Cool Results on Primes

LA Math Circle (Advanced)

January 24, 2016

Recall that last week we learned an algorithm that seemed to magically spit out greatest common divisors, but we weren't quite sure why it did. The algorithm went as follows:

Take two integers a and b, divide one by the other with remainder, then divide the divisor by the remainder, then divide the new divisor by the new remainder... Eventually we perform a division with remainder 0, and we look directly above the zero, and we find the greatest common divisor of a and b right there.

Example If $a = 77, b = 30$, then we get

$$\begin{aligned} 77 &= 2 \cdot 30 + 17 \\ 30 &= 1 \cdot 17 + 13 \\ 17 &= 1 \cdot 13 + 4 \\ 13 &= 3 \cdot 4 + \boxed{1} \\ 4 &= 4 \cdot 1 + 0 \end{aligned}$$

Problem 1 Perform the division algorithm on the following pairs of integers:

$a = 88, b = 254$ $\qquad\qquad$ $a = 107, b = 284$

$a = 65, b = 1035$ $a = 517, b = 352$

$a = 1053, b = 51$ $a = 1012, b = 528$

Now it's time to make an important observation. Let's start by rearranging the equations on the first page as follows:

$$17 = 77 - 2 \cdot 30 \tag{1}$$
$$13 = 30 - 1 \cdot 17 \tag{2}$$
$$4 = 17 - 1 \cdot 13 \tag{3}$$
$$\boxed{1} = 13 - 3 \cdot 4 \tag{4}$$

We can plug equation (3) into equation (4):

$$1 = 13 - 3 \cdot (17 - 1 \cdot 13) = 4 \cdot 13 - 3 \cdot 17 \tag{5}$$

Now we can plug equation (2) into equation (5):

$$1 = 4 \cdot (30 - 1 \cdot 17) - 3 \cdot 17 = 4 \cdot 30 - 7 \cdot 17 \tag{6}$$

Finally, if we plug equation (1) into equation (6):

$$1 = 4 \cdot 30 - 7 \cdot (77 - 2 \cdot 30) = 18 \cdot 30 - 7 \cdot 77 \tag{7}$$

Equation (7) may look uninteresting right now, but it expresses the output d of the Euclidean algorithm in the form

$$d = ax + by,$$

where a, b are the input and x and y are integers. We will see soon that this is actually extremely interesting.

Problem 2 Write the output d of the Euclidean algorithm in the form $ax+by$ where a and b are the input (use your work from page 2 to help):

$a = 88, b = 254$ $\qquad\qquad$ $a = 107, b = 284$

$a = 65, b = 1035$

$a = 517, b = 352$

$a = 1053, b = 51$

$a = 1012, b = 528$

We will soon use the equation $d = ax + by$ to prove that d is the greatest common divisor of a and b, but first, we will review from last class:

Problem 3 Explain why for any integers a and b which aren't zero, the Euclidean algorithm must eventually stop. (Hint: what happens to the remainders at each successive step?)

Problem 4 Let's say we pick integers a and b, we do the Euclidean algorithm with them, and it takes 4 steps:

$$\begin{aligned} a &= q \cdot b + r \\ b &= q_1 \cdot r + r_1 \\ r &= q_2 \cdot r_1 + r_2 \\ r_1 &= q_3 \cdot r_2 + r_3 \\ r_2 &= q_4 \cdot r_3 + 0 \end{aligned}$$

Prove that $r_3|a$ and $r_3|b$. (Hint: repeatedly use the fact that if $a|b$ and $a|c$, and x, y are integers, then $a|bx + cy$.)

Problem 5 If d is the output of the Euclidean algorithm with input a and b, we learned that we can always write $d = ax + by$ for some integers x and y. Use this fact to prove that if $e|a$ and $e|b$, then $e|d$.

Recall the definition of greatest common divisor:

If a, b, and d are integers, we say that d is a *greatest common divisor* of a and b if:

1. $d|a$ and $d|b$
2. If e is any other integer such that $e|a$ and $e|b$, then $e|d$.

If d is the output of the Euclidean algorithm with input a and b, then problem 4 shows that d satisfies condition 1, and problem 5 shows that d satisfies condition 2. So we did it! Now we know why our mysterious calculations always yield greatest common divisors! Actually, we learned some other things too:

1. Greatest common divisors always *exist*.

   Look at the definition of the greatest common divisor - it tells us when a number d is a greatest common divisor of a and b. But it's not obvious that two random integers a and b will actually *have* a greatest common divisor. You probably very strongly *believed* that all pairs of integers had greatest common divisors, but now for the very first time, you *know* it! If that doesn't help you sleep at night, I don't know what will.

2. You can easily (especially with the aid of a computer) *find* the greatest common divisor of any two integers.

3. If d is the greatest common divisor of a and b, then there are numbers x and y such that

   $$d = ax + by.$$

   This last discovery is very important from the theoretical point of view. We'll illustrate why by using it to prove some very cool things about primes - the goal of today's class.

Problem 6 If p is a prime number and a is a number which is not divisible by p, prove that 1 is a common divisor of a and p.

Problem 7 Prove that 1 also satisfies the second condition of being a greatest common divisor of a and p.

Problem 8 If p is a prime number and a is a number which is not divisible by p, prove that there are numbers x and y such that $ax + py = 1$.

Problem 9 If p is a prime number and a and b are numbers such that $p \not| a$ but $p|ab$, prove that $p|b$. (Hint: multiply the equation $ax + py = 1$ on both sides by b.)

So, we have arrived at what is easily the most important property of prime numbers: If p is prime, then

$$\boxed{p|ab \implies p|a \text{ or } p|b.}$$

Problem 10 Is this true when p is not prime?

We can use the fact in the box to prove an interesting fact about prime numbers: their square roots are not rational (rational numbers are fractions $\frac{a}{b}$ with a, b integers). For a very long time (probably until the 5th century BC), nobody knew that there were any irrational (= not rational) numbers. This seems reasonable: you probably know π is irrational, but 3.14159265358979323846264338327950288419716 9 is rational, and is very close to π.

Strategy It will help to have a strategy for proving a number is irrational. This strategy is called proof by contradiction: If we want to show the number x is irrational, we will assume it's rational, so we can write $x = \frac{a}{b}$, and show that this is actually impossible.

Problem 11 Use the strategy to prove that if x is a rational number and y is an irrational number, then $x + y$ is an irrational number.

Problem 12 Use the strategy to prove that $\sqrt{2}$ is irrational. (Hint: any fraction can be written in the form $\frac{a}{b}$ where a and b have no common divisors - that is, as a *reduced* fraction.)

Problem 13 Adapt the argument from problem 10 to show that $\sqrt{p}$ is irrational for any prime number p.

Next we want to show that any integer $n \geq 2$ can be written as a product $p_1 \cdot p_2 \cdots p_k$ of prime numbers $p_1, p_2, \ldots, p_k$.

Problem 14 Complete the following proof of the fact described above:

Suppose toward a contradiction that there are integers ≥ 2 which cannot be factored into primes. 2 can be factored into primes (it is a prime itself), so can 3, and $4 = 2 \cdot 2$, and so on. But eventually we must get to a *first* integer n which cannot be factored into primes - that is, n has no prime factorization, but every number smaller than n does... (Hint: can n be prime? Why or why not? What does this tell us?)

As an application of the existence of prime factorizations, we will prove Euclid's theorem that there are infinitely many primes:

Problem 15 Complete the following proof that there are infinitely many primes:

Suppose toward a contradiction that there are only finitely many primes. Then we can list them out as $p_1, p_2, \ldots, p_N$. Now consider the number $p_1 \cdot p_2 \cdots p_N + 1$. This number has a prime factorization, so in particular, it is divisible by some prime p...

To solve problem 13, the existence of a prime factorization was sufficient, but for many problems it's not. For them, we also need to know that this prime factorization is unique. More precisely:

If $p_1 \cdot p_2 \cdots p_k$ and $q_1 \cdot q_2 \cdots q_l$ are two prime factorizations of the same number n, then $k = l$ and the list $q_1, q_2, \ldots, q_l$ is a rearrangement of the list $p_1, p_2, \cdots, p_k$ [1].

Problem 16 Prove that prime factorizations of integers are unique. (Hint: $p_1 \cdot p_2 \cdots p_k = q_1 \cdot q_2 \cdots q_l$, so $p_1 | q_1 \cdot q_2 \cdots q_l$. Now from the property in the box on page 8, $p_1 | q_j$ for some j, so...)

[1] For example, 2, 3, 5, 3, 3, 5, 7 is a rearrangement of 3, 3, 3, 7, 5, 5, 2.

As a nice illustration of the power of the uniqueness theorem we've just proven, we can give a slightly simpler proof that $\sqrt{2}$ is irrational:

Suppose otherwise. Then we can write $\sqrt{2} = \dfrac{a}{b}$ where $a = p_1 p_2 \cdots p_k$ and $b = q_1 q_2 \cdots q_l$. If we multiply both sides of the equation by b and then square both sides, we get

$$2q_1^2 \cdot q_2^2 \cdots q_l^2 = p_1^2 \cdot p_2^2 \cdots p_k^2.$$

But 2 appears an odd number of times on the prime factorization on the left, and an even number of times on the prime factorization on the right, a contradiction.

Problem 17 Use the argument above to give another proof that $\sqrt{p}$ is irrational for any prime p.

Problem 18 Repeat the same argument to prove that actually, if $\sqrt{n}$ is rational, then n must be a perfect square. (Hint: If $n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$, where $p_1, p_2, \ldots, p_k$ are distinct primes, then it is enough to show that $e_1, e_2, \ldots, e_k$ are all even. Why?)

Problem 19 Suppose x, y, z, w are nonnegative integers and

$$2^x \cdot 3^y \cdot 5^z \cdot 7^w = 756.$$

Find $2x + 3y + 5z + 7w$.

Problem 20 In this problem, we'll give an example of an "object" which admits factorization into irreducible elements, but this factorization is not unique.

The "object" is the collection of all even integers. We can add, subtract, and multiply even integers, and the result is still an even integer, so we can consider this object as its own number system.

Explain why an even integer should be considered "irreducible" in this number system if it is divisible by 2 only once, and find two distinct factorizations of the number 36 into irreducibles.