EXAMPLE PROBLEMS FROM 1.8

Section 1.8, # 11

Let $a,b,c \in \mathbb{Z}$ nonzero such that a and b are coprime and a and c are coprime. Then a and bc are coprime.

[I'll give two different, equally valid, proofs]

Proof 1: Suppose $a,b,c \in \mathbb{Z}$ non zero with

$$\gcd(a,b) = \gcd(a,c) = 1.$$

Then $\exists\ x,y,s,t \in \mathbb{Z}$ with

$$ax + by = 1$$
$$as + ct = 1$$

So

$$by = 1 - ax$$
$$ct = 1 - as.$$

Then

$$bc(yt) = (1-ax)(1-as)$$
$$= 1 - ax - as + a^2 sx$$

$$\Rightarrow \quad a(x+s-asx) + bc(yt) = 1$$

So 1 can be expressed as a linear combination of a and bc, so $\gcd(a,bc) = 1$. ▨

__Proof 2__: We will prove the contrapositive.

Suppose $\gcd(a,bc) = d$ where $d \in \mathbb{N}$ with $d > 1$.

Then $\exists$ prime $p \in \mathbb{N}$ with $p \mid d$, since all natural numbers greater than 1 have a prime divisor. Since $d \mid a$ and $d \mid bc$ we conclude

$$p \mid a \text{ and } p \mid bc.$$

Since p is prime by Euclid's lemma

$$p \mid bc \Rightarrow p \mid b \text{ or } p \mid c.$$

Thus p is either a common divisor of a and b or a and c.

Thus $\gcd(a,b) = \gcd(a,c) = 1$ is false. $\blacksquare$

Section 1.8, #12

Let $a \in \mathbb{Z}$ and $p, q \in \mathbb{N}$ distinct primes. If $p|a$ and $q|a$ then $pq|a$.

Proof: Let a, p, q be as in the statement. Then $\exists\ k, l \in \mathbb{Z}$ with $a = pk = ql$. Since $pk = ql$ we see $p | ql$ so by Euclid's lemma $p|q$ or $p|l$. But p, q are prime and $p \neq q$ so $p \nmid q$. Thus $p | l$, so $\exists\ m \in \mathbb{Z}$ with $l = pm$. Finally

$$a = ql \Rightarrow a = qpm \Rightarrow qp | a,$$

as desired. $\blacksquare$