Divisibility

$b \not/ a$

b divides a
a is a multiple of b
b is a factor of a

$\exists k \in \mathbb{Z}$ s.t. $24 = 6 \cdot k$
$\exists k \in \mathbb{Z}$ s.t. $a = b \cdot k$

DEF: For integers a and b, $b \mid a$ means there is some integer k s.t. $a = b \cdot k$

$2 = 1 \cdot 2$ $24 = 6 \cdot 4$ $111 = 3 \cdot 37$

$1 \mid 2$ $6 \mid 24$ $37 \mid 111$ $1 \mid 0$ $0 = 1 \cdot 0$

$1 \mid 111$
$111 = 1 \cdot 111$

$3 \mid 23$? NO $3 \nmid 23$ 3716 $0 = 3716 \cdot k$

$\sim(\exists k \in \mathbb{Z}$ s.t. $23 = 3 \cdot k)$
$\forall k \in \mathbb{Z}, 23 \neq 3 \cdot k$

$a \mid 0$ $\exists k \in \mathbb{Z}$ s.t. $0 = a \cdot k$

$\_ \mid 1496474$

$\forall a \in \mathbb{Z}, 1 \mid a$

THM: For every integer a, $1 \mid a$

Let $a \in \mathbb{Z}$. [want: $1 \mid a$, iow $\exists k \in \mathbb{Z}$ s.t. $a = 1 \cdot k$]

Then $a = 1 \cdot a$ (identity)
So $\exists k \in \mathbb{Z}$ s.t. $a = 1 \cdot k$ (example $\therefore k = a$)
$1 \mid a$ (def $\mid$)

For all $a \in \mathbb{Z}$, $1 \mid a$ (gen. from generic particular)

$\forall a,b \in \mathbb{Z}\ (a>0 \wedge b>0) \rightarrow (a \mid b \rightarrow a \leq b)$
$\equiv \forall a,b \in \mathbb{Z}\ (a>0 \wedge b>0 \wedge a \mid b \rightarrow a \leq b)$

THM: For all integers a, b s.t. $a,b>0$, if $a \mid b$ then $a \leq b$

Proof: Let $a,b \in \mathbb{Z}$
Suppose $a,b>0$ and $a \mid b$ − +
Then $\exists k \in \mathbb{Z}$ s.t. $b = k \cdot a$; find that k. (def $\mid$)

$k<0 \vee k=0 \vee k>0$
$p \vee q \vee r$
$p \rightarrow c$
$\therefore \sim p$
$q \rightarrow c$
$\therefore \sim q$
$\therefore r$

Suppose $k<0$.
Then $ka<0$ (mult by negative)
and $b<0 \Rightarrow\Leftarrow$ $b<0 \wedge b>0$ (substitution)
$\therefore k<0 \rightarrow c$ (conclusion from supposition)
$\therefore k \geq 0$ (contradiction rule, negation of <)
Suppose $k=0$
Then $ka=0$ (mult by 0)
and $b=0 \Rightarrow\Leftarrow$ $b=0 \wedge b>0$ (substitution)
$\therefore k=0 \rightarrow c$ (concl from suppose)
$\therefore k \neq 0$ (contradiction rule)
$\therefore k>0$ (elimination)
$\therefore k \geq 1$ (k is an integer)
$\therefore ka \geq a$ (mult by positive)
$\therefore b \geq a$ (substitution)
$\therefore a,b>0$ and $a \mid b \rightarrow b \geq a$ (conclusion from supposition)
$\forall a,b \in \mathbb{Z}$ $a,b>0$ and $a \mid b \rightarrow b \geq a$ (generalization from generic particular)

$\forall a,b,c \in \mathbb{Z}$, $a \mid b \wedge b \mid c \rightarrow a \mid c$

THM: For all integers a, b, c, if $a \mid b$ and $b \mid c$ then $a \mid c$

Proof: Let $a,b,c \in \mathbb{Z}$ [want $a \mid b \wedge b \mid c \rightarrow a \mid c$]
Suppose $a \mid b$ and $b \mid c$
$\exists k \in \mathbb{Z}$ s.t. $b = a \cdot k$; find that k (def $\mid$; axiom choice)

Suppose $a|b$ and $b|c$

$\exists k \in \mathbb{Z}$ s.t. $b = a \cdot k$; find that k (def $|$; axiom choice)

$\exists l \in \mathbb{Z}$ s.t. $c = b \cdot l$; find that l (def $|$; axiom of choice)

So $c = a k \cdot l$ (substitution)

note $k \cdot l \in \mathbb{Z}$ (closure of $\mathbb{Z}$ under $\cdot$)

$\exists m \in \mathbb{Z}$ s.t. $c = a \cdot m$ (ex: $m = k \cdot l$)

$a|c$ (def $|$)

$a|b \wedge b|c \to a|c$ (conclusion of suppose)

$\forall a,b,c \in \mathbb{Z}\ a|b \wedge b|c \to a|c$ (generalization from generic particular)

$9=3.3$ $3|9$ $27=9.3$ $3|27$ $3|9+27$ $3=12 \cdot 3$ $3|36$ $36=3 \cdot 12$

THM: For all integers a,b,c, if $a|b$ and $a|c$, then $a|b+c$

Proof: Suppose $a,b,c \in \mathbb{Z}$ with $a|b$ and $a|c$ [want: $a|b+c$]

So by def of $|$, $\exists k \in \mathbb{Z}$ s.t. $b = k \cdot a$; find that k

Also by def of $|$ $\exists l \in \mathbb{Z}$ s.t. $c = l \cdot a$; find that l

So $b + c = k \cdot a + l \cdot a = a(k+l)$ where $k+l \in \mathbb{Z}$ by closure under $+$

So $\exists m \in \mathbb{Z}$ s.t. $b+c = a \cdot m$

namely $m = k+l$

So by def of $|$ $a|b+a$

So $\forall a,b,c \in \mathbb{Z}$, $a|b \wedge a|c \to a|b+c$

THM: $\forall a,b,c \in \mathbb{Z}$, $a|b \to a|bc$

$b = a \cdot k$ $bc = a(kc)$

COR: $\forall a,b \in \mathbb{Z}$, $a|b \to a|-b$

Proof: prev thm w/ $c=-1$

THM: For all integers n, if $2|n^2$ then $2|n$

n^2 is even; n is even

$2|a$ $\exists k \in \mathbb{Z}$ s.t. $a = 2k$

a is even

$p \to q$
$\equiv$
$\sim p \vee q \equiv \sim q \to \sim p$

$n^2 = 2k$

$n = \sqrt{2} \cdot \sqrt{k}$

Special case of QRT: every int is even or odd but not both

Proof: We prove the contrapositive : $\forall n \in \mathbb{Z}$, if $2 \nmid n$ then $2 \nmid n^2$

n is odd; n^2 is odd

Proof: Suppose $n \in \mathbb{Z}$ and $2 \nmid n$

Then n is not even ($2 \nmid n \equiv n$ is not even)

And so n is odd (QRT)

So $\exists k \in \mathbb{Z}$ s.t. $n = 2k+1$ (def odd)

Find that k

So $\exists k \in \mathbb{Z}$ s.t. $n = 2k+1$ (def odd)
Find that k

Then $n^2 = (2k+1)^2 = \underline{4k^2+4k}+1$

$= 2(2k^2+2k)+1$

where $\underline{2k^2+2k} \in \mathbb{Z}$ (closure of $\mathbb{Z}$ under $+, \cdot$)

And $\exists \ell \in \mathbb{Z}$ s.t. $n^2 = 2\ell+1$
namely $\ell = 2k^2+2k$

So n^2 is odd (def odd)

and $\underline{n^2 \text{ is not even}}$ (QRT)

so $2 \nmid n^2$ (def even, 1)

$\forall n \in \mathbb{Z}, \ 2 \nmid n \to 2 \nmid n^2$

$\forall n \in \mathbb{Z}, \ 2 \mid n^2 \to 2 \mid n$ (contrapos)

$$\begin{array}{r} q \qquad\quad\; r \\ 12 \overline{)\,149} = 12\ R\ 5 \\ \underline{12}\;\;\; \\ 29 \\ \underline{24} \\ 5 \end{array}$$

Quotient/Remainder Theorem

$n \div d = q\ R\ r$

THM (Quotient/Remainder Theorem): For any integer n and positive integer d, there exist unique integers q and r such that $n = q \cdot d + r$ and $0 \le r < 12$

q r

Ex: $132 = \underline{18} \cdot 7 + \underline{6}$

$99 = \underline{16} \cdot 6 + \underline{3}$

$-45 = \underline{-12} \cdot 4 + \underline{3}$

$d = 2$

QRT says all n are $2q+0$ (even) or $2q+1$ (odd) for some $q \in \mathbb{Z}$

but not both

DEF: For an integer n, n is prime means $n>1$ and $\forall d \in \mathbb{Z},\ d>0 \wedge d \mid n \rightarrow d=1 \vee d=n$

only positive divisors are 1 and n

n is composite means $n>1$ and $\exists s,t \in \mathbb{Z}$ s.t. $s \neq 1 \wedge t \neq 1 \wedge n = s \cdot t$

1, 3 — 3 is prime

1, 37 — 37 is prime T

6 is composite T (1, 2, 3, 6)

111 is composite T (1, 3, 37, 111)

0 is composite F (not > 1)

1 is neither prime nor composite (also not > 1)

THM: For any prime p, and $a \in \mathbb{Z}$, if $p \mid a$, then $p \nmid a+1$.

Proof: Suppose p is prime and $a \in \mathbb{Z}$ and $p \mid a$. [want $p \nmid a+1$]

Suppose $p \mid a+1$ [goal: contradiction]

- We have $p \mid -a$ (prev thm with $c=-1$)
- and so $p \mid (a+1)+-a$ i.o.w. $p \mid 1$ (prev thm $a \mid b \wedge a \mid c \rightarrow a \mid b+c$)
- and $p \leq 1$ (prev thm $a,b>0$ $a \mid b \rightarrow a \leq b$)
- but $p > 1$ (def prime) $\Rightarrow\Leftarrow$

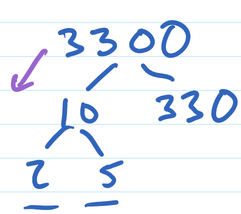
$a + b = a + (-b)$

So $p \mid a+1 \rightarrow c$

$\therefore p \nmid a+1$ (contradiction rule)

THM: For all integers $n \geq 2$, there is some prime p s.t. $p \mid n$

$3300 = 10 \cdot 330$



$n \mid 10 \qquad 10 \mid 3300$

THM: There are an infinite number of primes

Every finite list of primes is incomplete such that there is a prime not on the list.

Proof: Suppose $p_1, p_2, \ldots, p_k$ is a finite list of all primes. (need: a prime not on that list)

Let $a = p_1 \cdot p_2 \cdot \cdots \cdot p_k$

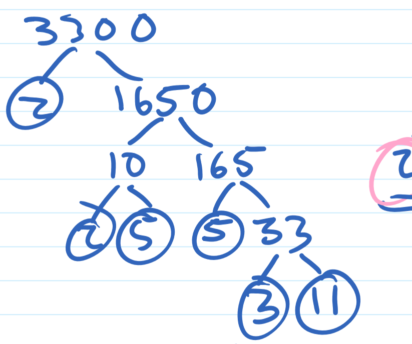
Note $p_i \mid a$ for all $1 \le i \le k$ $\quad a = p_i \cdot \underbrace{(p_1 \cdot \cdots \cdot p_{i-1} \cdot p_{i+1} \cdot \cdots \cdot p_k)}_{\text{integer b/c all } p_i \in \mathbb{Z} \text{ and } \mathbb{Z} \text{ closed under } \cdot}$

So $\underline{p_i \nmid a+1}$ for all $1 \le i \le k$ (prev. thm)

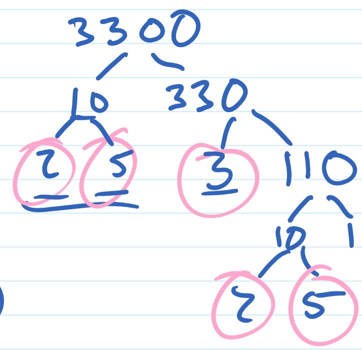
$a+1 \ge 2$ so there is a prime p s.t. $p \mid a+1$ (prev thm)

$p \ne p_i$ for all $1 \le i \le k$ b/c $p \mid a+1$ and $\underline{p_i \nmid a+1}$

So p is prime not on list $p_1, \ldots, p_k$



$2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 \cdot 11$



$3300 = 2 \cdot 5 \cdot 330$

$= 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 \cdot 11$

$3300 = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 \cdot 11$

$= 1 \cdot 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 \cdot 11$

$= 1 \cdot 1 \cdot 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 \cdot 11$

$\vdots$

Unique prime factorization (Fundamental Thm of Arithmetic)

THM: For all integers $n \ge 2$, there is some list of primes $p_1, \ldots, p_k$ s.t. $n = p_1 \cdot p_2 \cdot \cdots \cdot p_k$ and $p_1 \le p_2 \le \cdots \le p_k$ and that list is unique.