Math Circle
Beginners Group
February 28, 2016
Euclid and Prime Numbers

Warm-up Problems

1. What is a *prime* number? Give an example of an even prime number and an odd prime number.

   (a) Circle the prime numbers in the list of numbers below:

   1 4 8 13 17 101 121

2. The **Fundamental Theorem of Arithmetic** (also known as the **unique factorization theorem)** states that

   Any natural number greater than 1 *can be written as a product of prime numbers. Moreover, such a factorization is unique.*

   (a) Find prime factoriation of the following numbers:

   $3575 =$

   $7168 =$

(b) Should 1 be considered a prime number? Why or why not? (*Hint:* If we were to consider 1 a prime number, would the Fundamental Theorem of Arithmetic still be true?)

3. Explain what it means that two numbers p and q are *coprime.*

(a) For the given pairs of numbers, determine whether they are coprime.

i. 4, 8

ii. 13, 17

iii. 13, 51

(b) Do both numbers have to be prime in order for the pair to be coprime? If no, give an example.

(c) Does one of the numbers have to be prime in order for the pair to be coprime? If no, give an example.

(d) What is the greatest common divisor of two coprime numbers a and b?
$\mathbf{gcd}(a, b) =$

Euclid's lemma

Euclid of Alexandria was a Greek mathematician who lived in the 4^{th} century BC. Known as the "father of geometry" (remember Euclidean distance?), Euclid made immense contributions to many other fields of mathematics including algebra and number theory. We will be focusing on his work on prime numbers.

In mathematics, a lemma is a "helping theorem." It is a theorem with a simple proof that we largely use as a stepping stone to prove bigger theorems.

Euclid's lemma states that

If a prime number p divides the product of two numbers a and b, then p divides at least one of a or b.

We use the notation " $c \mid d$ " to show that the second number, d, is divisible by the first number, c.
We use the notation " $c \nmid d$ " to show that the second number, d, is not divisible by the first number, c.

With this notation, Euclid's lemma can be written as follows:

$$\text{If } p \mid a \cdot b, \text{ then } p \mid a \text{ or } p \mid b.$$

1. Let $p = 3$, $a = 5$, and $b = 6$.

   (a) Is p prime?

   (b) Does p divide $a \cdot b$?

   (c) What can we conclude using Euclid's lemma?

   (d) Which of the numbers, a or b, does p divide?

2. Write down the contrapositive to Euclid's lemma using the symbol $\nmid$.

   (a) Is this contrapositive true?

   (b) Give an example of a prime number p and two numbers a and b to test the contrapositive.

3. Write down the converse to Euclid's lemma using the symbols $\mid$ and $\nmid$.

   (a) Is this converse true?

   (b) Can you try to prove it?

4. Fill in the blanks:

   (a) $p \mid a \cdot b$ and $p \nmid a$, then _____.

   (b) If $p \mid a \cdot b$ and p is _____ to a, then $p \mid b$.

5. Let's test that this is only true when p is prime. Give an example of a composite number q and two numbers a and b, such that $q|a \cdot b$, but $q \nmid a$ and $q \nmid b$.

6. Does Euclid's lemma work when p divides the product of more than two numbers? Suppose that $p|a_1 \cdot a_2 \cdot a_3 \cdot ... \cdot a_n$. Does it follow that $p|a_1$ or $p|a_2$ or $p|a_3$ or ... or $p|a_n$?

   (a) Let $p = 2$, $a_1 = 3$, $a_2 = 2$, $a_3 = 5$, $a_2 = 4$. Is p prime?

   (b) Does p divide $a_1 \cdot a_2 \cdot a_3 \cdot a_4$?

   (c) What can we conclude using Euclid's lemma?

   (d) Which of the numbers, a_1, a_2, a_3 or a_4, does p divide?

7. We can use Euclid's lemma to prove that $\sqrt{2}$ is irrational. Recall that a number is called *rational* if it can be written in the form $\frac{m}{n}$, where m and n are coprime.

   (a) Let us suppose that $\sqrt{2}$ is rational. This means that

   $$\sqrt{2} = \frac{m}{n}, \qquad \text{where } m \text{ and } n \text{ are coprime.}$$

   (b) This is a proof by the method of _____.

   (c) Square both sides of the equality above.

   (d) Multiply both sides of the equality by n^2.

   (e) From the equality above, what do you know about the relationship between m^2 and 2? (Hint: Use the symbols $\mid$ or $\nmid$.)

   (f) Using the result above and fact that 2 is a prime number, explain what Euclid's lemma implies.

   (g) Is m even or odd? Why? What other form can m be written in?

(h) Therefore, $m^2 =$ _____.

(i) Substitute the new expression for m^2 into the equality you obtain for part c.

(j) Divide both sides of the equality by 2.

(k) From the equality above, what do you know about the relationship between n^2 and 2?

(l) Using the result above and fact that 2 is a prime number, what can we conclude from Euclid's lemma?

(m) Is n even or odd?

(n) Why have we reached a contradiction?

(o) What does this contradiction prove?

8. Using the same method, prove that $\sqrt{3}$ is irrational.

9. Using the same method as above, try to prove that $\sqrt{4}$ is irrational. Where does this proof fail?

The Goldbach Conjecture

In mathematics, a conjecture is a conclusion based on some information, for which a proof has not been found.

In 1742, the German mathematician Christian Goldbach noticed that, or so it seems, all even integers (except 2) can be written as the sum of two prime numbers. For example, $6 = 3 + 3$, $8 = 3 + 5$, or $24 = 13 + 11$.

Since then, computers have checked that the Goldbach Conjecture works for all even numbers up to 4×10^{18}. Many mathematicians have tried, but so far nobody was able to find a proof.

1. Express the following even numbers as a sum of two prime numbers.

   (a) $4 =$

   (b) $12 =$

   (c) $34 =$

   (d) $48 =$

   (e) $64 =$

2. Do you think the Goldbach Conjecture is true for odd numbers? Explain why or why not.