Divides

$a|b$ = a divides b for $a, b \in \mathbb{Z}$
if and only if $b = an$ for int n

"special cases": $7|0$ because $0 = 7 \cdot 0$
$b = a \cdot n$

$0 \nmid 7$ $\quad 7 \neq 0 \cdot n$

$-3|12$ $\quad 12 = -3 \cdot -4$

ex) For $a, b, c \in \mathbb{Z}$, if $\underbrace{a|b}_{\text{hyp.}}$ then $\underbrace{a|bc}_{\text{conclusion.}}$. Prove this by direct proof.

Suppose $a, b, c \in \mathbb{Z}$, and $a|b$. Then, by def'n of divides, $b = a \cdot n$ where $n \in \mathbb{Z}$. Multiply both sides by c, to get $bc = acn$. Since $n, c \in \mathbb{Z}$, $nc \in \mathbb{Z}$. We can define $m = cn \in \mathbb{Z}$. So $bc = a \cdot m$. Thus $a|bc$.

Goal: $\boxed{bc = a \cdot m}$ matches def'n of divides.

Primes

an integer $q \geq 2$ is prime if and only if the only positive factors of q are q and 1.

implies $\rightarrow$

biconditional $\leftrightarrow$

$a|b$ means a is a factor of b.

non-primes are composite

* all integers ≥ 2 can be written as the product of one or more prime factors (uniquely).

$20 = 2 \cdot 2 \cdot 5 = 2^2 5$

GCD and LCM → least common multiple

greatest common divisor (factor)

$\gcd(6,10) = 2$ $\qquad$ $\text{lcm}(6,10) = 30$

$2 \cdot 3 \quad 2 \cdot 5$

* if $\gcd(a,b) = 1$, they are relatively prime.

for $a, b \in \mathbb{Z}$, $b \geq 0$, there are unique integer q, r

$$a = b \cdot \underbrace{q}_{\text{quotient}} + \underbrace{r}_{\text{remainder}} \qquad 0 \leq r < b$$

$10 = 3 \cdot 3 + 1$

$-10 = 3 \cdot -4 + 2 \geq 0$

* $\gcd(a,b) = \gcd(b,r)$

Euclidean algorithm → computes GCD

```
gcd (a,b : pos int)
    x = a
    y = b
    while (y > 0)
      begin
      r = remainder (x,y)
      x = y
```

finding new remainder when dividing y by r

y = r
end
return x

★ gcd(x, y) = gcd(y, r)