# MAT1830

Lecture 2: Divisors and Primes

## Number theory - why should you care?

Number theory is used in tonnes of places across computer science:

- pseudorandom number generation
- hash functions
- memory management
- error correction
- fast arithmetic operations
- cryptography and authentication

**Definition** An *integer* is a "whole number". It may be positive or negative or zero.

So the integers are the numbers

$$\ldots\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\ldots.$$

Is 12 an integer? Yes.

Is $-6$ an integer? Yes.

Is $\frac{1}{2}$ an integer? No.

The set of all the integers is often written as $\mathbb{Z}$.

We say that integer $a$ *divides* integer $b$ if

$$b = qa \quad \text{for some integer } q.$$

**Example.** 2 divides 6 because $6 = 3 \times 2$.

This is the same as saying that division with remainder gives remainder 0. Thus $a$ does *not* divide $b$ when the remainder is $\neq 0$.

**Example.** 3 does not divide 14 because it leaves remainder 2: $\quad 14 = 4 \times 3 + 2$.

When $a$ divides $b$ we also say:

- $a$ is a *divisor* of $b$,
- $a$ is a *factor* of $b$,
- $b$ is *divisible* by $a$,
- $b$ is a *multiple* of $a$.

Does 7 divide 21? Yes (because $21 = 3 \times 7$).

Does 8 divide 12? No (because $12 = 1 \times 8 + 4$).

Does 25 divide 5? No (because $5 = 0 \times 25 + 5$).

**Flux Exercise** (LQMTZZ)

Does 10 divide 60? Does 11 divide 11?

**Answer:** Yes, Yes (because $60 = 6 \times 10$ and $11 = 1 \times 11$).

## 2.1 Primes

A positive integer $p > 1$ is a prime if its only positive integer divisors are 1 and $p$. Thus the first few prime numbers are

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, \ldots$$

The number 1 is not counted as a prime, as this would spoil the

**Fundamental Theorem of Arithmetic.** *Each integer $> 1$ can be expressed in exactly one way, up to order, as a product of primes.*

**Example.** $210 = 2 \times 3 \times 5 \times 7$, and this is the only product of primes which equals 210.

This would not be true if 1 was counted as a prime, because many factorisations involve 1. E.g.

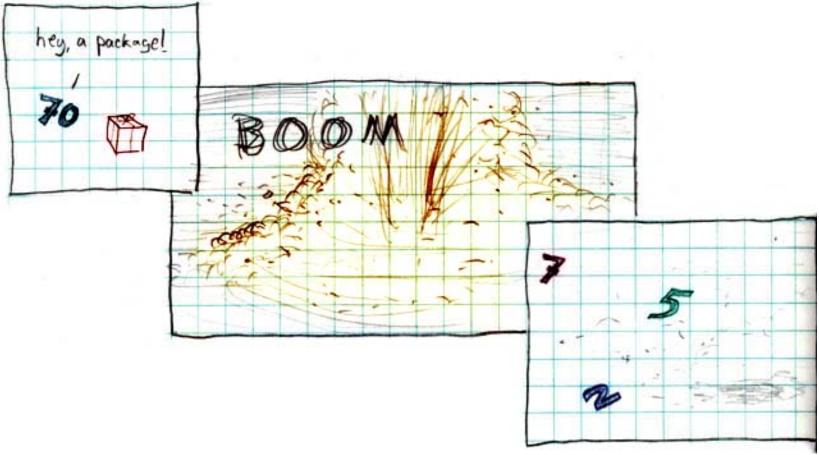
$$210 = 1 \times 2 \times 3 \times 5 \times 7 = 1^2 \times 2 \times 3 \times 5 \times 7 = \ldots$$

**Question 2.4** What are the prime factorisations of 999 and 1000?

### Answer

$$\begin{aligned} 999 &= 9 \times 111 \\ &= 3^2 \times (3 \times 37) \\ &= 3^3 \times 37 \end{aligned}$$

$$\begin{aligned} 1000 &= 10^3 \\ &= (2 \times 5)^3 \\ &= 2^3 \times 5^3 \end{aligned}$$


hey, a package!
70
BOOM
7
5
2

## 2.2 Recognising primes

If an integer $n > 1$ has a divisor, it has a divisor $\leqslant \sqrt{n}$, because for any divisor $a > \sqrt{n}$ we also have the divisor $n/a$, which is $< \sqrt{n}$.

Thus to test whether 10001 is prime, say, we only have to see whether any of the numbers $2, 3, 4, \ldots \leqslant 100$ divide 10001, since $\sqrt{10001} < 101$. (The least divisor found is in fact 73, because $10001 = 73 \times 137$.)

This explains a common algorithm for recognising whether $n$ is prime: try dividing $n$ by $a = 2, 3, \ldots$ while $a \leqslant \sqrt{n}$.

The algorithm is written with a boolean variable *prime*, and $n$ is prime if $\mathit{prime} = \mathsf{T}$ (true) when the algorithm terminates.

```
assign a the value 2.
assign prime the value T.
while a ⩽ √n and prime= T
    if a divides n
        give prime the value F
    else
        increase the value of a by 1.
```

Divisors come in pairs!

For example, the divisors of 40 are paired as follows:

- 1, 40
- 2, 20
- 4, 10
- 5, 8

**Fact** If $n = ab$ for integers $n$, $a$ and $b$, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Otherwise $a > \sqrt{n}$ and $b > \sqrt{n}$, and then $ab > n$.

## 2.2 Recognising primes

If an integer $n > 1$ has a divisor, it has a divisor $\leqslant \sqrt{n}$, because for any divisor $a > \sqrt{n}$ we also have the divisor $n/a$, which is $< \sqrt{n}$.

Thus to test whether 10001 is prime, say, we only have to see whether any of the numbers $2, 3, 4, \ldots \leqslant 100$ divide 10001, since $\sqrt{10001} < 101$. (The least divisor found is in fact 73, because $10001 = 73 \times 137$.)

This explains a common algorithm for recognising whether $n$ is prime: try dividing $n$ by $a = 2, 3, \ldots$ while $a \leqslant \sqrt{n}$.

The algorithm is written with a boolean variable *prime*, and $n$ is prime if $prime = \mathsf{T}$ (true) when the algorithm terminates.

```
assign a the value 2.
assign prime the value T.
while a ⩽ √n and prime= T
    if a divides n
        give prime the value F
    else
        increase the value of a by 1.
```

## 2.3 Finding divisors

This algorithm also finds a prime divisor of $n$.
Either
the least $a \leqslant \sqrt{n}$ which divides $n$,
or,
if we do not find a divisor among the $a \leqslant \sqrt{n}$, $n$ itself is prime.

**Definition** Suppose $m$ and $n$ are positive integers. Then a *common divisor* of $m$ and $n$ is an integer which divides both $m$ and $n$.

**Example** The common divisors of 30 and 45 are 1,3,5,15 (and their negatives).

**Definition** Suppose $m$ and $n$ are positive integers. Then the *greatest common divisor* (or gcd) of $m$ and $n$ is the greatest integer which is a common divisor of $m$ and $n$.

**Examples**
$\gcd(30, 45) = 15$
$\gcd(13, 21) = 1$
$\gcd(15, 21) = 3$

**Note** $\gcd(a, b)=\gcd(b, a)$ for any integers $a$ and $b$

## 2.4 The greatest common divisor of two numbers

It is remarkable that we can find the greatest common divisor of positive integers $m$ and $n$, $\gcd(m, n)$, without finding their prime divisors.

This is done by the famous *Euclidean algorithm*, which repeatedly divides the greater number by the smaller, keeping the smaller number and the remainder.

**Euclidean Algorithm.**
**Input:** positive integers $m$ and $n$ with $m \geqslant n$
**Output:** $\gcd(m, n)$

$a := m$, $b := n$
$r :=$ remainder when $a$ is divided by $b$
**while** $r \neq 0$ **do**
    $a := b$
    $b := r$
    $r :=$ remainder when $a$ is divided by $b$
**end**
return $b$

**Example.** $m = 237, n = 105$

The first values are $a = 237, b = 105$,
so $r = 237 - 2 \times 105 = 27$.
The next values are $a = 105, b = 27$,
so $r = 105 - 3 \times 27 = 24$.
The next values are $a = 27, b = 24$,
so $r = 27 - 1 \times 24 = 3$.
The next values are $a = 24, b = 3$,
so $r = 24 - 8 \times 3 = 0$.
Thus the final value of $b$ is 3, which is $\gcd(237, 105)$.

This can be set out more neatly:

$$\begin{array}{rcrcrcr}
237 & = & 2 & \times & 105 & + & 27 \\
105 & = & 3 & \times & 27 & + & 24 \\
27 & = & 1 & \times & 24 & + & \mathbf{3} \\
24 & = & 8 & \times & 3 & + & 0
\end{array}$$

# Example

Find $\gcd(165, 120)$.

$$\begin{array}{rcrcrcr} 165 & = & 1 & \times & 120 & + & 45 \\ 120 & = & 2 & \times & 45 & + & 30 \\ 45 & = & 1 & \times & 30 & + & 15 \\ 30 & = & 2 & \times & 15 & + & 0 \end{array}$$

**Flux:** What's the next line?

$\Leftarrow$ **Answer**

So $\gcd(165, 120) = 15$.

**Fact** $\gcd(a - kb, b) = \gcd(a, b)$ for any positive integers $a$, $b$, $k$.

**Proof** If $d$ is a common divisor of $a$ and $b$ then $d$ is a common divisor of $a - kb$ and $b$.

If $e$ is a common divisor of $a - kb$ and $b$ then $e$ is a common divisor of $a$ and $b$ (note $a = (a - kb) + kb$).

So the list of common divisors of $a - kb$ and $b$ is exactly the same as the list of common divisors of $a$ and $b$.

So the greatest common divisor of $a - kb$ and $b$ is equal to the greatest common divisor of $a$ and $b$. $\square$

## 2.5 The Euclidean algorithm works!

We start with the precondition $m \geqslant n > 0$. Then the division theorem tells us there is a remainder $r < b$ when $a = m$ is divided by $b = n$. Repeating the process gives successively smaller remainders, and hence the algorithm eventually returns a value.

That the value returned value is actually $\gcd(m, n)$ relies on the following fact.

**Fact.** If $a$, $b$ and $k$ are integers, then

$$\gcd(a - kb, b) = \gcd(a, b).$$

By using this fact repeatedly, we can show that after each execution of the while loop in the algorithm $\gcd(b, r) = \gcd(m, n)$. When the algorithm terminates, this means $b = \gcd(b, 0) = \gcd(m, n)$. (Equivalently, in the neat set out given above, the gcd of the numbers in the last two columns is always $\gcd(m, n)$.)

## 2.6 Extended Euclidean algorithm

If we have used the Euclidean algorithm to find that $\gcd(m,n) = d$, we can "work backwards" through its steps to find integers $a$ and $b$ such that $am + bn = d$.

**Example.** For our $m = 237$, $n = 105$ example above:

$$
\begin{aligned}
3 &= & 27 - 1\times 24 & & \\
3 &= & 27 - 1(105 - 3\times 27) &= & -105 + 4\times 27 \\
3 &= & -105 + 4(237 - 2\times 105) &= & 4\times 237 - 9\times 105
\end{aligned}
$$

So we see that $a = 4$ and $b = -9$ is a solution in this case.

Our first line above was a rearrangement of the second last line of our original Euclidean algorithm working. In the second line we made a substitution for 24 based on the second line of our original Euclidean algorithm working. In the third line we made a substitution for 27 based on the first line of our original Euclidean algorithm working.

**Question.** Find integers $a$ and $b$ such that $353a + 78b = 1$.

We first use the Euclidean algorithm to find $\gcd(353, 78)$:

$$
\begin{array}{rcccccc}
353 & = & 4 & \times & 78 & + & 41 \\
78 & = & 1 & \times & 41 & + & 37 \\
41 & = & 1 & \times & 37 & + & 4 \\
37 & = & 9 & \times & 4 & + & 1 \\
4 & = & 4 & \times & 1 & + & 0
\end{array}
$$

Then we use the extended Euclidean algorithm:

$$
\begin{array}{rcrcr}
1 & = & 37 - 9 \times 4 & & \\
1 & = & 37 - 9(41 - 37) & = & -9 \times 41 + 10 \times 37 \\
1 & = & -9 \times 41 + 10(78 - 41) & = & 10 \times 78 - 19 \times 41 \\
1 & = & 10 \times 78 - 19(353 - 4 \times 78) & = & -19 \times 353 + 86 \times 78
\end{array}
$$

So $-19 \times 353 + 86 \times 78 = 1$. One solution is $a = -19$, $b = 86$.

**Question 2.1 (hint)** Try something similar to what we did on the last slide.

**Question 2.2** Can a multiple of 15 and a multiple of 21 differ by 1?

**Answer**

Note $\gcd(15, 21) = 3$.

So 3 divides $x \times 21$
and 3 divides $y \times 15$.

So 3 divides $x \times 21 - y \times 15$.

The answer is no. The difference between a multiple of 15 and a multiple of 21 is always divisible by 3.

Earlier we saw that

$$\begin{aligned} 999 &= 3^3 \times 37 \\ 1000 &= 2^3 \times 5^3 \end{aligned}$$

So 999 and 1000 have no prime factors in common.

**Question 2.5** Is there a way of seeing this without factoring the numbers?

**Answer** Yes. If $d$ divides 999 and $d$ divides 1000 then $d$ must divide $1000 - 999 = 1$. So $d = 1$ and $d$ is not prime.