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.

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

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

Example 3
(a) Let

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

Find the value of b.

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

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

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

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

4 Problems

Here are some examples for you to try.

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

   (b) Find x, $y \in \mathbb{Z}$ such that
$$1\,147x + 851y = a.$$

2. (a) Let
$$h = \text{GCD}(1\,717, 1\,190).$$
Find the h.

   (b) Find x, $y \in \mathbb{Z}$ such that
$$1\,717x + 1\,190y = h.$$

3. Let
$$d = \text{GCD}(5\,925, 1\,095, 426).$$
Find x, y, and $z \in \mathbb{Z}$ such that
$$1\,219x + 1\,000y + 901z = d.$$

4. Solve completely the diophantine equation
$$35x + 25y = 15.$$