occurs after $n+1$ steps. Then the equations representing the steps are:

$$\begin{aligned}
&(1)\ b = q_1 a + r_1 && \text{with } 0 \le r_1 < a \\
&(2)\ a = q_2 r_1 + r_2 && \text{with } 0 \le r_2 < r_1 \\
&(3)\ r_1 = q_3 r_2 + r_3 && \text{with } 0 \le r_3 < r_2 \\
&\quad \cdots && \cdots \\
&\quad \cdots && \cdots \\
&\quad \cdots && \cdots \\
&(n-1)\ r_{n-3} = q_{n-1} r_{n-2} + r_{n-1} && \text{with } 0 \le r_{n-1} < r_{n-2} \\
&\quad (n)\ r_{n-2} = q_n r_{n-1} + r_n && \text{with } 0 \le r_n < r_{n-1} \\
&(n+1)\ r_{n-1} = q_{n+1} r_n + 0
\end{aligned}$$

THEOREM 11.1
In the above, the highest common factor hcf(a,b) is equal to r_n, the last non-zero remainder.

PROOF Let $d = \text{hcf}(a,b)$. We first show that $d|r_n$ by arguing from equation (1) downwards. By Proposition 11.2, d divides $b - q_1 a$, and hence by (1), $d|r_1$. Then by (2), $d|r_2$; by (3), $d|r_3$, and so on, until by (n), $d|r_n$.

Now we show that $d \ge r_n$ by working upwards from equation $(n+1)$. By $(n+1)$, $r_n|r_{n-1}$; hence by (n), $r_n|r_{n-2}$; hence by $(n-1)$, $r_n|r_{n-3}$, and so on, until by (2), $r_n|a$ and then by (1), $r_n|b$. Thus, r_n is a common factor of a and b, and so $d \ge r_n$.

We conclude that $d = r_n$, and the proof is complete. ∎

The next result is an important consequence of the Euclidean algorithm.

PROPOSITION 11.3
If $a,b \in \mathbb{Z}$ and $d = hcf(a,b)$, then there are integers s and t such that

$$d = sa + tb\ .$$

PROOF We use Equations $(1), \ldots, (n)$ above. By (n),

$$d = r_n = r_{n-2} - q_n r_{n-1}\ .$$

Substituting for r_{n-1} using Equation $(n-1)$, we get

$$d = r_{n-2} - q_n(r_{n-3} - q_{n-1} r_{n-2}) = x r_{n-2} + y r_{n-3}$$

where $x, y \in \mathbb{Z}$. Using Equation $(n-2)$ we can substitute for r_{n-2} in this (specifically, $r_{n-2} = r_{n-4} - q_{n-2} r_{n-3}$), to get

$$d = x' r_{n-3} + y' r_{n-4}$$

where $x', y' \in \mathbb{Z}$. Carrying on like this, we eventually get $d = sa + tb$ with $s,t \in \mathbb{Z}$, as required. ∎

Example 11.2
We know by Example 11.1 that $\text{hcf}(5817, 1428) = 21$. So by Proposition 11.3 there are integers s,t such that

$$21 = 5817s + 1428t\ .$$

Let us find such integers s,t.

To do this, we apply the method given in the proof of Proposition 11.3, using the equations in Steps 1 thrcugh 4 of Example 11.1. By Step 4,

$$21 = 63 - 42\ .$$

Hence by Step 3,

$$21 = 63 - (105 - 63) = -105 + 2 \cdot 63\ .$$

Hence by Step 2,

$$21 = -105 + 2(1428 - 13 \cdot 105) = 2 \cdot 1428 - 27 \cdot 105\ .$$

Hence by Step 1,

$$21 = 2 \cdot 1428 - 27(5817 - 4 \cdot 1428) = -27 \cdot 5817 + 110 \cdot 1428\ .$$

Thus we have found our integers s,t: $s = -27, t = 110$ will work. (But note that there are many other values of s,t which also work, for example $s = -27 + 1428, t = 110 - 5817$.)

Here is a consequence of Proposition 11.3.

PROPOSITION 11.4
If $a,b \in \mathbb{Z}$, then any common factor of a and b also divides $hcf(a,b)$.

PROOF Let $d = \text{hcf}(a,b)$. By Proposition 11.3, there are integers s,t such that $d = sa + tb$. If m is a common factor of a and b, then m divides $sa + tb$ by Proposition 11.2, hence m divides d. ∎

We are now in a position to prove a highly significant fact about prime numbers: namely, that if a prime number p divides a product ab of two integers, then p divides one of the factors a and b.