The Euclidean Algorithm
for Janet Vassilev's Math 327 course

Definition 0.1 *A positive integer d is the* **greatest common divisor** *of two nonzero integers n and m if*

- *d divides n and d divides m and*
- *for any c which divides both n and m then c divides d.*

The Euclidean Algorithm allows us to express the greatest common divisor of two nonzero integers n and m as an integral sum of n and m.

Theorem 0.2 Euclidean Algorithm *Let n and m be nonzero integer and d the greatest common divisor of n and m. There exists integers s and t such that $d = sn + tm$.*

Proof: Let $A = \{ns + mt \mid s, t \in \mathbb{Z}\}$. Since n, m, s and t are all integers $ns + mt$ is an integer. Suppose $d = ns + mt$ is the smallest positive integer contained in A. We claim that d is the greatest common divisor.

Suppose first that d is not a divisor of both n and m. In particular, d doesn't divide n. Then there exists unique q and r such that $n = qd + r$ with $0 < r < d$. Note that both $n = qd + r$ and $qd = nqs + mqt$ are in A. So $r = n - qd$ is in A but $r < d$ contradicts that d is the smallest positive integer in A. Similarly we can see that d must also divide m. So d must divide both n and m.

Suppose c is a divisor of both n and m. Then there exists a and b integers such that $ca = n = cb$. So $d = cas + cbt = c(as + bt)$ so c divides d. Since d satisfies the properties of a greatest common divisor, then d is the greatest common divisor of n and m and $d = ns + mt$.

The s and t in the Euclidean Algorithm are not unique. For example, 3 is the greatest common divisor of 9 and 15 but we can express 3 as different integral sums of 9 and 15. Two examples follow: $3 = 2 \cdot 9 + (-1) \cdot 15 = (-3) \cdot 9 + 2 \cdot 15$.

One way to find how to express the greatest common multiple of n and m as an integral sum of n and m is to repeatedly use the Division Algorithm and then use back substitution.

$$n = mq + r \text{ with } 0 \leq r < n$$

$$m = rq_1 + r_1 \text{ with } 0 \leq r_1 < r$$

$$r = r_1 q_2 + r_2 \text{ with } 0 \leq r_2 < r_1$$

$$\vdots$$

$$r_{n-1} = r_n q_{n+1} + r_{n+1} \text{ with } 0 \leq r_{n+1} < r_n$$

$$r_n = r_{n+1} q_{n+2}$$

Since r_{n+1} divides r_n, then it will divide $r_{n-1}, r_{n-2}, \cdots r_1, r, m$ and n by substituting back into the above equalities.

We can solve $r_{n+1} = r_{n-1} - r_n q_{n+1} = r_{n-1} - (r_{n-2} - r_{n-1} q_n) q_{n+1} = \cdots = sn + tm$.

For example,

Example 0.3 *Write the greatest common divisor of 48 and 27 as an integral multiple of 48 and 27.*

$$48 = 1 \cdot 27 + 21$$

$$27 = 1 \cdot 21 + 6$$

$$21 = 3 \cdot 6 + 3$$

$$6 = 2 \cdot 3$$

Now working backwards:

$$3 = 21 - 3 \cdot 6 = 21 - 3(27 - 21) = 4 \cdot 21 - 3 \cdot 27 = 4(48 - 27) - 3 \cdot 27 = 4 \cdot 48 - 7 \cdot 27$$

Another way to find the greatest common divisor of two numbers n and m as an integral multiple of the two is keep track of the multiple as you go. For example make a table where the left hand column keeps track of the successive ”remainders” and the second column keeps track of the multiple n and the second keeps track of the multiple of m. The first row will be $n, 1, 0$ and the second row will be $m, 0, 1$. To obtain the third and successive rows you subtract the appropriate q_i multiple of the row directly above the row you are computing from two rows above the one you are trying to compute. We will illustrate this for the example above.

	multiple of 48	multiple of 27
48	1	0
27	0	1
21	1	-1
6	-1	2
3	4	-3

You are less likely to make arithmetic or sign errors if you use this tabular approach.

For example, if we want to express the greatest common divisor of 144 and 100, first use our successive division algorithm to find the quotients and remainders:

$$144 = 1 \cdot 100 + 44$$

$$100 = 2 \cdot 44 + 12$$

$$44 = 3 \cdot 12 + 8$$

$$12 = 1 \cdot 8 + 4$$

$$8 = 2 \cdot 4$$

	multiple of 144	multiple of 100
144	1	0
100	0	1
44	1	-1
12	-2	3
8	7	-10
4	-9	13

So $4 = -9 \cdot 144 + 13 \cdot 100$.

Since you know that two relatively prime integers have greatest common divisor 1, one can use the Euclidean Algorithm to express 1 as an integral multiple of the two integers. This is particularly useful in proofs.

For example if you want to show the statement, " For relatively prime integers a and b, if a divides bc then a divides c."

We can write $1 = sa + tb$ for some integers s and t. Multiply both sides by c and we obtain $c = sac + tbc$. Now since a divides bc there is an integer r such that $ra = bc$. Replacing bc by ra in the previous equality we see that $c = sac + tra = a(sc + tr)$, showing that a divides c.