The Euclidean Algorithm

Highest Common Factor

A common factor of two integers means, not surprisingly, a number that is a factor of them both. Since 1 is a factor of every integer, any pair of integers has at least one common factor. We are often interested in the biggest of these, the **highest common factor (`hcf`)**. For example, 12 and 30 have common factors 1, 2, 3, and 6, and so

$$\mathrm{hcf}(12, 30) = 6.$$

(These ideas extend to negative numbers and negative factors.) Some books call the `hcf` the **greatest common divisor (`gcd`)**.

The **lowest common multiple (`lcm`)** of two integers is the smallest number that is a multiple of them both. For example, 12 and 30 have common multiples 60, 120, 180, ..., and

$$\mathrm{lcm}(12, 30) = 60.$$

One way to find the `hcf` and `lcm` of a pair of numbers is to factorise them as products of primes, though this is impracticable for large numbers.

It is easy to check that the `lcm` is the product of the two numbers divided by the `hcf`. In other words, for two integers a and b:

$$a \times b = \mathrm{hcf}(a, b) \times \mathrm{lcm}(a, b).$$

The Euclidean Algorithm

Multiplying two numbers together is easy, but finding the factors of a number is a hard problem if the number is large. However, finding the highest common factor of two numbers is surprisingly easy. We use a technique called the **Euclidean Algorithm**.

At each stage we divide the larger of the two numbers by the smaller. We then multiply the smaller number by the quotient and subtract the product from the larger. This gives the remainder. The process is repeated with this remainder and the smaller of the two previous numbers. We stop when the remainder is zero. The last non-zero remainder is the `hcf`.

We will use this to find the `hcf` of 48 and 11:

$$\begin{aligned} 48 &= 4 \times 11 + 4, \\ 11 &= 2 \times 4 + 3, \\ 4 &= 1 \times 3 + 1, \end{aligned}$$

$$3 = 3 \times 1 + 0.$$

So $\text{hcf}(48, 11) = 1$.

Video Visit the URL below to view a video:

`https://www.youtube.com/embed/NMX6rQDXVZo`

We can also use this for bigger numbers. For example, to find the `hcf` of 28907 and 120149 as $\text{hcf}(120149, 28907) = 137$.

$$\begin{aligned} 120149 &= 4 \times 28907 + 4521 \\ 28907 &= 6 \times 4521 + 1781 \\ 4521 &= 2 \times 1781 + 959 \\ 1781 &= 1 \times 959 + 822 \\ 959 &= 1 \times 822 + 137 \\ 822 &= 6 \times 137 + 0 \end{aligned}$$

The Extended Euclidean Algorithm

There is an alternative way of laying out the calculations of the algorithm. This will be especially useful later on when we look at RSA encryption. In this extended version of the algorithm, we keep track of the information slightly differently. The numbers in parentheses are called the coordinates of the numbers next to them. If you multiply the first coordinate by 48 and the second one by 11 and add them together, then you get the adjacent number. For example, $8 = (2 \times 48) + ((-8) \times 11)$. In particular, note that the `hcf` can be expressed in

$(1, 0)$	48	11	$(0, 1)$
$(0, 4)$	44	8	$(2, -8)$
$(1, -4)$	4	3	$(-2, 9)$
$(-2, 9)$	3	3	$(9, -39)$
$(3, -13)$	1	0	$(-11, 48)$

such a way: $1 = (3 \times 48) + ((-13) \times 11)$.

The basic rule is that you always start by associating one of the numbers with the coordinates $(1, 0)$ and the other with $(0, 1)$. Then to calculate further coordinates you always treat the coordinates in exactly the same way as the numbers with which they are associated. Let's work through an example using this method to see how this works.

Video Visit the URL below to view a video:

`https://www.youtube.com/embed/70i8Rg7Chok`

The extended Euclidean algorithm shows the following important result: The highest common factor of two integers a and b can be expressed as a linear combination

$$\text{hcf}(a, b) = ua + vb,$$

where both u and v are integers.

Two integers are called **coprime** if their `hcf` is 1; in other words, they are coprime if they have no prime factors in common. An important case of the result is: If two integers a and b are coprime then there exist integers u and v such that

$$1 = ua + vb.$$

This is the result that will be used in RSA encryption.

Concept Checks

Test Yourself Visit the URL below to try a numbas exam:
`https://numbas.mathcentre.ac.uk/question/66090/euclidean-algorithm/embed`