Summary on Lecture 13, April 25th, 2016

Euler function. Recall that for a for given positive integer n, consider the set of numbers m such that $1 \le m < n$ and $\gcd(m,n) = 1$. Leonhard Euler defined the function:

$$\phi(n) = |\{\ m \mid 1 \le m < n,\ \text{and}\ \gcd(m,n) = 1\ \}|.$$

Here is the values of $\phi(n)$ for some n:

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$\phi(n)$	1	2	2	4	2	6	4	9	4	10	4	12	6	8	8	16

There is a simple formula to compute $\phi(n)$. Recall that for every integer n there exist primes $p_1, \dots, p_s$ and positive $e_1, \dots, e_s$ such that $n = p_1^{e_1} \cdots p_s^{e_s}$. Here is the formula:

$$\phi(n) = n \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right)$$

Theorem 3. Let $n \ge 2$. Then there are exactly $\phi(n)$ units in $\mathbf{Z}/n$.

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".

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:

1	$17^{2^0} = 17$	$\equiv 17$	mod 113	17	mod 113
1	$17^{2^1} = 17^2 = 289$	$\equiv 63$	mod 113	$17 \cdot 63 \equiv 54$	mod 113
1	$17^{2^2} = 63^2 = 3,969$	$\equiv 14$	mod 113	$54 \cdot 14 \equiv 78$	mod 113
1	$17^{2^3} = 14^2 = 196$	$\equiv 83$	mod 113	$78 \cdot 83 \equiv 33$	mod 113
1	$17^{2^4} = 83^2 = 6,889$	$\equiv 109$	mod 113	$33 \cdot 109 \equiv 94$	mod 113
0	$17^{2^5} = 109^2 = 11,881$	$\equiv 16$	mod 113	94	mod 113
1	$17^{2^6} = 16^2 = 256$	$\equiv 30$	mod 113	$94 \cdot 30 \equiv 108$	mod 113
1	$17^{2^7} = 30^2 = 900$	$\equiv 109$	mod 113	$108 \cdot 109 \equiv 20$	mod 113
1	$17^{2^8} = 109^2 = 11,881$	$\equiv 16$	mod 113	$20 \cdot 16 \equiv 94$	mod 113
1	$17^{2^9} = 16^2 = 256$	$\equiv 30$	mod 113	$94 \cdot 30 \equiv 108$	mod 113
1	$17^{2^{10}} = 30^2 = 900$	$\equiv 109$	mod 113	$108 \cdot 109 \equiv 20$	mod 113

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

Remark. We can easily find $17^{2016} = 17^{2015} \cdot 17 \equiv 20 \cdot 17 = 340 \equiv 1 \mod 113$.

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