

Assignment 4

Matthew Nemitz, ID 260506071

November 6, 2016

Problem 1. *Solve for x in the congruence:*

$$32x \equiv 8 \pmod{13}$$

Solution. First we observe that 32 and 13 are coprime since

$$\gcd(32, 13) = 1$$

This means there is exactly one congruence class for x which satisfies this equation, and in order to find the base value for this congruence class, we need to find the multiplicative inverse of 32 under mod 13. In other words, we are looking for v such that:

$$32v \equiv 1 \pmod{13}$$

Since then we know,

$$x \equiv 8v \pmod{13}$$

In other words we want:

$$32v + 13k = 1$$

...for some k . To find this we can perform the extended Euclidean algorithm on 32 and 13:

$$32 = 2(13) + 6$$

$$13 = 2(6) + 1$$

so...

$$6 = 32 - 2(13)$$

$$1 = 13 - 2(6)$$

$$1 = 13 - 2(32 - 2(13))$$

$$1 = 13 - 2(32) + 4(13)$$

$$1 = -2(32) + 5(13)$$

$$v = -2, \quad k = 5$$

We have shown that -2 is the multiplicative inverse (mod 13) of 32. So we have

$$x \equiv -2(8) \equiv -16$$

Problem 2. *How many solutions does the following congruence have?*

$$51x \equiv 34 \pmod{646}$$

Solution. ...

Problem 3. *What is the last digit of 393 to the power of 4097?*

Solution. Start with the following observation:

$$\forall a \quad a \equiv b \pmod{10}$$

...where b is the last digit of a . Based on this observation, with 393 as our base, only the last digit 3 can have any effect on the last digit of any greater power of 393, since 393 is congruent to 3 mod 10, or more intuitively, all greater powers of 90 and 300 end in zero(es). Therefore, the last digit of 393^{4097} is the same as the last digit of 3^{4097} . We can then exploit the pattern of last digits of powers of 3 in mod 10:

3^0	1
3^1	3
3^2	9
3^3	27
3^4	81
3^5	243
3^6	729
...	...

From this pattern, we can see that 3^{4k} will always end in 1. We can also infer that for any 3^n , the last digit will be the same as that of $3^{(n\%4)}$. Since $4096\%4 = 1$, the last digit of 3^{4097} must be the same as that of 3^1 , which is 3. The last digit of 393^{4097} is therefore also **3**

Problem 4. Give an example of two functions f and g such that $g \circ f(x) = x$ for all x but $f \circ g(y) \neq y$ for some y .

Solution. Take for example $f(x) = \sqrt{x}$ and $g(y) = y^2$. It is true that $\forall x(\sqrt{x})^2 = x$ (even if x is negative, and \sqrt{x} is a complex number this still holds). However, $\exists y\sqrt{y^2} \neq y$, namely negative values of y , since $\sqrt{(-y)^2} = y \neq -y$.

Problem 5. a. How many injections are there from the set $A = \{1, 2, 3, 4\}$ to the set $B = \{1, 2, 3, 4, 5\}$?

b. How many surjections are there from A to B ?

Solution.

a. content...