UW Math Circle

Week 4 – Number Theory

1 Clock Math Time

1. Answer the following:

   (a) What day of the week will it be 200 days from now?

   (b) What time of day will it be 200 hours from now?

   (c) If you rotate this paper by 1000 degrees, what will it look like?

2. For each of the equations below, find integers (whole numbers) q and r that make the equation true so that r is positive and as small as possible.

   (a) $200 = 7 \cdot q + r$.

   (b) $200 = 24 \cdot q + r$.

   (c) $1000 = 360 \cdot q + r$.

3. In 31 days, the day of the week will Friday, which is 3 days after Tuesday because

$$31 = 7 \cdot 4 + 3.$$

In other words, dividing 31 by 7 has a remainder of 3. We say that "31 is congruent to $3 \bmod 7$," and we write this as

$$31 \bmod 7 = 3.$$

Find the following:

(a) $200 \bmod 7$

(b) $200 \bmod 24$

(c) $1000 \bmod 360$

4. Sean is thinking of a secret number x between 1 and 100. The other instructors whisper to you that $x \bmod 3 = 2$, $x \bmod 5 = 3$, and $x \bmod 7 = 5$. What is Sean's secret number?

Stop here. Request the next page from your instructor when your group is done.

2 Modular Arithmetic

5. Complete the following addition and multiplication tables mod 6 and mod 7. For example, $2 + 5 = 7$, which is congruent to **1** mod 6 and $2 \cdot 5 = 10$, which is congruent to **4** mod 6.

+	0	1	2	3	4	5
0						
1						
2						**1**
3						
4						
5						

×	0	1	2	3	4	5
0						
1						
2						**4**
3						
4						
5						

Above are the addition and multiplication tables mod 6

+	0	1	2	3	4	5	6
0							
1							
2							
3							
4							
5							
6							

×	0	1	2	3	4	5	6
0							
1							
2							
3							
4							
5							
6							

Above are the addition and multiplication tables mod 7

6. What patterns do you see in these tables? Pick one pattern you notice and justify why it holds.

7. For any number a from 0 to 5 (mod 6) inclusive, can you find:

   - a number between 0 and 5 that when added to a gives $0 \bmod 6$?
   - a number between 0 and 5 that when multiplied by a gives $1 \bmod 6$?

8. Repeat the above question for the mod 7 table. Does this differ from the mod 6 case? Why might that be?

9. Suppose we wanted to find the sum of two numbers (say, 17 and 57) mod 7. We can do this in two ways:

   - Find what both numbers are congruent to mod 7, and then take their sum mod 7.
   - Take the sum normally, and then take the result mod 7.

   Do these give the same answer? (Challenge: if you think these two processes always give the same answer, prove it!)

10. Repeat the above with finding the product of two numbers (say, 17 and 57) mod 7. Do these processes give the same answer? (Challenge: if you think these two processes always give the same answer, prove it!)

Stop here. Request the next page from your instructor when your group is done.

3 Divisibility Tricks

11. (a) Come up with a quick way to check if a number is divisible by 2.

    (b) Come up with a quick way to check if a number is divisible by 5.

12. One way to check if a number is divisible by 3 is to add up the digits of the number and see if their sum is divisible by 3. For example, 86 is not divisible by 3, since the digits of its sum is $8 + 6 = 14$ which is not divisible by 3. Let's see why this works!

    (a) For any digit a, how does $10 \cdot a \bmod 3$ relate to $a \bmod 3$? (Hint: what is $10 \bmod 3$? $20 \bmod 3$? $30 \bmod 3$?)

    (b) What about $100 \cdot a \bmod 3$? $1000 \cdot a \bmod 3$? $10^k \cdot a \bmod 3$?

    (c) When we write down a number like 6174 in our number system, we really mean to say the quantity $6 \cdot 10^3 + 1 \cdot 10^2 + 7 \cdot 10 + 4$. Using this idea, prove that any number is congruent to the sum of its digits mod 3.

13. The same trick for divisibility by 3 works to test divisibility by 9 as well! For example, 36 is divisible by 9 since the sum of its digits is $3 + 6 = 9$, which is divisible by 9. Follow a similar process as above to prove that this test works for divisibility by 9.

14. A similar trick works for divisibility by 11, but now we have to alternate adding and subtracting digits, starting from the right. For example, the number 1342 is divisible by 11, since $2 - 4 + 3 - 1 = 0$, which is divisible by 11. Show that if this alternating sum of digits of a number is divisible by 11, that number is divisible by 11.

15. (Challenge) Come up with your own digit-based rules for divisibility by 7 and 13.

Stop here. Request the next page from your instructor when your group is done.

4 Digit Games

16. Try the following process to generate a "magic number" from any three-digit number A:

Instructions	Example: $A = 278$
Let B be the three-digit number obtained by reversing the order of digits of A.	$B = 872$
Find the (positive) difference between A and B: $D = \lvert A - B \rvert$.	$D = 872 - 278 = 594$
Reverse the digits of D to get a new number E.	$E = 495$
Add D and E together to obtain a magic number $M = D + E$.	$M =$???

What are the possible magic numbers M that you can get with this process and why?

17. Now try *repeating* the following process for any three-digit number N:

Instructions	Example: $N = 512$
Sort the digits of N in increasing order to get a new three-digit number I.	$I = 125$
Sort the digits of N in decreasing order to get a new three-digit number D.	$D = 521$
Let $N = D - I$. Return to the first step.	$N = 396$ …

After doing this enough times starting from any number N you like, there are only a few possible values of N you can end up at. What are they and why?

18. Try the process in the previous problem for four-digit numbers N now. As an example:

Instructions	Example: $N = 2351$
Sort the digits of N in increasing order to get a new three-digit number I.	$I = 1235$
Sort the digits of N in decreasing order to get a new three-digit number D.	$D = 5321$
Let $N = D - I$. Return to the first step.	$N = 4086$ …

What possible values of N can you end up at? Why are these the only possibilities?

19. (Challenge) Try the same process as above with numbers of any length. What possible numbers can you end up at other than the three and four-digit numbers you found above? Can you show that these are all of the possibilities?

Stop here. Request the next page from your instructor when your group is done.

5 Sums of Squares

20. Notice we can write many numbers as the sum of square numbers. As some examples: $5 = 2^2 + 1^2$, $6 = 2^2 + 1^2 + 1^2$, and $14 = 3^2 + 2^2 + 1^2$. Write the following numbers as the sum of square numbers. For each, try to use the fewest amount of square numbers possible.

$$15 =$$
$$30 =$$
$$39 =$$

Then, choose any number and try to write it as the sum of the fewest amount of square numbers possible.

It turns out that *any* positive integer can be written as the sum of four or fewer squares, which is called the *Four Squares Theorem*. This is a difficult theorem to prove, but we will walk through one pieve of the argument in this section.

21. For every number $0 \leq x < 7$, list $x^2 \bmod 7$. How many distinct results are in your list?

22. Make two lists: $-x^2 \bmod 7$ for every $0 \leq x < 7$ and $y^2 + 1 \bmod 7$ for every $0 \leq y < 7$. Next, find two numbers x and y so that $y^2 + 1 \bmod 7$ is equivalent to $-x^2 \bmod 7$.

23. How many distinct results are in each of your two lists from the previous problem? If you only knew the number of distinct results in each list and not this lists themselves, explain how you could still conclude there must exist some such pair x and y (even if you might not know what the pair is).

24. If p is any odd prime number (try this for 3, 5, 7, 11, ...), then how many distinct results would be in the list $x^2 \bmod p$ for every number $0 \leq x < p$? Why?

    Hint: if two integers $0 \leq a, b < p$ give the same result, this means $a^2 - b^2 \bmod p = 0$ and therefore $(a-b)(a+b) \bmod p = 0$, so what can you say about a and b?

25. Suppose p is any odd prime number, and you make two lists: $-x^2 \bmod p$ for every $0 \leq x < p$ and $y^2 + 1 \bmod p$ for every $0 \leq y < p$. How many distinct results are in list? Explain how you can use the number of distinct results in each list to conclude there must be some pair x and y so that $y^2 + 1 \bmod p$ is equivalent to $-x^2 \bmod p$.

26. Explain how, for any odd prime p, you can alter the above argument to find a pair $0 \leq x, y \leq (p-1)/2$ so that $y^2 + 1 \bmod p$ is equivalent to $-x^2 \bmod p$.

Note: Question 26 is a first step towards proving the Four Squares Theorem. In fact, this immediately gives us a weaker result regarding the sums of squares. Rewriting the result gives that for any odd prime p, there is a pair x, y so that $x^2 + y^2 + 1 = 0 \bmod p$. Therefore, there is some m so that we can write mp as the sum of three squares: $x^2 + y^2 + 1^2 = mp$.

Stop here. Request the next page from your instructor when your group is done.