Math 300.2 Homework 4

Paul Hacking

February 21, 2012

Reading: Gilbert and Vanstone, Chapter 2.

(1) Let a, b, c be integers.

   (a) What is the precise meaning of the statement "a divides b" (also written $a \mid b$)?

   (b) Show that if $a \mid b$ then $ac \mid bc$.

   (c) Show that if $ac \mid bc$ and $c \neq 0$ then $a \mid b$.

(2) Let a, b, c, d be integers. For each of the following statements give either a proof or a counterexample.

   (a) If $a \mid b + c$ then either $a \mid b$ or $a \mid c$.

   (b) If $a \mid bc$ then either $a \mid b$ or $a \mid c$.

   (c) If $a \mid b$ and $c \mid d$ then $ac \mid bd$.

   (d) If $a \mid b$, $a \mid c$, and $a \mid d$, then $a^2 \mid (bc - d^2)$.

(3) Find the greatest common divisor of the following pairs of integers.

   (a) 53, 42.

   (b) 129, 57.

   (c) 189, 427.

(4) The Fibonacci numbers F_n, $n = 1, 2, \ldots$, are defined by $F_1 = 1$, $F_2 = 1$, and $F_{n+2} = F_{n+1} + F_n$ for $n \geq 1$. So the first few Fibonacci numbers are $1, 1, 2, 3, 5, 8, 13, 21, \ldots$.

(a) Show that $F_n \leq F_{n+1} < 2F_n$ for each $n \geq 3$.

(b) Now suppose we compute $\gcd(F_{n+1}, F_n)$ using the Euclidean algorithm. Describe the steps of the algorithm explicitly. How many steps are required in total? [Hint: If you are stuck, first perform the algorithm by hand for some small values of n.]

[Remark: There is the following explicit formula for the Fibonacci numbers (which can be proved by induction):

$$F_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right).$$

This formula implies that $n \approx \log_{10} F_n / \log_{10}((1+\sqrt{5})/2) \approx 5 \log_{10} F_n$ (here $\approx$ means "approximately equal to"). Since the behaviour in part (b) above is the "worst case scenario" (why?), it follows that the Euclidean algorithm for a, b requires at most $5 \log_{10} b$ steps, or roughly 5 times the number of digits of b.]

(5) For each of the following equations, either find a solution $x, y \in \mathbb{Z}$ or explain why a solution does not exist.

(a) $37x + 13y = 1$.

(b) $14x + 63y = 5$.

(c) $9x + 51y = 12$.

(6) Consider the equation $5x + 7y = 59$.

(a) Find all solutions of the equation with $x, y \in \mathbb{R}$. (Express your answer in terms of a parameter t.)

(b) Find all solutions with $x, y \in \mathbb{Z}$.

(c) Find all solutions in non-negative integers x, y.

(7) Let p be a prime number.

(a) Let a be an integer. Show that if $p \mid a^2$ then $p \mid a$.

(b) Show that $\sqrt{p}$ is not a rational number. That is, there do not exist integers a and b, with $b \neq 0$, such that $\sqrt{p} = a/b$. [Hint: Review the proof for the case $p = 2$ given in class and use part (a).]

(8) Let n be a positive integer. Show that if $2^n - 1$ is prime then n is prime. [Hint: Prove the contrapositive statement. To do this use the law of exponents $x^{ab} = (x^a)^b$ and the identity

$$(y^b - 1) = (y - 1)(y^{b-1} + y^{b-2} + \cdots + y + 1)$$

where y is a variable and b is a positive integer (compare HW2Q4(a)).]