Lemma 10. If $a = qb + r$, then $\gcd(a, b) = \gcd(b, r)$.

Proof. Let $d \in \mathbb{N}$. We need to show that $d|a$ and $d|b$ iff $d|r$ and $d|b$. [**iff** is short for "if and only if"]

"$\Longrightarrow$" (the "only if" part): $d|r$ because $\frac{r}{d} = \frac{a - qb}{d} = \frac{a}{d} - \frac{qb}{d}$ is an integer (since $d|a$ and $d|b$).

"$\Longleftarrow$" (the "if" part): $d|a$ because $\frac{a}{d} = \frac{qb + r}{d} = \frac{qb}{d} + \frac{r}{d}$ is an integer (since $d|b$ and $d|r$). □

Example 11. Using this lemma to compute gcd's is refered to as the **Euclidean algorithm**.

(a) $\underbrace{\gcd(30, 108)}_{108 = 3 \cdot 30 + 18} = \underbrace{\gcd(18, 30)}_{30 = 1 \cdot 18 + 12} = \underbrace{\gcd(12, 18)}_{18 = 1 \cdot 12 + 6} = \underbrace{\gcd(6, 12)}_{12 = 2 \cdot 6 + 0} = \gcd(0, 6) = 6$

Alternatively, taking a shortcut by allowing negative remainders:

$\underbrace{\gcd(30, 108)}_{108 = 4 \cdot 30 - 12} = \underbrace{\gcd(12, 30)}_{30 = 2 \cdot 12 + 6} = \underbrace{\gcd(6, 12)}_{12 = 2 \cdot 6 + 0} = 6$

(b) $\underbrace{\gcd(16, 25)}_{25 = 1 \cdot 16 + 9} = \underbrace{\gcd(9, 16)}_{16 = 1 \cdot 9 + 7} = \underbrace{\gcd(7, 9)}_{9 = 1 \cdot 7 + 2} = \underbrace{\gcd(2, 7)}_{7 = 3 \cdot 2 + 1} = \gcd(1, 2) = 1$

Alternatively, again, taking a shortcut by allowing negative remainders:

$\underbrace{\gcd(16, 25)}_{25 = 2 \cdot 16 - 7} = \underbrace{\gcd(7, 16)}_{16 = 2 \cdot 7 + 2} = \underbrace{\gcd(2, 7)}_{7 = 3 \cdot 2 + 1} = \gcd(1, 2) = 1$

Theorem 12. (Bézout's identity) Let $a, b \in \mathbb{Z}$ (not both zero). There exist $x, y \in \mathbb{Z}$ such that

$$\gcd(a, b) = ax + by.$$

Proof. We proceed iteratively:

$$\begin{aligned}
a &= q_1 b + r_1, & 0 < r_1 < b \\
b &= q_2 r_1 + r_2, & 0 < r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3, & 0 < r_3 < r_2 \\
&\vdots \\
r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1}, & 0 < r_{n-1} < r_{n-2} \\
r_{n-2} &= q_n r_{n-1} + r_n, & 0 < r_n < r_{n-1} \\
r_{n-1} &= q_{n+1} r_n + 0
\end{aligned}$$

Along the way, we have $\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \ldots = \gcd(r_{n-2}, r_{n-1}) = \gcd(r_{n-1}, r_n) = r_n$ (why is it obvious that the last gcd is r_n?).

By the second-to-last equation, $\gcd(a, b) = r_n = r_{n-2} - q_n r_{n-1}$ is a linear combination of r_{n-2} and r_{n-1}. Then, moving one up, we replace r_{n-1} with $r_{n-3} - q_{n-1} r_{n-2}$ to write $\gcd(a, b)$ as a linear combination of r_{n-3} and r_{n-2}. Continuing in that fashion, we ultimately obtain $\gcd(a, b)$ as a linear combination of a and b. □

Let us revisit the previous example to illustrate how the Euclidean algorithm provides us with a way to write $\gcd(a, b)$ as an integer linear combination of a and b.

Armin Straub
straub@southalabama.edu

Example 13. Find $d = \gcd(30, 108)$ as well as integers r, s such that $d = 38r + 108s$.

Solution. We apply the extended Euclidean algorithm:

$$\begin{array}{lll} \gcd(30,108) & \boxed{108} = 4 \cdot \boxed{30} - 12 & \text{or: } \boxed{A} \quad 12 = -1 \cdot \boxed{108} + 4 \cdot \boxed{30} \\ = \gcd(12,30) & \boxed{30} = 2 \cdot \boxed{12} + 6 & \qquad \boxed{B} \quad 6 = 1 \cdot \boxed{30} - 2 \cdot \boxed{12} \\ = \gcd(6,12) & \boxed{12} = 2 \cdot \boxed{6} + 0 & \\ = 6 & & \end{array}$$

Backtracking through this, we find that **Bézout's identity** takes the form

$$6 \underset{\boxed{B}}{=} 1 \cdot \boxed{30} - 2 \cdot \boxed{12} \underset{\boxed{A}}{=} 1 \cdot \boxed{30} - 2(-1 \cdot \boxed{108} + 4 \cdot \boxed{30}) = 2 \cdot \boxed{108} - 7 \cdot \boxed{30}$$

In summary, we have $2 \cdot 108 - 7 \cdot 30 = 6$.

Example 14. Find $d = \gcd(16, 25)$ as well as integers r, s such that $d = 16r + 25s$.

Solution. We apply the extended Euclidean algorithm:

$$\begin{array}{lll} \gcd(16,25) & \boxed{25} = 2 \cdot \boxed{16} - 7 & \text{or: } \boxed{A} \quad 7 = -1 \cdot \boxed{25} + 2 \cdot \boxed{16} \\ = \gcd(7,16) & \boxed{16} = 2 \cdot \boxed{7} + 2 & \qquad \boxed{B} \quad 2 = 1 \cdot \boxed{16} - 2 \cdot \boxed{7} \\ = \gcd(2,7) & \boxed{7} = 3 \cdot \boxed{2} + 1 & \qquad \boxed{C} \quad 1 = \boxed{7} - 3 \cdot \boxed{2} \\ = 1 & & \end{array}$$

Backtracking through this, we find that **Bézout's identity** takes the form

$$1 \underset{\boxed{C}}{=} \boxed{7} - 3 \cdot \boxed{2} \underset{\boxed{B}}{=} 7 \cdot \boxed{7} - 3 \cdot \boxed{16} \underset{\boxed{A}}{=} -7 \cdot \boxed{25} + 11 \cdot \boxed{16}$$

In summary, we have $-7 \cdot 25 + 11 \cdot 16 = 1$.

Example 15. (extra) Find $d = \gcd(17, 23)$ as well as integers r, s such that $d = 16r + 25s$.

Solution. We apply the extended Euclidean algorithm:

$$\begin{array}{lll} \gcd(17,23) & \boxed{23} = 1 \cdot \boxed{17} + 6 & \text{or: } \boxed{A} \quad 6 = 1 \cdot \boxed{23} - 1 \cdot \boxed{17} \\ = \gcd(6,17) & \boxed{17} = 3 \cdot \boxed{6} - 1 & \qquad \boxed{B} \quad 1 = -1 \cdot \boxed{17} + 3 \cdot \boxed{6} \\ = 1 & & \end{array}$$

Backtracking through this, we find that **Bézout's identity** takes the form

$$1 \underset{\boxed{B}}{=} -1 \cdot \boxed{17} + 3 \cdot \boxed{6} \underset{\boxed{A}}{=} 3 \cdot \boxed{23} - 4 \cdot \boxed{17}$$

In summary, we have $1 = 3 \cdot 23 - 4 \cdot 17$.

2 Diophantine equations

Diophantine equations are usual equations but we are only interested in integer solutions.

Example 16. Find the general solution to the diophantine equation $16x + 25y = 0$.

Solution. The non-diophantine equation $16x + 25y = 0$ has general solution $(x, y) = (25t, -16t)$ where the parameter t is any real number.

We need to figure out for which t this results in a solution where both coordinates $x = 25t$ and $y = -16t$ are integers. Obviously, t needs to be a rational number. Since $\gcd(16, 25) = 1$ the denominator of t must be 1, so that t must be an integer. In other words, the general solution to the diophantine equation $16x + 25y = 0$ is $(x, y) = (25t, -16t)$ where the parameter t is any integer.

Armin Straub
straub@southalabama.edu

Example 17. Find a solution to the diophantine equation $16x + 25y = 1$.

Solution. Since $\gcd(16, 25) = 1$, Bezout's theorem guarantees a solution, which we can find using the generalized Euclidean algorithm. Namely, in Example 14, we found that $-7 \cdot 25 + 11 \cdot 16 = 1$.

In other words, we have found the solution $x = 11$ and $y = -7$.

Are there other solutions? **Yes!** For instance, $x = -14$ and $y = 9$.

What is the **general solution**?

Solution. In the previous example we determined that the general solution to the corresponding **homogeneous (diophantine) equation** $16x + 25y = 0$ is $(x, y) = (25t, -16t)$ where the parameter t is any integer. We can add these solutions to any **particular solution** of $16x + 25y = 1$ to obtain the general solution to $16x + 25y = 1$. Therefore, the general solution is

$$(x, y) = (11, -7) + (25t, -16t) = (11 + 25t, -7 - 16t),$$

where t is any integer.

Comment. Note that choosing $t = -1$ results in $(x, y) = (11 - 25, -7 + 16) = (-14, 9)$, another solution that we observed earlier.

Example 18. Find the general solution to the diophantine equation $6x + 15y = 10$.

Solution. This equation has no (integer) solution because the left-hand side is divisible by $\gcd(6, 15) = 3$ but the right-hand side is not divisible by 3.

Lemma 19. Let $a, b \in \mathbb{Z}$ (not both zero). The diophantine equation $ax + by = c$ has a solution if and only if c is a multiple of $\gcd(a, b)$.

Proof.

"$\Longrightarrow$" (the "only if" part): Let $d = \gcd(a, b)$. Then d divides $ax + by$. This implies that $d|c$.

"$\Longleftarrow$" (the "if" part): This is a consequence of Bezout's identity. $\square$