1) a) Suppose that $p$ is a prime factor of $n^2 + 3$. Then

$$n^2 + 3 \equiv 0 \pmod{p}$$

$$n^2 \equiv -3 \pmod{p}$$

$$\Rightarrow \left( \frac{-3}{p} \right) = 1.$$ 

Now, since $n^2 + 3$ is odd, either $p \equiv 1 \pmod{4}$ or $p \equiv 3 \pmod{4}$.

If $p \equiv 1 \pmod{4}$, then

$$\left( \frac{-3}{p} \right) = \left( \frac{-1}{p} \right) \cdot \left( \frac{3}{p} \right) = 1 \cdot \left( \frac{p}{3} \right) = \left( \frac{p}{3} \right)$$

while if $p \equiv 3 \pmod{4}$, then

$$\left( \frac{-3}{p} \right) = \left( \frac{-1}{p} \right) \cdot \left( \frac{3}{p} \right) = (-1) \cdot \left[ \left( \frac{p}{3} \right) \right] = \left( \frac{p}{3} \right).$$

In either case, it follows that $\left( \frac{p}{3} \right) = 1$. Now, the only quad. residue mod 3 is 1, so $p \equiv 1 \pmod{3}$ as desired.

b) Suppose that $q_1, q_2, \ldots, q_e$ is any list of prime numbers that are all $1 \pmod{3}$. Then let

$$N = (2q_1 q_2 \ldots q_e)^2 + 3.$$ 

Since $2q_1 q_2 \ldots q_e$ is even and not divisible by 3, it follows from part (a) that all prime factors of $N$ are $1 \pmod{3}$.

Let $p$ be any prime factor of $N$. Then $p$ cannot equal any of $q_1, q_2, \ldots, q_e$ since otherwise $p$ divides $N - (2q_1 q_2 \ldots q_e)^2 = 3$, which is impossible. So $p$ is a new prime congruent to $1 \pmod{3}$ that isn't on our list.

This shows that no finite list exhausts the $1 \pmod{3}$ primes, hence there are infinitely many of them.
2) Since $31 - 1 = 2 \cdot 3 \cdot 5$, to check if a number $a$ is a prim. root it's enough to check whether

$$a^{\frac{30}{2}} = a^{15}$$

$$a^{\frac{30}{3}} = a^{10}$$

and

$$a^{\frac{30}{5}} = a^6$$

are all $\not\equiv 1 \mod 31$. We can find one p.r. by trying values.

$a = 2$ By successive squaring:

<table>
<thead>
<tr>
<th>$a$</th>
<th>$a^2$</th>
<th>$a^4$</th>
<th>$a^8$</th>
<th>$a^9$</th>
<th>$a^{16}$</th>
<th>$a^{32} \equiv 1$</th>
<th>$a^{30} \equiv 1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>4</td>
<td>16</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

(or we could just notice early that $a^5 \equiv 1$ & stop)

so 2 is not a prim. root.

$a = 3$ By succ. squaring:

<table>
<thead>
<tr>
<th>$a$</th>
<th>$a^2$</th>
<th>$a^4$</th>
<th>$a^8$</th>
<th>$a^{16}$</th>
<th>$a^{32} \equiv -5$</th>
<th>$a^{30} \equiv 25 \equiv -6$</th>
<th>$a^{31} \equiv (-5)(-6) \equiv 30$</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>9</td>
<td>81</td>
<td>1</td>
<td>81</td>
<td>31</td>
<td>31</td>
<td>31</td>
</tr>
</tbody>
</table>

$\equiv -5$

Since $a^6, a^{10}, a^{15}$ are all $\not\equiv 1 \mod 31$, 3 is a prim. root.

To find the others, we recall that they are

$$\{ g^e \mod 31 : \gcd(e, 30) = 1 \}.$$
The numbers in \{11, \ldots, 30\} coprime to 30 are:

1, 7, 11, 13, 17, 19, 23, 29

so the primitive roots are:

3', 3^2, 3^3, 3^4, 3^5, 3^6, 3^7, 3^8 \mod 31.

To compute these quickly, you can first write:

3' \equiv 3 \quad 3^2 \equiv 9 \quad 3^4 \equiv \frac{1}{3} - 12 \quad 3^8 \equiv -11 \quad 3^6 \equiv -3

then compute:

3^1 \equiv 3
3^2 = 3^1 \cdot 3 \equiv 3 \cdot 9 \cdot (-12) = (-4) \cdot (-12) \equiv 48 \equiv -17
3^3 = 3^2 \cdot 3 \equiv (-11) \cdot 9 \cdot 3 \equiv (-6)3 = 18
3^4 = 3^3 \cdot 3 \equiv (-11) \cdot (-12) \cdot 3 \equiv 8 \cdot 3 \equiv 24
3^5 = 3^4 \cdot 3 \equiv (-3) \cdot 3 \equiv -9 \equiv 22
3^6 = 3^5 \cdot 3 \equiv (-3) \cdot 9 \cdot 3 \equiv 4 \cdot 3 \equiv 12
3^7 = 3^6 \cdot 3 \equiv (-3) (-12) \cdot 9 \cdot 3 \equiv 6 \cdot 3 \equiv 18
3^8 = 3^7 \cdot 3 \equiv (-3) (-11) \cdot (-12) \cdot 3 \equiv (4)(4) \cdot 3 \equiv 11
3^9 \equiv 3^{10} \equiv 21

so the prim. roots are 3, 17, 13, 24, 22, 12, 11, and 21.

On, in sorted order, 3, 11, 12, 13, 17, 21, 22, and 24.

(3) Since \(c_i \equiv g^{a_i} \mod p\), and Bob knows \(b\), he can compute the remainder when \(c_b\) is divided by \(p\). Call this \(s\). Then:

\[ s \equiv (c^b) \equiv (g^a)^b \equiv g^{ab} \mod p. \]

b) Using the euclidean algorithm, Bob can find an inverse of \(s\) mod \(p\), i.e. an integer such that

\[ st \equiv 1 \mod p. \]
Now, since \( y^a \equiv (g^b)^a \equiv g^{ab} \equiv s \mod p \), it follows that
\[
y^a \cdot t \equiv st \equiv 1 \mod p.
\]
So Bob can compute \( c_2 \cdot t \equiv s \mod p \). Thus is the message \( m \), since
\[
c_2 \cdot t \equiv m \cdot y^a \cdot t \mod p
\]
\[
\equiv m \cdot (st) \mod p
\]
\[
\equiv m \mod p.
\]

\( c) \) Using the above procedure:

\[
b = 42
\]
\[
c_1 = 75
\]
\[
c_2 = 38
\]

So \( s = c_1^b \equiv 75^{42} \mod 101 \).

Using successive squaring (and a computer to multiply and to compute remainders):

\[
75^2 \equiv 70
\]
\[
75^4 \equiv 70^2 \equiv 52
\]
\[
75^8 \equiv 52 \cdot 75 \equiv 62
\]
\[
75^{10} \equiv 62^2 \equiv 6
\]
\[
75^{20} \equiv 6^2 \equiv 36
\]
\[
75^{21} \equiv 36 \cdot 75 \equiv 74
\]
\[
75^{42} \equiv 74^2 \equiv 22
\]

So \( s = 22 \equiv g^{ab} \mod p \). Now, the inverse \( t \) of \( s \) can be found with the Euclidean algorithm:

\[
\begin{align*}
\text{lcm} &= 101
\end{align*}
\]
\[
9 = 22 - 13 = 5 \cdot (22) - (101)
\]
\[
4 = 13 - 9 = 2 \cdot (101) - 9 \cdot (22)
\]
\[
1 = 9 - 2 \cdot 4 = 5 \cdot (22) - (101) - 4 \cdot (101) + 18(22) = 23(22) - 5(101)
\]
So \(23 \cdot 22 \equiv 1 \mod 101\), so \(t = 23\) is the inverse of \(s\). Thus

\[
m = C_2 \cdot t \mod 101
\]

\[
\equiv 38 \cdot 23 \mod 101
\]

\[
\equiv 66 \mod 101 \quad (\text{w/ calculator}).
\]

So the original message was \(m = 66\).