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

   Rephrase as
   $\sum 10^i a_i \equiv 0 \pmod 3$
   $\iff$
   $\sum a_i \equiv 0 \pmod 3$
   and use that
   $10 \equiv 1 \pmod 3$

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

   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)

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

follows directly from FLT, so no need to calculate

5.

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

Correct. We will see another proof in person as well, using that $153 = 9 \cdot 17$

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		

When asked for tables for some binary operation, it is common to make a square, e.g.

$(\mathbb{Z}_3,+)$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

· since we can easily read information from it,

- symmetry along diagonal = commutativity
- first row is same as "header" means $0 + a = a$

etc.

(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		

You know $n^3 \equiv \text{rem}(n,6)^3 \pmod 6$ by 2.1.2b or c. That says nothing about n^3 and n though. Instead show that $n^3 - n = (n-1)n(n+1) \equiv 0 \pmod 6$

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,

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

Here $1-j$ might be negative, so you use that mult. inverses mod p exist and are unique. More directly, FLT says $i^{p-1} \equiv 1$, so $i^{j(p-1)+1} \equiv (i^{p-1})^j \cdot i \equiv i$

As required.

9. $n^7 \equiv n \pmod 7$ By question 8
$n^7 \equiv n^3 n^3 n \equiv n \cdot n \cdot n \equiv n^3 \equiv n \pmod 6$ 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:

Why same n?

(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.

$n^7 \equiv n \pmod 6$ by above
$n^7 \equiv n \pmod 7$ by FLT
So $6 \mid n^7 - n$, $7 \mid n^7 - n$ & 6, 7 coprime
Thus $6 \cdot 7 \mid n^7 - n$.

2 2.3

1. **RTP:** $\forall n\, ((\exists i, j\; n = i^2 - j^2) \iff (n \equiv 0 \pmod 4 \vee n \equiv 1 \pmod 4 \vee n \equiv 3 \pmod 4)))$ 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.~~

   They are n can not be 0 and 1 mod 4 at the same time for example.

   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: $n \equiv 0 \pmod 4 \vee n \equiv 1 \pmod 4 \vee n \equiv 3 \pmod 4$

   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 $n \equiv 1 \pmod 4 \vee n \equiv 3 \pmod 4$

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

   Since you work mod 4, you can also use 2.3.3 and observe that

i^2	j^2	$n = i^2 - j^2$
0	0	0
0	1	3
1	0	1
1	1	0

   is exhaustive.

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 $(2a)^k - 1$ (mod ()4) in the two following exhaustive cases

   C0:
   $k2i$ for some integer i

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

   for $i \geq 1$ or equiv. $k \geq 2$.

   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 (mod 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.

Great proof!

Another idea: If $n = 2m$ is even, then for $k \geq 1$,

$$1+n+\dots+n^k \equiv 1+n+4\sum_{i=2}^{k} 2^{i-2} m^i$$

$$\equiv 1+n \pmod 4$$

so it suffices to have n even

- $1+n \equiv 3 \pmod 4$.

What happens for other bases? Can you find a counterexample to show this is not always true?