Peter Cholak and Juan Migliore Math 222 Monday, February 19, 2001
Quiz 3

Be sure to carefully write up your answers. It is suggested that you first write out a draft of your proposed questions and then carefully rewrite that draft to get your final version. You do *not* have to write the answers on this sheet of paper.

Consider the set of integers modulo 10, $\mathbb{Z}_{10}$.
(a) Identify the additive inverse of each element in $\mathbb{Z}_{10}$.
(b) Identify those elements that have a multiplicative inverse and what their inverses are.

Solution. (a) The additive inverse of j is $10 - j$ for $j \in \mathbb{Z}_{10}$.

(b) Each of $1, 3, 7, 9$ has a multiplicative inverse. The inverse of 1 is 1, the inverse of 3 is 7, the inverse of 7 is 3 and the inverse of 9 is 9.

Let n be a positive integer and consider the sum $1 + 2 + 3 + \ldots + (n-1)$ modulo n. Show that if n is odd, this sum is zero in $\mathbb{Z}_n$ and if n is even then the sum is $n/2$ in $\mathbb{Z}_n$. *Hint:* Use the formula for this sum which we saw when discussing induction.

Solution. We know that $S = 1 + 2 + 3 + \ldots + (n-1) = \frac{n(n-1)}{2}$. If n is odd, then $k = \frac{n-1}{2} \in \mathbb{Z}$ and hence $S = kn \equiv_n 0$, that is, S is zero in $\mathbb{Z}_n$. If n is even, say $n = 2m$, then $S = (n-1)m \equiv_n nm - m \equiv_n -m \equiv_n m \equiv_n \frac{n}{2}$, so S is $n/2$ in $\mathbb{Z}_n$.

In $\mathbb{Z}_{66}$, consider the elements 6, 8, 9, 15, 35 and 55. Identify the one that has a multiplicative inverse in $\mathbb{Z}_{66}$ and find that inverse.
Solution. The only one whose greatest common divisor with 66 is 1 is 35. (The other greatest common divisors are, respectively, 6, 2, 3, 3 and 11.) Using the Euclidean algorithm we get

$$\begin{aligned} 66 &= 1(35) + 31 \\ 35 &= 1(31) + 4 \\ 31 &= 7(4) + 3 \\ 4 &= 1(3) + 1. \end{aligned}$$

Hence $1 = 4 - 1(3) = 4 - [31 - 7(4)] = -31 + 8(4) = -31 + 8[35 - 31] = -9(31) + 8(35) = -9[66 - 35] + 8(35) = -9(66) + 17(35)$. So the multiplicative inverse of 35 in $\mathbb{Z}_{66}$ is 17.

Prove that if p is a prime and $\alpha, \beta \in \sqrt[p]{1}$ and $\alpha \neq 1$ then there exists an integer m such that $\alpha^m = \beta$. (Hints: First, write $\alpha = \zeta^k$ and $\beta = \zeta^r$ where ζ is the first pth roof of unity. Second, do k and r have multiplicative inverses in $\mathbb{Z}_p$?)
Proof. Write $\alpha = \zeta^k$ and $\beta = \zeta^r$ with $0 \leq k, r < p$ and ζ the first pth root of unity. By the assumption $\alpha \neq 1$, we have $0 < k < p$. By Proposition 4.3, k has a multiplicative inverse, say l, in $\mathbb{Z}_p$. Then $kl = qp + 1$ for some $q \in \mathbb{Z}$. Let $m = lr$. Then