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**
  $z \leftarrow z^2$
  $k \leftarrow 2k$
	$\Theta(n \log n)$	k doubles each time, so internal loop makes $\Theta(\log n)$ iterations. External loop makes n iterations.

for $i \leftarrow 1$ **to** $2n + 3$ **do**
  $z \leftarrow z + 5$
for $i \leftarrow 1$ **to** $7n$ **do**
  $z \leftarrow z^2$
	$\Theta(n)$	Two disjoint loops, each making $\Theta(n)$ iterations.

$j \leftarrow 1$
while $j < n$ **do**
  $z \leftarrow z + 5$
  for $i \leftarrow 1$ **to** j **do**
  $z \leftarrow z^2$
  $j \leftarrow 2j$
	$\Theta(n)$	Internal loop takes time j, with j's forming a geometric sequence $1, 2, 4, 8, \ldots$. So total is $\Theta(n)$.

for $i \leftarrow 1$ **to** n **do**
  $z \leftarrow z + 2$
  for $j \leftarrow 1$ **to** i **do**
  $z \leftarrow z^2$
	$\Theta(n^2)$	Internal loop takes time i. Adding over all i (arithmetic sequence), we get $\Theta(n^2)$.

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).

The list $k \cdot 19 + 1$ is $1, 20, 39, 58, 77, 96, ...$ Since $96 = 8 \cdot 12$, we get $12^{-1} \pmod{19} = 8$.

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

From Fermat's theorem, $a^{-1} \equiv a^{p-2} \pmod{p}$. Here, $a = 5$ and $p = 7$. So, computing modulo 7, we get

$$5^{-1} = 5^{7-2} = 5^5 = (-2)^5 = -32 = 3.$$

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

Computing modulo 13, we have

$$2^{4806} = 2^{12 \cdot 400 + 6} = (2^{12})^{400} \cdot 2^6 = 1 \cdot 2^6 = 64 = 12.$$

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

Computing modulo 20, we have

$$2^{18} = 4^9 = 4 \cdot 4^8 = 4 \cdot 16^4 = 4 \cdot (-4)^4 = 4 \cdot 16^2 = 4 \cdot (-4)^2 = 4 \cdot 16 = 64 = 4.$$

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

Both primes y and z appear in the factorization of x, so x is a multiple of yz.

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

x appears in prime factorization of yz, and each prime factor of yz is either a prime factor of y or a prime factor of z

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

Counter-example: 2 divides $3 + 3$ but it does not divide 3

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

Counterexample: 30 is a multiple of 6 and 30 is a multiple of 15, but 30 is not a multiple of $6 \cdot 15 = 90$.