Divisibility, Congruences, and More
Class Activity, Week 1

As one could guess from the name, number theory is the study of integers and their relationships with each others. We can look for integer solutions to certain equations (linear Diophantine equations) or we can see when two numbers do not share a common positive factor besides 1 (relatively prime numbers). In this activity, we will continue reviewing the two foundational ideas: divisibility and congruences, and work to make certain results more rigorous.

Divisibility and Primes

Recall: A non-zero integer a *divides* an integer b if $b = ak$ for some integer k and we denote this by $a|b$.

1. If $a|b$ and $b|c$, explain why $a|c$ using the definition and proper notation.

$b = aj \quad j \in \mathbb{Z}$

$c = bk \quad k \in \mathbb{Z}$

$c = ajk \quad jk \in \mathbb{Z}$ so $a|c$

2. If a divides b and c, explain why a divides $b + c$.

$b = aj \quad j \in \mathbb{Z}$

$c = ak \quad k \in \mathbb{Z}$

$b + c = aj + ak = a(j+k) \quad j+k \in \mathbb{Z}$ so $a|b+c$

3. Can you determine whether 456123 prime or not without using a calculator?

$3 | 456123$ because $3|(4+5+6+1+2+3) \rightarrow 3|21$

So not Prime

$456123 = 10^5 \cdot 4 + 10^4 \cdot 5 + \ldots = (9+1)^5 \cdot 4 + (9+1)^4 \cdot 5 + \ldots = 9k + 4 + 9j + 5 + \ldots$

$= 3m + 4 + 5 + 6 + 1 + 2 + 3$

4. Find the value of $n^3 - n$ for $n = 1, 2, 3, 4$ (and $n = 5, 6$ if you like). What divisibility property seems to be common to all these numbers? Can you justify your conjecture?

$n^3 - n = n(n+1)(n-1)$

$\boxed{6 | n^3 - n \text{ if } n \in \mathbb{Z}}$

n	$n^3 - n$
1	0
2	6
3	24
4	60
5	120
6	210

in any 3 consecutive integers, one will be a multiple of 3 and at least one will be a multiple of 2 so their product will be a multiple of $3 \cdot 2 = 6$

Over →

5. Look at your Fibonacci number sequence from your pre-class work. Do you notice a divisibility property common to the numbers f_{3n}? What about f_{4n}? What about f_{5n}? (You might want to go up to f_{20} if you don't see a pattern.)

f_{3n} are all even ($f_3 = 2$)
f_{4n} are all divisible by 3 ($f_4 = 3$)
f_{5n} are all divisible by 5 ($f_5 = 5$)

6. (If time) Justify the divisibility property you observed about f_{3n} using induction.

$f_3 = 2$ 2 is even

if f_{3n} is even then $f_{3(n+1)}$ is even

$$f_{3n+3} = f_{3n+1} + f_{3n+2}$$
$$= f_{3n+1} + f_{3n} + f_{3n+1}$$
$$= f_{3n} + 2f_{3n+1} \longrightarrow \text{even}$$

$f_4 = 3$ $3 | 3$

if $3 | f_{4n} \to 3 | f_{4(n+1)}$

$$f_{4n+4} = f_{4n+2} + f_{4n+3}$$
$$= f_{4n} + f_{4n+1} + f_{4n+1} + f_{4n+2}$$
$$= f_{4n} + 2f_{4n+1} + f_{4n} + f_{4n+1}$$
$$= 2f_{4n} + 3f_{4n+1}$$
$$3 | 2f_{4n} + 3f_{4n+1}$$

Congruences

Given a number n, we can partition all the integers into groups where the integers in the same group are congruent to each other. These groups are officially called the *residue classes* modulo n. There are n such classes and a natural choice of representatives for these classes are $0, 1, 2, \ldots, n-1$.

By working with congruences, we effectively reduce the set of all integers to a finite number of integers. This process has useful applications in cryptography (a future project topic) and in other areas in computer science, and also in other mathematical areas.

3, 9, 7, 1, 3, 9, 7

7. Determine the ones' digit of $3, 3^2, 3^3, 3^4, 3^5, 3^6, 3^7, \ldots$ until you notice a pattern. Use this pattern and properties of modular arithmetic modulo 10 to determine the ones' digit of 3^{2019}.

$$3^n \% 10 = 3^{n \% 4} \% 10$$

$$3^{2019} \% 10 = 3^{2019 \% 4} \% 10 = 3^3 \% 10 = 7$$

8. (If time) Pick a few different integers (carefully choose some good integers), square them and find which residue classes the squares belong to modulo 6. What possibilities are there? Does each residue class have a square in it?

only 0, 1, 3, 4

No

$$0^2 \% 6 = 0$$
$$1^2 \% 6 = 1$$
$$2^2 \% 6 = 4$$
$$3^2 \% 6 = 3$$
$$4^2 \% 6 = 4$$
$$5^2 \% 6 = 1$$

$(6k+n)^2 \% 6$
$= 36k^2 + 12kn + n^2 \% 6$
$= n^2 \% 6$ so 0–5 covers all integers