2 On numbers

2.1 Basic exercises

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

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

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

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

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

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

$$\begin{aligned} i \equiv j (\text{mod } m) &\iff \\ j \equiv i (\text{mod } m) &\text{ using (2)} \end{aligned} \tag{3}$$

$$j \equiv k (\text{mod } m) \tag{4}$$

Combining (3)and (4) gives:

$$i \equiv k (\text{mod } m) \iff \tag{5}$$

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

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

$$\begin{aligned} i \equiv j (\text{mod } m) &\iff \\ \exists a \in \mathbb{Z} : i = j + a \cdot m & \end{aligned} \tag{6}$$

$$\begin{aligned} k \equiv l (\text{mod } m) &\iff \\ \exists b \in \mathbb{Z} : k = l + b \cdot m & \end{aligned} \tag{7}$$

Adding (6) and (7) gives:

$$\begin{aligned} \exists a, b \in \mathbb{Z} : i + k = j + a \cdot m + l + b \cdot m &\iff \\ \exists a, b \in \mathbb{Z} : i + k = j + l + (a + b) \cdot m &\iff \\ i + k \equiv j + l (\text{mod } m) & \end{aligned} \tag{8}$$

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

$$\begin{aligned}
& i \equiv j (\text{mod } m) \iff \\
& (a) \exists p \in \mathbb{Z} : i = j + p \cdot m \\
& k \equiv l (\text{mod } m) \iff \\
& (b) \exists q \in \mathbb{Z} : k = l + q \cdot m \\
& \text{Combining (a) and (b) gives:} \\
& \exists p, q \in \mathbb{Z} : i \cdot k = (j + p \cdot m) \cdot (l + q \cdot m) \iff \\
& \exists p, q \in \mathbb{Z} : i \cdot k = j \cdot l + j \cdot q \cdot m + l \cdot p \cdot m + p \cdot q \cdot m \cdot m \iff \\
& \exists p, q \in \mathbb{Z} : i \cdot k = j \cdot l + (j \cdot q + l \cdot p + p \cdot q \cdot m) \cdot m \iff \\
& i \cdot k = j \cdot l (\text{mod } m)
\end{aligned} \tag{9}$$

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

Proof by induction:

At $n = 0$:

$$\begin{aligned}
\forall m \in \mathbb{Z} : 1 \equiv 1(\text{mod } m) \iff \\
\forall m \in \mathbb{Z} : i^0 \equiv j^0(\text{mod } m)
\end{aligned} \tag{10}$$

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

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

$$\text{By assumption: } i^k \equiv j^k(\text{mod } m) \tag{11}$$

$$\text{By assumption: } i \equiv j(\text{mod } m) \tag{12}$$

Using (9) we can combine (11) and (12)

$$\begin{aligned}
i^k \cdot i \equiv j^k \cdot j(\text{mod } m) \iff \\
i^{k+1} \equiv j^{k+1}(\text{mod } m)
\end{aligned} \tag{13}$$

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

$$\begin{aligned}
l = l(\text{mod } m) \iff \\
k \cdot m + l = l(\text{mod } m) \iff \\
\text{rem}(k \cdot m + l, m) = \text{rem}(l, m) \text{ as required}
\end{aligned} \tag{14}$$

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

$$\begin{aligned}
k + l = k + l(\text{mod } m) \iff \\
k + l = \text{rem}(k, m) + l(\text{mod } m) \iff \\
\text{rem}(k + l, m) = \text{rem}(\text{rem}(k, m) + l, m) \text{ as required}
\end{aligned} \tag{15}$$

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

$$\begin{aligned}
k \cdot l = k \cdot l(\text{mod } m) \iff \\
k \cdot l = k \cdot \text{rem}(l, m)(\text{mod } m) \iff \\
\text{rem}(k \cdot l, m) \neq \text{rem}(k \cdot \text{rem}(l, m), m) \text{ as required}
\end{aligned} \tag{16}$$

4. Let m be a positive integer.

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

$$\forall i, j, k \in \mathbb{Z}_m.(i +_m j) +_m k = i +_m (j +_m k) \text{ and } (i \cdot_m j) \cdot_m k = i \cdot_m (j \cdot_m k) \quad (17)$$

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

$$\begin{aligned} &\forall i, j, k \in \mathbb{Z}_m : s = (i +_m j) +_m k \iff \\ &\forall i, j, k \in \mathbb{Z}_m : s \equiv (i + j) + k(\text{mod } m) \iff \\ &\forall i, j, k \in \mathbb{Z}_m : s \equiv i + j + k(\text{mod } m) \iff \\ &\forall i, j, k \in \mathbb{Z}_m : s \equiv i + (j + k)(\text{mod } m) \iff \\ &\qquad\qquad \therefore \forall i, j, k \in \mathbb{Z}_m.(i +_m j) +_m k = i +_m (j +_m k) \text{ as required} \end{aligned} \quad (18)$$

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

$$\begin{aligned} \forall i, j, k \in \mathbb{Z}_m : p = (i \cdot_m j) \cdot_m k \iff \\ \forall i, j, k \in \mathbb{Z}_m : p \equiv (i \cdot j) \cdot k(\text{mod } m) \iff \\ \forall i, j, k \in \mathbb{Z}_m : p \equiv i \cdot j \cdot k(\text{mod } m) \iff \\ \forall i, j, k \in \mathbb{Z}_m : p \equiv i \cdot (j \cdot k)(\text{mod } m) \iff \\ \therefore \forall i, j, k \in \mathbb{Z}_m : (i \cdot_m j) \cdot_m k = i \cdot_m (j \cdot_m k) \text{ as required} \end{aligned} \quad (19)$$

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

$$\begin{aligned} [-k]_m &= -k + m \iff \\ k + [-k]_m &\equiv k - k + m(\text{mod } m) \iff \\ k + [-k]_m &\equiv m(\text{mod } m) \iff \\ k + [-k]_m &\equiv 0(\text{mod } m) \end{aligned} \quad (20)$$

   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.

$$i = 2,\ k = 1,\ l = 4,\ m = 3$$

$$\begin{aligned} 1 &\equiv 4(\text{mod } 3) \implies \\ k &\equiv l(\text{mod } m) \end{aligned} \quad (21)$$

$$\begin{aligned} 2 &\not\equiv 1(\text{mod } 3) \iff \\ 2^1 &\not\equiv 2^4(\text{mod } 3) \implies \\ i^k &\not\equiv i^l(\text{mod } m) \end{aligned} \quad (22)$$

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.

Let a_i be the i^{th} digit of $n \in \mathbb{Z}$.

$$
\begin{aligned}
n &\equiv \sum_{i=0}^{\infty} a_i \cdot 10^i (\text{mod } 3) \iff \\
n &\equiv \sum_{i=0}^{\infty} a_i + a_i \cdot (10^i - 1)(\text{mod } 3) \iff \\
\forall i \geq 1 : 10^i - 1 &= \sum_{j=0}^{i-1} 9 \cdot 10^j \iff \\
\forall i \geq 1 : 10^i - 1 &\equiv 9 \cdot \sum_{j=0}^{i-1} \cdot 10^j (\text{mod } 3) \iff \\
\forall i \geq 1 : 10^i - 1 &\equiv 0 (\text{mod } 3) \\
\text{for } i = 0 : 10^i - 1 &= 0 \iff \\
10^i - 1 &\equiv 0 (\text{mod } 3) \\
\therefore n &\equiv \sum_{i=0}^{\infty} a_i (\text{mod } 3) \\
n &\equiv 0 (\text{mod } 3) \iff 3 | n \\
\therefore \sum_{i=0}^{\infty} a_i &\equiv 0 (\text{mod } 3) \iff 3 | n
\end{aligned}
\tag{23}
$$

Let a_i be the i^{th} digit of $n \in \mathbb{Z}$.

$$
\begin{aligned}
n &\equiv \sum_{i=0}^{\infty} a_i \cdot 10^i (\text{mod } 9) \iff \\
n &\equiv \sum_{i=0}^{\infty} a_i + a_i \cdot (10^i - 1)(\text{mod } 9) \iff \\
\forall i \geq 1 : 10^i - 1 &= \sum_{j=0}^{i-1} 9 \cdot 10^j \iff \\
\forall i \geq 1 : 10^i - 1 &\equiv 9 \cdot \sum_{j=0}^{i-1} \cdot 10^j (\text{mod } 9) \iff \\
\forall i \geq 1 : 10^i - 1 &\equiv 0 (\text{mod } 9) \\
\text{for } i = 0 : 10^i - 1 &= 0 \iff \\
10^i - 1 &\equiv 0 (\text{mod } 9) \\
\therefore n &\equiv \sum_{i=0}^{\infty} a_i (\text{mod } 9) \\
n &\equiv 0 (\text{mod } 9) \iff 9 | n \\
\therefore \sum_{i=0}^{\infty} a_i &\equiv 0 (\text{mod } 9) \iff 9 | n
\end{aligned}
\tag{24}
$$

Let a_i be the i^{th} digit of $n \in \mathbb{Z}$.

TOTO: correct the below. It is wrong. Counterexample: $11 \nmid 999$

$$\begin{aligned} n &\equiv \sum_{i=0}^{\infty} a_i \cdot 10^i (\text{mod } 11) \iff \\ n &\equiv \sum_{i=0}^{\infty} a_i + a_i \cdot (10^i - 1) (\text{mod } 11) \iff \end{aligned} \tag{25}$$

Since $10^i - 1 \equiv 0 (\text{mod } 11)$ for $i \geq 1$:

$$\begin{aligned} n &\equiv \sum_{i=0}^{\infty} a_i (\text{mod } 11) \\ n &\equiv 0 (\text{mod } 11) \iff 11 | n \\ \therefore \sum_{i=0}^{\infty} a_i &\equiv 0 (\text{mod } 11) \iff 11 | n \end{aligned} \tag{26}$$

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:

$$\begin{aligned} &n \text{ is even:} \\ &\exists k \in \mathbb{Z} : n = 2 \cdot k \\ &\therefore \exists k \in \mathbb{Z} : n = 2 \cdot k (\text{mod } 4) \\ &n^2 = 4 \cdot k^2 (\text{mod } 4) \\ &n^2 = 0 (\text{mod } 4) \\ &\therefore \; n^2 \text{ divided by 4 is 0.} \end{aligned} \tag{27}$$

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

n i odd:

$$\begin{aligned} &\exists k \in \mathbb{Z} : n = 2 \cdot k + 1 \\ &\therefore \exists k \in \mathbb{Z} : n = 2 \cdot k + 1 (\text{mod } 4) \\ &n^2 = 4 \cdot k^2 + 4 \cdot k + 1 (\text{mod } 4) \\ &n^2 = 1 (\text{mod } 4) \end{aligned} \tag{28}$$

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 $\text{rem}(55^{78}, 79)$?

$$\begin{aligned} &\text{rem}(55^2, 79) \\ =&\text{rem}(3025, 79) \\ =&23 \end{aligned} \tag{29}$$

$$\begin{aligned} &\text{rem}(23^2, 79) \\ =&\text{rem}(529, 79) \\ =&55 \end{aligned} \tag{30}$$

$$\begin{aligned} &\text{rem}(23 \cdot 55, 79) \\ =&\text{rem}(1265, 79) \\ =&1 \end{aligned} \tag{31}$$

$$\begin{aligned}&\text{rem}(55^{78}, 79)\\ =&1 \text{ using Fermat's Little Theorem}\end{aligned} \tag{32}$$

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.

$$\begin{aligned}153 &= 128 + 16 + 8 + 1 \iff\\ 2^128 \cdot 2^16 \cdot 2^8 \cdot 2^1 &\equiv 2^{153}(\text{mod } 153)\\ 2^1 &\equiv 2(\text{mod } 153) \iff\\ 2^2 &\equiv 4(\text{mod } 153) \iff\\ 2^4 &\equiv 16(\text{mod } 153) \iff\\ 2^8 &\equiv 103(\text{mod } 153) \iff\\ 2^{16} &\equiv 52(\text{mod } 153) \iff\\ 2^{32} &\equiv 103(\text{mod } 153) \iff\\ 2^{64} &\equiv 52(\text{mod } 153) \iff\\ 2^{128} &\equiv 103(\text{mod } 153) \iff\\ 2^{153} &\equiv 103 \cdot 52 \cdot 103 \cdot 2 \iff\\ 2^{153} &\equiv 52 \cdot 52 \cdot 2 \iff\\ 2^{153} &\equiv 103 \cdot 2 \iff\\ 2^{153} &\equiv 206 \iff\\ 2^{153} &\equiv 53 \iff\end{aligned} \tag{33}$$

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

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:

$$\begin{aligned}
n &\equiv 1(\text{mod } p-1) \iff \\
\exists k \in \mathbb{Z} : n &= 1 + (p-1)\cdot k \iff \\
\exists k \in \mathbb{Z} : i^n &\equiv i^{1+(p-1)\cdot k}(\text{mod } p) \iff \\
\exists k \in \mathbb{Z} : i^n &\equiv i \cdot (i^{p-1})^k(\text{mod } p) \iff \\
\text{using Fermat's Little Theorem: } \exists k \in \mathbb{Z} : i^n &\equiv i \cdot 1^k(\text{mod } p) \iff \\
i^n &\equiv i \cdot 1(\text{mod } p) \iff \\
i^n &\equiv i(\text{mod } p) \text{ as required}
\end{aligned} \tag{34}$$

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

$$\begin{gathered}
n^3 - n = (n-1) \cdot n \cdot (n+1) \\
\forall n \in \mathbb{Z} : 2|(n-1) \cdot n \cdot (n+1) \land 3|(n-1) \cdot n \cdot (n+1) \iff \\
\forall n \in \mathbb{Z} : \exists i, j \in \mathbb{Z} : (n-1) \cdot n \cdot (n+1) = 2 \cdot i \land (n-1) \cdot n \cdot (n+1) = 3 \cdot j \\
\forall n \in \mathbb{Z} : 3 \cdot (n-1) \cdot n \cdot (n+1) - 2 \cdot (n-1) \cdot n \cdot (n+1) = 3 \cdot (2 \cdot i) - 2 \cdot (3 \cdot j) \iff \\
\forall n \in \mathbb{Z} : (n-1) \cdot n \cdot (n+1) = 6 \cdot (i - j) \iff \\
\forall n \in \mathbb{Z} : (n-1)n(n+1) \equiv 0 (\text{mod } 6) \iff \\
\forall n \in \mathbb{Z} : n^3 - n \equiv 0 (\text{mod } 6) \iff \\
\forall n \in \mathbb{Z} : n^3 \equiv n (\text{mod } 6) \text{ as required}
\end{gathered} \tag{35}$$

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

$$\begin{aligned}
&\forall n \in \mathbb{Z} : n^7 - n = (n-1) \cdot n \cdot (n+1) \cdot (n^2 - n + 1) \cdot (n^2 + n + 1) \implies \\
&\forall n \in \mathbb{Z} : \exists k \in \mathbb{Z} : n^7 - n = k \cdot n \cdot (n+1) \implies \\
&\forall n \in \mathbb{Z} : 2|(n^7 - n) \iff \\
&\forall n \in \mathbb{Z} : n^7 - n \equiv 0 (\text{mod } 2) \\
&\forall n \in \mathbb{Z} : n^7 - n = (n-1)n(n+1)(n^2 - n + 1)(n^2 + n + 1) \implies \\
&\forall n \in \mathbb{Z} : \exists k \in \mathbb{Z} : n^7 - n = k \cdot (n-1) \cdot n \cdot (n+1) \implies \\
&\forall n \in \mathbb{Z} : 3|(n^7 - n) \\
&\forall n \in \mathbb{Z} : n^7 - n \equiv 0 (\text{mod } 3) \\
&\forall n \in \mathbb{Z} : n^7 \equiv n (\text{mod } 7) \text{ using Fermat's Little Theorem} \iff \\
&\forall n \in \mathbb{Z} : n^7 - n \equiv 0 (\text{mod } 7)
\end{aligned} \tag{36}$$

$$\begin{gathered}
\forall n \in \mathbb{Z} : (n^7 - n) \equiv 0 (\text{mod } 2) \land (n^7 - n) \equiv 0 (\text{mod } 3) \land (n^7 - n) \equiv 0 (\text{mod } 7) \iff \\
\forall n \in \mathbb{Z} : \exists i, j, k \in \mathbb{Z} : (n^7 - n) = 2 \cdot i \land (n^7 - n) = 3 \cdot j \land (n^7 - n) = 7 \cdot k \implies \\
\forall n \in \mathbb{Z} : 21 \cdot (n^7 - n) - 14 \cdot (n^7 - n) - 6 \cdot (n^7 - n) = 21 \cdot (2 \cdot i) - 14 \cdot (3 \cdot j) - 6 \cdot (7 \cdot k) \iff \\
\forall n \in \mathbb{Z} : n^7 - n = 42 \cdot (i - j - k) \iff \\
\forall n \in \mathbb{Z} : n^7 - n = 0 (\text{mod } 42) \iff \\
\forall n \in \mathbb{Z} : n^7 = n (\text{mod } 42) \text{ as required}
\end{gathered} \tag{37}$$

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 $\exists k \in \mathbb{Z} : i = j + 2 \cdot k \lor \exists k \in \mathbb{Z} : i = j + 2 \cdot k + 1$.

$$\begin{aligned}
&\exists k \in \mathbb{Z} : i = j + 2 \cdot k \iff \\
&\exists k \in \mathbb{Z} : n = (j + 2 \cdot k)^2 - j^2 \iff \\
&\exists k \in \mathbb{Z} : n = j^2 + 4 \cdot k \cdot j + 4 \cdot k^2 - j^2 \iff \\
&\exists k \in \mathbb{Z} : n = 4 \cdot (k \cdot j + k^2) \iff \\
&\qquad n \equiv 0 (\text{mod } 4)
\end{aligned} \tag{38}$$

$$
\begin{aligned}
\exists j, k \in \mathbb{Z} : i = j + 2 \cdot k + 1 \iff \\
\exists j, k \in \mathbb{Z} : n = (j + 2 \cdot k + 1)^2 - j^2 \iff \\
\exists j, k \in \mathbb{Z} : n = j^2 + 2 \cdot j \cdot (2 \cdot k + 1) + (2 \cdot k + 1)^2 - j^2 \iff \\
\exists j, k \in \mathbb{Z} : n = 4 \cdot j \cdot k + 2 \cdot j + 4 \cdot k^2 + 4 \cdot k + 1 \iff \\
\exists j, k \in \mathbb{Z} : n = 2 \cdot j + 1 + 4 \cdot (j \cdot k + k^2 + k) \iff \\
\exists j \in \mathbb{Z} : n \equiv 2 \cdot j + 1 (\bmod 4) \iff \\
n \equiv 1 (\bmod 4) \lor n \equiv 3 (\bmod 4)
\end{aligned}
\tag{39}
$$

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

$(\Longleftarrow)$

$$
\begin{aligned}
n \equiv 0 (\bmod 4) \iff \\
\exists k \in \mathbb{Z} : n = 4 \cdot k \\
\text{Let } i = k + 1 \text{ and } j = k - 1 \\
i^2 - j^2 \\
=&(k + 1)^2 - (k - 1)^2 \\
=&k^2 + 2 \cdot k + 1 - k^2 + 2 \cdot k - 1 \\
=&4 \cdot k \\
=&n \\
\therefore n \equiv 0 (\bmod 4) \implies \exists i, j \in \mathbb{Z} : n = i^2 - j^2
\end{aligned}
\tag{40}
$$

$$
\begin{aligned}
n \equiv 1 (\bmod 4) \iff \\
\exists k \in \mathbb{Z} : n = 4 \cdot k + 1 \\
\text{Let } i = 2 \cdot k + 1 \text{ and } j = 2 \cdot k \\
i^2 - j^2 \\
=&(2 \cdot k + 1)^2 - (2 \cdot k)^2 \\
=&4 \cdot k^2 + 4 \cdot k + 1 - 4 \cdot k^2 \\
=&4 \cdot k + 1 \\
=&n \\
\therefore n \equiv 1 (\bmod 4) \implies \exists i, j \in \mathbb{Z} : n = i^2 - j^2
\end{aligned}
\tag{41}
$$

$$
\begin{aligned}
n \equiv 3 (\bmod 4) \iff \\
\exists k \in \mathbb{Z} : n = 3 + 4 \cdot k \\
\text{Let } i = 2 \cdot k + 2 \text{ and } j = 2 \cdot k + 1 \\
i^2 - j^2 \\
=&(2 \cdot k + 2)^2 - (2 \cdot k + 1)^2 \\
=&4 \cdot k^2 + 8 \cdot k + 4 - 4 \cdot k^2 - 4 \cdot k - 1 \\
=&4 \cdot k + 3 \\
=&n \\
\therefore n \equiv 3 (\bmod 4) \implies \exists i, j \in \mathbb{Z} : n = i^2 - j^2
\end{aligned}
\tag{42}
$$

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

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.
Assume there is a decimal repunit $r > 1$ that is a square.

$$\begin{gathered}
\text{Assume: } \exists k \in \mathbb{Z} : k^2 = r \\
\exists k \in \mathbb{Z} : k^2 = r \implies \\
\exists k \in \mathbb{Z} : k^2 \equiv 11 (\text{mod } 100) \implies \\
k^2 \equiv 1 (\text{mod } 10) \iff \\
\text{By inspection of the multiplication table of } \mathbb{Z}_m \\
\exists i \in \mathbb{Z} : k = 10 \cdot i + 1 \lor k = 10 \cdot i + 9
\end{gathered} \tag{43}$$

$$\begin{gathered}
\text{Case 1: } k = 10 \cdot i + 1 \\
(10 \cdot i + 1)^2 \equiv 11 (\text{mod } 100) \iff \\
100 \cdot i^2 + 20 \cdot i + 1 \equiv 11 (\text{mod } 100) \iff \\
20 \cdot i \equiv 10 (\text{mod } 100) \iff \\
2 \cdot i \equiv 1 (\text{mod } 10) \\
\text{Which is false, because by inspection} \\
\nexists i \in \mathbb{Z} : 2 \cdot i \equiv 1 (\text{mod } 10)
\end{gathered} \tag{44}$$

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

$$\begin{gathered}
\text{Case 2: } k = 10 \cdot i + 9 \\
(10 \cdot i + 9)^2 \equiv 11 (\text{mod } 100) \iff \\
100 \cdot i^2 + 20 \cdot i + 81 \equiv 11 (\text{mod } 100) \iff \\
20 \cdot i \equiv 30 (\text{mod } 100) \iff \\
2 \cdot i \equiv 3 (\text{mod } 10) \\
\text{Which is false because by inspection} \\
\nexists i \in \mathbb{Z} : 2 \cdot i \equiv 3 (\text{mod } 10)
\end{gathered} \tag{45}$$

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 any repunit $r > 1$. As required.

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

$$\begin{gathered}
\exists k \in \mathbb{Z} : k^2 = r \iff \\
\exists n \in \mathbb{Z} : (2 \cdot n)^2 = r \lor (2 \cdot n + 1)^2 = r
\end{gathered} \tag{46}$$

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

$$\begin{gathered}
\exists n \in \mathbb{Z} : (2 \cdot n)^2 = r \implies \\
\exists n \in \mathbb{Z} : 4 \cdot n^2 \equiv 3 (\text{mod } 4) \iff \\
0 \equiv 3 (\text{mod } 4)
\end{gathered} \tag{47}$$

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

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

$$\begin{aligned} \exists n \in \mathbb{Z} : (2 \cdot n + 1)^2 = r \implies \\ \exists n \in \mathbb{Z} : (2 \cdot n + 1)^2 \equiv 3 (\text{mod } 4) \iff \\ \exists n \in \mathbb{Z} : 4 \cdot n^2 + 4 \cdot n + 1 \equiv 3 (\text{mod } 4) \implies \\ 1 \equiv 3 (\text{mod } 4) \end{aligned} \tag{48}$$

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 $k^2 - 1$: $k^2 = 11_{k^2-1}$.