

Mathematics of Coding and Cryptography
Worksheet 3

1. Come up with a method for solving three simultaneous congruences. That is, suppose m_1 , m_2 and m_3 are pair-wise relatively prime positive integers and a_1 , a_2 and a_3 are arbitrary integers. Find a method for constructing the unique $x \pmod{m_1 m_2 m_3}$ satisfying

$$\begin{aligned}x &\equiv a_1 \pmod{m_1} \\x &\equiv a_2 \pmod{m_2} \\x &\equiv a_3 \pmod{m_3}\end{aligned}$$

2. Solve the congruence $x^4 \equiv 1 \pmod{505}$.
3. Secret sharing: Suppose we want to ‘share’ a secret integer N between 4 people by giving each person a ‘clue’ in the form $a \pmod{p}$ for some prime p and that the integer N satisfies

$$\sqrt[3]{N} < p < \sqrt{N} \tag{1}$$

For instance, suppose that person one knows $N \equiv 10 \pmod{11}$, that person two knows that $N \equiv 12 \pmod{13}$, person three knows that $N \equiv 14 \pmod{17}$ and person four knows that $N \equiv 12 \pmod{19}$.

- (a) What is the secret integer N ?
- (b) Show that any group of three can find N , but any group of two or less cannot.
- (c) Can you generalize this (i.e. find conditions on the primes akin to (1)) so that the secret integer is shared between M people so that at least K of them are needed to find the secret integer.

Review:

- (a) Diagonalize the matrix

$$\begin{bmatrix} 4 & 0 & 1 \\ -1 & -6 & -2 \\ 5 & 0 & 0 \end{bmatrix}$$

- (b) Consider the oriented curve C in the yz -plane given by the line from $(0, 0, 0)$ to $(0, 1, 0)$, the quarter circle from $(0, 1, 0)$ to $(0, 0, 1)$ and the line segment from $(0, 0, 1)$ to $(0, 0, 0)$. Suppose $F(x, y, z) = (y, z, x)$. Use Stoke’s Theorem to find

$$\int_C F \cdot ds.$$