Math 300.3 Homework 7

Paul Hacking

March 31, 2017

Reading: Sundstrom, Sections 8.1 and 8.2.

Justify your answers carefully.

(1) Find the greatest common divisor of each of the following pairs of integers. Use the Euclidean algorithm and show your work.

   (a) 126, 91.

   (b) 253,143.

   (c) 113, 51.

(2) For each of the following pairs of integers a and b, find integers x and y such that $ax + by = \gcd(a, b)$. Use the Euclidean algorithm and show your work.

   (a) 100, 31.

   (b) 169, 65.

(3) (a) Give a direct proof of the following statement: For all $a, b, d \in \mathbb{N}$ and $x, y \in \mathbb{Z}$, if $d \mid a$ and $d \mid b$ then $d \mid ax + by$.

   (b) Do there exist integers x and y such that $87x + 102y = 28$? Justify your answer carefully.

(4) Prove the following statement: For all $a, b, c \in \mathbb{N}$, if $a \mid c$ and $b \mid c$ and $\gcd(a, b) = 1$ then $ab \mid c$.

   [Hint: Recall the following result (proved in class): For all $l, m, n \in \mathbb{N}$, if $l \mid mn$ and $\gcd(l, m) = 1$, then $l \mid n$. Now write down the definition of $a \mid c$ and use this result to construct a direct proof of the statement.]

(5) Prove the following statement: For all $n \in \mathbb{N}$, $\gcd(7n + 17, 2n + 5) = 1$.

[Hint: Use the Euclidean algorithm.]

(6) Recall that the Fibonacci numbers $f_1, f_2, f_3, \ldots$ are defined by $f_1 = 1$, $f_2 = 1$, and $f_n = f_{n-1} + f_{n-2}$ for $n \geqslant 2$. Prove by induction that $\gcd(f_{n+1}, f_n) = 1$ for all $n \in \mathbb{N}$.

(7) Using prime factorizations or otherwise, compute the greatest common divisors of the following pairs of integers.

(a) $10!$, 6^5.

(b) 84^{10}, 90^7.

(8) In class we proved the "fundamental theorem of arithmetic": Every $n \in \mathbb{N}$ such that $n \geqslant 2$ may be expressed as a product of prime numbers, and this expression is unique (up to reordering the factors). The goal of this question is to convince you that the uniqueness of the factorization is not obvious and needs to be proved carefully.

Consider the set

$$S = \{n \in \mathbb{N} \mid n \equiv 1 \bmod 4\} = \{1, 5, 9, 13, \ldots\}.$$

We say an element $n \in S$ is a *pseudoprime* if $n \neq 1$ and the only elements of S which divide n are 1 and n.

(a) Write down all the pseudoprimes which are less than 100. [Hint: There are 25 elements of S less than 100 and 19 of these are pseudoprimes.]

(b) Show that if $a \in S$ and $b \in S$ then $ab \in S$.

(c) Suppose $n, d \in \mathbb{N}$ and $d \mid n$, that is, $n = qd$ for some $q \in \mathbb{Z}$. Show that if $d \in S$ and $n \in S$ then $q \in S$.

(d) Using part (c), prove the following statement by strong induction: For all $n \in S$ such that $n \geqslant 2$, n can be expressed as a product of pseudoprimes.

(e) Find an element $n \in S$ which can be expressed as a product of pseudoprimes in two different ways. (Here we regard two factorizations as the same if one is obtained from the other by reordering the factors.)