Lectures 18 and 19 - Number Theory I

We discussed operations in $\mathbb{Z}$, in particular division with remainder.

We say $a \mid b$, that is, a divides b, if the remainder when dividing b by a is 0, $b = k \cdot a$, $k \in \mathbb{Z}$.

We defined for $p > 1$, $p \in \mathbb{N}$ two definitions:

p is *irreducible*: for all $k \in \mathbb{N}$; $(k \mid p) \Rightarrow [(k = p) \vee (k = 1)]$

p is *prime*: for all $a, b \in \mathbb{N}$; $(p \mid ab) \Rightarrow [(p \mid a) \vee (p \mid b)]$

[Non-number theorists usually take the first one as the definition of prime. We will show later that that

$$(p \text{ is prime}) \iff (p \text{ is irreducible})$$

so for $\mathbb{Z}$ the distinction is mostly jargon.]

We introduced the Sieve of Eratosthenes: *If $p_1, \ldots p_n$ are the only primes in the set $\{1, 2, 3, \ldots, m\}$, then removing their multiples from $\{1, 2, 3, \ldots, m^2\}$ leaves only primes.*

We also defined $\gcd(a, b)$, the greatest common divisor of a and b and showed the Euclidean Algorithm to to computer $\gcd(a, b)$.

We also showed how to use the Euclidean Algorithm to compute λ and μ so that

$$\gcd(a, b) = \lambda \cdot a + \mu \cdot b$$

We also compared the work required to compute $\gcd(a, b)$ with by factoring a and b into primes and comparing them, versus using the Euclidean Algorithm.

Exercises for Lectures 18 and 19

In the following exercises, try not to use a calculator.

1. Google says that 2017 is prime. To check this by dividing by primes 2, 3, 5, 7, ..., p. What is the largest prime p that must be checked.

2. We know from class that 2, 3, 5, 7, 11, 13, 17, 19 all the primes below 20.

   Use the sieve to find all primes below 400. Note that for you need only sieve out the multiples of 13 beyond 169 - why?

3. Find a pair of numbers between 1776 and 2017 whose gcd is 111.

4. Let $n \geq 5$. What can you say about $k = \gcd(n + 2, n - 2)$. How many different values can k have? Give an example of each type.

5. Let $n \geq 1$. What can you say about $k = \gcd(n + 100, n)$? How many different values can k have? Give an example of each type.

6. 1215 is obviously not prime. Find the prime factorization of 1215. [Happy Magna Carta Day!]

7. 1776 is obviously not prime. Find the prime factorization of 1776. [Up the rebels!]

8. Find the prime factorization of 2018.

9. Find the the gcd of 1776 and 2018.

10. Find the the gcd of 1776 and 2018 using the Euclidean Algorithm.

11. Find λ and μ so that $\gcd(1776, 2018) = \lambda \cdot 1776 + \mu \cdot 2018$.

12. Find λ and μ so that $1 = \lambda \cdot 111 + \mu \cdot 1111$ or show that that is impossible.

13. Find λ and μ so that $1 = \lambda \cdot 1111 + \mu \cdot 111111$ or show that that is impossible.

14. Find λ and μ so that $1 = \lambda \cdot 21 + \mu \cdot 121$ or show that that is impossible.

15. Find λ and μ so that $1 = \lambda \cdot 169 + \mu \cdot 144$ or show that that is impossible.

16. We wrote the Sieve of Eratosthenes in class on a 10 × 10 grid with ten numbers in each row, say from 30 to 39 and we noticed that there was at least one survivor in each row. We only sieved out the primes less than 10, so just 2, 3, 5, and 7. Suppose we kept sieving out the multiples of these four primes, letting the array grow, always 10 numbers in the row. In the 10' row we have four survivors:

    $$\cancel{1}00, 101, \cancel{1}02, 103, \cancel{1}04, \cancel{1}05, \cancel{1}06, 107, \cancel{1}08, 109$$

    In the 11' row we have one survivor:

    $$\cancel{1}10, \cancel{1}11, \cancel{1}12, 113, \cancel{1}14, \cancel{1}15, \cancel{1}16, \cancel{1}17, \cancel{1}18, \cancel{1}19$$

    In the 12' row we have two survivors:

    $$\cancel{1}20, 121, \cancel{1}22, \cancel{1}23, \cancel{1}24, \cancel{1}25, \cancel{1}26, 127, \cancel{1}28, \cancel{1}29$$

    but they are not both primes. Why?

    How long would it be before you would have a whole row of 10 with no survivors.