A

1. $b^2 - 4ac$ is a quadratic residue mod N, so there exists a natural r such that $r^2 = b^2 - 4ac$.

$$ax^2 + bx + c \equiv 0[N]$$
$$\Leftrightarrow \quad a[(2a)^{-1}]^2[-b \pm r]^2 + b[-b \pm r][2a]^{-1} + c \equiv 0\ [N]$$
$$\Leftrightarrow \quad [4a]^{-1}[b^2 \mp 2br + r^2] + [-b\text{^}2 \pm \mathrm{b}r][2a]^{-1} + c \equiv 0\ [N]$$
$$\Leftrightarrow \quad [4a]^{-1}[2b^2 \mp 2br - 4ac] + [-b\text{^}2 \pm br][2a]^{-1} + c \equiv 0\ [N]$$
$$\Leftrightarrow \quad [2a]^{-1}[b^2 \mp br - 2ac] + [-b\text{^}2 \pm br][2a]^{-1} + c \equiv 0\ [N]$$
$$\Leftrightarrow \quad [2a]^{-1}[b^2 \mp br - 2ac - b\text{^}2 \pm br] + c \equiv 0\ [N]$$
$$\Leftrightarrow \quad [2a]^{-1}[2a][-c] + c \equiv 0\ [N]$$
$$\Leftrightarrow \quad -c + c \equiv 0\ [N]$$
$$\Leftrightarrow \quad 0 \equiv 0\ [N]$$

2. Necessary conditions for existance of solutions : the determinant $\sqrt{b^2 - 4ac}$ mod N exists
X is a solution to the system if $2ax \equiv -b \pm \sqrt{b^2 - 4ac}\ [N]$
Let $g = \gcd(2a, N)$
If g doesn't divide $-b \pm \sqrt{b^2 - 4ac}$ then there is no solution.
So let's assume that g divides $-b \pm \sqrt{b^2 - 4ac}$
If a=0 this is a linear equation, there are gcd(b,N) solutions.
If $N = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, let P={$p_1, p_2, \dots, p_k$} (p's are prime)
If g doesn't belong to P then there are 2^k solutions.(found through the Chinese remainder theorem with 2^k systems of equations)
If g belongs to P, $g = p_i$, then $2ax \equiv -b \pm \sqrt{b^2 - 4ac}\ [p_i]$ has p_i-1 solutions. So we have $2^{k-1}(p_i - 1)$ solutions
If g is the product of multiple elements in P, $g = p_i \dots p_j$, then there are $2^{k-t} * \sum_{l=i}^{j}(p_l - 1)$ solutions.

B

1. First let's compute the probability of finding a composite number :
There are $\frac{(2-1)*(3-1)*(5-1)*(7-1)*N}{210} = \frac{48N}{210} = \frac{8N}{35}$ numbers x between 0 and N that have gcd(x,210)=1
There are $\pi(N)$ primes smaller than N.
So there are $\frac{8N}{35}$ - $\pi(N)$ composite numbers x such that gcd(x,210)=1 and 1<x≤N
Thus the probability of getting a composite number is $\frac{\frac{8N}{35} - \pi(N)}{\frac{8N}{35}} = 1 - \frac{\pi(N)}{\frac{8N}{35}} = 1 - \frac{35\pi(N)}{8\mathrm{N}}$
We know the probability of returning "prime" is O($\frac{1}{4^t}$)
By the prime number theorem $\pi(N) = \frac{N}{m} log_2 e$
So we get the following bound for outputting a composite number instead of a prime after the two events :
O[($1 - \frac{35}{8\mathrm{N}} * \frac{N}{m} log_2 e) * \frac{1}{4^t}$] = O[($1 - \frac{35}{8\mathrm{m}} log_2 e) * \frac{1}{4^t}$]

2.

To guarantee a probability at most $\frac{1}{2\text{^}50} = \frac{1}{4\text{^}25}$ of outputting a composite number with m=4096 we need to have :

$$(1 - \frac{35}{8\mathrm{m}} log_2 e) * \frac{1}{4^t} \leq \frac{1}{4^{25}}$$

$$<=> \frac{4^t}{\left(1 - \frac{35}{8\mathrm{m}} log_2 e\right)} \leq 4^{25}$$

$$<=> 4^t \leq 4^{25} * \left(1 - \frac{35}{8\mathrm{m}} log_2 e\right)$$

$$<=> t * log(4) \leq 25 * \log(4) + log\left(1 - \frac{35}{8\mathrm{m}} log_2 e\right)$$

$$<=> t \leq 25 + \frac{log\left(1 - \frac{35}{8\mathrm{m}} log_2 e\right)}{\log(4)}$$

$$<=> t \leq 26$$

C

1. The probability Miller-Rabin declares prime for both q and p is 4^{-2t} so on average to get a prime we will run the algorithm 4^{2t} times. Miller Rabin runs in O(m^3t) so we can expect a running time of $O(4^{2t} * m^3 t)$ for the first step.
   The probability of getting a primitive element g of $\mathbb{F}_p$ is $\frac{\phi(p-1)}{p-1}$, so on average to get a primitive number we will run the random primitive element algorithm $\frac{p-1}{\phi(p-1)}$.
   From the formula that we assume true we get : $\frac{\log\log N}{e^{-\gamma}} \geq \frac{p-1}{\phi(p-1)}$.
   Moreover p-1=2*q which is a prime factorization so the algorithm runs in O(1).
   Thus the second step runs in $O(\frac{\log\log N}{e^{-\gamma}})$
   I am going to assume that $log\ N = \frac{e^{-\gamma}}{m}$ so that I can express the running time without N.
   So log $log\ N = -\gamma - \log m$
   The total running time is : $O(\frac{-\gamma - \log m}{e^{-\gamma}} + 4^{2t} * m^3 t)$

2. $P_{m,t}$ is the probability that Miller-Rabin(N,t) with gcd(N,210)=1 outputs 'prime' for p but p is composite.

To guarantee a probability at most $\frac{1}{2\text{^}50} = \frac{1}{4\text{^}25}$ of outputting a number which is not a Sophie-Germain prime with m=4096 we need to have:

$prob\ of\ q\ being\ a\ false\ prime + prob\ of\ p\ being\ a\ false\ prime +$
$prob\ of\ returning\ composite \leq 4^{-25}$

$P_{m,t} + P_{m,t} + 1 - 4^{-t} \leq 4^{-25}$
$P_{m,t} + P_{m,t} + 1 - 4^{-t} \leq 4^{-25}$
$2P_{m,t} - 4^{-t} \leq 4^{-25} - 1$
$-4^{-t} \leq 4^{-25} - 1 - 2P_{m,t} \leq \ 4^{-25}$
$4^{t} \leq 4^{25}$
$t \leq \log(4^{25}) \approx 25$

D

1. First let's show that if p is 3 mod 4 then r will always be odd when first computed:

$$p \equiv 3\ [4] \quad <=> \quad p-1 \equiv 2\ [4] \quad <=> \quad r\ = \frac{p-1}{2} \equiv 1\ [4]$$

Therefore r must be odd since any even number is 0 or 2 mod 4.

Thus the algorithm will not enter the while loop and directly return $a^{\frac{r+1}{2}}[p]$.

$\frac{r+1}{2} = \frac{\frac{p-1}{2}+1}{2} = \frac{p+1}{4}$

The algorithm will return $a^{\frac{p+1}{4}}[p]$.

2. $(g^n)^{q-1} = (g^{q-1})^n = 1^n = 1$ since $g^{q-1} = 1$
And $(g^n)^{m_i} = (g^{m_i})^n \neq 1^n = 1$ for all 1≤i≤k, since $g^{mi} \neq 1$
Therefore by the theorem g^n is a primitive of $\mathbb{F}q$

E

1.

s = 260 720 767, S={s,-s,3s,-3s}
N = 262 915 409= 16111*16319 =p*q
16111 and 16319 are both primes where $161111 \equiv 3[4]$ and $16319 \equiv 3[4]$
We use these to find which elements of S are quadratic residues mod N by extracting their square roots.
Let's find $r_p \equiv s_i^{(p+1)/4}[p]$ and $r_q \equiv s_i^{(q+1)/4}[q]$ These will hold if s_i is a quadratic residue
$r_p \equiv s^{4028}[16111]$ $r_p \equiv -s^{4028}[16111]$ $r_p \equiv 3s^{4028}[16111]$ $r_p \equiv -3s^{4028}[16111]$
$r_p \equiv 3785[16111]$ $r_p \equiv 3785[16111]$ $r_p \equiv 8188[16111]$ $r_p \equiv 8188[16111]$

$r_q \equiv \pm s^{4080}[16319]$ $r_q \equiv \pm 3s^{4080}[16319]$
$r_q \equiv 3955[16319]$ $r_q \equiv 593[16319]$

We use the Chinese Remainder Theorem to solve the four systems:
$r \equiv r_p[p]$ and $r \equiv r_q[q]$
$r \equiv -r_p[p]$ and $r \equiv r_q[q]$
$r \equiv r_p[p]$ and $r \equiv -r_q[q]$
$r \equiv -r_p[p]$ and $r \equiv -r_q[q]$

For $\pm s$:
$r \equiv 3785[16111]$ and $r \equiv 3955[16319]$
r ≡ 3785*16319*6274 + 3955*16111*9964 [N]

r ≡ 209 817 338 [N]
$r \equiv -3785[16111]$ and $r \equiv 3955[16319]$
r ≡ -3785*16319*6274 + 3955*16111*9964 [N]
r ≡ 226 919 650 [N]

$r \equiv 3785[16111]$ and $r \equiv -3955[16319]$
r ≡ 3785*16319*6274 + -3955*16111*9964 [N]
r ≡ 35 995 759 [N]

$r \equiv -3785[16111]$ and $r \equiv -3955[16319]$
r ≡ -3785*16319*6274 + -3955*16111*9964 [N]
r ≡ 53 098 071 [N]

For $\pm 3s$:
$r \equiv 8188[16111]$ and $r2 \equiv 593[16319]$
r ≡ 8188*16319*6274 + 593*16111*9964 [N]
r ≡ 176 294 750 [N]

$r \equiv -8188[16111]$ and $r2 \equiv 593[16319]$
r ≡ -8188*16319*6274 + 593*16111*9964 [N]
r ≡ 124 449 287 [N]

$r \equiv 8188[16111]$ and $r2 \equiv -593[16319]$
r ≡ 8188*16319*6274 + -593*16111*9964 [N]
r ≡ 138 466 122 [N]

$r \equiv -8188[16111]$ and $r2 \equiv -593[16319]$
r ≡ -8188*16319*6274 + -593*16111*9964 [N]
r ≡ 86 620 659 [N]

We get that only (176294750)^2 ≡ $3s \equiv 256331483[N]$
Therefore 3s is a quadratic residue.

2. The square roots are $\pm 176294750\ [N]$

3. $y \in \{x, -x, 3x, -3x\}$, gcd(x,N)=1
y is a quadratic residue mod N if and only if $\left(\frac{y}{p}\right) = \left(\frac{y}{q}\right) = 1$. *NB: same p and q as question 1*
We have : $\left(\frac{-1}{16111}\right) = (-1)^{8055} = -1$, $\left(\frac{-1}{16319}\right) = (-1)^{8159} = -1$,
$\left(\frac{3}{16111}\right) \equiv 3^{8055}[16111] = -1$, $\left(\frac{3}{16319}\right) \equiv 3^{8159}[16319] = 1$

$\left(\frac{-x}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{x}{p}\right) = -\left(\frac{x}{p}\right)$, $\left(\frac{3x}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{x}{p}\right) = -\left(\frac{x}{p}\right)$, $\left(\frac{-3x}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)\left(\frac{x}{p}\right) = \left(\frac{x}{p}\right)$
$\left(\frac{-x}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{x}{q}\right) = -\left(\frac{x}{q}\right)$, $\left(\frac{3x}{q}\right) = \left(\frac{3}{q}\right)\left(\frac{x}{q}\right) = \left(\frac{x}{q}\right)$, $\left(\frac{-3x}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{3}{q}\right)\left(\frac{x}{q}\right) = -\left(\frac{x}{p}\right)$

Now let's search case by case when do we have $\left(\frac{y}{p}\right) = \left(\frac{y}{q}\right) = +1$
if $\left(\frac{x}{p}\right) and\ \left(\frac{x}{q}\right)$ have different signs: $\left(\frac{x}{p}\right) positive$
then $x, -x,\ 3x \in QNR_N$ and $-\ 3x \in QR_N$
if $\left(\frac{x}{p}\right) and\ \left(\frac{x}{q}\right)$ have different signs: $\left(\frac{x}{p}\right) negative$
then $x, -x, -\ 3x \in QNR_N$ and $3x \in QR_N$

if $\left(\frac{x}{p}\right) and\ \left(\frac{x}{q}\right)$ have same signs: positive, then $-x, 3x, -3X \in QNR_N$ and $x \in QR_N$
if $\left(\frac{x}{p}\right) and\ \left(\frac{x}{q}\right)$ have same signs: negative, then $x, 3x, -3X \in QNR_N$ and $-x \in QR_N$

4.
With base a=2 Miller-Rabin(N,1) will return composite because N-1=131457704*2^1
And $2^{131457704} \equiv 10030295 \neq\ \pm 1\ [N]$