Test I Math 305 Spring 2022 (Solutions)

Dr Holmes

February 7, 2022

The exam begins officially at 12 noon and ends at 1:15 pm. What actually happens at 1:15 is that I give a five minute warning.

There are 10 numbered questions on this exam. Complete eight of them. If you do more than eight of them, you will receive credit for the best 8 of them, and some extra credit is possible if the dropped questions have significant value.

You may use a scientific calculator without graphing capability. You are strongly encouraged to use my table format for computing the extended Euclidean algorithm.

You may bring a single sheet of standard sized notebook paper to the exam, with whatever you like written or printed on it.

You may not use anything on the exam but your test paper, your writing instrument, your non-graphing calculator and your single sheet of notebook paper.

1. Prove using the well-ordering principle and standard algebra, including basic properties of order, that there is no integer between 0 and 1.

   Suppose for the sake of a contradiction that there is an integer n such that $0 < n < 1$. Then the set $\{k \in \mathbb{Z} : 0 < k < 1\}$ is nonempty, and so by the Well-Ordering Principle has a smallest element w. Since $0 < w < 1$ (which tells us w is positive) we have $0 < w^2 < w$. But then $0 < w^2 < w < 1$ tells us that $w^2 \in S$, which is a contradiction because w^2 is less than w, which is supposed to be the smallest element of S.

2. Prove by mathematical induction that $\sum_{i=1}^{n}(2i-1) = n^2$.

   We prove this by induction on n.

   $\sum_{i=1}^{1}(2i-1) = 2(1) - 1 = 1 = 1^2$, check

   Let k be an arbitrarily chosen positive integer.

   Assume (ind hyp) that $\sum_{i=1}^{k}(2i-1) = k^2$, completing the proof of the basis step.

   The induction goal is to show that $\sum_{i=1}^{k+1}(2i-1) = (k+1)^2$

   We prove the induction goal:

   $\sum_{i=1}^{k+1}(2i-1) = \sum_{i=1}^{k}(2i-1) + 2(k+1) - 1$ (facts about summation)

   $= k^2 + 2(k+1) - 1$ ind hype

   $= k^2 + 2k + 1 = (k+1)^2$ by algebra, which is what was to be proved in the induction step.

3. Find $\texttt{gcd}(37, 25)$ and find integers x and y such that $37x + 25y = \texttt{gcd}(37, 25)$. **using the extended Euclidean algorithm**. No substitutes accepted.

   Please make it clear that you know what $\texttt{gcd}(37, 25)$ is and what x and y are.

   You are **required** to present a calculation using a general procedure recognizable as the extended Euclidean algorithm to find these answers: preferably, use the table layout I use in class and in the notes. Of course you know what the gcd is and you might be able to find x and y by trial and error. This will not be good for much if any credit.

   Here is the table calculation in my format. Other similar procedures might have been accepted.

	x	y	q
37	1	0	
25	0	1	
$37 - (1)(25) = 12$	$1 - (1)0 = 1$	$0 - (1)1 = -1$	$37\texttt{div}25 = 1$
$25 - (2)(12) = 1$	$0 - (2)1 = -2$	$1 - (2)(-1) = 3$	$25\texttt{div}12 = 2$

   Of course, your table doesnt have to show all the calculations: I am doing this just to illustrate how the procedure works.

   $\texttt{gcd}(37, 25) = 1 = (-2)(37) + 3(25)$.

4. Prove Euclid's lemma using the Bezout identity.

   Euclid's lemma is the statement "for any integers a, b and prime p, if $p|ab$ then either $p|a$ or $p|b$"

   The Bezout identity is "for any a, b not both equal to 0, there are integers x and y such that $\texttt{gcd}(a, b) = ax + by$."

   Suppose that a, b are integers and p is prime.

   Suppose that $p|ab$: the goal is to show $p|a$ or $p|b$.

   If $p|a$ we are done; it remains to show that if $p \not| a$ it follows that $p|b$.

   If $p \not| a$ it follows (because p is prime) that $\texttt{gcd}(a, p) = 1$, so (Bezout identity) there are integers x and y such that $ax + py = 1$.

   and thus $b = 1b = (ax + py)b = abx + pyb$. abx is divisible by p because ab is divisible by p; pyb is divisible by p by inspection, so $abx + pyb = b$ is divisible by p, completing the proof.

5. Write three distinct primitive Pythagorean triples.

   Lots of different solutions for this: if s and t are odd and relatively prime, compute $a = st$, $b = \frac{s^2-t^2}{2}$, $c = \frac{s^2+t^2}{2}$

   Demonstrate (using mod 5 arithmetic) that if $a^2+b^2 = c^2$ then at least one of a, b, c is divisible by 5.

   The possible values for a square mod 5 are $0^2 = 0, 2^2 = 1, 2^2 = 4, 3^2 = 9 \equiv_5 4, 4^2 = 16 \equiv_5 1$

   To have $a^2 + b^2 = c^2$ and none of a, b, c divisible by 5, we need $a^2 \equiv_5 1$ or 4, $b^2 \equiv_5 1$ or 4. If $a^2 \equiv_5 4$ and $b^2 \equiv_5 1$ or vice versa, then $a^2+b^2 = c^2 \equiv_5 1+4 \equiv_5 0$, so c is divisible by 5, so we must have either $a^2 \equiv_5 b^2 \equiv_5 1$, in which case $a^2 + b^2 \equiv_5 2$, which cannot be congruent mod 5 to any square or $a^2 \equiv_5 b^2 \equiv_5 4$ in which case $a^2 + b^2 \equiv_5 8 \equiv_5 3$, which cannot be congruent to a square mod 5, so in no case can the sum of two squares not divisible by 5 be a square not divisible by 5.

   Why does this imply that in a primitive Pythagorean triple exactly one of a, b, c is divisible by 5?

   If two of a, b, c were divisible by 5, it is straightforward to show that the third is divisble by 5 so we do not have a primitive Pythagorean triple.

6. Explain (it is a fact about a suitable system of modular arithmetic) why any integer of the form $4k + 3$ must have a prime factor of the form $4k + 3$. Be sure that your explanation mentions facts about primes as well as facts about modular arithmetic.

   Any integer is a product of primes.

   Any integer of the form $4k + 3$ is odd, and so it is a product of odd primes.

   Suppose that an integer of the form $4k + 3$ has no prime factor of the form $4k + 3$. Then it has to be a product of primes of the form $4k + 1$. But the product of any number of factors congruent to 1 in mod 3 arithmetic is congruent to 1 (because $1 \cdot 1 = 1$ is an entry in the mod 3 multiplication table, and therefore of the form $4k + 1$, which is a contradiction.

7. Build the multiplication table of mod 7 arithmetic. Make a table of the multiplicative inverses of the nonzero residues in mod 7 arithmetic.

$*$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

It was not necessary to use the Euclidean algorithm to find the multiplicative inverses: they can be read right from the multiplication table, using the facts that (1)(1) = 1, (2)(4)=1, (3)(5) = 1, (6)(6)=1, so the inverse of 1 is 1, of 2 is 4, of 3 is 5, of 4 is 2, of 5 is 3, and of 6 is 6.

8. Compute $17^{375}\texttt{mod}100$ by the method of repeated squaring (this really means by the method of repeated squaring; other methods can be used as a check, but if you know another one you do need to do the official calculation).

   $375\ 17^{375} = (17^{187})^2 \cdot 17 \equiv_{100} 73^2 \cdot 17 = 90593 \equiv_{100} 93$

   $187\ 17^{187} = (17^{93})^2 \cdot 17 \equiv_{100} 37^2 \cdot 17 = 23273 \equiv_{100} 73$

   $93\ 17^{93} = (17^{46})^2 \cdot 17 \equiv_{100} 69^2 \cdot 17 = 80937 \equiv_{100} 37$

   $46\ 17^{46} = (17^{23})^2 \equiv_{100} 13^2 = 169 \equiv_{100} 69$

   $23\ 17^{23} = (17^1 1)^2 \cdot 17 \equiv_{100} = 33^2 \cdot 17 = 18513 \equiv_{100} 13$

   $11\ 17^{11} = (17^5)^2 \cdot 17 \equiv_{100} 57^2 \cdot 17 = 55233 \equiv_{100} 33$

   $5\ 17^5 = (17^2)^2 \cdot 17 \equiv_{100} 89^2 \cdot 17 = 134657 \equiv_{100} 57$

   $2\ 17^2 = 289 \equiv_{100} 89$

   $1\ 17^1\texttt{mod}100 = 17$

9. Do both parts. There is a connection.

   (a) Compute the multiplicative inverse of 25 in mod 137 arithmetic.

	x	y	q
137	1	0	
25	0	1	
12	1	-5	5
1	-2	11	2

   You can verify that (-2)(137)+(11)(25) = 1, so $11 \cdot 25 \equiv_{137} 1$, so **11** is the reciprocal of 25 in mod 137 arithmetic.

   (b) Find all solutions to

$$100x \equiv_{548} 16.$$

   List the residues mod 548 which are solutions.

   The gcd of 100, 548, and 16 is 4 (it has to be a power of 2, being a factor of 16, and testing reveals this easily).

   so solve $25x \equiv_{137} 4$. We showed in the previous part that 11 is the reciprocal of 25 in mod 137 arithmetic, so $x \equiv_{137} 44$.

   There are four solutions, all of the form 44+137k:: 44, 181, 315, 455.

10. Solve the system of simultaneous equations

$$x \equiv_{17} 4$$

$$x \equiv_{25} 11$$

State the smallest solution. State another solution.

$x = 11 + 25k$ by the second equation.

so we want to solve $11 + 25k \equiv_{17} 4$

equivalently

$11 + 8k \equiv_{17} 4$, for which we want the reciprocal of 8 in mod 17 arithmetic.

	x	y	q
17	1	0	
8	0	1	
1	1	-2	2

The reciprocal of 8 mod 17 is congruent to -2 mod 17 and so to 15.

$11 + 8k \equiv_{17} 4$ $8k \equiv_{17} -7 \equiv_{17} 10$ $k \equiv_{17} (10)(15) \equiv_{17} 14$ (multiplying both sides by the reciprocal)

so $x = 11 + 25 \cdot 14 = 361$

The smallest solution is 361 (you can check this): the next largest solution is 361+(17(25) = 786.