

Handout 23. Number theory 2: Euclid algorithm.**Notation recap**

Natural numbers:

$$\mathbb{N} = \{1, 2, 3, \dots\}$$

Integer numbers:

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\} = \mathbb{N} \cup \{0\} \cup \{-n \mid n \in \mathbb{N}\}$$

 d is a divisor of m , m is a multiple of d , ($\exists k \in \mathbb{Z}, m = d \cdot k$):

$$d \mid m$$

Division representation for natural numbers:

$$\forall n, d \in \mathbb{N}, \exists q, r \in \mathbb{N}, (0 \leq r < d), n = q \cdot d + r$$

Division representation for integer numbers:

$$\forall n \in \mathbb{Z}, d \in \mathbb{N}, \exists q \in \mathbb{Z}, r \in \mathbb{N}, (0 \leq r < d), n = q \cdot d + r$$

Euclid's algorithm**Theorem 6.** If $a = bq + r$, then the common divisors of pair (a, b) are the same as common divisors of pair (b, r) . In particular,

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

This theorem provides a very efficient way of computing the $\gcd(a, b)$, called Euclid's algorithm.**Corollary** (Euclid's algorithm). To compute the $\gcd(a, b)$:

1. If needed, switch the two numbers so that $a > b$
2. Compute the remainder r upon division of a by b : $a = bq + r$. Because $\gcd(a, b) = \gcd(b, r)$, we can 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,

$$\gcd(a, b) = \gcd(b, r) = \dots = \gcd(d, 0) = d$$

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

Proof. Left as a homework exercise. \square

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 7. Let $d = \gcd(a, b)$. Then, $\exists x, y \in \mathbb{Z}$ such that it is possible to write d in the form

$$d = xa + yb$$

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

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

$$(a, b) \rightarrow (a_1, b_1) \rightarrow (a_2, b_2) \rightarrow \cdots \rightarrow (d, 0)$$

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

We observe that (a_1, b_1) can be written as a linear combination of a, b . Indeed, because $a = qb + r$,

$$a_1 = b = 0a + 1b$$

$$b_1 = r = a - qb = 1a + (-q)b$$

By the same reasoning, one can write a_2, b_2 as a linear combination of a_1, b_1 ($a_2 = b_1 = q_1b_1 + b_2$, so

$$a_2 = b_1 = 0a_1 + 1b_1$$

$$b_2 = 1a_1 + (-q_1)b_1$$

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

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

$$16 = 100 - 2 \cdot 42$$

$$10 = 42 - 2 \cdot 16 = 42 - 2 \cdot (100 - 2 \cdot 42) = -2 \cdot 100 + 5 \cdot 42$$

$$6 = 16 - 10 = (100 - 2 \cdot 42) - (-2 \cdot 100 + 5 \cdot 42) = 3 \cdot 100 - 7 \cdot 42$$

$$4 = 10 - 6 = (-2 \cdot 100 + 5 \cdot 42) - (3 \cdot 100 - 7 \cdot 42) = -5 \cdot 100 + 12 \cdot 42$$

$$2 = 6 - 4 = (3 \cdot 100 - 7 \cdot 42) - (-5 \cdot 100 + 12 \cdot 42) = 8 \cdot 100 - 19 \cdot 42$$

Homework problems

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

1. Use Euclid's algorithm to compute
 - a. $\gcd(54,36)$
 - b. $\gcd(97,83)$
 - c. $\gcd(1003,991)$
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. Is it true that
 - a. $\forall a, b, \gcd(2a, b) = 2\gcd(a, b)$? If yes, prove; if not, give a counterexample.
 - b. $\exists a, b, \gcd(2a, b) = 2\gcd(a, b)$? If yes, give an example; if not, prove why it is impossible.
5.
 - a. Using Euclid's algorithm, compute $\gcd(14,8)$
 - 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, using Theorem 7)
 - 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. Find all integer values of c for which 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. Prove that
 - a. if $17c$ is divisible by 6, then c is divisible by 6. (Note: you cannot 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, if $a, b, c \in \mathbb{Z}$ are such that $a|bc$ and $\gcd(a, b) = 1$, then $a|c$.
9. Show that
 - a. if a is odd, then $\gcd(a, 2b) = \gcd(a, b)$. Hint: you can use "theorem" in 8(b) even if you haven't solved it.
 - b. * for $m, n \in \mathbb{N}$, $\gcd(2^n - 1, 2^m - 1) = 2^{\gcd(m,n)} - 1$