MATH 178 Homework #3

Tamir Enkhjargal

April 2019

NT

9.

i.

$$3x \equiv 2(\mathrm{mod} 14) \quad (1)$$
$$3x(\mathrm{mod} 14) \equiv 2 \quad (2)$$
$$x = 10 \quad (3)$$
$$3 * 10 = 30 \equiv 2(\mathrm{mod} 14) \quad (4)$$
$$\quad (5)$$

ii.

$$3x \equiv 2(\mathrm{mod} 15) \quad (1)$$
$$3x(\mathrm{mod} 15) \equiv 2 \quad (2)$$

This does not have any solutions because the only remainders for 3 into 15 are of the set $\{3, 6, 9, 12, 0\}$, and $2 \notin \{3, 6, 9, 12, 0\}$.

iii.

$$3x \equiv 6(\mathrm{mod} 15) \quad (1)$$
$$3x(\mathrm{mod} 15) \equiv 6 \quad (2)$$
$$x = \{2, 7, 12\} \quad (3)$$
$$3 * 2 = 6 \equiv 6(\mathrm{mod} 15) \quad (4)$$

iv.

$$37x \equiv 51(\mathrm{mod} 100) \quad (1)$$
$$37x(\mathrm{mod} 100) \equiv 51 \quad (2)$$
$$x = 23 \quad (3)$$
$$37 * 23 = 851 \equiv 51(\mathrm{mod} 100) \quad (4)$$

10.

n_1	n_2	$n_1^2 + n_2^2$	$(n_1^2 + n_2^2) \bmod 4$
1	9	82	2
3	11	130	2
5	13	194	2
7	15	274	2
9	17	370	2
11	19	482	2
13	21	610	2

Table 1: Sums of squares of two odd integers in modulo 4

n	n^2	$n^2 \bmod 4$
1	1	1
2	4	0
3	9	1
4	16	0
5	25	1
6	36	0
7	49	1
8	64	0
9	81	1
10	100	0

Table 2: Squares of integers in modulo 4

We can see that any sum of two odd integers modulo 4 is always 2, and that the squares of integers in modulo 4 are either 1 or 0. This means that they are not logically equivalent.

11.

We can use lemmas and general knowledge. Consider both situations, x is even and x is odd.

If x is even, then x^3 is an even number (even number multiplied by an even number is even). Adding x^3 and x is even (even number added even number is still even). And finally, when you add 1, it becomes odd.

If x is odd, then x^3 is an odd number (odd number multiplied by an odd number is odd). Adding two odd numbers $x^3 + x$ is always even. And then adding 1 at the end returns it to be odd.

From these two cases, we can say that $x^3 + x + 1$ is always odd.

12.

i. $\varphi(32) = \varphi(2^5) = (2^4(2-1)) = 16$

ii. $\varphi(100) = \varphi(2^2 * 5^2) = \varphi(2^2) * \varphi(5^2) = 2 * (5 * 4) = 40$

iii. $\varphi(3600) = \varphi(2^4 * 3^2 * 5^2) = \varphi(2^4)\varphi(3^2)\varphi(5^2) = 2^3(1) * 3(2) * 5(4) = 960$

iv. $\varphi(35) = \varphi(5 * 7) = \varphi(5)\varphi(7) = 4 * 6 = 24$

v. $\varphi(77) = \varphi(7 * 11) = \varphi(7)\varphi(11) = 6 * 10 = 60$

13.

$$\text{If } n = pq \text{ then } \varphi(n) = \varphi(p * q) = \varphi(p)\varphi(q) \tag{1}$$

15.

First, check if the gcd of a and m is 1. $gcd(3, 7) = 1$. Then $\varphi(7) = 6$.

$$1000000(\text{mod}6) = 4 \tag{1}$$
$$\therefore 3^{1000000} \equiv 3^4(\text{mod}7) = 81(\text{mod}7) = 4 \tag{2}$$

16.

The numbers n are of the set $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 18, 20, 21, 22, 24, 26, 28, 30, 36, 42\}$

17.

The cases when $\varphi(3n) = 3\varphi(n)$ occur when $3|n$. In general, if we are looking to see which numbers $\varphi(a * n) = a * \varphi(n)$ occur only when $a|n$.

SmC

1.

```
Z  CVRIEVU  KYVWFCCFNZEX  AFBV  KYV  CRJK  KZDV  Z  NFIBVU R  IVRC  AFS.
NYRK  UZU  KYVWZJY JRP NYVE YV YZK YZJ YVRU? URD
```

The highest frequencies of letters that appear in the ciphertext is `V` then `Y`. The highest frequencies of letters in the English language is E then T. The shift from E to V is 17. If we shift backwards 17 values, we get

```
I LEARNED THE FOLLOWING JOKE THE LAST TIME I WORKED A REAL
JOB. WHAT DID THE FISH SAY WHEN HE HIT HIS HEAD? DAM
```