1.3.4 a) Show if $a+b=a+c$ then $b=c$

Assume $a+b=a+c$

then $-a+(a+b)=-a+(a+c)$

use associativity $(-a+a)+b=(-a+a)+c$

inverse for addition $0+b=0+c$

identity for addition $b=c$

b) Show if $a\neq 0$ and $ab=ac$ then $b=c$

Assume $ab=ac$ $(a\neq 0)$

then $ab-ac=ac-ac$

distributive law $a(b-c)=0$

no zero divisors
$+ \; a\neq 0$ $\Rightarrow$ $b-c=0$

so $b=c$

1.5.2. Show that if $n \in \mathbb{Z}$ and $n > 1$, then n has a prime divisor.

Check base case $n=2$

this has a prime divisor, since n is prime

Assume all numbers $< n$ have prime divisors

Then either, no number $< n$ divides n,

then n is itself prime

or a number a divides n.

By induction hypothesis there is a prime $p | a$

Then $p | n$

Prove uniqueness of quotient and remainder in division alg.

1.5.6 Assume $a = bq + r$

and $a = bq' + r'$

Assume WLOG $q \geq q'$

Then $0 = bq - bq' + r - r'$

$= b(q - q') + r - r'$

$r' = b(q - q') + r$

if $q - q' > 0$, then $r' \geq b$, contradicting

that r' is a remainder

1.5.14

a) Prove that if a prime p divides $a_1 a_2 \cdots a_r$ then p must divide a_j for some j

Use induction on r

$r=1$ OK since $p | a_1 \Rightarrow p | a_1$

Assume OK for r and that

$p | a_1 a_2 \cdots a_{r+1}$

$p | (a_1 a_2 \cdots a_r) a_{r+1}$

By Euclids lemma either $p | a_{r+1}$, so OK

or $p | a_1 a_2 \cdots a_r$ then OK by induction

1.5.14 b)

Prove if p is prime and p does not divide n, then $\gcd(p,n)=1$

$\gcd(p,n)$ divides p, hence $\gcd(p,n)$ is equal to 1 or p. If it is equal to p, then p divides n, so proven by contradiction

Suppose it is now 7p.m, what time will it be after 101 hours.

1.6.1 $101 = 24 \cdot 4 + 5$, so

$101 \equiv 5 \pmod{24}$

So 101 hours after 7p.m it is $7+5=12$ a.m.

a.m. since it will be midnight

a) Compute $\gcd(83,38) = d$ by using Euclid's alg.

1.6.8 $\gcd(83,38)$

$83 = 2 \cdot 38 + 7$

$38 = 5 \cdot 7 + 3$

$7 = 2 \cdot 3 + 1$

so $\gcd(83,38) = 1$

b) Use the result from a) to write $d = 83m + 38n$

$1 = 7 - 2 \cdot 3$

$= 7 - 2 \cdot (38 - 5 \cdot 7) = 11 \cdot 7 - 2 \cdot 38$

$= 11 \cdot (83 - 2 \cdot 38) - 2 \cdot 38 = \underline{11 \cdot 83 - 24 \cdot 38}$

c) Use part b) to solve $38x \equiv 1 \pmod{83}$

$1 = 11 \cdot 83 - 24 \cdot 38$

so $1 \equiv -24 \cdot 38 \pmod{83}$ or $1 \equiv 59 \cdot 38 \pmod{83}$

since $59 \equiv -24 \pmod{83}$

1.6.10 Suppose $n \in \mathbb{Z}^+$ and n is odd

Show that

$1+2+3+\cdots+(n-1) \equiv 0 \pmod{n}$

Reorder the terms to

$1+(n-1)+2+(n-2)+\cdots+\frac{n-1}{2}+\frac{n+1}{2}$

$= n + n + \cdots + n \equiv 0 \pmod{n}$

The same congruence does not hold for even n

e.g. for $n=4$

$1+2+3 = 6 \equiv 2 \not\equiv 0 \pmod{4}$

In fact, for even n

$1+2+\cdots+n-1 \equiv \frac{n}{2} \pmod{n}$

1.7.3 Show that $a|b$ is <u>not</u> an equiv. rel. on $\mathbb{Z}$

$a|b$ is <u>not</u> an equivalence relation on $\mathbb{Z}$, since

the relation is not symmetric

$a|b$ does not imply $b|a$ as seen.

for example with

$2|6$ but $6 \nmid 2$

We see this from the figure since the figure is not symmetric along the diagonal

Note that this relation is reflexive and transitive

1.7.5 Show that the relation on $\mathbb{R}$ given by

$a \sim b$ if $a - b \in \mathbb{Z}$ is an equivalence relation

---

Reflexive:

for any $a \in \mathbb{R}$ $a \sim a$ since $a - a = 0 \in \mathbb{Z}$

Symmetric

If $a \sim b$, then $a - b \in \mathbb{Z}$, so $b - a \in \mathbb{Z}$

hence $b \sim a$

Transitive

If $a \sim b$ and $b \sim c$, then $a - b \in \mathbb{Z}$ and $b - c \in \mathbb{Z}$

so $a - b + b - c = a - c \in \mathbb{Z}$, hence $a \sim c$

A nice set of representatives is $[0, 1)$

17.7. Draw the poset diagram for the set of positive divisors of 30

Divisors of 30 are

1 2 3 5 6 10 15 30