that

$$q \le \frac{b}{a} < q+1$$

(this is just saying $\frac{b}{a}$ lies between two consecutive integers). Multiplying through by the positive integer a, we obtain $qa \le b < (q+1)a$, hence $0 \le b - qa < a$.

Now put $r = b - qa$. Then $b = qa + r$ and $0 \le r < a$, as required. ∎

PROPOSITION 11.2

Let $a, b, d \in \mathbb{Z}$, and suppose that $d|a$ and $d|b$. Then $d|(ma+nb)$ for any $m, n \in \mathbb{Z}$.

PROOF Let $a = c_1 d$ and $b = c_2 d$ with $c_1, c_2 \in \mathbb{Z}$. Then for $m, n \in \mathbb{Z}$,

$$ma + nb = mc_1 d + nc_2 d = (mc_1 + nc_2)\, d\,.$$

Hence $d|(ma+nb)$. ∎

The Euclidean Algorithm

The Euclidean algorithm is a step-by-step method for calculating the common factors of two integers. First we need a definition.

DEFINITION *Let $a, b \in \mathbb{Z}$. A* common factor *of a and b is an integer which divides both a and b. The* highest common factor *of a and b, written $hcf(a,b)$, is the largest positive integer that divides both a and b.*

For example, $\text{hcf}(2,3) = 1$ and $\text{hcf}(4,6) = 2$. But how do we go about finding the highest common factor of two large numbers, say 5817 and 1428? This is what the Euclidean algorithm does for us — in a few simple, mindless steps.

Before presenting the algorithm in all its full glory, let us do an example.

Example 11.1

Here we find $\text{hcf}(5817, 1428)$ in a few mindless steps, as advertised. Write $b = 5817, a = 1428$, and let $d = \text{hcf}(a,b)$.

Step 1 Divide a into b and get a quotient and remainder:

$$5817 = 4 \cdot 1428 + 105\,.$$

(*Deduction*: As $d|a$ and $d|b$, d also divides $a - 4b = 105$.)

Step 2 Divide 105 into 1428:

$$1428 = 13 \cdot 105 + 63\,.$$

(*Deduction*: As $d|1428$ and $d|105$, d also divides 63.)

Step 3 Divide 63 into 105:

$$105 = 1 \cdot 63 + 42\,.$$

(*Deduction*: $d|42$.)

Step 4 Divide 42 into 63:

$$63 = 1 \cdot 42 + 21\,.$$

(*Deduction*: $d|21$.)

Step 5 Divide 21 into 42:

$$42 = 2 \cdot 21 + 0\,.$$

Step 6 STOP!

We claim that $d = \text{hcf}(5817, 1428) = 21$, the last non-zero remainder in the above steps. We have already observed that $d|21$. To prove our claim, we work upwards from the last step to the first: namely, Step 5 shows that $21|42$; hence Step 4 shows that $21|63$; hence Step 3 shows that $21|105$; hence Step 2 shows that $21|1428$; hence Step 1 shows $21|5817$. Therefore, 21 divides both a and b, so $d \ge 21$. As $d|21$, it follows that $d = 21$, as claimed.

The general version of the Euclidean algorithm is really no more complicated than this example. Here it is.

Let a, b be integers. To calculate $\text{hcf}(a,b)$, we perform (mindless) steps as in the example: first divide a into b, getting a quotient q_1 and remainder r_1; then divide r_1 into a, getting remainder $r_2 < r_1$; then divide r_2 into r_1, getting remainder $r_3 < r_2$; and carry on like this until we eventually get a remainder 0 (which we must, as the r_is are decreasing and are ≥ 0). Say the remainder 0