

**book problems**

§9.3 # 1(a),(c),(e), 2, 5, 9

§10.3 #2

§11.2 # 1, 2, 3, 8, 16

**Non-book problem:**

1. For any prime  $p$  and any integer  $a$  such that  $\gcd(a, p) = 1$ , say that  $a$  is a *cubic residue* of  $p$  if  $x^3 \equiv a \pmod{p}$  has at least one solution. Prove the following statements.
  - a. If  $p$  is of the form  $3k + 2$  then all integers in a reduced residue system modulo  $p$  are cubic residues.
  - b. If  $p$  is of the form  $3k + 1$  only one third of the members of a reduced residue system are cubic residues.

**Extra credit problem:**

Prove that if  $r$  is a quadratic residue modulo  $m > 2$ , then  $r^{\phi(m)/2} \equiv 1 \pmod{m}$ . Note:  $m$  may be composite.