CSC281: Discrete Math for Computer Science

Computer Science Department — First Semester 1442

King Saud University — Tutorial 8: Number Theory

Question 1. Consider the following system of linear congruences:

$x \equiv 1 (mod\ 2)$

$x \equiv 2 (mod\ 3)$

$x \equiv 3 (mod\ 5)$

$x \equiv 4 (mod\ 11)$

Solve it using the construction in the proof of the Chinese remainder theorem.

Question 2. Find the discrete logarithms of 18 and 6 to the base 2 modulo 19.

Q2

If $r^e \mod p = a$ and $0 \le e \le p-1$, then we say that e is discrete logarithm of a modulo p to the base r.

$\log_r a = e$

since $18 = 2^9 \mod 19$

$\log_2 18 = 9$

since $6 = 2^{14} \mod 19$

$\log_2 6 = 14$

$2^9 \bmod 19 = 18$

$2^{14} \bmod 19 = 6$

Question 3. Encrypt the message **WATCH YOUR STEP** by translating the letters into numbers, applying the given encryption function and then translating the numbers back into letters (show your work):

a) $f(p) = (p + 14) \mod 26$

b) $f(p) = (-7p + 1) \mod 26$

Question 4. Encrypt the message **UP** using the RSA system with $n = 53 \times 61$ and $e = 17$, translating each letter into integers and grouping together pairs of integers. (Show your work).

Q3

Question 3. Encrypt the message **WATCH YOUR STEP** by translating the letters into numbers, applying the given encryption function and then translating the numbers back into letters (show your work):

a) $f(p) = (p + 14) \mod 26$

b) $f(p) = (-7p + 1) \mod 26$

Solution. In each case, we translate (map) the letters to numbers from 0 to 25, then apply the function, then translate back.

W A T C H Y O U R S T E P

In each case, the numerical message is 22-0-19-2-7 24-14-20-17 18-19-4-15.

a) Adding 14 to each number modulo 26 yields 10-14-7-16-21 12-2-8-5 6-7-18-3.
Translating back into letters yields KOHQV MCIF GHSD.

b) Multiplying each number by - 7, adding 1, and reducing modulo 26 yields 3-1-24-13-4 15-7-17-12 5-24-25-0.
Translating back into letters yields DBYNE PHRM FYZA.

Q1

[1]

$$m = m_1 \times m_2 \times m_3 \times m_4$$
$$m = 2 \times 3 \times 5 \times 11 = 330$$

[2]

$$M_k = m/m_k$$
$$M_1 = 330/2 = 165, \quad M_2 = 330/3 = 110,$$
$$M_3 = 330/5 = 66, \quad M_4 = 330/11 = 30$$

[3]

y_1 is an inverse of 165 mod 2 so $y_1 = 1$

y_2 is an inverse of 110 mod 3 so $y_2 = -1$

y_3 is an inverse of 66 mod 5 so $y_3 = 1$

y_4 is an inverse of 30 mod 11 so $y_4 = -4$

[3]

* $165 \bmod 2 = 1$
  $1 = 1(1) + 2(0)$
* $110 \bmod 3 = 2$
  $1 = 2(-1) + 3(1)$
* $66 \bmod 5 = 1$
  $1 = 1$
* $30 \bmod 11 = 8$
  $1 = 8(-4) + 11(3)$

$$x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 + a_4 M_4 y_4$$
$$x \equiv (1 \times 165 \times 1 + 2 \times 110 \times (-1) + 3 \times 66 \times 1 + 4 \times 30 \times (-4)) \mod 330$$
$$= -337 \mod 330$$
$$= 323$$

$(-337 - (\frac{-337}{330}) \times 330$

So, the solution is all integers of the form $323 + 330k$ where k is an integer. ■

Q2

$a = 1$	2^0	$\mod 19 = 1$	$\mod 19 = 1 = a$
$a = 2$	2^1	$\mod 19 = 2$	$\mod 19 = 2 = a$
$a = 3$	2^{13}	$\mod 19 = 8192$	$\mod 19 = 3 = a$
$a = 4$	2^2	$\mod 19 = 4$	$\mod 19 = 4 = a$
$a = 5$	2^{16}	$\mod 19 = 65536$	$\mod 19 = 5 = a$
$a = 6$	2^{14}	$\mod 19 = 16384$	$\mod 19 = 6 = a$
$a = 7$	2^6	$\mod 19 = 64$	$\mod 19 = 7 = a$
$a = 8$	2^3	$\mod 19 = 8$	$\mod 19 = 8 = a$
$a = 9$	2^8	$\mod 19 = 256$	$\mod 19 = 9 = a$
$a = 10$	2^{17}	$\mod 19 = 131072$	$\mod 19 = 10 = a$
$a = 11$	2^{12}	$\mod 19 = 4096$	$\mod 19 = 11 = a$
$a = 12$	2^{15}	$\mod 19 = 32768$	$\mod 19 = 12 = a$
$a = 13$	2^5	$\mod 19 = 32$	$\mod 19 = 13 = a$
$a = 14$	2^7	$\mod 19 = 128$	$\mod 19 = 14 = a$
$a = 15$	2^{11}	$\mod 19 = 2048$	$\mod 19 = 15 = a$
$a = 16$	2^4	$\mod 19 = 16$	$\mod 19 = 16 = a$
$a = 17$	2^{10}	$\mod 19 = 1024$	$\mod 19 = 17 = a$
$a = 18$	2^9	$\mod 19 = 512$	$\mod 19 = 18 = a$

Q4

Question 4. Encrypt the message **UP** using the RSA system with $n = 53 \times 61$ and $e = 17$, translating each letter into integers and grouping together pairs of integers. (Show your work).

Solution.

First we translate UP into numbers: 2015.

For each of these numbers, which we might call M, we need to compute

$C = M^e \mod n = M^{17} \mod 3233$.

Note that $n = 53 \times 61 = 3233$ and that $\gcd(e, (p-1)(q-1)) = \gcd(17, 52 \times 60) = 1$, as it should be.

A computational aid tells us that $2015^{17} \mod 3233 = 2545$. Therefore the encrypted message is 2545. ■