Solutions to the first midterm from Spring 2013.

1. Since 3, 5 and 7 are pairwise coprime, we can use the standard algorithm from the proof of CRT. We need to find integers z_1, z_2 and z_3 satisfying the congruences $5 \cdot 7 \cdot z_1 \equiv 1 \mod 3$, $\quad 3 \cdot 7 \cdot z_2 \equiv 1 \mod 5$ and $3 \cdot 5 \cdot z_3 \equiv 1 \mod 7$. Then $x_0 = 2(5 \cdot 7z_1) + 3(3 \cdot 7z_2) + 5(3 \cdot 5z_3)$ is a solution, and the general solution is $x = x_0 + 105k$ with $k \in \mathbb{Z}$.
The above congruences simplify to $2z_1 \equiv 1 \mod 3$, $z_2 \equiv 1 \mod 5$ and $z_3 \equiv 1 \mod 7$, so we can set $z_1 = 2$ and $z_2 = z_3 = 1$ which gives us a solution $x_0 = 140 + 63 + 75 = 278$. The general solution is $x = 278 + 105k$. We can find the smallest positive solution by starting with 278 and then subtracting 105 repeatedly until we get a non-positive solution. We have $278 - 2 \cdot 105 = 68 > 0$ while $278 - 3 \cdot 105 < 0$, so $x = 68$ is the smallest positive solution.

2. By Fermat's little theorem, for any prime p and any x with $p \nmid x$ we have $x^{p-1} \equiv 1 \mod p$, so $(x^{(p-1)/2})^2 \equiv 1 \mod p$, and therefore $x^{(p-1)/2} \equiv \pm 1 \mod p$. And if $p \mid x$, then of course $x^{(p-1)/2} \equiv 0 \mod p$.
Observing that $11 = (23-1)/2$, we reduce both sides of the original equation mod $p = 23$. The right-hand side is clearly congruent to 11. On the other hand, as shown above, $x^{11} \equiv 0$ or $\pm 1 \mod 23$ for any x, so the left-hand side is congruent to c for some $-10 \leq c \leq 10$. None of the numbers in this interval is congruent to 11 mod 23, so we reached a contradiction.

3. We begin by observing that

(i) given $k \in \mathbb{N}$, we have $x^k \equiv 1 \mod 120$ if and only if $[x]_{120}^m = [1]_{120}$ in $\mathbb{Z}_{120}$

(ii) an integer x is coprime to 120 if and only if $[x]_{120} \in U_{120}$.

In view of (i) and (ii), the number m we are asked to find in this problem is simply $\exp(U_{120})$, the exponent of U_{120}.
It is easy to check that for any finite groups $G_1, \ldots, G_k$ we have

$$\exp(G_1 \times \ldots \times G_k) = LCM(\exp(G_1), \ldots, \exp(G_k)).$$

By Corollary 8.3 from class, $U_{120} \cong U_3 \times U_5 \times U_8$, so

$$m = LCM(\exp(U_3), \exp(U_5), \exp(U_8)).$$

We know that the groups U_3 and U_5 are cyclic of orders 2 and 4, respectively, so $\exp(U_3) = 2$ and $\exp(U_5) = 4$. The group U_8 has 3 non-identity elements $[3]_8, [5]_8$ and $[7]_8$, all of which have order 2, so $\exp(U_8) = 2$. Therefore, $m = LCM(2, 4, 2) = 4$.

4. Let $f(x) = x^3 - a^2x^2 + p^2$. We start by solving the congruence $f(x) \equiv 0 \mod p$. We get $p \mid (x^3 - a^2x^2) = x^2(x - a^2)$, so $p \mid x$ or $p \mid (x - a^2)$; equivalently, $x \equiv 0$ or $a^2 \mod p$. To determine possible lifts of these solutions, we evaluate $f'(0)$ and $f'(a^2)$.
We have $f'(x) = 3x^2 - 2a^2x$, so $f'(a^2) = 3a^4 - 2a^4 = a^4 \not\equiv 0 \mod p$ since $p \nmid a$. Thus, $x = a^2$ lifts to a unique reduced solution to $f(x) \equiv 0 \mod p^k$ for any k; in particular, this is true for $k = 3$.

On the other hand, $f'(0) = 0$, so we cannot determine the number of lifts of $x = 0$ right away. Potential lifts of 0 have the form $x = pk$. Rather than starting with solving $f(x) \equiv 0 \mod p^2$, we plug in $x = pk$ directly into the congruence $f(x) \equiv 0 \mod p^3$.

We get $(pk)^3 - a^2(pk)^2 + p^2 \equiv 0 \mod p^3$. This simplifies to $(ak)^2 \equiv 1 \mod p$, which is equivalent to $ak \equiv \pm 1 \mod p$. Since $gcd(a, p) = 1$, each of the congruences $ak \equiv 1 \mod p$ and $ak \equiv -1 \mod p$ has unique solution in the interval $[0, p-1]$, call them k_0 and k_1; hence an arbitrary solution has the form $k = k_1 + pn$ or $k = k_2 + pn$ with $n \in \mathbb{Z}$. Moreover, $k_1 \not\equiv k_2 \mod p$ since $a(k_1 - k_2) = ak_1 - ak_2 \equiv 1 - (-1) = 2 \mod p$ and p is odd, so these two families are distinct.

The corresponding solutions to $f(x) \equiv 0 \mod p^3$ are $x = pk_1 + p^2n$ and $x = pk_2 + p^2n$. We may be tempted to say that there are two reduced solutions (namely pk_1 and pk_2), but remember that we are solving $f(x) \equiv 0 \mod p^3$ (not mod p^2), so reduced solutions are the ones in the interval $[0, p^3 - 1]$. Since $0 \leq k_1, k_2 \leq p - 1$ by construction, the number $pk_i + p^2n$ (for $i = 1, 2$) lies in the interval $[0, p^3 - 1]$ if and only if $0 \leq n \leq p - 1$.

Thus, the number of reduced solutions to $f(x) \equiv 0 \mod p^3$ satisfying $x \equiv 0 \mod p$ is equal to $2p$. Therefore, the total number of reduced solutions to $f(x) \equiv 0 \mod p^3$ is equal to $2p + 1$.

5. Let $p_1^{a_1} \dots p_k^{a_k}$ be a prime factorization of n. We will show that if all a_i are even, then $\sqrt{n}$ is an integer, and if at least one a_i is odd, then $\sqrt{n}$ is irrational.

The first statement is clear: if $a_i = 2b_i$ for some $b_i \in \mathbb{N}$ for each i, then $\sqrt{n} = p_1^{b_1} \dots p_k^{b_k} \in \mathbb{Z}$.

Now suppose that a_i is odd for some i. Assume that $\sqrt{n}$ is rational, so

$\sqrt{n} = \frac{e}{f}$ for some $e, f \in \mathbb{N}$. Multiplying both sides by f and squaring, we get $e^2 = f^2 n$. Applying the function ord_{p_i} to both sides and using the equality $ord_{p_i}(xy) = ord_{p_i}(x) + ord_{p_i}(y)$, we get $2ord_{p_i}(e) = ord_{p_i}(n) + 2ord_{p_i}(f) = a_i + 2ord_{p_i}(f)$. Therefore, $a_i = 2ord_{p_i}(e) - 2ord_{p_i}(f)$ is even, contrary to our assumption. Hence, $\sqrt{n}$ is irrational.