4.3 Primes and greatest common divisors

Definition: An integer is **prime** if it is at least 2 and its only factors are itself and 1. An integer is **composite** if it is at least 2 and not prime.

The integer 1 is special (identity for multiplication) and is not prime and not composite.

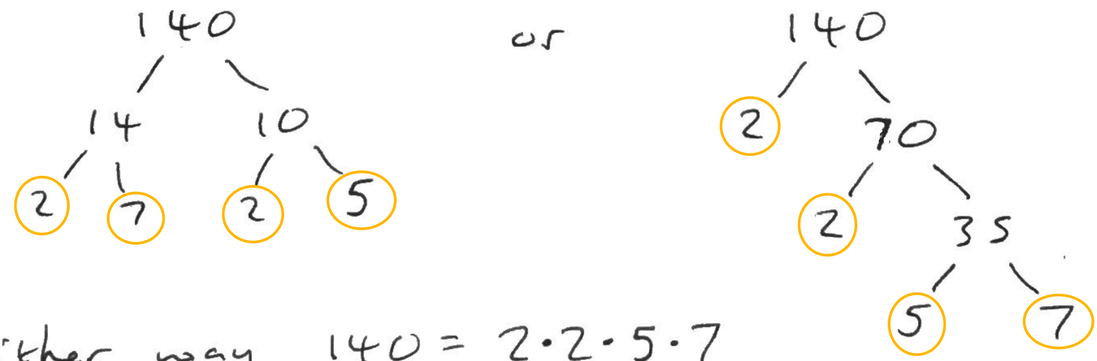
In our notation, an integer $n \geqslant 2$ is prime means that if $a \geqslant 1$ satisfies $a \mid n$ then we must have $a = 1$ or $a = n$.

$$\boxed{2}\quad \boxed{3}\quad 4\quad \boxed{5}\quad 6\quad \boxed{7}\quad 8\quad 9\quad 10\quad \boxed{11}\quad 12\ \ldots$$

primes.

Example ① Factor 140 into a product of primes.

Solution: We can use a factor "tree"



Either way $140 = 2 \cdot 2 \cdot 5 \cdot 7$

Fundamental theorem of arithmetic: Every integer at least 2 can be factored uniquely (up to ordering) into a product of primes.

- See examples 1, 2 p257.

Example ② Find the prime factorization of 539.

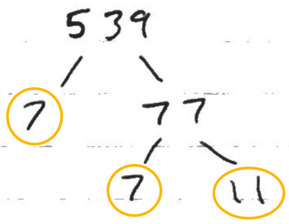
Solution: There are no obvious factors. 2 is not a factor, so try the next prime 3:

$$\begin{array}{r} 179 \\ 3\,\overline{)\,539} \\ -3 \\ \hline 23 \\ -21 \\ \hline 29 \\ -27 \\ \hline 2 \end{array}$$

$539 \bmod 3 = 2$ so $3 \nmid 539$.

$5 \nmid 539$ either, try 7 next

$$\begin{array}{r} 77 \\ 7\,\overline{)\,539} \\ -49 \\ \hline 49 \\ -49 \\ \hline 0 \end{array} \quad \checkmark$$



$$\boxed{539 = 7\cdot 7\cdot 11}$$

Example ③ Find the prime factorization of 541.

Solution: Try dividing by the first primes to find a factor

$$\begin{aligned} 541 \bmod 2 &= 1 \\ 541 \bmod 3 &= 1 \\ 541 \bmod 5 &= 1 \\ 541 \bmod 7 &= 2 \\ 541 \bmod 11 &= 2 \\ 541 \bmod 13 &= 8 \\ 541 \bmod 17 &= 14 \\ 541 \bmod 19 &= 9 \\ 541 \bmod 23 &= 12 \end{aligned}$$

the primes
2 to 23
do not divide
541

Note that $\sqrt{541} = 23.2594$ so if

$$541 = a \cdot b \quad \text{then} \quad a \le 23 \text{ or } b \le 23.$$

In other words, if 541 is composite then one of its factors must be less than or equal to 23. There were no such prime factors so 541 is prime. Its prime factorization is just 541.

In general, if n is composite then it must have a prime factor that is $\le \sqrt{n}$.

- See examples 3, 4 p 258.

Prime numbers have been studied for thousands of years – though it is obviously an advantage to have a calculator or computer.

In the sieve of Eratosthenes you can find primes by listing the integers. Circle 2 and remove its multiples. Then circle the next number and remove its multiples. Keep going and the primes will be all circled.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30

The largest known prime number is

$$2^{82589933} - 1$$

found in 2018, but a bigger one will certainly be found soon. Primes of the form

$2^n - 1$ are called Mersenne primes.

In fact there are infinitely many primes, so they go on forever.

- See p 260, 261.

Greatest common divisors

The divisors of an integer are just all its factors - the positive integers that divide it.

Examples: divisors of 10 are 1, 2, 5, 10

divisors of 18 are 1, 2, 3, 6, 9, 18

From these two lists we see the biggest divisor that 10 and 18 have in common is 2. So 2 is their greatest common divisor (or factor):

$$\gcd(10, 18) = 2$$

You also see the notation

gcf(10,18), GCF(10,18) or even (10,18).

Example ④ Find $\gcd(42, 70)$.

Solution: List all the divisors

42 : 1, 2, 3, 6, 7, 14, 21, 42
70 : 1, 2, 5, 7, 10, 14, 35, 70

So $\gcd(42, 70) = 14$.

Easier solution: use their prime factorizations

$$\left.\begin{aligned}42 &= 2\cdot 3\cdot 7\\ 70 &= 2\cdot 5\cdot 7\end{aligned}\right\}\ \gcd = 2\cdot 7$$

Definition: Two integers are relatively prime if their gcd is 1.

For example 14 and 33 are relatively prime. It means they have no factors in common and their prime factorizations must use different primes.

The Euclidean algorithm

This is one of the oldest and most famous algorithms. It gives an efficient way to find the gcd of two numbers and uses the division algorithm. Recall that says $a \div d = q$ remainder r so that

$$a = dq + r \qquad 0 \leq r \leq d-1.$$

Suppose a, b are integers with $a \geqslant b$ and we want $\gcd(a,b)$. First divide a by b and get quotient q_1 and remainder r_2:

$$a = b q_1 + r_2 \qquad 0 \leq r_2 < b$$

Now divide b by that remainder r_2:

$$b = r_2 q_2 + r_3 \qquad 0 \leq r_3 < r_2$$

Next divide r_2 by r_3:

$$r_2 = r_3 q_3 + r_4 \qquad 0 \leq r_4 < r_3$$

The remainders keep getting smaller. Repeat until you get a 0 remainder. The last nonzero remainder is the gcd we wanted.

If we let $a = r_0$ and $b = r_1$ above it makes it a little clearer.

Example ⑤ Use the Euclidean algorithm to find $\gcd(18, 10)$.

Solution: $a = r_0 = 18$, $b = r_1 = 10$

$$\begin{aligned} r_0 &= r_1 q_1 + r_2 &&: & 18 &= 10 \cdot 1 + 8 \\ r_1 &= r_2 q_2 + r_3 &&: & 10 &= 8 \cdot 1 + 2 \\ r_2 &= r_3 q_3 + r_4 &&: & 8 &= 2 \cdot 4 + 0 \end{aligned}$$

last nonzero remainder

$$\boxed{\gcd(18,10) = 2}$$

- See example 16 p 268.