Math Sec 1.4

Rex McArthur

September 11, 2015

Exercise. 1.19
(i) Proof: Given an integer $a = \sum_{k=0}^{n-1} a_k 10^k = a_0 10^0 + \cdots + a_{n-1}10^{n-1}$, Note that

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

Note that $3|a$ if and only if $3|\sum_{k=0}^{n-1} a_k$, by definition of divisibility, because it is apparent that 3 divides the first term.
(ii) Proof: Given an integer $a = \sum_{k=0}^{n-1} a_k 10^k = a_0 10^0 + \cdots + a_{n-1}10^{n-1}$, Note that

$$\begin{aligned} a &= \sum a_k 10^k \\ &= a_0 + \cdots + a_{n-1}10^{n-1} \\ &= (9a_1 + 99a_2 + \cdots + (10^{n-1} - 1)a_{n-1}) + (a_0 + a_1 + \cdots + a_{n-1}) \\ &= 9(1a_1 + 11a_2 + \cdots + (10^{n-1} - 1)/3a_{n-1}) + (a_0 + \cdots + a_{n-1}) \\ &= 9(1a_1 + 11a_2 + \cdots + (10^{n-1} - 1)/3a_{n-1}) + \sum_{k=0}^{n-1} a_k \end{aligned}$$

Note that $9|a$ if and only if $9|\sum_{k=0}^{n-1} a_k$, by definition of divisibility, because it is apparent that 9 divides the first term.
(iii) Proof: Given an integer $a = \sum_{k=0}^{n-1} a_k 10^k = a_0 10^0 + \cdots + a_{n-1}10^{n-1}$, Note that

$$
\begin{aligned}
a &= \sum_{k=0}^{n-1} a_k 10^k \\
&= a_0 10^0 + a_1 + 10^1 + \cdots + a_{n-1}10^{n-1} \\
&= (11a_1 + 99a_2 + 1001a_3 + \cdots + (10^{n-1} - 1) + a_{n-1}) + (a_0 - a_1 + a_2 - \cdots + (-1)^{n-1}a_{n-1}) \\
&\text{(Where the coefficients of } a_i^{th} \text{ term given by } 10^i - (-1)^{i-1}) \\
&= 11(a_1 + 9a_2 + 91a_3 + 909a_4 \cdots + ((10^{n-1} - 1)/11)a_{n-1}) + (a_0 - a_1 + a_2 \cdots + (-1)^{n-1}a_{n-1})
\end{aligned}
$$

Note that a is divisible by 11 if and only if the second expression is divisible by 11, by definition of divisiblity, since the entire first part is divisible by 11.

Exercise. 1.20
Since $a \equiv b (\text{mod } c)$, we know that $a - b = cn$ for some $n \in \mathbb{Z}$. Also, since $d|c$, we know that $c = dm$ for some $m \in \mathbb{Z}$. Note,

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

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

Exercise. 1.21
Note that $4^2 = 16 \equiv_{12} 4$.

$$34^{34} \equiv_{12} -2^{34} \equiv_{12} 4^{17} \equiv_{12} 4^2 4^2 4^2 4^2 4^2 4^2 4^2 4^2 4^2 4 \equiv_{12} 4^8 \equiv_{12} 4^2 4^2 4^2 \equiv_{12} 4^3 \equiv_{12} 4$$

Exercise. 1.22
(i): By Fermat's Little Theorem,

$$14^{127}14 \equiv_{127} 14^2 \equiv_{127} 69$$

(ii): By Fermat's Little Theorem,

$$(18^2)^{127} \equiv_{127} 18^2 \equiv_{127} 324 \equiv_{127} 197 \equiv_{127} 70$$

(iii): By Fermat's Little Theorem,

$$(25^5)^{127}25^5 \equiv_{127} 625^5 \equiv_{127} -5^5 \equiv_{127} -625 * 5 \equiv_{127} -5 * -5 \equiv_{127} 25$$

Exercise. 1.23
The necessary and sufficent conditions are that $\gcd(x, c) = 1$.
Proof: Suppose $\gcd(x, c) = 1$, and $ax \equiv bx (\text{mod } c)$. Thus $c|(ax - bx)$, and $c|(a - b)x$.
Because $\gcd(x, c) = 1$, $c|(a - b)$ by Proposition 1.4.9, and $a \equiv b (\text{mod } c)$.
Now, suppose $ax \equiv bx (\text{mod } c) \to a \equiv b (\text{mod } c)$. Thus, $c|(a-b)x$ implies that $c|(a-b)$.
This will only happen if c and x are relatively prime, which means that $\gcd(c, x) = 1$.

Exercise. 1.24
See attached code.

Exercise. 1.25
Note that the Eucledian algorithm has at most a steps, because if $a = b$, it has one step, and the worst case scenario is it decreases by one each time, and the remainder drops by one each time. Since the temporal complexity of the division algorithm is $O(f(a))$, it follows that the Eucledian algorithim would have a temporal complexity of at the very omost $O(af(a))$.