Euclid's algorithm

An important, non-trivial example: Euclid's Algorithm

Theorem (Book Proposition 7.1): If a and b are natural numbers, then there exist integers k and l for which

$$\gcd(a, b) = ak + bl.$$

Comments:

- logical structure of this statement is "For all a and b in $\mathbb{N}$ there exists k and l in $\mathbb{Z}$ such that $\gcd(a, b) = ak + bl$.
- Note that k and l will depend on a and b.

The hidden part

Two key ideas

Lemma: Suppose that A is a set of integers, and d is the smallest positive element of A. Then if $r \in A$, and $r < d$, we must have $r \leq 0$.

Lemma: If x is a common divisor of a and b, and, for all common divisors g of a and b we have $x \geq g$, then x is the *greatest* common divisor of a and b.

Proof from the book.

Proposition 7.1: If $a, b \in \mathbb{N}$, then there exist integers k and l so that

$$\gcd(a, b) = ak + bl.$$

Proof: The set $A = \{ax + by : x, y \in \mathbb{Z}\}$ contains positive and negative integers, as well as 0. Let d be the *smallest positive element of A*. Since $d \in A$, there are values of x and y so that $d = ax + by$. Call one set of these values k and l, so that $d = ak + bl$.

proof, cont'd.

Step 1. d is a common divisor of a and b.

Proof: Find q and r so that $a = qd + r$ and $0 \leq r < d$. Then

$$r = a - qd = a - q(ak + bl) = (1 - qk)a + b(-ql).$$

Therefore $r \in A$. Since $0 \leq r < d$, and d is the *smallest* positive element of A, we must have $r = 0$. Here we have used the lemma above. Therefore $a = qd$ and so d is a divisor of a. The same argument works for b.

proof, cont'd

Step 2: $d = ax + kl$ is the *greatest* common divisor of a and b.

Proof: Let $g \in \mathbb{N}$ be any common divisor of a and b. Then $a = ug$ and $b = vg$ for natural numbers u and v. Therefore

$$d = ugk + vgl = g(uk + vl).$$

As a result, g is a divisor of d and so $d \geq g$. Therefore d is the greatest common divisor.

Notes

- Notice that we in fact proved that every common divisor of a and b is a divisor of $\gcd(a, b)$.
- Implicit in the proof is an *algorithm* for finding $\gcd(a, b)$, as well as k and l so that $\gcd(a, b) = ak + bl$.