Problem Set 4

1. **Solving Modular Equations** (6 pts)
Solve the following equations for x and y or show that no solution exists. Show your work (in particular, what division must you carry out to solve each case).

   (a) $5x + 13 \equiv 11 \pmod{504}$

   (b) $9x + 80 \equiv 2 \pmod{81}$

   (c) The system of simultaneous equations $30x + 2y \equiv 0 \pmod{37}$ and $y \equiv 4 + 13x \pmod{37}$

2. **More Inverses** (6 pts)
Consider the sequence of integers (a_n) given by $a_1 = 1$, $a_2 = -1$, $a_3 = 3$, and in general by:

$$a_n = 1 + (-2) + 4 + (-8) + \cdots + (-2)^{n-1}$$

   (a) Prove that a_n is an inverse of 3 mod 2^n.

   (b) Find a similar formula for an inverse of 4 mod 3^n and prove that is correct.

3. **Polynomial Interpolation** (6 pts)
Consider the points $\{(1,1),(2,2),(4,3),(0,2)\}$ in the real plane ($\mathbb{R}^2$).

   (a) Through a system of linear equations construct a degree 3 polynomial that passes through these points.

   (b) Use Lagrange interpolation to find the degree 3 polynomial that passes through the points.

   (c) Now assume you were given the same points in $\mathbb{Z}_7^2$ (that is, both the x values and the y values are in $\mathbb{Z}_7$). Since 7 is prime, $\mathbb{Z}_7$ is a field (written as F_7 or $GF(7)$). Use Lagrange interpolation to find the degree 3 polynomial over F_7 that passes through these points.

4. **Parabolas in galois fields** (4 pts)
Let p be a prime. Consider the degree-2 polynomial $f(x) \equiv x^2 + ax + b \pmod{p}$ over $GF(p)$. Show that, if f has *exactly* one root, then $a^2 \equiv 4b$.