

Mathematics of Coding and Cryptography
Worksheet 3

1. Prove that the last non-trivial remainder in the Euclidean algorithm is the greatest common denominator of the integers input into the algorithm.
2. Use the Euclidean algorithm to find the gcd of 123456 and 7654321, and the integers x and y such that

$$\gcd(123456, 7654321) = 123456x + 7654321y.$$

3. (a) Let p be a prime. Suppose a and b are integers such that $ab \equiv 0 \pmod{p}$. Show that either $a \equiv 0$ or $b \equiv 0 \pmod{p}$.
(b) Show that if a, b, n are integers with $n|ab$ and $\gcd(a, b) = 1$, then $n|b$.
4. We have shown that given any two elements a and b in \mathbb{Z}_n that we can create unique elements $a + b, a - b$ and ab in \mathbb{Z}_n . Under what conditions on n is it possible to uniquely specify a number a/b in \mathbb{Z}_n which has the property that $(a/b)b \equiv a \pmod{n}$ for all possible values of a and $b \neq 0$.
5. Suppose you have a string of elements in \mathbb{Z}_5 given by $(4, 0, 2, 2, 3, 1, 0)$. Regard this as your plaintext, and encrypt the message by raising each element in \mathbb{Z}_5 to the 6th power mod 5 (That is, the ciphertext should be another string of elements in \mathbb{Z}_5). Can you find a decryption algorithm? Is this a good encryption algorithm? Can you classify which powers give good encryption algorithms?

6. Review questions:

- (a) Find the volume of the parallelepiped spanned by the vectors

$$\left\{ \begin{bmatrix} -4 \\ 5 \\ 1 \end{bmatrix}, \begin{bmatrix} 3 \\ -1 \\ 1 \end{bmatrix}, \begin{bmatrix} -2 \\ -1 \\ 0 \end{bmatrix} \right\}$$

- (b) Find the centroid of the cone

$$z^2 = x^2 = y^2 \quad 0 \leq z \leq 4.$$