Math 321
Number Theory Problem Set #6

Numerical Problems
1. Factor $x^{p-1} - 1$ into linear factors in $\mathbb{Z}_p$ for $p = 3, 5, 7, 11$. Any conjectures?

2. Factor $x^{(p-1)/2} - 1$ into linear factors in $\mathbb{Z}_p$ for $p = 3, 5, 7, 11$.

3. Find all perfect squares in $U_p$ for $p = 3, 5, 7, 11$. Compare your answer with problem 2 above. Any conjectures?

4. A natural number $n$ is said to be a sum of two squares if there is an integral solution $(x, y)$ of the Diophantine equation $x^2 + y^2 = n$. Find all $n$ less than 100 which are sums of two squares. Any conjectures? What structure do these numbers exhibit?

Exploration
5. Do the following examples show that unique prime factorization does not hold in $\mathbb{Z}[i]$?

\[
2 = (1 + i)(1 - i) = i(1 - i)^2; \\
5 = (2 + i)(2 - i) = (1 + 2i)(1 - 2i); \\
4 + 7i = (2 + i)(3 + 2i) = (2 - 3i)(-1 + 2i).
\]

Prove or Disprove and Salvage if Possible (PODASIP)
6. $a|bc$ and $(a, b) = 1 \implies a|c$ for all integers $a, b, c$.

7. If $a|c$, $b|c$ and $(a, b) = 1$ then $ab|c$.

8. For all integers $a, b$, if $p \in \mathbb{Z}$ is prime and $p|ab$ then $p|a$ or $p|b$.

9. An element $a$ in $\mathbb{Z}_m$ is a unit $\iff (a, m) = 1$.

10. Every integer $> 1$ is a product of positive primes.

For Fun
10. Prove that $n$ is a multiple of 3 if and only if the sum of the digits of $n$ is a multiple of 3. Prove that $n$ is a multiple of 9 if and only if the sum of the digits of $n$ is a multiple of 9. Hint: think “modularly”. Can you come up with an analogous statement for multiples of 11?