Notes and Worksheet on the Euclidean Algorithm

Given two integers \( a \) and \( b \), not both zero, we can compute the gcd of \( a \) and \( b \) using the Euclidean Algorithm. This Algorithm expresses the gcd in the form \( au + bv \), as predicted by Theorem 1.3 in the text.

Our starting point is Lemma 1.7:

**Lemma 1.7:** Let \( a, b \in \mathbb{Z} \), not both zero. Let \( q, r \in \mathbb{Z} \) be such that

\[
a = bq + r.
\]

Then \((a, b) = (b, r)\).

While Lemma 1.7 works even when \( q \) is not the quotient of the Division Algorithm and \( r \) is not the remainder in the Division Algorithm, that is the way we use it in the Euclidean Algorithm. First, recall that if \( a \neq 0 \), then \((a, 0) = |a|\).

**Problem:** Find the gcd of \( a \) and \( b \) when \( a > b > 0 \). (Note that since \( a \) and \(|a|\) have the same divisors, we see \( \gcd(a, b) = \gcd(|a|, |b|) \), so our assumption is more of a convenience rather than a real restriction.)

**Strategy:** If we use the Division Algorithm, we can find \( q, r \in \mathbb{Z} \) such that \( a = bq + r \) AND \( 0 \leq r < b \). Then, by Lemma 1.7, we have \((a, b) = (b, r)\) where \( b \) and \( r \) are smaller integers than \( a \) and \( b \). So \((b, r)\) should be easier to find than \((a, b)\).

**Improved Strategy:** As above, we see that by using the Division Algorithm, we can reduce the problem of finding \((a, b)\) to the easier problem of finding \((b, r)\) when \( a = bq + r \) and \( 0 \leq r < b \). If \( r = 0 \), we are done. If \( r > 0 \), we can now reduce the problem of finding \((b, r)\) by using the Division Algorithm again. In particular, we know \( b = rq_1 + r_1 \) for some \( q_1, r_1 \in \mathbb{Z} \) such that \( 0 \leq r_1 < r \). Then finding \((b, r)\) is the same as finding the easier \((r, r_1)\) since \( r < b \) and \( r_1 < r \). Now we can repeat this again and again until we get a remainder of zero.

The above improved strategy is the Euclidean Algorithm. Let’s see how this plays out first with a simple example, then with an exercise. We note that the example given could be done in your head, but we are working to develop an algorithm that can be programmed into a calculator or computer, so we are really interested in describing the procedure rather then getting a quick answer.

**Example:** Use the Euclidean Algorithm to find \((15, 24)\) AND express it in the form \( au + bv \).

If we just want to find \((15, 24)\), we note \( 24 = 15 \cdot 1 + 9 \) so \((24, 15) = (15, 9)\).

Now:
\[
15 = 9 \cdot 1 + 6 \Rightarrow (15, 9) = (9, 6).
\]

So:
\[
9 = 6 \cdot 1 + 3 \Rightarrow (9, 6) = (6, 3).
\]

Now:
\[
6 = 3 \cdot 2 + 0 \Rightarrow (6, 3) = (3, 0) = 3.
\]

Therefore, \((24, 15) = 3\).

The above computation does not express 3 in the form \( 24u + 15v \). To do this, we modify the above computation a bit. Let us consider the equations

\[
\begin{align*}
\text{Eqn 1:} & \quad x = 24 \\
\text{Eqn 2:} & \quad y = 15.
\end{align*}
\]

Now we have
\[
9 = 24 \cdot 1 + 15 \cdot (-1) = x - y \Rightarrow \text{Eqn 3:} \quad x - y = 9.
\]

Next:
\[
6 = 15 \cdot 1 + 9 \cdot (-1) = y - (x - y) = -x + 2y \Rightarrow \text{Eqn 4:} \quad -x + 2y = 6.
\]
Now, finally we have

\[ 3 = 9 \cdot 1 + 6 \cdot (-1) = (x - y) - (-x + 2y) = 2x - 3y. \]

So \( 24 \cdot 2 + 15 \cdot (-3) = 3 \) is the answer we are looking for.

As in linear algebra, carrying along these sets of equations gets repetitive, so we can reduce these equations to augmented matrices. Once we do this, we can then use row operations to keep track of our computations. So, in our above example, we have

\[
\begin{bmatrix}
1 & 0 & 24 \\
0 & 1 & 15
\end{bmatrix}
\xrightarrow{\text{Row 1 - Row 2}}
\begin{bmatrix}
0 & 1 & 15 \\
1 & -1 & 9
\end{bmatrix}
\xrightarrow{\text{Row 1 - Row 2}}
\begin{bmatrix}
1 & -1 & 9 \\
-1 & 2 & 6
\end{bmatrix}
\]

So \( 24(2) + 15(-3) = 3 \).

Exercise: Use the Euclidean Algorithm to find \((1071, 374)\) AND express it in the form \( au + bv \).
(Optional: Can you create a spreadsheet or program to do this?)