CSI 2101 Winter 2017
Prof Lucia Moura University of Ottawa

Assignment #2 SOLUTION

1. (8 marks) Given real numbers a and b we define: $\min(a,b) = a$ if $a \leq b$, and $\min(a,b) = b$, otherwise; we also define: $\max(a,b) = a$ if $a \geq b$, and $\max(a,b) = b$, otherwise.
   Use a proof by cases to prove each of the following statements for a, b, c real numbers:

   (a) $\min(a,b) + \max(a,b) = a + b$.

   (b) $\min(a, \min(b,c)) = \min(\min(a,b), c)$.

   Answer:

   (a) We will consider the following three cases: $a = b$, $a > b$ and $a < b$.
   Case 1: $a = b$.
   Applying the definitions to this case, $\min(a,b) = a$ and $\max(a,b) = a$. But since $a = b$, $\max(a,b) = b$. Therefore, $\min(a,b) + \max(a,b) = a + b$.
   Case 2: $a < b$.
   Applying the definitions to this case, $\min(a,b) = a$ and $\max(a,b) = b$, so $\min(a,b) + \max(a,b) = a + b$.
   Case 3: $a > b$.
   Applying the definitions to this case, $\min(a,b) = b$ and $\max(a,b) = a$, so $\min(a,b) + \max(a,b) = b + a = a + b$.
   In each of the three cases we got the formula given in (a), so we have completed the proof.

   (b) $\min(a, \min(b,c)) = \min(\min(a,b), c)$.
   We conveniently divide the possible scenarios into the 3 possible cases below. Your solution may involve more cases and sub-cases and be correct.
   Case 1: $b \leq c$
   In this case, $\min(b,c) = b$, so $\min(a, \min(b,c)) = \min(a,b)$.
   On the other, $\min(a,b) \leq b \leq c$, so $\min(\min(a,b), c) = \min(a,b)$
   Case 2: $b > c$ and $a > b$
   In this case, $a > c$, $\min(a,c) = c$, $\min(b,c) = c$, and $\min(a,b) = b$.
   So, $\min(a, \min(b,c)) = \min(a,c) = c$ and $\min(\min(a,b), c) = \min(b,c) = c$
   Case 3: $b > c$ and $a \leq b$
   In this case, $\min(b,c) = c$ and $\min(a,b) = a$.
   So, $\min(a, \min(b,c)) = \min(a,c)$ and $\min(\min(a,b), c) = \min(a,c)$. In each of the three cases we got the formula given in (b), so we have completed the proof.

2. (5 marks)
   (Advice: revise the definitions of odd *and* even *integer numbers as well as the fact that an integer number is either odd or even, but not both.)*
   Consider the following definition.
   Definition: An integer n is *grumpty* if and only if $n^2 + 2n$ is odd.
   Use a proof by contraposition to show that all grumpty integers are odd.

Answer:
We assume n is not odd, or in other words, n is even. So there exists k such that $n = 2k$. Thus, $n^2+2n = (2k)^2+2(2k) = 2(2k^2+2k)$. Thus n^2+2n is even, and therefore not grumpy.

3. (6 marks) *(Advice: revise the definitions of* rational *and* irrational *numbers.)*
Use a proof by contradiction to show the following: Let x and y be real numbers with $x \neq 0$. If x is rational and y is irrational, then xy is irrational.

Answer:
Recall that to prove $p \to q$ by contradiction we prove $(p \wedge \neg q) \to \mathbf{F}$, since $\neg(p \to q) \equiv (p \wedge \neg q)$. Assume x is rational, and y is irrational and xy is rational. Since x is rational, there exist integers a and b, $b \neq 0$ such that $x = a/b$.
Since xy is rational, there exist integers c and d, $d \neq 0$ such that $xy = c/d$.
Thus $\frac{c}{d} = xy = \frac{a}{b}y$. Then,

$$\begin{aligned} \frac{a}{b}\, y &= \frac{c}{d} \\ ay &= \frac{bc}{d}. \quad \text{(multiply both sides by } b\text{)} \\ y &= \frac{bc}{ad} \quad \text{(we can divide by } a, \text{ since } x \neq 0 \text{ implies a} \neq 0\text{)} \end{aligned}$$

Since we y can be written as one integer divided by another, y is rational, which contradicts the hypothesis that y is irrational.

4. (7 marks=2+5) Prove the following facts:

   (a) For every integer n, the number $n(n+1)$ is even.

   (b) If n is an odd positive number then $n^2 \equiv 1 \pmod 8$.

   Answer:

   (a) If n is even then there exists k such that $n = 2k$, so $n(n+1) = 2k(n+1)$, which implies $n(n+1)$ is even. If n is odd, then there exists k such that $n = 2k+1$, so $n(n+1) = (2k+1)(2k+2) = 2(2k+1)(k+1)$, which implies $n(n+1)$ is even.

   (b) Since n is odd, there exists k such that $n = 2k+1$. Thus, $n^2 = (2k+1)^2 = 4k^2+4k+1 = 4k(k+1)+1$. Since $k(k+1)$ is even, there exists an integer m such that $k(k+1) = 2m$. Substituting this equation back into the previous equation $n^2 = 4k(k+1)+1 = 4(2m)+1 = 8m+1$, and we get $n^2-1 = 8m$. Therefore, $8|(n^2-1)$ which implies $n^2 \equiv 1 \pmod 8$.

5. (4 marks) Let p, q, r, s be distinct prime numbers. If the product of two integers is $p^7q^8r^2s^{11}$ and their greatest common divisor is p^3q^4r what is their least common multiple?

   Answer: Since $a \cdot b = \text{lcm}(a,b) \cdot \gcd(a,b)$, we get $\text{lcm}(a,b) = (a \cdot b)/\gcd(a,b)$. Substituting the values above, $\text{lcm}(a,b) = (p^7q^8r^2s^{11})/(p^3q^4r) = p^4q^4rs^{11}$.

6. (6 marks) Use the extended Euclidean algorithm to express 2115 and 900 as a linear combination of $\gcd(2115, 900)$. Show your derivation to find the gcd and the steps of the backward substitution used to get integers s and t such that $s \cdot 2115 + t \cdot 900 = \gcd(2115, 900)$.

Answer:

$$\begin{aligned} 2115 &= 2 \cdot \mathbf{900} + \mathbf{315} \\ 900 &= 2 \cdot \mathbf{315} + \mathbf{270} \\ 315 &= 1 \cdot \mathbf{270} + \mathbf{45} \\ 270 &= 6 \cdot \mathbf{45} + \mathbf{0} \end{aligned}$$

Thus, $\gcd(2115, 900) = 45$. Now, doing back substitution

$$\begin{aligned} 45 &= 315 - 1 \cdot 270 \\ &= 315 - 1 \cdot (900 - 2 \cdot 315) = 3 \cdot 315 - 900 \\ &= 3 \cdot (2115 - 2 \cdot 900) - 900 = 3 \cdot 2115 + (-7) \cdot 900. \end{aligned}$$

So $s = 3$ and $t = -7$.

7. (6 marks) Use the extended Euclidean algorithm to compute an integer a, $0 \leq a < 28$, that is an inverse of 15 (mod 28). (Recall that by definition of inverse $15a \equiv 1 \pmod{28}$.)

   Answer:

$$\begin{aligned} 28 &= 1 \cdot \mathbf{15} + \mathbf{13} \\ 15 &= 1 \cdot \mathbf{13} + \mathbf{2} \\ 13 &= 6 \cdot \mathbf{2} + \mathbf{1} \\ 2 &= 2 \cdot \mathbf{1} + \mathbf{0} \end{aligned}$$

   Thus, $\gcd(28, 15) = 1$. Now, using the second to last equation until the first, in order, we get

$$\begin{aligned} 1 &= 13 - 6 \cdot 2 \\ &= 13 - 6 \cdot (15 - 1 \cdot 13) = 7 \cdot 13 - 6 \cdot 15 \\ &= 7 \cdot (28 - 1 \cdot 15) - 6 \cdot 15 = 7 \cdot 28 + (-13) \cdot 15. \end{aligned}$$

   So, $1 = 7 \cdot 28 + (-13) \cdot 15$, thus $1 - (-13) = 7 \cdot 28$, which implies $(-13) \equiv 1 \pmod{28}$. Thus the inverses of 15 are the integers of the form $-13 + d \cdot 28$ for some integer d. Taking $d = 1$ we obtain $a = 15$. Double checking $15 \cdot 15 = 8 \cdot 28 + 1$, so $15 \cdot 15 \equiv 1 \pmod{28}$.

8. (8 marks) Prove that for every positive integer n, there are n consecutive composite integers. Hint: Consider the n consecutive integers starting with $(n+1)! + 2$.
   Example: for $n = 3$, we verify that $4!+2 = 26$, $4!+3 = 27$, $4!+4 = 28$ are composite numbers, where $4! = 4 \cdot 3 \cdot 2 \cdot 1$.

   Answer:
   Let n be a positive integer. We claim $(n+1)! + 2, (n+1)! + 3, \ldots, (n+1)! + (n+1)$ are composite numbers. Note that $(n+1)! = (n+1) \cdot n \cdots 3 \cdot 2 \cdot 1$, we claim that $i | (n+1)! + i$, for $i = 2, 3, \ldots, (n+1)$. Indeed, since $i | (n+1) \cdot n \cdots 3 \cdot 2 \cdot 1$ and $i | i$, $i | (n+1)! + i$. Thus, $(n+1)! + i$ has a divisor for every i where $2 \leq i < (n+1)$. Therefore $(n+1)! + i$ is composite for $i = 2, 3, \ldots, (n+1)$ which are n consecutive composite integers.