

**Q04a** Let  $a$  be an arbitrary integer, we start with an if and only if statement which can be expressed as:

$$37|a \iff 37|S(a)$$

To prove this we will split it up by cases starting with:

$$37|a \implies 37|S(a)$$

Let assume that  $37|a$ , this would mean that from CTR:

$$a \pmod{37} = 0 \pmod{37}$$

We also know that  $a$  can be expressed in terms of its digits (where  $k$  is an integer and  $3|k$ , if any digit  $d_k$  is greater then what exists in  $a$  then  $d_k = 0$ ) :

$$\begin{aligned} 0 \pmod{37} &= a \pmod{37} \\ &= d_k(10^{k-1}) + d_{k-1}(10^{k-2}) + \dots + d^2(10^2) + d^1(10) + d_0 \pmod{37} \end{aligned}$$

We notice that the digit expression  $\pmod{37}$  must also be equal to 0, from CAM. We also notice the following pattern in terms of the coefficients of  $10$  ( $n$ ) and  $\pmod{37}$ :

$$\begin{aligned} (n=0) : (10^0) \pmod{37} &\implies 1 \pmod{37} \implies 1 \pmod{37} \\ (n=1) : (10^1) \pmod{37} &\implies 10 \pmod{37} \implies 10 \pmod{37} \\ (n=2) : (10^2) \pmod{37} &\implies 100 \pmod{37} \implies 26 \pmod{37} \\ (n=3) : (10^3) \pmod{37} &\implies 1000 \pmod{37} \implies 1 \pmod{37} \end{aligned}$$

Notice that this pattern repeats. Returning back to our digit expansion, we know we can group terms into threes like:

$$\begin{aligned} 0 \pmod{37} &= d_k(10^{k-1}) + d_{k-1}(10^{k-2}) + d_{k-2}(10^{k-3}) + \dots + d_2(10^2) + d_1(10) + d_0 \pmod{37} \\ &= (d_k(10^2) + d_{k-1}(10^1) + d_{k-2}(10^0))(10^{k-3}) + \dots + (d^2(10^2) + d_1(10) + d_0)(10^0) \pmod{37} \end{aligned}$$

Since  $3|k$  (so for some integer  $a$ ,  $3a = k$ ) this can be better expressed in sigma notation where:

$$\begin{aligned} 0 \pmod{37} &= \sum_{n=0}^a 10^{3n}(d_{2+3n}(10^2) + d_{1+3n}(10) + d_{3n}) \pmod{37} \\ &= \sum_{n=0}^a (10^3)^n(d_{2+3n}(10^2) + d_{1+3n}(10) + d_{3n}) \pmod{37} \\ &= \sum_{n=0}^a (1)^n(d_{2+3n}(10^2) + d_{1+3n}(10) + d_{3n}) \pmod{37} \\ &= \sum_{n=0}^a (d_{2+3n}(10^2) + d_{1+3n}(10) + d_{3n}) \pmod{37} \end{aligned}$$

Thus we can see that our equation is equivalent to  $S(a)$ , and thus:

1.  $S(a) = \sum_{n=0}^a (d_{2+3n}(10^2) + d_{1+3n}(10) + d_{3n}) \pmod{37}$
2.  $\sum_{n=0}^a (d_{2+3n}(10^2) + d_{1+3n}(10) + d_{3n}) \pmod{37} = 0 \pmod{37}$

This infers that  $S(a) = 0 \pmod{37}$ , which because of CTR proves that  $37|S(a)$ . We have thus proved one the first implication.

We will now try to prove the second case:

$$37|S(a) \implies 37|a$$

Let  $37|S(a)$  this means that:

$$S(a) \pmod{37} = 0 \pmod{37}$$

We know that we can express  $S(a)$  as:

$$0 \pmod{37} = \sum_{n=0}^a (d_{2+3n}(10^2) + d_{1+3n}(10) + d_{3n}) \pmod{37}$$

We know from CAM that we can multiply both sides by  $1 \pmod{37}$ , which could then become:

$$\begin{aligned} 0 \pmod{37} &= \sum_{n=0}^a (1)^n (d_{2+3n}(10^2) + d_{1+3n}(10) + d_{3n}) \pmod{37} \\ &= \sum_{n=0}^a (10^3)^n (d_{2+3n}(10^2) + d_{1+3n}(10) + d_{3n}) \pmod{37} \\ &= \sum_{n=0}^a 10^{3n} (d_{2+3n}(10^2) + d_{1+3n}(10) + d_{3n}) \pmod{37} \end{aligned}$$

Expanding out the sigma notation we get that:

$$\begin{aligned} 0 \pmod{37} &= d_k(10^{k-1}) + d_{k-1}(10^{k-2}) + \dots + d^2(10^2) + d^1(10) + d_0 \pmod{37} \\ 0 \pmod{37} &= a \end{aligned}$$

Therefore CTR shows us that  $37|a$  we have thus proved the second implications. Since we have proven both implication for all possible values of  $a$ , we have proved the if and only if statements.

**Q04b** Notice that in order for the previous if and only if statement to be true, you need a repeating pattern where  $10^3 \pmod{27} = 1$  plus  $10^2, 10^1$  and  $10^0$  need to have unique endings. Thus if we plug in the numbers 0-4 we should notice a similar pattern to the  $(\pmod{37})$  pattern:

$$(n=0) : (10^0) \pmod{27} \implies 1 \pmod{27} \implies 1 \pmod{27}$$

$$(n = 1) : (10^1) \pmod{27} \implies 10 \pmod{27} \implies 10 \pmod{27}$$

$$(n = 2) : (10^2) \pmod{27} \implies 100 \pmod{27} \implies 19 \pmod{27}$$

$$(n = 3) : (10^3) \pmod{27} \implies 1000 \pmod{27} \implies 1 \pmod{27}$$

Since  $10^3$  is 1, this means that you could get rid of  $10^{3n}$  term, which along with the previous conditions and CAM means that if question 1's mod was replaced with 27 the if and only if statement would be true.