Divisibility and the Euclidean Algorithm

LA Math Circle (Advanced)

January 17, 2016

Our lesson today is almost entirely based on the following definition:

If a and b are integers, we say that a *divides* b (or b is *divisible* by a) if there is an integer c so that $ac = b$.

The shorthand notation for the sentence"a divides b" is $a|b$.

Problem 1 True or false?

$3\|5$	$8\|8$	$7\|35$
$144\|0$	$3\|10$	$30\|20$
$-5\|125$	$-12\|3$	$16\|8$
$8\|-64$	$-4\|-2$	$3\|156782149$

Problem 2 List the first 7 nonnegative integers which are divisible by 8.

Problem 3 List the first 5 nonnegative numbers n such that $4|n-1$.

Problem 4 List all the prime numbers (with multiplicity) that divide the following numbers:

13	156	72
125	1034	1908

Problem 5 Prove that if $a|b$ and c is any integer, then $a|bc$.

Problem 6 Prove that if $a|b$ and $a|c$, then $a|b+c$.

Problem 7 Prove that if $a|b$, $a|c$, and x, y are any integers, then $a|bx+cy$.

Next, we'll define the greatest common divisor of two numbers. This is exactly how you remember it from elementary school.

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 $e|d$.

Note that the first condition says that d *is* a common divisor of a and b (i.e. it divides both of them), and the second condition says that among all common divisors e of a and b, d is the biggest. That is, the definition is exactly what you would expect it to be.

We'll give two methods for computing greatest common divisors in this handout.

Method 1 This is the method you've known since you were very young. Let's say the integers are 42 and 63. We start by factoring 42 and 63 into primes:

$$42 = 2 \cdot 3 \cdot 7$$
$$63 = 3 \cdot 3 \cdot 7$$

Now d will be the product of all the common prime factors of 42 and 63.

Does 2 go into d? No, because 2 is not a divisor of 63. However, 3 divides both, so three goes into d. Does 3 go into d a second time? No, because 3 only divides 42 once. Finally, 7 goes into d since 7 divides both 42 and 63. So, we get

$$d = 3 \cdot 7 = 21.$$

Problem 8 Use method 1 to find the greatest common divisors of the following pairs of integers:

$a = 144, b = 30$ $a = 6, b = 125$

$a = 583, b = 530$ $a = 1331, b = 297$

$a = 3591, b = 270$ $a = 3025, b = 143$

Method 2 This method is completely different. It's called the Euclidean algorithm, after the ancient Greek geometer. The basis for the Euclidean algorithm is elementary school division with remainder - if a, b are integers, and $b \neq 0$, then we can write $a = qb + r$ where r is the remainder, and $0 \leq r < b$. But now we can also divide b by r: $b = q_1 r + r_1$ with $0 \leq r_1 < r$. Now do it again: $r = q_2 r_1 + r_2$, and so on. It's not immediately clear why anyone would want to keep doing this, but let's just see what happens when we do:

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

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

Note that the boxed number is the greatest common divisor of 77 and 30!

Problem 9 Try the algorithm out with the same numbers you used in problem 8. Does the algorithm output the same results you got in that problem?

$a = 144, b = 30$ $a = 6, b = 125$

$a = 583, b = 530$ $a = 1331, b = 297$

$a = 3591, b = 270$ $a = 3025, b = 143$

The real advantages of method 2 over method 1 are that you can easily make a computer do method 2, and that method 2 is much faster for very large integers:

Problem 10 Find the greatest common divisor of 53024 and 4033. Use whichever method you want!

Problem 11 A farmer buys 2871 apple trees and 1716 orange trees, and he wants to plant them in rows which all have the same number of trees, and such that each row contains only one type of tree. What is the largest number of trees he can plant per row?

Now it's time to figure out why the algorithm works.

Problem 12 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 13 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: we know $r_3|r_2$, and using problem 7, we can see that $r_3|r_1$ . . .)

This shows that the output of the Euclidean algorithm satisfies condition 1 of the definition of greatest common divisor (flip back to page 3). Now to see that it satisfies condition 2, we will use the following observation:

If d is the output of the Euclidean algorithm when the input is a, b, then we can always write

$$d = ax + by$$

for some integers x and y.

For instance, in the example on page 5,

$$\begin{aligned} 1 &= 13 - 3 \cdot 4 = 13 - 3(17 - 1 \cdot 13) = 4 \cdot 13 - 3 \cdot 17 \\ &= 4(30 - 1 \cdot 17) - 3 \cdot 17 = 4 \cdot 30 - 7 \cdot 17 \\ &= 4 \cdot 30 - 7(77 - 2 \cdot 30) = 18 \cdot 30 - 7 \cdot 77. \end{aligned}$$

Problem 14 Express the greatest common divisors of a and b in the form $d = ax + by$ using the method shown above (It'll help to flip back to page 5).

$a = 144, b = 30$ $\qquad\qquad$ $a = 6, b = 125$

$a = 583, b = 530$ $\qquad\qquad$ $a = 1331, b = 297$

Problem 15 Let d be the output of the Euclidean algorithm from the input a, b. Use the observation that $d = ax + by$ for some integers x, y combined with problem 7 to prove that d is the greatest common divisor of a and b.

Quick Summary

So now we've discovered that:

1. Greatest common divisors always *exist*.

   Look back 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 the most important from the theoretical point of view. We'll see why on the next page.

Problem 16 If p is a prime number and a is a number which is not divisible by p, prove that a and p have greatest common divisor 1 (Check that both conditions in the definition of greatest common divisor hold).

Problem 17 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 18 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 arrive at what is easily the most important property of prime numbers: If p is prime, then

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