Homework 1.4

Chris Rytting

September 11, 2015

1.19 (i)

Given an integer $a = \sum_{k=0}^{n-1} a_k 10^k = a_0 10^0 + a_1 10^1 + \cdots + a_{n-1} 10^{n-1}$ Note that

$$\begin{aligned}
a &= \sum_{k=0}^{n-1} a_k 10^k \\
&= a_0 10^0 + a_1 10^1 + \cdots + a_{n-1} 10^{n-1} \\
&= (9a_1 + 99a_2 + \cdots + (10^{n-1} - 1)a_{n-1}) + (a_0 + a_1 + \cdots + a_{n-1}) \\
&= 3(3a_1 + 33a_2 + \cdots + ((10^{n-1} - 1)/3)a_{n-1}) + (a_0 + a_1 + \cdots + a_{n-1})
\end{aligned}$$

Note that a is divisible by 3 if and only if the second term $(a_0 + a_1 + \cdots + a_{n-1})$ is divisible by 3, since it should be apparent that every term in the first expression is divisible by 3.

1.19(ii)

Given an integer $a = \sum_{k=0}^{n-1} a_k 10^k = a_0 10^0 + a_1 10^1 + \cdots + a_{n-1} 10^{n-1}$ Note that

$$\begin{aligned}
a &= \sum_{k=0}^{n-1} a_k 10^k \\
&= a_0 10^0 + a_1 10^1 + \cdots + a_{n-1} 10^{n-1} \\
&= (9a_1 + 99a_2 + \cdots + (10^{n-1} - 1)a_{n-1}) + (a_0 + a_1 + \cdots + a_{n-1}) \\
&= 9(a_1 + 11a_2 + \cdots + ((10^{n-1} - 1)/9)a_{n-1}) + (a_0 + a_1 + \cdots + a_{n-1})
\end{aligned}$$

Note that a is divisible by 9 if and only if the second term $(a_0 + a_1 + \cdots + a_{n-1})$ is divisible by 9, since it should be apparent that every term in the first expression is divisible by 9

1.19(iii)

Given an integer $a = \sum_{k=0}^{n-1} a_k 10^k = a_0 10^0 + a_1 10^1 + \cdots + a_{n-1} 10^{n-1}$ Note that

$$\begin{aligned}
a &= \sum_{k=0}^{n-1} a_k 10^k \\
&= a_0 10^0 + a_1 10^1 + \cdots + a_{n-1} 10^{n-1} \\
&= (11a_1 + 99a_2 + 1001a_3 \cdots + (10^{n-1} - 1)a_{n-1}) + (a_0 - a_1 + a_2 - a_3 \cdots + (-1)^{n-1} a_{n-1}) \\
&\text{(With the coefficients of } a_i \text{ being given by } 10^i + (-1)^{i-1}) \\
&= 11(a_1 + 9a_2 + 91a_3 \cdots + ((10^{n-1} - 1)/11)a_{n-1}) + (a_0 - a_1 + a_2 - a_3 \cdots + (-1)^{n-1} a_{n-1})
\end{aligned}$$

Note that a is divisible by 11 if and only if the second expression $(a_0 + a_1 + \cdots + a_{n-1})$ is divisible by 11, since every term in the first expression is divisible by 11.

1.20

Since $a \equiv b (\text{mod } c)$, we know that $a - b = cn$ for some $n \in \mathbb{Z}$. Furthermore, since $d|c$, we know that $c = dm$ for some $m \in \mathbb{Z}$. Note that

$$a - b = cn = dmn \implies a - b = dk \implies d|(a - b) \implies a \equiv b (\text{mod } d)$$

where $k = mn \implies k \in \mathbb{Z}$.

1.21

$$\begin{aligned}
34^{34} &= -2^{34} \\
&= 2^{34} \\
&= (2^6)^5 2^4 \\
&= (4^5) 2^4 \\
&= 4^6 \\
&= 4^2 4^2 4^2 \\
&= 4 \cdot 4 \cdot 4 \\
&= 4 \cdot 4 \\
&= 4
\end{aligned}$$

1.22 (i)

$$
\begin{aligned}
((((((14^2)^2)^2)^2)^2)^2)^2 &= (((((69^2)^2)^2)^2)^2)^2 \\
&= ((((62^2)^2)^2)^2)^2 \\
&= (((34^2)^2)^2)^2 \\
&= ((13^2)^2)^2 \\
&= (42^2)^2 \\
&= 113^2 \\
&= 69
\end{aligned}
$$

1.22 (ii)

$$
\begin{aligned}
18^{254} &= (18^{15})^{16} 18^{14} \\
&= (76^{16})103 \\
&= (76^8)^2 103 \\
&= 47^2 103 \\
&= 50 \cdot 103 \\
&= 70
\end{aligned}
$$

1.22 (iii)

$$
\begin{aligned}
25^{640} &= (25^{10})^{64} \\
&= (76^8)^8 \\
&= 47^8 \\
&= 76
\end{aligned}
$$

1.23

We need $\gcd(x, c) = 1$.
For the sufficient condition, we have Proposition 1.4.9 which states that for any integers a, b, c if $\gcd(a, b) = 1$, then $a|bc$ implies that $a|c$.
For the necessary condition, note that for $m, n \in \mathbb{Z}$ we need

$$ax \equiv bx (\text{mod } c) \implies ax - bx = cn \implies x(a - b) = cn$$

$$\implies a \equiv b (\text{mod } c) \implies a - b = cm$$

Now let $a - b = \alpha \quad x = \xi d$ where $d = \gcd(x, c)$. If we let $d > 1$, contrary to the condition we've required, then

$$\xi d\alpha = cn \;\not\Rightarrow\; \alpha = cm$$

For the only way to guarantee that $c|\alpha$ (since we have no control over m or n), is to require α to be the only term such that $c|\alpha$. If $d|cn$ where $d \neq 1$, then α can take on any number of values to fulfill the first condition that will not imply the second.

1.25

We know $a \geq b \quad a, b \in \mathbb{Z}$. In the case that $a = b$, the program will terminate in one step, which is obviously $O(af(a)) \quad a > b$, since $f(a)$ is nondecreasing. In the case that $a > b$, we know that, since $a, b \in \mathbb{Z}$, $a \geq b+1$. In this case, the EA will terminate in, at most, $b + 1$ steps (since $b > 0$ and at each stage we have $r_k > r_{k+1}, \geq 0$, so $|b| > r_0 > r_1 > \cdots \leq 0$). So even in the worst case scenario, the algorithm will be $O(b + 1f(a)) \leq O(af(a))$ since $f(a)$ is non-decreasing and therefore at least a constant function.