Dr Oliver Mathematics
Greatest Common Divisor

Clearly, we could find the *greatest common divisor* (or *highest common factor*) by simply doing the prime factorisation of the numbers but there is a faster way to do this.

1 Definitions

If a, $b \in \mathbb{Z}$, then c is a *common divisor* of a and b if $c|a$ and $c|b$.

Since the set of common divisors is finite (why?) and is bounded above (why?), there exists a *greatest common divisor*; the greatest common divisor of a and b is denoted by $\text{GCD}(a, b)$.

If $\text{GCD}(a, b) = 1$, then a and b called *coprime* or *relatively prime*.

2 Some theorems

Theorem 1
If a, $b \in \mathbb{Z}$ such that $a = bq + r$, then $\text{GCD}(a, b) = \text{GCD}(b, r)$.

Proof. Let $c = \text{GCD}(a, b)$ and $d = \text{GCD}(b, r)$. Now,

$$\begin{aligned} c|a \text{ and } c|b &\Rightarrow c|(a - bq) \\ &\Rightarrow c|r \text{ (which means } c|b \text{ and } c|r) \\ &\Rightarrow c \leqslant d \end{aligned}$$

and

$$\begin{aligned} d|b \text{ and } d|r &\Rightarrow d|(bq + r) \\ &\Rightarrow d|a \text{ (which means } d|a \text{ and } d|b) \\ &\Rightarrow d \leqslant c. \end{aligned}$$

Finally, $c = d$ and

$$\text{GCD}(a, b) = \text{GCD}(b, r). \quad \blacksquare$$

Theorem 2
If $c = \text{GCD}(a, b)$, then there exist x, $y \in \mathbb{Z}$ such that

$$ax + by = c.$$

3 Examples

Example 1
Let

$$a = \text{GCD}(240, 84).$$

Find the value of a.

Solution

How many times does 84 goes into 240?
2.
So

$$240 = 84 \times 2 + 72.$$

How many times does 72 goes into 84?
1.
So

$$84 = 72 \times 1 + 12.$$

How many times does 12 goes into 72?
6 – and there is no remainder.
So

$$72 = 12 \times 6 + 0.$$

Hence,

$$\text{GCD}(240, 84) = \underline{\underline{12}}.$$

Example 2
Find x, $y \in \mathbb{Z}$ such that

$$240x + 84y = 12.$$

Solution

We work backwards:

$$\begin{aligned} 12 &= 84 - 72 \\ &= 84 - (240 - 84 \times 2) \\ &= \underline{\underline{240 \times (-1) + 84 \times 3}}; \end{aligned}$$

thus,

$$\underline{\underline{x = -1 \text{ and } y = 3}}.$$

Example 3

(a) Let

$$b = \text{GCD}(1\,960, 1\,320, 500).$$

Find the value of b.

Solution

How do we do this? We will take the first two numbers and find $b = \text{GCD}(1\,960, 1\,320)$.
How many times does 1 320 goes into 1 960?
1.
So

$$1\,960 = 1\,320 \times 2 + 640.$$

How many times does 640 goes into 1 320?
2.
So

$$1\,320 = 640 \times 2 + 40.$$

How many times does 40 goes into 640?
16 – and there is no remainder.
So

$$640 = 40 \times 16 + 0.$$

Hence,

$$\text{GCD}(1\,960, 1\,320) = 40.$$

Now, we take 40 and apply the same to $b = \text{GCD}(500, 40)$.
How many times does 40 goes into 500?
12.
So

$$500 = 40 \times 12 + 20.$$

How many times does 20 goes into 40?
2 – and there is no remainder.
So

$$40 = 20 \times 2 + 0.$$

Hence,

$$\text{GCD}(1\,960, 1\,320, 500) = \underline{\underline{20}}.$$

(b) Find x, y, and $y \in \mathbb{Z}$ such that

$$1\,960x + 1\,320y + 500z = b.$$

Solution

$$\begin{aligned}20 &= 500 - 40 \times 12 \\ &= 500 - 12(1\,320 - 640 \times 2) \\ &= 500 - 1\,320 \times 12 + 640 \times 24 \\ &= 500 - 1\,320 \times 12 + 24(1\,960 - 1\,320) \\ &= \underline{\underline{1\,960 \times 24 + 1\,320 \times (-36) + 500}};\end{aligned}$$

thus,

$$\underline{\underline{x = 24, y = -36, \text{ and } z = 1}}.$$

And, of course, we can keep on going with four (I think it is best to divide the two numbers and work out their greatest common divisor, the last two numbers and work out *their* greatest common divisor, and then work out the greatest common divisor of the pair), five, et cetera.

The diophantine equation equation

$$ax + by = c, \text{ GCD}(a, b) = 1,$$

has infinitely many solutions. If

$$(x_0, y_0)$$

is one solution, then *all* solutions are of the form

$$(x_0 + na, y_0 - na)$$

for all $n \in \mathbb{Z}$.

Example 4
Solve completely the diophantine equation

$$119x + 19y = 8.$$

Solution

How many times does 19 goes into 119?
6.
So

$$119 = 19 \times 6 + 5.$$

How many times does 5 goes into 19?
3.
So
$$19 = 5 \times 3 + 4.$$
How many times does 4 goes into 5?
1.
So
$$5 = 4 \times 1 + 1.$$
Hence
$$\text{GCD}(119, 19) = 1.$$
Now,
$$\begin{aligned} 1 &= 5 - 4 \\ &= 5 - (19 - 5 \times 3) \\ &= 5 \times 4 - 19 \\ &= 4(119 - 19 \times 6) - 19 \\ &= 119 \times 4 - 19 \times 25 \end{aligned}$$
which means
$$8 = 119 \times 32 + 19 \times (-200).$$
Next,
$$(x, y) = (32, -200)$$
is a solution set which means the general solution set is
$$\underline{\underline{\{(32 + 19n, -200 - 119n) : n \in \mathbb{Z}\}}}.$$

4 Problems

Here are some examples for you to try.

1. (a) Let
$$a = \text{GCD}(851, 1\,147).$$
Find the a.

Solution

How many times does 851 goes into 1 147?
1.
So

$$1\,147 = 851 \times 1 + 296.$$

How many times does 296 goes into 851?
2.
So

$$851 = 296 \times 2 + 259.$$

How many times does 296 goes into 259?
1.
So

$$296 = 259 \times 1 + 37.$$

How many times does 259 goes into 37?
7 – and there is no remainder.
So

$$259 = 37 \times 7 + 0.$$

Finally,

$$\text{GCD}(851, 1\,147) = \underline{\underline{37}}.$$

(Of course, we could also the fact use 296 goes into 851 *almost* three times:
How many times does 851 goes into 1 147?
1.
So

$$1\,147 = 851 \times 1 + 296.$$

How many times does 296 goes into 851?
3.
So

$$851 = 296 \times 3 - 37.$$

How many times does 37 goes into 296?
8 – and there is no remainder.
So

$$296 = 37 \times 8 + 0$$

and so on.)

(b) Find x, $y \in \mathbb{Z}$ such that

$$1\,147x + 851y = a.$$

Solution

$$
\begin{aligned}
37 &= 296 - 259 \\
&= 296 - (851 - 296 \times 2) \\
&= 296 \times 3 - 851 \\
&= 3(1\,147 - 851) - 851 \\
&= \underline{\underline{1\,147 \times 3 + 851 \times (-4)}};
\end{aligned}
$$

thus,

$$\underline{\underline{x = 3 \text{ and } y = -4}}.$$

2. (a) Let

$$h = \text{GCD}(1\,717, 1\,190).$$

Find the h.

Solution

$$
\begin{aligned}
1\,717 &= 1\,190 \times 1 + 527, \\
1\,190 &= 527 \times 2 + 136, \\
527 &= 136 \times 3 + 119, \\
136 &= 119 \times 1 + 17, \\
119 &= 17 \times 7 + 0,
\end{aligned}
$$

and hence

$$\text{GCD}(1\,717, 1\,190) = \underline{\underline{17}}.$$

(b) Find x, $y \in \mathbb{Z}$ such that

$$1\,717x + 1\,190y = h.$$

Solution

$$
\begin{aligned}
17 &= 136 - 119 \\
&= 136 - (527 - 136 \times 3) \\
&= 136 \times 4 - 527 \\
&= 4(1\,190 - 527 \times 2) - 527 \\
&= 1\,190 \times 4 - 527 \times 9 \\
&= 1\,190 \times 4 - 9(1\,717 - 1\,190) \\
&= \underline{\underline{1\,717 \times (-9) + 1\,190 \times 13}},
\end{aligned}
$$

thus,

$$\underline{\underline{x = -9 \text{ and } y = 13}}.$$

3. Let

$$d = \text{GCD}(5\,925, 1\,095,\ 426).$$

Find x, y, and $z \in \mathbb{Z}$ such that

$$1\,219x + 1\,000y + 901z = d.$$

Solution

We will take the first two numbers and find GCD(5 925, 1 095).

$$
\begin{aligned}
5\,925 &= 1\,095 \times 5 + 450, \\
1\,095 &= 450 \times 2 + 195, \\
450 &= 195 \times 2 + 60, \\
195 &= 60 \times 3 + 15, \\
60 &= 15 \times 4 + 0,
\end{aligned}
$$

hence

$$\text{GCD}(5\,925, 1\,095) = 15.$$

Now, we want to calculate GCD(426, 15):

$$
\begin{aligned}
426 &= 15 \times 28 + 6, \\
15 &= 6 \times 2 + 3, \\
6 &= 3 \times 2 + 0,
\end{aligned}
$$

hence

$$\text{GCD}(426, 15) = 3.$$

Finally,

$$\begin{aligned}
3 &= 15 - 6 \times 2 \\
&= 15 - 2(426 - 15 \times 28) \\
&= 15 \times 57 - 426 \times 2 \\
&= 57(195 - 60 \times 3) - 426 \times 2 \\
&= 195 \times 57 - 60 \times 171 - 426 \times 2 \\
&= 195 \times 57 - 171(450 - 195 \times 2) - 426 \times 2 \\
&= 195 \times 399 - 450 \times 171 - 426 \times 2 \\
&= 399(1\,095 - 450 \times 2) - 450 \times 171 - 426 \times 2 \\
&= 1\,095 \times 399 - 450 \times 969 - 426 \times 2 \\
&= 1\,095 \times 399 - 969(5\,925 - 1\,095 \times 5) - 426 \times 2 \\
&= \underline{\underline{5\,925 \times (-969) + 1\,095 \times 5\,244 + 426 \times (-2)}},
\end{aligned}$$

thus,

$$\underline{\underline{x = -969, y = 5\,244, \text{ and } z = -2}}.$$

4. Solve completely the diophantine equation

$$35x + 25y = 15.$$

Solution

$$\begin{aligned}
35 &= 25 \times 1 + 10, \\
25 &= 10 \times 2 + 5, \\
10 &= 5 \times 2 + 0,
\end{aligned}$$

and so

$$\text{GCD}(35, 25) = 5.$$

Now,

$$\begin{aligned}
5 &= 25 - 10 \times 2 \\
&= 25 - 2(35 - 25 \times 1) \\
&= 35 \times (-2) + 25 \times 3,
\end{aligned}$$

which mean

$$15 = 35 \times (-6) + 25 \times 9.$$

Next,

$$(x, y) = (-6, 9)$$

is a solution set which means the general solution set is

$$\underline{\underline{\{(-6 + 25n, 9 - 35n) : n \in \mathbb{Z}\}}}.$$