Math 300 HW #5

Section 4.8 16, 19, 21

Section 8.4 9b, 14

4.8 #16 $\gcd(4131, 2431)$

$4131 \bmod 2431 = 1700$

$2431 \bmod 1700 = 731$

$1700 \bmod 731 = 238$

$731 \bmod 238 = 17$

$238 \bmod 17 = 0$

$= \gcd(2431, 1700)$

$= \gcd(1700, 731)$

$= \gcd(731, 238)$

$= \gcd(238, 17)$

$= 17$

~~822292~~

So $\gcd(4131, 2431) = 17$

4.8 #19 Thm $a|b \iff \gcd(a,b) = a$

Pf $\Rightarrow$ If $a|b$, then a is a common divisor of a & b. It must also be the greatest common divisor, since nothing greater than a is a divisor of a. So $\gcd(a,b) = a$.

$\Leftarrow$ If $\gcd(a,b) = a$, then a is a common divisor, so $a|a$ and $a|b$. and $a|b$ is what we needed to show.

4.8 #21 Thm If $a, b \in \mathbb{Z}$ with $b \neq 0$ and

$$a = bq + r,$$

then $\gcd(b,r) \leq \gcd(a,b)$.

Pf Let c be any common div. of b, r. It's enough to show c is a common div. of a, b. c is already a divisor of b, so we need only show $c|a$. We know $c|b$ and $c|r$, so $b = lc$ and $r = kc$ for some $l, k \in \mathbb{Z}$. Then

$$a = bq + r = lcq + kc = c(lq + k)$$

so $c|a$ Shown.

8.4 #96 Thm If $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$ then $a-b \equiv c-d \pmod{n}$

Pf We have $a = c + kn$ and $b = d + \ell n$, then

$$a-b = c+kn-(d+\ell n)$$
$$= c-d+(k-\ell)n$$

So $a-b \equiv c-d \pmod{n}$

8.4 #14

$14^2 = 196 \equiv 31 \mod 55$

$14^4 = (14^2)^2 = 31^2 = 961 \equiv 26 \mod 55$

$14^8 = 26^2 = 676 \equiv 16 \mod 55$

$14^{16} = 16^2 = 256 \equiv 36 \mod 55.$