MA 261 — Euclidean Algorithm

1. Use some combination or subset of Theorems 1.1–1.3 and 1.6 to prove the following:

   (a) Theorem 1.32. Let a, n, b, r, and k be integers. If $a = nb + r$ and $k|a$ and $k|b$, then $k|r$.

   Proof. If $k|b$, then by Theorem 1.6, $k|nb$. But $k|a$, so by Theorem 1.2, $k|(a - nb)$. Therefore $k|r$.

   (b) Let a, n, b, r, and k be integers. If $a = nb + r$ and $k|b$ and $k|r$, then $k|a$.

   Proof. If $k|b$, then by Theorem 1.6, $k|nb$. But $k|r$, so by Theorem 1.1, $k|(nb + r)$. Therefore $k|a$.

2. Use the above to prove Theorem 1.33: Let a, b, n_1, and r_1 be integers with a and b not both 0. If $a = n_1 b + r_1$, then $(a, b) = (b, r_1)$.

   Proof. By (1a), if d is a divisor of both a and b, then d is also a divisor of both b and r_1. By (1b), if d is a divisor of both b and r_1, then d is also a divisor of both a and b. Therefore, the pair a, b has exactly the same set of common divisors as the pair b, r_1; therefore, they have the same greatest common divisor.

3. Let a, b, n_1, and r_1 be integers with a and b not both 0. If x, y, and d are integers such that $a = n_1 b + r_1$ and $bx_1 + r_1 y_1 = d$, find formulas for integers x, y such that $ax + by = d$.

   This is a straightforward substitution. Knowing $r_1 = a - n_1 b$, substitute this expression for r_1 into the expression for d:

$$\begin{aligned} d &= bx_1 + r_1 y_1 \\ &= bx_1 + (a - n_1 b) y_1 \\ &= ay_1 + b(x_1 - n_1 y_1) \end{aligned}$$

   So we can take $x = y_1$ and $y = x_1 - n_1 y_1$.