Notes on Problem Set 3

1. The message is **God does not play dice.** This is a famous quote from Einstein, who was expressing his dissatisfaction with quantum theory. The quote is very famous, but unfortunately gives a distorted view of Einstein's real concerns about quantum mechanics. However, this is a topic for a different course.

3. Complete the proof of the gcd recursion theorem (Theorem 1.6 in the number theory notes).

Proof We're given $d = gcd(a, b), d' = gcd(b, a \bmod b)$. We've already shown that $d \leq d'$, and want now to show that $d' \leq d$.

By the division algorithm,

$$a = \lfloor a/b \rfloor b + a \bmod b.$$

Thus a is a linear combination of b and $a \bmod b$. Since $d'|b$ and $d'|a \bmod b$, it follows that $d'|a$. Therefore, d' is a common divisor of a and b. Since d is the *greatest* common divisor of a and b, we must have $d' \leq d$.

4. Complete the proof of Theorem 1.13 in the notes: If there are integers x, y such that $ax + by = 1$, then $gcd(a, b) = 1$.

Proof Let $d = gcd(a, b)$. Then $d|a$ and $d|b$. Therefore d divides $ax + by$, which is a linear combination of a and b. Since $ax + by = 1$, this means that $d|1$. But the only divisors of 1 are ± 1; since d is the *greatest* common divisor of a and b, we must have $d = 1$.

Note It's tempting to try to apply Theorem 1.9 here, and argue something like this: "Theorem 1.9 says that $gcd(a, b) = ax + by$; $ax + by = 1$; therefore, $gcd(a, b) = 1$." The problem with this argument is that 1.9 tells us only that for *some* u, v, $gcd(a, b) = au + bv$. We're given that $ax + by = 1$. But why should u and v be the same as x and y?

In other words, 1.9 does not say that *every* linear combination of a and b equals $gcd(a, b)$. For example, $3(1) + 5(2) = 13$. Therefore, there exist x, y such that $3x + 5y = 13$. But it doesn't follow that $gcd(3, 5)$ equals 13.

What problem 4 is saying is that 1 is a special case; if $ax + by = 1$, then we *can* infer that $gcd(a, b) = 1$. But this does not follow from Theorem 1.9.

5. Prove the following: If $a|c$, $b|c$, and $gcd(a, b) = 1$, then $ab|c$.

Proof Since $gcd(a, b) = 1$, there are integers x and y such that $ax + by = 1$. Multiplying both sides of this equation by c, we obtain

$$c = cax + cby. \tag{1}$$

Since $a|c$ and $b|c$, there are integers u and v such that $c = au$ and $c = bv$. Substituting these equations into the right hand side of equation (1) yields

$$c = abvx + abuy. \tag{2}$$

Since ab divides the right hand side of (2), we must have $ab|c$.

6. Prove that if $m \perp n$, $a \equiv b \pmod{m}$, and $a \equiv b \pmod{n}$, then $a \equiv b \pmod{mn}$

Proof Since $a \equiv b \pmod{m}$, $a - b = km$ for some integer k.

Since $a \equiv b \pmod{n}$, $a - b = ln$ for some integer l

Therefore, $km = ln$. By the definition of divisibility, this means that m is a divisor of ln. Since $m \perp n$, Theorem 1.14 tells us that m must be a divisor of l; that is, $l = jm$ for some j.

So we have

$$a - b = ln = jmn.$$

Thus mn is a divisor of $a - b$, implying (once again by our workhorse basic fact (i)) that $a \equiv b \pmod{mn}$.

A second proof (A number of you noticed that you could use problem 5 to prove this one. This fact didn't occur to me when I made up the problem set; it was not my intention to give you problems that were so closely related.) By basic fact (i):

$$\begin{aligned} a \equiv b \pmod{m} &\Longrightarrow m|(a - b) \\ a \equiv b \pmod{n} &\Longrightarrow n|(a - b) \end{aligned}$$

Since $m \perp n$, problem 5 implies that $mn|(a - b)$. Therefore, by the basic fact, $a \equiv b \pmod{mn}$.

7. Let a be a non-negative integer, b, c, M positive integers. Let $d = gcd(c, M)$. Prove:

If there exists a k such that $a + kc \equiv b \bmod M$, then $d|(b - a)$.

Proof Assume that such a k does indeed exist. Then by basic fact (i) of modular equivalence, there is some x such that

$$(a + kc) - b = xM;$$

that is,

$$a - b = xM - kc. \tag{3}$$

Now let $d = gcd(c, M)$. Then d is a common divisor of c and M. Therefore, d divides the right hand side of (3). Therefore, d divides the left hand side; that is, d divides $a - b$.