Problem Set 4

Due: Wednesday, April 26, by 11:59pm

Instructions

Solutions submission. You must submit your solution via Gradescope. In particular:

- Submit a single PDF file in Gradescope containing the written solution to all the regular tasks in the homework.

- The extra credit is submitted separately in Gradescope

Task 1 – Oddly Even [14 pts]

Let n be an integer.

a) Give an English proof that if n^3 is even then n is even. (Try experimenting with different proof strategies if you don't see how to do this right away.)

b) Give an English proof that if n^3 is odd then n is odd.

Task 2 – Modular Numerology [20 pts]

Let a, b be integers and c, m be positive integers.
Prove that $a \equiv b$ (mod m) if and only if $ca \equiv cb$ (mod cm).
(Remember that there are two directions to prove.)

Task 3 – Prime Examples [16 pts]

Prove that for any prime $p > 3$, either $p \equiv 1 \pmod 6$ or $p \equiv 5 \pmod 6$.

Task 4 – Prime Rib [10 pts]

Prove or disprove: For every integer $n \geqslant 0$, $n^2 + n + 17$ is prime.

Task 5 – GCD [10 pts]

Compute the following GCDs using Euclid's algorithm. Show your work in tableau form. Clearly indicate which number is your answer.

a) $gcd(91, 69)$

b) $gcd(90, 38)$

Task 6 – Multiplicative inverse [10 pts]

Let $a = 26$ and $m = 49$. Compute the multiplicative inverse of a modulo m (i.e., the integer b with $0 \leqslant b < m$ such that $ab \equiv 1 \pmod{m}$). Use the Extended Euclidean Algorithm. Show your work by including the forward tableau, the rearranged tableau, and the chain of back-substitutions.

Finally, compute the integer ab and show its quotient and remainder when dividing by m. (The remainder should be 1 if you have done the problem correctly.)

Task 7 – Solving congruences I [10 pts]

This problem walks through how to solve a modular congruence.

a) Consider the congruence $8x - 2 \equiv 1 \pmod{21}$, where x is an integer. Using the fact from lecture that we can add the same number to both sides of a congruence, rearrange this congruence so that the $8x$ appears by itself on the left side, and a single number appears on the right side.

b) Using our intuition from algebra, we would next like to "divide" by 8. To do so, we will multiply by the multiplicative inverse of 8 modulo 21. Let b stand for the multiplicative inverse of 8 modulo 21. Compute b using the Extended Euclidean Algorithm, showing your work by including the forward tableau, the rearranged tableau, and the chain of back-substitutions.

c) Now multiply both sides of your congruence by b to get a congruence with x by itself on the left side and a single number on the right side. Simplify the number on the right so that it is non-negative and less than 21. Let c stand for this right-hand side. (We have shown that every solution to the original congruence is congruent to c modulo 21.)

d) Plug the specific number c from the previous part in for x in the original congruence $8x - 2 \equiv 1 \pmod{21}$ and show that the congruence holds by simplifying. (This shows that c *is* a solution to the original congruence.)

Task 8 – Solving congruences II [10 pts]

In this problem, we will see that even when the multiplicative inverse does not exist, it is still *sometimes* possible to solve modular congruences.

a) Consider the congruence $16x \equiv 14 \pmod{22}$. Explain why we cannot just divide by 16 here. (You do not need to show any calculations you do, just explain why the results of those calculations show that we cannot divide by 16.)

b) Use the result you proved in Task 2 to write a simplified version of the congruence from part (a) by pulling out and eliminating a common factor. Your simplified congruence should have the form $ax \equiv d \pmod{m}$ for some integers a, d and m such that $gcd(a, m) = 1$.

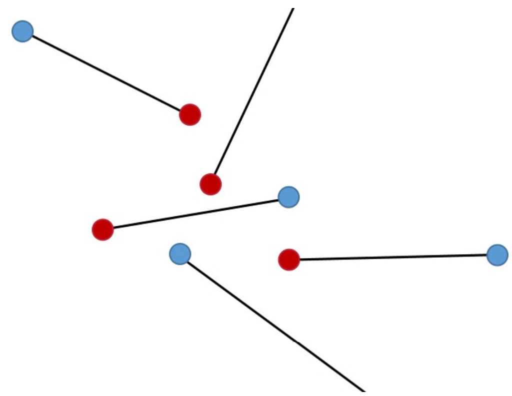
c) Use the Extended Euclidean Algorithm to compute the multiplicative inverse of a modulo m. Call that number b. Show your work by including the forward tableau, the rearranged tableau, and the chain of back-substitutions. Simplify your value of b so that it is non-negative and less than m.

d) Now multiply both sides of your congruence by b to get a congruence with x by itself on the left side and a single number on the right side. Simplify the number on the right so that it is non-negative and less than m. Let c stand for this right-hand side. (We have shown that every solution to the original congruence is congruent to c modulo m.)

e) Plug the specific number c from the previous part in for x in the original congruence $16x \equiv 14 \pmod{22}$ and show that the congruence holds by simplifying. (This shows that c *is* a solution to the original congruence.)

Task 9 – Extra Credit: Matchmaker, Matchmaker, Make Me a Match

In this problem, you will show that given n red points and n blue points in the plane such that no three points lie on a common line, it is possible to draw line segments between red-blue pairs so that all the pairs are matched and none of the line segments intersect. Assume that there are n red and n blue points fixed in the plane.



A *matching* M is a collection of n line segments connecting distinct red-blue pairs. The *total length* of a matching M is the sum of the lengths of the line segments in M. Say that a matching M is *minimal* if there is no matching with a smaller total length.

Let IsMinimal(M) be the predicate that is true precisely when M is a minimal matching. Let HasCrossing(M) be the predicate that is true precisely when there are two line segments in M that cross each other.

a) Give an argument in English explaining why there must be at least one matching M so that IsMinimal(M) is true, i.e.

$$\exists M \ \text{IsMinimal}(M)$$

b) Give an argument in English explaining why

$$\forall M \ (\text{HasCrossing}(M) \rightarrow \neg\text{IsMinimal}(M))$$

c) Now use the two results above to give a proof of the statement:

$$\exists M \ \neg\text{HasCrossing}(M).$$