Modular Numbers

Two integers, m and n, are said to be congruent modulo d if they have the same remainder when divided by d. This is written $m \equiv n \mod d$.

Consider integers mod 4. Regardless of which integer you pick, that integer must be congruent to 0, 1, 2, or 3 modulo 4 because those are the only possibilities for remainders after dividing by 4. So, for example, we say that all of the numbers in $..., -3, 1, 5, 9, ...$ belong to the same congruence class mod 4. It would be nice to pick just one representative of that congruence class, and nicest of all to make that representative the smallest non-negative member of the equivalence class. So, we would say that the *canonical complete residue system* modulo 4 is 0, 1, 2, 3 or $\mathbb{Z}_4$.

Henceforth, $\mathbb{Z}_n$ will refer to the set of integers from 0 to $n-1$, which represents all of the congruence classes modulo n.

1. Consider the integers modulo 6.

   (a) Construct a table for addition modulo 6.

+	**0**	**1**	**2**	**3**	**4**	**5**
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

   (b) Construct a table for subtraction modulo 6.

−	**0**	**1**	**2**	**3**	**4**	**5**
0	0	1	2	3	4	5
1	5	0	1	2	3	4
2	4	5	0	1	2	3
3	3	4	5	0	1	2
4	2	3	4	5	0	1
5	1	2	3	4	5	0

   (c) Construct a table for multiplication modulo 6.

×	**0**	**1**	**2**	**3**	**4**	**5**
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

2. Which decimal digits occur as the final digit of a fourth power of an integer?
   $0^4 = 0, 1^4 = 1, 2^4 = 16, 3^4 = 81, 4^4 = 256, 5^4 = 625, 6^4 = 1296, 7^4 = 2401, 8^4 = 4096, 9^4 = 6561$
   $0, 1, 5,$ and 6 can occur as the final digit of the fourth power of an integer.

3. Compute the number k in $\mathbb{Z}_{12}$ such that $37^{453} \equiv k \mod 12$. Explain how you did it.
   $(37^{453} = 37 \times 37 \times 37 \times ...)$ and $((A \times B) \bmod C = (A \bmod C \times B \bmod C) \bmod C)$. Therefore, $37^{453} \bmod 12 = (37 \bmod 12)^{453} \bmod 12 = 1^{453} \bmod 12 = 1$. So, $37^{453} \equiv 1 \mod 12$.

4. Compute the number k in $\mathbb{Z}_7$ such that $2^{50} \equiv k \mod 7$ without using a computer.
   $2^{50} = 2^{48} \times 2^2 = (2^3)^{16} \times 2^2$. Therefore, $2^{50} \bmod 7 = ((8^{16} \bmod 7) \times 4) \bmod 7 = 1^{16} \times 4 \bmod 7 = 4 \bmod 7$. So, $2^{50} \equiv 4 \mod 7$.

5. Compute the number k in $\mathbb{Z}_7$ such that $39^{453} \equiv k \mod 12$ without using a computer.
   $39^{453} \equiv 3^{453} \equiv (3^3)^{151} \equiv 27^{151} \equiv 3^{151} \equiv (3^3)^{50} \times 3 \equiv 27^{50} \times 3 \equiv 3^{50} \times 3 \equiv 3^{51} \equiv 27^{27} \equiv 3^{27} \equiv 27^9 \equiv 3^9 \equiv 27^3 \equiv 3^3 \equiv 27 \equiv 3$. So, $39^{453} \equiv 3 \mod 12$.

6. Find the numbers in $\mathbb{Z}_{47}$ that are congruent to each of the following without using a computer:

(a) 2^{32}
$2^{32} = (2^8)^4 = 256^4 \equiv 21^4 = 441^2 \equiv 18^2 = 324 \equiv 42 \mod 47$. So, $2^{32} \equiv 42 \mod 47$.

(b) 2^{47}
$2^{47} = 2^{32} \times 2^{15} \equiv 42 \times 2^{15} = 21 \times 2^{16} = 21 \times (2^8)^2 = 21 \times 256^2 \equiv 21 \times 21^2 = 21 \times 441 \equiv 21 \times 18 = 378 \equiv 2 \mod 47$. So, $2^{47} \equiv 2 \mod 47$.

(c) 2^{200}
$2^{200} = (2^{47})^4 \times 2^{12} \equiv 2^4 \times 2^{12} = 2^{16} = 256^2 \equiv 21^2 = 441 \equiv 18 \mod 47$. So, $2^{200} \equiv 18 \mod 47$

7. Find the canonical residue congruent to each of the following without using a computer.

(a) $3^{10} \mod 11$
$3^{10} = (3^3)^3 \times 3 = 27^3 \times 3 \equiv 5^3 \times 3 = 25 \times 5 \times 3 = 25 \times 15 \equiv 3 \times 4 = 12 \equiv 1 \mod 11$.

(b) $2^{12} \mod 13$
$2^{12} = (2^4)^3 = 16^3 \equiv 3^3 = 27 \equiv 1 \mod 13$.

(c) $5^{16} \mod 17$
$5^{16} = (5^2)^8 = 25^8 \equiv 8^8 = (2^3)^8 = 2^{24} = (2^4)^6 = 16^6 \equiv (-1)^6 = 1 \mod 17$.

(d) $3^{22} \mod 23$
$3^{22} = (3^3)^7 \times 3 = 27^7 \times 3 \equiv 4^7 \times 3 = (4^3)^2 \times 4 \times 3 = 64^2 \times 12 \equiv (-5)^2 \times 12 = 25 \times 12 \equiv 2 \times 12 = 24 \equiv 1 \mod 23$.

(e) Make a conjecture based on the congruences in this problem.
For $n, x \in \mathbb{Z}$, $x^{n+1} \equiv 1 \mod n$.