Dr. Z.'s Number Theory Lecture 8 Handout: The Euclidean Algorithm

By Doron Zeilberger

The Original Euclidean Algorithm

Input: Two positive integers a and b, with $a > b$.

Output: The positive integer $gcd(a, b)$, their greatest common divisor.

If $b = 0$ then RETURN a, else find the q and r (quotiend and remainder) of dividing a by b:

$$a = qb + r \quad (0 \leq r < b) \quad ,$$

then

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

Keep going until you get $gcd(something, 0)$ and the output is *something*.

Note: The reason that $gcd(a, b) = gcd(b, r)$ is that *any* common divisor of a and b is also a divisor of r (and hence a common divisor of b and r) and vice versa. Hence the **greatest** common divisors are the same.

Problem 8.1: Find $gcd(252, 198)$.

Solution to 8.1:

$252 = 1 \cdot 198 + 54 \quad , \quad$ so $r(252, 190) = 54$ and

$gcd(252, 198) = gcd(198, 54)$;

$198 = 3 \cdot 54 + 36 \quad$ so $r(198, 54) = 36$ and

$gcd(198, 54) = gcd(54, 36)$;

$54 = 1 \cdot 36 + 18, \quad$ so $r(54, 36) = 18$ and

$gcd(54, 36) = gcd(36, 18)$;

$36 = 2 \cdot 18 + 0, \quad$ so $r(36, 18) = 0$ and

$gcd(36, 18) = gcd(18, 0)$.

We are done! $gcd(18, 0) = 18$, so

Ans. to 8.1: $gcd(252, 198) = 18$.

How to find the gcd of several integers

$gcd(a, b, c) = gcd(a, gcd(b, c))$ etc.

Problem 8.2: Find the greatest common divisor of $6, 10, 15$.

Solution to 8.2: $gcd(15, 10) = gcd(10, 5) = gcd(5, 0) = 5$. $gcd(6, 5) = gcd(5, 1) = gcd(1, 0) = 1$.
Ans.: $gcd(15, 10, 6) = 1$.

A **linear combination** of two integers a and b is something of the form $ma + nb$ where m and n are integers. Of course any common divisor, of a and b is also a divisor of any linear combination, in particular $gcd(a, b)$ is a divisor of any linear combination. Thanks to the **Extended Euclidean Algorithm** we know that the greatest common divisor of m and n can be expressed as a linear combination of them.

The Extended Euclidean Algorithm

Input: Two positive integers a and b, with $a > b$

Output: The positive integer $d = gcd(a, b)$, their greatest common divisor. **and** integers m and n such that

$$d = ma + nb \quad .$$

If $b = 0$ then RETURN $d := a$, and $d = 1 \cdot a$.

Else find the q and r (quotiend and remainder) of dividing a by b:

$$a = qb + r \quad (0 \leq r < b) \quad ,$$

then

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

and r can be expressed as a linear combination of a and b as $r = a - qb$. Every time you get a "new" r, express it as a linear combination of the current a and b, and then plug-in the expressions of these current a and b in terms of the original a and b. Keep going until you get $r = 0$ and the penultimate r is the gcd, and you have it as a linear combination of the original a and b.

Problem 8.3: Find $d = gcd(39, 14)$ and find integers m and n such that $d = m \cdot 39 + n \cdot 14$.

Solution to 8.3:

$39 = 2 \cdot 14 + 11$,

so $gcd(39, 14) = gcd(14, 11)$ and $11 = 1 \cdot \mathbf{39} - 2 \cdot \mathbf{14}$

$14 = 1 \cdot 11 + 3$, so

$gcd(14, 11) = gcd(11, 3)$ and $3 = \mathbf{14} - 11 = \mathbf{14} - (\mathbf{39} - 2 \cdot \mathbf{14}) = 3 \cdot \mathbf{14} - \mathbf{39}$;

$11 = 3 \cdot 3 + 2$, so

$gcd(11, 3) = gcd(3, 2)$ and $2 = 11 - 3 \cdot 3 = (\mathbf{39} - 2 \cdot \mathbf{14}) - 3(3 \cdot \mathbf{14} - \mathbf{39}) = 4 \cdot \mathbf{39} - 11 \cdot \mathbf{14}$

$3 = 1 \cdot 2 + 1$, so

$gcd(3, 2) = gcd(2, 1)$ and $1 = 3 - 1 \cdot 2 = (3 \cdot \mathbf{14} - \mathbf{39}) - (4 \cdot \mathbf{39} - 11 \cdot \mathbf{14}) = 14 \cdot \mathbf{14} - 5 \cdot \mathbf{39}$

$2 = 2 \cdot 1 + 0$, so

$gcd(2, 1) = gcd(1, 0) = 1$ and

$$1 = -5 \cdot \mathbf{39} + 14 \cdot \mathbf{14} \quad .$$

Ans. to 8.3: $gcd(29, 14) = 1$ and $1 = -5 \cdot \mathbf{39} + 14 \cdot \mathbf{14}$ (so $m = -5$, $n = 14$).