

**Homework 4**

due Monday, February 8, in class

Hand in:

From the text:

Section §1.4 #10, 12, 24, 28 (5 pts each)

10. Let  $(a, n) = 1$ . If  $[a]$  has multiplicative order  $k$  in  $\mathbf{Z}_n^\times$ , show that  $k \mid \varphi(n)$ .
12. We say that the set of units  $\mathbf{Z}_n^\times$  of  $\mathbf{Z}_n$  is **cyclic** if it has an element of multiplicative order  $\varphi(n)$ . Show that  $\mathbf{Z}_{10}^\times$  and  $\mathbf{Z}_{11}^\times$  are cyclic, but  $\mathbf{Z}_{12}^\times$  is not.
24. Show that if  $p$  is a prime number, then the congruence  $x^2 \equiv 1 \pmod{p}$  has only the solutions  $x \equiv 1$  and  $x \equiv -1$ .
28. Prove that if  $\gcd(m, n) = 1$ , then  $n^{\varphi(m)} + m^{\varphi(n)} \equiv 1 \pmod{mn}$ .

Recommended (don't hand these in, since the solutions are available):

From the Study Guide: page 15 §1.4 #32, 34, 35, 38, 39

32. Find the multiplicative inverse of each nonzero element of  $\mathbf{Z}_{13}$ .
34. Find the multiplicative order of each element of  $\mathbf{Z}_9^\times$ .
35. Find  $[91]_{501}^{-1}$ , if possible (in  $\mathbf{Z}_{501}^\times$ ).
38. In  $\mathbf{Z}_{24}$ : find all units (list the multiplicative inverse of each); find all idempotent elements; find all nilpotent elements.
39. Show that  $\mathbf{Z}_{17}^\times$  is cyclic.