More on congruence (mod n)

Group HW 7 task 2

I found this by trial and error:

mod 3: 0 has no inverse

$1^{-1} = 1$ (since $1 \cdot 1 = 1$)

$2^{-1} = 2$ (since $2 \cdot 2 = 4 \equiv 1 \pmod 3$)

mod 4: 0 has no inverse

$1^{-1} = 1$ (since $1 \cdot 1 = 1$)

2 has no inverse (can't multiply anything by 2 and get a remainder of 1 mod 4)

$3^{-1} = 3$ ($3 \cdot 3 = 9 \equiv 1 \pmod 4$)

mod 5: 0 has no inverse

$1^{-1} = 1$ ($1 \cdot 1 = 1$)

$2^{-1} = 3$ ($2 \cdot 3 = 6 \equiv 1 \pmod 5$)

$3^{-1} = 2$

$4^{-1} = 4$ ($4 \cdot 4 = 16 \equiv 1 \bmod 5$)

mod 6: $1^{-1} = 1$

$5^{-1} = 5$

nothing else has inverses

mod 7: 0 has no inverse

$1^{-1} = 1$

$2^{-1} = 4$ ($2 \cdot 4 = 1 \bmod 7$)

$3^{-1} = 5$

$4^{-1} = 2$

$5^{-1} = 3$

$6^{-1} = 6$

mod 8: $1^{-1} = 1$ 0, 2, 4, 6 have no inverses

$7^{-1} = 7$

$3^{-1} = 3$

$5^{-1} = 5$

mod 9 : $1^{-1} = 1$

$8^{-1} = 8$

$2^{-1} = 5$

$4^{-1} = 7$

$7^{-1} = 4$

$5^{-1} = 2$

0, 3, 6 have no inverses mod 9

mod 10 : $1^{-1} = 1$

$3^{-1} = 7$

$7^{-1} = 3$

$9^{-1} = 9$

0, 2, 4, 5, 6, 8 have no inverses mod 10

mod 11 : $1^{-1} = 1$

$2^{-1} = 6$

$3^{-1} = 4$

$4^{-1} = 3$

$5^{-1} = 9$

$6^{-1} = 2$

$7^{-1} = 8$

$8^{-1} = 7$

$9^{-1} = 5$

$10^{-1} = 10$

only 0 has no inverse mod 11

mod 12 : $1^{-1} = 1$

$5^{-1} = 5$

$7^{-1} = 7$

$11^{-1} = 11$

0, 2, 3, 4, 6, 8, 9, 10 have no inverses mod 12

Conjectures:
- If n is prime, all numbers other than 0 have a multiplicative inverse
- If $\gcd(n, k) = 1$, then k has an inverse mod n
- $1^{-1} \equiv 1 \pmod{n}$
- $(n-1)^{-1} \equiv n-1 \pmod{n}$. This makes sense, since $n-1 \equiv -1 \pmod{n}$ and $(-1)\cdot(-1) = 1$.