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?

Let's start the 7-minute and the 11-minute hourglass at the same time.

When the 7-minute timer ends, flip it. We have now measured 7 minutes.

Just when the 11-minute timer ends, 4 minutes would have passed on the 7-minute hourglass. We have now measured 11 minutes.

Flip the 7-minute timer again. Because we flipped the 7-minute hourglass when 4 minutes had passed on it, we can measure 4 minutes after flipping it.

After the 7-minute hourglass runs out this time, we would have measured 4 minutes since flipping it, and 15 minutes in total.

Review

1. Find the prime factorization of the following numbers:

   (a) 5040
   $5040 = 2^4 \times 3^2 \times 5 \times 7$

   (b) 111111
   $111111 = 3 \times 7 \times 11 \times 13 \times 37$

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

   According to Euclid's lemma,

   $$\textit{if } p \mid a \cdot b, \textit{ then } p \mid a \textit{ or } p \mid b.$$

   For example, let $p = 3$, $a = 2$ *and* $b = 12$.

   Therefore, $3 \mid 24$ *and* $3 \mid 12$.

3. Describe all positive integers that have

   (a) exactly three positive divisors

   Only perfect squares of prime numbers have exactly three positive divisors.

   For example, for a prime number p, $N = p^2$ *has three divisors:* 1, p, *and* N *itself.*

   (b) exactly four positive divisors?

   Perfect cubes of prime numbers as well as a product of two distinct prime numbers have exactly four positive divisors.

   For example, for a prime number p, $N = p^3$ *has four divisors:* 1, p, p^2, *and* N *itself.*

   Secondly, for prime numbers p_1 *and* p_2, $M = p_1 \cdot p_2$ *has four divisors:* 1, p_1, p_2, *and* N *itself.*

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

   We know that $9P < 400$.

   Therefore, $P < 44.44$. *The largest prime number smaller than* 44.44 *is* 43.

   Thus, $P = 43$.

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?

   Say, the number that lies opposite 14 *is* x.

   Since the numbers on opposite faces make the same sum, $14+x$ *must be greater than* 35. *In fact,* $14+x$ *must be greater than* 37, *because the smallest prime number that can be opposite* 35 *is* 2.

   So, $37 - 14 = 23$, *and since* 23 *is prime, it lies opposite* 14.

   To check, $37 - 18 = 29$, *which is also prime.*

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.

   The gaps between consecutive prime numbers are:

   1, 2, 2, 4, 2, 4, 2, 4, 6, 2, 6, 4, 2, 4, 6, 6, 2, 6, 4, 2, 6, 4, 6, 9

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?)

   As the prime numbers get larger, the gaps between consecutive prime numbers become larger as well.

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

   As we move to larger numbers, we should be able to keep finding prime numbers. This is because even though the gaps between consecutive primes become larger, the gaps are still finite.

   This means that there may be infinitely many 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: $p_1,\ p_2,\ p_3, ..., p_n$.

   $$A = p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot ... \cdot p_n$$

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

   $$B = p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot ... \cdot p_n + 1$$

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?)

   B is not divisible by any of the given prime numbers. If you divide B by p_1, the quotient is $p_2 \cdot p_3 \cdot p_4 \cdot ... \cdot p_n + \frac{1}{p_1}$. The quotient is not a natural number, and the remainder is not 0. Similarly with the other given prime numbers.

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

   Since B is not divisible by any of the given prime numbers, it is also a prime number.

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

   Since B is also a prime number and is larger than p_n, our assumption of a given set of prime numbers $\{p_1,\ p_2,\ p_3, ..., p_n\}$ is incorrect.

6. What is your conclusion?

   This must mean that the set of prime numbers is not finite and that there are infinitely many primes.

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?

   $101! + 2$ *is a composite number since it is divisible by* 2*.*

   $\frac{101!+2}{2} = (1 \times 3 \times 4 \times 5 \times ... \times 100 \times 101 + 1)$

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

   $101! + 3$ *is also a composite number since it is divisible by* 3*.*

   $\frac{101!+3}{3} = (1 \times 2 \times 4 \times 5 \times ... \times 100 \times 101 + 1)$

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

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

   Similarly, all numbers in this sequence are composite.

   For example, $101! + 5$ *is also a composite number since it is divisible by* 5*.*

   $\frac{101!+5}{5} = (1 \times 2 \times 3 \times 4 \times 6 \times ... \times 100 \times 101 + 1)$

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

   $101! + 53$ *is also a composite number since it is divisible by* 53*.*

   $\frac{101!+53}{53} = (1 \times 2 \times 3 \times 4 \times 5 \times ...51 \times 52 \times 54 \times 55 \times ... \times 100 \times 101 + 1)$

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

   There are 100 *numbers in the sequence above.*

   As a result, we have a list of <u>100</u> consecutive composite numbers.
   Do you think you can construct a similar list of 543 consecutive composite numbers?

   Of course! Here it is:

   $544! + 2,\ 544! + 3,\ 544! + 4, ...,\ 544! + 543,\ 544! + 544.$

   There are 543 *numbers in this list all of which are composite for the same reasons as those given above.*

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.

   All prime numbers, except 2, *differ from the multiples of* 4 *by* 1.

   For example, $3 = 4 \times 1 - 1$, $5 = 4 \times 1 + 1$, $53 = 4 \times 13 + 1$, $83 = 4 \times 21 - 1$.

   (a) Complete the following table:

n	$4n-1$	$4n+1$
1	*3*	*5*
2	*7*	*9*
3	*11*	*13*
4	*15*	*17*
5	*19*	*21*
6	*23*	*25*
7	*27*	*29*
8	*31*	*33*
9	*35*	*37*

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

   (The numbers in red are primes.)

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

   Yes, all prime numbers, except 2, *can be written as* $4n+1$ *or* $4n-1$.

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

   No, $4n+1$ *and* $4n-1$ *are not always prime numbers.*
   For example, $4 \times 7 - 1 = 27$ *or* $4 \times 5 + 1 = 21$.

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

   Prime numbers of the form $4n+1$ *can always be written as sums of two squares.*
   For example, $5 = 2^2 + 1^2$, $13 = 3^2 + 2^2$, $37 = 6^2 + 1^2$.

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

i. $17 = 4^2 + 1^2$

ii. $29 = 5^2 + 2^2$

iii. $61 = 5^2 + 6^2$

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

Some prime numbers of the form $5n + 1$ *or* $5n - 1$ *are prime numbers.*

For example, $5 \times 2 + 1 = 11$ *and* $5 \times 4 - 1 = 19$.

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

n *must be even for* $5n+1$ *or* $5n-1$ *to be prime. This is because for odd* n, $5n+1$ *and* $5n-1$ *must be even, and all even numbers, except* 2, *are always composite.*

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

For an even n, $5n + 1$ *and* $5n - 1$ *are not always prime.*

For example, $5 \times 4 + 1 = 21$ *and* $5 \times 2 - 1 = 9$, *which are both composite.*

This is a converse to what we found in part a, and this shows that converses are not always true if the statements are true.

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.

   All prime numbers, except 2 and 3, differ from the multiples of 6 by 1.

   For example, $5 = 5 \times 1 - 1$, $7 = 6 \times 1 + 1$, $53 = 6 \times 9 - 1$, $83 = 6 \times 14 - 1$.

   (a) Complete the following table:

n	$6n-1$	$6n+1$
1	*5*	*7*
2	*11*	*13*
3	*17*	*19*
4	*23*	*25*
5	*29*	*31*
6	*35*	*37*
7	*41*	*43*
8	*47*	*49*
9	*53*	*55*

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

   (The numbers in red are primes.)

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

   All prime numbers, except 2 and 3, can be written as $6n+1$ *or* $6n-1$.

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

   No, $6n+1$ *and* $6n-1$ *are not always prime numbers.*

   For example, $6 \times 6 - 1 = 35$ *or* $6 \times 8 + 1 = 49$.

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

   The twin prime pairs less than 100 *are:*

   $(3,5)$, $(5,7)$, $(11,13)$, $(17,19)$, $(29,31)$, $(41,43)$, $(59,61)$, $(71,73)$

(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.

The isolated primes less than 100 *are:*

2, 23, 37, 47, 53, 67, 79, 83, 89, 97

(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?

Answers can vary.

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 $b = 42$.

$$455 = 42 \times 10 + 35$$
$$42 = 35 \times 1 + 7$$
$$35 = 7 \times 5 + 0$$

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) $gcd(225, 135)$

$$225 = 135 \times 1 + 90$$

$$135 = 90 \times 1 + 45$$

$$90 = 45 \times 2 + 0$$

$$gcd(225, 135) = 45$$

(b) $gcd(12576, 4052)$

$$12576 = 4052 \times 3 + 420$$

$$4052 = 420 \times 9 + 272$$

$$420 = 272 \times 1 + 148$$

$$272 = 148 \times 1 + 124$$

$$148 = 124 \times 1 + 24$$

$$124 = 24 \times 5 + 4$$

$$24 = 4 \times 6 + 0$$

$$gcd(12576, 4052) = 4$$

(c) $gcd(867, 255)$

$$867 = 255 \times 3 + 102$$

$$255 = 102 \times 2 + 51$$

$$102 = 51 \times 2 + 0$$

$$gcd(867, 255) = 51$$

(d) $gcd(367, 256)$

$$367 = 256 \times 1 + 111$$

$$256 = 111 \times 2 + 34$$

$$111 = 34 \times 3 + 9$$

$$34 = 9 \times 3 + 7$$

$$9 = 7 \times 1 + 2$$

$$7 = 2 \times 3 + 1$$

$$2 = 1 \times 1 + 0$$

$$gcd(367, 256) = 1$$

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, $d \mid \underline{a}$ and $d \mid \underline{b}$.

      ii. If d is a common divisor of a and b, does d divide $a - bq$? Why or why not?
      Since a is divisible by d, and bq is also divisible by d, $a-bq$ must be divisible by d.

      iii. Therefore, $d \mid \underline{a - bq}$.

      iv. But we know that $a - bq = \underline{r}$. (Hint: Look at the lemma above.)

      v. Therefore, $d \mid \underline{r}$.

      vi. This shows that d is a *common divisor* 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 of b and r.

      viii. Why does this mean $gcd(a, b) = gcd(b, r)$?
      If the set of common divisors of a and b is the same as the set of common divisors of b and r, the largest common divisor in the sets must also be the same.

   (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?

      $$gcd(\underline{2322}, \underline{654}) = gcd(\underline{654}, \underline{360})$$

ii. The next step to the algorithm is

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

What do we know from the lemma we proved above?

$$gcd(\underline{654}, \underline{360}) = gcd(\underline{360}, \underline{294})$$

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

$$\begin{aligned} 360 &= 294 \times 1 + 66 && \Rightarrow && gcd(360, 294) = gcd(294, 66) \\ 294 &= 66 \times 4 + 30 && \Rightarrow && gcd(294, 66) = gcd(66, 30) \\ 66 &= 30 \times 2 + 6 && \Rightarrow && gcd(66, 30) = gcd(30, 6) \\ 30 &= 6 \times 5 + 0 && \Rightarrow && gcd(30, 6) = 6 \end{aligned}$$

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

v. What is $gcd(2322, 654)$?
$gcd(2322, 654) = 6$

vi. Are they equal? Why or why not?
Look at parts i, ii, and iii. Because of the lemma that we proved above, the greatest common divisors are equal at every step of Euclid's Algorithm.