Group Project 1: Modular Arithmetic

Jeremy Gruzka and Ian Goodbody
Math 340
LtCol Alfonso

April 20, 2015

Problem Set

Problem 10

Find all solutions to x in the equations:

$$3x - 1 \equiv_8 7 \tag{1}$$

$$2x - 1 \equiv_{20} 6 \tag{2}$$

To solve equation 1, we start with $1 \equiv_8 1$ and using *Therom 2* procede to solve.

$$\begin{aligned} 3x - 1 &\equiv_8 7 \\ (3x - 1) + 1 &\equiv_8 7 + 1 \\ 3x &\equiv_8 8 \\ 3x &\equiv_8 0 \end{aligned}$$

The reciporical of this equation becomes trivial as the product between 0 and any potential factor will invariably yield 0 therefore:

$$x \equiv_8 0$$

or x is any integer multiple of 8.

To sovle equation 2, we will similary start with the statemnt $1 \equiv_{20} 1$ and procede to solve.

$$\begin{aligned} 2x - 1 &\equiv_{20} 6 \\ (2x - 1) + 1 &\equiv_{20} 6 + 1 \\ 2x &\equiv_{20} 7 \end{aligned}$$

Now we must find the reciporical for 2 in mod 20. However, because 2 and 20 share a common factor other than 1, we cannot have a reciporical. This can be expressed by the implication

$$\begin{aligned} &\text{Let: } K, L, k, l, n \in \mathbb{Z} \mid K = n \cdot k,\ L = n \cdot l \\ &(n \neq 1) \ \Rightarrow \ (\forall x \in \mathbb{Z} \mid K \cdot x \bmod L \neq 1) \end{aligned}$$

and can be proven using the contrapositive:

$$\begin{aligned} &(\exists x \in \mathbb{Z} \mid K \cdot x \bmod L = 1) \ \Rightarrow (n = 1) \\ &\text{Assume: } K \cdot x = L \cdot q + 1, \text{ where } q \in \mathbb{Z} \\ &n \cdot k \cdot x = n \cdot l \cdot q + 1 \\ &\frac{1}{n} = k \cdot x - l \cdot q \end{aligned}$$

The conclusion then follows from the closure properties of integers over multiplication and addition

$$\begin{aligned} k \cdot x - l \cdot q &\in \mathbb{Z} \\ \frac{1}{n} &\in \mathbb{Z} \\ n &= 1 \end{aligned}$$

Because 2 and 20 share a factor of 2, no integer reciporical for exists and there is no solution for x.

Problem 12

Show that if none of the numbers in the list $1 \cdot a, 2 \cdot a, \ldots, (p-1) \cdot a$ are congruent to 0 mod p, then no two numbers in the list are congruent to eachother $\pmod{p}$.

Given a prime number p and an integer a the problem above can be written

$$\text{Let } A \equiv \{1 \cdot a, 2 \cdot a, \ldots, (p-1) \cdot a\}$$
$$\forall x \in A,\ x \bmod p \neq 0 \ \Rightarrow\ \forall y, z \in A \ \mid y \neq z,\ (y \bmod p) \neq (z \bmod p)$$

The implication can then be proven by the contrapositive.

$$\text{Assume } y, z \in A \mid y \neq z,\ (y \bmod p) = (z \bmod p)$$
$$y = m \cdot a = k \cdot p + r$$
$$z = n \cdot a = l \cdot p + r$$
$$\text{where } k, l, m, n, r \in \mathbb{Z} \mid m, n, r < p \quad k \neq l \quad m \neq n$$

Subtracting z from y then taking the modulus by p simplifes the expression.

$$a(m-n) = p(k-l)$$
$$[a \cdot (m-n)] \bmod p = 0$$

By *Therom 2*, the two factors can be seperated, and by the zero property of multiplication we can condlude that one or both of the terms must be 0.

$$(a \bmod p) \cdot [(m-n) \bmod p] = 0$$
$$a \bmod p = 0 \quad \vee \quad (m-n) \bmod p = 0$$
$$m, n < p \ \Rightarrow\ (m-n) \bmod p \neq 0$$
$$\text{Therefore: } a \bmod p = 0$$

a then must be a multiple of p so we can conclude:

$$\forall x \in A,\ x \bmod p = 0$$

Therefore, by the contapositive the original implication must be true.

Problem 16

Given that we have RSA encrypted string with public key $n = 2773$ and an encryption key $e = 157$ we are tasked with decrypting the message:
`0245 2040 1698 1439 1364 1758 0946 0881 1979 1130`

The key to decrptying this message is to derrive the decryption key d using the publicly available encryption key e and the value n. First, a computer alogorithm was used to compute the prime roots of n which were then arbitrarily set as constans p and q. (Because n is relatively small and the prime factors are easiy to compute, this is a fairly easy encrption to break.)

$$n = 2773 = (47)(59)$$
$$p = 47 \quad q = 59$$

The next constant to be calculate is k which can be found with the equation:

$$k = (p-1)(q-1) \tag{3}$$

$$k = (47-1)(59-1)$$
$$k = 2668$$

The final step in finding d is to solve the following equation for integer values of v and d.

$$d \cdot e - v \cdot k = 1 \tag{4}$$

Solving with an initial guess of $v = 1$ fortunately yields an integer value for d.

$$d \cdot e - k = 1$$
$$d = \frac{1+k}{e}$$
$$d = \frac{2668+1}{157}$$
$$d = 17$$

Decrpyting the message now relies on the coupled encryption and decryption equations, 5 and 6 respectively, where M is the raw message number and C is the codded message number.

$$C = M^e \bmod n \tag{5}$$

$$M = C^d \bmod n \tag{6}$$

Using equation 6 the coded message can be converted into pairs of letters.

C	$M = C^{17} \bmod 2773$	String
0245	2308	`WH`
2040	0120	`AT`
1698	1905	`SE`
1439	2112	`UL`
1364	0518	`ER`
1758	1906	`SF`
0946	0918	`IR`
0881	1920	`ST`
1979	1401	`NA`
1130	1305	`ME`

Ignoring the fact that spaces would be a trivial thing to add to the cypher, the string can be broken apart as `WHATS EULERS FIRST NAME`? Then assuming that *Euler* refers to the 18^{th} century swiss mathematician, the answer is *Leonhard*.