MATH 13 WINTER 2016 HOMEWORK 4

Due: Friday February 26 Please turn in at the lecture.

Each group please turn in only one paper. If you prefer to work alone, that is fine: A group can consist of one member.

Student name/id (include all students in the group):

IMPORTANT INSTRUCTIONS: It is crucial that you write your arguments clearly and that each argument clearly shows how you arrive at the conclusions from the assumptions. This is the point of homeworks – to practice understanding of the material, proofwriting, and the ability to express your understanding.

When preparing the homeworks, please follow the **Rules for homeworks** on the course webpage under **Course information and policies** and also the guidelines under **Grading**. In particular, keep in mind the **Aspects of grading** in the **Grading** section.

Recall that if a, b are integers then $d = \gcd(a, b)$ if and only if $d > 0$ and the following two conditions are satisfied:

(G1) d is a common divisor of a, b, and
(G2) If d' is any common divisor of a, b then $d' \mid d$.

1. (7pt) This exercise is on Euclid's algorithm. Recall that given two integers a, b Euclid's algorithm runs as follows:

$$
\begin{aligned}
(1) \qquad a &= b \cdot q_1 + r_1 \\
(2) \qquad b &= r_1 \cdot q_2 + r_2 \\
(3) \qquad r_1 &= r_2 \cdot q_3 + r_3 \\
(4) \qquad &\vdots \\
(5) \qquad r_{k-2} &= r_{k-1} \cdot q_k + r_k \\
(6) \qquad r_{k-1} &= r_k \cdot q_{k+1}
\end{aligned}
$$

That is, $r_{k+1} = 0$ and k is the least number with this property. We say that k is the **length of the run** of the algorithm at (a, b).

In the lecture I sketched an argument that $r_k = \gcd(a, b)$ but did not give a rigorous proof. The proof is done by induction on k, which is the length of the run of the algorithm. Write this induction rigorously following the guidelines below.

(A) **(3pt)** Prove by induction on k that r_k divides both a and b.

Hint. To handle the induction step, you need to assume that r_k divides both a' and b' **whenever** a', b' are such that the length of the run of the algorithm at a', b' is k. Then prove that r_{k+1} divides both a, b whenever $k+1$ is the length of the run of the algorithm at (a, b).

Important point: Notice that if $k+1$ is the length of the run of the algorithm at (a, b) then the length of the run of the algorithm at (b, r_1) is k.

(B) **(4pt)** Prove by induction on k that there are integers x, y such that $r_k = a \cdot x + b \cdot y$.

Hint. Similarly as in Case A, to handle the induction step you need to assume that if a', b' are such that the length of the run of the algorithm at (a', b') is k then $r_k = a' \cdot x + b' \cdot y$ for some integers x, y. Then prove that if the run of the algorithm at (a, b) is of length $k+1$ then $r_{k+1} = a \cdot x + b \cdot y$ for some integers x, y.

Important point. The same point as in Case A.

2. (4pt: 1pt for each proof that the solution exists/does not exist; 2pt for finding the solution) Which of the following two equations has an integer solution? In each case give a proof that the solution either exists or does not exist. If a solution exists, use Euclid's algorithm to find **one** such solution.

(a) $144x + 90y = 54$
(b) $144x + 90y = 100$

3. (5pt: 3pt for (G1), 2pt for (G2) Let a, b be integers. Let

$d =$ the smallest **positive** number of the form $a \cdot x + b \cdot y$ where x, y are integers.

Prove that $d = \gcd(a, b)$.

Hint. You need to verify both (G1) and (G2) above. Regarding (G1), argue by contradiction. Assume for instance that d does not divide a and use the division algorithm to show that d is not smallest possible.

4. (4pt: 2pt for each inclusion) Let A and B be sets. Is the following formula true?

$$A \setminus (A \setminus B) = A \cap B.$$

Give a rigorous argument.