P. Set 11 Solutions

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

$$n^2+3 \equiv 0 \bmod p$$

$$n^2 \equiv -3 \bmod p$$

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

Now, since n^2+3 is odd, either $p \equiv 1 \bmod 4$ or $p \equiv 3 \bmod 4$.
If $p \equiv 1 \bmod 4$, 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 $p \equiv 3 \bmod 4$, then $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)\cdot\left[-\left(\frac{p}{3}\right)\right] = \left(\frac{p}{3}\right)$.

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

b) Suppose that $q_1, q_2, \cdots, q_\ell$ is any list of ~~odd~~ prime numbers that are all $1 \bmod 3$. Then let

$$N = (2q_1 q_2 \cdots q_\ell)^2 + 3.$$

Since $2q_1 \cdots q_\ell$ is even and not divis. by 3, it follows from part (a) that all prime factors of N are $1 \bmod 3$.

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

This shows that no finite list exhausts the $1 \bmod 3$ 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

$$a^{\frac{30}{2}} = a^{15}$$
$$a^{30/3} = a^{10}$$
and $$a^{30/5} = a^{6}$$

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

$\underline{a=2}$ By successive squaring:

$a\equiv 2$	$a\equiv 2$	$a\equiv 2$
$a^2\equiv 4$	$a^2\equiv 4$	$a^2\equiv 4$
$a^3\equiv 8$	$a^4\equiv 16$	$a^4\equiv 16$
$\underline{a^6\equiv 64\equiv 2}$	$a^5\equiv 32\equiv 1$	$a^5\equiv 1$
	$\underline{a^{10}\equiv 1}$	$a^{10}\equiv 1$
		$\underline{a^{15}\equiv 1}$

(or we could just notice early that $a^5\equiv 1$ & stop)
so 2 is <u>not a prim. root</u>.

$\underline{a=3}$ By succ. squaring:

$a\equiv 3$	$a\equiv 3$	$a^5\equiv -5$
$a^2\equiv 9$	$a^2\equiv 9$	$a^{10}\equiv 25\equiv -6$
$a^3\equiv 27\equiv -4$	$a^4\equiv 81\equiv 19$	$a^{15}\equiv(-5)(-6)\equiv 30$
$\underline{a^6\equiv 16}$	$a^5\equiv 3\cdot 19\equiv 57$	$\underline{\equiv -1}$
	$\equiv -5$	
	$\underline{a^{10}\equiv 25}$	

Since a^6, a^{10}, a^{15} are all $\not\equiv 1 \bmod 31$, <u>3 is a prim. root</u>.

To find the others, ~~no~~ recall that they are

$$\{g^e \bmod 31 : \gcd(e,30)=1\}.$$

The numbers in $\{1, \cdots, 30\}$ coprime to 30 are:

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

so the primitive roots are:

$3^1, 3^7, 3^{11}, 3^{13}, 3^{17}, 3^{19}, 3^{23}, 3^{29} \bmod 31.$

To compute these quickly, you can first write:

$3^1 \equiv 3 \quad 3^2 \equiv 9 \quad 3^4 \equiv -12 \quad 3^8 \equiv -11 \quad 3^{16} \equiv -3$

then compute:

$$\begin{aligned}
3^1 &\equiv 3 \\
3^7 &\equiv 3^1 \cdot 3^2 \cdot 3^4 \equiv 3 \cdot 9 \cdot (-12) \equiv (-4)(-12) \equiv 48 \equiv 17 \\
3^{11} &\equiv 3^8 \cdot 3^2 \cdot 3^1 \equiv (-11) \cdot 9 \cdot 3 \equiv (-6)3 \equiv 13 \\
3^{13} &\equiv 3^8 \cdot 3^4 \cdot 3^1 \equiv (-11)(-12) \cdot 3 \equiv 8 \cdot 3 \equiv 24 \\
3^{17} &\equiv 3^{16} \cdot 3^1 \equiv (-3) \cdot 3 \equiv -9 \equiv 22 \\
3^{19} &\equiv 3^{16} \cdot 3^2 \cdot 3^1 \equiv (-3) \cdot 9 \cdot 3 \equiv 4 \cdot 3 \equiv 12 \\
3^{23} &\equiv 3^{16} \cdot 3^4 \cdot 3^2 \cdot 3^1 \equiv (-3)(-12) \cdot 9 \cdot 3 \equiv (5) 9 \cdot 3 \equiv 14 \cdot 3 \equiv 11 \\
3^{29} &\equiv 3^{16} \cdot 3^8 \cdot 3^4 \cdot 3^1 \equiv (-3)(-11) \cdot (-12) \cdot 3 \equiv (+2)(-12) \cdot 3 \equiv (+7) \cdot 3 \equiv 21
\end{aligned}$$

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

Or, in sorted order, $\boxed{3, 11, 12, 13, 17, 21, 22, \text{ and } 24.}$

3

a) Since $c_1 \equiv g^a \bmod p$ and Bob knows b, he can compute the remainder when c_1^b is divided by p. Call this s. Then:

$$s \equiv (c_1^b) \equiv (g^a)^b \equiv g^{ab} \bmod p.$$

b) Using the euclidean algorithm, Bob can find an inverse t of $s \bmod p$, ie. an integer such that

$$st \equiv 1 \bmod p.$$

Now, since $y^a \equiv (g^b)^a \equiv g^{ab} \equiv s \bmod p$, it follows that

$$y^a \cdot t \equiv st \equiv 1 \bmod p.$$

So Bob can compute $c_2 \cdot t \% p$. This is the message m, since

$$c_2 \cdot t \equiv m \cdot y^a \cdot t \bmod p$$

$$\equiv m \cdot (st) \bmod p$$

$$\equiv m \bmod p.$$

c) Using the above procedure:

$b = 42$
$c_1 = 75$
$c_2 = 38$

So $s \equiv c_1^b \equiv 75^{42} \bmod 101$.

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

$75^2 \equiv 70$
$75^4 \equiv 70^2 \equiv 52$
$75^5 \equiv 52 \cdot 75 \equiv 62$
$75^{10} \equiv 62^2 \equiv 6$
$75^{20} \equiv 6^2 \equiv 36$
$75^{21} \equiv 36 \cdot 75 \equiv 74$
$75^{42} \equiv 74^2 \equiv 22$

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

101 22
$13 = (101) - 4(22)$
$9 = 22 - 13 = 5 \cdot (22) - (101)$
$4 = 13 - 9 = 2 \cdot (101) - 9 \cdot (22)$
$1 = 9 - 2 \cdot 4 = 5 \cdot (22) - (101) - 4(101) + 18(22) = 23(22) - 5(101)$

So $23 \cdot 22 \equiv 1 \bmod 101$. so $t = 23$ is the inverse of s. Thus

$$m \equiv c_2 \cdot t \mod 101$$
$$\equiv 38 \cdot 23 \mod 101$$
$$\equiv 66 \mod 101 \quad \text{(w/ calculator)}.$$

So the original message was $\boxed{m = 66}$.