CRYPTOGRAPHY HANDOUT 09

CONGRUENCES

1. Properties of Congruences

Theorem 1.1. *Let a, b, c, n be integers with $n \neq 0$.*

1. $a \equiv 0 \bmod n$ *if and only if* $n \mid a$.

2. $a \equiv a \bmod n$.

3. $a \equiv b \bmod n$ *if and only if* $b \equiv a \bmod n$.

4. If $a \equiv b$ *and* $b \equiv c \bmod n$, *then* $a \equiv c \bmod n$.

Write the proof for property 3, keeping in mind you must show the if and only if statement:

Theorem 1.2. *Let a, b, c, d, n be integers with $n \neq 0$, and suppose $a \equiv b \bmod n$ and $c \equiv d \bmod n$. Then:*

- $a + c \equiv b + d (\mathrm{mod} n)$,
- $a - c \equiv b - d (\mathrm{mod} n)$, *and*
- $ac \equiv bd (\mathrm{mod} n)$.

Note. This basically tells us that we have addition, subtraction, and multiplication operations which behave the way we expect.

Example. Addition and Multiplication with $\mathbb{Z}_5$:

+	0	1	2	3	4
0					
1					
2					
3					
4					

×	0	1	2	3	4
0					
1					
2					
3					
4					

Example. Addition and Multiplication with $\mathbb{Z}_4$:

+	0	1	2	3
0				
1				
2				
3				

×	0	1	2	3
0				
1				
2				
3				

Question: Do you notice any patterns or differences between $\mathbb{Z}_5$ and $\mathbb{Z}_4$?

2. Division and Inverses

Recall: This was a problem from Mission 2: the ciphertext `GEZXDS` was encrypted by a Hill cipher with a 2×2 matrix. The plaintext is `solved`. Find the encryption matrix M.

Problems:

Question: How do we know when we have a multiplicative inverse or not? (We'll figure it out.)

1. Go back to your $\mathbb{Z}_5$ and $\mathbb{Z}_4$ multiplication tables. Which elements have inverses?

2. Compute the gcd of all of these elements with inverses with n in $\mathbb{Z}_n$.

3. Form a conjecture about which elements have inverses. If you're not sure, write out the multiplication tables for $\mathbb{Z}_6$ and $\mathbb{Z}_7$ too, and do the same steps as above.

4. Given what you have conjectured, which elements should have inverses in $\mathbb{Z}_{20}$? Which elements do not have inverses?