Midterm 2 solutions.

1a: Let g be a generator of $(\mathbb{Z}/p)^\times$. Then $a = g^\alpha$ for some α. Suppose $\alpha = 7s + r$ with $0 \le r < 7$. Then

$$a^{(p-1)/7} \equiv g^{(7s+r)\cdot\frac{p-1}{7}} \equiv g^{s(p-1)} \cdot g^{r\cdot\frac{p-1}{7}} \equiv g^{r\cdot\frac{p-1}{7}} \mod p.$$

Since $r < 7$, $r \cdot \frac{p-1}{7} < p - 1 = \text{order}(g)$, so $a^{(p-1)/7} \equiv 1 \mod p$ if and only if $r = 0$. If a is a seventh power, then $r = 0$, so $a^{(p-1)/7} \equiv 1 \mod p$. Conversely, if $a^{(p-1)/7} \equiv 1 \mod p$, then $r = 0$, so a is a seventh power.

1b: Let g be a generator of $(\mathbb{Z}/101)^\times$. Then $17 \equiv g^s \mod 101$ for some s. Since $0^7 \not\equiv 17 \mod 101$, any solution must be a unit. So any solution must be of the form $x \equiv g^h \mod 101$ for some $0 \le h < 100$. But $(g^h)^7 \equiv g^s \mod 101$ if and only if $7h \equiv s \mod 100$. Since $\gcd(7, 100) = 1$, there is a unique value of h that satisfies this equation for any given s, namely $h \equiv vs \mod 100$ where $7v \equiv 1 \mod 100$. Thus, the original equation has exactly one solution.

2a: By Euler's criterion, $35^{(p-1)/2} \equiv \left(\frac{35}{p}\right) \mod p$. We have that $\left(\frac{35}{p}\right) = \left(\frac{5}{2^{31}-1}\right)\left(\frac{7}{2^{31}-1}\right)$. We have that $2^{31} - 1 \equiv -1 \equiv 3 \mod 4$, $5 \equiv 1 \mod 4$, and $7 \equiv 3 \mod 4$, so applying quadratic reciprocity, we have $\left(\frac{5}{2^{31}-1}\right) = \left(\frac{2^{31}-1}{5}\right)$ and $\left(\frac{7}{2^{31}-1}\right) = -\left(\frac{2^{31}-1}{7}\right)$. By Euler's theorem, $2^4 \equiv 1 \mod 5$, so $2^{31} - 1 \equiv (2^4)^7 \cdot 2^3 - 1 \equiv 8 - 1 \equiv 2 \mod 5$. Similarly, $2^6 \equiv 1 \mod 7$, so $2^{31} - 1 \equiv (2^6)^5 \cdot 2 - 1 \equiv 1 \mod 7$. Putting it all together, we have that

$$35^{(p-1)/2} \equiv \left(\frac{35}{p}\right) \equiv \left(\frac{5}{2^{31}-1}\right)\left(\frac{7}{2^{31}-1}\right) \equiv -\left(\frac{2^{31}-1}{5}\right)\left(\frac{2^{31}-1}{7}\right) \equiv -\left(\frac{2}{5}\right)\left(\frac{1}{7}\right) \equiv 1 \mod p.$$

2b: By CRT, 35 is a square modulo $113 \cdot 167$ if and only if it is a square modulo both 113 and 167. We compute, using the Jacobi version of quadratic reciprocity, that

$$\left(\frac{35}{113}\right) = (-1)^{\frac{34}{2}\cdot\frac{112}{2}}\left(\frac{113}{35}\right) = +\left(\frac{8}{35}\right) = \left(\frac{4}{35}\right)\left(\frac{2}{35}\right) = 1 \cdot (-1) = -1$$

where the second to last equality uses that $\left(\frac{2}{35}\right) = -1$ since $35 \equiv 3 \mod 8$. Thus, 35 is not a square modulo 113, so it's not a square modulo $133 \cdot 167$.

3: Suppose $\gcd(a, 91) = 1$. Then $\gcd(a, 7) = \gcd(a, 13) = 1$. By CRT, we have that $a^{5k} \equiv a \mod 91$ if and only if $a^{5k} \equiv a \mod 7$ and $a^{5k} \equiv a \mod 13$. To get the first congruence, it suffices to have $5k \equiv 1 \mod 6$ by Euler's theorem. Similarly, to get the second congruence, it suffices to have $5k \equiv 1 \mod 12$. So $k = 5$ does the trick.

4a: Notice that $(53^3)^2 \equiv 1^2 \mod n$, but $53^3 \not\equiv \pm 1 \mod n$. So we have that $(148877 - 1)(148877 + 1) \equiv (53^3 - 1)(53^3 + 1) \equiv 0 \mod n$. If either factor were relatively prime to n, the other would have to be divisible by n, which it isn't. So each factor must have some non-trivial gcd with n. That is, computing either $\gcd(1448876, n)$ or $\gcd(1448878, n)$ will give a proper factor of n.

4b: Since $36^{51} \equiv 1 \mod n$, we have that $36^{51} \equiv 1 \mod p$, so the order of 36 modulo p must be a divisor of 51, and we are given that it is less than 51, so the order must be 1, 3, or 17. If a is the order of 36 modulo p, then we have that $36^a - 1$ is divisible by p, but not divisible by n, so $\gcd(36^a - 1, n)$ will be a proper factor of n. Thus, we can factor n by computing $\gcd(36^1 - 1, n)$, $\gcd(36^3 - 1, n)$, and $\gcd(36^{17} - 1, n)$.