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 15 words).

Pseudo-code	Running time	Justification

for $i \leftarrow 1$ **to** n **do**
    $z \leftarrow z + 5$
    $k \leftarrow 1$
    while $k < n$ **do**
        $z \leftarrow z^2$
        $k \leftarrow 2k$		

for $i \leftarrow 1$ **to** $2n + 3$ **do**
    $z \leftarrow z + 5$
for $i \leftarrow 1$ **to** $7n$ **do**
    $z \leftarrow z^2$		

$j \leftarrow 1$
while $j < n$ **do**
    $z \leftarrow z + 5$
    for $i \leftarrow 1$ **to** j **do**
        $z \leftarrow z^2$
    $j \leftarrow 2j$		

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

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

Problem 2: (a) Compute $12^{-1} \pmod{19}$ using the method of linear combinations (listing the multiples of 19 plus 1).

(b) Show how to compute $5^{-1} \pmod{7}$ using Fermat's theorem.

(c) Compute $2^{4806} \pmod{13}$ using Fermat's theorem.

(d) Compute $2^{18} \pmod{20}$ using the doubling method (a.k.a. squaring method).

Problem 3: In the statements below x, y, z denote positive integers. For each statement below tell whether it is true (circle your answer) and justify your answer.

(a) Assume that y, z are different primes. If x is a multiple of y an x is a multiple of z then x is a multiple of yz. TRUE FALSE

(b) If x is prime and x divides yz then x divides y or z. TRUE FALSE

(c) If x is prime and x divides $y + z$ then x divides y or z. TRUE FALSE

(d) If x is a multiple of y and x is a multiple of z then x is a multiple of yz. TRUE FALSE