# Primes and divisibility

**Prime factorization.** Primes are numbers that cannot be factored, i.e. numbers that cannot be written as a product of smaller integers. 6 is not a prime because it is the product of 2 and 3. 2 and 3 are both primes, however. We have thus found the *prime factorization* of 6, i.e. we have written 6 as a product of primes, namely $6 = 2 \times 3$. We can find the prime factorization of greater integers by repeated factoring, such as $48 = 2 \times 24 = 2 \times 2 \times 12 = 2 \times 2 \times 2 \times 6 = 2 \times 2 \times 2 \times 2 \times 3 = 2^4 \times 3$.

**Divisibility.** We can read off from the prime factorization of an integer which numbers it is divisible by. For example, from the factorization $48 = 2^4 \times 3$ we see that 48 is divisible by $2, 2^2, 2^3, 2^4, 3, 2 \times 3, 2^2 \times 3, 2^3 \times 3$ and $2^4 \times 3$. The following quicker tests for divisibility are also useful. An integer is divisible by 2 if it is even, i.e. if its last digit is divisible by 2. An integer is divisible by 3 if the sum of its digits is divisible by 3; e.g. 39 is divisible by 3 since $3 + 9 = 12$ is divisible by 3. An integer is divisible by 5 if its last digit is 0 or 5. An integer is divisible by 9 if the sum of its digits is divisible by 9; e.g. 812,763 is divisible by 9 since $8 + 1 + 2 + 7 + 6 + 3 = 27$ is divisible by 9.

**Irrationality of $\sqrt{2}$.** We shall now illustrate the power of these ideas by proving that $\sqrt{2}$ is irrational, i.e. that $\sqrt{2}$ is not a ratio of two integers. To do so we suppose that $\sqrt{2}$ is in fact a ratio of two integers and show that this leads to a contradiction. Suppose $\sqrt{2} = \frac{m}{n}$, where we have cancelled out any common factors from the nominator and denominator; in particular both $m$ and $n$ cannot be even for then we would have cancelled out a factor 2, and so on. Now take $\sqrt{2} = \frac{m}{n}$ and square both sides. This gives $2 = \frac{m^2}{n^2}$, and when we multiply up the denominator we get $2n^2 = m^2$. Now, since the left hand side is even (i.e. divisible by 2), the right hand side must also be even, i.e. $m^2$ is even, but then $m$ must be even and thus it can be written as 2 times something, let's say $m = 2k$. So now $m^2 = 4k^2$. And above we had $2n^2 = m^2$, so we get $2n^2 = 4k^2$, which gives $n^2 = 2k^2$. But look! The right hand side is certainly even so $n^2$ must also be even, so $n$ must be even, and we have our contradiction. To sum up: we assumed that $\frac{m}{n}$ was a fully simplified fraction equal to $\sqrt{2}$, but it then followed that both $m$ and $n$ were even, which contradicted our assumption. Therefore no fraction equal to $\sqrt{2}$ can exist.

**Infinitude of primes.** There are infinitely many primes. We shall now look at Euclid's proof of this theorem, which dates from around 300 BC (*Elements*, Book IX, Proposition 20). Some people consider it very pretty. It goes like this. Suppose there are only finitely many primes. Multiply all of these together and call the result $\Pi$. Now consider the number $\Pi + 1$. Any prime of course divides $\Pi$, and therefore $\Pi + 1$ divided by any prime would leave the remainder 1, i.e. $\Pi + 1$ is not evenly divisible by any prime, i.e. $\Pi + 1$ must itself be prime, contrary to our assumption. QED.