Discrete Maths Supervision Work 2

Morgan Saville

November 17, 2020

1 2.2

1. $(i, k, l, m) = (-1, 1, 6, 5)$ meets the requirement

2. **RTP:** $\forall N\, \forall k_0, k_1.k_2, ...k_N\, (\exists a\, \sum_{i=0}^{N} k_i 10^i = 3a \iff \exists b\, \sum_{i=0}^{N} k_i = 3b)$
   Let N arbitrary natural number, and let $k_0, k_1, k_2, ..., k_N$ arbitrary natural numbers.
   First we prove '$\Rightarrow$'.
   Assume $\exists a\, \sum_{i=0}^{N} k_i 10^i = 3a$
   Instantiating, let a such that $\sum_{i=0}^{N} k_i 10^i = 3a$
   RTP: $\exists b\, \sum_{i=0}^{N} k_i = 3b$

   INCOMPLETE

3. **RTP:** $\forall n\, (\text{rem}(n^2 + 1, 4) = 0 \vee \text{rem}(n^2 + 1, 4) = 1)$

   C0:
   $n = 2k$ for some integer k
   $\text{rem}(n^2, 4) = \text{rem}((2k)^2, 4) = \text{rem}(4k^2, 4) = 0$

   C1:
   $n = 2k + 1$ for some integer k
   $\text{rem}(n^2, 4) = \text{rem}((2k + 1)^2, 4) = \text{rem}(4k^2 + 4k + 1, 4) = \text{rem}(4(k^2 + k) + 1, 4) = 1$

   Since the above cases are exhaustive, we have shown the required statement.

4.
   (a) $\text{rem}(55^2, 79) = \text{rem}(3025, 79) = 23$
   (b) $\text{rem}(23^2, 79) = \text{rem}(529, 79) = 55$
   (c) $\text{rem}(23 \cdot 55, 79) = \text{rem}(1265, 79) = 1$
   (d)

$$\begin{aligned}
\text{rem}(55^{78}, 79) &= \text{rem}((55^2)^{39}, 79) \\
&= \text{rem}(23^{39}, 79) \\
&= \text{rem}(23 \cdot (23^2)^{19}, 79) \\
&= \text{rem}(23 \cdot 55 \cdot (55^2)^9, 79) \\
&= \text{rem}(23 \cdot (23^2)^4, 79) \\
&= \text{rem}(23 \cdot 55^2 \cdot 55^2, 79) \\
&= \text{rem}(23 \cdot 23 \cdot 23, 79) \\
&= \text{rem}(55 \cdot 23, 79) \\
&= 1
\end{aligned}$$

5.

$$
\begin{aligned}
2^{153} &\equiv 2 \cdot (2^8)^{19} \\
&\equiv 2 \cdot 256^{19} \\
&\equiv 2 \cdot 103^{19} \\
&\equiv 206 \cdot (103^2)^9 \\
&\equiv 53 \cdot 10609^9 \\
&\equiv 53 \cdot 52^9 \\
&\equiv 2756 \cdot (52^2)^4 \\
&\equiv 2 \cdot (103^2)^2 \\
&\equiv 2 \cdot 52^2 \\
&\equiv 2 \cdot 103 \\
&\equiv 206 \\
&\equiv 53 \pmod{153}
\end{aligned}
$$

This does not contradict Fermat's Little Theorem because 153 is not prime.

6.

(a) $\mathbb{Z}_3$

a	b	$a+b$	ab	$-b$	$\frac{1}{b}$
0	0	0	0	0	
0	1	1	0	2	1
0	2	2	0	1	2
1	1	2	1		
1	2	0	2		
2	2	1	1		

(b) $\mathbb{Z}_6$

a	b	$a+b$	ab	$-b$	$\frac{1}{b}$
0	0	0	0	0	
0	1	1	0	5	1
0	2	2	0	4	
0	3	3	0	3	
0	4	4	0	2	
0	5	5	0	1	5
1	1	2	1		
1	2	3	2		
1	3	4	3		
1	4	5	4		
1	5	0	5		
2	2	4	4		
2	3	5	0		
2	4	0	2		
2	5	1	4		
3	3	0	3		
3	4	1	0		
3	5	2	3		
4	4	2	4		
4	5	3	2		
5	5	4	1		

(c) $\mathbb{Z}_7$

a	b	$a+b$	ab	$-b$	$\frac{1}{b}$
0	0	0	0	0	
0	1	1	0	6	1
0	2	2	0	5	4
0	3	3	0	4	5
0	4	4	0	3	2
0	5	5	0	2	3
0	6	6	0	1	6
1	1	2	1		
1	2	3	2		
1	3	4	3		
1	4	5	4		
1	5	6	5		
1	6	0	6		
2	2	4	4		
2	3	5	6		
2	4	6	1		
2	5	0	3		
2	6	1	5		
3	3	0	2		
3	4	0	5		
3	5	1	1		
3	6	2	4		
4	4	1	2		
4	5	2	6		
4	6	3	3		
5	5	3	4		
5	6	4	2		
6	6	5	1		

7. Assume $n^3 \equiv (\text{rem}(n,6))^3 \pmod 6$. We can therefore check all possibilities for $\text{rem}(n,6)$

$\text{rem}(n,6)$	$(\text{rem}(n,6))^3$	$\text{rem}((\text{rem}(n,6))^3,6)$
0	0	0
1	1	0
2	8	6
3	27	3
4	64	4
5	125	5

Since $\text{rem}((\text{rem}(n,6))^3,6) \equiv (\text{rem}(n,6))^3 \equiv n^3 \pmod 6$, we can see that $\forall n\, n^3 \equiv n \pmod 6$

8. Assume $n \equiv 1 \pmod{p-1}$.
Equivalently, assume $n = j(p-1)+1$ for some integer j
RTP: $\forall i$ not multiple of p $i^n \equiv i \pmod p$
By universal instantiation, let i some positive integer not a multiple of p.
RTP: $i^n \equiv i \pmod p$
Equivalently, **RTP:** $i^n = kp + i$ for some integer k.
Substituting n into the left-hand side,

$$\begin{aligned} i^{j(p-1)+1} &\equiv i^{jp+(1-j)} \\ &\equiv (i^p)^j \cdot i^{1-j} \\ &\equiv i^j \cdot i^{(}1-j) \text{ by Fermat's Little Theorem} \\ &\equiv i^1 \\ &\equiv i \pmod p \end{aligned}$$

As required.

9. $n^7 \equiv n \pmod 7$ By question 8
$n^7 \equiv n^3n^3n \equiv n \cdot n \cdot n \equiv n^3 \equiv n \pmod 6$ By question 7
We can therefore claim that $n^7 \equiv 36n + 7n \pmod{42}$ and we prove this below by showing that this solution satisfies both of the above equations:

   (a) $n^7 \equiv (36n + 7n) \equiv 1n + 0 \equiv n \pmod 7$

(b) $n^7 \equiv (36n + 7n) \equiv 0 + 1n \equiv n \pmod 6$

Therefore, $n^7 \equiv 43n \equiv n \pmod{42}$ as required.

2 2.3

1. **RTP:** $\forall n\, ((\exists i, j\; n = i^2 - j^2) \iff (n \equiv 0 \pmod 4 \lor n \equiv 1 \pmod 4 \lor n \equiv 3 \pmod 4))$ Let n arbitrary integer.
First we prove '$\Leftarrow$'.
RTP: $\exists i, j\; n = i^2 - j^2$
Note that the following cases are exhaustive but not mutually exclusive.

C0:
$n \equiv 0 \pmod 4$
$\therefore n = 4a$ for some integer a
$\therefore n = (a+1)^2 - (a-1)^2$

C1:
$n \equiv 1 \pmod 4$
$\therefore n = 4a + 1$ for some integer a
$\therefore n = (2a+1)^2 - (2a)^2$

C2:
$n \equiv 3 \pmod 4$
$\therefore n = 4a + 3$ for some integer a
$\therefore n = (2a+2)^2 - (2a+1)^2$

Now we prove '$\Rightarrow$'
Assume $\exists i, j\; n = i^2 - j^2$
Let i, j such that $n = i^2 - j^2 = (i-j)(i+j)$
RTP: $n \equiv 0 \pmod 4 \lor n \equiv 1 \pmod 4 \lor n \equiv 3 \pmod 4$

C0:
i is odd and j is odd
Therefore $i - j = 2a, i + j = 2b$ for some integers a, b
Therefore $n = (i-j)(i+j) = 4ab \equiv 0 \pmod 4$

C1:
Exactly one of i and j is even. Without loss of generality, take i is odd and j is even.
Therefore $i - j = 2a + 1, i + j = 2b + 1$ for some integers a, b
Therefore $n = (i-j)(i+j) = 4ab + 2(a+b) + 1 \equiv 2c + 1 \pmod 4$ where $c = a + b$
Therefore $n \equiv 1 \pmod 4 \lor n \equiv 3 \pmod 4$

C2:
i is even and j is even
Therefore $i - j = 2a, i + j = 2b$ for some integers a, b
Therefore $n = (i-j)(i+j) = 4ab \equiv 0 \pmod 4$

2.

(a) 1, 11, 111
1, 3, 7

(b) The k^{th} decimal repunit in base n can be written as $\frac{n^k-1}{n-1}$
Consider the expression $(2a)^k - 1 \pmod{}4$ in the two following exhaustive cases

C0:
$k2i$ for some integer i

$$\begin{aligned}(2a)^k - 1 &\equiv 4^i \cdot a^k - 1 \\ &\equiv -1 \\ &\equiv 3 \pmod 4\end{aligned}$$

C1:
$k = 2i + 1$ for some integer i

$$\begin{aligned}(2a)^l - 1 &\equiv 4^i \cdot 2 \cdot a^k - 1 \\ &\equiv -1 \\ &\equiv 3 \pmod 4\end{aligned}$$

As such, the expression is always congruent to $3 \pmod 4$.
Next, note that $n-1$ is a square number $\Rightarrow$ ($\frac{n^k-1}{n-1}$ is a square number $\Rightarrow n^k - 1$ is a square number)
Therefore, for all bases n such that n is even and $n-1$ is square (for example, $n = 2$ or $n = 10$), then $\frac{n^k-1}{n-1} \equiv 3 \pmod 4$, which, by Lemma 26, means it cannot be a square number.