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.

Hidden part

$a = 7,\ b = 3 \qquad \gcd(a,b) = 1$

$1 = \underline{7k + 3l} \qquad k = 1,\ l = -2$

$a = 17 \quad b = 5 \qquad 17 \cdot -2 + 7 \cdot 5 = 1$

$k = -2 \quad l = 7$

$a = 15 \quad b = 9 \qquad \gcd = 3$

$3 = 2 \cdot 15 + 9(-3)$

$7k + 3l$

$l \backslash k$	-2	-1	0	1	2
-2			-6	1	8
-1			-3	4	11
0	-14	-7	0	7	14
1	-11	-4	3	10	17
2	-8	-1	6		

...

$1 = 7 \cdot 1 + 3 \cdot (-2)$

$2 = 7 \cdot 2 + 3(-4)$

$5 = 7 \cdot 5 + 3(-10)$

Hidden part continued

$$15k + 9\ell = 3(5k + 3\ell)$$

$\ell \backslash k$	-2	-1	0	1	2
-2	-48	-33	-18	-3	12
-1		-24	-9	6	
0			0	15	
1			9	24	
2			18	33	

Conjecture:
Smallest positive value of the form $ak + b\ell$ as k, ℓ vary is the $\gcd(a,b)$.

A Lemma

Lemma: Let a and b be natural numbers. The set $A = \{ax + by : x, y \in \mathbb{Z}\}$ is *closed* under addition, meaning the sum (and difference) of any two elements of A is an element of A.

Proof:

$$t = ax_0 + by_0 \qquad x_0, y_0, x_1, y_1 \in \mathbb{Z}$$

$$s = ax_1 + by_1$$

$$t \pm s = a(x_0 \pm x_1) + b(y_0 \pm y_1)$$

$$t \pm s \in A$$

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 $0 \le r < d$. Then qd is in A and a is in A, so $r = a - qd$ is in A, since A is closed under addition.

$a \in A$ $\quad a = a \cdot 1 + b \cdot 0$ $\quad$ $d \in A$ so $qd \in A$ because $qd = \underbrace{d + d + d \cdots + d}_{q \text{ times}}$ $\quad qd \in A$ $\quad$ so $r \in A$

Since $0 \le r < d$, and d is the *smallest* positive element of A, we must have $r = 0$.

Therefore $a = qd$ and so d is a divisor of a. The same argument works for b.

smallest positive $ak + bl$ is a divisor of both a and b.

proof, cont'd

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

we will show $d \geq g$

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.

$\gcd(8, 12) = 4$

1, 2, 4 are common divisors.

all divide 4.

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