Jan. 2008 — Advanced Algorithms — Max: 1 Hour
Calculators are **not** permitted
Proper justification to your answers is **absolutely** necessary.

Name and Roll No.: _____

1. Is 2 primitive (i.e., a generator) in Z_{19}^*? [3]

2. Find a primitive element in Z_{197}^* (Hint: $2^{18} = 58 \mod 361$). [3]

3. How many elements $1 \leq i \leq n = 2700$ satisfy $GCD(n, i) = 3$? [3]

4. Evalutate $17^{119} \mod 99$. Don't evaluate directly. [3]

5. Find a solution for the equation $x^2 = 1 \mod 323$ other than $x \in \{+1, -1\}$. (Note: $323 = 17 \times 19$). [3]

6. Let p be odd prime. Let $q_1, ..., q_k$ be prime factors of $p-1$. Show that $a \in Z_p^*$ generates Z_p^* if and only if $a^{(p-1)/q_i} \neq 1 \mod p$ for all $1 \leq i \leq k$. [4]

7. Show that the equation $x^2 + 1 = 0 \mod p$, p odd prime has a solution if and only if $p = 1 \mod 4$. (Hint: show that $a \in Z_p^*$ has a square root in Z_p if and only if $a^{(p-1)/2} = 1 \mod p$). [4]