Problem 1.1.7 - (a) and (b) - (6 points):

```
def bezout(n,m):
    #returns [x,y] s.t. nx+my = 1 if a,b are any coprime integers
    n_buffer = False

    s_n = 1
    s_m = 1

    if n < 0:
        s_n = -1
        n = abs(n)
    if m < 0:
        s_m = -1
        m = abs(m)

    if m > n:
        n_buffer = n
        n = m
        m = n_buffer

    a = [n, m]
    q = []

    n = 0
    while a[len(a)-1] != 0:
        a.append(a[n] % a[n+1])
        q.append(a[n] // a[n+1])
        n += 1

    x = len(a) * [0]

    x[n] = 1
    x[n+1] = 0

    i = n-1
    while i >= 0:
        x[i] = x[i+2]
        x[i+1] = x[i+1] - q[i] * x[i+2]
        i -= 1
    if n_buffer:
        return(s_m * x[1], s_n * x[0])
    else:
        return(s_n * x[0], s_m * x[1])
```

Running it on $(n, m) = (12345678901, 10987654321)$ gives $(x, y) = (3733873449, -4195363388)$.

Problem 1.1.5 - (3 points):

```
def euclid(a,b):

while True:
    if a%b == 0:
        return(b)
    else:
        b_buffer = a%b
        a = b
        b = b_buffer
        continue
```

```
euclid(1027,1738)
```

The output was 79. Now we have $\frac{1}{79}(1027, 1738) = (13, 22)$ and running bezout(13,22) from the previous problem we get $(-5, 3)$ so $13 \cdot (-5) + 22 \cdot 3 = 1$ and then

$$(13 \cdot 79) \cdot (-5) + (22 \cdot 79) \cdot 3 = 1027 \cdot (-5) + 1738 \cdot 3 = 79 = \gcd(1027, 1738)$$

so $(\gcd(1027, 1738), x, y) = (79, -5, 3)$ works.

Problem 1.1.1 - (1 point): Looking at the quadratic residues modulo 4 we find

$$0^2 \equiv 0, 1^2 \equiv 1, 2^2 \equiv, 3^2 \equiv 1 \pmod 4$$

so for any $x, y \in \mathbb{Z}$, we have $x^2, y^2 \in \{0, 1\} \pmod 4$, so

$$x^2 + y^2 \in \{0, 1, 2\} \pmod 4$$

and hence $x^2 + y^2 \not\equiv 3 \equiv n \pmod 4$.