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. (You don't need to give any justification.)

Pseudo-code	Running time

for $i \leftarrow 1$ **to** $2n$ **do**
    for $j \leftarrow 1$ **to** i **do**
        $x \leftarrow 2x + 7$
	$\Theta(n^2)$

$j \leftarrow 1$
while $j < n$ **do**
        $x \leftarrow 2x + 7$
        $j \leftarrow j + 2$
	$\Theta(n)$

for $i \leftarrow 1$ **to** n **do**
    $j \leftarrow 1$
    while $j < n$
            $x \leftarrow 2x + 7$
            $j \leftarrow 3j$
	$\Theta(n \log n)$

for $i \leftarrow n/2$ **to** n **do**
    $x \leftarrow 2x + 7$
for $j \leftarrow 1$ **to** $3n$ **do**
    $x \leftarrow 2x + 7$
	$\Theta(n)$

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

Problem 2: (a) State Euclid's Algorithm.

function gcd(a, b)
  if $a = b$ **then return** a
  if $a < b$ **then** swap(a, b)
  return gcd$(a - b, b)$

(b) Use Euclid's Algorithm to compute the greatest common divisor of 323 and 456. Show your work. (No guessing, you must follow Euclid's algorithm.)

$$\begin{aligned} 323, 456 &\rightarrow 323, 133 \rightarrow 190, 133 \rightarrow 57, 133 \\ &\rightarrow 57, 76 \rightarrow 57, 19 \rightarrow 38, 19 \rightarrow 19, 19. \end{aligned}$$

Problem 3: (a) Compute $5^{40} \operatorname{rem} 13$. Show your work.

$$\begin{aligned} 5^{40} \operatorname{rem} 13 &= (5^2)^{20} \operatorname{rem} 13 \\ &= 25^{20} \operatorname{rem} 13 \\ &= (-1)^{20} \operatorname{rem} 13 \\ &= 1. \end{aligned}$$

(b) Compute $5^{-1} \pmod{11}$. Show your work.

We first find α, β for which $\alpha \cdot 5 + \beta \cdot 11 = 1$. This gives us $\alpha = 9$ and $\beta = -4$. So $5^{-1} = 9 \pmod{11}$.

To verify: $(5 \cdot 9) \operatorname{rem} 11 = 45 \operatorname{rem} 11 = 1$.