

Cracking the Code – The Mathematics of Cryptanalysis

Lesson 5 – More Modular Arithmetic

Questions

1. What strategies did you use to decipher Cypher #3?
2. Encrypt the following message using the same code that was used to encrypt Cypher #3:

Ask not for whom the bell tolls.

3. This message was encrypted using the same code that was used to encrypt Cypher #3. Decrypt it.

EKPLSQP

Terminology

- The result of multiplying two numbers together is called the *product* of the two numbers. For example, since 3 times 4 is 12, we say that 12 is the *product* of 3 and 4.
- If the product of two numbers is 1, we say that the numbers are *multiplicative inverses* of each other.
- The *integers* are $\{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$
- An integer larger than 1 is said to be *prime* if the only numbers which evenly divide it are itself and 1.
- Two integers greater than 1 are *relatively prime* if their greatest common divisor is 1.

Questions Continued

4. Encrypt the message in Question 2 above using 2 as the multiplicative key. Do you notice any problems?
5. Encrypt the message in Question 2 above using 4 as the multiplicative key. Do you notice any problems?
6. What is the multiplicative inverse of 3 mod 26?
7. Find each of these inverses if possible. If you do not think it is possible to find a particular inverse, explain why.
 - a. The multiplicative inverse of 5 mod 26.
 - b. The multiplicative inverse of 2 mod 26.

- c. The multiplicative inverse of 11 mod 26.
 - d. The multiplicative inverse of 13 mod 26.
 - e. The multiplicative inverse of 15 mod 26.
8. Can you describe a procedure for finding multiplicative inverses?
 9. Can you describe a way to predict whether or not a number will have a multiplicative inverse mod 26?
 10. Which numbers larger than 1 and smaller than 12 have multiplicative inverses mod 12?
 11. Give three examples of prime numbers.
 12. Give two numbers which are not prime but which are relatively prime to each other.
 13. Is 15 prime? Is 15 relatively prime to 26?
 14. According to the website www.mersenne.org, what is the largest known prime? How many digits does it have?
 15. Suppose that a message is encoded with a multiplicative cipher with key 5. What is the multiplicative key which would be used to decode the message?