Math 218: Elementary Number Theory

HOMEWORK 9 : DUE OCTOBER 18

2.2 #13. See the problem writeup in the book. As a kid, you likely learned that 9 divides a number n if and only if the sum of the digits of n is divisible by 9. In this problem, you are proving why that divisibility test works.

2.3 #4. **Without using any computer/calculator aid** calculate $(m-1)!$ mod m for $m = 4$, 5, 8, 9, 10, 12, 14, and 15. You do not need to write many words, but do show me all the steps you use to compute them. Also, be clever and use the arithmetic of congruences to your advantage. No credit will be given if you just multipy out 12! and then find the remainder of that number by division on 12.

2.3 #6. If a is a unit in Z_m, prove that $m - a$ is also a unit in Z_m.

2.3 #8. (a) Prove that if m is composite and greater than 4, then $(m-1)! \equiv 0 \bmod m$.

(b) Use (a) and problem 2.3 #4 above to prove the converse of Wilson's Theorem.

2.3 #11. If p is prime, prove that $(p-2)! \equiv 1 \bmod p$.

2.3 #14. Let p and q be odd primes. Which $a \in Z_{pq}$ are such that $a^2 \equiv 1 \bmod pq$?