TEST KALEIDOSCOPE (PART: MODULAR ARITHMETIC),
December 2nd, 2019, 19:00pm–22:00pm,
Aletta Jacobshal 02.

Please provide **complete** *arguments for each of your answers. The exam consists of* 3 *questions. You can score up to* 9 *points for each question, and you obtain* 2 *points for free.*
In this way you will score in total between 2 *and* 20 *points.*

(1) For every integer $n \geq 0$ we write $a_n := (7 \cdot 10^n - 1)/3$. So, for example, $a_0 = 2$ and $a_1 = 23$ and $a_2 = 233$, et cetera.
  (a) (3 points.) Show that for every $n \geq 0$ the number a_n is an integer, and moreover
$$2 \,|\, a_n \iff n = 0.$$
  (b) (3 points.) Explain why a_n is not divisible by 42, for all $n \geq 0$.
  (c) (3 points.) Explain why a_n is not divisible by 13, for all $n \geq 0$.

(2) Given an integer $a > 0$, put $n := a^2 - a + 1$.
  (a) (3 points.) Show that $\overline{a}^{-1} = \overline{1} - \overline{a}$ in $(\mathbb{Z}/n\mathbb{Z})^\times$.
  (b) (3 points.) Show that for every *odd* integer $m > 0$ it holds that $(a^2 - a + 1) \,|\, (a^{3m} + 1)$.
  (c) (3 points.) Now take $a = 5$, so that $n = 21$. Find two distinct solutions (x, y) with x, y in $\mathbb{Z}/21\mathbb{Z}$ of the system
$$\begin{cases} \overline{2}x - y &= \overline{6} \\ x + \overline{3}y &= -\overline{4}. \end{cases}$$

Solutions / grading.

(1) (a) a_n is an integer: since $10 \equiv 1 \bmod 3$, it follows that $7 \cdot 10^n \equiv 7 \cdot 1^n \bmod 3 = 7 \bmod 3$ and therefore $7 \cdot 10^n - 1 \bmod 3 = 6 \bmod 3 = 0 \bmod 3$. So $3|7 \cdot 10^n - 1$ and hence $(7 \cdot 10^n - 1)/3$ is an integer.

Other solution: use induction: it is true for $n = 0$. If for some $n \geq 0$ the number a_n is an integer, then $a_{n+1} = (70 \cdot 10^n - 1)/3 = (63 \cdot 10^n + 7 \cdot 10^n - 1)/3 = 21 \cdot 10^n + a_n$ which, using the induction hypothesis, is also an integer.

Third solution: note that $a_{n+1} = 10a_n + 3$. Since a_0 is an integer, it follows by induction that the other a_n (for $n > 0$) are integers as well.

(ANY of these solutions, or a similar one: 1 point)

Note that a_n is even, if and only if $3a_n$ is. Since $3a_n = 7 \cdot 10^n - 1 equiv 10^n - 1 \bmod 2$, and 10^n is even for $n > 0$ and odd for $n = 0$, the result follows.

Alternative solution: using $a_{n+1} = 10a_n + 3$ you see that $a_{n+1} \equiv 1 \bmod 2$, for every $n \geq 0$. Since a_0 is even, the result follows.

(2 points for any solution like this)

(b) Since a_n is odd for $n > 0$, these a_n cannot be multiples of 42. And clearly also a_0 is not divisible by 42.

Alternative solution: if $42|a_n$ then also $42|3a_n = 7 \cdot 10^n - 1$. The latter number is clearly not a multiple of 7, and therefore not a multiple of $42 = 7 \cdot 6$.

Yet another solution: From $a_{n+1} = 10a_n + 3$ one concludes $a_{n+1} \equiv a_n \bmod 3$. Hence all $a_n \bmod 3$ are equal, namely $2 \bmod 3$. In particular they are not divisible by 3, and therefore not by $42 = 3 \cdot 14$.

One more solution: mod 42 note that $10 * 23 + 3 \bmod 42 = 233 \bmod 42 = 23 \bmod 42$. Hence the formula $a_{n+1} = 10a_n + 3$ and $a_1 = 23$ implies $a_n \equiv 23 \bmod 42$, for every $n > 0$. So these a_n are not multiples of 42, and clearly neither is a_0.

(3 points for any correct and complete solution)

FOR PARTIAL ANSWERS, GIVE POINTS ONLY IF THE ARGUMENT CLEARLY POINTS IN THE DIRECTION OF A CONCEIVABLY CORRECT PROOF...

(c) The sequence $a_n \bmod 13$ looks like

$$\overline{2},\ \overline{10},\ \overline{12},\ \overline{6},\ \overline{11},\ \overline{9},\ \cdot\cdot$$

(periodic, with period 6), as one computes, e.g., using the formula $a_{n+1} = 10a_n + 3$. As the residue class $0 \bmod 13$ does not occur, none of the a_n is divisible by 13.

(3 points for any correct and complete solution)

(2) (a) $(\overline{1} - \overline{a}) \cdot \overline{a} = \overline{a - a^2} = \overline{1}$ (since $n|(a - a^2 - 1)$). This shows that $\overline{a}$ is invertible, with inverse $\overline{1} - \overline{a}$.

(2 points for the calculation, 1 point for then remarking that indeed we have the correct inverse. In total 1 point for only showing correctly that $\gcd(a, n) = 1$. Note that this can also be solved via an appropriate extended gcd calculation).

(b) Note that $\overline{a}^3 = \overline{a} \cdot \overline{a^2} = \overline{a} \cdot \overline{a-1} = \overline{a^2 - a} = \overline{-1}$. Hence for odd $m > 0$ it follows that $\overline{a^3}^m = \overline{-1}^m = \overline{-1}$. This means $a^{3m} + 1$ is divisible by $n = a^2 - a + 1$.

Other solution: note that $a^6 - 1 = (a+1)(a-1)(a^2+a+1)(a^2-a+1)$. For $m = 1$ the divisibility holds since $a^3 + 1 = (a+1)(a^2 - a + 1)$. If it holds for some odd $m > 0$, then the next odd number is $m + 2$, and $a^{3(m+2)} + 1 = a^6 \cdot a^3 m + 1 = (a^6 - 1)a^{3m} + (a^{3m} + 1)$. By what we remarked above and by the induction hypothesis, both terms are divisible by n. This finishes the proof by induction.
(3 POINTS FOR ANY CORRECT AND COMPLETE SOLUTION. ONLY 1 POINT IF, E.G., MERELY THE CASE M=1 IS DONE.)

(c) Substituting either $y = \overline{2}x - \overline{6}$ or $x = -\overline{4} - \overline{3}y$ in the 'other' equation, one is left with, e.g., $x + \overline{3}(\overline{2}x - \overline{6}) = -\overline{4}$. This can be rewritten as $\overline{7}x = \overline{14}$. So we look for integers x such that $21|(7x - 14)$, which simply means $3|(x-2)$. Two solutions are $x = 2$ and $x = 5$, with corresponding y respectively -2 and 4.
(-1 FOR A CALCULATION ERROR, -2 IF ONLY ONE SOLUTION IS FOUND. -1 IF IT IS NOT CLEAR WHETHER THE GIVEN SOLUTIONS ARE DISTINCT MODULO 21)