Integers mod $n$ and simplest ciphers.

Here is the Caesar cipher. We numerate the alphabet

| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |

Now we choose a key $0 \leq \kappa \leq 25$. Then we define a function $E : \mathbb{Z}/26 \to \mathbb{Z}/26$ as $E : \theta \mapsto (\theta + \kappa) \mod 26$.

Say, if $\kappa = 7$, we obtain the following encryption for our cipher:

| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g |

Thus we can encrypt the famous Caesar’s message: “I came, I saw, I conquered”:

| p | j | h | t | l | p | z | h | d | p | j | v | u | x | b | l | y | l | k |

The message now looks like “pjhtlpzhpjvuxbylk”. To decrypt the message, we should use the function $D : \theta \mapsto (\theta - \kappa) \mod 26$.

There is an obvious modification: let $\alpha$ be an integer $1 \leq \alpha \leq 25$ such that $\gcd(\alpha, 26) = 1$. Then new encryption function $E$ is given as $E : \theta \mapsto (\alpha\theta + \kappa) \mod 26$. The corresponding decryption function is given as $D(\theta) = \alpha^{-1}\theta - \alpha^{-1}\kappa$.

Example. Let $\kappa = 7$ and $\alpha = 15$, and $E(\theta) = 15\theta + 7$. Then we can find that $\alpha^{-1} = 7 \mod 26$. Then the decryption function is $D(\theta) = 7\theta - 7^2 = 7\theta - 49 = 7\theta + 3 \mod 26$.

Exercise. Encrypt and decrypt the message “I came, I saw, I conquered”.

Exponentiation mod $n$

We would like to compute $17^{2015} \mod 113$. Clearly a direct computation does not work here. We decompose 2015 into binaries:

$$2015 = 2^{10} + 2^9 + 2^8 + 2^7 + 2^6 + 2^4 + 2^3 + 2^2 + 2^1 + 2^0.$$ 

Then we compute:

<table>
<thead>
<tr>
<th>$17^0$</th>
<th>$17^1$</th>
<th>$17^2$</th>
<th>$17^3$</th>
<th>$17^4$</th>
<th>$17^5$</th>
<th>$17^6$</th>
<th>$17^7$</th>
<th>$17^8$</th>
<th>$17^9$</th>
<th>$17^{10}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>17</td>
<td>17</td>
<td>289</td>
<td>3,969</td>
<td>196</td>
<td>8,889</td>
<td>11,881</td>
<td>256</td>
<td>900</td>
<td>900</td>
<td>900</td>
</tr>
<tr>
<td>17</td>
<td>63</td>
<td>144</td>
<td>83</td>
<td>109</td>
<td>16</td>
<td>30</td>
<td>90</td>
<td>90</td>
<td>90</td>
<td>90</td>
</tr>
<tr>
<td>mod 113</td>
<td>mod 113</td>
<td>mod 113</td>
<td>mod 113</td>
<td>mod 113</td>
<td>mod 113</td>
<td>mod 113</td>
<td>mod 113</td>
<td>mod 113</td>
<td>mod 113</td>
<td>mod 113</td>
</tr>
<tr>
<td>17</td>
<td>63</td>
<td>54</td>
<td>78</td>
<td>33</td>
<td>94</td>
<td>94</td>
<td>108</td>
<td>108</td>
<td>108</td>
<td>108</td>
</tr>
</tbody>
</table>

We obtain: $17^{2015} = 20 \mod 113$.

Comment. Study Example 14.16 in section 14.3 how to compute $5^{143} \mod 222$.

Exercise. Compute last three digits of the power $2015^{2015}$. 

Powers of numbers mod $n$

First, we consider a simple example: $\mathbb{Z}/7$. We list the powers of non-zero elements in $\mathbb{Z}/7$:

- $1^2 = 1$
- $1^3 = 1$
- $1^4 = 1$
- $1^5 = 1$
- $1^6 = 1$
- $2^1 = 2$
- $2^2 = 4$
- $2^3 = 1$
- $2^4 = 2$
- $2^5 = 4$
- $2^6 = 1$
- $3^1 = 3$
- $3^2 = 2$
- $3^3 = 6$
- $3^4 = 4$
- $3^5 = 5$
- $3^6 = 1$
- $4^1 = 4$
- $4^2 = 2$
- $4^3 = 1$
- $4^4 = 4$
- $4^5 = 2$
- $4^6 = 1$
- $5^1 = 5$
- $5^2 = 4$
- $5^3 = 6$
- $5^4 = 2$
- $5^5 = 3$
- $5^6 = 1$
- $6^1 = 6$
- $6^2 = 1$
- $6^3 = 6$
- $6^4 = 1$
- $6^5 = 6$
- $6^6 = 1$

We notice an interesting pattern: $a^6 = 1 \mod 7$ for all $a \in \mathbb{Z}/7$, $a \neq 0$. The following is a remarkable general result:

**Theorem 1.** (Fermat’s Little Theorem) Let $p$ be a prime number. Then

$$a^{p-1} \equiv \begin{cases} 1 \mod p & \text{if } a \neq 0 \mod p \\ 0 \mod p & \text{if } a = 0 \mod p \end{cases}$$

**Proof.** If $a = 0 \mod p$, then any power $a^k$ is zero mod $p$. We consider the case when $a \neq 0 \mod p$. We consider the numbers

- $a$
- $2a$
- $3a$
- $\cdots$
- $(p-1)a$ mod $p$.

There are $(p-1)$ numbers here. We notice that they all are different. Indeed, let $i \cdot a = j \cdot a$ mod $p$, where $1 \leq i, j \leq p-1$. Then $(i-j)a = 0 \mod p$. Thus the product $(i-j)a$ is divisible by $p$. Since $a$ is not divisible by $p$, then $(i-j)$ is divisible by $p$. But $1 \leq i, j \leq p-1$, which means that the only option is that $i = j$, i.e., $i - j = 0$. Now the list of $p-1$ numbers

- $a$
- $2a$
- $3a$
- $\cdots$
- $(p-1)a$ mod $p$

up to the order coincides with the list $1, \ldots, (p-1)$. Then we have

$$a \cdot 2a \cdot 3a \cdots (p-1)a = 1 \cdot 2 \cdots (p-1) \mod p.$$

The right-hand side is equal to $a^{p-1}(p-1)!$. We obtain:

$$a^{p-1}(p-1)! = (p-1)! \mod p$$

Since $(p-1)! \neq 0 \mod p$, there exists an integer $q$ such that $(p-1)! \cdot q = 1 \mod p$. We multiply both sides of the equation $a^{p-1}(p-1)! = (p-1)!$ by $q$ to get

$$a^{p-1} = 1 \mod p.$$

This proves Theorem 1. \qed

The number $p = 15485863$ is prime. Thus $2015^{15485862} \equiv 1 \mod 15485863$. Give an estimate on how many digits does the number $2015^{15485862}$ have?