

Announcements

1) Reading for Tuesday : Section 3.3

Definition: (divisors, multiples)

Let $m, n \in \mathbb{Z}$, $m \neq 0$. We say m divides n if $\exists k \in \mathbb{Z}$ with $n = mk$. We say m is a divisor (or factor) of n , and n is a multiple of m .

Notation: $m \mid n$ ("m divides n")

If $p \in \mathbb{Z}$, p is prime if $p > 1$ and the only positive divisors of p are 1 and p .

Definition: (\mathbb{Z}_p) Let p be a prime number. Then \mathbb{Z}_p is the set of equivalence classes of \mathbb{Z} under the equivalence relation

$$m \sim n \quad \text{if} \quad p \mid (n - m)$$

In fact, this definition works just fine if p is not a prime!

If $k \in \mathbb{N}$, \mathbb{Z}_k is the
set of equivalence classes
of integers under

$$m \sim n \text{ if } k \mid (n - m).$$

Proof that this is an equivalence relation:

Symmetry, Reflexivity, Transitivity

Reflexivity: Let $m \in \mathbb{Z}$. Is

$$m \sim m? \quad m - m = 0,$$

so $k \mid m - m = 0$ for all

$k \in \mathbb{N}$.

Symmetry: Suppose $m, n \in \mathbb{Z}$

and $m \sim n$. Is $n \sim m$?

Well, $m \sim n$ means $k \mid (n-m)$,

and $n \sim m$ means $k \mid (m-n)$.

But if $k \mid (n-m)$, then

$$m-n = (-1)(n-m), \text{ and so}$$

$$k \mid (m-n).$$

Transitivity: Let $m, n, j \in \mathbb{Z}$.

Suppose $m \sim n$, $n \sim j$. Is

$m \sim j$?

If $m \sim n$, then $k \mid (n-m)$,
and if $n \sim j$, then $k \mid (j-n)$.

We want to show that also

$k \mid (j-m)$.

We have

$$\begin{aligned} j - m &= j \overset{=0}{(-n + n)} - m \\ &= (j - n) + (n - m) \end{aligned}$$

Since $k \mid (n-m)$ and $k \mid (j-n)$,

$\exists l, a \in \mathbb{Z}$,

$$kl = n-m + ka = j-n,$$

So

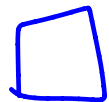
$$j-m = (j-n) + (n-m)$$

$$= ka + kl$$

$$= k(a+l) \quad \text{and}$$

$k \mid (j-m)$ and we are

done!



More Methods of Proof

(Section 3.2)

The Contrapositive: recall that

for a statement $P \Rightarrow Q$,

the contrapositive is the

statement $(\neg Q) \Rightarrow (\neg P)$.

These are logically equivalent statements, so proving one proves the other.

Example 1: Let $n, m \in \mathbb{Z}$. Then if
 $n \in 2\mathbb{Z}$, $nm \in 2\mathbb{Z}$.

Proof: Prove the contrapositive:

If $nm \notin 2\mathbb{Z}$, then $n \notin 2\mathbb{Z}$.

If $nm \notin 2\mathbb{Z}$, then 2 does not divide nm . But then 2 cannot divide n . \square