Summary on Lecture 13, April 27th, 2016

Integers mod n and simplest ciphers.

Here is the **Ceasar 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** $0 \le \kappa \le 25$. Then we define a function $E : \mathbf{Z}/26 \to \mathbf{Z}/26$ 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 enrypt the famous Ceaser's message: "I came, I saw, I conquered":

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

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

There is an obvious modification: let α be an integer $1 \le \alpha \le 25$ 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".

Powers of numbers mod n

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

$$\begin{array}{llllll}
1^2 = 1 & 1^2 = 1 & 1^3 = 1 & 1^4 = 1 & 1^5 = 1 & 1^6 = 1 \\
2^1 = 2 & 2^2 = 4 & 2^3 = 1 & 2^4 = 2 & 2^5 = 4 & 2^6 = 1 \\
3^1 = 3 & 3^2 = 2 & 3^3 = 6 & 3^4 = 4 & 3^5 = 5 & 3^6 = 1 \\
4^1 = 4 & 4^2 = 2 & 4^3 = 1 & 4^4 = 4 & 4^5 = 2 & 4^6 = 1 \\
5^1 = 5 & 5^2 = 4 & 5^3 = 6 & 5^4 = 2 & 5^5 = 3 & 5^6 = 1 \\
6^1 = 6 & 6^2 = 1 & 6^3 = 6 & 6^4 = 1 & 6^5 = 6 & 6^6 = 1
\end{array}$$

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

Theorem 1. (Fermat's Little Theorem) Let p be a prime number. Then

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

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

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

There are $(p-1)$ numbers here. We notice that they all are different. Indeed, let $i \cdot a = j \cdot a \mod p$, where $1 \le i, j \le p-1$. 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 $1 \le i, j \le p-1$, which means that the only option is that $i = j$, i.e., $i - j = 0$. Now the list of $p-1$ numbers

$$a, \quad 2a, \quad 3a, \quad \ldots, \quad (p-1)a \mod p$$

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. $\square$

Exercise. The number $p = 15485863$ is prime. Thus $2016^{15485862} \equiv 1 \mod 15485863$. Give an estimate on how many digits does the number $2016^{15485862}$ have?