Exercises 1: Modular Arithmetic

Exercises

Calculators aren't needed for these questions - you can always use them to check, but you should focus on getting to grips with modular arithmetic as a way of thinking before reaching for the technology. Try to avoid doing arithmetic with numbers bigger than 100 - see if you can reduce them first.

1. For each of the pairs of integers a and b below, find integers q and r such that $a = qb + r$.
   (a) $a = 100$, $b = 57$,
   (b) $a = 407$, $b = 10$,
   (c) $a = 10$, $b = 407$.
2. Working in terms of the modulus n for each part below, find three numbers which are equivalent when considered modulo n.
   (a) modulo 2,
   (b) modulo 5,
   (c) modulo 10,
   (d) modulo 12,
   (e) modulo 17.
3. What is 123 (mod 17)?
4. Is $528 \equiv 9 \pmod{37}$? Justify your answer by showing your calculations.
5. What is $(823 \times 456) \pmod{97}$?
6. Use modular arithmetic to do the following calculations - you can always check your answer on a calendar after.
   (a) What day of the week will 31st December fall on this year?
   (b) What day of the week will 14th February fall on next year?
7. (a) Calculate 100 modulo 24.
   (b) Calculate 1000 modulo 24.

(c) What time of day will it be 3000 hours from now?

8. Find the value of $7^{137} \pmod{11}$.

9. Find the value of $7^{137} \pmod{8}$. (Hint: Don't just jump into this. If you think about this in the right way, it ends up being very easy.)

10. Find the last 2 digits of 3^{124}.

11. (Challenge)

    (a) For each $a \in \{1, 2, 3, \ldots, p-1\}$, calculate $a^p \pmod{p}$ for each value of p given below:

    i. $p = 2$,
    ii. $p = 3$,
    iii. $p = 4$,
    iv. $p = 5$,
    v. $p = 6$,
    vi. $p = 7$,
    vii. $p = 8$,
    viii. $p = 9$.

    You may find the table below useful for recording your calculations.

$a \setminus p$	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
1								
2	-							
3	-	-						
4	-	-	-					
5	-	-	-	-				
6	-	-	-	-	-			
7	-	-	-	-	-	-		
8	-	-	-	-	-	-	-	

    (b) For which values of p does $a^p \pmod{p}$ always equal a? Do these values of p share any special property?

    (c) Once you have tried the questions above, look up Fermat's Little Theorem and compare it to what you have discovered.

Solutions

1. For each of the pairs of integers a and b below, find integers q and r such that $a = qb + r$.

    (a) $a = 100$, $b = 57$: $100 = 1 \times 57 + 43$, so $q = 1$, $r = 43$;

    (b) $a = 407$, $b = 10$: $407 = 40 \times 10 + 7$, so $q = 40$, $r = 7$;

    (c) $a = 10$, $b = 407$: $10 = 0 \times 407 + 10$, so $q = 0$, $r = 10$.

2. Working in terms of the modulus n for each part below, find three numbers which are equivalent when considered modulo n.

(a) modulo 2: any three even numbers, or any three odd numbers,

(b) modulo 5: e.g., $-25 = 0 = 5 \pmod 5$, or $23 = 8 = -7 \pmod 5$,

(c) modulo 10 e.g., $-25 = 5 = 125 \pmod{10}$, or $23 = 13 = -7 \pmod{10}$,

(d) modulo 12 e.g., $-25 = -1 = 11 \pmod{12}$, or $-4 = 8 = 20 \pmod{12}$,

(e) modulo 17 e.g., $-25 = 9 = 43 \pmod{17}$, or $23 = 6 = -11 \pmod{17}$.

3. What is 123 (mod 17)?

   Perform the division $123 \div 17$, which gives a quotient of 7 and a remainder of 4. Therefore,
   $$123 = 4 \pmod{17}.$$

4. Is $528 = 9 \pmod{37}$? Justify your answer by showing your calculations.

   If 528 and 9 were equivalent modulo 37, then their difference would be a multiple of 7. However, $528 - 9 = 519$ is not a multiple of 37, so they are not equivalent.

   Alternatively, perform the division $528 \div 37$, which gives a quotient of 14 and a remainder of 10. Since
   $$528 \pmod{37} = 10 \neq 9,$$
   the statement $528 = 9 \pmod{37}$ is false.

5. What is $(823 \times 456) \pmod{97}$?

   First, compute 823 (mod 97) and 456 (mod 97):
   $$823 = 47 \pmod{97}, 456 = 68 \pmod{97}.$$
   Now, calculate $(47 \times 68) \pmod{97}$:
   $$47 \times 68 = 3196.$$
   Therefore,
   $$(823 \times 456) = 3196 = 92 \pmod{97}.$$

6. (a) Work out the number of days left until 31st December. Then reduce this number modulo 7. Check against a calendar.

   (b) Do the same as above but for 14th February.

7. (a) $100 = 4 \pmod{24}$

   (b) Calculate 1000 modulo 24.

   (c) What time of day will it be 3000 hours from now?

$a \setminus p$	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
1	1	1	1	1	1	1	1	1
2	-	2	0	2	4	2	0	8
3	-	-	1	3	3	3	1	0
4	-	-	-	4	4	4	0	1
5	-	-	-	-	1	5	1	8
6	-	-	-	-	-	6	0	0
7	-	-	-	-	-	-	1	1
8	-	-	-	-	-	-	-	8

8. First break up the power into powers of 2: $7^{137} = 7^{128} \times 7^8 \times 7^1$. Then build it up in stages:

$$\begin{aligned}
7^1 &= 7 \pmod{11}, \\
7^2 &= 49 = 5 \pmod{11}, \\
7^4 &= (7^2)^2 = 5^2 = 25 = 3 \pmod{11}, \\
7^8 &= 3^2 = 9 \pmod{11}, \\
7^{16} &= 9^2 = 81 = 4 \pmod{11}, \\
7^{32} &= 4^2 = 16 = 5 \pmod{11}, \\
7^{64} &= 5^2 = 3 \pmod{11}, \\
7^{128} &= 3^2 = 9 \pmod{11}.
\end{aligned}$$

   Then

$$7^{137} = 7^{128} \times 7^8 \times 7^1 = 9 \times 9 \times 7 = 81 \times 7 = 4 \times 7 = 28 = 6 \pmod{11}.$$

9. If you look at this the right way, it's very easy. Remember that we can use negative integers as well as positive integers. Since we are working modulo 8, then we have that

$$7 = -1 \pmod{8}.$$

   From this we can then conclude that

$$7^{137} = (-1)^{137} = -1 = 7 \pmod{8}.$$

10. To find this, work out $3^{124} \pmod{100}$.

11. (Challenge)

    (a) All of the values have been calculated in the table below. The values of a are listed in the column on the left, while the values of p are listed in the top row.

(b) The values where $a^p = a \pmod{p}$ occurs are when $p \in \{2, 3, 5, 7\}$. At first glance these are all odd numbers, but the column for 9 does not meet this requirement. So we might conjecture that this only works for *prime* numbers.

(c) If you have already clicked through the link, you may have noticed that we have been collecting evidence towards Fermat's Little Theorem, which is explained in much more detail in the article.