Chapter 4, # 8

Suppose a is an integer. If $5|2a$ then $5|a$.

Proof: Suppose $a \in \mathbb{Z}$ and $5|2a$. By definition of "divides", there is a $d \in \mathbb{Z}$ such that $5d = 2a$. Since $2a$ is even (by def. of even), it follows that $5d$ is even. The number $5 = 2 \cdot 2 + 1$ is odd. If d were also odd, then the product $5d$ would be odd. (by Chapter 4, #4). So d must be even, & thus by the definition of even, there is a number $c \in \mathbb{Z}$ such that $2c = d$. Substituting $d = 2c$ into $5d = 2a$ gives $5(2c) = 2a$. Simplifying gives $5c = a$, where $c \in \mathbb{Z}$, so by the def. of "divides", we know $5|a$. ▨

Chapter 4, # 28

If $a, b, c \in \mathbb{Z}$, then $c \cdot \gcd(a,b) \leq \gcd(ca, cb)$.

Proof: Say $a, b, c \in \mathbb{Z}$. Let $d = \gcd(ca, cb)$. By the definition of gcd, $d|ca$ and $d|cb$. also, if $l|ca$ and $l|cb$, then $l \leq d$ (because d is the <u>greatest</u> common divisor.

Now let $e = \gcd(a,b)$.

Since $e|a$ and $e|b$ (def. of g.c.d.), there is a $k \in \mathbb{Z}$ and $m \in \mathbb{Z}$ such that $e.k = a$ and $em = b$. This means $cek = ca$ and $cem = cb$. By def. of "divides", we have that $ce|ca$ and $ce|cb$. So ce is a common divisor of ca and cb, and thus $ce \leq \gcd(ca, cb)$.

$c \cdot \gcd(a,b) \leq \gcd(ca, cb)$ ▨