answer to these kinds of questions. There are infinitely many which all have the form:

$$x = x_o + k \times M, k \in Z^+$$

where x_o is the smallest positive answer possible. The Chinese Remainder Theorem only works for integers that only have a common factor of 1, meaning that the integers have to be coprime.

Solving Sun Tsu's Puzzle:

Now using the Chinese Remainder Theorem we can solve Sun Tsu's puzzle:

$$x \equiv 1 \ (mod \ 3) \quad x \equiv 2 \ (mod \ 5) \quad x \equiv 3 \ (mod \ 7)$$

$$M = 3 \times 5 \times 7 = 105$$

$$M_1 = 35 \quad M_2 = 21 \quad M_3 = 15$$

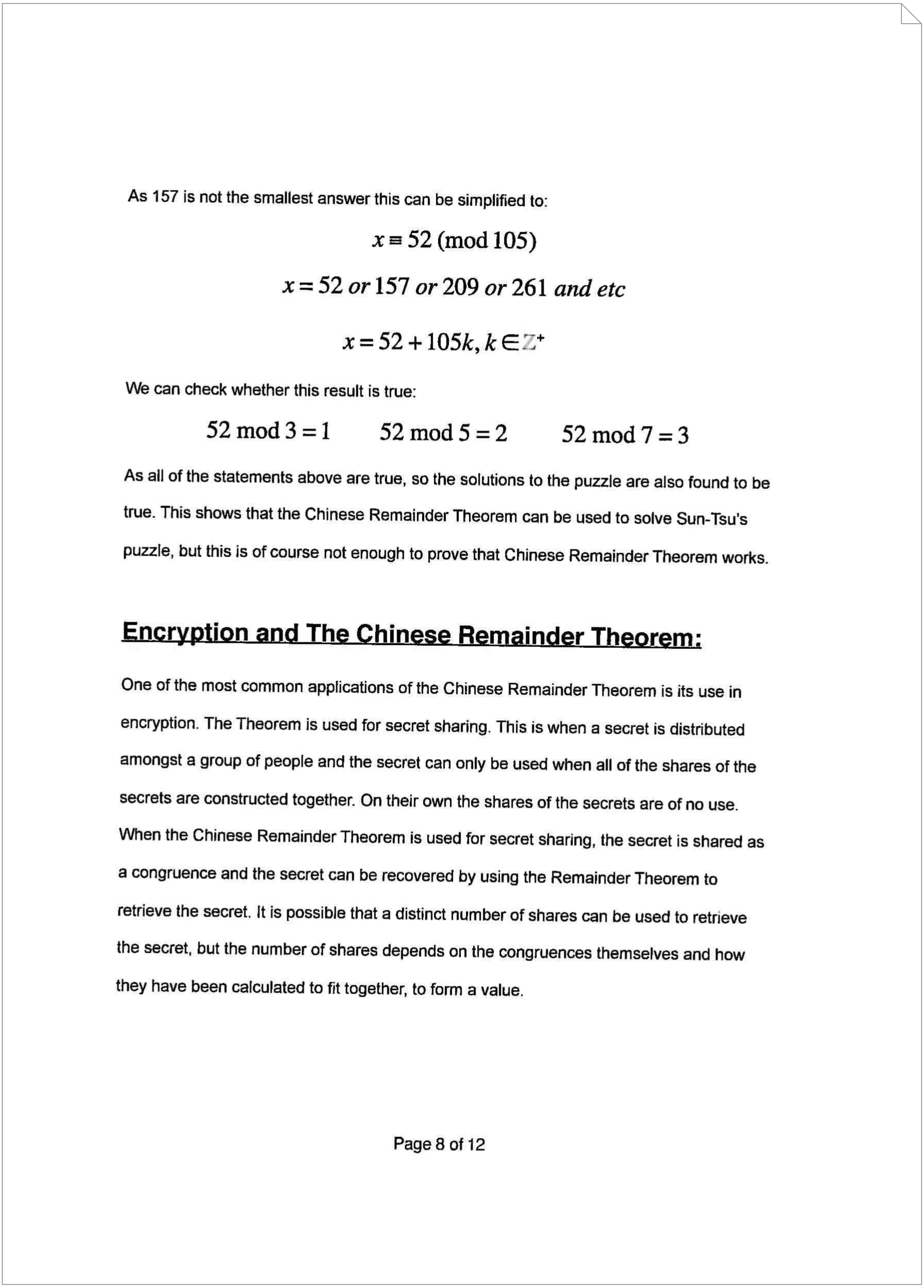
$$35x_1 \equiv 1 \ (\text{mod } 3) \longrightarrow 3 | 35x_1 - 1 \longrightarrow 3 | 70 - 1 \longrightarrow 3 | 35 \times 2 - 1 \longrightarrow x_1 = 2$$

$$21x_2 \equiv 1 \ (\text{mod } 5) \longrightarrow 5 | 21x_2 - 1 \longrightarrow 5 | 21 - 1 \longrightarrow 3 | 21 \times 1 - 1 \longrightarrow x_2 = 1$$

$$15x_3 \equiv 1 \ (\text{mod } 7) \longrightarrow 7 | 15x_3 - 1 \longrightarrow 7 | 15 - 1 \longrightarrow 7 | 15 \times 1 - 1 \longrightarrow x_3 = 1$$

$$x \equiv 1 \times 35 \times 2 + 2 \times 21 \times 1 + 3 \times 15 \times 1 \ (\text{mod } 105)$$

$$x \equiv 157 \ (\text{mod } 105)$$



As 157 is not the smallest answer this can be simplified to:

$$x \equiv 52 \ (\text{mod}\ 105)$$

$$x = 52 \ or \ 157 \ or \ 209 \ or \ 261 \ and \ etc$$

$$x = 52 + 105k, k \in \mathbb{Z}^{+}$$

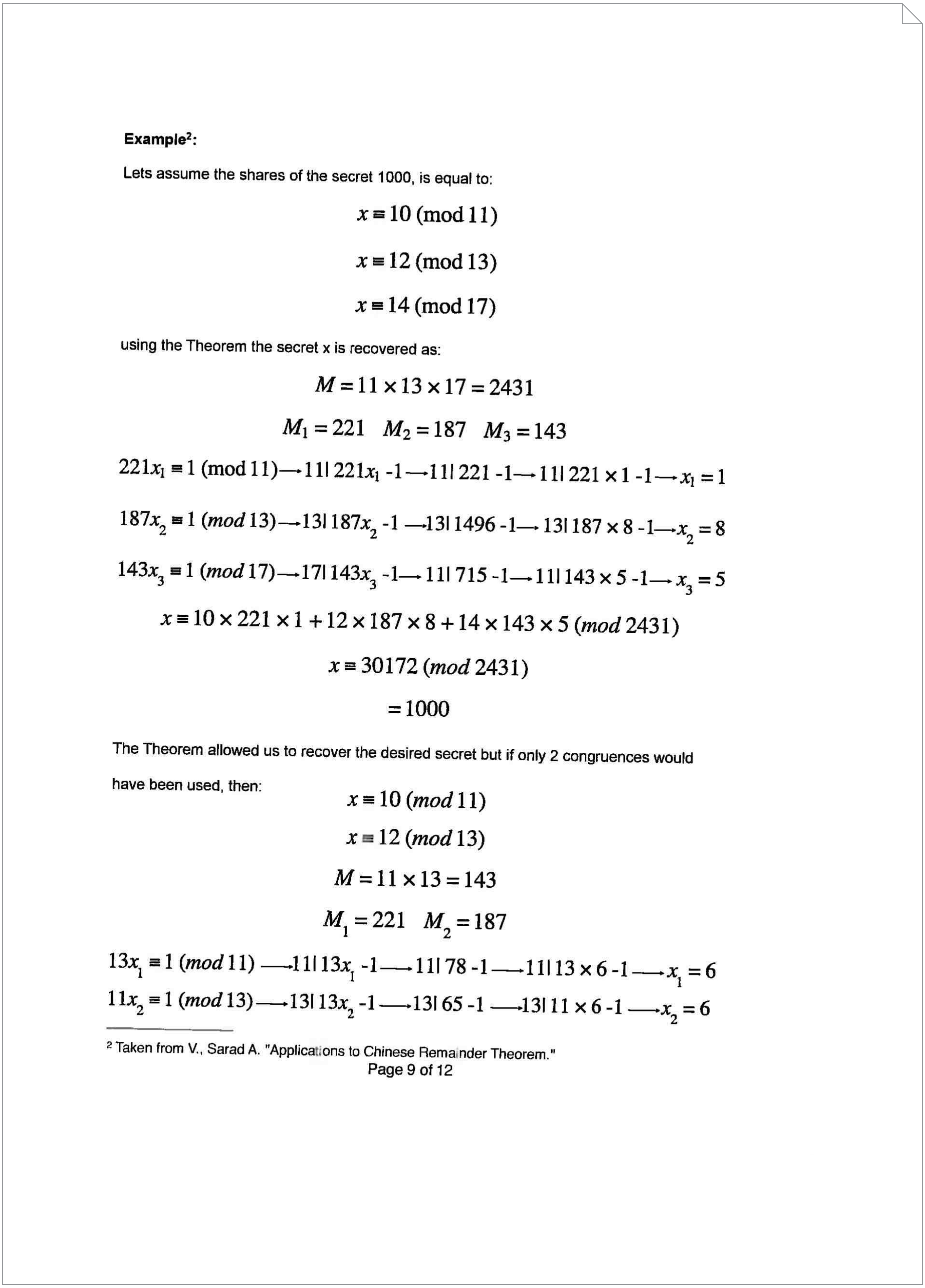
We can check whether this result is true:

$$52 \text{ mod } 3 = 1 \qquad 52 \text{ mod } 5 = 2 \qquad 52 \text{ mod } 7 = 3$$

As all of the statements above are true, so the solutions to the puzzle are also found to be true. This shows that the Chinese Remainder Theorem can be used to solve Sun-Tsu's puzzle, but this is of course not enough to prove that Chinese Remainder Theorem works.

Encryption and The Chinese Remainder Theorem:

One of the most common applications of the Chinese Remainder Theorem is its use in encryption. The Theorem is used for secret sharing. This is when a secret is distributed amongst a group of people and the secret can only be used when all of the shares of the secrets are constructed together. On their own the shares of the secrets are of no use. When the Chinese Remainder Theorem is used for secret sharing, the secret is shared as a congruence and the secret can be recovered by using the Remainder Theorem to retrieve the secret. It is possible that a distinct number of shares can be used to retrieve the secret, but the number of shares depends on the congruences themselves and how they have been calculated to fit together, to form a value.



Example[2]:

Lets assume the shares of the secret 1000, is equal to:

$$x \equiv 10\ (\text{mod}\,11)$$

$$x \equiv 12\ (\text{mod}\,13)$$

$$x \equiv 14\ (\text{mod}\,17)$$

using the Theorem the secret x is recovered as:

$$M = 11 \times 13 \times 17 = 2431$$

$$M_1 = 221 \quad M_2 = 187 \quad M_3 = 143$$

$$221x_1 \equiv 1\ (\text{mod}\,11) \longrightarrow 11|\,221x_1\ \text{-}1 \longrightarrow 11|\,221\ \text{-}1 \longrightarrow 11|\,221 \times 1\ \text{-}1 \longrightarrow x_1 = 1$$

$$187x_2 \equiv 1\ (mod\,13) \longrightarrow 13|\,187x_2\ \text{-}1 \longrightarrow 13|\,1496\ \text{-}1 \longrightarrow 13|\,187 \times 8\ \text{-}1 \longrightarrow x_2 = 8$$

$$143x_3 \equiv 1\ (mod\,17) \longrightarrow 17|\,143x_3\ \text{-}1 \longrightarrow 11|\,715\ \text{-}1 \longrightarrow 11|\,143 \times 5\ \text{-}1 \longrightarrow x_3 = 5$$

$$x \equiv 10 \times 221 \times 1 + 12 \times 187 \times 8 + 14 \times 143 \times 5\ (mod\,2431)$$

$$x \equiv 30172\ (mod\,2431)$$

$$= 1000$$

The Theorem allowed us to recover the desired secret but if only 2 congruences would have been used, then:

$$x \equiv 10\ (mod\,11)$$

$$x \equiv 12\ (mod\,13)$$

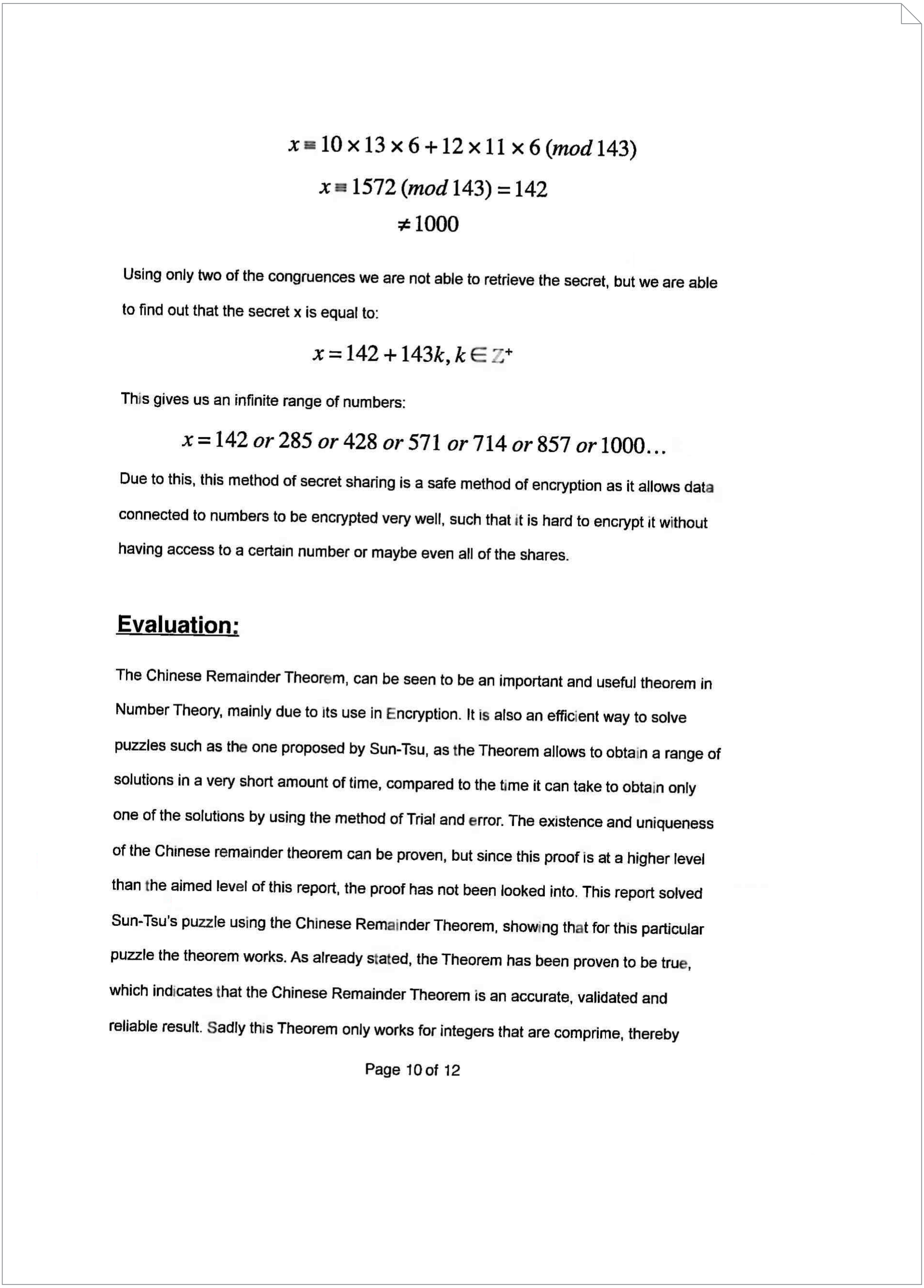
$$M = 11 \times 13 = 143$$

$$M_1 = 221 \quad M_2 = 187$$

$$13x_1 \equiv 1\ (mod\,11) \longrightarrow 11|\,13x_1\ \text{-}1 \longrightarrow 11|\,78\ \text{-}1 \longrightarrow 11|\,13 \times 6\ \text{-}1 \longrightarrow x_1 = 6$$

$$11x_2 \equiv 1\ (mod\,13) \longrightarrow 13|\,13x_2\ \text{-}1 \longrightarrow 13|\,65\ \text{-}1 \longrightarrow 13|\,11 \times 6\ \text{-}1 \longrightarrow x_2 = 6$$

[2] Taken from V., Sarad A. "Applications to Chinese Remainder Theorem."



$$x \equiv 10 \times 13 \times 6 + 12 \times 11 \times 6 \ (mod\ 143)$$

$$x \equiv 1572 \ (mod\ 143) = 142$$

$$\neq 1000$$

Using only two of the congruences we are not able to retrieve the secret, but we are able to find out that the secret x is equal to:

$$x = 142 + 143k, k \in Z^{+}$$

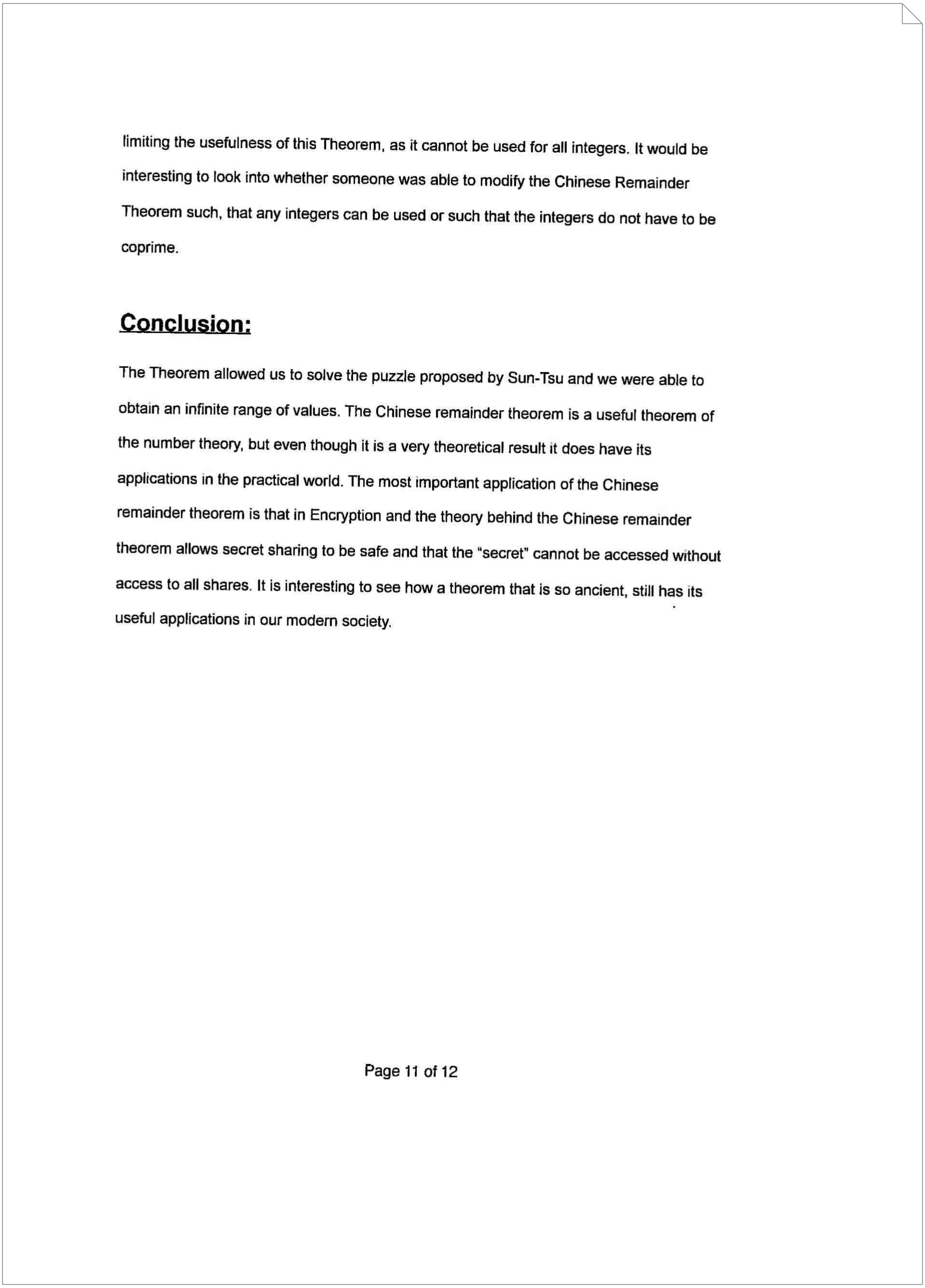
This gives us an infinite range of numbers:

$$x = 142 \ or \ 285 \ or \ 428 \ or \ 571 \ or \ 714 \ or \ 857 \ or \ 1000\ldots$$

Due to this, this method of secret sharing is a safe method of encryption as it allows data connected to numbers to be encrypted very well, such that it is hard to encrypt it without having access to a certain number or maybe even all of the shares.

Evaluation:

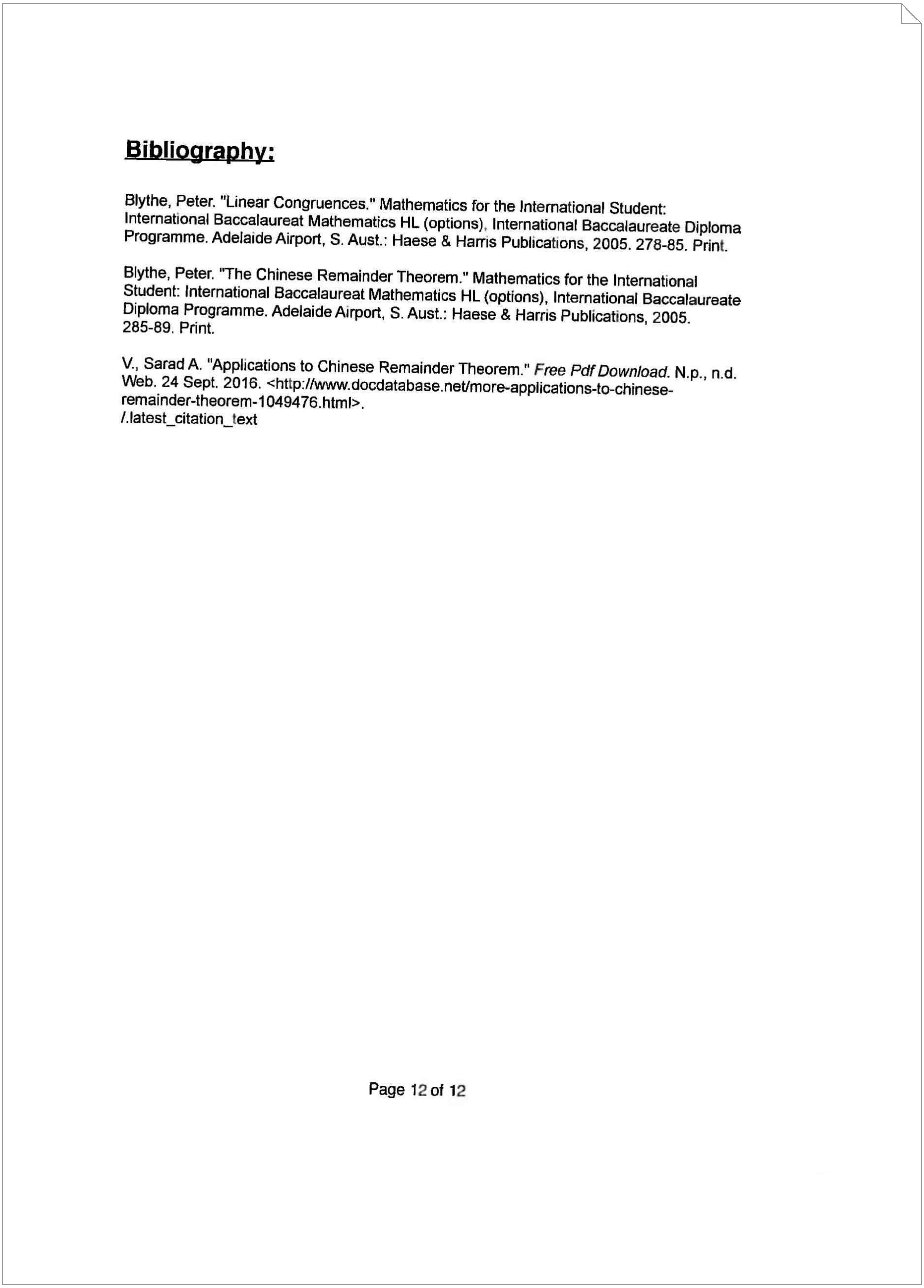
The Chinese Remainder Theorem, can be seen to be an important and useful theorem in Number Theory, mainly due to its use in Encryption. It is also an efficient way to solve puzzles such as the one proposed by Sun-Tsu, as the Theorem allows to obtain a range of solutions in a very short amount of time, compared to the time it can take to obtain only one of the solutions by using the method of Trial and error. The existence and uniqueness of the Chinese remainder theorem can be proven, but since this proof is at a higher level than the aimed level of this report, the proof has not been looked into. This report solved Sun-Tsu's puzzle using the Chinese Remainder Theorem, showing that for this particular puzzle the theorem works. As already stated, the Theorem has been proven to be true, which indicates that the Chinese Remainder Theorem is an accurate, validated and reliable result. Sadly this Theorem only works for integers that are comprime, thereby



limiting the usefulness of this Theorem, as it cannot be used for all integers. It would be interesting to look into whether someone was able to modify the Chinese Remainder Theorem such, that any integers can be used or such that the integers do not have to be coprime.

Conclusion:

The Theorem allowed us to solve the puzzle proposed by Sun-Tsu and we were able to obtain an infinite range of values. The Chinese remainder theorem is a useful theorem of the number theory, but even though it is a very theoretical result it does have its applications in the practical world. The most important application of the Chinese remainder theorem is that in Encryption and the theory behind the Chinese remainder theorem allows secret sharing to be safe and that the “secret” cannot be accessed without access to all shares. It is interesting to see how a theorem that is so ancient, still has its useful applications in our modern society.



Bibliography:

Blythe, Peter. "Linear Congruences." Mathematics for the International Student: International Baccalaureat Mathematics HL (options), International Baccalaureate Diploma Programme. Adelaide Airport, S. Aust.: Haese & Harris Publications, 2005. 278-85. Print.

Blythe, Peter. "The Chinese Remainder Theorem." Mathematics for the International Student: International Baccalaureat Mathematics HL (options), International Baccalaureate Diploma Programme. Adelaide Airport, S. Aust.: Haese & Harris Publications, 2005. 285-89. Print.

V., Sarad A. "Applications to Chinese Remainder Theorem." *Free Pdf Download*. N.p., n.d. Web. 24 Sept. 2016. <http://www.docdatabase.net/more-applications-to-chinese-remainder-theorem-1049476.html>.
/.latest_citation_text