A **prime** number is a whole number greater than 1, whose only two whole-number factors are 1 and itself. The first few prime numbers are: 2, 3, 5, 7, 11... Any numbers that aren't primes are called **composite** numbers.

1 Review

Find the prime factorization of the following numbers:

1. 540

   540 $= 2^2 \times 3^3 \times 5$

2. 5040

   5040 $= 2^4 \times 3^2 \times 5 \times 7$

2 Infinitely Many Primes

Euclid was one of the first people to prove the existence of infinitely many primes. Let's take a look to see if we can too!

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: Look at the size of the gaps.)

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

3. As we go to bigger numbers, do you think we can keep finding more 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.

3 Proof By Contradiction

We will now follow Euclid's proof to show that there are infinitely many prime numbers.

We will argue by **contradiction**. If we assume that the opposite proposition is true, then that shows that such an assumption leads to a contradiction. To begin, let's *assume* that there is a finite number of primes. Then we can list all the primes as:

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

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

1. Write down an expression for a number, A, such that A is divisible by all prime numbers.

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

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

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

3. Is B divisible by any of the prime numbers $p_1, p_2, p_3, ..., p_n$? (Hint: Find 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.

Wow! Together, we just showed that there indeed are infinitely many prime numbers through proof by contradiction. That's a pretty big feat! Give yourself a pat on your back!

4 Twin Primes

Twin primes are pairs of prime numbers that differ by 2. Let's see if we can do more...

1. Find all the *twin primes* among prime numbers less than 100.

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

2. A prime number is called an *isolated prime* if it isn't part of a twin pair. 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

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

   Answers can vary.

5 A Prime Age for Prime Numbers

Prime numbers are very unique numbers. Being so unique, it might seem that this would leave no numbers after a certain point, but we just proved that there are an infinite number of primes! In fact, that's part of what makes primes so interesting: not only is the number line studded with primes all the way up to infinity, but that entire number line can be produced using nothing but primes.

Primes are relevant in certain fields due to their special properties for factorization. While it is relatively easy to find larger prime numbers, it's *a lot harder* to factor large numbers back into primes. It's one thing to figure out that 20 is $(2 \times 2 \times 5)$ and another to figure out that 2,244,354 is $(2 \times 3 \times 7 \times 53,437)$. It's quite another again to find the prime factors of a number fifty digits long. Though the best mathematicians have chewed on the problem for hundreds of years, there just doesn't seem to be any way to factor large numbers efficiently.

That fact makes primes vitally important to communications. Most modern computer cryptography works by using the prime factors of large numbers. The large number that was used to encrypt a file can be publicly known and available, because the encryption works so only the prime factors of that large number can be used to decrypt it again. Though finding those factors is technically only a matter of time, it's a matter of so much time that we say it cannot be done. A modern super-computer could chew on a 256-bit factorization problem for longer than the current age of the universe, and still not get the answer.

Primes are of the utmost importance to number theorists because they are the building blocks of whole numbers, and important to the world because their odd mathematical properties make them perfect for our current uses. It truly is a prime age for prime numbers.