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

Warm-up Problems

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

   A prime number is a natural number greater than 1 that is only divisible by 1 and itself.

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

   $$1 \quad 4 \quad 8 \quad 13 \quad 17 \quad 101 \quad 121$$

   The prime numbers are 13, 17, and 101.

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:

   $$3575 = 5^2 \times 11 \times 13$$

   $$7168 = 2^{10} \times 7$$

(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?)

1 is neither a prime nor a composite number. If 1 were considered prime, the Fundamental Theorem of Arithmetic would fail to be true because prime factorizations of numbers would not remain unique.

For example, the prime factorization of 5 could be written as 5×1 *or* $5 \times 1 \times 1$*, making the factorization not unique.*

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

Two numbers p *and* q *are said to be coprime if the only positive integer that divides them both is* 1*.*

Or, in fewer words, $gcd(p, q) = 1$ *if* p *and* q *are coprime.*

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

i. 4, 8

Not coprime. $gcd(4, 8) = 2$*.*

ii. 13, 17

Coprime. $gcd(13, 17) = 1$*.*

iii. 13, 51

Coprime. $gcd(13, 51) = 1$*.*

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

No, both numbers do not have to be prime in order for the pair to be coprime. For example, 3 *and* 4 *are coprime, but* 4 *is not prime.*

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

No, even one of the numbers does not have to be prime in order for the pair to be coprime. For example, 4 *and* 9 *are coprime, but neither* 4 *nor* 9 *is prime.*

(d) What is the greatest common divisor of two coprime numbers a and b?

$\mathbf{gcd}(a, b) = 1$

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?
   Yes.

   (b) Does p divide $a \cdot b$?
   Yes, $5 \times 6 = 30$ *is divisible by* 3.

   (c) What can we conclude using Euclid's lemma?
   According to Euclid's lemma, 3 *must divide at least one of* 5 *or* 6.

   (d) Which of the numbers, a or b, does p divide?
   3 *divides* 6.

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

   The contrapositive to Euclid's lemma states that

   $$\textit{if } p \nmid a \textit{ and } p \nmid b, \textit{ then } p \nmid a \cdot b.$$

   (a) Is this contrapositive true?

   If Euclid's lemma is true, then its contrapositive must also be true.

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

   For example, if $4 \nmid 11$ *and* $4 \nmid 9$, *then* $p \nmid 99$.

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

   The converse to Euclid's lemma states that

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

   (a) Is this converse true?

   The converse may or may not be true. We need to prove it.

   (b) Can you try to prove it?

   Say, without loss of generality, $p \mid a$ *and* $p \nmid b$.
   Therefore, $a = k \cdot p$.
   So, $a \cdot b = p \cdot k \cdot b$.
   We know that $p \mid p \cdot k \cdot b$. *Therefore,* $p \mid a \cdot b$.
   Thus, the converse is true.

4. Fill in the blanks:

   (a) $p \mid a \cdot b$ and $p \nmid a$, then $\underline{p \mid b}$.

   (b) If $p \mid a \cdot b$ and p is $\underline{\textit{coprime}}$ 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 $q \nmid b$.

   Say, $q = 4$, $a = 6$, *and* $b = 10$.

   $4 \mid 60$, *but* $4 \nmid 6$ *and* $4 \nmid 10$.

   Therefore, Euclid's lemma is only true for prime numbers.

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?
   Yes.

   (b) Does p divide $a_1 \cdot a_2 \cdot a_3 \cdot a_4$?
   Yes, $3 \times 2 \times 5 \times 4 = 120$ *is divisible by* 2.

   (c) What can we conclude using Euclid's lemma?
   According to Euclid's lemma, 2 *must divide at least one of* 3 *or* 2 *or* 5 *or* 4.

   (d) Which of the numbers, a_1, a_2, a_3 or a_4, does p divide?
   2 *divides* 2 *and* 4.

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 *contradiction*.

   (c) Square both sides of the equality above.
   $2 = \frac{m^2}{n^2}$

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

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

   (f) Using the result above and fact that 2 is a prime number, explain what Euclid's lemma implies.
   According to Euclid's lemma, if $2 \mid m^2$, *then* $2 \mid m$.

   (g) Is m even or odd? Why? What other form can m be written in?
   Because m *is divisible by* 2, m *is even. Therefore,* m *can be written as* $m = 2k$.

   (h) Therefore, $m^2 = 4k^2$.

(i) Substitute the new expression for m^2 into the equality you obtain for part d.
$2n^2 = 4k^2$

(j) Divide both sides of the equality by 2.
$n^2 = 2k^2$

(k) From the equality above, what do you know about the relationship between n^2 and 2?
Since n^2 *is divisible by* 2, $2 \mid n^2$.

(l) Using the result above and fact that 2 is a prime number, what can we conclude from Euclid's lemma?
According to Euclid's lemma, if $2 \mid n^2$, *then* $2 \mid n$.

(m) Is n even or odd?
Because n *is divisible by* 2, n *is even.*

(n) Why have we reached a contradiction?
According to our original assumption, m *and* n *were coprime. However, as proven above, they are both even and have a common prime factor of* 2. *This contradicts our assumption.*

(o) What does this contradiction prove?
We now know that $\sqrt{2}$ *must be irrational, since it cannot be written in the smallest form* $\frac{m}{n}$, *where* m *and* n *are coprime.*

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

Let us suppose that $\sqrt{3}$ is rational. This means that

$$\sqrt{3} = \frac{m}{n}, \qquad \text{where } m \text{ and } n \text{ are coprime.}$$

Squaring both sides of the equality above, $3 = \frac{m^2}{n^2}$.

Multiplying both sides of the equality by n^2, $3n^2 = m^2$.

From the equality above, we know that m^2 is divisible by 3.
Therefore, $3 \mid m^2$.

According to Euclid's lemma, if $3 \mid m^2$, then $3 \mid m$.

Since m is divisible by 3, m can be written as $m = 3k$.

Therefore, $m^2 = 9k^2$.

Substituting the new expression for m^2, we get $3n^2 = 9k^2$.

Dividing both sides of the equality by 3, $n^2 = 3k^2$.

Since n^2 is divisible by 3, $3 \mid n^2$.

According to Euclid's lemma, if $3 \mid n^2$, then $3 \mid n$.
Therefore, n is divisible by 3.

According to our original assumption, m and n were coprime. However, as proven above, they are both divisible by 3. This contradicts our assumption.

We now know that $\sqrt{3}$ must be irrational, since it cannot be written in the smallest form $\frac{m}{n}$, where m and n are coprime.

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

   To try to prove that $\sqrt{4}$ is irrational by the method of contradiction, let us suppose that $\sqrt{4}$ is rational. This means that

   $$\sqrt{4} = \frac{m}{n}, \qquad \text{where } m \text{ and } n \text{ are coprime.}$$

   Squaring both sides of the equality above, $4 = \frac{m^2}{n^2}$.

   Multiplying both sides of the equality by n^2, $4n^2 = m^2$.

   From the equality above, we know that m^2 is divisible by 4.

   Therefore, $4 \mid m^2$.

   We cannot apply Euclid's lemma here because 4 is not a prime number. We cannot continue, and here is where the proof fails.

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) $4 = 2 + 2$

   (b) $12 = 5 + 7$

   (c) $34 = 23 + 11$

   (d) $48 = 17 + 31$

   (e) $64 = 23 + 41$

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

   The Goldbach Conjecture is not true for all odd numbers. This is because only the sum of an odd and an even number make an odd number. The only even prime number is 2. Only the odd numbers which differ from a prime number by 2 can be written as the sum of two prime numbers.