Math Circle
Beginners Group
March 6, 2016
Euclid and Prime Numbers II

Warm-up problem

You have two hourglasses: a 7-minute one and an 11-minute one. Using just these hourglasses and nothing else, how can you accurately time 15 minutes?

Review

1. Find the prime factorization of the following numbers:

   (a) 5040

   (b) 111111

2. State Euclid's lemma, and give an example where the lemma applies.

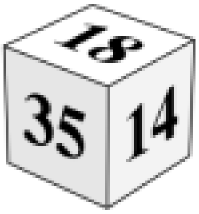
3. Describe all positive integers that have

   (a) exactly three positive divisors

   (b) exactly four positive divisors?

4. What is the largest prime number, P, such that 9 times P is less than 400?

5. In the picture, there is a special die. Numbers on the opposite faces always make the same sum. The numbers that we cannot see in the picture are all prime numbers. Which number lies opposite to 14?



Infinitely Many Primes

Euclid was one of the first people to prove the existence of infinitely many primes. Let us look at a simple way to think about the existence of infinitely many primes.

Here are all the prime numbers less than 100:
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97

1. Compute the gaps between consecutive prime numbers given above.

2. Do you notice any pattern in the gaps you computed above? (Hint: What happens to the size of the gaps as the prime numbers get bigger?)

3. As you move to larger numbers, do you think you can keep finding prime numbers?

Now, we will follow Euclid's proof to show the that there are infinitely many prime numbers.

We will argue by **contradiction**. Assume that there is a finite number of primes. Then we can list all the primes:

$$p_1,\ p_2,\ p_3, \ldots,\ p_n$$

This means that p_n is the largest prime number. Therefore, all natural numbers larger than p_n are composite numbers.

1. Write down an expression for a number, A, such that A is divisible by all prime numbers: $p_1,\ p_2,\ p_3, ..., p_n$.

$$A =$$

2. Write down an expression for $B = A + 1$ in terms of $p_1,\ p_2, \ldots, p_n$.

   $$B =$$

3. Is B divisible by any of the prime numbers $p_1,\ p_2,\ p_3, ..., p_n$? (Hint: What is the remainder when you divide B by each of the given prime numbers?)

4. Can we conclude that B is prime? Why or why not?

5. Why does this mean that we got a contradiction with our assumption?

6. What is your conclusion?

Recall that

$$101! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot ... \cdot 99 \cdot 100 \cdot 101.$$

Consider the sequence $101! + 2,\ 101! + 3,\ ...,\ 101! + 100,\ 101! + 101.$

1. Is $101! + 2$ a prime or a composite number?

2. Is $101! + 3$ a prime or a composite number?

3. Show that all of the numbers in the sequence are composite.

   For example, what is $(101! + 5)$ divisible by?

   What is $(101! + 53)$ divisible by?

4. How many numbers are there in the sequence above?

   As a result, we have a list of ____ consecutive composite numbers.
   Do you think you can construct a similar list of 543 consecutive composite numbers?

Prime Number Theory

Let us look at the distribution of prime numbers and notice some interesting phenomena.

Here is the list of prime numbers under 100.
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97

1. Compare these prime numbers less than 100 with multiples of 4, i.e., 4, 8, 12, 16, 20 and so on. What do you notice? Explain in your own words. Start by writing several more multiples of 4 below 100, and explain in your own words.

   (a) Complete the following table:

n	$4n-1$	$4n+1$
1		
2		
3		
4		
5		
6		
7		
8		
9		

   (b) Circle the prime numbers under the columns "$4n+1$" and "$4n-1$" in the table above.

   (c) Can all prime numbers be written as $4n+1$ or $4n-1$, for any natural number n?

   (d) Are $4n+1$ and $4n-1$ always prime?

   (e) What is special about the prime numbers of the form $4n+1$? (Hint: Think about Pythagorean triplets.)

(f) Prime numbers of the form $4n + 1$ are called Pythagorean primes. Express the following Pythagorean primes as the sum of two squares.

i. $17 =$

ii. $29 =$

iii. $61 =$

2. Do you think there are numbers of the form $5n + 1$ or $5n - 1$ that are prime?

(a) What must n be for $5n + 1$ or $5n - 1$ to be a prime number, and why?

(b) For such an n, are $5n + 1$ and $5n - 1$ always prime numbers? If yes, explain why. If no, give an example.

3. Compare these prime numbers less than 100 with multiples of 6, i.e., 6, 12, 18, 24, 30 and so on. What do you notice? Explain in your own words.

   (a) Complete the following table:

n	$6n-1$	$6n+1$
1		
2		
3		
4		
5		
6		
7		
8		
9		

   (b) Circle the prime numbers under the columns "$6n+1$" and "$6n-1$" in the table above.

   (c) Can all prime numbers be written as $6n+1$ or $6n-1$, for any natural number n?

   (d) Are $6n+1$ and $6n-1$ always prime?

4. **Twin primes** are pairs of prime numbers that differ by 2.

   (a) Find all the *twin primes* among prime numbers less than 100. Here are all the prime numbers less than 100:
   2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97

   (b) A prime number is called an *isolated prime* if it is not a part of a twin pair, i.e., p is an isolated prime if $p+2$ and $p-2$ are not prime numbers. Find all the isolated primes among prime numbers less than 100.

(c) Euclid was one of the first to conjecture that there are an infinite number of twin primes. However, to this day, there is no proof to this conjecture. Do you think there are infinitely many twin primes?

Euclid's Algorithm and the Greatest Common Divisor

Euclid's Algorithm is used to find the greatest common divisor of two numbers.

Let the two numbers be a and b. Here are the steps to the algorithm:

Step 1: Write an expression with a and b such that $a = bq + r$.

Step 2: Replace a by b above and b by r above, and repeat the steps until the remainder is 0.

For example, let $a = 455$ and $b = 42$.

$$\begin{tikzcd}
455 = & 42 \arrow[dl, bend right] & \times 10 + & 35 \arrow[dll, bend left] \\
42 = & 35 \arrow[dl, bend right] & \times 1 + & 7 \arrow[dll, bend left] \\
35 = & 7 & \times 5 + 0 &
\end{tikzcd}$$

Now, we can claim that the *gcd* of 455 and 42 is 7. We will prove this claim later.

1. Using Euclid's Algorithm, find

   (a) $gcd(225, 135)$

(b) $gcd(12576, 4052)$

(c) $gcd(867, 255)$

(d) $gcd(367, 256)$

Let us now try to prove why the final non-zero remainder is the greatest common divisor of a and b. This proof depends on the following lemma:

$$\text{If } a = bq + r, \text{ then } gcd(a, b) = gcd(b, r).$$

1. We will first show that if $a = bq + r$, then the common divisors of a and b are the same as the common divisors of b and r.

   (a) Let d be a common divisor of a and b.

      i. Therefore, $d \mid$ ____ and $d \mid$ ____.

      ii. If d is a common divisor of a and b, does d divide $a - bq$? Why or why not?

iii. Therefore, $d \mid$ ________.

iv. But we know that $a - bq =$ ____. (Hint: Look at the lemma above.)

v. Therefore, $d \mid$ ____.

vi. This shows that d is a ____________________________ of b and r.

vii. Therefore, every common divisor of a and b is also a common divisor of b and r, and vice-versa. This means that the set of common divisors of a and b is the same as the set of common divisors for b and r.

viii. Why does this mean $gcd(a, b) = gcd(b, r)$?

(b) We will now see with an example how that Euclid's Algorithm gives us the greatest common divisor of a and b. Let $a = 2322$ and $b = 654$.

i. According to Euclid's Algorithm,

$$2322 = 654 \times 3 + 360.$$

What do we know from the lemma we proved above?

$$gcd(\underline{\hspace{1cm}}, \underline{\hspace{1cm}}) = gcd(\underline{\hspace{1cm}}, \underline{\hspace{1cm}})$$

ii. The next step to the algorithm is

$$654 = 360 \times 1 + 294.$$

What do we know from the lemma we proved above?

iii. Complete the algorithm and write down what the lemma tells us at every step.

iv. What is $gcd(30, 6)$ from your work above?

v. What is $gcd(2322, 654)$?

vi. Are they equal? Why or why not?