MA 300 HW #6

Section 8.4 # 31a, 33, 37, 40, 41a

#31 a inverse for 210 mod 13:

First, $\gcd(210, 13) = 1$, we want a linear combo:

$$210 = 16 \cdot 13 + 2 \qquad 1 = 13 - 6 \cdot 2$$

$$13 = 6 \cdot 2 + 1 \qquad 1 = 13 - 6(210 - 16 \cdot 13)$$

$$2 = 2 \cdot 1 + 0 \qquad 1 = 13 - 6 \cdot 210 + 96 \cdot 13$$

$$1 = 97 \cdot 13 - 6 \cdot 210$$

so $-6 \cdot 210 = 1 - 97 \cdot 13 \equiv 1 \pmod{13}$

So -6 is the inverse

#33 If $\gcd(a,b)=1$ and $a|c$ and $b|c$ then $ab|c$

Pf Let $\gcd(a,b)=1$ and $a|c$ and $b|c$.

Then $\exists k, l$ with $1 = la + kb$, mult. by c:

$$c = cla + ckb$$

$a|c$ so $\exists n$ with $an = c$

$b|c$ so $\exists m$ with $bm = c$

so

$$\begin{aligned} c &= bmla + ankb \\ &= abml + abnk \\ &= ab(ml + nk) \end{aligned}$$

so $ab|c$.

#37 $p=23 \quad q=31 \quad e=43 \quad pq=713$

To encrypt we do $C = M^e \bmod (p-1)(q-1) = M^{43} \bmod 713$

First letter: "C" = 03 so $M=3$

so $C = 3^{43} \bmod 713$

$= \ldots$ (usual tricks for powers)

$= 675$

Next letter: "O" = 15

so $C = 15^{43} \bmod 713 = 89$

Next: "M" = 13

so $C = 13^{43} \bmod 713 = 476$

Next: "E" = 05

so $C = 5^{43} \bmod 713 = 129$

So the encrypted message is 675 089 476 129

#40 First we find d, the inverse to $\underset{43}{e} \bmod \underset{22 \cdot 30 = 660.}{(p-1)(q-1)}$

$$\begin{aligned}
660 &= 15 \cdot 43 + 15 \\
43 &= 2 \cdot 15 + 13 \\
15 &= 1 \cdot 13 + 2 \\
13 &= 6 \cdot 2 + 1 \\
2 &= 2 \cdot 1 + 0
\end{aligned}$$

$$\begin{aligned}
1 &= 13 - 6 \cdot 2 = 13 - 6(15 - 13) = 7 \cdot 13 - 6 \cdot 15 \\
&= 7 \cdot (43 - 2 \cdot 15) - 6 \cdot 15 = 7 \cdot 43 - 20 \cdot 15 \\
&= 7 \cdot 43 - 20(660 - 15 \cdot 43) \\
&= 7 \cdot 43 - 20 \cdot 660 + 300 \cdot 43 \\
&= 307 \cdot 43 - 20 \cdot 660
\end{aligned}$$

So the inverse is $307 = d$.

Now decrypt:

028: $28^{307} \bmod 713 = 14$ = "N"

018: $18^{307} \bmod 713 = 9$ = "I"

675: $675^{307} \bmod 713 = 3$ = "C"

129: $129^{307} \bmod 713 = 5$ = "E"

NICE!

#41a Thm For all $s > 0$, if $p, q_1, q_2, \ldots, q_s$ are prime and $p \mid q_1 q_2 \cdots q_s$,

then $p = q_i$ for some $1 \le i \le s$.

Pf By induction on s.

Base case $s=1$ WTS: If $p \mid q_1$ then $p = q_1$.

Let $p \mid q_1$, since p & q_1 are prime this means $p = q_1$, since q_1 has no divisors other than 1 & q_1, and $p \neq 1$ since p is prime.

Inductive step:

Induction Hypothesis $(s=k)$ Assume if $p \mid q_1 \cdots q_k$ then $p = q_i$ for some $1 \le i \le k$.

[WTS if $p \mid q_1 \cdots q_{k+1}$ then $p = q_i$ for some $1 \le i \le k+1$.]

Let $p \mid q_1 \cdots q_{k+1}$, so $\underset{a}{p} \mid \underset{b}{(q_1 \cdots q_k)} \cdot \underset{c}{q_{k+1}}$.

Since these are all prime we have $\gcd(p, q_{k+1}) = 1$, so Euclid's Lemma applies and we have $p \mid \underline{q_1 \cdots q_k}$ or $p \mid \underline{q_{k+1}}$.

If $p \mid q_{k+1}$ then $p = q_{k+1}$ as in the base case, so we are done.

Otherwise, if $p \mid q_1 \cdots q_k$ then the induction hyp. says $p = q_i$ for some i, as desired.