Math 214 – Foundations of Mathematics **Homework 3/4** **Sam Harrington**

(Due Tuesday, March 25)

Proposition 6.15: The integer m is odd if and only if there exists $q \in \mathbb{Z}$ such that $m = 2q + 1$.

Proof. (starting with an odd integer) Let $o, q \in \mathbb{Z}$ and o is odd Then,
The set of odd integers $\mathcal{O}$ is defined $\mathbb{Z} - \mathcal{E}$ where:

$$\begin{aligned} \mathcal{E} \text{ is the set defined as } \{x : x \in \mathbb{Z}, 2|x\} \\ \mathcal{E}^c = \mathcal{O} \\ \mathcal{O} \text{ contains all elements where } o \notin \mathcal{E} \end{aligned}$$

Either $o \notin \mathbb{Z}$ or o is not divisible by 2
Since $o \in \mathbb{Z}$ by definition, o must not be divisible by 2
By THM 6.13:

$$o = 2q + r$$

Since $n = 2, r$ is either 0 or 1
When $r = 0, o$ is divisible by 2 so $r \neq 0$
So:

$$o = 2q + 1$$

(starting with $o = 2q + 1$), Let $x, o, q \in \mathbb{Z}$ and $o = 2q + 1$. Then,
If o is even, $o = 2q = 2q + 0$
By THM 6.13, since $r = 0$ when even and for $o, r \neq 0$, o is not even.
Because $o \in \mathbb{Z}$ and not even, it must be odd. So, when $o = 2q + 1$, o is odd
Proving The integer m is odd if and only if there exists $q \in \mathbb{Z}$ such that $m = 2q + 1$. $\square$

COMPLETTED Proposition 6.25: Let $a, a', b, b' \in \mathbb{Z}$ and $n \in \mathbb{N}$. If $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, then $a + b \equiv a' + b' \pmod{n}$ and $ab \equiv a'b' \pmod{n}$.

Proof. Let $a, a', b, b' \in \mathbb{Z}$ and $n \in \mathbb{N}$. Also let $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$. Then,

$$\begin{aligned}
n|(a-a') &\qquad \text{def of } \equiv \\
n|(b-b') &\qquad \text{def of } \equiv \\
a-a' = nx & \\
b-b' = ny & \\
(a-a')+(b-b') = nx+ny & \\
(a+b)-(a'+b') = n(x+y) & \\
n|((a+b)-(a'+b')) & \\
a+b \equiv a'+b' \pmod{n} &\qquad \text{def of } \equiv
\end{aligned}$$

For the second part of the Prop:

$$\begin{aligned}
n|(a-a') &\qquad \text{def of } \equiv \\
n|(b-b') &\qquad \text{def of } \equiv \\
a-a' = nx & \\
b-b' = ny & \\
b(a-a') = bnx & \\
ab-a'b = bnx & \\
b = ny+b' & \\
ab-a'(ny+b') = bnx & \\
ab-a'b'-a'ny = bnx & \\
ab-a'b' = bnx+a'ny & \\
ab-a'b' = n(bx+a'y) & \\
n|(ab-a'b') & \\
ab \equiv a'b' \pmod{n} &\qquad \text{def of } \equiv
\end{aligned}$$

$\square$