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) $n = 56$, $d = 7$ yes: $56 = 8(7) + 0$

(b) $n = 56$, $d = -14$ yes: $56 = -4(-14) + 0$

(c) $n = -157$, $d = 6$ no : $-157 = -27(6) + 5$ $\neq 0$ remainder is $5 \neq 0$

(d) $n = 0$, $d = 359$ yes: $0 = 0(359) + 0$

Example: List all divisors of 30.

$\pm 1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 10, \pm 15, \pm 30$

Example: List the common divisors of 30 and 48.

divisors of 48: $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 12, \pm 16, \pm 24, \pm 48$

common divisors of 30 & 48: $\pm 1, \pm 2, \pm 3, \pm 6$

Definition:

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

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

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

6

Theorem 3.3:

division algorithm

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?

This allows us to find the gcd of 2 numbers by finding the gcd of progressively smaller numbers. Because m & -m have the same divisors we can assume m, n are nonnegative (i.e. gcd(m,n) = gcd(|m|, |n|) & eventually this process will terminate in a 0 remainder — we have a decreasing sequence of nonnegative values.

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

work to show

$357 = 1(\underline{249}) + \underline{108}$ $\quad 0 \leq 108 < 249$

$249 = 2(108) + 33$ $\quad (2 \times 108 = 216,\ 249 - 216 = 33)$

$108 = 3(33) + 9$

$33 = 3(9) + 6$

$9 = 1(6) + 3$

$6 = 2(3) + 0$

$\gcd(357, 249) = \gcd(249, 108) = \gcd(108, 33) = \gcd(33, 9) = \gcd(9, 6) = \gcd(6, 3) = 3$

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

$870 = 1(465) + 405$

$465 = 1(405) + 60$

$405 = 6(60) + 45$

$60 = 1(45) + 15$

$45 = 3(15) + 0$

$\gcd(870, 465) = 15$

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

$949 = 1(657) + 292$
$657 = 2(292) + 73 \leftarrow$
$292 = 4(73) + 0$

$\gcd(949, 657) = 73$

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

$949 = 2(462) + 25$
$462 = 18(25) + 12$
$25 = 2(12) + 1 \leftarrow$
$12 = 12(1) + 0$

$\gcd(949, 462) = 1$
(means 949 & 462 are relatively prime

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

$60 = 0(132) + 60$
$132 = 2(60) + 12 \leftarrow$ $\gcd(60, 132) = 12$
$60 = 5(12) + 0$

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.

$462y = 1 - 949x \Rightarrow y = -\frac{949}{462}x + \frac{1}{462}$

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

$m = 949,\ n = 462$

$949 = 2(462) + 25 \longrightarrow 949 - 2(462) = 25$

$462 = 18(25) + 12 \longrightarrow 462 - 18(25) = 12$

$25 = 2(12) + 1 \longrightarrow 25 - 2(12) = 1$

$12 = 12(1) + 0$

$\boxed{\text{Thus } x = 37,\ y = -76}$

$25 - 2(12) = 1$

$\Rightarrow 25 - 2(462 - 18(25)) = 1$

$\Rightarrow 1(25) - 2(462) + 36(25) = 1$

$\Rightarrow -2(462) + 37(25) = 1$

$\Rightarrow -2(462) + 37(949 - 2(462)) = 1$

$\Rightarrow -2(462) + 37(949) - 74(462) = 1$

$\Rightarrow -76(462) + 37(949) = 1$

$\Rightarrow 462(-76) + 949(37) = 1$

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

$25\big(949(37) + 462(-76)\big) = 1(25)$ (multiply both sides by 25)

$949(25 \cdot 37) + 462(-76 \cdot 25) = 25$

$949(\underbrace{925}_{x}) + 462(\underbrace{-1900}_{y}) = 25$

in this case $949 - 2(462) = 25$
so $1 = x$, $y = -2$ another solution

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.

$315 = 1(225) + 90 \longrightarrow 315 - 1(225) = 90$

$225 = 2(90) + 45 \longrightarrow 225 - 2(90) = 45$

$90 = 2(45) + 0$

$225 - 2(90) = 45$

$\Rightarrow 225 - 2(315 - 1(225)) = 45$

$\Rightarrow 225 - 2(315) + 2(225) = 45$

$\Rightarrow \underbrace{-2}_{x}(315) + \underbrace{3}_{y}(225) = 45$

$\boxed{x = -2 \quad y = 3}$

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

$990/45 = 22$

$315(-2) + 225(3) = 45$

$22\big(315(-2) + 225(3)\big) = 22(45)$

$315(-44) + 225(66) = 990$ $\boxed{x = -44 \quad y = 66}$

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

$690/45$ not an integer solution

$45a = 690$ has no a where a is an integer

$\Rightarrow$ no such x, y exists