Problem Set 5

1. **Extended GCD-10 points** Use the Extended Euclid algorithm to find integers k and l such that $42k + 30l = gcd(42, 30)$.

2. **The Lowest Common Denominator-15 points** When combining two fractions with different denominators, one usually elects to use the lowest common denominator of the two fractions, as in

$$\frac{7}{15} + \frac{2}{21} \quad = \quad \frac{59}{105} \ .$$

   That is, the single resulting fraction has the smallest denominator consistent with those of the original fractions, if its denominator is chosen as the lowest common multiple (LCM) of the two original denominators. Find a way to write the LCM of two integers a and b in terms of $gcd(a, b)$. Prove that your expression is true for all $a, b \in \mathbb{Z}$.

3. **Diophantine Equations-20 points** A diophantine equation (to be exact, a linear diophantine equation in two variables) is an equation of the following form:

$$ax + by = c \ ,$$

   where the constant coefficients a, b, c and the variables x, y are all integers. For fixed constants a, b, c a solution to the corresponding diophantine equation is just an integer value for each of x and y such that $ax + by = c$ is satisfied.

   (a) Prove that a diophantine equation has a solution iff $gcd(a, b) \mid c$.

   (b) Prove that if a diophantine equation has a solution then it has infinitely many solutions. Show how to compute all of these solutions using a, b, c and $d = gcd(a, b)$.

   (c) Compute the solutions of $21x + 12y = 102$.

4. **Polynomial Interpolation- 15 points** Consider the points $\{(1, 1), (2, 2), (4, 3), (0, 2)\}$.

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

   (b) Find the degree 3 Lagrange interpolation polynomial that passes through the points.

5. **Hierarchical Secret Sharing - 30 points**

   (a) Suppose that you want to share a secret key 7 among 5 people by giving each person a share of information, such that any 2 of the 5 people can recover the secret from their shares but no single person can. Working modulo 11, describe how the 5 shares will be computed.

   (b) Now suppose that the 5 people are the 3 GSI's and the two lecturers of a class; and the secret is the solution to the final (i.e. encoded as a natural number). Any group of people should be able to recover the secret provided that the group contains all three GSIs OR both lecturers OR one lecturer and two GSIs. Describe a very simple modification of the secret sharing protocol to achieve this.

(c) Finally suppose that the secret is to be shared by three groups of five people each. A set of the 15 people can recover the secret if it contains majorities (at least 3 of five) of at least two of the groups. Describe another modification of the secret sharing scheme to achieve this variation.

6. **Feedback - 10 points for answering all questions.**

1) The pace of the course is:
   a) Speed of light (very fast)
   b) A bit too fast
   c) Close to my pace
   d) A bit too slow
   e) I sleep in the lectures
2) How challeging do you find the material covered in class?
   a) Rocket science
   b) Fairly challenging
   c) Just right
   d) I did this in kindergarden
3) The sections/office hours are:
   a) Very helpful
   b) Useful at times
   c) Pointless
   d) What sections?
4) The homeworks are:
   a) Akin to medioeval methods of torture
   b) Challenging, but help understand the material
   c) Challenging but useless
   d) Of reasonable difficulty
   e) Could be more difficult
5) Give two suggestions for making the sections/office hours more helpful.
6) Give two suggestions for making the lectures better.

   Please add any other comments you might have on any part of the course. Thank you.