1 Divisors and Greatest Common Divisor

Recall for integers n, q, d, d divides n means $n = qd$ (i.e., the remainder is 0) and that d is a divisor of n.

Example: Does d divide n (is d a divisor of n) for the following?

(a) $n = 56$, $d = 7$

(b) $n = 56$, $d = -14$

(c) $n = -157$, $d = 6$

(d) $n = 0$, $d = 359$

Example: List all divisors of 30.

Example: List the common divisors of 30 and 48.

Definition:

Given integers m and n, not both zero, the ________________________ of n and m is the largest integer that divides both m and n (i.e., the largest divisor of m and n), denoted ____________.

Note: for $m \neq 0$, $\gcd(m, 0) = |m|$.

Example: What is the greatest common divisor of 30 and 48?

Theorem 3.3:

Let a, b, c, q be integers with $b > 0$. If $a = qb + c$, then $\gcd(a, b) = \gcd(b, c)$.

Why is this helpful?

2 Euclidean Algorithm and Extended Euclidean Algorithm

(This one really is an algorithm.)

Euclidean Algorithm:

Given nonnegative integers m and n that are not both 0, this algorithm computes $\gcd(m, n)$.

Step 1 (initialization): Set $r_{-1} = m$, $r_0 = n$, $i = 0$.

Step 2 (apply division algorithm): while $r_i \neq 0$

(a) Replace i with $i + 1$.

(b) Determine the quotient q_i and remainder r_i in the division of r_{i-2} by r_{i-1}.

endwhile

Step 3 (output greatest common divisor): Print r_{i-1}.

Translation: Use the division algorithm with m as your first dividend (number to go into) and n as your first divisor. Then use the division algorithm with n as your dividend and the first remainder as the divisor. Repeat this process until you obtain a remainder of 0. The last remainder before you get 0 is the greatest common divisor (gcd).

Example: Find the greatest common divisor of m and n for the following, using the Euclidean Algorithm:

(a) $m = 357$, $n = 249$

(b) $m = 870$, $n = 465$

(c) $m = 949$, $n = 657$

(d) $m = 949$, $n = 462$

(e) $m = 60$, $n = 132$

Extended Euclidean Algorithm:

Given nonnegative integers m and n that are not both 0, this algorithm computes $\gcd(m, n)$ and integers x, y such that $mx + ny = \gcd(m, n)$.

Step 1 (initialization): Set $r_{-1} = m$, $x_{-1} = 1$, $y_{-1} = 0$, $r_0 = n$, $x_0 = 0$, $y_0 = 1$, $i = 0$.

Step 2 (apply division algorithm): while $r_i \neq 0$

(a) Replace i with $i + 1$.

(b) Determine the quotient q_i and remainder r_i in the division of r_{i-2} by r_{i-1}.

(c) Set $x_i = x_{i-2} - q_i x_{i-1}$ and $y_i = y_{i-2} - q_i y_{i-1}$.

endwhile

Step 3 (output $\gcd(m, n)$, x, and y): Print $r_{i-1}, x_{i-1}, y_{i-1}$.

Translation/alterative: Use the Euclidean Algorithm to find the gcd. Rearrange the equation with the gcd so the other values = gcd. Substitute the prior equation in the Euclidean Algorithm for the prior remainder. Rearrange so that you have a sum/difference of the prior values. Repeat this process till you reach a sum/difference of the original m and n = gcd.

Example: Find integers x and y such that $949x + 462y$ =gcd(949,462) using the Extended Euclidean Algorithm.

Example: Find, if possible, integers x and y such that $949x + 462y = 25$.

Example: Find the greatest common divisor of $m = 315$ and $n = 225$ and integers x and y such that $315x + 225y$ =gcd(315, 225) using the Extended Euclidean Algorithm.

Example: Find, if possible, integers x and y such that $315x + 225y = 990$.

Example: Find, if possible, integers x and y such that $315x + 225y = 690$.

Rachel Rupnow. Compiled: February 7, 2023