pg 5

5. Use the algorithm from the textbook to find the four square roots of 37 in Z_{77}

$77 = 7 \cdot 11$ $\quad x^2 \equiv 37 \bmod 7$ $\quad x^2 = 37 \bmod 11$

$3 = 3 \bmod 4$ ✓ $\quad 11 = 3 \bmod 4$ ✓

$\pm 37^{(7+1)/4}$ $\quad \pm 37^{(11+1)/4}$

$\pm 37^2 \bmod 7$ $\quad \pm 37^3 \bmod 11$

$(1369, -1369) \bmod 7$ $\quad (50653, -50653) \bmod$

$(4, 3)$ $\quad 9, 2$

a $x = 4 \bmod 7$
$x \equiv 9 \bmod 11$

c $x \equiv 4 \bmod 7$
$x \equiv 2 \bmod 11$

b $x \equiv 3 \bmod 7$
$x \equiv 9 \bmod 11$

d $x \equiv 3 \bmod 7$
$x \equiv 2 \bmod 11$

(a) $4 + 7k = 9 \bmod 11$
$7^{-1} \cdot 7k = 5 \cdot 7 \bmod 11$
$k = 55 \bmod 11$
$k = 55 + 11j$
$x = 4 + 7(55 + 11j)$
$x = 389 + 77j$
(389)

(b) $3 + 7k = 9 \bmod 11$
$7k = 6 \bmod 11$
$k = 66 \bmod 11$
$k = 66 + 11j$
$x = 3 + 7(66 + 11j)$
$x = 465 + 77j$
(465)