Math 1C03 Problem Sheet 5 Solutions

1) Tribonacci sequence: $T_1 = T_2 = T_3 = 1$

$T_n = T_{n-1} + T_{n-2} + T_{n-3}$ for $n \geq 4$

$P(n)$: $T_n < 2^n$.

(i)

$T_1 = 1$, $2^1 = 2$ so $P(1)$ holds

$T_2 = 1$, $2^2 = 4$ so $P(2)$ holds

$T_3 = 1$, $2^3 = 8$ so $P(3)$ holds

(ii) $T_4 = T_1 + T_2 + T_3 = 1 + 1 + 1$

$< 2 + 4 + 8$

$< 2^1 + 2^2 + 2^3$

$< 2(1 + 2 + 4)$

$< 2 \cdot 7$

$< 2 \cdot 8$

$T_4 < 2^4$.

Thus $P(4)$ holds.

(iii) Assume $P(i)$ holds for all $i \leq k$.

$T_{k+1} = T_k + T_{k-1} + T_{k-2}$

$T_{k+1} < 2^k + 2^{k-1} + 2^{k-2}$ by inductive hypothesis

$< 2^{k-2}(2^2 + 2 + 1)$

$< 2^{k-2} \cdot 7$

$< 2^{k-2} 2^3$

$T_{k+1} < 2^{k+1}$.

Thus the inductive hypothesis implies that $P(k+1)$ holds.

(iv) By strong induction, $P(n)$ holds for all n.

2) (i) Fermat's Little Theorem: if p is prime and $p \nmid a$ then $a^{p-1} \equiv 1 \bmod p$.

Apply with $a = 10$. If p is a prime $p \neq 2$ and $p \neq 5$ then $p \nmid 10$. So by FLT,

$\Rightarrow 10^{p-1} \equiv 1 \bmod p$. Thus $r = p-1$.

(ii) If p, q are primes and $p \neq 2$, $p \neq 5$ and $q \neq 2$, $q \neq 5$. By FLT $10^{p-1} \equiv 1 \bmod p$.

As the only primes that divide 10^{p-1} are 2 and 5, can apply FLT with $a = 10^{p-1}$

to deduce that $(10^{p-1})^{q-1} \equiv 1 \bmod q$.

We want to show that also $(10^{p-1})^{q-1} \equiv 1 \bmod pq$.

We have $(10^{p-1})^{q-1} - 1 = mq$ for some integer m.

Now $(10^{p-1})^{q-1} - 1 = (10^{p-1} - 1)\left((10^{p-1})^{q-2} + (10^{p-1})^{q-3} + \ldots + 10^{p-1} + 1\right)$

(In general, because 1 is a root of $X^n - 1$, then $X - 1$ is a factor of $X^n - 1$).

As $p \mid (10^{p-1} - 1)$, also $p \mid \left((10^{p-1})^{q-1} - 1\right)$.

We thus have $(10^{p-1})^{q-1} - 1 = pM = qN$ for some integers M and N. As ~~$p \nmid pM$ and~~ $p \mid qN$ and $p \nmid q$, also $p \mid N$. Thus

$(10^{p-1})^{q-1} - 1 = pqN'$ i.e. is divisible by pq.

(iii) This is a rather challenging problem, and does not work exactly as outlined on the Problem Sheet. Argue as in the proof of FLT in class to show that

$10^{p^i - 1} \equiv 1 \bmod p^i$ for any $i \geq 1$.

(in fact, $a^{p^{i-1}} \equiv 1 \bmod p^i$ if $\gcd(a, p) = 1$)

iv) Let $n = p_1^{m_1} \cdots p_s^{m_s}$, where p_i are all distinct primes.

As $\gcd(n,10) = 1$, $p_i \neq 2$ and $p_i \neq 5$ for all i.

Show by induction on s that there is $r \in \mathbb{Z}^+$ s.t.

$10^r \equiv 1 \mod n$ (this is the property $P(s)$).

Base case $s=1$: Then $n = p^s$. The fact that $P(1)$ holds was shown in (iii).

Inductive step: Assume that, if $n = p_1^{m_1} \cdots p_k^{m_k}$ then there is a positive integer r_k st $10^{r_k} \equiv 1 \mod n$.

Now let $n = p_1^{m_1} \cdots p_k^{m_k} p_{k+1}^{m_{k+1}}$.

By IH, $10^{r_k} \equiv 1 \mod p_1^{m_1} \cdots p_k^{m_k}$

By ~~[illegible]~~, the proof of (iii),

$$(10^{r_k})^{p_{k+1}^{m_{k+1}} - 1} \equiv 1 \mod p_{k+1}^{m_{k+1}}$$

as in the proof of (ii),

$$(10^{r_k})^{p_{k+1}^{m_{k+1}} - 1} - 1 = (10^{r_k} - 1) f(10^{r_k}), \text{ where}$$

f is a polynomial of degree $p_{k+1}^{m_{k+1}} - 2$.

As $p_1^{m_1} \cdots p_k^{m_k}$ divides $10^{r_k} - 1$, it also divides

$(10^{r_k})^{p_{k+1}^{m_{k+1}}} - 1$.

thus $(10^{r_k})^{p_{k+1}^{m_{k+1}}} - 1 = p_1^{m_1} \cdots p_k^{m_k} M$

and $(10^{r_k})^{p_{k+1}^{m_{k+1}}} - 1 = p_{k+1}^{m_{k+1}} N$

for some integers M and N.

So $p_{k+1}^{m_{k+1}}$ divides $p_1^{m_1} \cdots p_k^{m_k} M$.

As the primes are all distinct, $p_{k+1}^{m_{k+1}}$ divides M.

Hence $p_1^{m_1} \cdots p_{k+1}^{m_{k+1}}$ divides $(10^{r_k})^{p_{k+1}^{m_{k+1}}} - 1$,

and the next required r is $r_k p_{k+1}^{m_{k+1}}$.

This finishes the inductive step, so concludes the proof.

v) In the notation of the proof of Theorem 5.43, we have

$$10 r_i = a_{i+1} n + r_{i+1}$$

$$10 r_{i+1} = a_{i+2} n + r_{i+2}$$

$$\vdots$$

$$10 r_{i+s-1} = a_{i+s} n + r_{i+s} = a_{i+s} n + r_i,$$

as $r_i = r_{i+s}$.

Sequentially substitute for r_{i+j} into the previous equation as follows:

$$10^s r_i = 10^{s-1}(a_{i+1}n + r_{i+1})$$

$$= 10^{s-1}a_{i+1}n + 10^{s-2}(10r_{i+1})$$

$$= 10^{s-1}a_{i+1}n + 10^{s-2}(a_{i+2}n + r_{i+2})$$

$$= 10^{s-1}a_{i+1}n + 10^{s-2}a_{i+2}n + 10^{s-3}a_{i+3}n + 10^{s-3}r_{i+3}$$

$$= \sum_{j=1}^{s-1} 10^{s-j}a_{i+j}n + a_{i+s}n + r_{i+s}$$

$$10^s r_i = \sum_{j=1}^{s} 10^{s-j}a_{i+j}n + r_i$$

Subtracting: $(10^s - 1)r_i = \left(\sum_{j=1}^{s} 10^{s-j}a_{i+j}\right)n$.

thus $n \mid (10^s - 1)r_i$. (*)

this calculation started with $1 = bn + r_0$, and recall from Prop 2.21 that $\gcd(1, n) = \gcd(n, r_0) = 1$. At every step of the calculation, $\gcd(n, r_j) = 1$. By Prop 2.28, it follows from (*) that $n \mid (10^s - 1)$, as required.

vi) Suppose $\frac{1}{n}$ has a periodic decimal expansion with period s. As shown in v), then $n \mid (10^s - 1)$.

Suppose there is $r < s$ s.t. $n \mid (10^r - 1)$.

Write $\frac{1}{n} = 0.a_1 \ldots a_k \overline{a_{k+1} \cdots a_{k+s}}$

and $10^k \frac{1}{n} = a_1 \ldots a_k . \overline{a_{k+1} \cdots a_{k+s}}$

Multiply by 10^r: $10^r \, 10^k \frac{1}{n} = a_1 \ldots a_k \, a_{k+1} \ldots a_{k+r} \bullet \overline{a_{k+r+1} \ldots a_{k+s} \, a_{k+1} \ldots a_{k+s}}$

Subtract: $(10^r - 1) \, 10^k \frac{1}{n} = a_1 \ldots a_k \, a_{k+1} \ldots a_{k+r} - a_1 \ldots a_k$

$+ 0.a_{k+r+1} \ldots a_{k+s} \, a_{k+1} \ldots a_{k+s}$

$- 0.a_{k+1} \ldots a_{k+s}$.

Notice that the terms after the decimal point do not cancel out, so the ~~left~~ right hand side is not an integer.

But $n \mid (10^r - 1)$, so the left hand side is an integer. This contradiction proves that there is no r smaller than s with $n \mid (10^r - 1)$.

To prove the other direction, suppose that s is the least integer s.t. $10^s \equiv 1 \bmod n$. As $\frac{1}{n}$ is rational, it has a periodic decimal expansion. The same calculation shows that this period must be s.