CS 1050 Homework 11 Solutions

1a. Proof of Lemma: We are given that d is a divisor of both a and b. So, $a = k_1 d$ and $b = k_2 d$ for some integers k_1 and k_2. So, $a - b = k_1 d - k_2 d = (k_1 - k_2)d = kd$, where $k = k_1 - k_2$ is an integer. So, $a - b$ is divisible by d.

b. Proof of Theorem 1: We prove it by contradiction. Let $d = gcd(x, m)$. We are given that $d > 1$. Assume that the multiplicative inverse of x modulo m exists. Call it y. Therefore $xy \equiv 1 \pmod{m}$. So $xy - 1 = km$ for some integer k. That is, $xy - km = 1$. Now, d is the gcd of x and m. So, it divides both x and m. Therefore it divides xy and km also. Using the previous lemma we get that d divides $xy - km$, that is, d divides 1, which is impossible since $d > 1$. So we reach a contradiction. Therefore the multiplicative inverse of x modulo m does not exist.

2a. $gcd(1575, 231) = gcd(231, 1575 \ mod \ 231) = gcd(231, 189)$

$= gcd(189, 231 \ mod \ 189) = gcd(189, 42)$

$= gcd(42, 189 \ mod \ 42) = gcd(42, 21)$

$= gcd(21, 42 \ mod \ 21) = gcd(21, 0) = 21$

b. $gcd(100996, 20048) = gcd(20048, 100996 \ mod \ 20048) = gcd(20048, 756)$

$= gcd(756, 20048 \ mod \ 756) = gcd(756, 392)$

$= gcd(392, 756 \ mod \ 392) = gcd(392, 364)$

$= gcd(364, 392 \ mod \ 364) = gcd(364, 28)$

$= gcd(28, 364 \ mod \ 28) = gcd(28, 0) = 28$

3. $Extgcd(98, 42)$ calls $Extgcd(42, 14)$ (since $14 = 98 \ mod \ 42$)

$Extgcd(42, 14)$ calls $Extgcd(14, 0)$ (since $0 = 42 \ mod \ 14$)

$Extgcd(14, 0)$ returns $(14, 1, 0)$ to $Extgcd(42, 14)$

$Extgcd(42, 14)$ returns $(14, 0, 1 - 0 \cdot (42 \ div \ 14)) = (14, 0, 1)$ to $Extgcd(98, 42)$

$Extgcd(98, 42)$ returns $(14, 1, 0 - 1 \cdot (98 \ div \ 42)) = (14, 1, -2)$.

Therefore $(d, b, a) = (14, 1, -2)$, where $gcd(98, 42) = 14 = 1 \cdot 98 + (-2) \cdot 42$.

4. For $n = 5$:
$a = 1$. $1^{5-1} \bmod 5 = 1^4 \bmod 5 = 1$.
$a = 2$. $2^{5-1} \bmod 5 = 2^4 \bmod 5 = 16 \bmod 5 = 1$.
$a = 3$. $3^{5-1} \bmod 5 = 3^4 \bmod 5 = 81 \bmod 5 = 1$.
$a = 4$. $4^{5-1} \bmod 5 = 4^4 \bmod 5 = 256 \bmod 5 = 1$.
$a = 5$. $5^{5-1} \bmod 5 = 5^4 \bmod 5 = 0$.
For $n = 5$, since 5 is a prime, all the values are as predicted by Fermat's little theorem.

For $n = 6$:
$a = 1$. $1^{6-1} \bmod 6 = 1^5 \bmod 6 = 1$.
$a = 2$. $2^{6-1} \bmod 6 = 2^5 \bmod 6 = 32 \bmod 6 = 2$.
$a = 3$. $3^{6-1} \bmod 6 = 3^5 \bmod 6 = 243 \bmod 6 = 3$.
$a = 4$. $4^{6-1} \bmod 6 = 4^5 \bmod 6 = 1024 \bmod 6 = 4$.
$a = 5$. $5^{6-1} \bmod 6 = 5^5 \bmod 6 = 3125 \bmod 6 = 5$.
$a = 6$. $6^{6-1} \bmod 6 = 6^5 \bmod 6 = 0$.

For $n = 7$:
$a = 1$. $1^{7-1} \bmod 7 = 1^6 \bmod 7 = 1$.
$a = 2$. $2^{7-1} \bmod 7 = 2^6 \bmod 7 = 64 \bmod 7 = 1$.
$a = 3$. $3^{7-1} \bmod 7 = 3^6 \bmod 7 = 729 \bmod 7 = 1$.
$a = 4$. $4^{7-1} \bmod 7 = 4^6 \bmod 7 = 4096 \bmod 7 = 1$.
$a = 5$. $5^{7-1} \bmod 7 = 5^6 \bmod 7 = 15625 \bmod 7 = 1$.
$a = 6$. $6^{7-1} \bmod 7 = 6^6 \bmod 7 = 46656 \bmod 7 = 1$.
$a = 7$. $6^{7-1} \bmod 7 = 7^6 \bmod 7 = 0$.
For $n = 7$, since 7 is a prime, all the values are as predicted by Fermat's little theorem.

For $n = 8$:
$a = 1$. $1^{8-1} \bmod 8 = 1^7 \bmod 8 = 1$.
$a = 2$. $2^{8-1} \bmod 8 = 2^7 \bmod 8 = 128 \bmod 8 = 0$.
$a = 3$. $3^{8-1} \bmod 8 = 3^7 \bmod 8 = 2187 \bmod 8 = 3$.
$a = 4$. $4^{8-1} \bmod 8 = 4^7 \bmod 8 = 16834 \bmod 8 = 0$.
$a = 5$. $5^{8-1} \bmod 8 = 5^7 \bmod 8 = 78125 \bmod 8 = 5$.
$a = 6$. $6^{8-1} \bmod 8 = 6^7 \bmod 8 = 279936 \bmod 8 = 0$.
$a = 7$. $6^{8-1} \bmod 8 = 7^7 \bmod 8 = 823543 \bmod 8 = 7$.
$a = 8$. $8^{8-1} \bmod 8 = 8^7 \bmod 8 = 0$.

For $n = 9$:
$a = 1$. $1^{9-1} \bmod 9 = 1^8 \bmod 9 = 1$.
$a = 2$. $2^{9-1} \bmod 9 = 2^8 \bmod 9 = 256 \bmod 9 = 4$.
$a = 3$. $3^{9-1} \bmod 9 = 3^8 \bmod 9 = 6561 \bmod 9 = 0$.
$a = 4$. $4^{9-1} \bmod 9 = 4^8 \bmod 9 = 65536 \bmod 9 = 7$.
$a = 5$. $5^{9-1} \bmod 9 = 5^8 \bmod 9 = 390625 \bmod 9 = 7$.
$a = 6$. $6^{9-1} \bmod 9 = 6^8 \bmod 9 = 1679616 \bmod 9 = 0$.
$a = 7$. $6^{9-1} \bmod 9 = 7^8 \bmod 9 = 5764901 \bmod 9 = 4$.
$a = 8$. $8^{9-1} \bmod 9 = 8^8 \bmod 9 = 16777216 \bmod 9 = 1$.
$a = 9$. $9^{9-1} \bmod 9 = 9^8 \bmod 9 = 0$.

5a. By the definition of logarithms, $\log_a x = d \Leftrightarrow a^d = x$. Therefore $a^{\log_a x} = x$.

b. $$\begin{aligned} \sqrt{2}^{\log_2 n} &= (2^{\frac{1}{2}})^{\log_2 n} \\ &= 2^{(\frac{1}{2}\log_2 n)} \\ &= 2^{\log_2 n^{\frac{1}{2}}} \\ &= n^{\frac{1}{2}} \end{aligned}$$

c. $$\begin{aligned} 4^{\log_2 n} &= (2^2)^{\log_2 n} \\ &= 2^{2\log_2 n} \\ &= 2^{\log_2 n^2} \\ &= n^2 \end{aligned}$$

d. $$\begin{aligned} 2^{\log_2^2 n} &= 2^{(\log_2 n)^2} \\ &= (2^{\log_2 n})^{\log_2 n} \\ &= n^{\log_2 n} \end{aligned}$$

e. $$\begin{aligned} \log_2^2 n &= (\log_2 n)^2 \\ &= ((\log_2 e)\log_e n)^2 \quad \text{(since } \log_a b = (\log_a c)\log_c b) \\ &= (\log_2 e)^2(\log_e n)^2 \\ &= c\log_e^2 n \quad \text{(where } c = \log_2^2 e \text{ is a constant)} \end{aligned}$$

Therefore $\log_2^2 n = O(\log_e^2 n)$.