NAME: SID:

Problem 1: For each piece of pseudo-code below, give its asymptotic running time as a function of n. Express this running time using the $\Theta()$ notation. Include a brief justification (at most 25 words).

Pseudo-code	Running time	Justification

for $i \leftarrow 1$ **to** $3n^2$ **do**
  $x \leftarrow x^2$
for $j \leftarrow 1$ **to** $n+3$ **do**
  $z \leftarrow x + z$		

for $i \leftarrow 1$ **to** n **do**
  $j \leftarrow 1$
  while $j < n$ **do**
  $j \leftarrow 4j$
  $x \leftarrow j \cdot x$		

for $i \leftarrow 1$ **to** n^2 **do**
  $k \leftarrow 1$
  while $k < n$
  $x \leftarrow x^2$
  $k \leftarrow k + 3$		

for $i \leftarrow n/2$ **to** n **do**
  $x \leftarrow 2x - 1$
  for $j \leftarrow 1$ **to** $2i$ **do**
  $x \leftarrow 2j \cdot x$		

$k \leftarrow 1$
for $i \leftarrow 1$ **to** n **do**
  while $k < 9i$ **do**
  $k \leftarrow k + 1$
  $x \leftarrow x^2$		

Note 1: "$\leftarrow$" denotes the assignment statement. The scope and nesting of loops is indicated by the indentation.

Problem 2: (a) Give a complete statement of Fermat's Little Theorem.

(b) Compute $3^{1895} \pmod{19}$. (You must use Fermat's Little Theorem.)

Problem 3: For each statement below tell whether it is true or false and give a brief justification (at most 50 words). All numbers a, b, c are positive integers.

(a) If a is prime and a is a divisor of bc then a is a divisor of b or c. TRUE FALSE

(b) If a and b are divisors of c then ab is a divisor of c TRUE FALSE

(c) $\gcd(ab, c) = \gcd(a, c) \cdot \gcd(b, c)$. TRUE FALSE

(d) $\gcd(a + b, b) = \gcd(a, b)$. TRUE FALSE