MA312 Assignment #1

#2/ (e) gcd: pq^2
lcm: p^2q^3

#4/ $1 = 7s + 11t$
$1 = 7(-3) + 11(2)$

#6/ assume: $a|c$, $b|c$, $\gcd(a,b)=1$ prove: $ab|c$

proof: By assumption $c = am = bn$ for some $m, n \in \mathbb{Z}$. $\exists\, s,t$ s.t. $as + bt = 1$.
Mult. by c: $cas + cbt = c$. Using the assumptions we get
$bnas + ambt = c$. Now factor,
$ab(ns + mt) = c$. Thus $ab|c$.

If a,b not rel. prime: $2|6$, $6|6$ but $2 \cdot 6 \nmid 6$.

#9/ Let $n \in \mathbb{Z}^+$. If $a \bmod n = a'$, $b \bmod n = b'$, prove $(a+b) \bmod n = (a'+b') \bmod n$
& $ab \bmod n = a'b' \bmod n$

proof: $(a+b) \bmod n = a \bmod n + b \bmod n = a' + b' \pmod n$
$ab \bmod n = a \bmod n \cdot b \bmod n = a'b' \pmod n$

#11/ Let $n, a \in \mathbb{Z}^+$, $d = \gcd(a,n)$. Show $ax \bmod n = 1$ has sol'n $\Leftrightarrow$ $d = 1$.

$\Rightarrow$ If $ax \bmod n = 1$ has sol'n then $\exists\, y$ s.t. $ay \bmod n = 1$. Thus,
$ay + 1 = nq$ or $ay' + nq = 1$ w/ $y', q \in \mathbb{Z}$, implying $d = 1$.

$\Leftarrow$ If $d = 1$ then $\exists\, s,t \in \mathbb{Z}$ s.t. $as + nt = 1$ or $as + 1 = n(-t)$ implying $(as) \bmod n = 1$
& s is a sol'n to the given.

#14/ p, q, r primes $\neq 3$. Show $3 \mid p^2+q^2+r^2$.

$p = 3k+1$ or $p = 3k+2$ for $k \in \mathbb{Z}$.
$q = 3l+1$ or $q = 3l+2$ $\quad l \in \mathbb{Z}$
$r = 3s+1$ or $r = 3s+2$ $\quad s \in \mathbb{Z}$

Either way $p = \pm 1 \bmod 3$
$q = \pm 1 \bmod 3$
$r = \pm 1 \bmod 3$.

So $p^2 + q^2 + r^2 = (\pm 1)^2 + (\pm 1)^2 + (\pm 1)^2 \bmod 3$
$= 1 + 1 + 1 \bmod 3$
$= 3 \bmod 3 = 0$.

So $3 \mid p^2 + q^2 + r^2$.

#16/ $7^{1000} \bmod 6 = (7 \bmod 6)^{1000} = 1$

$6^{1001} \bmod 7 = (-1)^{1001} \bmod 7 = -1 \bmod 7 = 6$

#18/ $8^{402} \bmod 5 = 8^{2 \cdot 201} \bmod 5$
$= 16^{201} \bmod 5$
$= (16 \bmod 5)^{201}$
$= 1$

#20/ Let $p_1, p_2, \ldots, p_n$ be primes. Show $p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$ is divisible by none of the p_i.

Set $n = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$

$n \bmod p_i = 1$ for each $i \in 1, \ldots, n$.

If $p_i \mid n$ then $n = p_i q$ implying $n \bmod p_i = 0$. QED.

#21/ There are ∞'ly primes.

Proof: Proceed by contradiction. Assume there are only a finite # of primes, $p_1, p_2, \ldots, p_n$. Let $n = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$.

By #20 n is not divisible by any of the p_i. Since these are all the primes this means n is not divisible by any other prime. By defn n must be prime. But n is not on the list (if it were then we'd have $p_i \mid n$ for some i. Thus the p_i are not the only primes & we conclude there must be an ∞ # of primes.