MATH 8
HANDOUT 20: EUCLID'S ALGORITHM

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

In the last assignment, we proved the following:

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,*

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

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:

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

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*

$$d = ka + lb$$

for some $k, l \in \mathbb{Z}$.

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

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

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

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 $(d, 0)$. $\square$

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. Write each of the numbers appearing in the computation of $\gcd(100, 42)$ above in the form $k \cdot 100 + l \cdot 42$, for some integers k, l. For example,

$$16 = 1 \cdot 100 - 2 \cdot 42,$$
$$10 = 42 - 2 \cdot 16 = 42 - 2(100 - 2 \cdot 42) = \dots$$

6. (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?

7. If I only have 15-cent coins and 12-cent coins, can I pay $1.35? $1.37?

8. Let $a, b, c \in \mathbb{Z}$ be such that $a|bc$ and $\gcd(a, b) = 1$. Prove that then one must have $a|c$. [Remember, you can not use prime factorization - we have not yet proved that it is unique!]
Hint: if $\gcd(a, b) = 1$, then $xa + yb = 1$ for some x, y, and therefore $c = (xa + yb)c$.

9. (a) Show that if a is odd, then $\gcd(a, 2b) = \gcd(a, b)$.
*(b) Show that for $m, n \in \mathbb{N}$, $\gcd(2^n - 1, 2^m - 1) = 2^{\gcd(m,n)} - 1$