Take-Home Test 4

Due: Thursday, October 29

Solo – No Collaboration Allowed

On this test, your work is to be your own with no consultation with any other person (in this class or not) except for the instructor. Feel free to ask me any questions. I won't give you any answers to the exercises but will be happy to try to clarify any confusion you may have, probably by asking you more questions. You may feel free to use any written references or books, just not any consultation with any persons. Be sure to acknowledge any written or internet sources you use.

As usual, you will be graded both on mathematical content and on clarity of expression. Points for this test are distributed as follows: Exercises 1 and 2 are worth up to 6 points each; Exercises 3, 4, and 5 are worth a maximum of 12 points each; and your choice of Exercise 6 or 7 (you only submit a solution to one of these) is worth a maximum of 12 points. Some of the questions are a bit open-ended, so be creative, make conjectures, and back up your assertions by providing proofs or counter-examples. In writing your answers, use complete sentences (with punctuation!) and be sure to say exactly what you mean. Papers will be graded on the basis of what you have written, so be sure to take the time to express yourself clearly. If you are stuck on a problem and have no idea where to begin, a good way to get started is to look at lots of specific examples and try to find a pattern.

Exercises:

(1) Find the smallest positive integer n which satisfies all of the following congruences:

$$\begin{aligned} n &\equiv 1 \pmod 2 \\ n &\equiv 1 \pmod 3 \\ n &\equiv 3 \pmod 4 \\ n &\equiv 3 \pmod 5 \end{aligned}$$

Form a conjecture that describes all positive integers n with this property. You do not have to prove this conjecture, but back up your claim with 2 or 3 concrete examples.

(2) Use congruences to prove that $4^m + 5^m$ is divisible by 9 for every odd integer $m \geq 1$. (*Hint:* First look for patterns to determine what 4^m and 5^m are congruent to modulo 9 for odd integers $m \geq 1$.)

(3) Accompanying this test are multiplication tables for the integers modulo m, for $m = 3, 4, \ldots, 16$. In each table, the entry in row r and column c is the value of $rc \pmod m$. For example, the entry in row 6 and column 5 of the multiplication table mod 13 is 4 since $6 \cdot 5 \equiv 4 \pmod{13}$. Look at these tables and see if you can discover some patterns. When you make a conjecture, make the strongest statement you can: if you believe something is "if and only if", then say so. You do not have to prove your conjectures, but you should provide plenty of examples which support your claim.

(a) For a fixed modulus m and a given integer a, what condition guarantees that there is some integer x such that $ax \equiv 1 \pmod m$? (This is really asking for a condition when a has an inverse for multiplication.) (*Hint:* For each m, make

a list of the numbers of the rows which have a 1 in them. What do you notice about the relationship of the numbers of these rows to the modulus m?)

(b) For a fixed modulus m and a given integer a, what condition guarantees that the integers $0a, 1a, 2a, 3a, \ldots, (m-1)a$ are all different (i.e., incongruent) modulo m?

(c) For every modulus m, you will note that $1^2 \equiv 1 \pmod{m}$ and $(m-1)^2 \equiv (-1)^2 \equiv 1 \pmod{m}$. For $m = 5$, for example, these are the only two positive integers (modulo 5) with the property that $a^2 \equiv 1 \pmod{5}$, since we have $1^2 \equiv 1 \pmod{5}, 2^2 \equiv 4 \pmod{5}, 3^2 \equiv 4 \pmod{5}$ and $4^2 \equiv 1 \pmod{5}$. On the other hand, for example, when $m = 8$, we get four values a which work: 1, 3, 5, and 7. Find a set consisting of infinitely many integers m such that 1 and $m-1$ are the only two positive integers (modulo m) with the property that $a^2 \equiv 1 \pmod{m}$?

(4) This exercise deals with numbers modulo 4.

(a) Let p be an odd prime. Prove that $p \equiv 1 \pmod{4}$ or $p \equiv 3 \pmod{4}$.

(b) Let n be a positive integer such that $n \equiv 3 \pmod{4}$. Prove that n is divisible by some prime p such that $p \equiv 3 \pmod{4}$. (*Hint:* Apply the Fundamental Theorem of Arithmetic to n. Can 2 be one of the primes in the factorization of n? Once you answer this question, argue by contradiction and apply part (a).)

(c) Prove that there are infinitely many primes which are congruent to 3 modulo 4. (*Hint:* Try to mimic Euclid's proof that there are infinitely many primes (see your notes from September 22). You may want to evaluate an expression of the form $(p_1^2 p_2^2 \cdots p_k^2 + 2)\,\%4$.)

(5) Every book has assigned to it an *International Standardized Book Number*, or *ISBN* for short. This is a 10-digit number and can usually be found on the back of the book. The first 9 digits contain information about the book – typically the first digit represents the language of the country in which the book was published, the next 4 represent the publisher, and the next 4 are assigned to that particular book by the publisher. The last digit is a check digit, and it is determined by the values of the first 9 digits. The idea is that a computer can be programmed to check to see if a potential ISBN is valid. This means, for example, if a clerk is typing an ISBN into a computer and makes a mistake, usually the computer will beep, announcing an error has occurred. Here is how the check digit is determined. Let $a_1, \ldots, a_9$ be the first 9 digits of an ISBN number. Then the 10-th digit a_{10} is chosen so that

$$a_1 + 2a_2 + \cdots + 9a_9 + 10a_{10} \equiv 0 \pmod{11}.$$

A 10-digit number with digits $a_1, \ldots, a_{10}$ is called *ISBN valid* if this congruence equation holds.

(a) Sometimes you'll come across a book whose ISBN ends in "X" rather than a digit. For example, the book *Codes and Curves* by Professor Judy Walker in the Department of Mathematics here at UNL, has ISBN 0-8218-2628-X. What does the X mean?

(b) Suppose Alice and Bob were at a coffee shop one day discussing books, and Bob wrote down on a napkin the ISBN for a book he thought Alice would enjoy. Unfortunately, Alice put her coffee cup on the napkin and smudged one of the digits of Bob's ISBN. What she has left is 0-8218-51?4-1, where ? is the smudged digit. Use the equation above to determine the value of the missing digit. Then find the title and publisher of the book which Bob recommended to Alice. (*Hint*:

Most library search engines can search for a book by its ISBN. Some search engines want spaces rather than dashes; others want just the numbers with no spaces or dashes.)

Only submit a solution to one of the following two exercises. If you submit solutions to both then I will grade the first one and not necessarily the best one.

(6) Let n be a positive integer.
   (a) Show that n is divisible by 77 if and only if n is divisible by both 7 and 11. (*Hint*: Use the definition of divisibility and a previous fact concerning a prime dividing the product of two integers.)
   (b) Use the result of part (a) to determine if $2222^{5555} + 5555^{2222}$ is divisible by 77.

(7) Both parts of this exercise concern divisibility.
   (a) Find the last two digits of 2002^{2002}. Fully explain your work.
   (b) Find a divisibility test for dividing an integer by 101 in terms of the digits in its base 10 representation. Prove your test.

Statement of Sources: As this was a "Solo" exam, you shouldn't have talked with anyone besides the instructor about this exam. Please write the following statement on your exam, and sign your name:

I have neither given nor received any help on this exam.

Also, if you used any references besides the class notes, list them as well.

Multiplication Tables Modulo m

Multiplication Modulo 3

	1	2
1	1	2
2	2	1

Multiplication Modulo 4

	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

Multiplication Modulo 5

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Multiplication Modulo 6

	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

Multiplication Modulo 7

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Multiplication Modulo 8

	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	0	2	4	6
3	3	6	1	4	7	2	5
4	4	0	4	0	4	0	4
5	5	2	7	4	1	6	3
6	6	4	2	0	6	4	2
7	7	6	5	4	3	2	1

Multiplication Modulo 9

	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	4	6	8	1	3	5	7
3	3	6	0	3	6	0	3	6
4	4	8	3	7	2	6	1	5
5	5	1	6	2	7	3	8	4
6	6	3	0	6	3	0	6	3
7	7	5	3	1	8	6	4	2
8	8	7	6	5	4	3	2	1

Multiplication Modulo 10

	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9
2	2	4	6	8	0	2	4	6	8
3	3	6	9	2	5	8	1	4	7
4	4	8	2	6	0	4	8	2	6
5	5	0	5	0	5	0	5	0	5
6	6	2	8	4	0	6	2	8	4
7	7	4	1	8	5	2	9	6	3
8	8	6	4	2	0	8	6	4	2
9	9	8	7	6	5	4	3	2	1

Multiplication Modulo 11

	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	1	3	5	7	9
3	3	6	9	1	4	7	10	2	5	8
4	4	8	1	5	9	2	6	10	3	7
5	5	10	4	9	3	8	2	7	1	6
6	6	1	7	2	8	3	9	4	10	5
7	7	3	10	6	2	9	5	1	8	4
8	8	5	2	10	7	4	1	9	6	3
9	9	7	5	3	1	10	8	6	4	2
10	10	9	8	7	6	5	4	3	2	1

Multiplication Modulo 12

	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11
2	2	4	6	8	10	0	2	4	6	8	10
3	3	6	9	0	3	6	9	0	3	6	9
4	4	8	0	4	8	0	4	8	0	4	8
5	5	10	3	8	1	6	11	4	9	2	7
6	6	0	6	0	6	0	6	0	6	0	6
7	7	2	9	4	11	6	1	8	3	10	5
8	8	4	0	8	4	0	8	4	0	8	4
9	9	6	3	0	9	6	3	0	9	6	3
10	10	8	6	4	2	0	10	8	6	4	2
11	11	10	9	8	7	6	5	4	3	2	1

Multiplication Modulo 13

	1	2	3	4	5	6	7	8	9	10	11	12
1	1	2	3	4	5	6	7	8	9	10	11	12
2	2	4	6	8	10	12	1	3	5	7	9	11
3	3	6	9	12	2	5	8	11	1	4	7	10
4	4	8	12	3	7	11	2	6	10	1	5	9
5	5	10	2	7	12	4	9	1	6	11	3	8
6	6	12	5	11	4	10	3	9	2	8	1	7
7	7	1	8	2	9	3	10	4	11	5	12	6
8	8	3	11	6	1	9	4	12	7	2	10	5
9	9	5	1	10	6	2	11	7	3	12	8	4
10	10	7	4	1	11	8	5	2	12	9	6	3
11	11	9	7	5	3	1	12	10	8	6	4	2
12	12	11	10	9	8	7	6	5	4	3	2	1

Multiplication Modulo 14

	1	2	3	4	5	6	7	8	9	10	11	12	13
1	1	2	3	4	5	6	7	8	9	10	11	12	13
2	2	4	6	8	10	12	0	2	4	6	8	10	12
3	3	6	9	12	1	4	7	10	13	2	5	8	11
4	4	8	12	2	6	10	0	4	8	12	2	6	10
5	5	10	1	6	11	2	7	12	3	8	13	4	9
6	6	12	4	10	2	8	0	6	12	4	10	2	8
7	7	0	7	0	7	0	7	0	7	0	7	0	7
8	8	2	10	4	12	6	0	8	2	10	4	12	6
9	9	4	13	8	3	12	7	2	11	6	1	10	5
10	10	6	2	12	8	4	0	10	6	2	12	8	4
11	11	8	5	2	13	10	7	4	1	12	9	6	3
12	12	10	8	6	4	2	0	12	10	8	6	4	2
13	13	12	11	10	9	8	7	6	5	4	3	2	1

Multiplication Modulo 15

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14
2	2	4	6	8	10	12	14	1	3	5	7	9	11	13
3	3	6	9	12	0	3	6	9	12	0	3	6	9	12
4	4	8	12	1	5	9	13	2	6	10	14	3	7	11
5	5	10	0	5	10	0	5	10	0	5	10	0	5	10
6	6	12	3	9	0	6	12	3	9	0	6	12	3	9
7	7	14	6	13	5	12	4	11	3	10	2	9	1	8
8	8	1	9	2	10	3	11	4	12	5	13	6	14	7
9	9	3	12	6	0	9	3	12	6	0	9	3	12	6
10	10	5	0	10	5	0	10	5	0	10	5	0	10	5
11	11	7	3	14	10	6	2	13	9	5	1	12	8	4
12	12	9	6	3	0	12	9	6	3	0	12	9	6	3
13	13	11	9	7	5	3	1	14	12	10	8	6	4	2
14	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Multiplication Modulo 16

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	2	4	6	8	10	12	14	0	2	4	6	8	10	12	14
3	3	6	9	12	15	2	5	8	11	14	1	4	7	10	13
4	4	8	12	0	4	8	12	0	4	8	12	0	4	8	12
5	5	10	15	4	9	14	3	8	13	2	7	12	1	6	11
6	6	12	2	8	14	4	10	0	6	12	2	8	14	4	10
7	7	14	5	12	3	10	1	8	15	6	13	4	11	2	9
8	8	0	8	0	8	0	8	0	8	0	8	0	8	0	8
9	9	2	11	4	13	6	15	8	1	10	3	12	5	14	7
10	10	4	14	8	2	12	6	0	10	4	14	8	2	12	6
11	11	6	1	12	7	2	13	8	3	14	9	4	15	10	5
12	12	8	4	0	12	8	4	0	12	8	4	0	12	8	4
13	13	10	7	4	1	14	11	8	5	2	15	12	9	6	3
14	14	12	10	8	6	4	2	0	14	12	10	8	6	4	2
15	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1