Divisibility Theory in the Integers

A SET HAS THE CLOSURE PROPERTY UNDER A PARTICULAR OPERATION IF THE RESULT OF THE OPERATION IS ALWAYS AN ELEMENT IN THE SET. IF A SET HAS THE CLOSURE PROPERTY UNDER A PARTICULAR OPERATION, THEN WE SAY THAT THE SET IS CLOSED UNDER THE OPERATION. FOR INSTANCE, THE SET $\{1,2,3,4\} \subseteq \mathbb{N}$ IS NOT CLOSED UNDER THE USUAL ADDITION BECAUSE $2+3=5$ AND 5 IS NOT IN $\{1,2,3,4\}$. SIMILARLY, THE SET $\mathbb{N}$ OF ALL POSITIVE INTEGERS IS NOT CLOSED UNDER THE USUAL SUBSTRACTION SINCE $2-3=-1$ AND $-1 \notin \mathbb{N}$. HOWEVER, WE OBSERVE $\mathbb{N}$ IS CLOSED UNDER THE USUAL ADDITION AND MULTIPLICATION SINCE GIVEN ANY TWO INTEGERS a, b WE HAVE $a+b \in \mathbb{N}$ AND $a.b \in \mathbb{N}$.

LET $\mathbb{Z}$ DENOTE THE SET OF ALL INTEGERS. NOTICE $\mathbb{Z}$ IS CLOSED UNDER THE USUAL ADDITION, SUBSTRACTION AND MULTIPLICATION. THAT IS, GIVEN ANY TWO INTEGERS a, b WE HAVE $a+b \in \mathbb{Z}$, $a-b \in \mathbb{Z}$ AND $a.b \in \mathbb{Z}$. HOWEVER, $\mathbb{Z}$ IS NOT CLOSED UNDER THE USUAL DIVISION OF INTEGERS SINCE, FOR INSTANCE, $\frac{15}{8} \notin \mathbb{Z}$. ALTHOUGH $\mathbb{Z}$ HAS NOT THE CLOSURE PROPERTY UNDER THE DIVISION, WE OBSERVE FOR SOME $a, b \in \mathbb{Z}$ THE NUMBER $\frac{a}{b} \in \mathbb{Z}$. FOR INSTANCE, $\frac{12}{4}$, $\frac{12}{3}$, $\frac{12}{-6}$ ARE INTEGERS.

THIS REMARK ALLOWS US TO INTRODUCE THE NEXT DEFINITION:

DEFINITION: GIVEN $a, b \in \mathbb{Z}$, WE SAY THAT a DIVIDES b IF THERE EXISTS AN INTEGER $c \in \mathbb{Z}$ SUCH THAT $b = a.c$. IN THIS CASE, WE WRITE $a \mid b$.

WE NEXT GIVE SOME EXAMPLES:

- $3 \mid 0$ SINCE THERE EXISTS $0 \in \mathbb{Z}$ SUCH THAT $0 = 3.0$.
- $15 \mid -90$ SINCE THERE EXISTS $-6 \in \mathbb{Z}$ SUCH THAT $-90 = 15.(-6)$.
- $14 \nmid 21$ SINCE THERE IS NO INTEGER k SUCH THAT $21 = 14k$.
- $0 \mid 0$ SINCE $0 = 0.0$.
- THE DIVISORS OF 12 ARE $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$.

Exercises

(1) GIVEN $a, b, c \in \mathbb{Z}$, PROVE THE FOLLOWING DIVISIBILITY PROPERTIES:

(i) a DIVIDES 0 FOR EVERY $a \in \mathbb{Z}$.

GIVEN ANY INTEGER a, WE OBSERVE THERE EXISTS $0 \in \mathbb{Z}$ SUCH THAT $0 = a.0$. THEN, $a \mid 0$.

(ii) $0 \mid a$ iff $a = 0$

WE ALREADY OBSERVED THAT $0 \mid 0$. SUPPOSE NOW THAT $0 \mid a$. THEN, THERE EXISTS $k \in \mathbb{Z}$ SUCH THAT $a = 0.k$. THIS SHOWS THAT $a = 0$.

(iii) $1 \mid a$ AND $-1 \mid a$ FOR EVERY $a \in \mathbb{Z}$.

GIVEN ANY INTEGER $a \in \mathbb{Z}$, NOTE THERE EXIST $a, -a \in \mathbb{Z}$ SUCH THAT $a = 1.a$ AND $a = (-1).(-a)$. THEN, $1 \mid a$ AND $-1 \mid a$.

(iv) $a|1$ or $a|-1$ iff $a=1$ or $a=-1$.

SUPPOSE FIRST THAT $a|1$. THEN, THERE EXISTS $k \in \mathbb{Z}$ SUCH THAT $1 = a.k$. TAKING ABSOLUTE VALUE, WE GET $1 = |a|.|k|$. NOTE THAT $|a|, |k| \in \mathbb{N}$. IF $|a|>1$ THEN $1 = |a||k| > 1$ WHICH SHOWS THAT $|a| = 1$. THEN, $a \in \{-1,1\}$. SIMILARLY, IF $a|-1$ THEN $-1 = a.k'$ FOR SOME $k' \in \mathbb{Z}$. TAKING ABSOLUTE VALUE, WE GET $1 = |a|.|k'|$ WHICH IMPLIES $|a|=1$. THUS, $a \in \{1,-1\}$. CONVERSELY, IF $a=1$ or $a=-1$, IT IS CLEAR THAT $a|1$ AND $a|-1$. THE CLAIM FOLLOWS.

(v) $a|a$ FOR ALL $a \in \mathbb{Z}$

GIVEN $a \in \mathbb{Z}$, NOTICE THERE EXISTS $1 \in \mathbb{Z}$ SUCH THAT $a = 1.a$. THIS SHOWS $a|a$.

(vi) $a|b$ AND $b|a$ iff $a=b$ or $a=-b$.

IF $a|b$ AND $b|a$ THEN THERE EXIST $k, h \in \mathbb{Z}$ SUCH THAT $b = a.k$ AND $a = b.h$. SO, $b = (bh)k = b(hk)$. THIS MEANS THAT $b.(hk-1) = 0$. THEREFORE, EITHER $b=0$ OR $hk=1$. IF $b=0$, SINCE $b|a$, BY (ii), WE HAVE $a=0$ AND SO $a=b$. IF $hk=1$ THEN $h|1$ AND, BY (iv), $h \in \{1,-1\}$. THEN, SINCE $a=bh$, IT FOLLOWS THAT $a=b$ OR $a=-b$. THE CONVERSE IS TRIVIAL SINCE $a|a$, $a|-a$ AND $-a|a$ FOR EVERY $a \in \mathbb{Z}$.

(vii) $a|b$ AND $b|c$ THEN $a|c$.

IF $a|b$ AND $b|c$ THERE EXIST $h, k \in \mathbb{Z}$ SUCH THAT

$b = a.h$ AND $c = b.k$. THEN, WE OBSERVE THERE EXISTS $hk \in \mathbb{Z}$ SUCH THAT $c = bk = (ah)k = a(hk)$ WHICH SHOWS THAT $a \mid c$.

(viii) $a \mid b$ iff $a \mid -b$ iff $-a \mid b$ iff $-a \mid -b$

WE WILL PROVE THAT $a \mid b$ iff $a \mid -b$. THE OTHER PROOFS ARE SIMILAR AND THEREFORE LEFT AS AN EXERCISE.

IF $a \mid b$ THEN $b = a.k$ FOR SOME $k \in \mathbb{Z}$. THEN, WE CAN WRITE $-b = a.(-k)$ AND SINCE $-k \in \mathbb{Z}$ WE HAVE $a \mid -b$.

CONVERSELY, IF $a \mid -b$ THEN $-b = a.h$ FOR SOME $h \in \mathbb{Z}$. SO, $b = (-1).(-b) = (-1).a.h = a.(-h)$ WITH $-h \in \mathbb{Z}$. THEN, $a \mid b$.

(ix) IF $a, b \in \mathbb{N}$ AND $a \mid b$ THEN $a \leq b$.

LET $a, b \in \mathbb{N}$. IF $a \mid b$ THEN $b = a.k$ FOR SOME $k \in \mathbb{Z}$. SINCE $a, b \in \mathbb{N}$, WE HAVE $k \in \mathbb{N}$. THEN $k \geq 1$. THIS SHOWS $b = a.k > a$. THE CLAIM FOLLOWS.

(x) IF $a \mid b$ AND $a \mid c$ THEN $a \mid b+c$

SUPPOSE THAT $a \mid b$ AND $a \mid c$. THEN THERE EXISTS $k, h \in \mathbb{Z}$ SUCH THAT $b = ak$ AND $c = ah$. SO, THERE EXISTS $k+h \in \mathbb{Z}$ SUCH THAT $b+c = ak + ah = a(k+h)$ WHICH MEANS $a \mid b+c$.

(xi) IF $a \mid b$ THEN $a \mid bc$ FOR EVERY $c \in \mathbb{Z}$.

IF $a \mid b$ THEN THERE EXISTS $k \in \mathbb{Z}$ SUCH THAT $b = ak$. THEREFORE, FOR EVERY $c \in \mathbb{Z}$, $bc = akc = a(kc)$. SINCE $kc \in \mathbb{Z}$ WE HAVE $a \mid bc$.

(xii) IF $a \mid b+c$ AND $a \mid b$ THEN $a \mid c$

SUPPOSE THAT $a \mid b+c$ AND $a \mid b$. THEN, THERE EXIST $k, h \in \mathbb{Z}$ SUCH THAT $b+c = k.a$ AND $b = a.h$. NOTICE THAT

$c = (b+c) - b = k.a - a.h = a.(k-h)$ AND $k-h \in \mathbb{Z}$.

THUS, $a \mid c$.

(xiii) $a \mid b$ AND $a \mid c$ THEN $a \mid b-c$.

IF $a \mid b$ AND $a \mid c$ THEN $b = ak$ AND $c = ah$ FOR SOME $k, h \in \mathbb{Z}$. THEN, $b-c = ak - ah = a(k-h)$ WITH $k-h \in \mathbb{Z}$. THIS SHOWS $a \mid b-c$.

(2) FIND ALL VALUES OF $a \in \mathbb{Z}$ SUCH THAT $a+1 \mid 2a^2+9$.

LET $a \in \mathbb{Z}$ SUCH THAT $a+1 \mid 2a^2+9$. BY (V), $a+1 \mid a+1$ AND BY (xi), $a+1 \mid (a+1).c$ FOR EVERY $c \in \mathbb{Z}$. IN PARTICULAR, TAKING $c = 2a-2 \in \mathbb{Z}$ WE HAVE $a+1 \mid (a+1)(2a-2) = 2a^2-2$. THEREFORE, $a+1 \mid 2a^2+9$ AND $a+1 \mid 2a^2-2$. BY (xiii) WE HAVE $a+1 \mid (2a^2+9) - (2a^2-2)$. THAT IS, $a+1 \mid 11$. NOTE THAT THE ONLY DIVISORS OF 11 ARE $\pm 1, \pm 11$. THEN, WE GET $a+1 \in \{\pm 1, \pm 11\}$ WHICH MEANS $a \in \{0, -2, 10, -12\}$. NOW, WE CHECK WHICH THE POSSIBLE VALUES OF a ARE.

IF $a = 0$ WE GET $1 \mid 9$ WHICH IS TRUE.

IF $a = -2$ WE GET $-1 \mid 17$ WHICH IS TRUE.

IF $a = 10$ WE GET $11 \mid 209$ WHICH IS TRUE AS $11.19 = 209$.

IF $a = -12$ WE GET $-11 \mid 297$ WHICH IS TRUE AS $(-11).(-27) = 297$.

THEREFORE, $\{a \in \mathbb{Z} : a+1 \mid 2a^2+9\} = \{0, -2, 10, -12\}$. $\blacksquare$

(3) FIND ALL VALUES OF $m \in \mathbb{N}$ SUCH THAT:

(i) $3m-1 \mid m+7$.

LET $m \in \mathbb{N}$ SUCH THAT $3m-1 \mid m+7$. NOTE THAT $3m-1 \mid 3m-1$ AND $3m-1 \mid 3(m+7) = 3m+21$. THEN, $3m-1 \mid (3m+21)-(3m-1) = 20$. NOTE THAT THE POSITIVE DIVISORS OF 20 ARE $1,2,4,5,10,20$. THEN, $3m-1 \in \{1,2,4,5,10,20\}$. SO, $3m \in \{2,3,5,6,11,21\}$. NOTE THAT $3m \in \{3,6,21\}$ SINCE $m \in \mathbb{N}$. THIS SHOWS $m \in \{1,2,7\}$. IF $m=1$ WE GET $2 \mid 8$ WHICH IS TRUE. IF $m=2$ WE GET $5 \mid 9$ WHICH IS NOT TRUE. IF $m=7$ WE GET $20 \mid 14$ WHICH IS NOT TRUE. WE THEREFORE HAVE

$$\{m \in \mathbb{N} : 3m-1 \mid m+7\} = \{1\}.$$

(ii) $m-2 \mid m^3-8$

LET $m \in \mathbb{N}$ SUCH THAT $m-2 \mid m^3-8$. NOTE WE CAN WRITE $m^3-8 = (m-2)(m^2+2m+4)$. SINCE $m \in \mathbb{N}$ AND $\mathbb{N}$ IS CLOSED UNDER THE USUAL ADDITION AND MULTIPLICATION, WE HAVE $m^2+2m+4 \in \mathbb{N}$. THIS MEANS $m-2 \mid m^3-8$ FOR EVERY $m \in \mathbb{N}$. THEN, $\{m \in \mathbb{N} : m-2 \mid m^3-8\} = \mathbb{N}$. $\blacksquare$

(4) LET $a,b \in \mathbb{Z}$.

(i) SHOW THAT $a-b \mid a^m - b^m$ FOR EVERY $m \in \mathbb{N}$.

WE PROCEED BY INDUCTION ON $m \in \mathbb{N}$. LET S BE THE SET DEFINED BY $S = \{m \in \mathbb{N} : a-b \mid a^m - b^m\}$. OBSERVE THAT $1 \in S$ SINCE $a-b \mid a^1 - b^1 = a-b$. SUPPOSE NEXT $h \in S$ FOR SOME $h > 1$. THEN $a-b \mid a^h - b^h$. THIS MEANS THERE EXISTS

$k \in \mathbb{Z}$ SUCH THAT $a^h - b^h = (a-b)k$. WE WILL SHOW THAT $h+1 \in S$. NOTE THAT

$$\begin{aligned} a^{h+1} - b^{h+1} &= a \cdot a^h - b \cdot b^h = a \cdot [(a-b)k + b^h] - b \cdot b^h \\ &= a \cdot (a-b)k + a b^h - b \cdot b^h \\ &= a \cdot (a-b)k + b^h \cdot (a-b) \\ &= (a-b) \cdot [ak + b^h] \end{aligned}$$

SINCE $a, b, k \in \mathbb{Z}$, $h \in \mathbb{N}$ THE NUMBER $ak + b^h \in \mathbb{Z}$. THUS, $a-b \mid a^{h+1} - b^{h+1}$. WE THEREFORE HAVE $a-b \mid a^m - b^m$ FOR EVERY $m \in \mathbb{N}$ BY THE PRINCIPLE OF INDUCTION.

(ii) IF $m \in \mathbb{N}$ IS EVEN, SHOW THAT $a+b \mid a^m - b^m$.

SINCE m IS EVEN AND $m \in \mathbb{N}$, WE OBSERVE $m = 2k$ FOR SOME $k \in \mathbb{N}$. THEN, IT IS ENOUGH TO SHOW $a+b \mid a^{2k} - b^{2k}$ FOR EVERY $k \in \mathbb{N}$. WE WILL PROCEED BY INDUCTION ON k.

IF $k = 1$ WE OBSERVE THAT $a+b \mid a^2 - b^2$ SINCE $a^2 - b^2 = (a-b)(a+b)$ AND $a+b \in \mathbb{Z}$. SUPPOSE NEXT THAT $a+b \mid a^{2h} - b^{2h}$ FOR SOME $h \in \mathbb{N}$, $h > 1$. THEN, THERE EXISTS $m \in \mathbb{Z}$ SUCH THAT $a^{2h} - b^{2h} = (a+b)m$. NOTICE THAT

$$\begin{aligned} a^{2(h+1)} - b^{2(h+1)} &= a^{2h} \cdot a^2 + b^{2h} \cdot b^2 = [(a+b)m + b^{2h}]a^2 - b^{2h} \cdot b^2 \\ &= (a+b)m \cdot a^2 + b^{2h} \cdot a^2 - b^{2h} \cdot b^2 \\ &= (a+b)\, m a^2 + b^{2h}(a^2 - b^2) \\ &= (a+b)\, m a^2 + b^{2h} \cdot (a+b)(a-b) \\ &= (a+b) \cdot [m a^2 + b^{2h} \cdot (a-b)] \end{aligned}$$

SINCE $a, b, m \in \mathbb{Z}$, $h \in \mathbb{N}$ WE OBSERVE $m a^2 + b^{2h}(a-b) \in \mathbb{Z}$.

THIS SHOWS THAT $a+b \mid a^{2(h+1)} - b^{2(h+1)}$. THE CLAIM NOW FOLLOWS BY THE INDUCTION PRINCIPLE.

(iii) IF $m \in \mathbb{N}$ IS AN ODD NUMBER SHOW $a+b \mid a^m + b^m$.

NOTE THE RESULT HOLDS WHEN $m=1$ AS $a+b \mid a+b$. ASSUME $m>1$. SINCE m IS odd, $m = 2k+1$ FOR SOME $k \in \mathbb{N}$. WE NEXT SHOW THAT $a+b \mid a^{2k+1} + b^{2k+1}$ FOR EVERY $k \in \mathbb{N}$. IF $k=1$ WE OBSERVE $a^3+b^3 = (a+b)(a^2 - ab + b^2)$ AND $a^2 - ab + b^2 \in \mathbb{Z}$. THIS SHOWS $a+b \mid a^3+b^3$. ASSUME $a+b \mid a^{2h+1} + b^{2h+1}$ FOR SOME $h \in \mathbb{N}$, $h>1$. THEN, THERE EXISTS $q \in \mathbb{Z}$ SUCH THAT $a^{2h+1} + b^{2h+1} = (a+b) \cdot q$. WE NEXT NOTE

$$
\begin{aligned}
a^{2(h+1)+1} + b^{2(h+1)+1} &= a^{2h+1} \cdot a^2 + b^{2h+1} \cdot b^2 \\
&= \left((a+b)q - b^{2h+1}\right) a^2 + b^{2h+1} \cdot b^2 \\
&= (a+b) q a^2 + b^{2h+1}(b^2 - a^2) \\
&= (a+b) q a^2 + b^{2h+1}(b-a)(a+b) \\
&= (a+b) \cdot \left[q a^2 + b^{2h+1}(b-a) \right]
\end{aligned}
$$

SINCE $a, b, q \in \mathbb{Z}$, $h \in \mathbb{N}$, WE HAVE $q a^2 + b^{2h+1}(b-a) \in \mathbb{Z}$. THIS SHOWS $a+b \mid a^{2(h+1)+1} + b^{2(h+1)+1}$. HENCE, THE RESULT HOLDS BY THE PRINCIPLE OF INDUCTION. $\blacksquare$

(5) LET $a \in \mathbb{Z}$ BE AN ODD INTEGER. SHOW THAT $2^{m+2} \mid a^{2^m} - 1$ FOR ALL $m \in \mathbb{N}$.

SINCE $a \in \mathbb{Z}$ IS ODD, THERE EXISTS $k \in \mathbb{Z}$ SUCH THAT $a = 2k+1$. WE WILL PROCEED BY INDUCTION ON $m \in \mathbb{N}$. IF $m=1$ WE HAVE

TO SHOW THAT $8 \mid a^2-1$. NOTE THAT

$$a^2-1 = (a+1)(a-1) = (2k+2)2k = 2(k+1)2k = 4k(k+1).$$

IN ADDITION, $2 \mid k(k+1)$ SINCE EITHER k OR $k+1$ IS EVEN.

IT FOLLOWS FROM THE ABOVE COMMENTS THAT $8 \mid a^2-1$.

ASSUME NOW THAT $2^{n+2} \mid a^{2^n}-1$ FOR SOME $n \in \mathbb{N}$, $n>1$.

THEN, THERE EXISTS $l \in \mathbb{Z}$ SUCH THAT $a^{2^n}-1 = 2^{n+2} \cdot l$.

NEXT WE OBSERVE

$$a^{2^{n+1}} - 1 = a^{2^n \cdot 2} - 1 = a^{2^n})^2 - 1 = (a^{2^n}+1)(a^{2^n}-1).$$

WE NEXT PROVE THAT $2 \mid a^m + 1$ FOR EVERY $m \in \mathbb{N}$.

RECALL THAT a IS odd. SO, $a = 2k+1$ FOR SOME $k \in \mathbb{Z}$.

LET $S = \{ m \in \mathbb{N} : 2 \mid a^m + 1 \}$. OBSERVE THAT $1 \in S$

SINCE $a^1 + 1 = a+1 = (2k+1)+1 = 2k+2 = 2(k+1)$ AND $k+1 \in \mathbb{Z}$.

GIVEN $n \in \mathbb{N}$, $n>1$, SUPPOSE $n \in S$. THEN, THERE EXISTS

$q \in \mathbb{Z}$ SUCH THAT $a^n + 1 = 2q$. HENCE, WE NOTICE

$$\begin{aligned} a^{n+1} + 1 &= a \cdot a^n + 1 = a(2q-1)+1 \\ &= (2k+1)(2q-1) + 1 \\ &= 4kq - 2k + 2q - 1 + 1 \\ &= 2(2kq - k + q) \end{aligned}$$ WHERE $2kq-k+q \in \mathbb{Z}$.

THIS SHOWS THAT $2 \mid a^{n+1}+1$. WE THEREFORE HAVE

$S = \mathbb{N}$. IN PARTICULAR, $2^n \in S$. THIS MEANS THAT

$2 \mid a^{2^n}+1$. SO THERE EXISTS $m \in \mathbb{Z}$ SUCH THAT

$a^{2^n}+1 = 2m$. HENCE, IT FOLLOWS FROM THE

ABOVE COMMENTS,

$$a^{2^{n+1}} - 1 = \left(a^{2^n}+1\right)\left(a^{2^n}-1\right) = 2m.2^{n+2}\ell = 2^{n+3}m\ell = 2^{(n+1)+2}m\ell$$

WITH $m\ell \in \mathbb{Z}$. WE THEREFORE HAVE $2^{(n+1)+2} \mid a^{2^{n+1}} - 1$. THE RESULT FOLLOWS FROM THE PRINCIPLE OF INDUCTION. $\blacksquare$

(6) LET $m \in \mathbb{N} \cup \{0\}$.

(i) PROVE THAT, FOR EVERY $0 \leq k \leq m$ THE NUMBER $\binom{m}{k}$ IS A NATURAL NUMBER.

(ii) SHOW THAT $m+1$ DIVIDES $\binom{2m}{m}$.

(i) LET $S = \{ m \in \mathbb{N} : \binom{m}{k} \in \mathbb{N},$ FOR ALL $0 \leq k \leq m \}$. WE FIRST SHOW THAT $1 \in S$. TO DO THIS, WE NEED TO PROVE THAT $\binom{1}{k} \in \mathbb{N}$ FOR ALL $0 \leq k \leq 1$. IF $k=0$, NOTE $\binom{1}{0} = \dfrac{1!}{0!\,1!} = 1$ WHILE IF $k=1$ THEN $\binom{1}{1} = \dfrac{1!}{1!\,0!} = 1$. THIS SHOWS THAT $\binom{1}{0} \in \mathbb{N}$ AND $\binom{1}{1} \in \mathbb{N}$. SO, $1 \in S$. GIVEN $n \in \mathbb{N}$, $n > 1$, LET'S ASSUME $\binom{n}{k} \in \mathbb{N}$ FOR EVERY $0 \leq k \leq n$. WE WILL PROVE THAT $n+1 \in S$. SO, WE NEED TO SHOW THAT $\binom{n+1}{k} \in \mathbb{N}$ FOR EVERY $0 \leq k \leq n+1$. NOTE THAT $\binom{n+1}{0} = \binom{n+1}{n+1} = 1 \in \mathbb{N}$. IT REMAINS TO PROVE THAT $\binom{n+1}{k} \in \mathbb{N}$ FOR ALL $1 \leq k \leq n$. BY PASCAL'S RULE WE NOTICE $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$. NOTE ALSO THAT $0 \leq k-1 \leq n-1 < n$. THEREFORE, BY THE INDUCTION HYPOTHESIS THE NUMBERS $\binom{n}{k} \in \mathbb{N}$ AND $\binom{n}{k-1} \in \mathbb{N}$. HENCE, AS $\mathbb{N}$ IS CLOSED UNDER THE ADDITION, WE

HAVE $\binom{n+1}{k} \in \mathbb{N}$ FOR ALL $1 \le k \le n$. THE RESULT NOW FOLLOWS BY THE PRINCIPLE OF INDUCTION.

(ii) WE OBSERVE THAT

$$(2m+1)\cdot\binom{2m}{m} = (2m+1)\cdot\frac{2m!}{m!\;m!} = \frac{m+1}{m+1}\cdot\frac{(2m+1)!}{m!\;m!}$$

$$= (m+1)\cdot\frac{(2m+1)!}{(m+1)!\;m!} = (m+1)\cdot\binom{2m+1}{m}.$$

THEREFORE, WE CAN WRITE

$$\begin{aligned}\binom{2m}{m} &= (2m+2)\binom{2m}{m} - (2m+1)\binom{2m}{m}\\ &= (2m+2)\binom{2m}{m} - (m+1)\binom{2m+1}{m}\\ &= (m+1)\cdot\left[2\binom{2m}{m} - \binom{2m+1}{m}\right].\end{aligned}$$

BY (i), THE NUMBERS $\binom{2m}{m} \in \mathbb{N}$, $\binom{2m+1}{m} \in \mathbb{N}$. THIS SHOWS THAT $2\cdot\binom{2m}{m} - \binom{2m+1}{m} \in \mathbb{Z}$. HENCE, $m+1$ DIVIDES $\binom{2m}{m}$. $\blacksquare$

(7) PROVE THAT $56 \mid 13^{2m} + 28m^2 - 84m - 1$ FOR ALL $m \in \mathbb{N}$.

WE WILL PROCEED BY INDUCTION. LET S BE THE SET $S = \{ m \in \mathbb{N} : 56 \mid 13^{2m} + 28m^2 - 84m - 1 \}$. NOTE THAT $13^2 + 28 - 84 - 1 = 112 = 56 . 2$ WHICH SHOWS THAT $1 \in S$. ASSUME NOW THAT $h \in S$ FOR SOME $h \in \mathbb{N}, h > 1$. THEN, THERE EXISTS $k \in \mathbb{N}$ SUCH THAT $13^{2h} + 28h^2 - 84h - 1 = 56k$. WE WILL SHOW NOW THAT $h+1 \in S$. TO DO THIS, NOTICE

$$
\begin{aligned}
13^{2(h+1)} + 28(h+1)^2 - 84(h+1) - 1 &= 13^2 . 13^{2h} + 28(h^2+2h+1) - 84h - 84 - 1 \\
&= 169 . 13^{2h} + 28(2h+1) + (28h^2 - 84h - 1) - 84 \\
&= 169 . 13^{2h} + 56h + 28 + 56k - 13^{2h} - 84 \\
&= 168 . 13^{2h} + 56h + 56k - 56 \\
&= 56 (3 . 13^{2h} + h + k - 1)
\end{aligned}
$$

SINCE $k \in \mathbb{Z}, h \in \mathbb{N}$, THE NUMBER $3 . 13^{2h} + h + k - 1 \in \mathbb{Z}$. THEN, $56 \mid 13^{2(h+1)} + 28(h+1)^2 - 84(h+1) - 1$ AND SO, $h+1 \in S$. THEREFORE, BY THE PRINCIPLE OF INDUCTION, THE SET $S = \mathbb{N}$. $\blacksquare$

THEOREM: (DIVISION ALGORITHM) GIVEN INTEGERS a AND b, WITH $b \neq 0$, THERE EXIST UNIQUE INTEGERS q AND r SUCH THAT

$$a = q \cdot b + r \quad \text{AND} \quad 0 \leq r < |b|.$$

THE INTEGERS q AND r ARE CALLED, RESPECTIVELY, THE QUOTIENT AND REMAINDER IN THE DIVISION OF a BY b.

(8) PROVE THAT IF a AND b ARE INTEGERS, WITH $b > 0$, THEN THERE EXIST UNIQUE INTEGERS q AND r SATISFYING $a = qb + r$ WHERE $2b \leq r < 3b$.

BY THE DIVISION ALGORITHM THEOREM, GIVEN $a, b \in \mathbb{Z}$, $b \neq 0$, THERE EXIST UNIQUE INTEGERS q' AND r' SUCH THAT $a = q'b + r'$ WITH $0 \leq r' < b$. THEN, WE OBSERVE

$$a = q'b + r' = q'b + r' + 2b - 2b = (q' - 2)b + (r' + 2b).$$

LET $q := q' - 2$ AND $r := r' + 2b$. NOTICE q, r ARE UNIQUE SINCE q', r' ARE UNIQUE. MOREOVER, $a = qb + r$ AND SINCE $0 \leq r' < b$ THEN $2b \leq r' + 2b < 3b$. $\blacksquare$

(9) (i) SHOW THAT THE SQUARE OF ANY INTEGER IS EITHER OF THE FORM $3k$ OR $3k+1$, FOR SOME $k \in \mathbb{Z}$.

(ii) PROVE THAT $3a^2 - 1$ IS NOT A PERFECT SQUARE.

(i) LET $a \in \mathbb{Z}$. BY THE DIVISION ALGORITHM THEOREM, THERE EXIST UNIQUE INTEGERS q, r SUCH THAT $a = 3q + r$ WITH $r \in \{0, 1, 2\}$.

THEN, $a^2 = (3q + r)^2 = 3^2 q^2 + 2 \cdot 3q \cdot r + r^2 = 3(3q^2 + 2qr) + r^2$.

IF $r = 0$ THEN $a^2 = 3k$ WITH $k := 3q^2 \in \mathbb{Z}$.

IF $r = 1$ THEN $a^2 = 3k + 1$ WITH $k := 3q^2 + 2q \in \mathbb{Z}$.

IF $r=2$ THEN $a^2 = 3k+1$ WITH $k := 3q^2+4q+1 \in \mathbb{Z}$.

(ii) SUPPOSE THAT $3a^2-1$ IS A PERFECT SQUARE. THEN, THERE EXISTS $m \in \mathbb{Z}$ SUCH THAT $3a^2-1 = m^2$. NOTICE,

$$m^2 = 3a^2-1 = 3a^2-1+3-3 = 3(a^2-1)+2$$

WHICH MEANS, BY THE DIVISION ALGORITHM THEOREM, THAT m^2 HAS REMAINDER 2 IN THE DIVISION BY 3. OBSERVE THIS CONTRADICTS (i) SINCE THE SQUARE OF ANY INTEGER HAS EITHER REMAINDER 0 OR 1 IN THE DIVISION BY 3. THEREFORE, $3a^2-1$ IS NOT A PERFECT SQUARE. $\blacksquare$

(10) GIVEN $a, b \in \mathbb{Z}$ WITH $b \neq 0$, PROVE THERE EXIST UNIQUE INTEGERS q AND r THAT SATISFY $a = bq+r$ WHERE $-1/2\,|b| < r \leq 1/2\,|b|$.

BY THE DIVISION ALGORITHM THEOREM, THERE EXIST UNIQUE $q', r' \in \mathbb{Z}$ SUCH THAT $a = bq'+r'$ WHERE $0 \leq r' < |b|$.

IF $0 \leq r' \leq 1/2\,|b|$, TAKE $q := q'$ AND $r := r'$ SO THAT $a = bq'+r' = bq+r$ AND $-\frac{1}{2}|b| < 0 \leq r' = r \leq \frac{1}{2}|b|$.

NOW, ASSUME $1/2\,|b| < r' < |b|$. THEN, $-\frac{1}{2}|b| < r'-|b| < 0$.

NOTE WE CAN WRITE $a = bq'+r' = bq' + |b| + r' - |b|$.

IF $b > 0$ THEN $a = b(q'+1) + (r'-|b|)$ AND WE CAN TAKE $q := q'+1$ AND $r := r'-|b|$. ON THE OTHER HAND, IF $b < 0$ THEN $a = b(q'-1) + (r'-|b|)$ AND SO, WE CAN TAKE $q := q'-1$ AND $r := r'-|b|$. THE CLAIM HOLDS. $\blacksquare$

(11) PROVE THAT NO INTEGER IN THE FOLLOWING SEQUENCE IS A PERFECT SQUARE: 11, 111, 1111, 11111, ...

LET a_m BE THE M-TH NUMBER OF SUCH SEQUENCE. NOTE

$a_1 = 11 = 1 + 10$

$a_2 = 111 = 1 + 10 + 10^2$

$a_3 = 1111 = 1 + 10 + 10^2 + 10^3$

$a_4 = 11111 = 1 + 10 + 10^2 + 10^3 + 10^4$

SO, IN GENERAL, $a_m = \sum_{k=0}^{m} 10^k$. FOR $m \geq 2$ WE OBSERVE

$a_m = \sum_{k=0}^{m} 10^k = 1 + 10 + \sum_{k=2}^{m} 10^k = 11 + 100 \sum_{k=2}^{m} 10^{k-2}$. SINCE

$k \geq 2$, THE NUMBER $k := \sum_{k=2}^{m} 10^{k-2} \in \mathbb{N}$. SO, $a_m = 100k + 11$ FOR

SOME $k \in \mathbb{Z}$. THEN, $a_m = 4(25k+2) + 3$ FOR $m \geq 2$.

IF $m = 1$, $a_m = 11 = 4.2 + 3$. THEREFORE, FOR EVERY $m \in \mathbb{N}$,

$a_m = 4.q_m + 3$ FOR SOME $q_m \in \mathbb{Z}$. BY THE DIVISION ALGORITHM THEOREM, a_m HAS REMAINDER 3 IN THE DIVISION BY 4 FOR EVERY $m \in \mathbb{N}$. HENCE, BY (9)(i), a_m IS NOT A PERFECT SQUARE. $\blacksquare$

(12) THE REMAINDER IN THE DIVISION OF AN INTEGER a BY 18 EQUALS 5. FIND THE REMAINDER

(i) IN THE DIVISION OF $a^2 - 3a + 11$ BY 18

BY THE DIVISION ALGORITHM THEOREM, WE KNOW THERE EXIST UNIQUE $q \in \mathbb{Z}$ SUCH THAT $a = 18q + 5$. THEN

$$a^2 - 3a + 11 = (18q+5)^2 - 3(18q+5) + 11$$

$$= 18 \cdot 18q^2 + 2 \cdot 18q \cdot 5 + 5^2 - 3 \cdot 18q - 3 \cdot 5 + 11$$

$$
\begin{aligned}
&= 18(18q^2 + 2q.5 - 3q) + (5^2 - 3.5 + 11)\\
&= 18(18q^2 + 2q.5 - 3q) + 21\\
&= 18(18q^2 + 10.q - 3q) + 18 + 3\\
&= 18(18q^2 + 7q + 1) + 3
\end{aligned}
$$

BY THE DIVISION ALGORITHM THEOREM, THERE EXIST UNIQUE $q', r' \in \mathbb{Z}$ SUCH THAT $a^2 - 3a + 11 = 18q' + r'$ WITH $0 \leq r' \leq 17$. THEREFORE, $q' := 18q^2 + 7q + 1$ AND $r' = 3$.

(ii) IN THE DIVISION OF a BY 3.

BY THE DIVISION ALGORITHM THEOREM, WE KNOW THERE EXIST UNIQUE $q \in \mathbb{Z}$ SUCH THAT $a = 18q + 5$. THEN

$$a = 18q + 5 = 18q + 5 = 18q + 3 + 2 = 3(6q + 1) + 2$$

SINCE $6q + 1 \in \mathbb{Z}$ AND $0 < 2 < 3$, BY THE ALGORITHM DIVISION THEOREM, THE DESIRED REMAINDER IS 2.

(iii) IN THE DIVISION OF $1 - 3a$ BY 27

BY THE DIVISION ALGORITHM THEOREM, WE KNOW THERE EXIST UNIQUE $q \in \mathbb{Z}$ SUCH THAT $a = 18q + 5$. THEN

$$
\begin{aligned}
1 - 3a &= 1 - 3(18q + 5) = 1 - 54q - 15 = -54q - 14\\
&= 27.(-2)q - 14 = 27.(-2)q + 27.(-1) + 13\\
&= 27.(-2q - 1) + 13
\end{aligned}
$$

WE THUS HAVE THE DESIRED REMAINDER IS 13 SINCE $-2q - 1 \in \mathbb{Z}$ AND $0 < 13 < 27$. $\blacksquare$

(13)

(i) PROVE THAT, FOR ALL $m \in \mathbb{N}$, 2^{5m} HAS REMAINDER EQUALS 1 IN THE DIVISION BY 31.

FOR EVERY $m \in \mathbb{N}$, WE OBSERVE

$$2^{5m} = (2^5)^m = 32^m = (31+1)^m = \sum_{k=0}^{m} \binom{m}{k} \cdot 31^k$$

RECALL THAT $\binom{m}{k} \in \mathbb{N}$ FOR ALL $0 \leq k \leq m$. THEN,

$$2^{5m} = \sum_{k=0}^{m} \binom{m}{k} \cdot 31^k = \binom{m}{0} \cdot 31^0 + \sum_{k=1}^{m} \binom{m}{k} \cdot 31^k$$

$$= 1 + 31 \cdot \sum_{k=1}^{m} \binom{m}{k} \cdot 31^{k-1}$$

NOTE $\sum_{k=1}^{m} \binom{m}{q} \cdot 31^{k-1} \in \mathbb{N}$. THEN, BY THE ALGORITHM DIVISION THEOREM, THE REMAINDER OF 2^{5m} IN THE DIVISION BY 31 IS 1.

(ii) FIND THE REMAINDER OF 2^{51833} IN THE DIVISION BY 31.

NOTE $51833 = 5 \cdot 10366 + 3$ AND SO $5 \nmid 51833$.
BY (i), THE REMAINDER OF 2^{51830} IN THE DIVISION BY 31 IS 1. THEN, WE CAN WRITE

$$2^{51830} = 31 \cdot q + 1 \quad \text{FOR SOME } q \in \mathbb{Z}.$$

WE NEXT NOTICE

$$2^{51833} = 2^{51830+3} = 2^{51830} \cdot 2^3 = 8 \cdot 2^{51830}$$

$$= 8 \cdot (31q+1) = 31 \cdot (8q) + 8.$$

THIS SHOWS THE REMAINDER OF 2^{51833} IN THE DIVISION BY 31 IS 8.

(iii) LET $k \in \mathbb{N}$. IF $31 \mid 2^k - 39$, FIND THE REMAINDER IN THE DIVISION OF k BY 5.

BY THE ALGORITHM DIVISION THEOREM, THERE EXIST UNIQUE $q, r \in \mathbb{N}$ SUCH THAT $k = 5q + r$ WITH $r \in \{0,1,2,3,4\}$. BY (i), THERE EXISTS $m \in \mathbb{Z}$ SUCH THAT $2^{5q} = 31 \cdot m + 1$. THEN,

$$2^k - 39 = 2^{5q+r} - 39 = 2^r(31m+1) - 39$$
$$= 31 \cdot 2^r \cdot m + 2^r - 39$$
$$= 31(2^r \cdot m - 1) + (2^r - 8)$$

SINCE $31 \mid 2^k - 39$ WE HAVE $2^r - 8 = 0$.

THIS SHOWS THAT $r = 3$.

(iv) FIND THE REMAINDER IN THE DIVISION OF
$43 \cdot 2^{163} + 11 \cdot 5^{221} + 61^{999}$ BY 31.

NOTE THAT $61 = 2 \cdot 31 - 1 = 31 \cdot 2 + (-1)$. THEN, BY THE BINOMIAL THEOREM,

$$61^{999} = [31 \cdot 2 + (-1)]^{999} = \sum_{k=0}^{999} \binom{999}{k} \cdot (31 \cdot 2)^k \cdot (-1)^{999-k}$$
$$= \sum_{k=0}^{999} \binom{999}{k} \cdot 31^k \cdot 2^k \cdot (-1)^{999-k}$$

$$= \binom{999}{0} \cdot 31^0 \cdot 2^0 \cdot (-1)^{999} + \sum_{k=1}^{999} \binom{999}{k} \cdot 31^k \cdot 2^k \cdot (-1)^{999-k}$$

$$= -1 + 31 \cdot \underbrace{\sum_{k=1}^{999} \binom{999}{k} \cdot 31^{k-1} \cdot 2^k \cdot (-1)^{999-k}}_{\in \mathbb{Z} \quad \text{Why?}}$$

THIS SHOWS $61^{999} = 31 \cdot q + (-1)$ FOR SOME $q \in \mathbb{Z}$.

WE ALSO OBSERVE $5^3 = 125 = 31 \cdot 4 + 1$. THEN, FOR ANY $m \in \mathbb{N}$, BY THE BINOMIAL THEOREM,

$$5^{3m} = (5^3)^m = 125^m = (31 \cdot 4 + 1)^m = \sum_{k=0}^{m} \binom{m}{k} \cdot 31^k \cdot 4^k \cdot 1^{m-k}$$

$$= \binom{m}{0} \cdot 31^0 \cdot 4^0 + \sum_{k=1}^{m} \binom{m}{k} 31^k \cdot 4^k$$

$$= 1 + 31 \cdot \underbrace{\sum_{k=1}^{m} \binom{m}{k} \cdot 31^{k-1} \cdot 4^k}_{\in \mathbb{Z} \quad \text{Why?}}$$

$$= 31 \cdot q_m + 1 \quad \text{FOR SOME } q_m \in \mathbb{Z}.$$

NOTE $221 = 3 \cdot 73 + 2$. SO, FROM THE ABOVE COMMENTS, THERE EXISTS $q'' := q_{73} \in \mathbb{Z}$ SUCH THAT

$$5^{219} = 5^{3 \cdot 73} = 31 \cdot q'' + 1$$

IN ADDITION, BY (i) ABOVE, SINCE $163 = 5 \cdot 32 + 3$,

THERE EXISTS $q''' \in \mathbb{Z}$ SUCH THAT

$$2^{160} = 2^{5.32} = \left(2^5\right)^{32} = 31.q''' + 1.$$

LET $m = 43.2^{163} + 11.5^{221} + 61^{999}$.

IT FOLLOWS FROM THE ABOVE COMMENTS,

$$\begin{aligned}
m &= 43.2^{160}.2^3 + 11.5^{219}.5^2 + 61^{999} \\
&= 43.8.(31q''' + 1) + 11.25.(31q'' + 1) + 31q - 1 \\
&= 31(43.8.q''' + 11.25.q'' + q) + 43.8.1 + 11.25.1 - 1 \\
&= 31\underbrace{(43.8.q''' + 11.25.q'' + q)}_{\in \mathbb{Z} \quad \text{Why?}} + 618 \\
&= 31.t + 31.19 + 29 \qquad \text{FOR SOME } t \in \mathbb{Z}. \\
&= 31.(t+1) + 29
\end{aligned}$$

WE THUS OBSERVE $m = 31.(t+1) + 29$ WHERE $t+1 \in \mathbb{Z}$ AND $0 < 29 < 31$. THEN, BY THE DIVISION ALGORITHM THEOREM, THE REMAINDER OF m IN THE DIVISION BY 31 EQUALS 29. $\blacksquare$