Integers

$\mathbb{Z}$ is the set of all integers, positive and negative

$\mathbb{Z} = \mathbb{N} \cup \{-n : n \in \mathbb{Z}_+\}$ $\quad -n < 0 \ \forall n \in \mathbb{Z}_+$

$\forall n \in \mathbb{Z}$ exactly one of the following holds: $n > 0$, $n < 0$ or $n = 0$

If $m, n \in \mathbb{N}$ with $n \leq m$ then $m - n$ is the unique natural number such that

$$n + (m - n) = m$$ In particular $n - n = 0$.

Arithmetic of the integers satisfies

$$-(-n) = n \quad \forall n \in \mathbb{Z} \qquad 0 = -0$$

$$m + (-n) = m - n \quad \forall m, n \in \mathbb{Z}$$

$$-(m+n) = (-m) + (-n) \quad \forall m, n \in \mathbb{Z}$$

$$(-m)n = -(mn) \quad \forall m, n \in \mathbb{Z}$$

We are now going to start talking about divisibility of one integer by another. The

Odd and even integers

Definition $n \in \mathbb{Z}$ is even if $n = 2m$ for some $m \in \mathbb{Z}$

If $n \in \mathbb{N}$ is even then $n = 2m$ for some $m \in \mathbb{N}$.

$n \in \mathbb{Z}$ is odd if n is not even.

Examples $0 = 2 \times 0$ is even. 1 is odd because $\nexists\, m \in \mathbb{N}$ s.t. $1 = 2m$

$m \neq 0 \Rightarrow 2 \times 0 = 0$ $\quad m \in \mathbb{Z}_+ \Rightarrow 2m > 1$.

Theorem $\forall n \in \mathbb{Z}$, either n is even or $n+1$ is even (but not both)

Proof Since $n = 2m \Leftrightarrow -n = 2(-m)$ so n is even $\Leftrightarrow -n$ is even

Prove by induction that $\forall n \in \mathbb{N}$, either n is even or $n+1$ is even.

Base case $n = 0 = 2 \times 0$ is even So true for $n = 0$

Inductive step Suppose $n \in \mathbb{N}$ and either n or $n+1$ is even.

If $n+1$ is even then $n+1$ is even

If n is even then $n = 2m$ for some $m \in \mathbb{N}$ and $(n+1)+1 = 2m+2 = 2(m+1)$ is even

So n or n+1 even $\Rightarrow$ n+1 or (n+1)+1 even.

If $n \in \mathbb{N}$ is even, show n+1 not even.

$n = 2m$, then $k \in m \Rightarrow 2k \in n$ $k > m \Rightarrow k \geq m+1 \Rightarrow$

$2k \geq 2m+2 > 2m+1 = n+1$ So n+1 not even.

Corollary $n \in \mathbb{N}$ is odd $\Leftrightarrow n = 2k+1$ some $k \in \mathbb{N}$

Similarly $n \in \mathbb{Z}$ is odd $\Leftrightarrow n = 2k+1$, some $k \in \mathbb{Z}$.

Proof $n \in \mathbb{N}$ is odd $\Leftrightarrow$ n+1 even $\Leftrightarrow$ n-1 even $\Leftrightarrow n-1 = 2k$, some $k \in \mathbb{N}$

~~(k ∈ ℕ, k ∈ ℕ)~~

Examples $17 = 2\times 8 + 1$ is odd $27 = 2\times 13 + 1$ is odd.

This gives the following:

Theorem $n \in \mathbb{Z}$ is even $\Leftrightarrow n^2$ is even.

Proof It suffices to show n even $\Rightarrow n^2$ even and n odd $\Rightarrow$ (n^2 not even) $\Rightarrow n^2$ odd

Let $n \in \mathbb{Z}$ be even, so that $n = 2k$, $k \in \mathbb{Z}$

$n = 2k \Rightarrow n^2 = 4k^2 = 2(2k^2)$ is even

Now let n be odd, so that $n = 2k+1$, some $k \in \mathbb{Z}$

$n = 2k+1 \Rightarrow n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$

is odd. □

Dividing

Def^n Let $m, n \in \mathbb{Z}$. m divides n, written $m \mid n$, if $n = mk$ for some $k \in \mathbb{Z}$. In this case we say that m is a divisor of n, or a factor of n (Also, k is a divisor/factor of n)

we also say n is divisible by m.

Examples $n = n \times 1$. So, $\forall n \in \mathbb{Z}$, 1 and n divide n, and 1 and n are divisors of n $\quad 1 \mid n \quad n \mid n$

The Euclidean property of the integers

This is expressed by the following

Theorem If $k, m \in \mathbb{Z}$ and $k \neq 0$, then $\exists\, q \in \mathbb{Z}$ and $r \in \mathbb{Z}$ with $0 \leq r < |k|$ with

$$m = qk + r,$$

Remark
If $k = 2$ this simply says that $m = 2q$ or $2q+1$, some $q \in \mathbb{Z}$ — which we already know.
If $k = 3$ then $m = 3q$ or $3q+1$ or $3q+2$, some $q \in \mathbb{Z}$.

Proof of the theorem is omitted, but it uses Peano's fifth axiom — can be written out as an induction, just as the characterisation of odd integers.

Examples Write $n = qk + r$ with $0 \leq r < |k|$ where

① $n = 17$ $k = 4$ $\quad 17 = 4 \times 4 + 1$ $\quad q = 4$ $r = 1$ $\quad 0 \leq 1 < 4$

② $n = 17$, $k = 104$ $\quad 17 = 0 \times 104 + 17$ $\quad q = 0$ $r = 17$ $\quad 0 \leq r < 104$

③ $n = 104$ $k = 17$ $\quad 104 = 6 \times 17 + 2$ $\quad q = 6$ $r = 2$ $\quad 0 \leq 2 < 17$

④ $n = 26$ $k = 6$ $\quad 26 = 4 \times 6 + 2$

⑤ $n = 2088$ $k = 18$ $\quad 2088 = 116 \times 18 + 0$ $\quad 18 \mid 2088$

Examples of finding divisors

① What are the divisors of 28?

$28 = 4 \times 7 = 2^2 \times 7$ $\quad (2+1) \times (1+1) = 6$

1, 2, 4, 7, 14, 28

What are the divisors of 45?

$45 = 9 \times 5 = 3^2 \times 5$ $\quad (2+1) \times (1+1) = 6$

1, 3, 9, 5, 15, 45.

Also $n = (-n)\times(-1)$ $\forall n \in \mathbb{Z}$, so $-n \mid n$ and $-1 \mid n$

$4 = 2\times 2$ so $2 \mid 4$

$15 = 3\times 5$ so $3 \mid 15$ and $5 \mid 15$

$n \times 0 = 0$ so $n \mid 0$ $\forall n \in \mathbb{Z}$.

$-2 \mid 8$ because $8 = (-2)\times(-4)$

Defn $n \in \mathbb{Z}$ is prime if the only divisors of n are $\pm n, \pm 1$ and $n \neq 0, \pm 1$.

So If $n \in \mathbb{N}$, then n is prime if the only divisors in $\mathbb{N}$ are n, 1. and $n \neq 0, 1$.

Examples 2 is prime: the only divisors in $\mathbb{N}$ are 1 and 2 because $k > 2$ if $k \in \mathbb{N}$, $k \neq 1, 2$

Write $\nmid$ for "does not divide"

$\forall n \in \mathbb{Z}_+$, $0 \nmid n$.

$3 \nmid 8$ because $2\times 3 = 6 < 8$ $3\times 3 = 9 > 8$

$3k < 8$ $\forall k \in \mathbb{Z}$, $k \leq 2$

$3k > 8$ $\forall k \in \mathbb{Z}$, $k \geq 3$

This gives an indication of how we decide whether or not one integer divides another.

Product Notation $\prod_{k=1}^{n} a_k = a_1 \times a_2 \cdots \times a_n$

Examples $n! = \prod_{k=1}^{n} k$ $2^n = \prod_{k=1}^{n} 2$ $\prod_{k=1}^{n} \frac{k}{k+1} = \frac{1}{2}\times\frac{2}{3}\cdots\times\frac{n}{n+1}$

(3) What are the divisors of 2088?

$2088 = 2\times1044 = 4\times522 = 8\times261 = 2^3\times9\times29 = 2^3\times3^2\times29$

The divisors are

1, 2, 4, 8, 3, 6, 12, 24, 9, 18, 36, 72, 29, 58, 116, 232,

87, 174, 348, 696, 261, 522, 1044, 2088

24 divisors. $(3+1)\times(2+1)\times(1+1) = 24$

Properties of divisors

Integers that have a large divisor in common do have something in common! Understanding an integer means knowing its divisors. A very basic lemma about common divisors is the following.

Lemma $m|n \wedge n|p \Rightarrow m|p \quad \forall m,n,p\in\mathbb{Z}$.

e.g. $1044|2088 \wedge 522|1044 \Rightarrow 522|2088$!

Proof Definition chasing!

$m|n \iff mk_1 = n$, some $k_1\in\mathbb{Z}$

$n|p \iff nk_2 = p$, some $k_2\in\mathbb{Z}$

$mk_1 = n \wedge nk_2 = p \Rightarrow nk_2 = m(k_1k_2) = p$

$k_1, k_2\in\mathbb{Z} \Rightarrow k_1k_2\in\mathbb{Z}$

So $m|n \wedge n|p \Rightarrow m|p$ □.

Greatest common divisors

An integer k is a <u>common divisor</u> of integers m and n if $k|m$ and $k|n$.

Examples 4 is a common divisor of 28 and 20. 9 is a common divisor of 18 and 45

In both cases these are actually greatest common divisors.

The existence and definition of greatest common divisors (also called gcd's) is given by the following theorem - which also suggests how to find gcd's.

Theorem Let m and n be non-zero integers. Then $\exists\, g \in \mathbb{Z}_+$ with the following properties

1. $g \mid m \wedge g \mid n$, that is, g is a common divisor
2. $k \in \mathbb{Z} \wedge k \mid m \wedge k \mid n \Rightarrow k \mid g$
3. $g = am + bn$ for some $a, b \in \mathbb{Z}$ and $g \leq |a_1 m + b_1 n| \quad \forall a_1, b_1 \in \mathbb{Z}$ with $a_1 m + b_1 n \neq 0$

Definition $g \in \mathbb{Z}_+$ satisfying 1 and 2 is called the greatest common divisor (gcd) of m and n.

This makes sense because by property 2, if $k \in \mathbb{Z}$ with $k \mid m$ and $k \mid n$ then $k \mid g$, and so $|k| \leq g$

The gcd of m and n is unique