Cryptology Packet Pt2

ID: 1747

January 2023

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	5	4	3	2	1
1	1	0	5	4	3	2
2	2	1	0	5	4	3
3	3	2	1	0	5	4
4	4	3	2	1	0	5
5	5	4	3	2	1	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?

   $0, 1, 5, 6$. If a number is raised to the power of 4, it will be divisible by 10 except for the final digit. To check the final digit of a fourth power of an integer, we can check the 10 cases for the final digit $(0-9)$. Finally, to find the possible options, we take mod 10 of each final digit to the power of 4.

Proof:
$0^4 \bmod 10 = 0$
$1^4 \bmod 10 = 1$
$2^4 \bmod 10 = 6$
$3^4 \bmod 10 = 1$
$4^4 \bmod 10 = 6$
$5^4 \bmod 10 = 5$
$6^4 \bmod 10 = 0$
$7^4 \bmod 10 = 1$
$8^4 \bmod 10 = 6$
$9^4 \bmod 10 = 1$

3. Compute the number k in $\mathbb{Z}_{12}$ such that $37^{453} \equiv \bmod 12$. Explain.

   We need to find a number k that is from $0-11$. We can use a multiple of 12 to find what k is. For example, we know that $37 \equiv 1 \bmod 36$. So, $37^{453} \equiv 1^{453} \bmod 36$ will also be true. Therefore, $37^{453} \equiv 1 \bmod 12$ and $k = 1$.

4. Compute the number k in $\mathbb{Z}_7$ such that $2^{50} \equiv \bmod 7$ without using a computer.

   We need to find a number k that is from $0-6$. There is a pattern that repeats that can be seen as $2^0 \equiv 1 \bmod 7$, $2^1 \equiv 2 \bmod 7$, $2^2 \equiv 4 \bmod 7$, $2^3 \equiv 1 \bmod 7$. Since 50 is equivalent to $3*16+2$, $2^{50} = 2^{3*16+2} = 2^{3*16} * 2^2 = (1)^{16} * 4 = 4$. Therefore, $k = 4$.

5. Compute the number k in $\mathbb{Z}_{12}$ such that $39^{453} \equiv \bmod 12$ without using a computer.

   We need to find a number k that is from $0-11$. There is a pattern that repeats that can be seen as $3^1 \equiv 3 \bmod 12$, $3^2 \equiv 9 \bmod 12$, $3^3 \equiv 3 \bmod 12$, $3^4 \equiv 9 \bmod 12$.

   $3^{453} \equiv k \bmod 12$
   $k \equiv 3^{453} \bmod 12$
   $k \equiv 3^{(3*151)} \bmod 12$
   $k \equiv 3^{(3)(151)} \bmod 12$
   $k \equiv 3^{151} \bmod 12$
   $k \equiv 3^{3*50+1} \bmod 12$
   $k \equiv 3^{3(50)} * 3 \bmod 12$
   $k \equiv 3^{(51)} \bmod 12$

$k \equiv 3^{(17*3)} \bmod 12$
$k \equiv 3^{(17)} \bmod 12$
$k \equiv 3^{3*5+2} \bmod 12$
$k \equiv (3^3)^5 * 3^2 \bmod 12$
$k \equiv (3^7) \bmod 12$
$k \equiv (3^{3*2+1}) \bmod 12$
$k \equiv (3^3)^2 * 3^1 \bmod 12$
$k \equiv (3^2 * 3) \bmod 12$
$k \equiv (3^3) \bmod 12$
$k \equiv (3) \bmod 12$
$3^{453} \equiv 3 \bmod 12$

Instead of doing all the work above, since 453 is odd, it will follow the odd pattern, $3^1 \equiv 3 \bmod 12$, $3^3 \equiv 3 \bmod 12$, and so on so that $k = 3$

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

a. 2^{32}

$2^{32} \equiv k \mod 47$
$k \equiv 2^{32} \mod 47$
$k \equiv 2^{16*2} \mod 47$
$k \equiv 256^4 \mod 47$
$k \equiv 21^4 \mod 47$
$k \equiv 21^4 \mod 47$
$k \equiv 3^4 * 7^4 \mod 47$
$k \equiv 81 * 7^4 \mod 47$
$k \equiv 34 * 49^2 \mod 47$
$k \equiv 34 * 2^2 \mod 47$
$k \equiv 34 * 4 \mod 47$
$k \equiv 136 \mod 47$
$2^{32} \equiv 42 \mod 47$

b. 2^{47}

From Fermat's little theorem, $a^p \equiv a \mod p$. Therefore, $2^{47} \equiv 2 \mod 47$

c. 2^{200}

$2^{200} \equiv k \mod 47$
$k \equiv 2^{200} \mod 47$
$k \equiv 2^{47*4} * 2^{12} \mod 47$
$k \equiv 2^4 * 2^{12} \mod 47$
$k \equiv 2^4 * 2^{4*3} \mod 47$
$k \equiv 16 * 16^3 \mod 47$

$k \equiv 16^4 \mod 47$
$k \equiv 256 * 256 \mod 47$
$k \equiv 21 * 21 \mod 47$
$k \equiv 49 * 9 \mod 47$
$k \equiv 2 * 9 \mod 47$
$k \equiv 18 \mod 47$
$2^{200} \equiv 18 \mod 47$

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

   a. $3^{10} \mod 11$

   $3^{10} \mod 11$
   $3^{11} * 3^{-1} \mod 11$
   $3 * (1/3) \mod 11$
   $1 \mod 11$
   1

   b. $2^{12} \mod 13$

   $2^{12} \mod 13$
   $2^{13} * 2^{-1} \mod 13$
   $2 * 2^{-1} \mod 13$
   $2 * (1/2) \mod 13$
   $1 \mod 13$
   1

   c. $5^{16} \mod 17$

   $5^{16} \mod 17$
   $5^{17} * 2^{-1} \mod 17$
   $5 * 5^{-1} \mod 13$
   $5 * (1/5) \mod 13$
   $1 \mod 13$
   1

   d. $3^{22} \mod 23$

   $3^{22} \mod 23$
   $3^{23} * 3^{-1} \mod 23$
   $3 * 3^{-1} \mod 23$
   $3 * (1/3) \mod 23$
   $1 \mod 23$
   1

e. Make a conjecture based on the congruences in this problem

For a number a in the canonical complete residue system modulo p, $a^{p-1} \equiv 1 \pmod{p}$