The Euclidean Algorithm and Diophantine Equations

Math 149
Burger
California State University, Fresno

Greatest Common Divisor

d is the **greatest common divisor** of integers a and b if d is the largest integer which is a common divisor of both a and b.

Notation: $d = \gcd(a, b)$

Example: ±2, ±7, and ±14 are the only integers that are common divisors of both 42 and 56. Since 14 is the largest, $\gcd(42, 56) = 14$.

Use of the gcd

Reducing fractions

Ex. $$\frac{42}{56} = \frac{14 \cdot 3}{14 \cdot 4} = \frac{3}{4}$$

However: not all fractions are easily reduced!

Ex. $$\frac{8051}{8633}$$

The Division Algorithm

(proof on p. 99)

For integers a and b, with $a > 0$, there exist integers q and r such that

$$b = qa + r \quad \text{and} \quad 0 \leq r < a.$$

Euclidean Algorithm

(p. 102)

To find gcd(a, b) where $b < a$:

Divide b into a and let r_1 be the remainder.
Divide r_1 into b and let r_2 be the remainder.
Divide r_2 into r_1 and let r_3 be the remainder.

Continue to divide the remainder into the divisor until you get a remainder of zero.

gcd(a, b) $=$ the last nonzero remainder.

Ex) Find gcd(8633, 8051)

$$\begin{array}{r} 1\ R.582 \\ 8051\overline{)8633} \end{array} \quad \begin{array}{r} 13\ R.485 \\ 582\overline{)8051} \end{array} \quad \begin{array}{r} 1\ R.97 \\ 485\overline{)582} \end{array} \quad \begin{array}{r} 5\ R.0 \\ 97\overline{)485} \end{array}$$

gcd = last nonzero remainder

$$\frac{8051}{8633} = \frac{97 \cdot 83}{97 \cdot 89} = \frac{83}{89}$$

Theorem

(3.2.2, p.105)

For any nonzero integers a and b, there exist integers x and y such that

$$\gcd(a, b) = ax + by.$$

Here's how you use the Euclidean Algorithm to write gcd(8633, 8051) as a linear combination of 8633 and 8051.

- Use the Euclidean Algorithm to find gcd(8633, 8051).

$$8051 \overline{)8633} \quad 1 \ R.582$$

$$582 \overline{)8051} \quad 13 \ R.485$$

$$485 \overline{)582} \quad 1 \ R.97$$

$$97 \overline{)485} \quad 5 \ R.0$$

- Solve each division problem, except the last one, for the remainder ($r = a - bq$) . Take note of the quotient in each solution.

$$8051\overline{)8633}\ \ 1\ R.582 \Rightarrow 582 = 8633 - 1 \cdot 8051$$

$$582\overline{)8051}\ \ 13\ R.485 \Rightarrow 485 = 8051 - 13 \cdot 582$$

$$485\overline{)582}\ \ 1\ R.97 \Rightarrow 97 = 582 - 1 \cdot 485$$

$$97\overline{)485}\ \ 5\ R.0$$

- Use these equations in reverse order to find the linear combination.

1: $582 = 8633 - 1 \cdot 8051$

2: $485 = 8051 - 13 \cdot 582$

3: $97 = 582 - 1 \cdot 485$

$$
\begin{aligned}
97 &= 582 - 1 \cdot 485 && \text{Eq. 3} \\
&= 582 - 1 \cdot (8051 - 13 \cdot 582) && \text{Eq. 2} \\
&= 14 \cdot 582 - 1 \cdot 8051 && \text{Simp.} \\
&= 14 \cdot (8633 - 1 \cdot 8051) - 1 \cdot 8051 && \text{Eq. 1} \\
&= 14 \cdot 8633 + (-15) \cdot 8051 && \text{Simp.}
\end{aligned}
$$

Ex) Now use the Euclidean Algorithm to write gcd(486, 434) as a linear combination of 486 and 434.

A *Diophantine* equation is any equation for which you are interested only in the integer solutions to the equation.

A ***linear Diophantine equation*** is a linear equation $ax + by = c$ with integer coefficients for which you are interested only in finding integer solutions.

Theorem 1

For any nonzero integers a and b, there exist integers x^* and y^* such that

$$\gcd(a,b) = ax^* + by^*.$$

(Proof for Math 133!)

When you have a linear Diophantine equation to solve, the first question you should ask about that Diophantine equation is whether or not the equation admits solutions in integers.

The following theorem tells you how to find the answer to this question.

Theorem 3

If gcd(a,b) $\nmid$ c, then the linear Diophantine equation $ax + by = c$ has no solution.

Proof: Let $d = \gcd(a,b)$. Then there are integers r and s such that $dr = a$ and $ds = b$.

By way of contradiction, assume that $ax + by = c$ does have a solution x_o, y_o.

Then $c = ax_o + by_o = drx_o + dsy_o$.

But this says that $d|c$ since $c = d(rx_o + sy_o)$.

Since this is a contradiction, the Diophantine equation has no solution.

Theorem 4

If gcd(a,b) $|$ c, then the linear Diophantine equation $ax + by = c$ has a solution.

Proof: Let $d = \gcd(a,b)$. Since $d|c$, $dp = c$ for some integer p.

By Theorem 1, there are integers x^* and y^* such that $d = ax^* + by^*$.

So $c = dp = a(x^*p) + b(y^*p)$.

Hence $ax + by = c$ has a solution, namely $x_o = x^*p$ and $y_o = y^*p$.

Q. If a linear Diophantine equation $ax + by = c$ does admit a solution (since $\gcd(a,b) \mid c$), then how do you find it?

Using Division and Euclidean Algorithms to Solve Diophantine Equations

To solve $ax + by = c$:

1. Use the Division Algorithm to find d=gcd(a,b).
2. Use the Euclidean Algorithm to find x^* and y^* such that $d = ax^* + by^*$.
3. Find p such that $c = dp$. (p exists since $d \mid c$.)
4. Then $x_o = x^*p$ and $y_o = y^*p$ are solutions since $c = dp = a(x^*p) + b(y^*p)$.

Find a solution to the Diophantine equation

$$172x + 20y = 1000.$$

- Use the Division Algorithm to find $d = \gcd(172, 20)$.

$$\begin{array}{r} 8\ R.\ 12 \\ 20\overline{)172} \end{array} \quad \begin{array}{r} 1\ R.\ 8 \\ 12\overline{)20} \end{array} \quad \begin{array}{r} 1\ R.\ 4 \\ 8\overline{)12} \end{array} \quad \begin{array}{r} 2\ R.\ 0 \\ 4\overline{)8} \end{array}$$

gcd = last nonzero remainder

- Use the Euclidean Algorithm to find *x** and *y** such that $d = ax^* + by^*$.

Solve for the remainder.

$$\begin{array}{r} 8 \ \textit{R.}\, 12 \\ 20\overline{)172} \end{array} \Rightarrow 12 = 172 - 1 \cdot 20 \quad \textit{Eq.}1$$

$$\begin{array}{r} 1 \ \textit{R.}\, 8 \\ 12\overline{)20} \end{array} \Rightarrow 8 = 20 - 1 \cdot 12 \quad \textit{Eq.}2$$

$$\begin{array}{r} 1 \ \textit{R.}\, 4 \\ 8\overline{)12} \end{array} \Rightarrow 4 = 12 - 1 \cdot 8 \quad \textit{Eq.}3$$

Using these equations we get:

$$12 = 172 - 1 \cdot 20 \quad Eq.1$$

$$8 = 20 - 1 \cdot 12 \quad Eq.2$$

$$4 = 12 - 1 \cdot 8 \quad Eq.3$$

$$4 = 12 - 1 \cdot 8 \quad Eq.3$$

$$4 = 12 - 1 \cdot (20 - 1 \cdot 12) \quad Eq.2$$

$$4 = 2 \cdot 12 - 1 \cdot 20 \quad Simp.$$

$$4 = 2 \cdot (172 - 8 \cdot 20) - 1 \cdot 20 \quad Eq.1$$

$$4 = 2 \cdot 172 + (-17) \cdot 20 \quad Simp.$$

So $x^* = 2$ and $y^* = -17$

Solve $172x + 20y = 1000$

$$4 = 2 \cdot 172 + (-17) \cdot 20$$

- Find p such that $c = dp$.

$$d = \gcd(172, 20) = 4$$
$$c = 1000$$

so $1000 = 4 \cdot 250$.

Solve $172x + 20y = 1000$

$$4 = 2 \cdot 172 + (-17) \cdot 20$$

- Then $x_o = x^*p$ and $y_o = y^*p$ are particular solutions since $c = dp = a(x^*p) + b(y^*p)$.

$$1000 = 4 \cdot 250 = [2 \cdot 172 + (-17) \cdot 20] \cdot 250$$

$$1000 = 172 \cdot (500) + 20 \cdot (-\ 4250)$$

So a ‘particular’ solution is

$x_o = 500$ and $y = -\ 4250$.

Theorem 4

If the linear Diophantine equation $ax + by = c$ does have a solution, then all such solutions are given by

$$x = x_o + (b/d)t \quad \text{and} \quad y = y_o - (a/d)t$$

where $d = \gcd(a,b)$, x_o, y_o is a particular solution to the equation and t ranges over the integers.

Solve $172x + 20y = 1000$

- Then all solutions are $x = x_o + (b/d)t$ and $y = y_o - (a/d)t$ where t is an integer.

From the equation $172x + 20y = 1000$, we see that $a = 172$ and $b = 20$.

From our previous work, $x_o = 500$, $y_o = -4250$, and $d = 4$.

So the solutions, in integers, are

$$x = 500 + 5t \quad \text{and} \quad y = -4250 - 43t$$

where t ranges over the integers.

Example
Find all *positive* solutions to the Diophantine equation $172x + 20y = 1000$.

we need to find those values of t for which

$x = 500 + 5t > 0$ and $y = - 4250 - 43t > 0$.

Find all *positive* integer solutions to the equation

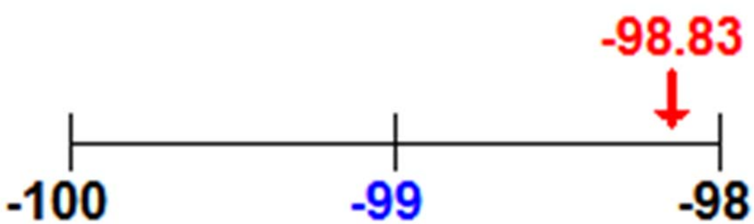
$$172x + 20y = 1000.$$

All solutions are $x = 500 + 5t$ and $y = -4250 - 43t$.

$$x = 500 + 5t > 0 \Rightarrow t > -100.$$

$$y = -4250 - 43t > 0 \Rightarrow t < -98.83\ldots$$

Since t must be an integer, $t \le -99$.



So $-100 < t \le -99$.

Find all *positive* integer solutions to the equation

$$172x + 20y = 1000.$$

All solutions are $x = 500 + 5t$ and $y = -4250 - 43t$.

We just found that $-100 < t \leq -99$.

Since t must be an integer,

$-100 < t \leq -99 \Rightarrow t = -99$. So there is only one positive solution to the Diophantine equation, namely

$$x = 500 + 5t = \cdots = 5 \text{ and}$$

$$y = -4250 - 43t = \cdots = 7.$$