Congruence of Integers

Problem 1
(a)Find r with $0 \leqslant r \leqslant 10$ such that $7^{137} \equiv$ r mod 11.
(b)Find r with $0 \leqslant r < 645$ such that $2^{81} \equiv$ r mod 645.
(c) Find the last two digits of 3^{124} (when expressed in decimal notation).
(d) Show that there is a multiple of 21 which has 241 as its last three digits.

(a) We have:

$$\begin{aligned}
7^1 &\equiv -4 \mod 11\\
7^2 &\equiv 5 \mod 11\\
7^4 &\equiv 3 \mod 11\\
7^8 &\equiv -2 \mod 11\\
7^{16} &\equiv 4 \mod 11\\
7^{32} &\equiv 5 \mod 11\\
7^{64} &\equiv 3 \mod 11\\
7^{128} &\equiv -2 \mod 11
\end{aligned}$$

Therefore, $7^{137} \equiv 7^1 7^{128} 7^8 7^1 \equiv (-2)(-2)(-4) \mod 11 \equiv 6 \mod 11$. Therefore, r = 6. ■

(b)

$$\begin{aligned}
2^1 &\equiv 2 \mod 645\\
2^2 &\equiv 4 \mod 645\\
2^4 &\equiv 16 \mod 645\\
2^8 &\equiv 256 \mod 645\\
2^{16} &\equiv 391 \mod 645\\
2^{32} &\equiv 16 \mod 645\\
2^{64} &\equiv 256 \mod 645
\end{aligned}$$

Therefore, $2^{81} \equiv 2^{16} 2^{64} 2^1 \equiv 391(256)(2) \mod 645 \equiv 242 \mod 645$ ■

(c) To find the last two digits, we can modulo the number by 100. Therefore we have:

$$\begin{aligned}3^2 &\equiv 9 \mod 100\\ 3^4 &\equiv 81 \mod 100\\ 3^8 &\equiv 61 \mod 100\\ 3^{16} &\equiv 21 \mod 100\\ 3^{32} &\equiv 41 \mod 100\\ 3^{64} &\equiv 81 \mod 100\end{aligned}$$

We can write $3^{124} = 3^{64}3^{32}3^{16}3^{8}3^{4} \equiv 3^{32}3^{16}3^{8}3^{8} \mod 100 \equiv 3^{64} \mod 100 \equiv 81 \mod 100$. Therefore, the last two digits are 81. ∎

(d) The statement in the question is equivalent as saying $21k \equiv 241 \mod 1000$ for some $k \in \mathbb{Z}$, and we can write this in the form of $21k - 1000r = 241$ for some $r \in \mathbb{Z}$. Since hcf(21, 1000) = 1, there exist k and r to satisfy this equation, and that for some multiple of 21, the last three digits will be 241. ∎

Problem 3
For each of the following congruence equations, either find a solution x $\in \mathbb{Z}$ or show that no solution exists:
(a) 99x $\equiv$ 18 mod 30.
(b) 91x $\equiv$ 84 mod 143.
(c) $x^2 \equiv$ 2 mod 5.
(d) x^2 + x + 1 $\equiv$ 0 mod 5.
(e) x^2 + x + 1 $\equiv$ 0 mod 7.

(a) We can write the original equation as $99x - 30r = 18$ for some $r \in \mathbb{Z}$. Since hcf(99, 30) = 3, and that 18 is a multiple of 3, the above equation holds for integer x and r. Therefore, there is integer solution to this congruence equation. x = 2 would be one solution. ∎

(b) We can write the original equation as $91x - 143r = 84$ for some $r \in \mathbb{Z}$. We have hcf(91, 143) = 13, which is not a factor of 84. Therefore, $91x - 143r \neq 84$, and there is no solution for the original equation. ∎

(c) We need to investigate the remainders of squares modulo 5.
CASE I. $x \equiv 1 \mod 5$: $x^2 \equiv 1 \mod 5$
CASE II. $x \equiv 2 \mod 5$: $x^2 \equiv 4 \mod 5$
CASE III. $x \equiv 3 \mod 5$: $x^2 \equiv 1 \mod 5$
CASE IV. $x \equiv 4 \mod 5$: $x^2 \equiv 1 \mod 5$
CASE V. $x \equiv 5 \mod 5$: $x^2 \equiv 0 \mod 5$
We can see that all squares are congruent to 0, 1, 4 modulo 5, but not 2 modulo 5. Therefore, there is no integer solution for this congruence equation. ∎

(d) We need to investigate the remainders of different cases modulo 5:
CASE I. $x \equiv 1 \mod 5$: $x^2 + x + 1 \equiv 3 \mod 5$
CASE II. $x \equiv 2 \mod 5$: $x^2 + x + 1 \equiv 2 \mod 5$
CASE III. $x \equiv 3 \mod 5$: $x^2 + x + 1 \equiv 3 \mod 5$
CASE IV. $x \equiv 4 \mod 5$: $x^2 + x + 1 \equiv 1 \mod 5$
CASE V. $x \equiv 5 \mod 5$: $x^2 + x + 1 \equiv 1 \mod 5$
We can see that all $x^2 + x + 1$ are congruent to 1, 2, 3 modulo 5, but not 0 modulo 5. Therefore, there is no integer solution for this congruence equation. ■

(e) We need to investigate the remainders of different cases modulo 7:
CASE I. $x \equiv 1 \mod 7$: $x^2 + x + 1 \equiv 3 \mod 7$
CASE II. $x \equiv 2 \mod 7$: $x^2 + x + 1 \equiv 0 \mod 7$
There is no need to explore more cases since we already hit a solution where $x^2 + x + 1 \equiv 0 \mod 7$. $x \equiv 2 \mod 7$ is a solution for this equation, say, x = 2. ■

Problem 4
(a) Prove the rule of 9: an integer is divisible by 9 if and only if the sum of its digits is divisible by 9.
(b) Prove the rule of 11 stated in Example 13.6. Use this rule to decide in your head whether the number 82918073579 is divisible by 11.

(a) For any integer $a_1 a_2 a_3 ... a_n$ such that each $0 \leq a_n \leq 9, a_n \in \mathbb{Z}$, for some $n \in \mathbb{Z}$, is a digit of the integer. We can express the integer as $a_1(10^{n-1}) + a_2(10^{n-2}) + ... + a_n(10^0)$. We have:

$$10^0 \equiv 1 \mod 9$$
$$10^1 \equiv 1 \mod 9$$
$$10^2 \equiv 1 \mod 9$$

By having the above congruence, we know that all powers of 10 are congruent to 1 mod 9. The integer can now be written as congruent to $a_1 + a_2 + ... + a_n \mod 9$. Therefore, if we have all the digits added up to be divisible by 9, then the original integer will also be divisible by 9. ■

(b) For any integer $a_1 a_2 a_3 ... a_n$ such that each $0 \leq a_n \leq 9, a_n \in \mathbb{Z}$, for some $n \in \mathbb{Z}$, is a digit of the integer. We can express the integer as $a_1(10^{n-1}) + a_2(10^{n-2}) + ... + a_n(10^0)$. We have:

$$10^0 \equiv 1 \mod 11$$
$$10^1 \equiv -1 \mod 11$$
$$10^2 \equiv 1 \mod 11$$
$$10^3 \equiv -1 \mod 11$$

By having the above congruence, we know that all powers of 10 are congruent to 1 or -1 mod 11, 1 for even powers and -1 for odd powers. The integer can now be written as congruent to $a_n - a_{n-1} + an - 2... + (-1)^{n-1}a_1 \mod 11$. Therefore, we start from the adding right most digit of the integer, subtracting the second right most, adding the third right most... until the left most digit. If the number we get is divisible by 11, then the integer is divisible by 11. For integer 82918073579, we have 9-7+5-3+7-0+8-1+9-2+8 = 33. Therefore, this number is divisible by 11. ■

Problem 5
(a)Use the fact that 7 divides 1001 to find your own rule of 7. Use your rule to work out the remainder when 6005004003002001 is divided by 7.
(b) 13 also divides 1001. Use this to get a rule of 13 and find the remainder when 6005004003002001 is divided by 13.
(c) Use the observation that 27 $\times$ 37 = 999 to work out a rule of 37, and find the remainder when 6005004003002001 is divided by 37.

(a) Since we have $1001 \equiv 0 \mod 7$, we have $1000 \equiv -1 \mod 7$. Therefore, $1000^2 \equiv 1$ mod 7. We can then split the given integer into groups from the right most, each group of size three. Then we can add then subtract alternate respectively from the right most group. For integer 6005004003002001 we have 1 - 2 + 3 - 4 + 5 - 6 = -3, so the remainder of this integer divided by 7 is 4. ■

(b) Since we have $1001 \equiv 0 \mod 13$, we have $1000 \equiv -1 \mod 13$. Therefore, $1000^2 \equiv 1$ mod 13. We can then split the given integer into groups from the right most, each group of size three. Then we can add then subtract alternate respectively from the right most group. For integer 6005004003002001 we have 1 - 2 + 3 - 4 + 5 - 6 = -3, so the remainder of this integer divided by 13 is 10. ■

(c) Since we have $999 \equiv 0 \mod 37$, we have $1000 \equiv 1 \mod 37$. Therefore, $1000^2 \equiv 1 \mod 37$. We can then split the given integer into groups from the right most, each group of size three. Then we can then add from the right most group. For integer 6005004003002001 we have 1 + 2 + 3 + 4 + 5 + 6 = 21, so the remainder of this integer divided by 37 is 21. ■

Problem 7 Show that every square is congruent to 0, 1 or -1 modulo 5, and is congruent to 0, 1 or 4 modulo 8. Suppose n is a positive integer such that both 2n + 1 and 3n + 1 are squares. Prove that n is divisible by 40. Find a value of n such that 2n+1 and 3n+1 are squares. Can you find another value? (Calculators allowed!)

To investigate the congruence of squares modulo 5, we can examine by cases. Let k be the base of the square, for some k $\in \mathbb{Z}$:
CASE I. $k \equiv 1 \mod 5$: $k^2 \equiv 1 \mod 5$
CASE II. $k \equiv 2 \mod 5$: $k^2 \equiv -1 \mod 5$

CASE III. $k \equiv 3 \mod 5$: $k^2 \equiv 1 \mod 5$
CASE IV. $k \equiv 4 \mod 5$: $k^2 \equiv 1 \mod 5$
CASE V. $k \equiv 5 \mod 5$: $k^2 \equiv 0 \mod 5$

Then to investigate the congruence of squares modulo 8, we can examine by cases. Let k again be the base of the square, for some k $\in \mathbb{Z}$:
CASE I. $k \equiv 1 \mod 8$: $k^2 \equiv 1 \mod 8$
CASE II. $k \equiv 2 \mod 8$: $k^2 \equiv 4 \mod 8$
CASE III. $k \equiv 3 \mod 8$: $k^2 \equiv 1 \mod 8$
CASE IV. $k \equiv 4 \mod 8$: $k^2 \equiv 0 \mod 8$
CASE V. $k \equiv 5 \mod 8$: $k^2 \equiv 1 \mod 8$
CASE III. $k \equiv 6 \mod 8$: $k^2 \equiv 4 \mod 8$
CASE IV. $k \equiv 7 \mod 8$: $k^2 \equiv 1 \mod 8$
CASE V. $k \equiv 8 \mod 8$: $k^2 \equiv 0 \mod 8$

Then we want to investigate the product of 2n + 1 and 3n + 1 to see if it is divisible by 5. Since both are squares, we can write $2n + 1 \equiv 0, 1, -1 \mod 5$ and $3n + 1 \equiv 0, 1, -1 \mod 5$. Then we can write $(2n + 1) + (3n + 1) \equiv 2 \mod 5$, which gives that $2n + 1 \mod 5 = 3n + 1 \mod 5$.
Let x = $2n + 1 \mod 5$, and y = $3n + 1 \mod 5$,
$(2n + 1) + (3n + 1) = 5n + 2 \equiv 2 \mod 5 \equiv x + y \mod 5$
$5n + 2 - 2(2n + 1) \equiv x + y - 2x \mod 5$
Therefore we have $n \equiv y - x \mod 5$. Since x = y, we have n divisible by 5.

Then we want to investigate the product of 2n + 1 and 3n + 1 to see if it is divisible by 8. Since both are squares, we can write $2n + 1 \equiv 0, 1, 4 \mod 5$ and $3n + 1 \equiv 0, 1, 4 \mod 5$. Then we can write $(2n + 1) + 2(3n + 1) \equiv 3 \mod 8$, which gives that $2n + 1 \mod 8 = 3n + 1 \mod 8$.
Let x = $2n + 1 \mod 8$, and y = $3n + 1 \mod 8$,
$(2n + 1) + 2(3n + 1) = 8n + 3 \equiv 3 \mod 8 \equiv x + 2y \mod 8$
$8n + 3 - 2(2n + 1) - (3n + 1) \equiv x + 2y - 2x - y \mod 8$
Therefore we have $n \equiv y - x \mod 8$. Since x = y, we have n divisible by 8. Therefore, n is divisible by 40. Two of the values that works for n are 40 and 3960. ∎