

Unless otherwise specified, the problems listed below are from *Discrete Mathematics and Its Applications, Sixth Ed.*, by Kenneth H. Rosen.

1. Prove that multiplication is well defined on the integers modulo  $n$ . In other words, prove that if  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$  then  $ac \equiv bd \pmod{m}$ .
2. Prove that if  $a, b \in \mathbb{Z}$  with  $b$  not zero, then  $\gcd(a, b) = \gcd(b, a \% b)$ . (Note that  $x \% y$  means “the remainder when  $x$  is divided by  $y$ .” Note also that the point of this problem is to prove a step in the Euclidean algorithm, so don’t assume the Euclidean algorithm works inside your proof.)
3. section 3.5 problems: 15, 32
4. section 3.7 problems: 16, 17, 18, 20, 40