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?

$3|5$ F

$144|0$ T

$-5|125$ T

$8|-64$ T

$8|8$ T

$3|10$ F

$-12|3$ F

$-4|-2$ F

$7|35$ T

$30|20$ F

$16|8$ F

$3|156782149$ F

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

0, 8, 16, 24, 32, 40, 48

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

1, 5, 9, 13, 17

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

13   13   156 $2^2\cdot 3\cdot 13$ 72 $2\cdot 2\cdot 2\cdot 3\cdot 3$

125   $5\cdot 5\cdot 5$ 1034 $2\cdot 11\cdot 47$ 1908 $2\cdot 2\cdot 3\cdot 3 . 53$

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

Given:

There is an integer m so that $a\cdot m=b$

Goal:

There is an integer n so that $a\cdot n=bc$.

We Know

$bc=(a\cdot m)c=a\cdot(mc)$, so if we set $n=mc$,

then $a\cdot n=bc$, which was our goal.

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

Given:

There are integers m_1 and m_2 so that $a\cdot m_1=b$ and $a\cdot m_2=c$.

Goal.

There is an integer n so that $a\cdot n=b+c$.

We Know that

$b+c=a\cdot m_1+a\cdot m_2=a(m_1+m_2)$ so that if we set $n=m_1+m_2$, then $a\cdot n=b+c$.

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

By 5, $a|bx$ and $a|cy$, but then by 6, $a|bx+cy$.

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:

$$\begin{aligned} 42 &= 2 \cdot 3 \cdot 7 \\ 63 &= 3 \cdot 3 \cdot 7 \end{aligned}$$

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:

$a = 144, b = 30$

6

$a = 6, b = 125$

1

$a = 583, b = 530$

53

$a = 1331, b = 297$

11

$a = 3591, b = 270$

27

$a = 3025, b = 143$

11

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?

$a = 144, b = 30$

$$
\begin{aligned}
144 &= 4 \cdot 30 + 24 \\
30 &= 1 \cdot 24 + \boxed{6} \\
24 &= 4 \cdot 6 + 0
\end{aligned}
$$

$a = 6, b = 125$

$$
\begin{aligned}
125 &= 20 \cdot 6 + 5 \\
6 &= 1 \cdot 5 + \boxed{1} \\
5 &= 5 \cdot 1 + 0
\end{aligned}
$$

$a = 583, b = 530$

$$
\begin{aligned}
583 &= 1 \cdot 530 + \boxed{53} \\
530 &= 10 \cdot 53 + 0
\end{aligned}
$$

$a = 1331, b = 297$

$$
\begin{aligned}
1331 &= 4 \cdot 297 + 143 \\
297 &= 2 \cdot 143 + \boxed{11} \\
143 &= 13 \cdot 11 + 0
\end{aligned}
$$

$a = 3591, b = 270$

$$
\begin{aligned}
3591 &= 13 \cdot 270 + 81 \\
270 &= 3 \cdot 81 + \boxed{27} \\
81 &= 3 \cdot 27 + 0
\end{aligned}
$$

$a = 3025, b = 143$

$$
\begin{aligned}
3025 &= 21 \cdot 143 + 22 \\
143 &= 6 \cdot 22 + \boxed{11} \\
22 &= 2 \cdot 11 + 0
\end{aligned}
$$

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!

$53024 = 13 \cdot 4033 + 595$

$4033 = 6 \cdot 595 + 463$

$595 = 1 \cdot 463 + 132$

$463 = 3 \cdot 132 + 67$

$132 = 1 \cdot 67 + 65$

$67 = 1 \cdot 65 + 2$

$65 = 32 \cdot 2 + \boxed{1}$

$2 = 2 \cdot 1 + 0$

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?

$2871 = 1 \cdot 1716 + 1155$

$1716 = 1 \cdot 1155 + 561$

$1155 = 2 \cdot 561 + \boxed{33}$

$561 = 17 \cdot 33 + 0$

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?)

The remainders get smaller at each step (see problem 10) because the remainder when a is divided by b is always less than b. So, the remainders will get to 0 in $\leq b$ steps.

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 $r_3|r_1 \ldots$)

$r_2 = q_4 \cdot r_3$ so $r_3 | r_2$ by definition.

Now $r_3 | r_3$ and $r_3 | r_2$ so by problem 7, $r_3 | q_3 \cdot r_2 + r_3 = r_1$.

But now $r_3 | r_2$ and $r_3 | r_1$, so $r_3 | r = q_2 \cdot r_1 + r_2$ by problem 7.

Now $r_3 | r_1$ and $r_3 | r$, so $r_3 | b = q_1 \cdot r + r_1$.

Now $r_3 | r$ and $r_3 | b$ so $r_3 | q \cdot b + r = a$.

So, $\boxed{r_3 | a \text{ and } r_3 | b}$.