MCS 150 Final Exam Solutions

Dec 15, 2017

1. (10 pts) The Division Algorithm says that if $n \in Z$ and $d \in \mathbb{Z}^+$, then there exist unique integers q, r such that $n = qd + r$ where $0 \le r < d$. Give a proof.

   Let $S = \{n - kd \mid k \in \mathbb{Z} \text{ and } n - kd \ge 0\}$. Notice that S is nonempty because if $n \ge 0$ then $n \in S$ and if $n < 0$ then $n - nd = n(1 - d) \ge 0$ since $1 - d \le 0$. Hence S is a nonempty set of nonnegative integers. By the Well-Ordering Principle, S contains a smallest element r. This must be of the form $r = n - qd$ for some $q \in \mathbb{Z}$. Obviously, $r \ge 0$ since $r \in S$. Now, suppose $r \ge d$. Then $0 \le r - d = n - (q + 1)d$ must also be in S. But $r - d < r$, so this would contradict the minimality of r. Hence we can conclude $0 \le r < d$ and $n = qd + r$.

   For the uniqueness, suppose $n = q_1 d + r_1 = q_2 d + r_2$ for some $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ and $0 \le r_1, r_2 < d$. Then $r_1 - r_2 = q_2 d - q_1 d = (q_2 - q_1)d$. This shows $r_1 - r_2$ is a multiple of d. But we know $0 \le r_1, r_2 < d$, so $-d < r_1 - r_2 < d$. The only multiple of d in that range is 0. Hence $r_1 - r_2 = 0$, which shows $r_1 = r_2$. Since $d \ne 0$, it now follows that $q_1 - q_2 = 0$, and hence $q_1 = q_2$. Therefore there is only one way to write $n = qd + r$ where $q, r \in \mathbb{Z}$ and $0 \le r < d$.

2. (5 pts each)

   (a) Let A and B be sets. Is the following statement true? If you think it is true, find a convincing argument to show it is true; if not, find an argument or a counterexample to show it is false.

   $$(A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A)$$

   This is true.

   $$(A \cup B) \setminus (A \cap B) = \{x \mid x \in A \text{ or } x \in B \text{ and } x \text{ is not in both } A \text{ and } B\}.$$

   $$(A \setminus B) \cup (B \setminus A) = \{x \mid x \in A \text{ but } x \notin B \text{ or } x \in B \text{ but } x \notin A\}.$$

   That is the sets on both sides contain those elements that are in exactly one of A or B and not in the other. Hence the two sides are equal.

   (b) Prove or disprove (e.g. by finding a counterexample) the following statement. If n is an integer such that $2|n$ and $3|n$ then $6|n$.

   This is also true. It follows from the general fact that if a and b are relatively prime integers and $a|n$ and $b|n$ then $ab|n$. Here is why. Since $a|n$ we have $n = ka$ for some $k \in \mathbb{Z}$. Similarly, we have $n = mb$ for some $m \in \mathbb{Z}$. As a and b are relatively prime, we know $1 = la + zb$ for some $l, z \in \mathbb{Z}$. Hence

   $$k = k(la + zb) = l(ka) + kzb = l(mb) + kzb = (lm + kz)b$$

   Obviously, $lm + kz \in \mathbb{Z}$. Let $t = lm + kz$. The $n = ka = (tb)a = t(ab)$.
   Since 2 and 3 are relatively prime, $2|n$ and $3|n$ implies $6|n$.

   Of course, in this particular case, a quicker argument to make is that since $3|n$, $n = 3k$ for some $k \in \mathbb{Z}$ and since $2|3k$ and 2 is a prime number, either $2|3$ or $2|k$ by Euclid's Lemma. Since $2 \not| 3$, it nust be that $2|k$, So $k = 2m$ for some $m \in \mathbb{Z}$. Now $n = 3(2m) = 6m$.

   (c) Let x, y be odd integers. Use modular arithmetic modulo some appropriate $n \in \mathbb{Z}$ to prove that $4 \nmid (x^2 + y^2)$.

We will work modulo 4. If x is odd, then $x \equiv 1 \pmod 4$ or $x \equiv 3 \pmod 4$. Hence $x^2 \equiv 1 \pmod 4$ or $x^2 \equiv 9 \equiv 1 \pmod 4$. The same is true for y. So $x^2 + y^2 \equiv 1 + 1 \equiv 2 \pmod 4$. Therefore $x^2 + y^2$ is not divisible by 4.

3. (10 pts) In this exercise, you will prove that our definition of the greatest common divisor is equivalent to the one you learned in middle school. Let $m, n \in \mathbb{Z}$ not both 0.

   Suppose $d_1 > 0$ is the greatest common divisor of m and n according to our definition:
   (a) $d_1|m$ and $d_1|n$,
   (b) if c is an integer such that $c|m$ and $c|n$ then $c|d_1$.

   Let d_2 be the common divisor of m and n that is the largest number among the common divisors. That is we know
   (a) $d_2|m$ and $d_2|n$,
   (b) if c is an integer such that $c|m$ and $c|n$ then $c \leq d_2$.

   Show that $d_1 = d_2$.

   Since $d_1|m$ and $d_1|n$, we know $d_1 \leq d_2$. Since $d_2|m$ and $d_2|n$, we know $d_2|d_1$. So $d_1 = kd_2$ for some $k \in \mathbb{Z}$. Notice that k must be positive as d_1 and d_2 are both positive. Now, $kd_2 = d_1 \leq d_2$, and dividing by $d_2 > 0$ shows $k \leq 1$. The only such positive integer is $k = 1$. Hence $d_1 = d_2$.

4. Let $n \in \mathbb{Z}^+$.
   (a) (3 pts) If $x \in \mathbb{Z}$, define the multiplicative order of x modulo n.

   The multiplicative order of an integer x modulo n is the least $k \in \mathbb{Z}^+$ such that

   $$x^k \equiv 1 \pmod n.$$

   (b) (6 pts) Prove that there is a positive integer k such that $x^k \equiv 1 \pmod n$ if and only if x is relatively prime to n.

   Suppose $x^k \equiv 1 \pmod n$ for some $k \in \mathbb{Z}^+$. Then $x^k = 1 + zn$ for some $z \in \mathbb{Z}$. Hence $1 = x^k - zn$. Let $d = \gcd(x, n)$. Since $d|x^k$ and $d|zn$, so $d|x^k - zn = 1$. Hence $d = 1$ and x and n are relatively prime.
   Conversely, suppose x is relatively prime to n. Look at the list $x, x^2, x^3, \ldots$. Since there are only n different remainders after division by n, the elements in this list cannot all be different modulo n. There must be some $a < b$ such that $x^a \equiv x^b \pmod n$. We know x is relatively prime to n, so x has a multiplicative inverse x^{-1} modulo n. Multiply both sides by $\left(x^{-1}\right)^a$ to get

   $$1 \equiv \left(x^{-1}\right)^a x^a \equiv \left(x^{-1}\right)^a x^b \equiv x^{b-a} \pmod n.$$

   Now, $k = b - a$ is a positive integer and $x^{b-a} \equiv 1 \pmod n$.

   (c) (6 pts) Prove that if x is relatively prime to n, then $x^{\phi(n)} \equiv 1 \pmod n$ where $\phi(n)$ is the Euler (totient) function.

   Let $S = \{y \mid y \in \mathbb{Z}, 0 \leq y < n, \text{ and } \gcd(y, n) = 1\}$. Notice that S consists of those canonical representatives modulo n that are units. We know S has $\phi(n)$ elements. Let us label them $S = \{y_1, y_2, \ldots, y_{\phi(n)}\}$. Now, let $T = \{xy_i \mid i = 1, \ldots \phi(n)\}$. Since x and y_i here are all units, each xy_i is also a unit by problem 2 on Homework 5. Now, if $xy_i \equiv xy_j \pmod n$ then $y_i \equiv x^{-1}xy_i \equiv x^{-1}xy_j \equiv y_j \pmod n$. Hence the xy_i's in T are all distinct. Therefore T also consists of all of the units modulo n. That is $S = T$. So the product of all the elements in S is the same as the product of all the elements in T:

   $$y_1 y_2 \cdots y_{\phi(n)} \equiv (xy_1)(xy_2) \cdots (xy_{\phi(n)}) \pmod n.$$

Rearranging this a bit gives

$$y_1 y_2 \cdots y_{\phi(n)} \equiv x^{\phi(n)} y_1 y_2) \cdots x_{\phi(n)} \pmod{n}.$$

Since the y's are all units, we can cancel them from this equivalence by multiplying both sides by their inverses This results in $1 \equiv x^{\phi(n)} \pmod{n}$.

5. (10 pts) Bob, the carpenter likes to do his calculations in base 9, for reasons that should be obvious if you think about it a little. But many materials Bob uses come in sizes that are multiples of 4, e.g. 4' by 8' plywood sheets. Help Bob by devising a quick and easy strategy to check if a positive integer expressed in base 9 is divisible by 4. Prove that your divisibility test works.

   Bob can check for divisibility by 4 by adding the digits of the integer and checking if their sum is divisible by 4. E.g. starting with the number 723_9, he would add $7+2+3 = 13_9$ and $4|13_9$, so $4|723_9$. Note that he can check if $4|13_9$ either directly, or by adding $1+3=4$ and noting that $4|4$. To show this test works, let $n = d_k 9^k + d_{k-1} 9^{k-1} + \cdots + d_1 9 + d_0$. Notice that $9 \equiv 1 \pmod{4}$, and hence $9^j \equiv 1^j \equiv 1 \pmod{4}$ for any $j \in \mathbb{Z}^{\geq 0}$. Therefore

$$n \equiv d_k 9^k + d_{k-1} 9^{k-1} + \cdots + d_1 9 + d_0 \pmod{4} \equiv d_k + d_{k-1} + \cdots + d_1 + d_0 \pmod{4}.$$

   This shows that $4|n$ if and only if $4|d_k + d_{k-1} + \cdots + d_1 + d_0$.

6. (10 pts) The Lucas numbers are defined by the following recursive relationship:

$$\begin{aligned} L_0 &= 2 \\ L_1 &= 1 \\ L_n &= L_{n-1} + L_{n-2} && \text{for } n \geq 2. \end{aligned}$$

   Here are the first few Lucas numbers:

$$2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, \ldots.$$

   Prove that any two consecutive Lucas numbers are relatively prime.

   This can be done by induction, exactly the same way we proved that two consecutive Fibonacci numbers are relatively prime. Notice that L_0 and L_1 are relatively prime. This establishes the base case for our induction. For the inductive hypothesis, suppose that L_n and L_{n+1} are relatively prime. Now suppose that $d \in \mathbb{Z}^+$ divides both L_{n+1} and L_{n+2}. Then d also divides $L_{n+2} - L_{n+1} = L_n$. Hence d is a common divisor of L_n and L_{n+1}. By the inductive hypothesis, $d = 1$. So L_{n+1} and L_{n+2} are relatively prime.

7. (5 pts each) **Extra credit problem.** Let $S_1, S_2, \ldots, S_n$ be finite sets. Our goal in this problem is to prove the Inclusion-Exclusion Principle, which says

$$|S_1 \cup \cdots \cup S_n| = \sum_{i=1}^{n} |S_i| - \sum_{1 \leq i < j \leq n} |S_i \cap S_j| + \sum_{1 \leq i < j < k \leq n} |S_i \cap S_j \cap S_k| - \cdots - (-1)^n |S_1 \cap \cdots \cap S_n|.$$

   For example, if $n = 3$ then

$$|S_1 \cup S_2 \cup S_s| = |S_1| + |S_2| + |S_3| - |S_1 \cap S_2| - |S_1 \cap S_3| - |S_2 \cap S_3| + |S_1 \cap S_2 \cap S_3|.$$

   (a) Suppose that x is in m of the sets and not in the other $n-m$. How many different ways can you choose k out of the sets $S_1, S_2, \ldots, S_n$ so that their intersection contains x?

   In order for x to be in the intersection of k of the sets, all of them must contain x. So we must choose the k sets from among the m that contain x. There are $\binom{m}{k}$ ways to choose k out of m objects if the order does not matter. And the order obviously does not matter as the intersection of sets is commutative.

(b) Prove that

$$\binom{n}{1} - \binom{n}{2} + \binom{n}{3} - \cdots - (-1)^n \binom{n}{n} = 1.$$

Hint: Use the binomial theorem.

By the binomial theorem

$$\begin{aligned}
0 &= ((-1)+1)^n \\
&= \binom{n}{n}(-1)^n 1^0 + \binom{n}{n-1}(-1)^{n-1}1^1 + \cdots + \\
&\quad \binom{n}{2}(-1)^2 1^{n-2} + \binom{n}{1}(-1)^1 1^{n-1} + \binom{n}{0}(-1)^0 1^n \\
&= (-1)^n \binom{n}{n} + (-1)^{n-1}\binom{n}{n-1} + \cdots + \binom{n}{2} - \binom{n}{1} + \binom{n}{0}
\end{aligned}$$

By moving all but the $\binom{n}{0}$ term to the other side, it follows that

$$1 = \binom{n}{0} = -(-1)^n \binom{n}{n} - (-1)^{n-1}\binom{n}{n-1} - \cdots - \binom{n}{2} + \binom{n}{1},$$

which is what we wanted to show.

(c) Prove the Inclusion-Exclusion Principle by looking at how many times each element $x \in S_1 \cup \cdots \cup S_n$ is counted in the expression

$$\sum_{i=1}^{n} |S_i| - \sum_{1 \le i < j \le n} |S_i \cap S_j| + \sum_{1 \le i < j < k \le n} |S_i \cap S_j \cap S_k| - \cdots + (-1)^n |S_1 \cap \cdots \cap S_n|.$$

If $x \in S_1 \cup \cdots \cup S_n$, then x is counted exactly once in $|S_1 \cup \cdots \cup S_n|$ on the left-hand side of the equation. Let's see how many times x is counted on the right-hand side. Since x is in the union, it must be in some of the sets. Suppose it is in k of the n sets. Then it is counted k times in $\sum_{i=1}^{n} |S_i|$. It is also in $\binom{k}{2}$ of the pairwise intersections, so it is counted $\binom{k}{2}$ times in $\sum_{1 \le i < j \le n} |S_i \cap S_j|$. It shows up $\binom{k}{3}$ times in the intersections of three sets. And so on. No intersection of more than k of the sets contains x, so it is counted 0 times in such higher intersections. Therefore x contributes

$$k - \binom{k}{2} + \binom{k}{3} - \cdots - (-1)^k \binom{k}{k}$$

times to the number

$$\sum_{i=1}^{n} |S_i| - \sum_{1 \le i < j \le n} |S_i \cap S_j| + \sum_{1 \le i < j < k \le n} |S_i \cap S_j \cap S_k| - \cdots - (-1)^n |S_1 \cap \cdots \cap S_n|.$$

But as we showed in part (b),

$$k - \binom{k}{2} + \binom{k}{3} - \cdots - (-1)^k \binom{k}{k} = 1.$$

So each element $x \in S_1 \cup \cdots \cup S_n$ is counted exactly once on each side of

$$|S_1 \cup \cdots \cup S_n| = \sum_{i=1}^{n} |S_i| - \sum_{1 \le i < j \le n} |S_i \cap S_j| + \sum_{1 \le i < j < k \le n} |S_i \cap S_j \cap S_k| - \cdots - (-1)^n |S_1 \cap \cdots \cap S_n|.$$

Therefore the two sides are indeed equal.