Problem Set 3

Due: Start of Class, Tuesday, September 24.

Reading: Sections 1.4-1.5, 2.3-2.5, 3.3, 6.1-6.2, 6.5.

Problem 1. **[15 points]**

Show all your work in the following:

1. Use the Euclidean algorithm to calculate $\gcd(294, 1386)$.
2. Use the Euclidean algorithm to express $\gcd(294, 1386)$ as a linear combination of the numbers 294 and 1386.
3. What is the least common multiple of 294 and 1386, $\operatorname{lcm}(294, 1386)$?

Problem 2. **[15 points]** In class, it was shown that the number of passes used in the Euclidean GCD algorithm for arguments x and y is at most $x + y$. It is possible to improve this bound.

1. Prove that when the Euclidean algorithm with inputs x on y calls itself on new arguments x' and y', then the sum $x' + y'$ is at most $(\frac{3}{4})(x + y)$.
2. Use part (1) to get a better bound on the number of passes, using induction.

Problem 3. **[10 points]** Encrypt the message **ATTACK** using the **RSA** system with $n = 43 \cdot 59$ and $e = 13$, translating each letter into integers and grouping together pairs of integers, as done in Example 10.

Problem 4. **[15 points]** Olympic Hopscotch is played on a two-dimensional field of squares, numbered by pairs of integers representing x and y coordinates in the usual way. You may assume that the field is infinite in all directions.

You are supposed to start in square $(0, 0)$. You are allowed to jump in only the following ways:

- 12 squares north, south, east or west.
- 9 squares north or south.

- 15 squares east or west.

At the beginning of a game, the referee calls out the number of a square, and you are supposed to tell him either that it is *impossible* for you to jump to that square using the given moves, or else to actually jump there.

1. How do you determine whether or not it is possible to jump to a given square?
2. For those squares that it's possible to reach, give a method for jumping there.

Problem 5. **[15 points]** Let A, B, and C be sets. Which of the following are correct set identities? For each, if it is a set identity, give a proof that it is (using the style of argument used in class to prove the basic set identities, or using the basic set identities themselves). If it is not a set identity, then give a counterexample.

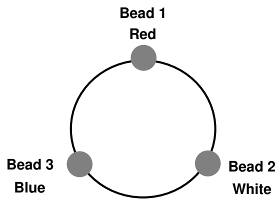
1. $(A - B) \cap (B - C) = \emptyset$
2. $(B - A) \cup (C - A) = (B - (C \cup A)) \cup (C - (B \cup A))$
3. $(A \oplus B) \oplus C = A \oplus (B \oplus C)$
4. $(A \cap B) \times (B \cap C) = (A \times C) \cap B^2 \cap (A \times B) \cap (B \times C)$

Problem 6. **[15 points]**

1. List the 16 different binary relations on the set $\{0, 1\}$.
2. Which of the 16 relations in part (1) are reflexive? symmetric? antisymmetric? transitive?

Problem 7. **[15 points]**

Each bead on a bracelet with three beads is either red, white, or blue as illustrated in the example shown. Define the relation R between bracelets as follows: (B_1, B_2), where B_1 and B_2 are bracelets, belongs to R if and only if B_2 can be obtained from B_1 by rotating it or rotating it and then reflecting it.



- Show that R is an equivalence relation.
- What are the equivalence classes of R?