Number Theory Section Summary: 5.4
Wilson's Theorem

1. Summary

Wilson's theorem provides a mechanism for detecting whether an integer is prime, but because of the factorial function involved, is practically useless! Factorials grow so fast that the numbers involved spin rapidly into the stratosphere....

Check out the interesting story behind this theorem! The comment by Gauss is especially amusing: "notationes versus notiones...." – Can't you just see the great man grumbling?! Then to have Lagrange and Leibniz tied up with the theorem....

2. **Theorems**

Theorem 5.4 (Wilson's Theorem): If p is prime, then

$$(p-1)! \equiv -1(\text{mod p})$$

Exercise #1, p. 101

Converse to Wilson's Theorem): If

$$(p-1)! \equiv -1(\text{mod p})$$

then p is prime.

Exercise #2, p. 101

Theorem 5.5: The quadratic congruence $x^2 + 1 \equiv 0(\text{mod p})$, where p is an odd prime, has a solution if and only if $p \equiv 1(\text{mod } 4)$.

3. Properties/Tricks/Hints/Etc.

Once again we make good use of the result that

$a \equiv b(\text{mod n})$ and $a \equiv b(\text{mod m})$ with gcd(n,m)=1 $\Longrightarrow a \equiv b(\text{mod mn})$

Exercise #6, p. 101 $(p-1)! \equiv p-1 \ (\text{mod } 1+2+\ldots+p-1)$, $\frac{(p-1)\cdot p}{2}$

#2 p 101

$16! \equiv -1 \ (\text{mod } 17)$? If so, 17 is prime.

$16! = 16 \cdot 15 \cdot 14 \cdot 13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$

$$\equiv -1 \cdot -2 \cdot -3 \cdot -4 \cdot -5 \cdot -6 \cdot -7 \cdot -8 \;\; 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \pmod{17}$$

$$\equiv 4 \cdot 5 \cdot 7 \cdot 7 \cdot 5 \cdot 4 \pmod{17}$$

$$\equiv -1 \pmod{17}$$

17 is prime

#11 $x^2 + 1 \equiv 0 \pmod{p}$ has a soln $\iff$

$p \equiv 1 \pmod 4$

$x^2 \equiv -1 \pmod{37}$ $\qquad 37 \equiv 1 \pmod 4$

$x = \pm 6 + n \cdot 37$

$x = 6$ or $x = 31 \; (\equiv -6 \pmod{37})$

$x^2 \equiv -1 \pmod{37} \equiv 36 \pmod{37}$