DEFINITION *If $a,b \in \mathbb{Z}$ and $\text{hcf}(a,b) = 1$, we say that a and b are* coprime *to each other.*

For example, 17 and 1024 are coprime to each other. Note that by Proposition 11.3, if a,b are coprime to each other, then there are integers s,t such that $1 = sa + tb$.

PROPOSITION 11.5
Let $a,b \in \mathbb{Z}$.
(a) *Suppose c is an integer such that a,c are coprime to each other, and $c|ab$. Then $c|b$.*
(b) *Suppose p is a prime number and $p|ab$. Then either $p|a$ or $p|b$.*

PROOF (a) By Proposition 11.3, there are integers s,t such that $1 = sa + tc$. Multiplying through by b gives

$$b = sab + tcb\ .$$

Since $c|ab$ and $c|tcb$, the right-hand side is divisible by c. Hence $c|b$.

(b) We show that if p does not divide a, then $p|b$. Suppose then that p does not divide a. As the only positive integers dividing p are 1 and p, $\text{hcf}(a,p)$ must be 1 or p; it is not p as p does not divide a, hence $\text{hcf}(a,p) = 1$. Thus a,p are coprime to each other, and $p|ab$. It follows by part (a) that $p|b$, as required. ∎

Proposition 11.5(b) will be crucial in our proof of the uniqueness of prime factorization in the next chapter. To apply it there, we need to generalize it slightly to the case of a prime dividing a product of many factors, as follows.

PROPOSITION 11.6
Let $a_1,a_2,\ldots,a_n \in \mathbb{Z}$, and let p be a prime number. If $p|a_1a_2\ldots a_n$, then $p|a_i$ for some i.

PROOF We prove this by induction. Let $P(n)$ be the statement of the proposition.

First, $P(1)$ says "if $p|a_1$ then $p|a_1$," which is trivially true.

Now suppose $P(n)$ is true. Let $a_1,a_2,\ldots,a_{n+1} \in \mathbb{Z}$, with $p|a_1a_2\ldots a_{n+1}$. We need to show that $p|a_i$ for some i.

Regard $a_1a_2\ldots a_{n+1}$ as a product ab, where $a = a_1a_2\ldots a_n$ and $b = a_{n+1}$. Then $p|ab$, so by Proposition 11.5(b), either $p|a$ or $p|b$. If $p|a$, that is to say $p|a_1a_2,\ldots,a_n$, then by $P(n)$ we have $p|a_i$ for some i; and if $p|b$ then $p|a_{n+1}$. Thus, in either case, p divides one of the factors $a_1,a_2,\ldots,a_{n+1}$.

We have established that $P(n) \Rightarrow P(n+1)$. Hence, by induction, $P(n)$ is true for all n. ∎

Exercises for Chapter 11

1. For each of the following pairs a,b of integers, find the highest common factor $d = \text{hcf}(a,b)$, and find integers s,t such that $d = sa + tb$:
   (i) $a = 17, b = 29$
   (ii) $a = 713, b = 552$
   (iii) $a = 299, b = 345$.

2. Show that if a,b are positive integers and $d = \text{hcf}(a,b)$, then there are positive integers s,t such that $d = sa - tb$.
   Find such positive integers s,t in each of cases (i)–(iii) in Question 1.

3. A train leaves Moscow for St. Petersburg every 7 hours, on the hour. Show that on some days it is possible to catch this train at 9 A.M.
   Whenever there is a 9 A.M. train, Ivan takes it to visit his aunt Olga. How often does Olga see her nephew?
   Discuss the corresponding problem involving the train to Vladivostock, which leaves Moscow every 14 hours.

4. Show that for all positive integers n,
   $$\text{hcf}(6n+8, 4n+5) = 1\ .$$

5. Let m,n be coprime integers, and suppose a is an integer which is divisible by both m and n. Prove that mn divides a.
   Show that the above conclusion is false if m and n are not coprime (i.e., show that if m and n are not coprime, there exists an integer a such that $m|a$ and $n|a$, but mn does not divide a).

6. Let $a,b,c \in \mathbb{Z}$. Define the highest common factor $\text{hcf}(a,b,c)$ to be the largest positive integer that divides a,b and c. Prove that there are integers s,t,u such that
   $$\text{hcf}(a,b,c) = sa + tb + uc\ .$$
   Find such integers s,t,u when $a = 91, b = 903, c = 1792$.