Theorem 4.35

~~Thm 6.31~~ $(U(n), \cdot \bmod n)$ is a group.

Sketch of proof: Recall that

$$U(n) = \{ k \in \mathbb{Z}_n \mid \gcd(n,k) = 1 \}.$$

That is, $U(n)$ is the set of numbers in $\mathbb{Z}_n$ that are relatively prime to n. We need to show that $U(n)$ is a group under multiplication mod n (i.e., mult two #'s from $U(n)$, div by n, and take remainder). We must show:

(0) $U(n)$ is closed under $\cdot \bmod n$.

(1) The operation is associative.

(2) $\exists$ an identity elmt.

(3) $\forall\, g \in U(n)$, $\exists\, g^{-1} \in U(n)$.

(0) Closure: Let $a, b \in U(n)$. Then

$\gcd(n,a) = 1$ and $\gcd(n,b) = 1$.

By the Fundamental Thm of Arithmetic, n and a have no prime factors in common. ~~Similar~~ Similarly, n and b have no prime factors in common. It follows that n and ab have no prime factors in common, and hence $\gcd(n, ab) = 1$. However, it is possible that $ab > n$.

By the Division Algorithm, $\exists !$ $q, r \in \mathbb{Z}$ s.t.

$$ab = nq + r,$$

where $0 \leq r < n$. Then $ab \equiv r \pmod{n}$.

We need to show that $\gcd(n, r) = 1$. Assume otherwise. Then $\exists$ a prime p that divides both n and r. This implies that $n = pk_1$ and $r = pk_2$ for some $k_1, k_2 \in \mathbb{Z}$. But ~~thath~~ then

$$ab = nq + r = (pk_1)q + pk_2$$

$$= p(k_1 q + k_2),$$

which implies that p divides ab.

This contradicts $\gcd(n, ab) = 1$. So, $\gcd(n, r) = 1$. It follows that $r \in U(n)$, and hence $U(n)$ is closed under mult mod n.

(1) Associativity: Let $a, b, c \in U(n)$. We need to show that

$$(ab \bmod n) \cdot c \bmod n$$
$$= a\,(bc \bmod n) \bmod n.$$

Write $(ab \bmod n) = ab + mn$ for some $m \in \mathbb{Z}$. Then $(ab + mn)\,c \bmod n$
$= (ab + mn)c + \ell n = abc + (mc + \ell)n$ for some $\ell \in \mathbb{Z}$. Similarly, $a\,(bc \bmod n) \bmod n$
$= a(bc + kn) + qn = abc + (ak + q)n$

for some $k, q \in \mathbb{Z}$. But ~~that~~ we have

$$abc + (mc+\ell)n \equiv_{\text{mod } n} abc + (ak+q)n.$$

This implies that

$$(ab \bmod n) \cdot c \bmod n = a(bc \bmod n) \bmod n.$$

(2) Identity: For any $a \in U(n)$, we have $a \cdot 1 = 1 \cdot a = a$, and so 1 is the identity in $U(n)$.

(3) Inverses: Let $a \in U(n)$. Then $\gcd(n, a) = 1$. By Bezout's Lemma, $\exists\, s, t \in \mathbb{Z}$ s.t.

$$sa + tn = 1.$$

$$sa = 1 - tn$$

$$sa = 1 \bmod n.$$

It appears that s is our candidate for the mult inverse. However, s may not be among $\{1, \dots, n-1\}$.

But $s \bmod n$ certainly is among $\{1, \dots, n-1\}$. By the Div Alg, $\exists!$ $q, r \in \mathbb{Z}$ s.t.

$$s = nq + r,$$

where $0 \leq r < n$. Then $s \bmod n = r$.

We need to show that $\gcd(n, r) = 1$.

Since $sa + tn = 1$ and $s = nq + r$, we have

$$(nq + r)a + tn = 1$$

$$nqa + ra + tn = 1$$

$$(qa + t)n + ra = 1.$$

By Bezout's Lemma, $\gcd(n, r) = 1$, and so $r \in U(n)$. Moreover, we have

$$ra = 1 - (qa + t)n$$

$$ra \bmod n = 1.$$

Therefore, r is the mult inverse of a. $\square$