PROJECTED WRITTEN NOTES FROM THE M325K LECTURE ON THURSDAY, APRIL 4, 2024, on Section 8.4 (Epp's 4th Edition) — SOLVING SIMPLE CONGRUENCES, Computer ENCRYPTION, ENCRYPTION AND DECRYPTION IN THE RSA Crypto-System

CLASS #22

Unless otherwise stated, all variables represent integers and $n \geq 1$

Def's: A Simple Congruence is a statement of congruence that involves a variable,

e.g. $Bx \equiv D \pmod{n}$ such that $\gcd(B, n) = 1$

Ex: $7x \equiv 2 \pmod{64}$ and $\gcd(7, 64) = 1$

$[64 = 2^6,\ 7 = 7^1]$

So, "$7x \equiv 2 \pmod{64}$" is a Simple Congruence.

A solution of "$Bx \equiv D \pmod{n}$" is a particular integer x_0 such that "$Bx_0 \equiv D \pmod{n}$" is a true statement.

For example: $x_0 = 174$ is a solution of "$7x \equiv 2 \pmod{64}$".

Since $\underset{a}{(7 \times 174)} \underset{=}{=} \underset{n\ k\ +\ b}{(64)(9) + 2}$, $(7 \times 174) \equiv 2 \pmod{64}$, by Thm 8.4.1.

FACT: If x_0 is a solution of "$Bx \equiv D \pmod{n}$"
and if $x_1 \equiv x_0 \pmod{n}$,
then x_1 is also a solution of "$Bx \equiv D \pmod{n}$"

Proof: Left as an exercise. (Apply Thm 8.4.3)

Ex: Recall that $x_0 = 174$ is a solution of $7x \equiv 2 \pmod{64}$.

$x_1 = 110 = 174 - 64$, ~~so~~ and, $\underset{a}{174} = \underset{n}{64} \times \underset{k}{1} + \underset{b}{110}$

So, $110 \equiv 174 \pmod{64}$ by Thm 8.4.3 and Symmetry.

$x_1 = 110$ is also a solution of the congruence.

Check: $\underset{a}{7 \times 110} = \underset{n \cdot k}{(64)(12)} + \underset{b}{2}$,

so $7 \times 110 \equiv 2 \pmod{64}$. ✓

2

FACT (Thm (N)1554):

For any integer l, $l \equiv (l \bmod n) \pmod{n}$

Proof outline: By the Q-R Thm, there exists an integer q such that

$l = n \cdot q + (l \bmod n)$

$a = n \cdot k + b$

So, $l \equiv (l \bmod n) \pmod{n}$ by Thm. 8.4.1.

Ex: $52 = 6 \times 8 + 4$ and $0 \leq 4 < 6$

$a = n * k + b$

$\therefore (52 \bmod 6) = 4$.

$52 \equiv 4 \pmod{6}$ by Thm 8.4.1.

$52 \equiv (52 \bmod 6) \pmod{6}$

FACT: If x_0 is any one solution of "$Bx \equiv D \pmod{n}$", then the "$\equiv \pmod{n}$" Equivalence Class $[x_0]_n$ is the solution set for "$Bx \equiv D \pmod{n}$"

Problem: Solve the Simple Congruence "$7x \equiv 2 \pmod{64}$".

Sol'n: From earlier, we saw that $x_0 = 174$ is a solution of "$7x \equiv 2 \pmod{64}$"

The least non-negative solution of this congruence is $(174 \bmod 64)$.

Since $(174 \bmod 64) = 46$ since $174 = (64)(2) + 46$ and $0 \le 46 < 64$.

So 46 is the least non-negative solution of "$7x \equiv 2 \pmod{64}$".

$174 \equiv 46 \pmod{64}$

FACT If x_0 is any one solution of "$Bx \equiv D \pmod{n}$", then $x_1 = (x_0 \bmod n)$ is the least non-negative sol'n of this congruence.

Sol'n (cont.)

$[46]_{(\equiv (\text{mod } 64))} = \{ \ldots, -18, 46, 110, 174, \ldots \} = [174]$

is the Solution Set for "$7x \equiv 2 \pmod{64}$"

Solving Simple Congruences

Suppose "$Bx \equiv D \pmod n$" is a congruence such that $\gcd(B, n) = 1$, i.e. it is a Simple Congruence.

then there exists an integer A such that A is a (mod n) Inverse of B, i.e.,

$BA \equiv 1 \pmod n$.

Let $x_0 = AD$.

We show that $x_0 = AD$ is one solution of the this congruence

$Bx_0 = B(AD) = (BA)D \equiv 1 \cdot D \equiv D \pmod n$

$Bx_0 \equiv D \pmod n$, by Transitivity,

So $x_0 = AD$ is one solution.

The Solution set for "$Bx \equiv D \pmod n$" is

$[x_0] = [AD]_{\equiv (\text{mod } n)}$

$\forall$ $r = (x_0 \text{ mod } n)$, $[x_0] = [AD] = [(AD \text{ mod } n)]$.

$Bx \equiv D \pmod{n}$

Problem: Solve the Congruence $99x \equiv 5 \pmod{13}$

Sol$_n$: $99 = 3^2 \times 11$, $13 = 13^1$, $\gcd(99, 13) = 1$

This is a simple Congruence.

With some effort, we can discover that

$A = 31$ is a (mod 13) inverse of 99

Verify this:

$$(31)(99) = (13)(286) + 1$$
$$a \qquad\quad n \quad k \qquad + b$$

$$(31)(99) \equiv 1 \pmod{13}$$

$x_0 = AD = (31)(5) = 155$ is one solution of this congruence.

$(155 \bmod 13) = 12$. $\therefore$ 12 is the least non-negative sol^n of "$99x \equiv 5 \pmod{13}$"

The Solution Set of this congruence is

$[12] = \{ \ldots -1, 12, 25, \ldots, 155, \ldots \} = [155]$
($\equiv \pmod{13}$)

Cryptography

How can we send information over a computer network encrypted so that secrecy of the content is assured ?

Unfortunately, total 100 % assurance is impossible, but there are encryption methods for which the task of breaking their codes is not feasible in the sense that it would take a ridiculously long time and cost billions of dollars in computer usage to break these codes.

Terminology: Message, Encoding of the message, Plaintext after the encoding, Encryption of the plaintext, Ciphertext after the encryption of the plaintext, Encryption Method, Cipher, Caesar Cipher, Encryption Key, Deciphering or Decryption of the ciphertext to recover the plaintext, Decryption Method, Decryption Key

These terms will be discussed in the context of a Caesar Cipher (defined below) which encodes the 26 letters of the alphabet as follows:

Letter:	A	B	C	D	. . .	X	Y	Z
Letter Code:	01	02	03	04	. . .	24	25	00

The Message to be encrypted is the message content in human-readable form consisting of a series of characters, which we may consider to be words: Example: " H I ".

In a computer, these characters are not stored in the form of "letters" but in a machine-readable form with each letter represented by its numeric code. The storing of the codes of the characters of the message in the computer is the encoding of the message , and the list of numeric codes which ultimately represent the particular letters of the message in numeric form is called the Plaintext of the message.

Example: Using the encoding method described above, the message " H I ", after its encoding, is stored in the computer as "08 09" . Thus, the Plaintext of the message " H I " is the list "08 09".

This list of numeric codes will be transformed according to an Encryption Method (also called a Cipher) into a different list of numbers and this transformation is called the encryption of the plaintext or the encryption of the message. The new list resulting from encryption process is called the Ciphertext of the the message.

For example: In the encryption formula that follows, "M" will represent the plaintext encoding of one letter and "C" will represent the encrypted ciphertext corresponding to the plaintext M. Let K be any integer with $0 \leq K \leq 25$. A Caesar Cipher is one for which the formula for encryption is

$$C = ((M + K) \bmod 26),$$ (assuming that only 26 symbols are possible for transmission).

In this example, the value that we will use for the parameter K is $K = 3$.
Thus, the formula for this encryption method is : $C = ((M + 3) \bmod 26)$.
Thus, this message is encoded and then encrypted as follows:

Message	H	I	
Encoding:	08	09	This is the plaintext M of the message.
	↓	↓	Calculations:
			$C = ((08 + 3) \bmod 26) = (11 \bmod 26) = 11$
			$C = ((09 + 3) \bmod 26) = (12 \bmod 26) = 12$
Encryption:	11	12	This is the ciphertext C of the message.

The ciphertext is the content of the message which is sent over the computer network.
The value of the parameter K (here, K = +3) is called the Encryption Key. Knowledge of the encryption key is necessary for the encryption process to be accomplished correctly.

After the ciphertext of the message has been received, this list of numbers is transformed into the original plaintext of the message using a Deciphering Method (also called a Decryption Method). To decipher the ciphertext for this message, the decryption formula used is: $M = (C - 3) \bmod 26$.

Data received:	11	12	This is the ciphertext C of the message.
	↓	↓	Calculations:
			$M = ((11 - 3) \bmod 26) = (8 \bmod 26) = 8$
			$M = ((12 - 3) \bmod 26) = (9 \bmod 26) = 9$
Decryption:	08	09	This is the plaintext M of the message.
Decoding:	H	I	This is the original message decrypted and decoded.

The value -3 is called a Decryption Key and knowledge of the particular decryption key is necessary for the decryption process to be accomplished correctly. Here, it is not too difficult to derive knowledge of the decryption key from knowledge of the encryption key.

A Private-Key Crypto-system is one in which both the sender and receiver know both the encryption key and the decryption key, and from knowledge of the value of one key, it is not difficult to derive the value of the other key (as in +3 and –3).

A Public-Key Crypto-system is one in which only the receiver knows the decryption key. The encryption key is made public and anyone can know it and use it to send encrypted messages to the receiver. Only the receiver knows the decryption key. The decryption key is relatively safe because the time and money it would take to derive the decryption key from encryption key is so great that it is not feasible to try.

The RSA Crypto-system is a public-key cryptosystem, developed in the 1970s by Ronald Rivest, Adi Shamir, and Leonard Adleman. The details of this encryption/decryption method are presented below.

There are two positive integer public encryption keys, here represented by N and e. The integer N is the product of two prime numbers, that is, $N = p \cdot q$ where p and q are prime numbers, each with 200 or more digits in its decimal representation, so N has over 400 digits in its representation. The number N is published, but not its factorization $p \cdot q$. Knowledge of these prime factors is necessary for deciphering the ciphertext of a message encrypted with the RSA crypto-system.

As the number of digits in an integer increases, the complexity of the problem of factoring that integer explodes and it becomes extremely difficult and expensive to solve that problem. This difficulty makes this encryption method very difficult to break (though not impossible).

The other encryption key, e, is a positive integer which is relatively prime to the integer $(p-1)\cdot(q-1)$, that is, e is a positive integer such that $\gcd(\, e \, , \, (p-1)\cdot(q-1)\,) = 1$.

Once the integers N and e have been selected, the RSA Encryption Formula is as follows:
For message plaintext M, the ciphertext C corresponding to the plaintext is computed by the formula:

RSA Encryption Formula: $$C = \left(M^{e} \bmod p \cdot q \right) .$$

The RSA Decryption Method has two decryption keys, N and d. The value of N is the same product of two primes as that used in the encryption of the message.

The integer d is a (mod $(p-1)\cdot(q-1)$) inverse of e.

Thus, $N = p \cdot q$, as before, and d is a positive integer such that $e \cdot d \equiv 1 \pmod{(p-1)\cdot(q-1)}$.

Once the value of d (as an inverse of e) has been selected, the RSA Decryption Formula is as follows:

For ciphertext C , the plaintext M corresponding to the ciphertext is computed by the formula:

RSA Decryption Formula: $M = \left(C^{d} \bmod p \cdot q \right)$.

Example: Using the same message " H I " with the same encoding " 08 09 ", we will perform an RSA encryption and the corresponding RSA decryption of the message. For simplicity of calculation, the values of the primes p and q and the consequent keys N, e, and d will be so small as not to be practical for actual use, but the principles used here are the same as those used in the actual application of this crypto-system.

Let $p = 5$ and $q = 11$.

Let $N = p \cdot q = 55$. Here, $(p-1)\cdot(q-1) = (4)(10) = 40 = 2^3\, 5^1$.

Let $e = 3$. We require that $\gcd(e, (p-1)\cdot(q-1)) = 1$, which is true here since $\gcd(3, 40) = 1$.

Encryption:

Message : H I

Plaintext M : 08 09

$\downarrow$ $\downarrow$

Ciphertext C : 17 14

Calculations:

$C = \left((08)^3 \bmod 55 \right) = (512 \bmod 55) = 17$ when M = " 08 "

$C = \left((09)^3 \bmod 55 \right) = (729 \bmod 55) = 14$ when M = " 09 "

Decryption:

We find a decryption key d by determining a (mod 40) inverse of $e = 3$:

First, perform the Euclidean Algorithm to show that $\gcd(3, 40) = 1$, and then express 1 as $1 = (3)(s) + (40)(t)$. This can be accomplished with the first division:

$$1 = (3)(-13) + (40)(1) .$$

$x = -13$ is a (mod 40) inverse of 3, however, to have a *positive* value for d, we add 40.

Thus, $d = 27 = (-13) + 40$ is the decryption key we will use.

To check that d is a (mod 40) inverse of 3, verify that $(3)(27) \equiv 1 \pmod{40}$.

Calculations:

Ciphertext C : 17 14

$\downarrow$ $\downarrow$

Plaintext M : 08 09

$M = \left((17)^{27} \bmod 55 \right) = 8$ when C = " 17 "

$M = \left((14)^{27} \bmod 55 \right) = 9$ when C = " 14 "

According to the Letter Codes, the message is " H I " .

RSA DECRYPTION EXAMPLE

Using ENCRYPTION Keys: $N = pq = 713$
where $p = 23$ and $q = 31$.

(so, $(p-1)(q-1) = 22 \times 30 = 660$)

The other Key e = any positive integer that is relatively prime to $(p-1)(q-1)$.

For instance, we can use $e = 43$ since $\gcd(43, 660) = 1$.
43 is prime and $660 = 20 \times 30$.

Task: Decrypt the received ciphertext $C = 129$.

Decryption Rule: Plaintext $M = C^d \bmod pq$
where
d is an inverse of e (mod $(p-1)(q-1)$).

Here, we can use $d = 307$ since 307 is a (mod 660) inverse of $e = 43$.

That is, $(43)(307) \equiv 1 \pmod{660}$

Sol'n: $M = (129)^{307} \bmod 713$

$307 = 256 + 32 + 16 + 2 + 1$

$(129)^{307} = (129)^{256} \cdot (129)^{32} \cdot (129)^{16} \cdot (129)^{2} \cdot (129)^{1}$

See the report from the Power Calculator.

$(129)^{307} \equiv (315)\cdot(87)\cdot(284)(242)(129) \pmod{713}$

$(315)\cdot(87) \equiv 311 \pmod{713}$

$(284)\cdot(242) \equiv 280 \pmod{713}$

$(280)\cdot(129) \equiv 470 \pmod{713}$

$(311)\cdot(470) \equiv 5 \pmod{713}$

$\therefore (129)^{307} \equiv 5 \pmod{713}$ and $0 \leq 5 < 713$.

$\therefore$ By Thm(W13)6, $\left((129)^{307} \bmod 713\right) = 5$.

The message sent and received is "E".