MATH10101, optional exercises on linear and non-linear congruences. Will not be discussed in the supervisions — SOLUTIONS

Opt7. Alice comes home from school and tells her baby brother Bob: "Our mum's age, expressed in *months*, is congruent to 20 modulo 17 and is congruent to 17 modulo 20." What is most likely the age of their mother?

Opt7 - solution. The possible values of the mother's age are solutions x of the following two simultaneous congruences:

$$x \equiv 20 \bmod 17 \qquad \text{and} \qquad x \equiv 17 \bmod 20.$$

Since 17 and 20 are coprime and $17 \times 20 = 340$, the Chinese Remainder Theorem gives the general solution as

$$x \equiv x_0 \bmod 340$$

where x_0 is a particular solution. We can find x_0 by inspection if we notice that $17 + 20$ is congruent to 20 mod 17 and is congruent to 17 mod 20. Hence $x_0 = 17 + 20 = 37$ is a particular solution.

However, in the context of the question, a mother cannot be 37 *months* old, hence we consider the next solution, $37 + 340 = 377$. The age of 377 months $= 31$ year 5 months is the most likely answer.

Opt8. a) By using the method of *successive squaring*, find the remainders of the following numbers on dividing by 41: (i) 5^4, (ii) 5^{16}, (iii) 5^{64}.

In particular, check that 5^4 and 5^{64} leave the same remainder when divided by 41.

b) Use the answers to part (a) to find an $n \in \mathbb{N}$ such that $5^n \equiv 1 \mod 41$.

c) Use part (b) to solve $25x \equiv 7 \mod 41$.

Opt8 - solution. a) Squaring,

$$\begin{aligned} 5^2 = 25 &\equiv -16 \bmod 41, \\ \text{i) } 5^4 \equiv (16)^2 &\equiv \mathbf{10} \mod 41, \\ 5^8 \equiv 10^2 &\equiv 18 \mod 41, \\ \text{ii) } 5^{16} \equiv 18^2 &\equiv \mathbf{37} \equiv -4 \mod 41, \\ 5^{32} \equiv 4^2 &\equiv 16 \mod 41, \\ \text{iii) } 5^{64} = 16^2 &\equiv \mathbf{10} \mod 41. \end{aligned}$$

b) From this list we note that $5^{64} \equiv 10 \equiv 5^4 \mod 41$, and so on dividing through by 5^4 (coprime to 41) gives $5^{60} \equiv 1 \mod 41$.

Alternatively, you might note from the list that

$$5^{16} \times 5^4 \equiv -4 \times 10 \equiv 1 \mod 41.$$

So $5^{20} \equiv 1 \bmod 41$.

c) Multiply both sides of $5^2 x \equiv 7 \mod 41$ by 5^{58} to get $5^{60} x \equiv 7 \times 5^{58}$ i.e. $x \equiv 7 \times 5^{58} \mod 41$. Here

$$\begin{aligned} 7 \times 5^{58} &= 7 \times 5^{32} \times 5^{16} \times 5^8 \times 5^2 \\ &\equiv 7 \times 16 \times (-4) \times 18 \times (-16) \mod 41 \\ &\equiv 38 \mod 41. \end{aligned}$$

Opt9. What are the remainders when 3^{40} and 40^{35} are divided by 11? Prove that $3^{40} + 40^{35}$ is divisible by 11.

Opt9 - solution. Squaring,

$$\begin{aligned} 3^2 &= 9 \equiv -2 \bmod 11, \\ 3^4 &\equiv (-2)^2 \equiv 4 \bmod 11, \\ 3^8 &\equiv 4^2 \equiv 5 \bmod 11, \\ 3^{16} &\equiv 5^2 \equiv 3 \bmod 11, \\ 3^{32} &\equiv 9 \bmod 11. \end{aligned}$$

So $3^{40} = 3^{32} 3^8 \equiv 9 \times 5 \equiv 1 \bmod 11$.

Note that $40^{35} \equiv 7^{35} \equiv (-4)^{35} \equiv -(4^{35}) \bmod 11$. Also, from this list we see that $4 \equiv 3^4 \bmod 11$ so we can read off the first few lines below from the list above.

$$\begin{aligned} 4^2 &\equiv 3^8 \equiv 5 \bmod 11, \\ 4^4 &\equiv 3^{16} \equiv 3 \bmod 11, \\ 4^8 &\equiv 3^{32} \equiv 9 \equiv -2 \bmod 11, \\ 4^{16} &\equiv (-2)^2 \equiv 4 \bmod 11, \\ 4^{32} &\equiv 4^2 \equiv 5 \bmod 11. \end{aligned}$$

Thus $40^{35} \equiv -(4^{32} \times 4^2 \times 4) \equiv -(5 \times 5 \times 4) \equiv 10 \bmod 11$.

Finally, $3^{40} + 40^{35} \equiv 1 + 10 \equiv 0 \bmod 11$.

Opt10. Show that $7x^4 + 2y^3 = 3$ has no integer solutions.

Opt10 - solution. Work modulo 7. Assume $(x, y) \in \mathbb{Z}^2$ is a solution. Then $0x^4 + 2y^3 \equiv 3 \mod 7$. Multiply through by 4; it follows that $8y^3 \equiv 12 \mod 7$, equivalently $y^3 \equiv 5 \mod 7$. Yet cubes modulo 7 only leave remainders 0, 1 or 6: indeed, $0^3 \equiv 0$, $1^3 \equiv 1$, $2^3 \equiv 1$, $3^3 \equiv 6$, $4^3 \equiv -3^3 \equiv 1$, $5^3 \equiv -2^3 \equiv 6$, $6^3 \equiv -1^3 \equiv 6 \mod 7$. This is a contradiction which shows that integer solutions do not exist.

Opt11. Show that $2x^3 + 27y^4 = 21$ has no integer solutions.

Opt11 - solution. Trying small moduli, one observes that considering this equation as a congruence modulo 2, 3, 4, 5, 7 does not lead to a contradiction. Generally in problems of this type one uses a modulus which is either a prime number or a power of a prime number (we do not justify this approach in the course and leave it as an empirical rule) Hence we try modulus 9.

Assume that $(x, y) \in \mathbb{Z}^2$ is a solution. Considering the equation modulo 9, we obtain

$$2x^3 \equiv 3 \mod 9.$$

We can multiply through by 5, which is the inverse of 2 mod 9, to obtain an equivalent congruence

$$10x^3 \equiv 15 \mod 9 \iff x^3 \equiv 6 \mod 9.$$

From here, one can proceed in two ways.

Way 1. Consider all possible remainders left by cubes when divided by 9 and observe that 6 is not among them:

$a \mod 9$	0	1	2	3	4	5	6	7	8
$a^3 \mod 9$	0	1	8	0	1	8	0	1	8

Way 2. Assume for contradiction that $x^3 \equiv 6 \mod 9$, so that $x^3 = 9k + 6$ for some $k \in \mathbb{Z}$. By considering remainders modulo 3 we observe that $x^3 \equiv x \mod 3$. Since $x^3 = 3(3k + 2)$ is divisible by 3, we conclude that x is also divisible by 3, $x = 3m$ with $m \in \mathbb{Z}$. But then $x^3 = 27m^3 = 9(3m^3)$ is divisible by 9 and is not congruent to 6 modulo 9, a contradiction.

Either way, we arrive at a contradiction which shows that the assumption that a solution $(x, y) \in \mathbb{Z}^2$ exists was false.

Opt12. Show that $7x^5 + 3y^4 = 2$ has no integer solutions.

Opt12 - solution. Work modulo 7. Assuming that a solution $(x, y) \in \mathbb{Z}^2$ exists, we arrive at the congruence $3y^4 \equiv 2 \mod 7$ which is multiplied through by 5, the inverse of 3 mdo 7, to give an equivalent congruence $15y^4 \equiv 10 \mod 7$, same as $y^4 \equiv 3 \mod 7$. Now one can observe that a **square** cannot be congruent to 3 modulo 7:

$a \mod 7$	0	1	2	3	4	5	6
$a^2 \mod 7$	0	1	4	2	2	4	1

Hence $y^4 = (y^2)^2$ is not congruent to 3 mod 7, a contradiction.

Opt13. Show that 7 never divides $n^4 + n^2 + 2$ for $n \in \mathbb{Z}$.

Opt13 - solution. To show that 7 never divides n^4+n^2+2 for $n \in \mathbb{Z}$ we need to show that there are no solutions of $n^4+n^2+2 \equiv 0 \mod 7$. For this we can use the table:

$n \mod 7$	$n^2 \mod 7$	$n^4=(n^2)^2 \mod 7$	$n^4+n^2+2 \mod 7$
0	0	0	2
1	1	1	4
2	4	2	1
3	2	4	1
4	2	4	1
5	4	2	1
6	1	1	4

and observe that residue 0 does not occur in the last column. Hence, whatever remainder is left by n when divided by 7, n^4+n^2+2 won't leave remainder 0.

Remark A different, ad-hoc way to attack this question is to write

$$a^4+a^2+2 \equiv a^4+a^2+2+7(-a^2+1) = a^4-6a^2+9 = (a^2-3)^2$$

and to observe that, as a^2-3 is never divisible by 7 (from the above), $(a^2-3)^2$ is never divisible by 7.

Opt14. (i) Show that n^2-n+41 is never divisible by 2, 3, 4, 5, 6, 7, 8, 9 nor by 10.

(ii) If you have time, show that n^2-n+41 is never divisible by any integer from $\{10,11,\ldots,40\}$. (*Warning*: (ii) can be done by "brute force" which is time-consuming. A conceptual solution which shows that (i) implies (ii) is beyond the scope of this course.)

Opt14 - solution. Looking at residues mod 2, mod 3, mod 5 and mod 7, we conclude that n^2-n+41 is never congruent to 0 modulo these numbers. (Look at residues of squares in these moduli — all were obtained above.) Now, if a number is not divisible by 2, then it is not divisible by any even number, including $4,6,8$; if it is not divisible by 3, then it is not divisible by 9.

In fact, Euler noticed that n^2-n+41 is a *prime number* (greater than 40) for all $n=0,1,2,\ldots,40$. But this brings us to the next chapter of the course.