CS 173, Spring 2009
Homework 2 Solutions

1. **[8 points]** Primes

   (a) Express the numbers 350, 105, and 64 as products of primes.

   Solution: $350 = 2 \cdot 5^2 \cdot 7$, $105 = 3 \cdot 5 \cdot 7$, and $64 = 2^6$

   (b) Compute GCD$(350, 105)$, GCD$(105, 64)$, and LCM$(350, 64)$. Feel free to give large results as products of primes; multiplying them out is not necessary.

   Solution:
   $GCD(350, 105) = 5 \cdot 7$
   $GCD(105, 64) = 1$
   $LCM(350, 64) = 2^6 \cdot 5^2 \cdot 7$

   (c) According to the definitions given in the book (or in lecture 7), which integers are neither prime nor composite?

   Solution: All integers which are strictly less than 2.

2. **[7 points]** Divisibility, congruence mod k

   Which of the following statements are correct? Show work or give brief explanations for your answers.

   Solution:

   (a) $-6 \mid 30$ is correct because $30 = (-6) \cdot (-5)$.
   (b) $30 \mid -6$ is incorrect because $\nexists k \in \mathbb{Z}$ such that $-6 = 30 \cdot k$.
   (c) $6 \mid -30$ is correct because $-30 = 6 \cdot (-5)$.
   (d) $-19 \equiv 7 \pmod{13}$ is correct because $13|(-19 - 7)$. Note that $-26 = 13 \cdot (-2)$.
   (e) $-6 \equiv 6 \pmod{4}$ is correct because $4|(-6 - 6)$. Note that $-12 = 4 \cdot (-3)$.
   (f) $-6 \equiv 6 \mod 24$ is incorrect because $24 \nmid (-6 - 6)$. Note that $-12 \neq 24 \cdot k$ for any $k \in \mathbb{Z}$.
   (g) $0 \equiv 17 \mod 17$ is correct because $17|(0 - 17)$. Note that $-17 = (-1) \cdot 17$.

3. **[10 points]** Direct proof using congruence mod k

   In the book, you will find several equivalent ways to define congruence mod k. For this problem, use the following definition: for any integers x and y and any positive integer m, $x \equiv y \pmod{m}$ if there is an integer k such that $x = y + km$.

   Using this definition prove that, for all integers x, y, p, q and m, with $m > 0$, if $x \equiv p \pmod{m}$ and $y \equiv q \pmod{m}$, then $(x^2 + y^2) \equiv (p^2 + q^2) \pmod{m}$.

   Solution: Let x, y, p, q and m all be integers satisfying the hypotheses given in the problem. Since $x \equiv p \pmod{m}$, by definition, there exists an integer k such that $x = p + k \cdot m$. Similarly, since $y \equiv q \pmod{m}$, there exists an integer l such that $x = q + l \cdot m$. Squaring both sides of the equations for x and y and then adding them together we obtain

$$\begin{aligned} x^2 + y^2 &= (p + km)^2 + (q + lm)^2 \\ &= (p^2 + 2pkm + k^2m^2) + (q^2 + 2qlm + l^2m^2) \\ &= (p^2 + q^2) + (2pkm + 2qlm + k^2m^2 + l^2m^2) \\ &= (p^2 + q^2) + (2pk + 2ql + k^2m + l^2m) \cdot m \\ &= (p^2 + q^2) + t \cdot m, \end{aligned}$$

   where we have let $t = 2pk + 2ql + k^2m + l^2m$. Notice that t is an integer, so, by definition, we have $(x^2 + y^2) \equiv (p^2 + q^2) \pmod{m}$, as desired.

4. **[10 points]** Proof by contradiction

   Consider the following claim

   $\forall x \in \mathbb{R}$, if $x^2 - 3x + 2 > 0$, then $x > 2$ or $x < 1$.

   (a) State the negation of this claim, moving all instances of "not" onto individual propositions and then making them disappear by inverting the inequalities.

   Solution: $\exists x \in \mathbb{R}$ such that $x^2 - 3x + 2 > 0$ and $x \leq 2$ and $x \geq 1$.
   Note that $x \leq 2$ and $x \geq 1$ may be rewritten as $1 \leq x \leq 2$.

   (b) Prove the claim using proof by contradiction.

   Solution: Let $x \in \mathbb{R}$ such that $x^2 - 3x + 2 > 0$ and $1 \leq x \leq 2$. Observe that we may factor $x^2 - 3x + 2$ as $(x - 2)(x - 1)$. Since $1 \leq x \leq 2$, we must have $(x - 2) \leq 0$ and $(x - 1) \geq 0$. Therefore, their product is either negative or zero, so $x^2 - 3x + 2 = (x - 2)(x - 1) \leq 0$, which contradicts our assumption that $x^2 - 3x + 2 > 0$. So by contradiction we have proven the claim.

5. **[15 points]** Another direct proof

For any two real numbers x and y, the harmonic mean of x and y is $H(x, y) = \frac{2xy}{x+y}$. This is a form of averaging that penalizes the case when either of the inputs is very small, often used for combining two performance numbers when evaluating a computer program.

(a) This definition has a small but important bug. What is it?

Solution: If $x + y = 0$, then the denominator is zero, so $H(x, y)$ is not defined when $x = -y$.

(b) The more familiar arithmetic mean is $M(x, y) = \frac{x+y}{2}$. When is $H(x, y)$ equal to $M(x, y)$?

Solution: Observe that

$$\begin{aligned} M(x,y) = H(x,y) &\implies \frac{x+y}{2} = \frac{2xy}{x+y} \\ &\implies (x+y)^2 = 4xy \\ &\implies (x+y)^2 - 4xy = 0 \\ &\implies x^2 - 2xy + y^2 = 0 \\ &\implies (x-y)^2 = 0 \\ &\implies x = y \end{aligned}$$

Thus, $M(x, y) = H(x, y)$ when $x = y$. (And, obviously, when x is not $-y$, because then $H(x, y)$ isn't defined.)

(c) Rephrase your answer to (b) in the form $\forall x, y \in \mathbb{R}, P(x, y) \rightarrow Q(x, y)$, for some suitable choice of predicates $P(x, y)$ and $Q(x, y)$. (Hint: in this case, the predicates are equations.)

Solution: $\forall x, y \in \mathbb{R}\big[(M(x, y) = H(x, y)) \rightarrow (x = y)\big]$

(d) Prove that your answer to (b) is correct.

Solution: Let $x, y \in \mathbb{R}$. Suppose $M(x, y) = H(x, y)$. By the string of implications in part (b), we conclude that $x = y$. Thus, $M(x, y)$ and $H(x, y)$ are equal only when $x = y$.