Assignment 1

Weishi Wang, ID 260540022

February 23, 2018

Problem 1. ***Solving equations***

For each equation, either find all solutions or explain why none exist.
(a) 235x ≡ 12 (mod 243)
(b) 235x ≡ 12 (mod 245)
(c) 235x ≡ 10 (mod 245)

Solution. 1. (a) gcd(235, 243) = 1
So find the linear combination of these two number:
235 = 0(243) + 235
243 = 1(235) + 8
235 = 29(8) + 3
8 = 2(3) + 2
3 = 1(2) +1

Now, back substitute:
1 = 3 - 2
= 3 - [8 - 2(3)]
= 3(3) -8
= 3[235 - 9(8)] - 8
= 3(235) -28(8)
= 3(235) -28(243 - 235)
= 31(235) - 28(243)

Therefore 1 ≡ 31(235) (mod 243)
so 235^{-1} ≡ 31 (mod 243)
Then, x ≡ 12 ×(235^{-1}) (mod 243)
x ≡ 12 × 31 (mod 243)
x ≡ 651 (mod 243)
x ≡ 165 (mod 243)
The set of all solutions is {165+ 243k, k∈ℤ}.

(b) 235 ≡ 12 (mod 245)
⇒ 235x - 12 = 245k, k∈ℤ
⇒ 12 = 235x - 245k, k∈ℤ

Since gcd(235,245) = 5,

5|235 and 5|245

So 5 | 235x and 5 | 245k

However, $5 \nmid 12$

Therefore 12 = 235 - 245k, k$\in\mathbb{Z}$ implies that 5 must divide 12, which leads to contradiction.

Thus, solution does not exist.

(c) gcd(235,245) = 5, and 5 | 10

So divide both side by 5.

47x $\equiv$ 2 (mod 49)

now gcd(47,49) = 1

Find their linear combination:

47 = 0(49) + 47

49 = 1(47) + 2

47 = 23(2) + 1

2 = 2(1) + 0

Back substitute:

1 = 47 - 23(2)

1 = 47 - 23[49 - 47)]

1 = 24(47) - 23(49)

Thus, 1 $\equiv$ 24(47) (mod 49)

$47^{-1} \equiv 24$ (mod 49)

Then, x $\equiv 47^{-1} \times 2$ (mod 49)

x $\equiv$ 48 (mod 49)

The set of all solutions is {48+49k, k$\in\mathbb{Z}$}.

Problem 2. ***Congruence***

(a) There is a divisibility rule for dividing an integer n by 11:

Label the digits (starting with the ones place and moving right to left) with the labels 0, 1, 2, ... and so on. Sum the digits with even labels, sum the digits with the odd labels, and subtract one sum from the other. The result is divisible by 11 if and only if n is divisible by 11. For example, consider 5; 195; 407; 283. We check (3+2+0+5+1) | (8+7+4+9+5) = (11) - (33) = -22. Since 11 | 22, we also have 11 | 5, 195, 407, 283.

Prove this rule is correct. HINT: FInd an appropriate way to represent a number in terms of its digits, and think modulo 11.

Solution. (a) Let the number be x, and the digits of x is labelled as the question suggested. Then $x = d_0d_1d_2d_3d_4...d_{2n}d_{2n+1}$

We can also represent x using decimal representation:

$x = d_0(10)^0 + d_1(10)^1 + d_2(10)^2 + ... + d_{2n}(10)^{2n} + d_{2n+1}(10)^{2n+1}$

Since 10 $\equiv$ -1 (mod 11)

$x \equiv d_0(-1)^0 + d_1(-1)^1 + d_2(-1)^2 + ... + d_{2n}(-1)^{2n} + d_{2n+1}(-1)^{2n+1}$ (mod 11)

$x \equiv d_0 - d_1 + d_2 - ... + d_{2n} - d_{2n+1}$ (mod 11)

$x \equiv (d_0 + d_2 + d_4 + d_6... + d_{2n}) - (d_1 + d_3 + d_5 + d_7... + d_{2n+1})$ (mod 11)

Which is the difference between sum of even labelled numbers and sum of odd labelled numbers

W.L.O.G. let s be their difference i.e.: $s = s_{even} - s_{odd}$

So,

$x \equiv s$ (mod 11)

Now, we claim that 11 divides x if and only if 11 divides s.

($\Rightarrow$)

if 11 divides x, then x = $11k_1$ $k_1 \in \mathbb{Z}$

we know that $x \equiv s$ (mod 11)

$\Rightarrow x - s = 11k,\ k \in \mathbb{Z}$

$\Rightarrow s = x - 11k,\ k \in \mathbb{Z}$

$\Rightarrow s = 11k_1 - 11k,\ k, k_1 \in \mathbb{Z}$

$\Rightarrow s = 11(k_1 - k),\ (k_1 - k) \in \mathbb{Z}$

$\Rightarrow 11|s$

($\Leftarrow$)

if 11 divides s, then s = $11k_2$ $k_2 \in \mathbb{Z}$

we know that $x \equiv s$ (mod 11)

$\Rightarrow x - s = 11k,\ k \in \mathbb{Z}$

$\Rightarrow x = s + 11k,\ k \in \mathbb{Z}$

$\Rightarrow x = 11k_2 + 11k,\ k, k_2 \in \mathbb{Z}$

$\Rightarrow x = 11(k_2 + k),\ (k_2 + k) \in \mathbb{Z}$

$\Rightarrow 11|x$

Therefore, the statement is proven. ■

Problem 3. ***Cryptography***

You have stmbled across a (bad) RSA encryption system with public key n = 221, e = 113.

(a) Find primes p, q such that n = pq. (b) You intercept the message E = 2. Decode it using the single private key d as described in the handout. (c) Decode E using two private key s and the Chinese Remainder Theorem as described in the handout.

Solution. (a) p and q need to satisfy n=pq=221, and also (p-1)(q-1) is relatively prime with e.

$221 = 17 \times 13$

That implies a potential combination of p and q is p=17 and q=13.

also, $16 \times 12 = 192$,

check if gcd(113,192) = 1,

$192 = 1(113) + 79$
$113 = 1(79) + 34$
$79 = 2(34) + 11$
$34 = 3(11) + 1$
$11 = 1(11) + 0$

Therefore, gcd(113,192)=1

So, p =17 and q = 13.

(b) Now, we can find a linear combination os 113 and 192 to represent 1

1 = 34 - 3(11)
= 34 - 3(79 - 2(34))
= 7(34) - 3(79)
= 7(113 - 79) - 3(79)
= 7(113) - 10(79)
= 7(113) + 10(113) - 10(192)
= 17(113) - 10(192)

Then $1 \equiv 17(113) \pmod{192}$
$113^{-1} = 17$
Thus, d = 17

M $\equiv E^d \pmod{n}$
$\equiv 2^{17} \pmod{221}$
$\equiv 2^{17} \pmod{221}$
$\equiv 2(2^{16}) \pmod{221}$
$\equiv 2(2^8)^2 \pmod{221}$
$\equiv 2(256)^2 \pmod{221}$
$\equiv 2(35)^2 \pmod{221}$
$\equiv 2450 \pmod{221}$
$\equiv 2450 - 2210 \pmod{221}$
$\equiv 240 \pmod{221}$
$\equiv 19 \pmod{221}$

Thus, M is 19.

(c) Now decode this message using Chinese Remainder Theorem.
p = 17 and q =13
So, p-1 = 16 and q-1 = 12
Reduce e,
e = 113 $\Rightarrow$ e $\equiv$ 1 (mod 16) and e $\equiv$ 5 (mod 12)
which means that x $\equiv 2^5$ (mod 13) and x $\equiv 2^1$ (mod 17)
x $\equiv$ 32 (mod 13) and x $\equiv$ 2 (mod 17)
x = $13k_1 + 32$ $k_1 \in \mathbb{Z}$ and x = $17k_2 + 2$ $k_2 \in \mathbb{Z}$
One solution is x = 19, which is consistent with the answer obtained in (b).