MATH 135: Extra Practice Set 5

These problems are for extra practice and are not to be handed in. Solutions will not be posted but, unlike assignment problems, they may discussed in depth on Piazza.

- The warm-up exercises are intended to be fairly quick and easy to solve. If you are unsure about any of them, then you should review your notes and possibly speak to an instructor before beginning the corresponding assignment.
- The recommended problems supplement the practice gained by doing the corresponding assignment. Some should be done as the material is learned and the rest can be left for exam preparation.
- A few more challenging extra problems are also included for students wishing to push themselves even harder. Do not worry if you cannot solve these more difficult problems.

Warm-up Exercises

1. Disprove the following. Let $a, b, c \in \mathbb{Z}$. Then $\gcd(a, b) = \gcd(a, c) \cdot \gcd(b, c)$.
2. Let $a, b, c \in \mathbb{Z}$. Consider the statement S: If $\gcd(a, b) = 1$ and $c \mid (a + b)$, then $\gcd(a, c) = 1$. Fill in the blanks to complete a proof of S.
   (a) Since $\gcd(a, b) = 1$, by __________ there exist integers x and y such that $ax + by = 1$.
   (b) Since $c \mid (a + b)$, by __________ there exists an integer k such that $a + b = ck$.
   (c) Substituting $a = ck - b$ into the first equation, we get $1 = (ck - b)x + by = b(-x + y) + c(kx)$.
   (d) Since 1 is a common divisor of b and c and $-x + y$ and kx are integers, $\gcd(b, c) = 1$ by __________.

Recommended Problems

1. (a) Use the Extended Euclidean Algorithm to find three integers x, y and $d = \gcd(1112, 768)$ such that $1112x + 768y = d$.
   (b) Determine integers s and t such that $768s - 1112t = \gcd(768, -1112)$.
2. Prove that for all $a \in \mathbb{Z}$, $\gcd(9a + 4, 2a + 1) = 1$
3. Let $\gcd(x, y) = d$. Express $\gcd(18x + 3y, 3x)$ in terms of d and prove that you are correct.
4. Prove that if $\gcd(a, b) = 1$, then $\gcd(2a + b, a + 2b) \in \{1, 3\}$.
5. Prove that for every integer k, $\gcd(a, b) \leq \gcd(ak, b)$.
6. Given a rational number r, prove that there exist coprime integers p and q, with $q \neq 0$, so that $r = \dfrac{p}{q}$.
7. Prove that: if $a \mid c$ and $b \mid c$ and $\gcd(a, b) = 1$, then $ab \mid c$.
8. Let $a, b, c \in \mathbb{Z}$. Prove that if $\gcd(a, b) = 1$ and $c \mid a$, then $\gcd(b, c) = 1$.
9. Prove that if $\gcd(a, b) = 1$, then $\gcd(a^m, b^n) = 1$ for all $m, n \in \mathbb{N}$. You may use the result of an example in the notes.

10. Suppose a, b and n are integers. Prove that $n \mid \gcd(a, n) \cdot \gcd(b, n)$ if and only if $n \mid ab$.

Challenge(s)

1. Prove that for any integers $a \neq 1$ and $n \in \mathbb{N}$, $\gcd\left(\frac{a^n-1}{a-1}, a-1\right) = \gcd(n, a-1)$.
2. Let n be a positive integer for which $\gcd(n, n+1) < \gcd(n, n+2) < \cdots < \gcd(n, n+20)$. Prove that $\gcd(n, n+20) < \gcd(n, n+21)$.
3. Let a and b be nonnegative integers. Prove that $\gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a,b)} - 1$.