Congruences

DEFINITION: Let m be a fixed positive integer. Two integers a, b are said to be congruent modulo m, symbolized by $a \equiv b \pmod m$ or simply, $a \equiv_m b$ if m divides the difference $a-b$.

EXERCISE 1: Let $m \in \mathbb{N}, m > 1$ be fixed and $a, b, c \in \mathbb{Z}$. Prove the following properties hold:

(i) $a \equiv_m a$

(ii) if $a \equiv_m b$ then $b \equiv_m a$.

(iii) if $a \equiv_m b$ and $b \equiv_m c$ then $a \equiv_m c$.

(iv) if $a \equiv_m b$ then $a+c \equiv_m b+c$ for every $c \in \mathbb{Z}$.

(v) if $a \equiv_m b$ then $a.c \equiv_m b.c$ for every $c \in \mathbb{Z}$.

(vi) if $a \equiv_m b$ and $c \equiv_m d$ then $a+c \equiv_m b+d$.

(vii) if $a \equiv_m b$ and $c \equiv_m d$ then $ac \equiv_m bc$.

(viii) if $a \equiv_m b$ then $a^k \equiv_m b^k$ for all $k \in \mathbb{N}$.

(ix) $a \equiv_m r_m(a)$ where $r_m(a)$ denotes the remainder in the division of a by m. Moreover, if $0 \leq r < m$ and $a \equiv_m r$ then $r = r_m(a)$.

(x) $a \equiv_m 0$ iff $m \mid a$.

(xi) $a \equiv_m a + mq$ for every $q \in \mathbb{Z}$.

(xii) Suppose $c \in \mathbb{N}$. Then, $a \equiv_m b$ iff $ac \equiv_{m.c} bc$.

SOLUTION: Let $m \in \mathbb{N}$ and let $a, b, c, d \in \mathbb{Z}$.

(i) Note that $m \mid 0$ and $0 = a - a$. Then, $m \mid a - a$ which means $a \equiv_m a$.

(ii) If $a \equiv_m b$ then $m \mid a-b$. So, $m \mid (a-b).(-1)$. Then, $m \mid b - a$. That is, $b \equiv_m a$.

(iii) IF $a \equiv_m b$ AND $b \equiv_m c$ THEN $m \mid a-b$ AND $m \mid c-b$. NOW, WE OBSERVE $a-c = a-b+b-c = (a-b)+(b-c) = (a-b)-(c-b)$. WE THEREFORE HAVE $m \mid (a-b)-(c-b)$ WHICH YIELDS $m \mid a-c$. THIS SHOWS $a \equiv_m c$.

(iv, v) SUPPOSE $a \equiv_m b$. THEN $m \mid a-b$ AND SO $mk = a-b$ FOR SOME $k \in \mathbb{Z}$. NOW, NOTE THAT $mk = a-b = a+c-c-b = (a+c)-(b+c)$ AND THEN, $m \mid (a+c)-(b+c)$. MOREOVER, $mkc = (a-b)c = ac-bc$ AND $m \mid ac-bc$. HENCE $a+c \equiv_m b+c$ AND $ac \equiv_m bc$.

(vi, vii) SUPPOSE $a \equiv_m b$ AND $c \equiv_m d$. THEN, BY (iv) $a+c \equiv_m b+c$ AND $c+b \equiv_m d+b$. SO, BY (iii), $a+c \equiv_m b+c \equiv_m b+d$. SIMILARLY, BY (v), $ac \equiv_m cb$ AND $bc \equiv_m bd$. THEN, BY (iii), $ac \equiv_m bc \equiv_m bd$.

(viii) IMMEDIATELY BY (vii) ABOVE AND A STRAIGHTFORWARD INDUCTION ARGUMENT.

(ix) BY THE ALGORITHM DIVISION THEOREM, THERE EXIST UNIQUE $\alpha, \beta \in \mathbb{Z}$ SUCH THAT $a = \alpha m + \beta$ WHERE $0 \leq \beta < m$. THEN, $a - r_m(a) = a - \beta = m.\alpha$ AND SO, $a \equiv_m r_m(a)$. MOREOVER, IF $a \equiv_m r$ AND $0 \leq r < m$. THEN, $a - r = mq$ FOR SOME $q \in \mathbb{Z}$. THAT IS, $a = mq + r$ WITH $0 \leq r < m$. SINCE THE QUOTIENT AND THE REMAINDER IN THE DIVISION OF a BY m ARE UNIQUE, IT MUST BE $q = \alpha$ AND $r = \beta = r_m(a)$.

(x) NOTE $a \equiv_m 0$ IFF $m \mid a-0$ IFF $m \mid a$.

(xi) NOTE THAT $m \mid mq$. THEN BY (x), $mq \equiv_m 0$. BY (i), WE ALSO HAVE $a \equiv_m a$.
THEN, BY (vi), $a + mq \equiv_m a+0$. THAT IS, $a \equiv_m a + mq$.

(xii) LET $c \in \mathbb{N}$. SUPPOSE FIRST $a \equiv_m b$. THEN $a-b = mk$ FOR SOME $k \in \mathbb{Z}$. THEREFORE,
$ac - bc = (a-b)c = mk.c = mc.k$ AND SO, $mc \mid ac-bc$. THIS SHOWS $ac \equiv_{mc} bc$.
CONVERSELY, IF $ac \equiv_{mc} bc$ THEN $mc \mid ac-bc$ AND SO $mck = ac-bc$ FOR SOME $k \in \mathbb{Z}$. THEN, $c(mk-(a-b)) = 0$ AND SINCE $c \neq 0$, IT MUST BE $mk = a-b$. WE THUS HAVE $m \mid a-b$ AND SO, $a \equiv_m b$.

EXERCISE 2: PROVE EACH OF THE FOLLOWING ASSERTIONS:

(i) IF $a \equiv_M b$ AND $m | M$ THEN $a \equiv_m b$.

(ii) IF $a \equiv_m b$ AND $c > 0$ THEN $ca \equiv_{cm} cb$.

(iii) IF $a \equiv_m b$ AND THE INTEGERS a, b, c ARE ALL DIVISIBLE BY $d > 0$, THEN

$$\frac{a}{d} \equiv_{\frac{m}{d}} \frac{b}{d}.$$

SOLUTION:

(i) IF $a \equiv_M b$ THERE IS SOME $k \in \mathbb{Z}$ SUCH THAT $a - b = k.M$. AS m/M, WE CAN WRITE $M = m.t$ FOR SOME $t \in \mathbb{Z}$. THEN, $a - b = k.M = k.(mt) = (kt)m$ WHICH YIELDS $m / a-b$.

WE THUS HAVE $a \equiv_m b$.

(ii) SEE EXERCISE 1 (xii).

(iii) LET a, b, m BE INTEGERS ALL DIVISIBLE BY $d > 0$. THEN, WE CAN WRITE $a = k_1.d$, $b = k_2.d$, $m = k_3.d$ FOR SOME $k_1, k_2, k_3 \in \mathbb{Z}$. SINCE $a \equiv_m b$, THERE IS SOME $t \in \mathbb{Z}$ SUCH THAT $a - b = t.m$. THEN, $k_1 - k_2 = t k_3$ AND SO $\frac{a}{d} - \frac{b}{d} = k_1 - k_2 = t.k_3 = t.\frac{m}{d}$ WHICH IMPLIES THAT $\frac{a}{d} \equiv_{\frac{m}{d}} \frac{b}{d}$.

EXERCISE 3: IF $a \equiv_m b$, PROVE THAT $\gcd(a,m) = \gcd(b,m)$.

SOLUTION: LET $d = \gcd(a,m)$ AND $d^* = \gcd(b,m)$. SINCE $a \equiv_m b$ WE KNOW $a - b = mk$ FOR SOME $k \in \mathbb{Z}$. AS d/a AND d/m WE HAVE $d/(a - mk)$ AND SO, d/b. THEN, $d/b, d/m$ IMPLIES THAT d/d^*. SIMILARLY, IF d^*/b AND d^*/m THEN $d^*/mk+b$, THAT IS d^*/a. WE THUS HAVE d^*/d. SINCE d^*/d AND d/d^* WE HAVE $d = d^*$. RECALL THAT $d > 0$, $d^* > 0$.

EXERCISE 4: PROVE THAT $53^{103} + 103^{53}$ IS DIVISIBLE BY 39 AND $111^{333} + 333^{111}$ IS DIVISIBLE BY 7.

SOLUTION: WE FIRST OBSERVE THAT $53^{103}+103^{53}$ IS DIVISIBLE BY 39 IFF $53^{103}+103^{53}\equiv_{39} 0$. EVEN MORE, SINCE $39=3.13$ AND $\gcd(3,13)=1$, IF $3 \mid 53^{103}+103^{53}$ AND $13 \mid 53^{103}+103^{53}$ WE GET $39 \mid 53^{103}+103^{53}$. SO, WE WILL SHOW THAT $53^{103}+103^{53}$ IS DIVISIBLE BY 3 AND 13.

AS $53=3.17+2$ AND $103=3.34+1$ WE HAVE, BY EX.1 (ix), THAT $53\equiv_3 2$ AND $103\equiv_3 1$. THEN, BY EX.1(viii), $53^{103}\equiv_3 2^{103}$ AND $103^{53}\equiv_3 1^{53}\equiv_3 1$. NOW, OBSERVE

$$2^{103}\equiv_3 2^{2.51+1}\equiv_3 (2^2)^{51}.2\equiv_3 4^{51}.2\equiv_3 1^{51}.2\equiv_3 1.2\equiv_3 2.$$ THIS IMPLIES THAT

$53^{103}+103^{53}\equiv_3 2^{103}+1\equiv_3 2+1\equiv_3 3\equiv_3 0$. SO, $3 \mid 53^{103}+103^{53}$. SIMILARLY, WE HAVE $53=13.4+1$ AND $103=13.7+12$ WHICH MEANS $103\equiv_{13} 12$ AND $53\equiv_{13} 1$. NOW, OBSERVE

$103\equiv_{13} 12\equiv_{13} (-1)$. THEN $103^{53}\equiv_{13} (-1)^{53}\equiv_{13} -1\equiv_{13} -13+12\equiv_{13} 12$. IN ADDITION, $53^{103}\equiv_{13} 1^{103}\equiv_{13} 1$. WE THUS HAVE $53^{103}+103^{53}\equiv_{13} 1+12\equiv_{13} 13\equiv_{13} 0$. SO, $13 \mid 53^{103}+103^{53}$. THIS SHOWS THAT $39 \mid 53^{103}+103^{53}$.

WE NEXT SHOW THAT $7 \mid 111^{333}+333^{111}$. WE OBSERVE $111=7.15+6$ AND $333=47.7+4$. THIS MEANS THAT $111\equiv_7 6\equiv_7 -1$ AND $333\equiv_7 4$. NOW, $111^{333}\equiv_7 (-1)^{333}\equiv_7 -1$. MOREOVER, $333^{111}\equiv_7 4^{111}\equiv_7 2^{222}\equiv_7 (2^6)^{37}\equiv_7 64^{37}\equiv_7 1^{37}\equiv_7 1$. WE THEREFORE HAVE $7 \mid 333^{111}+111^{333}$ SINCE $333^{111}+111^{333}\equiv_7 (-1)+1\equiv_7 0$.

EXERCISE 5: FOR $m\geqslant 1$, USE CONGRUENCE THEORY TO SHOW $43 \mid 6^{m+2}+7^{2m+1}$.

SOLUTION: WE WILL PROVE THAT $6^{m+2}+7^{2m+1}\equiv_{43} 0$. WE OBSERVE

$$6^{m+2}+7^{2m+1}\equiv_{43} 6^m.6^2+(7^2)^m.7\equiv_{43} 6^m.36+49^m.7\equiv_{43} 6^m.36+6^m.7\equiv_{43} 43.6^m\equiv_{43} 0.$$

WHICH ARE THE PROPERTIES WE USED TO PROVE THIS? WRITE THEM! :)

EXERCISE 6: SHOW THAT $(-13)^{m+1}\equiv_{181} (-13)^m+(-13)^{m-1}$ FOR EVERY $m\in\mathbb{N}$.

SOLUTION: LET $S=\{m\in\mathbb{N}: (-13)^{m+1}\equiv_{181} (-13)^m+(-13)^{m-1}\}$. NOTE THAT $S\subseteq\mathbb{N}$. OBSERVE $1\in S$ IFF $(-13)^2\equiv_{181} (-13)^1+(-13)^0$ IFF $(-13)^2\equiv_{181} -12$. THEN, NOTE WE HAVE $(-13)^2-(-12)=169+12=181=181.1$ WHICH SHOWS $181 \mid (-13)^2-(-12)$ AND $(-13)^2\equiv_{181} -12$.

THIS IMPLIES THAT $1 \in S$. NOW WE ASSUME $h \in S$, FOR SOME $h \in \mathbb{N}$, $h > 1$. THEN, $(-13)^{h+1} \equiv_{181} (-13)^{h} + (-13)^{h-1}$. WE THEREFORE HAVE

$$(-13)^{(h+1)+1} \equiv_{181} (-13)^{h+1} \cdot (-13) \equiv_{181} (-13) \cdot [(-13)^{h} + (-13)^{h-1}] \equiv_{181} (-13)^{h+1} + (-13)^{h}.$$

THIS IMPLIES THAT $h+1 \in S$. HENCE, BY THE PRINCIPLE OF MATHEMATICAL INDUCTION, $S = \mathbb{N}$. THE RESULT FOLLOWS.

EXERCISE 6: PROVE THE ASSERTTIONS BELOW:

(i) IF a IS AN ODD INTEGER THEN $a^2 \equiv_8 1$.

(ii) FOR ANY INTEGER a, EITHER $a^4 \equiv_5 0$ OR $a^4 \equiv_5 1$.

(iii) FOR ANY INTEGER a, EITHER $a^3 \equiv_7 0$, $a^3 \equiv_7 1$ OR $a^3 \equiv_7 6$.

(iv) IF THE INTEGER a IS NOT DIVISIBLE BY 2 OR 3, THEN $a^2 \equiv_{24} 1$.

SOLUTION:

(i) SUPPOSE $a \in \mathbb{Z}$ IS ODD. BY THE ALGORITHM DIVISION THEOREM, $a = 4q + r$ WHERE $q, r \in \mathbb{Z}$ AND $r \in \{1, 3\}$. NOTE $r \notin \{0, 2\}$ AS a IS ODD. THUS,

$a^2 \equiv_8 (4q + r)^2 \equiv_8 16q^2 + 8qr + r^2 \equiv_8 r^2 \equiv_8 1$ SINCE $1^2 \equiv_8 1$ AND $3^2 \equiv_8 9 \equiv_8 1$.

(ii) BY THE ALGORITHM DIVISION THEOREM, $a = 5q + r$ WITH $q, r \in \mathbb{Z}$, $0 \le r \le 4$. WE OBSERVE $a^4 \equiv_5 (5q + r)^4 \equiv_5 \sum_{k=0}^{4} \binom{5}{k} (5q)^k \cdot r^{4-k} \equiv_5 r^4 + 5 \cdot \sum_{k=1}^{4} \binom{5}{k} (5q)^{k-1} \cdot r^{4-k} \equiv_5 r^4$.

IF $r = 0$ THEN $r^4 \equiv_5 0$. IF $r = 1$ THEN $r^4 \equiv_5 1^4 \equiv_5 1$.

IF $r = 2$ THEN $r^4 \equiv_5 2^4 \equiv_5 16 \equiv_5 1$. IF $r = 3$ THEN $r^4 \equiv_5 3^4 \equiv_5 81 \equiv_5 1$.

HENCE, EITHER $a^4 \equiv_5 0$ OR $a^4 \equiv_5 1$.

(iii) BY THE A.D.T WE CAN WRITE $a = 3q + r$ WHERE $q, r \in \mathbb{Z}$, $0 \le r \le 6$.

THEN, WE OBSERVE $a^3 \equiv_7 (3q + r)^3 \equiv_7 r^3$ BY THE BINOMIAL THEOREM. NOW, WE HAVE $r^3 \in \{0, 1, 8, 27, 64, 125, 216\}$ WHICH SHOWS $r^3 \equiv_7 0$ IF $r = 0$,

$r^3 \equiv_7 1$ if $r \in \{1,2,4\}$ and $r^3 \equiv_7 6$ if $r \in \{3,5,6\}$.

(iv) Let $a \in \mathbb{Z}$. Suppose $2 \nmid a$ and $3 \nmid a$. Then, by the A.D.T, $a = 24q + r$ where $q, r \in \mathbb{Z}$ and $r \in \{1, 5, 7, 11, 13, 17, 19\}$. So, $a^2 \equiv_{24} (24q+r)^2 \equiv_{24} r^2$. Note that $r^2 \in \{1, 25, 49, 121, 169, 289, 361\}$ and the remainder in the division of r^2 by 24 equals 1 as

$1 = 24.0 + 1$	$49 = 24.2 + 1$	$169 = 24.7 + 1$	$361 = 24.15 + 1$
$25 = 24.1 + 1$	$121 = 24.5 + 1$	$289 = 24.12 + 1$	

Hence $a^2 \equiv_{24} r^2 \equiv_{24} 1$. The claim follows.

Exercise 8: If p is a prime satisfying $m < p < 2m$, show

$$\binom{2m}{m} \equiv_p 0.$$

Solution: Let $m \in \mathbb{N}$. Recall that $\binom{2m}{m} \in \mathbb{N}$. Moreover, we can write

$$\binom{2m}{m} = \frac{(2m)!}{m!\,m!} = \frac{(2m).(2m-1).\ \dots\ p \dots (m+1)}{m!}$$

since $m < p < 2m$. We thus have $p \mid \binom{2m}{m}.\, m!$. Since p is prime, either $p \mid m!$ or $p \mid \binom{2m}{m}$. If $p \mid m!$ then there exists $k \in \mathbb{N}, 1 \leq k \leq m$ such that $p \mid k$. This shows $p \leq k \leq m$ contradicting that $m < p$. Therefore, $p \nmid m!$ and so, $p \mid \binom{2m}{m}$. This shows $\binom{2m}{m} \equiv_p 0$.

Exercise 9: Let $a, b \in \mathbb{Z}$ and let p be a prime number. Show

$$(a+b)^p \equiv_p a^p + b^p$$

Solution: Let $a, b \in \mathbb{Z}$ and let $p \in \mathbb{N}$. Suppose that p is prime. Then $p \geq 2$. So, $p-1 \geq 1$. For every $k \in \mathbb{N}$ such that $1 \leq k \leq p-1$, recall that the number $\binom{p-1}{k-1} \in \mathbb{N}$. Moreover, observe $p.\binom{p-1}{k-1} = \frac{p!}{(k-1)!\,(p-k)!} = k.\binom{p}{k}$. Then, $p \mid k.\binom{p}{k}$ for $1 \leq k \leq p-1$. Then, since p is prime, either

$P \mid k$ OR $P \mid \binom{P}{k}$. SINCE $k < P$ WE HAVE $P \nmid k$ AND SO $P \mid \binom{P}{k}$ FOR $1 \leq k \leq P-1$. THIS SHOWS $\binom{P}{k} \equiv_P 0$ FOR EVERY $1 \leq k \leq P-1$. THEREFORE, BY THE BINOMIAL THEOREM,

$$(a+b)^P \equiv_P \sum_{k=0}^{P} \binom{P}{k} . a^k . b^{P-k} \equiv_P b^P + \sum_{k=1}^{P-1} \binom{P}{k} a^k b^{P-k} + a^P \equiv_P a^P + b^P .$$

EXERCISE 10: VERIFY THAT IF $a \equiv_{m_1} b$ AND $a \equiv_{m_2} b$ THEN $a \equiv_m b$ WHERE $m = \ell cm(m_1, m_2)$. IN PARTICULAR, IF m_1 AND m_2 ARE COPRIME, $a \equiv_{m_1 . m_2} b$.

SOLUTION: SINCE $a \equiv_{m_1} b$ AND $a \equiv_{m_2} b$, THERE EXIST $s, t \in \mathbb{Z}$ SUCH THAT $a - b = m_1 . s = m_2 . t$. LET $d = gcd(m_1, m_2)$ AND $m = \ell cd(m_1, m_2)$. SINCE $d \mid m_1$ WE HAVE $m_1 = d . k$ FOR SOME $k \in \mathbb{Z}$. THEN,

$$a - b = m_2 . t = m_2 . t . 1 = m_2 . t . \frac{m_1}{dk} = \frac{m_1 m_2}{d} . \frac{t}{k} = m . \frac{t}{k} .$$

SINCE $d \mid m_2$ WE HAVE $m_2 = d . k'$ FOR SOME $k' \in \mathbb{Z}$. THEN $m_1 s = m_2 t$ IMPLIES THAT $d . k . s = d k' . t$ AND SO $d(ks - k't) = 0$. AS $d > 0$ WE GET $ks = k't$ WHICH YIELDS $k \mid k't$. SINCE k AND k' ARE COPRIME, WE MUST HAVE $k \mid t$ AND THE NUMBER $\frac{t}{k} \in \mathbb{Z}$. THIS SHOWS $m \mid a - b$ AND SO $a \equiv_m b$. NOTE $m = m_1 . m_2$ IF $gcd(m_1, m_2) = 1$. THE RESULT FOLLOWS.

EXERCISE 11: IF a IS AN ODD INTEGER, SHOW $a^{2^m} \equiv_{2^{m+2}} 1$ FOR EVERY POSITIVE INTEGER $m \geq 1$.

SOLUTION: LET $a \in \mathbb{Z}$. SUPPOSE a IS ODD. WE WILL PROCEED BY INDUCTION ON $m \in \mathbb{N}$. IF $m = 1$ THE RESULT HOLDS BY EX. 6 (i). WE ASSUME NEXT THAT $a^{2^h} \equiv_{2^{h+2}} 1$ FOR SOME $h \in \mathbb{N}$, $h > 1$. THEN, $2^{h+2} \mid a^{2^h} - 1$ AND WE

CAN WRITE $a^{2^n}-1=2^{n+2}\cdot q$ FOR SOME $q\in\mathbb{Z}$. THEN,

$$a^{2^{n+1}}-1=a^{2^n\cdot 2}-1=\left(a^{2^n}\right)^2-1=\left(a^{2^n}+1\right)\left(a^{2^n}-1\right)=\left(a^{2^n}+1\right)\cdot 2^{n+2}\cdot q$$

OBSERVE SINCE a IS ODD, $a\equiv_2 1$ AND SO $a^{2^n}\equiv_2 1^{2^n}\equiv_2 1$. THEREFORE,

$a^{2^n}+1\equiv_2 1+1\equiv_2 0$. THIS SHOWS $2\mid a^{2^n}+1$ AND SO, $a^{2^n}+1=2\cdot q'$, $q'\in\mathbb{Z}$.

HENCE, $a^{2^{n+1}}-1=2^{n+2}\cdot 2\,q\,q'=2^{n+3}\cdot qq'=2^{(n+1)+2}\cdot qq'$.

THIS IMPLIES $2^{(n+1)+2}\mid a^{2^{n+1}}-1$ AND SO, $a^{2^{n+1}}\equiv_{2^{(n+1)+2}}1$. THE RESULT NOW IS A CONSEQUENCE OF THE P.M.I.

EXERCISE 12: PROVE THAT FOR ANY $a\in\mathbb{N}$, THE UNIT DIGIT OF a^4 IS 0, 1, 5 OR 6.

SOLUTION: SINCE $a\in\mathbb{N}$, a CAN BE WRITTEN UNIQUELY IN TERMS OF POWERS OF 10 AS FOLLOWS:
$a=\sum_{k=0}^{m}a_k\cdot 10^k$ WHERE $a_k\in\{0,1,2,3,4,5,6,7,8,9\}$ FOR EVERY $0\le k\le m$. NOTE THAT 10 DIVIDES $a-a_0$ SINCE $a-a_0=\sum_{k=1}^{m}a_k\cdot 10^k$. THEN $a\equiv_{10}a_0$ AND SO $a^4\equiv_{10}a_0^4$. NOTICE THAT $a_0^2\in\{0,1,4,9,25,36,49,64,81\}$ AND $r_{10}(a_0^2)\in\{0,1,4,5,6,9\}$. WE THUS HAVE
$a^4\equiv_{10}a_0^4\equiv_{10}a_0^2\cdot a_0^2\equiv_{10}r_{10}(a_0^2)\cdot r_{10}(a_0^2)\equiv_{10}\alpha$ WHERE $\alpha\in\{0,1,5,6\}$. NOW, WE OBSERVE $a^4=\sum_{k=0}^{m}b_k\cdot 10^k=b_0+\sum_{k=1}^{m}b_k\cdot 10^k$ AND $a^4\equiv_{10}b_0$ WHERE b_0 IS THE UNIT DIGIT OF a^4. SO, $b_0\equiv_{10}a^4\equiv_{10}\alpha$ AND $b_0=r_{10}(a^4)=\alpha$. THIS SHOWS THE POSSIBLE VALUES OF b_0 ARE 0, 1, 5, 6. WE NEXT NOTICE ALL OF THEM ARE POSSIBLE AS $0^4=0$, $1^4=1$, $5^4=3125$ AND $2^4=16$.

EXERCISE 13: FIND THE LAST TWO DIGITS OF THE NUMBER 9^{9^9}.

SOLUTION: NOTICE 9^{9^9} CAN BE WRITTEN UNIQUELY AS $\sum_{k=0}^{m}a_k\cdot 10^k$ FOR SOME $m\in\mathbb{N}$ AND $a_k\in\mathbb{Z}$, $0\le a_k\le 9$ FOR EVERY $0\le k\le m$. SO, THE LAST TWO DIGITS ARE a_0 AND a_1. OBSERVE THE NUMBER $a_1a_0=a_1\cdot 10+a_0$ AND $9^{9^9}-a_1a_0\equiv_{100}0$. SINCE $0\le a_1a_0<100$ WE FURTHER HAVE $a_1a_0=r_{100}(9^{9^9})$. SO, TO DETERMINE a_1a_0 WE WILL COMPUTE $r_{100}(9^{9^9})$. WE NOW OBSERVE $9^9\equiv_{10}9^{3\cdot 3}\equiv_{10}(9^3)^3\equiv_{10}9^3\equiv_{10}9$ SINCE $9^3-9=9(9^2-1)=9\cdot 80=10\cdot 72$.

THIS SHOWS $9^9 = 10q+9$ FOR SOME $q \in \mathbb{Z}$. WE ALSO OBSERVE THAT $9 \equiv_4 1$ AND $9^{10} \equiv_4 1^{10} \equiv_4 1$. MOREOVER, $9^{10} \equiv_{25} (9^2)^5 \equiv_{25} 81^5 \equiv_{25} 6^5 \equiv_{25} (6^2)^2.6 \equiv_{25} 11^2.6 \equiv_{25} 121.6$ AND SO, $9^{10} \equiv_{25} (-4).6 \equiv_{25} -24 \equiv_{25} 1$. SINCE $25 | 9^{10}-1$, $4 | 9^{10}-1$ AND $(25,4)=1$ WE HAVE $100 | 9^{10}-1$ AND $9^{10} \equiv_{100} 1$. WE THEREFORE HAVE

$$9^{9^9} \equiv_{100} 9^{10q+9} \equiv_{100} (9^{10})^q . 9^9 \equiv_{100} 1^q . 9^9 \equiv_{100} 9^9 \equiv_{100} 14 .$$

IN FACT, $9 \equiv_4 1$ SHOWS THAT $9^9 \equiv_4 1$ AND WE ALSO HAVE $9^9 \equiv_{25} 14$ AS $9^9 \equiv_{25} 3^{18} \equiv_{25} (3^3)^6 \equiv_{25} 2^6 \equiv_{25} 64 \equiv_{25} 14$. SINCE $\gcd(4,25)=1$, $9^9 \equiv_{100} 14$.

WE THEREFORE CONCLUDE THE LAST TWO DIGITS OF 9^{9^9} ARE $a_1=1$, $a_0=4$.

EXERCISE 14: SHOW THAT AN INTEGER IS DIVISIBLE BY 4 IFF THE NUMBER FORM BY ITS TENS AND UNITS DIGITS IS DIVISIBLE BY 4.

SOLUTION: LET $a \in \mathbb{N}$. WE CAN WRITE $a = \sum_{k=0}^{m} a_k . 10^k$ FOR SOME $a_k \in \mathbb{N}$ WITH $0 \le a_k \le 9$. NOTE ALSO THAT $4 | 100$ AND $100 | 10^k$ FOR EVERY $k \ge 2$. WE THUS HAVE $a \equiv_4 \sum_{k=0}^{m} a_k . 10^k \equiv_4 a_0 + 10.a_1 + \sum_{k=2}^{m} a_k . 10^k \equiv_4 10.a_1 + a_0$. NOW, IF a IS DIVISIBLE BY 4 THEN $a \equiv_4 0$ AND SO $10a_1 + a_0 \equiv_4 a \equiv_4 0$ WHICH MEANS THE NUMBER $a_1 a_0 = 10a_1 + a_0$ IS DIVISIBLE BY 4. CONVERSELY, IF THE NUMBER $a_1 a_0 = 10a_1 + a_0$ IS DIVISIBLE BY 4 THEN $10a_1 + a_0 \equiv_4 0$ AND SO $a \equiv_4 0$. THE CLAIM FOLLOWS.

EXERCISE 15: FIND ALL POSSIBLE VALUES OF X, Y SUCH THAT THE NUMBER 273X49Y5 IS DIVISIBLE BY 495.

SOLUTION: LET $a = 273X49Y5$ FOR SOME INTEGERS $0 \le x, y \le 9$. NOTE WE CAN WRITE $a = 2.10^7 + 7.10^6 + 3.10^5 + x.10^4 + 4.10^3 + 9.10^2 + y.10 + 5$. THAT IS,

$a = \sum_{k=0}^{7} a_k 10^k$ WHERE $a_0=5, a_1=y, a_2=9, a_3=4, a_4=x, a_5=3, a_6=7, a_7=2$.

OBSERVE ALSO THAT $495 = 5.9.11$ AND $\gcd(5,9,11)=1$. WE THUS HAVE $495 | a$ IFF $5|a$, $9|a$ AND $11|a$. NOW WE OBSERVE $5 | 10$ AND SO $a \equiv_5 a_0 \equiv_5 5 \equiv 0$.

SINCE $10 \equiv_9 1$ WE HAVE $10^k \equiv_9 1$. THEN, $a \equiv_9 \sum_{k=0}^{7} a_k 10^k \equiv_9 \sum_{k=0}^{7} a_k$.

THAT IS, $a \equiv_9 5+y+9+4+x+3+7+2 \equiv_9 x+y+30 \equiv_9 x+y+3$. SINCE $a \equiv_9 0$ WE GET $x+y+3 \equiv_9 0$ OR EQUIVALENTLY, $x+y \equiv_9 6$. ON THE OTHER HAND, WE NOTE $10 \equiv_{11} -1$ AND SO $10^k \equiv_{11} (-1)^k$. THIS SHOWS $a \equiv_{11} \sum_{k=0}^{7} (-1)^k . a_k \equiv_{11} 0$ AS $11 | a$. THEN, $a_0 - a_1 + a_2 - a_3 + a_4 - a_5 + a_6 - a_7 \equiv_{11} 5-y+9-4+x-3+7-2 \equiv_{11} x-y+12$.

SO, WE HAVE $x-y+12 \equiv_{11} x-y+1 \equiv_{11} 0$ OR EQUIVALENTLY, $x-y \equiv_{11} 10$. SINCE $0 \le x,y \le 9$ WE HAVE $-6 \le x+y-6 \le 12$ AND $-19 \le x-y-10 \le -1$.

MOREOVER, $9 | (x+y-6)$ AND $11 | (x-y-10)$ IMPLIES THAT $x+y-6 \in \{0,9\}$ AND $x-y-10 \in \{-11, 0\}$.

WE THEREFORE HAVE FOUR POSSIBLE CASES:

$$\begin{cases} x+y=6 \\ x-y=-1 \end{cases} \qquad \begin{cases} x+y=6 \\ x-y=10 \end{cases} \qquad \begin{cases} x+y=15 \\ x-y=10 \end{cases} \qquad \begin{cases} x+y=15 \\ x-y=-1 \end{cases}$$

HOWEVER, SINCE $x,y \in \mathbb{Z}$, $0 \le x,y \le 9$ THE ONLY POSSIBLE CASE IS THE CASE WHEN $x+y=15$ AND $x-y=-1$. THIS SHOWS THAT $x=7$ AND $y=8$.

HENCE, THE NUMBER IS 27374985.

EXERCISE 16: LET $a_m a_{m-1} a_{m-2} \dots a_2 a_1 a_0$ BE A NATURAL NUMBER OF $m+1$ DIGITS WHERE $0 \le a_k \le 9$ FOR $0 \le k \le m$. PROVE THAT THE GIVEN NUMBER IS DIVISIBLE BY 6 IFF $6 | a_0 + 4a_1 + 4a_2 + \dots + 4a_{m-1} + 4a_m$.

SOLUTION: LET $a = a_m a_{m-1} \dots a_1 a_0$. NOTE THAT $a = \sum_{k=0}^{m} a_k . 10^k$. WE NEXT CLAIM THAT $10^m \equiv_6 4$ FOR EVERY $m \in \mathbb{N}$. IF $m=1$ THEN $10^1 \equiv_6 10 \equiv_6 4$.

SUPPOSE $10^h \equiv_6 4$ FOR SOME $h \in \mathbb{N}, h > 1$. THEN, $10^{h+1} \equiv_6 10 . 10^h \equiv_6 10.4 \equiv_6 4.4 \equiv_6 4$.

NOW THE CLAIM HOLDS BY A STRAIGHTFORWARD INDUCTION ARGUMENT.

HENCE, $a \equiv_6 \sum_{k=0}^{m} a_k . 10^k \equiv_6 a_0 + \sum_{k=1}^{m} a_k . 10^k \equiv_6 a_0 + 4 . \sum_{k=1}^{m} a_k$. WE THUS HAVE $6 \mid a$ IFF $6 \mid a_0 + 4a_1 + 4a_2 + \dots + 4a_m$. THE RESULT FOLLOWS.

EXERCISE 17: GIVEN AN INTEGER N, LET M BE THE INTEGER FORMED BY REVERSING THE ORDER OF THE DIGITS OF N. VERIFY THAT THE DIFFERENCE $N - M$ IS DIVISIBLE BY 9.

SOLUTION: LET $N = \sum_{k=0}^{m} a_k . 10^k$ THE DECIMAL EXPANSION OF N, WHERE $0 \leq a_k \leq 9$. THEN, $M = a_m + a_{m-1} . 10 + \dots + a_1 . 10^{m-1} + a_0 . 10^m = \sum_{k=0}^{m} a_{m-k} . 10^{m-k}$. WE THUS HAVE $N - M \equiv_9 \sum_{k=0}^{m} a_k . 10^k - \sum_{k=0}^{m} a_{m-k} . 10^{m-k} \equiv_9 \sum_{k=0}^{m} a_k - \sum_{k=0}^{m} a_{m-k} \equiv_9 0$. THIS SHOWS THAT 9 DIVIDES $N - M$.

$\vdots$

b_{4t+1}