MATH 4000/6000 – Homework #2

posted January 27; due by end of day on February 5

Mathematics is not a deductive science – that's a cliché. When you try to prove a theorem, you don't just list the hypotheses, and then start to reason. What you do is trial and error, experimentation, guesswork.
— Paul Halmos (1916–2006)

Assignments are expected to be neat and stapled. **Illegible work may not be marked**. Starred problems (*) are required for those in MATH 6000 and extra credit for those in MATH 4000.

0. (UNDERSTANDING CHECKS; DO NOT TURN IN)

   (a) Prove the *law of cancelation* in $\mathbb{Z}$: If $ab = ac$ and $a \neq 0$, then $b = c$.

   If $ab = ac$, then $a(b - c) = 0$. Now look back at Problem #4 on HW 1.

   (b) Recall that $\mathrm{CD}(a, b) = \{d \in \mathbb{Z} : d \mid a \text{ and } d \mid b\}$. Suppose $a, b, q, r \in \mathbb{Z}$ and $a = bq + r$. We claimed in class that $\mathrm{CD}(a, b) = \mathrm{CD}(b, r)$ and proved $\mathrm{CD}(a, b) \subseteq \mathrm{CD}(b, r)$. Complete the proof of our claim by showing the reverse containment, that $\mathrm{CD}(b, r) \subseteq \mathrm{CD}(a, b)$.

   (c) Fix $m \in \mathbb{Z}$. Prove that congruence modulo m is both symmetric and transitive.

---

1. For each integer a, put $D(a) = \{d \in \mathbb{Z} : d \mid a\}$. That is, $D(a)$ is the set of integers dividing a.

   (a) Prove, starting from the definition of "divides", that $D(a) = D(-a)$ for all $a \in \mathbb{Z}$.

   (b) Using (a), show that if b is a nonzero integer, then $\gcd(0, b) = |b|$.

   (c) Using (a), show that if a and b are both negative integers, then $\gcd(a, b) = \gcd(|a|, |b|)$.

   The moral of this problem: If we understand $\gcd(a, b)$ when a and b are positive integers, then we understand $\gcd(a, b)$ for all pairs of integers a, b.

2. Let a and b be integers. In class, we showed that if d is any integer for which $d \mid a$ and $d \mid b$, then $d \mid ax + by$ for all $x, y \in \mathbb{Z}$. We also claimed that $\gcd(a, b)$ can be written in the form $ax + by$ for some $x, y \in \mathbb{Z}$. (You will see why this claim holds Exercise 5 below.) Putting these two facts together, it follows immediately that

   $\gcd(a, b)$ is divisible by every common divisor of a and b.

   (All of this is given; you aren't being asked to prove the above.)

   Now let a and b be integers, not both 0.

   (a) Show that $\gcd(a, b) = 1 \iff$ there are integers x, y with $ax + by = 1$.

   (b) Give an example of integers a, b and d where $ax + by = d$ and where $d \neq \gcd(a, b)$.

3. Let a, b, and d be integers.

   (a) Prove that if $a \mid x$ and $b \mid y$ (where $x, y \in \mathbb{Z}$), then $ab \mid xy$.

   (b) Prove that if $d = \gcd(a, b)$, then $\gcd(a/d, b/d) = 1$.

   (c) Prove or give a counterexample: If $d = \gcd(a, b)$, then $\gcd(a/d, b) = 1$.

4. Suppose a, b, and n are positive integers for which $\gcd(a, n) = \gcd(b, n) = 1$. Prove or give a counterexample: $\gcd(ab, n) = 1$.

5. In class, it was claimed that for every pair of integers a, b (not both zero), there are $x, y \in \mathbb{Z}$ with $ax + by = \gcd(a, b)$.

   The Euclidean algorithm gives a constructive proof of this theorem. We illustrate with the example of $x = 942$ and $y = 408$. Here the Euclidean algorithm runs as follows:

$$\begin{aligned} 942 &= 408 \cdot 2 + 126 \\ 408 &= 126 \cdot 3 + 30 \\ 126 &= 30 \cdot 4 + 6 \\ 30 &= 6 \cdot 5 + 0. \end{aligned}$$

   In particular, $\gcd(942, 408) = 6$. So there should be $x, y \in \mathbb{Z}$ with $942x + 408y = 6$.

   We can find x, y by backtracking through the algorithm. First,

$$6 = 126 + 30(-4), \qquad \text{so we get 6 as a combination of } 126, 30.$$

   Next,

$$\begin{aligned} 6 &= 126 + (408 - 126 \cdot 3)(-4) \\ &= 408(-4) + 126(13), \qquad \text{so we get 6 as a combination of } 408, 126. \end{aligned}$$

   Continuing,

$$\begin{aligned} 6 &= 408(-4) + (942 - 408 \cdot 2)(13) \\ &= 942 \cdot 13 + 408(-30), \qquad \text{so we get 6 as a combination of } 942, 408. \end{aligned}$$

   (a) Using this method, find integers x and y with $17x + 97y = \gcd(17, 97)$.

   (b) Find integers x and y with $161x + 63y = \gcd(161, 63)$.

   Make sure you see why this method applies even if one or both of a and b is negative (see Problem #1). To test your understanding, after doing part (b), you should see how to write $\gcd(-161, 63)$ as $-161X + 63Y$ for some integers X, Y.

6. Let p be a prime number. Prove that if $a^2 \equiv b^2 \pmod{p}$, then $a \equiv b \pmod{p}$ or $a \equiv -b \pmod{p}$.

7. (Divisibility in Pythagorean triples) Recall that an ordered triple of integers x, y, z is called **Pythagorean** if $x^2 + y^2 = z^2$.

   (a) Show that in any Pythagorean triple, at least one of x, y, z is a multiple of 3.

   (b) Do part (a) again but with "3" replaced by "4", and then do it once more with "3" replaced by "5".

8. Let n be a positive integer. Suppose that the decimal digits of n — read from right-to-left — are $a_0, a_1, \ldots, a_k$. Show that

$$n \equiv a_0 + a_1 + a_2 + a_3 + \cdots + a_k \pmod{9}.$$

   Use this to determine the remainder when 2025 is divided by 9.

9. (Fermat's little theorem again) Complete the proof from class that when p is prime, $a^p \equiv a \pmod{p}$ for **all** integers a. In class, we [will have] only handled the case when $a \in \mathbb{Z}^+$.

   Hint: Don't reinvent the wheel. Find a way to deduce the general result from the case handled in class.

10. [REMOVED; DO NOT TURN IN!] ~~Solve the following congruences.~~

    (a) $3x \equiv 2 \pmod{5}$

    (b) $243x + 17 \equiv 101 \pmod{725}$

    (c) $20x \equiv 30 \pmod{4}$

    (d) $15x \equiv 25 \pmod{35}$

11(*). (a) Prove that there are infinitely many prime numbers.

(b) Prove that there are infinitely many prime numbers p satisfying $p \equiv 3 \pmod 4$.

12(*). The **Hilbert numbers** are the integers $1, 5, 9, 13, \ldots$ from the set $H = \{4k + 1 : k = 0, 1, 2, 3, \ldots\}$. If p is a Hilbert number, we call p a **Hilbert prime** if $p > 1$ and p cannot be factored in the form $p = ab$, where a and b are Hilbert numbers larger than 1.

(a) Prove that every Hilbert number $n > 1$ can be factored (in at least one way) as a product of Hilbert primes. (As in class, we allow factorizations involving a single prime.)

(b) Prove or give a counterexample: Every Hilbert number $n > 1$ factors uniquely as a product of Hilbert primes. (As in class, "unique" means unique up to rearrangement of the factors.)