Harry Langford
hjel2@cam.ac.uk

2 On numbers

2.1 Basic exercises

1. Let i, j be integers and let m, n be positive integers. Show that:

   (a) $i \equiv i (\text{mod } m)$

$$\begin{gathered} m|0 \iff \\ m|(i-i) \iff \\ i - i \equiv 0(\text{mod } m) \iff \\ i \equiv i(\text{mod } m) \text{ as required} \end{gathered} \tag{1}$$

   (b) $i \equiv j(\text{mod } m) \implies j \equiv i(\text{mod } m)$

$$\begin{gathered} i \equiv j(\text{mod } m) \iff \\ \exists k \in \mathbb{Z} : i \equiv j + k \cdot m \iff \\ \exists k \in \mathbb{Z} : j \equiv i - k \cdot m \iff \\ j \equiv i(\text{mod } m) \text{ as required} \end{gathered} \tag{2}$$

I'm used to seeing dot instead of colon: "$\exists k \in \mathbb{Z} . (\ldots)$"

   (c) $i \equiv j(\text{mod } m) \wedge j \equiv k(\text{mod } m) \implies i \equiv k(\text{mod } m)$

Confusing solution!

labels for future ref. usually go on the right end just like (2), (3).

$$\begin{gathered} i \equiv j(\text{mod } m) \iff \\ (a)\ j \equiv i(\text{mod } m) \text{ using } (2) \\ j \equiv k(\text{mod } m) \iff \\ (b)\ i(\text{mod } m) \equiv k(\text{mod } m) \iff \\ \text{Combining (a) and (b) gives:} \\ \exists a, b : i + a \cdot m \equiv k + b \cdot m) \iff \\ \exists a, b : i \equiv k + (b - a) \cdot m \iff \\ i \equiv k(\text{mod } m) \text{ as required} \end{gathered} \tag{3}$$

where did this come from? It's the statement you're RTP

was this meant to be here?

2. Prove that for all integers i, j, k, l, m, n with m positive and n nonnegative,

   (a) $i \equiv j(\text{mod } m) \wedge k \equiv l(\text{mod } m) \implies i + k \equiv j + l(\text{mod } m)$

$$\begin{gathered} i \equiv j(\text{mod } m) \iff \\ (a)\ \exists a \in \mathbb{Z} : i \equiv j + a \cdot m \\ k \equiv l(\text{mod } m) \iff \\ (b)\ \exists b \in \mathbb{Z} : k \equiv l + b \cdot m \\ \text{Adding (a) and (b) gives:} \\ \exists a, b \in \mathbb{Z} : i + k \equiv j + a \cdot m + l + b \cdot m \iff \\ \exists a, b \in \mathbb{Z} : i + k \equiv j + l + (a + b) \cdot m \iff \\ i + k \equiv j + l(\text{mod } m) \end{gathered} \tag{4}$$

these are just "=" not "≡".

Otherwise, nice and clear proof!

   (b) $i \equiv j(\text{mod } m) \wedge k \equiv l(\text{mod } m) \implies i \cdot k \equiv j \cdot l(\text{mod } m)$

$$
\begin{aligned}
i \equiv j(\text{mod } m) &\iff \\
(a)\exists p \in \mathbb{Z} : i &= j + p \cdot m \\
k \equiv l(\text{mod } m) &\iff \\
(b)\exists q \in \mathbb{Z} : k &= l + q \cdot m \\
&\text{Combining (a) and (b) gives:} \\
&\exists p, q \in \mathbb{Z} : i \cdot k = (j + p \cdot m) \cdot (l + q \cdot m) \iff \\
&\exists p, q \in \mathbb{Z} : i \cdot k = j \cdot l + j \cdot q \cdot m + l \cdot p \cdot m + p \cdot q \cdot m \cdot m \iff \\
&\exists p, q \in \mathbb{Z} : i \cdot k = j \cdot l + (j \cdot q + l \cdot p + p \cdot q \cdot m) \cdot m \iff \\
i \cdot k &\equiv j \cdot l(\text{mod } m)
\end{aligned} \tag{5}
$$

✓

(c) $i \equiv j(\text{mod } m) \implies i^n \equiv j^n(\text{mod } m)$

Proof by induction:

At $n = 0$:

$$
\begin{aligned}
\forall m \in \mathbb{Z} : 1 \equiv 1(\text{mod } m) &\iff \\
\forall m \in \mathbb{Z} : i^0 \equiv j^0(\text{mod } m)
\end{aligned} \tag{6}
$$

✓

So the statement is true for $n = 0$.

Assume that the statement also holds true for $n = k$.

$$
\begin{aligned}
(a)\ i^k &\equiv j^k(\text{mod } m) \\
(b)\ i &\equiv j(\text{mod } m) \\
&\text{Using 5 we can combine (a) and (b)} \\
\therefore i^k \cdot i &\equiv j^k \cdot j(\text{mod } m) \iff \\
i^{k+1} &\equiv j^{k+1}(\text{mod } m)
\end{aligned} \tag{7}
$$

Make it explicit you've assuming this to prove the implication for $n=k+1$.

redundant

So if the statement holds for $n = k$, then it also holds for $n = k + 1$. Since the statement is true for $n = 0$; by induction it must also be true for all $n \in \mathbb{N}$. ✓

3. Prove that for all natural numbers k, l and positive integers m,

(a) $\text{rem}(k \cdot m + l, m) = \text{rem}(l, m)$

Proof by contradiction:

$$
\begin{aligned}
\text{Assume } \text{rem}(k \cdot m + l, m) &\neq \text{rem}(l, m) \\
\text{rem}(k \cdot m + l, m) \neq \text{rem}(l, m) &\iff \\
k \cdot m + l \neq l(\text{mod } m) &\iff \\
l \neq l(\text{mod } m)
\end{aligned} \tag{8}
$$

Correct but if you have equivalences everywhere, you didn't really need to prove it by contrad.!

However, from (1) $\forall i, m \in \mathbb{Z} : i \equiv i(\text{mod } m)$.
So our initial assumption must be wrong – hence $\text{rem}(k \cdot m + l, m) = \text{rem}(l, m)$.

(b) $\text{rem}(k + l, m) = \text{rem}(\text{rem}(k, m) + l, m)$

Proof by contradiction:

Same here!

$$
\begin{aligned}
\text{Assume } \text{rem}(k + l, m) &\neq \text{rem}(\text{rem}(k, m) + l, m) \\
\text{rem}(k + l, m) \neq \text{rem}(\text{rem}(k, m) + l, m) &\iff \\
k + l \neq \text{rem}(k, m) + l(\text{mod } m) &\iff \\
k + l \neq k + l(\text{mod } m)
\end{aligned} \tag{9}
$$

Just change $\neq$ to $=$ and you have a proof
$\text{rem}(km+l,m) = \text{rem}(l,m) \iff l \equiv l(\text{mod } m)$. QED

However, from (1) $\forall i, m \in \mathbb{Z} : i = i(\text{mod } m)$.
So our initial assumption must be wrong – hence $\text{rem}(k+l, m) = \text{rem}(\text{rem}(k, m)+l, m)$.

(c) $\text{rem}(k \cdot l, m) = \text{rem}(k \cdot \text{rem}(l, m), m)$

Proof by contradiction:

$$\begin{aligned}
\text{Assume } \text{rem}(k \cdot l, m) &\neq \text{rem}(k \cdot \text{rem}(l, m), m) \\
\text{rem}(k \cdot l, m) &\neq \text{rem}(k \cdot \text{rem}(l, m), m) \iff \\
k \cdot l &\neq k \cdot \text{rem}(l, m)(\text{mod } m) \iff \\
\forall a \in \mathbb{Z} : k \cdot l &\neq k \cdot l + (a \cdot k) \cdot m(\text{mod } m) \iff \\
k \cdot l &\neq k \cdot l(\text{mod } m)
\end{aligned} \tag{10}$$

~~what~~ not clear how this happened? Explain.

Can just use rem$(l, m) \equiv l$ (mod m)

However, from (1) $\forall i, m \in \mathbb{Z} : i = i(\text{mod } m)$.
So our initial assumption must be wrong – hence $\text{rem}(k \cdot l, m) = \text{rem}(k \cdot \text{rem}(l, m), m)$. ✓

4. Let m be a positive integer.

(a) Prove the associativity of the addition and multiplication operations in $\mathbb{Z}_m$; that is:

$$\forall i, j, k \in \mathbb{Z}_m.(i +_m j) +_m k = i +_m (j +_m k) \text{ and } (i \cdot_m j) \cdot_m k = i \cdot_m (j \cdot_m k) \tag{11}$$

Proof of the associativity of the addition operation in $\mathbb{Z}_m$:

$$\begin{aligned}
&\forall i, j, k \in \mathbb{Z}_m : s = (i +_m j) +_m k \iff \\
&\forall i, j, k \in \mathbb{Z}_m : s = (i + j)(\text{mod } m) + k(\text{mod } m) \iff \\
&\forall i, j, k \in \mathbb{Z}_m : s = i + j + k(\text{mod } m) \iff \\
&\forall i, j, k \in \mathbb{Z}_m : s = i + (j + k(\text{mod } m))(\text{mod } m) \iff \\
&\qquad \therefore \forall i, j, k \in \mathbb{Z}_m.(i +_m j) +_m k = i +_m (j +_m k) \text{ as required}
\end{aligned} \tag{12}$$

Be careful with notation. Only usage of (mod m) that's defined is in: $x \equiv y$ (mod m).

You probably should use the rem function in these exercises, defining $i +_m j$ to mean rem$(i+j, m)$ and then you can do reasoning about integers and use properties of rem function from prev. exercise.

Proof of the associativity of the multiplication operation in $\mathbb{Z}_m$:

$$\begin{aligned}
&\forall i, j, k \in \mathbb{Z}_m : p = (i \cdot_m j) \cdot_m k \iff \\
&\forall i, j, k \in \mathbb{Z}_m : p = (i \cdot j(\text{mod } m))) \cdot k(\text{mod } m) \iff \\
&\forall i, j, k \in \mathbb{Z}_m : p = i \cdot j \cdot k(\text{mod } m) \iff \\
&\forall i, j, k \in \mathbb{Z}_m : p = i \cdot (j \cdot k(\text{mod } m))(\text{mod } m) \iff \\
&\qquad \therefore \forall i, j, k \in \mathbb{Z}_m : i \cdot_m (j \cdot_m k) \text{ as required}
\end{aligned} \tag{13}$$

(b) Prove that the additive inverse of k in $\mathbb{Z}_m$ is $[-k]_m$.

$$\begin{aligned}
[-k]_m &= -k + m \iff \\
k + [-k]_m &\equiv k - k + m(\text{mod } m) \iff \\
k + [-k]_m &\equiv m(\text{mod } m) \iff \\
k + [-k]_m &\equiv 0(\text{mod } m)
\end{aligned} \tag{14}$$

Since $k + [-k]_m \equiv 0(\text{mod } m)$; $[-k]_m$ is the additive inverse of k in $\mathbb{Z}_m$ as required.

2.2 Core exercises

1. Find an integer i, natural numbers k, l and a positive integer m for which $k \equiv l(\text{mod } m)$ holds while $i^k \equiv i^l(\text{mod } m)$ does not.

Wikipedia says 0^0 has no agreed upon value :p

$$i = 0,\ k = 0,\ l = 2,\ m = 2$$

$$\begin{aligned} 0 &\equiv 2 (\text{mod } 2) \implies \\ k &\equiv l (\text{mod } m) \end{aligned} \tag{15}$$

$$\begin{aligned} 1 &\not\equiv 0 (\text{mod } 2) \iff \\ 0^0 &\not\equiv 0^2 (\text{mod } 2) \implies \\ i^k &\not\equiv i^l (\text{mod } m) \end{aligned} \tag{16}$$

2. Formalise and prove the following statement: A natural number is a multiple of 3 iff so is the number obtained by summing its digits. Do the same for analogous criterion for multiples of 9 and a similar condition for multiples of 11.

$$\begin{aligned} &\text{Let } a_i \text{ be the } i^{th} \text{ digit of } n \in \mathbb{Z}. \\ &n \equiv \sum_{i=0}^{\infty} a_i \cdot 10^i (\text{mod } 3) \iff \\ &n \equiv \sum_{i=0}^{\infty} a_i + a_i \cdot (10^i - 1) (\text{mod } 3) \iff \\ \text{Since } 10^i - 1 \equiv 0 (\text{mod } 3) : &n \equiv \sum_{i=0}^{\infty} a_i (\text{mod } 3) \\ &n \equiv 0 (\text{mod } 3) \iff 3|n \\ \therefore &\sum_{i=0}^{\infty} a_i \equiv 0 (\text{mod } 3) \iff 3|n \end{aligned} \tag{17}$$

I'd just go from here to $3|n \iff 3|\Sigma a_i$.

✓

Authors may have hoped you'd prove this

$$\begin{aligned} &\text{Let } a_i \text{ be the } i^{th} \text{ digit of } n \in \mathbb{Z}. \\ &n \equiv \sum_{i=0}^{\infty} a_i \cdot 10^i (\text{mod } 9) \iff \\ &n \equiv \sum_{i=0}^{\infty} a_i + a_i \cdot (10^i - 1) (\text{mod } 9) \iff \\ \text{Since } 10^i - 1 \equiv 0 (\text{mod } 9) : &n \equiv \sum_{i=0}^{\infty} a_i (\text{mod } 9) \\ &n \equiv 0 (\text{mod } 9) \iff 9|n \\ \therefore &\sum_{i=0}^{\infty} a_i \equiv 0 (\text{mod } 9) \iff 9|n \end{aligned} \tag{18}$$

✓

And not this cause it's fake!

$$\begin{aligned} &\text{Let } a_i \text{ be the } i^{th} \text{ digit of } n \in \mathbb{Z}. \\ &n \equiv \sum_{i=0}^{\infty} a_i \cdot 10^i (\text{mod } 11) \iff \\ &n \equiv \sum_{i=0}^{\infty} a_i + a_i \cdot (10^i - 1) (\text{mod } 11) \iff \\ \text{Since } 10^i - 1 \equiv 0 (\text{mod } 11) : &n \equiv \sum_{i=0}^{\infty} a_i (\text{mod } 11) \\ &n \equiv 0 (\text{mod } 11) \iff 11|n \\ \therefore &\sum_{i=0}^{\infty} a_i \equiv 0 (\text{mod } 11) \iff 11|n \end{aligned} \tag{19}$$

✗

3. Show that for every integer n, the remainder when n^2 is divided by 4 is either 0 or 1.

   This can be divided into two cases: n is even or n is odd:

$$\begin{aligned} &n \text{ is even:} \\ &\exists k \in \mathbb{Z} : n = 2 \cdot k \\ \therefore\ &\exists k \in \mathbb{Z} : n = 2 \cdot k (\text{mod } 4) \\ &n^2 = 4 \cdot k^2 (\text{mod } 4) \\ &n^2 = 0 (\text{mod } 4) \\ \therefore\ &n^2 \text{ divided by 4 is 0.} \end{aligned} \tag{20}$$

✓

So if n is even; the remainder when n^2 is divided by 4 is 0.

$$\begin{aligned} &n \text{ i odd:} \\ &\exists k \in \mathbb{Z} : n = 2 \cdot k + 1 \\ \therefore\ &\exists k \in \mathbb{Z} : n = 2 \cdot k + 1 (\text{mod } 4) \\ &n^2 = 4 \cdot k^2 + 4 \cdot k + 1 (\text{mod } 4) \\ &n^2 = 1 (\text{mod } 4) \end{aligned} \tag{21}$$

✓

So if n is odd; the remainder when n^2 is divided by 4 is 1.

Since every integer n is either even or odd; the remainder when n is divided by 4 is either 0 or 1. ✓

4. What are $\text{rem}(55^2, 79)$, $\text{rem}(23^2, 79)$, $\text{rem}(23 \cdot 55, 79)$ and $\text{rem}(55^{78}, 79)$?

$$\begin{aligned} &\text{rem}(55^2, 79) \\ =&\text{rem}(3025, 79) \\ =&23 \end{aligned} \tag{22}$$

$$\begin{aligned} &\text{rem}(23^2, 79) \\ =&\text{rem}(529, 79) \\ =&55 \end{aligned} \tag{23}$$

$$\begin{aligned} &\text{rem}(23 \cdot 55, 79) \\ =&\text{rem}(1265, 79) \\ =&1 \end{aligned} \tag{24}$$

$$\begin{aligned} &\text{rem}(55^{78}, 79) \\ =&1 \text{ using Fermat's Little Theorem} \end{aligned} \tag{25}$$

✓

5. Calculate that $2^{153} \equiv 53(\text{mod } 153)$. At first sight this seems to contradict Fermat's Little Theorem, why isn't this the case though? *Hint*: Simplify the problem by applying known congruences to subexpressions.

   This does not contradict Fermat's Little Theorem since 153 is not prime and Fermat's Little Theorem only applies to primes.

✓ Nice and to the point.

Another way is to not decompose 153 but go:

$2^8 = 256 \equiv \ldots \pmod{153}$

$2^{16} \equiv \ldots^2$

$2^{32} \equiv \ldots$

$2^{64} \equiv \ldots$

$2^{128} \equiv \ldots$

by squaring and taking remainder,

And then:

$2^{153} = 2^{128} \cdot 2^{16} \cdot 2^8 \cdot 2^1 \equiv \ldots \cdot \ldots \cdot \ldots \cdot \ldots \equiv \ldots$

$$
\begin{aligned}
2^6 &\equiv 64 (\text{mod } 9) \iff \\
2^6 &\equiv 1 (\text{mod } 9) \iff \\
\text{using (7): } (2^6)^{25} &\equiv 1^{25} (\text{mod } 9) \iff \\
2^{150} &\equiv 1 (\text{mod } 9) \iff \\
2^{153} &\equiv 8 (\text{mod } 9) \iff \\
2^{153} &\equiv 8 + 9 \cdot 56 (\text{mod } 9) \iff \\
2^{153} &\equiv 512 (\text{mod } 9) \iff \\
2^{153} - 512 &\equiv 0 (\text{mod } 9) \\
\text{using Fermat's Little Theorem: } 2^{17} &\equiv 2 (\text{mod } 17) \iff \\
\text{using (7): } (2^{17})^9 &\equiv 2^9 (\text{mod } 17) \iff \\
2^{153} &\equiv 2^9 (\text{mod } 17) \iff \\
2^{153} &\equiv 512 (\text{mod } 17) \iff \\
2^{153} - 512 &\equiv 0 (\text{mod } 17) \\
(2^{153} - 512) \equiv 0 (\text{mod } 9) \wedge (2^{153} - 512) &\equiv 0 (\text{mod } 17) \iff \\
\exists i, j \in \mathbb{Z} : (2^{153} - 512) = 9 \cdot i \wedge (2^{153} - 512) &= 17 \cdot j \iff \\
\exists i, j \in \mathbb{Z} : 18 \cdot (2^{153} - 512) - 17 \cdot (2^{153} - 512) &= 18 \cdot (17 \cdot j) - 17 \cdot (9 \cdot i) \iff \\
\exists i, j \in \mathbb{Z} : 2^{153} - 512 &= 153 \cdot (2 \cdot j - i) \iff \\
2^{153} - 512 &\equiv 0 (\text{mod } 153) \iff \\
2^{153} &\equiv 512 (\text{mod } 153) \iff \\
2^{153} &\equiv 53 (\text{mod } 153) \text{ as required}
\end{aligned}
\tag{26}
$$

But this is cool too! Though requires more thinking to combine 9 & 17 (for now...)

6. Calculate the addition and multiplication tables, and the additive and multiplicative inverse tables for $\mathbb{Z}_3$, $\mathbb{Z}_6$ and $\mathbb{Z}_7$.

Additive table for $\mathbb{Z}_3$

	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Additive inverse table for $\mathbb{Z}_3$

	0	1	2
inverse	0	2	1

Multiplication table for $\mathbb{Z}_3$

	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Multiplicative inverse table for $\mathbb{Z}_3$

number	0	1	2
inverse		1	2

I trust you

Additive table for $\mathbb{Z}_6$

	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Additive inverse table for $\mathbb{Z}_6$

number	0	1	2	3	4	5
inverse	0	5	4	3	2	1

Multiplication table for $\mathbb{Z}_6$

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Multiplicative inverse table for $\mathbb{Z}_6$

number	0	1	2	3	4	5
inverse		1				5

✓

Additive table for $\mathbb{Z}_7$

	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Additive inverse table for $\mathbb{Z}_7$

number	0	1	2	3	4	5	6
inverse	0	6	5	4	3	2	1

Multiplication table for $\mathbb{Z}_7$

	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Multiplicative inverse table for $\mathbb{Z}_7$

number	0	1	2	3	4	5	6
inverse		1	4	5	2	3	6

7. Let i and n be positive integers and let p be a prime. Show that if $n \equiv 1 (\text{mod } p-1)$ then $i^n \equiv i (\text{mod } p)$ for all i not multiple of p.

   If i is not a multiple of p then we can use Fermat's Little Theorem:

$$\begin{aligned}
n &\equiv 1 (\text{mod } p-1) \iff \\
\exists k \in \mathbb{Z} : n &= 1 + (p-1) \cdot k \iff \\
\exists k \in \mathbb{Z} : i^n &\equiv i^{1+(p-1)\cdot k} (\text{mod } p) \iff \\
\exists k \in \mathbb{Z} : i^n &\equiv i \cdot (i^{p-1})^k (\text{mod } p) \iff \qquad (27) \\
\text{using Fermat's Little Theorem: } \exists k \in \mathbb{Z} : i^n &\equiv i \cdot 1^k (\text{mod } p) \iff \\
i^n &\equiv i \cdot 1 (\text{mod } p) \iff \\
i^n &\equiv i (\text{mod } p) \text{ as required}
\end{aligned}$$

Very nice! ✓

8. Prove that $n^3 \equiv n (\text{mod } 6)$ for all integers n.

$$\begin{gathered}
n^3 - n = (n-1)\cdot n\cdot(n+1) \\
\forall n \in \mathbb{Z} : 2|(n-1)\cdot n\cdot(n+1) \land 3|(n-1)\cdot n\cdot(n+1) \iff \\
\forall n \in \mathbb{Z} : \exists i, j \in \mathbb{Z} : (n-1)\cdot n\cdot(n+1) = 2\cdot i \land (n-1)\cdot n\cdot(n+1) = 3\cdot j \\
\forall n \in \mathbb{Z} : 3\cdot(n-1)\cdot n\cdot(n+1) - 2\cdot(n-1)\cdot n\cdot(n+1) = 3\cdot(2\cdot i) - 2\cdot(3\cdot j) \iff \\
\forall n \in \mathbb{Z} : (n-1)\cdot n\cdot(n+1) = 6\cdot(i-j) \iff \\
\forall n \in \mathbb{Z} : (n-1)n(n+1) \equiv 0 (\text{mod } 6) \iff \\
\forall n \in \mathbb{Z} : n^3 - n \equiv 0 (\text{mod } 6) \iff \\
\forall n \in \mathbb{Z} : n^3 \equiv n (\text{mod } 6) \text{ as required}
\end{gathered} \tag{28}$$

✓

9. Prove that $n^7 \equiv n(\text{mod } 42)$ for all integers n.

$$\begin{gathered}
\forall n \in \mathbb{Z} : n^7 - n = (n-1)\cdot n\cdot(n+1)\cdot(n^2-n+1)\cdot(n^2+n+1) \implies \\
\forall n \in \mathbb{Z} : \exists k \in \mathbb{Z} : n^7 - n = k\cdot n\cdot(n+1) \implies \\
\forall n \in \mathbb{Z} : 2|(n^7-n) \iff \\
\forall n \in \mathbb{Z} : n^7 - n \equiv 0(\text{mod } 2) \\
\forall n \in \mathbb{Z} : n^7 - n = (n-1)n(n+1)(n^2-n+1)(n^2+n+1) \implies \\
\forall n \in \mathbb{Z} : \exists k \in \mathbb{Z} : n^7 - n = k\cdot(n-1)\cdot n\cdot(n+1) \implies \\
\forall n \in \mathbb{Z} : 3|(n^7-n) \\
\forall n \in \mathbb{Z} : n^7 - n \equiv 0(\text{mod } 3) \\
\forall n \in \mathbb{Z} : n^7 \equiv n(\text{mod } 7) \text{ using Fermat's Little Theorem} \iff \\
\forall n \in \mathbb{Z} : n^7 - n \equiv 0(\text{mod } 7)
\end{gathered} \tag{29}$$

This is ~~also~~ good formatting but more visual separation would make it even easier to read. E.g. \vspace{0.5in}

$$\begin{gathered}
\forall n \in \mathbb{Z} : (n^7-n) \equiv 0(\text{mod } 2) \land (n^7-n) \equiv 0(\text{mod } 3) \land (n^7-n) \equiv 0(\text{mod } 7) \iff \\
\forall n \in \mathbb{Z} : \exists i, j, k \in \mathbb{Z} : (n^7-n) = 2\cdot i \land (n^7-n) = 3\cdot j \land (n^7-n) = 7\cdot k \implies \\
\forall n \in \mathbb{Z} : 21\cdot(n^7-n) - 14\cdot(n^7-n) - 6\cdot(n^7-n) = 21\cdot(2\cdot i) - 14\cdot(3\cdot j) - 6\cdot(7\cdot k) \iff \\
\forall n \in \mathbb{Z} : n^7 - n = 42\cdot(i-j-k) \iff \\
\forall n \in \mathbb{Z} : n^7 - n = 0(\text{mod } 42) \iff \\
\forall n \in \mathbb{Z} : n^7 = n(\text{mod } 42) \text{ as required}
\end{gathered} \tag{30}$$

✓

2.3 Optional exercises

1. Prove that for all integers n, there exist natural numbers j and j such that $n = i^2 - j^2$ iff $n \equiv 0(\text{mod } 4)$ or $n \equiv 1(\text{mod } 4)$ or $n \equiv 3(\text{mod } 4)$.

   $(\implies)$

   Assume $\exists i, j \in \mathbb{N} : n = i^2 - j^2$
   The difference between i and j can either be even or odd.
   So either $\exists k \in \mathbb{Z} : i = j + 2\cdot k \lor \exists k \in \mathbb{Z} : i = j + 2\cdot k + 1$.

$$\begin{aligned}
\exists k \in \mathbb{Z} : i = j + 2\cdot k \iff& \\
&n = (j+2\cdot k)^2 - j^2 \iff \\
&n = j^2 + 4\cdot k\cdot j + 4\cdot k^2 - j^2 \iff \\
&n = 4\cdot(k\cdot j + k^2) \iff \\
&n \equiv 0(\text{mod } 4)
\end{aligned} \tag{31}$$

it disappeared?

$$
\begin{aligned}
\exists k \in \mathbb{Z} : i = j + 2 \cdot k + 1 \iff& \\
n = (j + 2 \cdot k + 1)^2 - j^2 \iff& \\
n = j^2 + 2 \cdot j \cdot (2 \cdot k + 1) + (2 \cdot k + 1)^2 - j^2 \iff& \\
n = 4 \cdot j \cdot k + 2 \cdot j + 4 \cdot k^2 + 4 \cdot k + 1 \iff& \\
n = 2 \cdot j + 1 + 4 \cdot (j \cdot k + k^2 + k) \iff& \\
n \equiv 2 \cdot j + 1 (\text{mod } 4). & \\
\exists j . 2j+1=n \iff (n \equiv 1 (\text{mod } 4) \lor n \equiv 3 (\text{mod } 4)) & \\
\therefore \exists i, j \in \mathbb{N} : n = i^i - j^2 \implies n \equiv 0 (\text{mod } 4) \lor n \equiv 1 (\text{mod } 4) \lor n \equiv 3 (\text{mod } 4) &
\end{aligned}
\tag{32}
$$

$(\Longleftarrow)$ consistent placement

$$
\begin{aligned}
& n \equiv 0 (\text{mod } 4) \iff \\
& \exists k \in \mathbb{Z} : n = 4 \cdot k \\
& \quad \text{Let } i = k + 1 \text{ and } j = k - 1 \\
& \quad i^2 - j^2 \\
& \quad = (k + 1)^2 - (k - 1)^2 \\
& \quad = k^2 + 2 \cdot k + 1 - k^2 + 2 \cdot k - 1 \\
& \quad = 4 \cdot k \\
& \quad = n \\
& \quad \therefore n \equiv 0 (\text{mod } 4) \implies \exists i, j \in \mathbb{Z} : n = i^2 - j^2
\end{aligned}
\tag{33}
$$

✓

$$
\begin{aligned}
& n \equiv 1 (\text{mod } 4) \iff \\
& \exists k \in \mathbb{Z} : n = 4 \cdot k + 1 \\
& \quad \text{Let } i = 2 \cdot k + 1 \text{ and } j = 2 \cdot k \\
& \quad i^2 - j^2 \\
& \quad = (2 \cdot k + 1)^2 - (2 \cdot k)^2 \\
& \quad = 4 \cdot k^2 + 4 \cdot k + 1 - 4 \cdot k^2 \\
& \quad = 4 \cdot k + 1 \\
& \quad = n \\
& \quad \therefore n \equiv 1 (\text{mod } 4) \implies \exists i, j \in \mathbb{Z} : n = i^2 - j^2
\end{aligned}
\tag{34}
$$

✓

$$
\begin{aligned}
& n \equiv 3 (\text{mod } 4) \iff \\
& \exists k \in \mathbb{Z} : n = 3 + 4 \cdot k \\
& \quad \text{Let } i = 2 \cdot k + 2 \text{ and } j = 2 \cdot k + 1 \\
& \quad i^2 - j^2 \\
& \quad = (2 \cdot k + 2)^2 - (2 \cdot k + 1)^2 \\
& \quad = 4 \cdot k^2 + 8 \cdot k + 4 - 4 \cdot k^2 - 4 \cdot k - 1 \\
& \quad = 4 \cdot k + 3 \\
& \quad = n \\
& \quad \therefore n \equiv 3 (\text{mod } 4) \implies \exists i, j \in \mathbb{Z} : n = i^2 - j^2
\end{aligned}
\tag{35}
$$

✓

$$\therefore \exists i, j \in \mathbb{N} : n = i^i - j^2 \Longleftarrow n \equiv 0 (\text{mod } 4) \lor n \equiv 1 (\text{mod } 4) \lor n \equiv 3 (\text{mod } 4)$$

$$\therefore \exists i, j \in \mathbb{N} : n = i^i - j^2 \iff n \equiv 0 (\text{mod } 4) \lor n \equiv 1 (\text{mod } 4) \lor n \equiv 3 (\text{mod } 4)$$

2. A *decimal* (respectively *binary*) *repunit* is a natural number whose decimal (respectively binary) representation consists solely of 1's.

(a) What are the first three decimal repunits? And the first three binary ones?

The first three decimal repunits are 1_{10}, 11_{10} and 111_{10}. ✓
The first three binary repunits are 1_2 (1_{10}), 11_2 (3_{10}) and 111_2 (7_{10}).

(b) Show that no decimal repunit strictly greater than 1 is a square, and that the same holds for binary repunits. Is this the case for every base?

Show that there is no number which squares to end in 11_{10}.

Proof by contradiction. greater than 1
Assume there is a decimal repunit r that is a square.

$$\begin{aligned} &\text{Assume: } \exists k \in \mathbb{Z} : k^2 = r \\ &\exists k \in \mathbb{Z} : k^2 = r \implies \\ &\exists k \in \mathbb{Z} : k^2 \equiv 11 (\text{mod } 100) \implies \\ &k^2 \equiv 1 (\text{mod } 10) \iff \\ &\exists i \in \mathbb{Z} : k = 10 \cdot i + 1 \lor k = 10 \cdot i + 9 \end{aligned} \tag{36}$$

(by inspection of multiplicative table of $\mathbb{Z}_{10}$)?

$$\begin{aligned} &\text{Case 1: } k = 10 \cdot i + 1 \\ &(10 \cdot i + 1)^2 \equiv 11 (\text{mod } 100) \iff \\ &100 \cdot i^2 + 20 \cdot i + 1 \equiv 11 (\text{mod } 100) \iff \\ &20 \cdot i \equiv 10 (\text{mod } 100) \iff \\ &2 \cdot i \equiv 1 (\text{mod } 10) \\ &\nexists i \in \mathbb{Z} : 2 \cdot i \equiv 1 (\text{mod } 10) \end{aligned} \tag{37}$$

, which is false, because: by inspection.

However, this contradicts the original assumption that $\exists i \in \mathbb{Z} : (10 \cdot i + 1)^2 = r$. ✓

$$\begin{aligned} &\text{Case 2: } k = 10 \cdot i + 9 \\ &(10 \cdot i + 9)^2 \equiv 11 (\text{mod } 100) \iff \\ &100 \cdot i^2 + 20 \cdot i + 81 \equiv 11 (\text{mod } 100) \iff \\ &20 \cdot i \equiv 30 (\text{mod } 100) \iff \\ &2 \cdot i \equiv 3 (\text{mod } 10) \\ &\nexists i \in \mathbb{Z} : 2 \cdot i \equiv 3 (\text{mod } 10) \end{aligned} \tag{38}$$

✓ ... see above (more explanation to what you're writing)

However, this contradicts the original assumption that $\exists i \in \mathbb{Z} : (10 \cdot i + 9)^2 = r$.

So $\nexists k \in \mathbb{Z} : k^2 = r$ for ~~some~~ any repunit $r >= 11$. As required.

Assume that there is an integer k such that $k^2 = r$ for some binary repunit.

$$\begin{aligned} &\exists k \in \mathbb{Z} : k^2 = r \iff \\ &\exists n \in \mathbb{Z} : (2 \cdot n)^2 = r \lor (2 \cdot n + 1)^2 = r \end{aligned} \tag{39}$$

Case 1: $\exists n \in \mathbb{Z} : (2 \cdot n)^2 = r$.

$$\begin{aligned} &\exists n \in \mathbb{Z} : (2 \cdot n)^2 = r \implies \\ &\exists n \in \mathbb{Z} : 4 \cdot n^2 \equiv 3 (\text{mod } 4) \iff \\ &0 \equiv 3 (\text{mod } 4) \end{aligned} \tag{40}$$

However, this is not true. So $\nexists n \in \mathbb{Z} : (2 \cdot n)^2 = r$

Case 2: $\exists n \in \mathbb{Z} : (2 \cdot n + 1)^2 = r$

$$\begin{aligned} &\exists n \in \mathbb{Z} : (2 \cdot n + 1)^2 = r \implies \\ &\exists n \in \mathbb{Z} : (2 \cdot n + 1)^2 \equiv 3 (\text{mod } 4) \iff \\ &\exists n \in \mathbb{Z} : 4 \cdot n^2 + 4 \cdot n + 1 \equiv 3 (\text{mod } 4) \implies \\ &1 \equiv 3 (\text{mod } 4) \end{aligned} \tag{41}$$

However, this is not true. So $\nexists n \in \mathbb{Z} : (2 \cdot n + 1)^2 = r$.

Since all numbers are even or odd and r cannot be the square of an even number or an odd number: r cannot be the square of any number – hence r cannot be a square number. Since r was arbitrary this proves that there are no binary repunits that are square numbers.

This is not the case for every base: consider base $k^2 - 1$ for some number k.
In base $k^2 - 1$: $k^2 = 11_{k^2-1}$.

✓ nice!

Good work and you improved using comments from last SV!

Things to improve:

1 in some cases more English description of your logic would help with readability.

2 be mindful of $=$ vs $\equiv$ and make sure you use $x \equiv y \pmod{m}$ notation correctly

Otherwise great work! Much more readable than last time.