HW 7

1) a) $a_0$ $a_1 x$ $a_2 x \cdot x$ $a_3 x \cdot x \cdot x$ $a_n x \cdot x \cdot \cdots \cdot x$

# multiplications = $0 + 1 + 2 + 3 + \cdots + n$

$= \frac{n(n+1)}{2}$ [see Workshop 12]

# additions = $n$

So the time complexity is $n + \frac{n(n+1)}{2} = \Theta(n^2)$.

b)
```
val := a_0
xpower := 1
For i = 1 to n
    xpower := xpower · x
    val := val + a_i · xpower
End-for
Return val
```

The for loop executes $n$ times, and each iteration uses only $\Theta(1)$ operations (and only $\Theta(1)$ operations before/after the loop).
So the time complexity is $\Theta(n)$.

2) a) $n \cdot \left(\Theta(n) + \Theta(n \log n)\right) = n \cdot \Theta(n \log n) = \Theta(n^2 \log n)$

For loop runs n times, each iteration runs both wibble & blarg

b) $n \cdot \Theta(n) = \Theta(n^2)$

this time blarg is never called

c) $\log_5(n) \cdot \left(\Theta(n) + \Theta(n \log n)\right) + (n - \log_5 n) \cdot \Theta(n)$

$= \Theta(\log n) \cdot \Theta(n \log n) + \Theta(n) \cdot \Theta(n)$

$= \Theta(n \log^2 n) + \Theta(n^2)$

$= \Theta(n^2)$.

3) No; for example, $p=4$ and $a=b=2$ is a counterexample.

4) We need to show: $\forall a,b \in \mathbb{Z}_p$, if $ab=0$, then $a=0$ or $b=0$.

[actually, "if and only if," but "if $a=0$ or $b=0$, then $ab=0$" is obvious]

Direct proof. Let $a,b \in \mathbb{Z}_p$ and suppose $a \cdot b = 0$.

$ab=0$ in $\mathbb{Z}_p$ means $ab \bmod p = 0$

i.e. $p \mid (ab)$.

The fact in #3 implies $p \mid a$ or $p \mid b$,

but $a,b \in \mathbb{Z}_p$ implies $0 \le a,b \le p-1$, so $a=0$ or $b=0$.

5) Let $n$ be composite. Then $n = a \cdot b$ for some $a,b \in \mathbb{Z}$, $1 < a \le b < n$.

Then in $\mathbb{Z}_n$, $a \neq 0$ and $b \neq 0$ but $a \cdot b \bmod n = n \bmod n = 0$,

so the Zero Product Property fails.

6) a) $x \bmod 28 = 9$ means $x = 28q + 9$ for some $q \in \mathbb{Z}$,

so $6x = 6(28q+9)$

$= 28(6q) + 54$

$= 28(6q) + 28 + 26$

$= 28(6q+1) + 26$, so $6x \bmod 28 = 26$.

– OR –

$6x \bmod 28$

$= (6 \bmod 28) \cdot (x \bmod 28) \bmod 28$

$= 6 \cdot 9 \bmod 28$

$= 54 \bmod 28$

$= 26$.

b) $y \bmod 15 = 4$ means $y = 15q + 4$ for some $q \in \mathbb{Z}$.

So $10y = 10(15q+4)$

$= 3(50q) + 40$

$= 3(50q) + 39 + 1$

$= 3(50q+13) + 1$, so $10y \bmod 3 = 1$.