

**MATH 8**  
**NUMBER THEORY 2: EUCLID'S ALGORITHM**  
MARCH 15, 2026

NOTATION

$\mathbb{Z}$  — all integers

$\mathbb{N}$  — positive integers:  $\mathbb{N} = \{1, 2, 3 \dots\}$ .

$d|a$  means that  $d$  is a divisor of  $a$ , i.e.,  $a = dk$  for some integer  $k$ .

$\gcd(a, b)$ : greatest common divisor of  $a, b$ .

EUCLID'S ALGORITHM

**Theorem.** *If  $a = bq + r$ , then the common divisors of pair  $(a, b)$  are the same as common divisors of pair  $(b, r)$ . In particular,*

$$\gcd(a, b) = \gcd(b, r)$$

(a special case of this was in your last HW).

*Proof.* Let  $d$  be a common divisor of  $(a, b)$ . Since  $r = a - bq$ , and both  $a, bq$  are divisible by  $d$ ,  $r$  is also divisible by  $d$ , so  $d$  is a common divisor of  $a, r$ . Proof in the opposite direction is similar.  $\square$

This gives a very efficient way of computing the greatest common divisor of  $(a, b)$ , called Euclid's algorithm:

1. If needed, switch the two numbers so that  $a > b$
2. Compute the remainder  $r$  upon division of  $a$  by  $b$ . Replace pair  $(a, b)$  with the pair  $(b, r)$
3. Repeat the previous step until you get a pair of the form  $(d, 0)$ . Then  $\gcd(a, b) = \gcd(d, 0) = d$ .

For example:

$$\begin{aligned} \gcd(42, 100) &= \gcd(42, 16) && \text{(because } 100 = 2 \cdot 42 + 16) \\ &= \gcd(16, 10) = \gcd(10, 6) = \gcd(6, 4) \\ &= \gcd(4, 2) = \gcd(2, 0) = 2 \end{aligned}$$

As a corollary of this algorithm, we also get the following two important results.

**Theorem.** *Let  $d = \gcd(a, b)$ . Then  $m$  is a common divisor of  $a, b$  if and only if  $m$  is a divisor of  $d$ .*

In other words, common divisors of  $a, b$  are the same as divisors of  $d = \gcd(a, b)$ , so knowing the gcd gives us **all** common divisors of  $a, b$ .

**Theorem.** *Let  $d = \gcd(a, b)$ . Then it is possible to write  $d$  in the following form*

$$d = xa + yb$$

for some  $x, y \in \mathbb{Z}$ .

(Expressions of this form are called linear combinations of  $a, b$ .)

*Proof.* Euclid's algorithm produces for us a sequence of pairs of numbers:

$$(a, b) \rightarrow (a_1, b_1) \rightarrow (a_2, b_2) \rightarrow \dots$$

and the last pair in this sequence is  $(d, 0)$ , where  $d = \gcd(a, b)$ .

We claim that we can write  $(a_1, b_1)$  as linear combination of  $a, b$ . Indeed, by definition

$$\begin{aligned} a_1 &= b = 0 \cdot a + 1 \cdot b \\ b_1 &= r = a - qb = 1 \cdot a - qb \end{aligned}$$

where  $a = qb + r$ .

By the same reasoning, one can write  $a_2, b_2$  as linear combination of  $a_1, b_1$ . Combining these two statements, we get that one can write  $a_2, b_2$  as linear combinations of  $a, b$ . We can now continue in the same way until we reach  $(d, 0)$ .  $\square$

Here is an example. We have shown above that  $\gcd(100, 42) = 2$  using Euclid's algorithm. We can now use that computation to write 2 as a linear combination of 100 and 42:

$$\begin{aligned} 16 &= 100 - 2 \cdot 42 \\ 10 &= 42 - 2 \cdot 16 = 42 - 2(100 - 2 \cdot 42) = -2 \cdot 100 + 5 \cdot 42 \\ 6 &= 16 - 10 = (100 - 2 \cdot 42) - (-2 \cdot 100 + 5 \cdot 42) = 3 \cdot 100 - 7 \cdot 42 \\ 4 &= 10 - 6 = (-2 \cdot 100 + 5 \cdot 42) - (3 \cdot 100 - 7 \cdot 42) = -5 \cdot 100 + 12 \cdot 42 \\ 2 &= 6 - 4 = (3 \cdot 100 - 7 \cdot 42) - (-5 \cdot 100 + 12 \cdot 42) = 8 \cdot 100 - 19 \cdot 42 \end{aligned}$$

#### PROBLEMS

When doing this homework, be careful that you only used the material we had proved or discussed so far — in particular, please do not use the prime factorization. And I ask that you only use integer numbers — no fractions or real numbers.

1. Use Euclid's algorithm to compute  $\gcd(54, 36)$ ;  $\gcd(97, 83)$ ;  $\gcd(1003, 991)$
2. Use Euclid's algorithm to find **all** common divisors of 2634 and 522.
3. Prove that  $\gcd(n, a(n+1)) = \gcd(n, a)$
4. (a) Is it true that for all  $a, b$  we have  $\gcd(2a, b) = 2 \gcd(a, b)$ ? If yes, prove; if not, give a counterexample.  
 (b) Is it true that *for some*  $a, b$  we have  $\gcd(2a, b) = 2 \gcd(a, b)$ ? If yes, give an example; if not, prove why it is impossible.
5. (a) Compute  $\gcd(14, 8)$  **using Euclid's algorithm**  
 (b) Write  $\gcd(14, 8)$  in the form  $8k + 14l$ . (You can use guess and check, or proceed in the same way as in the previous problem)  
 (c) Does the equation  $8x + 14y = 18$  have integer solutions? Can you find at least one solution?  
 (d) Does the equation  $8x + 14y = 17$  have integer solutions? Can you find at least one solution?  
 (e) Can you give complete answer, for which integer values of  $c$  the equation  $8x + 14y = c$  has integer solutions?
6. If I only have 15-cent coins and 12-cent coins, can I pay \$1.35? \$1.37?
7. You have two cups, one 240 ml, the other 140 ml. What amounts of water can be measured using these two cups? [You can assume that you also have a large bucket of unknown volume.]
8. (a) Show that if  $17c$  is divisible by 6, then  $c$  is divisible by 6.  
 Note: you can not use prime factorization - we have not yet proved that it is unique! Instead, you can argue as follows: since  $\gcd(17, 6) = 1$ , we can write  $1 = 17x + 6y$ . Thus,  $c = (17x + 6y)c$ . Now argue why the right-hand side is divisible by 6.  
 \*(b) More generally, prove that if  $a, b, c \in \mathbb{Z}$  are such that  $a|bc$  and  $\gcd(a, b) = 1$ , then one must have  $a|c$ .
9. (a) Show that if  $a$  is odd, then  $\gcd(a, 2b) = \gcd(a, b)$ .  
 \*(b) Show that for  $m, n \in \mathbb{N}$ ,  $\gcd(2^n - 1, 2^m - 1) = 2^{\gcd(m, n)} - 1$