Proof that the Euclidean Algorithm Works

Recall this definition: When a and b are integers and $a \neq 0$ we say a divides b, and write $a|b$, if b/a is an integer.

1. Use the definition to prove that if a, b, c, x and y are integers and $a|b$ and $a|c$, then $a|(bx+cy)$.

Answer: We are given that the two quotients b/a and c/a are integers. Therefore the integer linear combination $(b/a) \times x + (c/a) \times y = (bx+cy)/a$ is an integer, which means that $a|(bx+cy)$.

2. Use Question 1 to prove that if a is a positive integer and b, q and r are integers with $b = aq + r$, then $\gcd(b,a) = \gcd(a,r)$.

Answer: Write $m = \gcd(b,a)$ and $n = \gcd(a,r)$. Since m divides both b and a, it must also divide $r = b - aq$ by Question 1. This shows that m is a common divisor of a and r, so it must be $\leq n$, their greatest common divisor. Likewise, since n divides both a and r, it must divide $b = aq + r$ by Question 1, so $n \leq m$. Since $m \leq n$ and $n \leq m$, we have $m = n$.

Alternative answer: Let c be a common divisor of b and a. Then by Question 1, c must divide $r = b - aq$. Thus, the set D of common divisors of b and a is a subset of the set E of common divisors of a and r. Now let d be a common divisor of a and r. Then by Question 1, d must divide $b = aq + r$. Thus, the set E of common divisors of a and r is a subset of the set D of common divisors of b and a. Hence $D = E$ and the largest integer in this set is both $\gcd(b,a)$ and $\gcd(a,r)$. Therefore $\gcd(b,a) = \gcd(a,r)$.

Recall the Euclidean algorithm:

Let $r_0 = a$ and $r_1 = b$ be integers with $a > b > 0$. Apply the division algorithm $x = yq + r$, $0 \leq r < y$ iteratively to obtain

$$r_i = r_{i+1}q_{i+1} + r_{i+2} \text{ with } 0 < r_{i+2} < r_{i+1}$$

for $0 \leq i < n - 1$ and $r_{n+1} = 0$.

3. Prove that $\gcd(a, b) = r_n$, the last nonzero remainder. Hint: First show that the algorithm terminates. Then use mathematical induction and Question 2.

Answer: First we show that the algorithm terminates. Since $r_{i+2} < r_{i+1}$, we have $r_0 > r_1 > r_2 > \cdots > r_n > r_{n+1} = 0$. This shows that the remainders are monotonically strictly decreasing positive integers until the last one, which is $r_{n+1} = 0$. Therefore the algorithm stops after no more than b divisions.

We prove by induction the claim that for each i in $0 \leq i \leq n$ we have $\gcd(a, b) = \gcd(r_i, r_{i+1})$.

For the base step $i = 0$, we have $\gcd(a, b) = \gcd(r_0, r_1)$ by definition of $r_0 = a$ and $r_1 = b$.

For each i in $0 \leq i < n$ we have $\gcd(r_i, r_{i+1}) = \gcd(r_{i+1}, r_{i+2})$ by Question 2. This shows that if $\gcd(a, b) = \gcd(r_i, r_{i+1})$, then $\gcd(a, b) = \gcd(r_{i+1}, r_{i+2})$, which is the induction step. This ends the proof of the claim.

Now use the claim with $i = n$: $\gcd(a, b) = \gcd(r_n, r_{n+1})$. But $r_{n+1} = 0$ and r_n is a positive integer by the way the Euclidean algorithm terminates. Every positive integer divides 0. If r_n is a positive integer, then the greatest common divisor of r_n and 0 is r_n. Thus, the Euclidean algorithm correctly computes the greatest common divisor of its input a and b as $\gcd(a, b) = r_n$.