**Assignment – 1**

**Computer Security - 1**

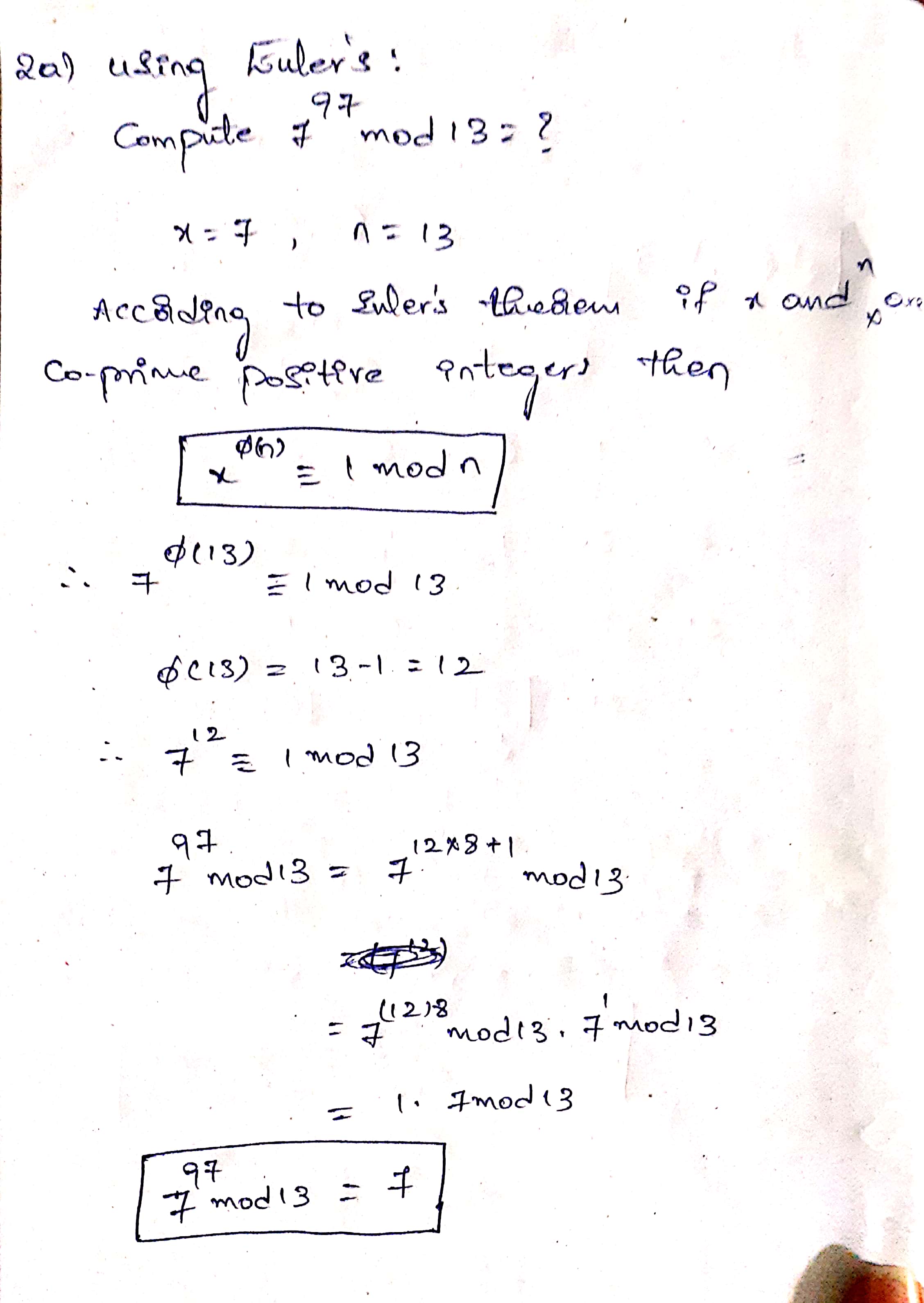
**Q1) Explain briefly why the only secret in a secure communication system is the encryption/decryption key and not the encryption/decryption algorithm.**

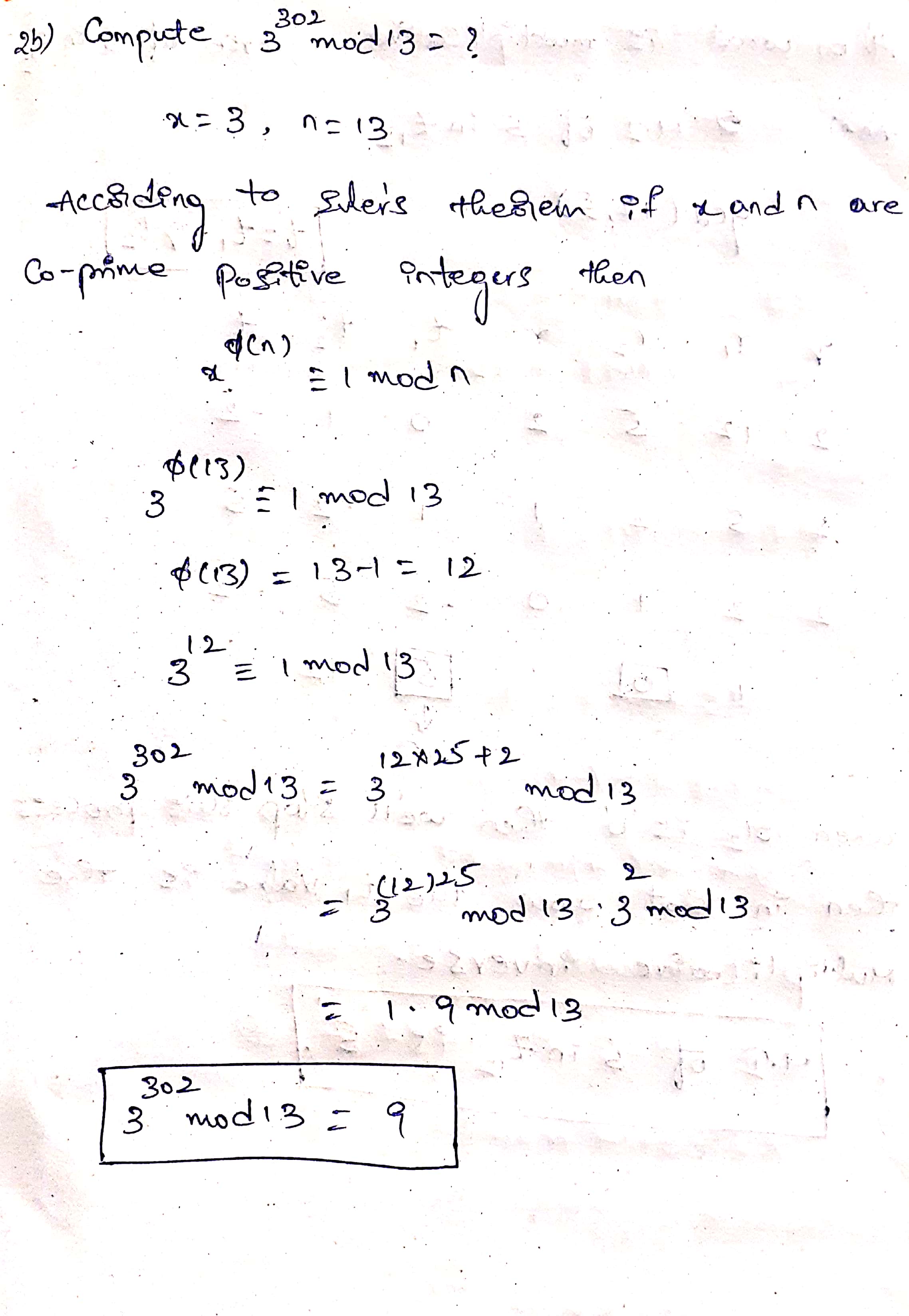
Ans) According to the secure communication system, the algorithm is the process of implementing some steps (for example, Simply algorithm means a type of source code), which most of the persons are aware of that process. So there is no point in maintaining the algorithm as a secret in the communication. Also, by knowing the process of algorithm, the hackers can easily hack the information and misuse it. But when it comes to the keys, the communication will be very secure. We can encrypt the message using our public keys and the receiver will decrypt it by using his own private key, Others will not have any idea of the public and private keys. So in this case it’ll be very difficult to the hackers to steal the encrypted information. This is why we use keys as a secret in the secure communication.

**Q2) Using Euler’s:**

**(a) Compute 797 mod 13=?**

**(b) compute 3302 mod 13=?**





**Q3. (a) Briefly describe the key expansion algorithm. What is AES encryption? How does it**

**work? Give few examples.**

Ans) Firstly, AES means Advanced Encryption Standard. Most of the drawbacks in the DES is addressed in the AES. It is widely used encryption algorithm.

**Key Expansion Algorithm:**

Originally, we have the key length of the 128 bits or 192 or 256 bits in the AES, for each bits we have corresponding rounds and its keys. By taking the initial key we’ll generate the remaining keys. That is called the key expansion. Firstly, we will represent the bytes in the form of matrix. We will convert those bytes to words. By considering the first set of words we’ll calculate the remaining words too by using the simple XOR with the function g. The function g will have the following steps. Rotwords, which means 1 bit rotation of words. Then subwords perform the substitution using the S-box. The outputs of these two steps will be XOR with the round constant. This is the brief about the key expansion algorithm.

**What is AES Encryption:**

AES means Advanced Encryption Standard. It is a modern symmetric algorithm, which means the encryption and decryption will be done using a single key. AES works on the block cipher technique. The size of the plain text and the cipher text will be same. AES encryption is comprises with the multiple rounds of encryption which makes difficult to steal the information. The simple concept is we’ll encrypt the plain text and transforms it into cipher text and on the otherhand the decryption will decrypt the cipher text and gets the original message.

**Working of AES:**

1. Initially, we take the plain text and add cipher key to that using XOR operation and then we go through with the N-1 rounds to extend the key and to encrypt the data.
2. **Sub Bytes:** Here, take the block of the plain text and using the S-boxes we’ll substitute the each bytes with the blocks in the look-up table. Repeat this for all blocks in the plaintext.
3. **Shift Rows:** Each row we’ll shift the block with the 1 hexadecimal place and so on…. For each row we’ll rotate the blocks for row no.of times, i.e., for row2 we rotate the blocks 2 places right.
4. **Mix Columns:** In this step, we’ll mix up the columns. Take a column of data and then multiply it with some specific matrix. Do this for each column.
5. **RoundKey:** Adding the round key, it is the value produced in the each round. Now XOR this round key with each column of our block. In the each round the round key will changes.i.e., the round key is the computed value based on the previous round.
6. Do this process for all the rounds and finally we’ll get the cipher text.

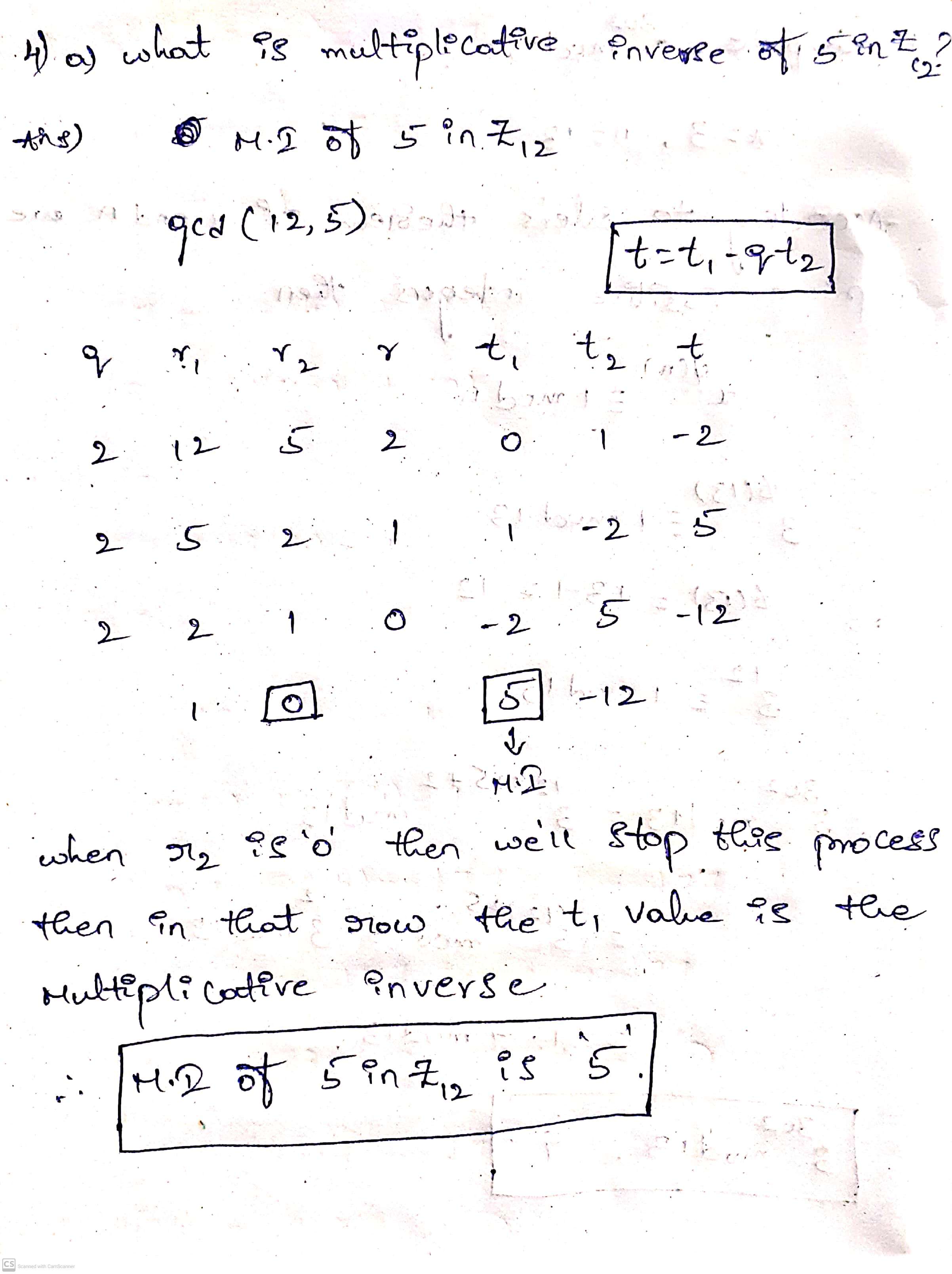
**Examples of AES:**

Now-a-days AES is widely used all types of communications like Safe Browsing, General file encryption and wireless security like Wifi etc…

**(b) Compare AES, DES and Triple DES ?**

|  |  |  |
| --- | --- | --- |
| **DES** | **3DES** | **AES** |
| DES stands for Data Encryption Standard. | 3DES is using DES three times. | AES stands for Advanced Encryption Standard. |
| Developed by IBM in the year 1997. | Developed in the year 1998. | Proposed by the NIST in the year 2001. |
| It uses the Encryption key length of 56 bits. | Encryption Key length is 168 bits. | Encryption key length is 128, 192, 256 bits. |
| Block size is 64 bits | Block size is 64 bits | Block size is 128 bits |
| Security is very low, in 1998 DES encrypted message is cracked in 3 days | Security is moderate, Not as good as AES. | Security is very high. |
| Performance is moderate. | Performance is very low because of it’s complex structure. | Performance is high. |

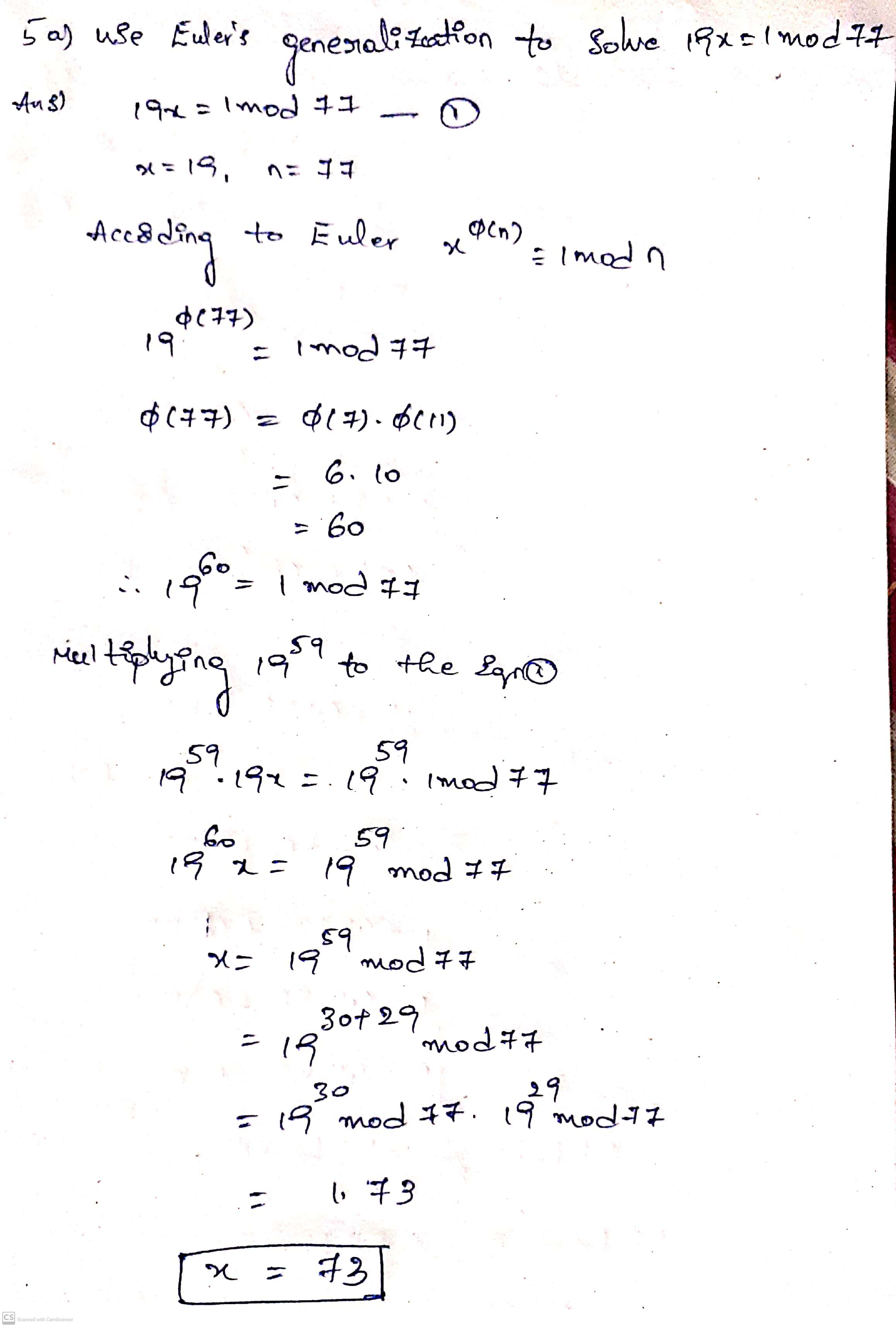
**Q4) (a) what is multiplicative inverse of 5 in Z12?**

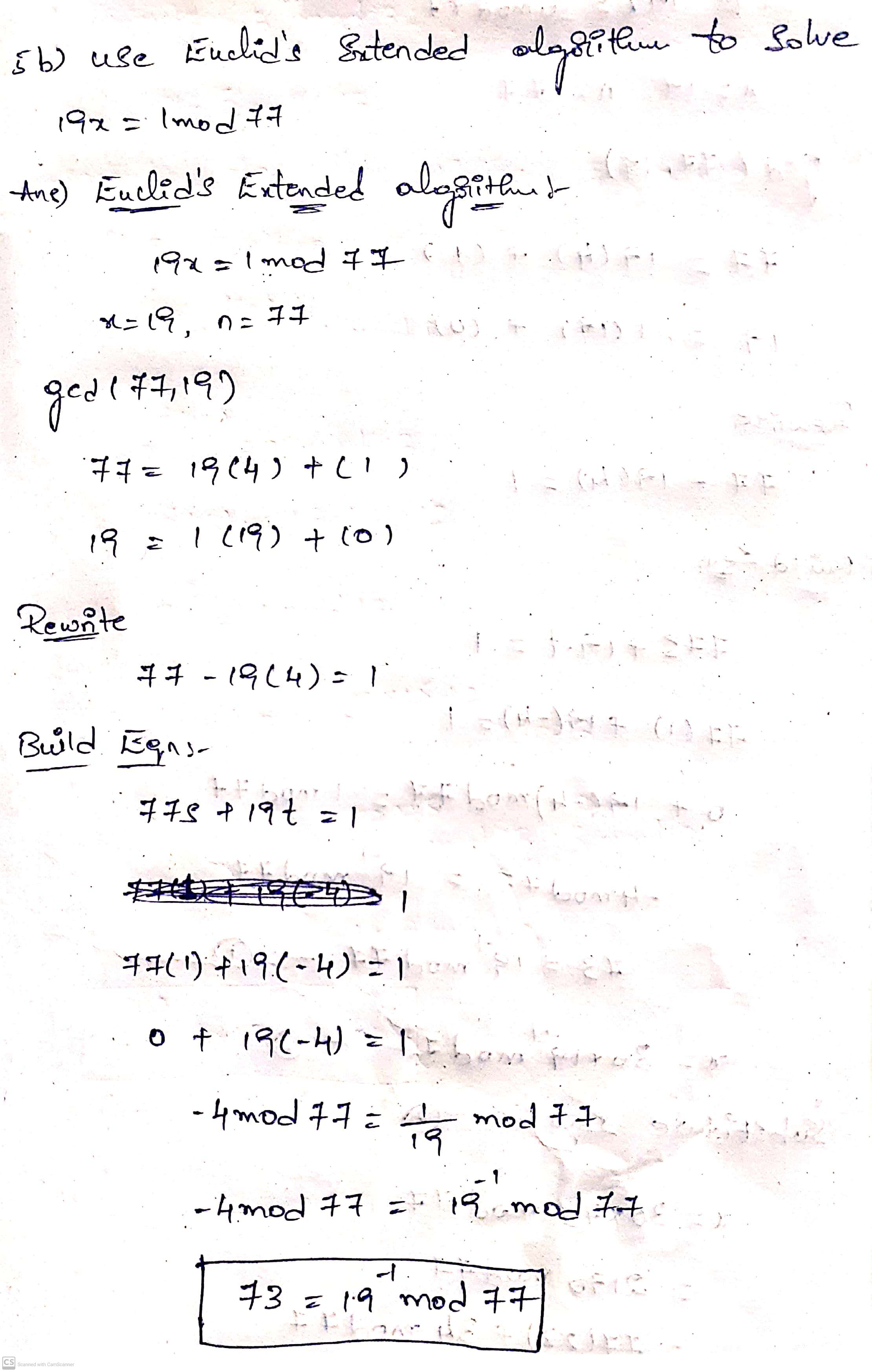


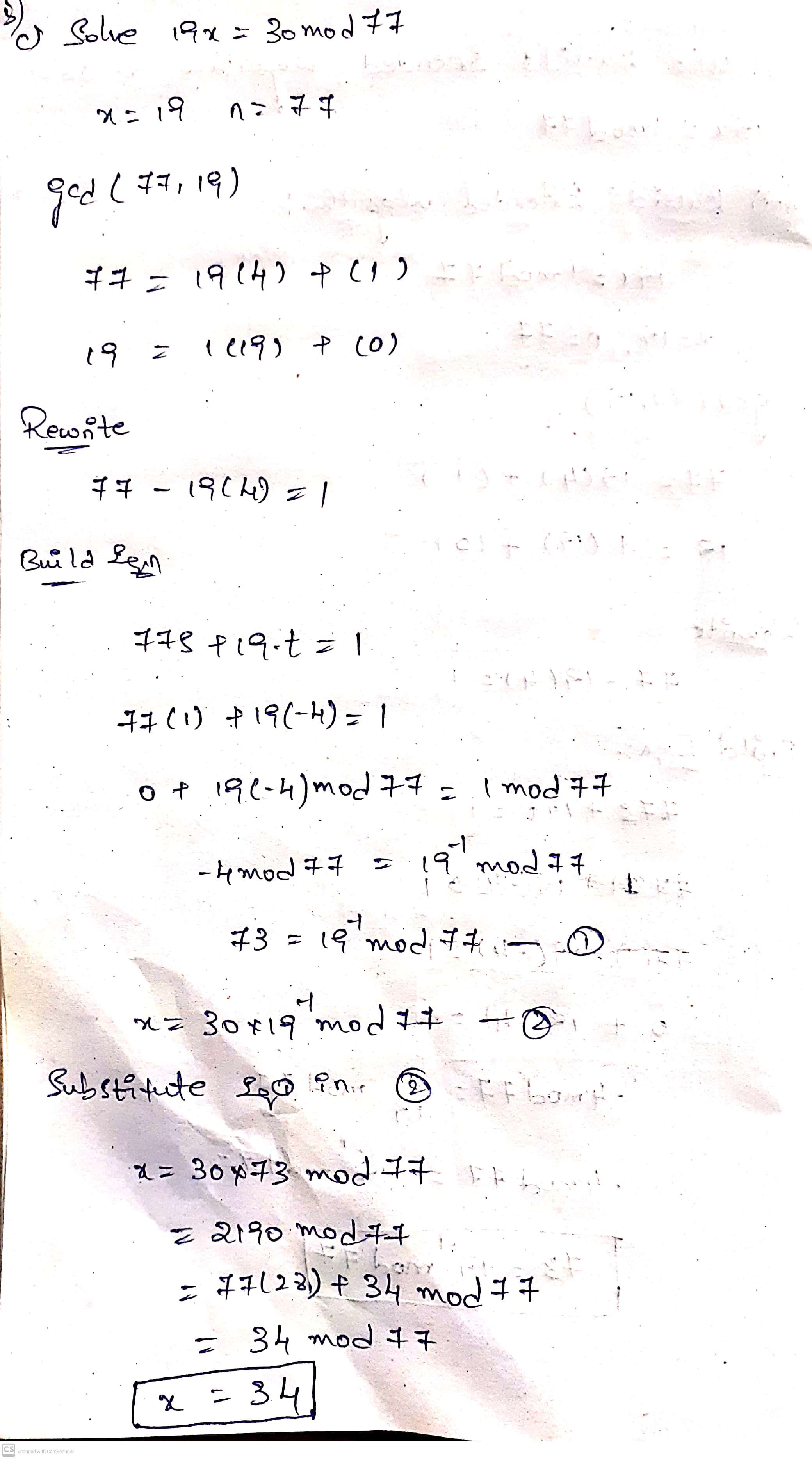
**Q5) (a) Use Euler’s generalization to solve 19x =1 mod 77.**

**(b) Use Euclid’s extended algorithm to solve 19x =1 mod 77.**

**(c) Solve 19x =30 mod 77.**

****

****

****