Lecture 15.

A few words about groups.

Def-n. A *group* is a set G with a binary operation
$$*: G\times G \to G,$$
satisfying the following requirements:

- $(a*b)*c = a*(b*c)$ $\forall a,b,c\in G$ (associativity);
- there exists an *identity el-t* $e\in G$:
$$e*g = g*e = g \quad \forall g\in G;$$
- $\forall g\in G$ $\exists a\in G$: $a*g = g*a = e$ (*inverse* of g, denoted by g^{-1}).

Rmk. A group G is called *commutative (abelian)* if
$$a*b = b*a \quad \forall a,b\in G.$$

Examples.

(1) $(\mathbb{Z},+)$. Here $e=0$ and $a^{-1}=-a$.

(2) $(n\mathbb{Z},+)$, i.e. integers divisible by n.

(3) $(\mathbb{Z}_n^\times$, mult-n$)$ and $(\mathbb{Z}_n,+)$.

$\mathbb{Z}_n = \{0,1,2,\dots,n-1\}$ and $\mathbb{Z}_n^\times \subset \mathbb{Z}_n$ consists of el-ts invertible modulo n.

(4) $(GL_n(\mathbb{K}),*)$ - invertible matrices with coeff-nt in $\mathbb{K}$. (under mult-n)

$\mathbb{K}=\mathbb{C},\mathbb{R},\mathbb{Q},\dots$

Consider the set $C(\mathbb{R}) = \{$continuous f-ns $\mathbb{R} \to \mathbb{R}\}$.

Q.: do they form a group?

(a) Under addition (pointwise).

(b) Under multiplication (pointwise).

(c) Composition.

Answers.

(a) Yes, $e = f \equiv 0$, i.e. $f(x) = 0$ $\forall x \in \mathbb{R}$, the inverse of $g(x)$ is given by $-g(x)$.

(b) Here is an issue: the inverse of a f-n $f(x)$ must be $\frac{1}{f(x)}$, however, if $f(x_0) = 0$ at a point x_0, then $\frac{1}{f(x)}$ would fail to be continuous (even defined) at this point. We can take the subset $\text{Good} \subset C(\mathbb{R})$. Then $(\text{Good}, \text{mult-n})$ will be a group.

$\text{Good} = \{f \in C(\mathbb{R}) \mid f(x) \neq 0 \ \forall x \in \mathbb{R}\}$.

(c) Again, problem with inverses: many continuous f-ns do not pass the 'horizontal line test' (attain same value multiple times), hence, do not have an inverse. One can 'restrict attention' to the subset of invertible f-ns and get a group structure on it.

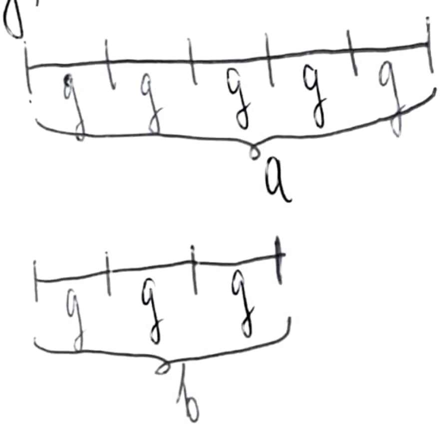
$\mathbb{Z}_n^\times$ and Euler's totient function.

We already mentioned the multiplicative group of integers modulo n: $\mathbb{Z}_n^\times = \{1 \leq a \leq n-1 \mid a \text{ is invertible modulo } n\}$.

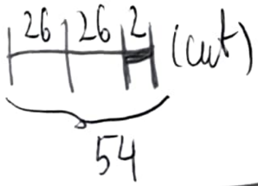
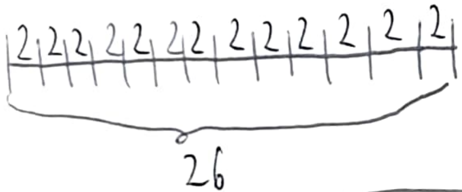
(1) How can we check (effectively) that a is invertible?

(2) What is the cardinality of $\mathbb{Z}_n^\times$?

In order to answer the first question, we will need to recall (extended) Euclid's algorithm. This algorithm is designed to effectively compute the gcd of two integers (the largest positive integer that divides both). It first appeared in Euclid's Elements (c. 300 BC) and was formulated in a more geometric way: the gcd of two numbers (lengths) a and b is the greatest length g that measures a and b evenly, i.e. a and b are integer multiples of g:



Algorithm for $a=242$, $b=54$.

	Geometrically	Algebraically
Step 1.		$242=54\cdot4+26$
Step 2.		$54=26\cdot2+2$
Step 3.		$26=2\cdot13$

The algorithm allows us to do a bit more: if x and y are positive integers with $\gcd(x,y)=g$, then there are integers a and b with $ax+by=g$. In order to find such a and b, we need to 'reverse the steps' of the algorithm. Let's demonstrate how that works on our example above:

From Step 2 we find $\gcd(242,54)=2=54-26\cdot2$, while step 1 allows to express $26=242-54\cdot4$, giving rise to

$$2=54-26\cdot2=54-(242-54\cdot4)\cdot2=\underline{\underline{-2}}\cdot\underline{242}+\underline{54}\cdot\underline{\underline{9}}$$

and $a=-2$, $b=9$.

<u>Prop-n.</u> x is invertible modulo $n \iff \gcd(x,n)=1$.

<u>Pf:</u> $\Rightarrow$ x is invertible modulo n, so there is $1\le a\le n-1$ with $ax\equiv1 \pmod n \iff ax=1+bn \iff ax-bn=1$.

$\Leftarrow$ $\gcd(x,n)=1 \iff \exists a,b: ax+bn=1 \iff ax\equiv1 \pmod n$.

Next we answer the second question.

Def-n. The **Euler totient function** is the f-n

$$\varphi: \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{>0}$$

given by $\varphi(n) = \#\{a \in \mathbb{Z}_n^{\times} \mid \gcd(a,n)=1\}$.

Set $\varphi(0) = \varphi(1) = 1$.

Rmk. The notation $\varphi(n)$ comes from Gauss' 1801 treatise 'Disquisitiones Arithmeticae', while the term 'totient' is due to Sylvester.

Properties.

1. $\varphi(p) = p-1$ for any prime p ($\gcd(a,p)=1$ for any $1 \leq a \leq p-1$).
2. $\varphi(mn) = \varphi(m)\varphi(n)$ for any m,n with $\gcd(m,n)=1$. (multiplicativity)
3. Euler's product formula: any $n \in \mathbb{Z}_{>0}$ can be written as $n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$ with p_i's distinct prime numbers.
$$\varphi(n) = p_1^{k_1-1}(p_1-1)\, p_2^{k_2-1}(p_2-1) \cdots p_s^{k_s-1}(p_s-1).$$

Examples.

1. $\varphi(20) = 2^{2-1}(2-1)(5-1) = 8 \quad (20 = 2^2 \cdot 5)$
2. $\varphi(225) = 3^{2-1}(3-1)\,5^{2-1}(5-1) = 120 \quad (225 = 3^2 \cdot 5^2)$

Def-n. The order of a finite group G is the number of elements in G. The order of an element $g \in G$ is the smallest positive integer $s \in \mathbb{Z}_{>0}$ with $g^s = e$.

Fact. The order of an element divides the order of the group.

Rmk. An element $g \in G$ generates a cyclic subgroup $\langle g \rangle = \{e, g, g^2, \dots, g^s\} \subset G$. The Fact above follows from a more general result that the order of a subgroup divides the order of the group. This is known as Lagrange's theorem.

We are going to discuss one of the widely used public key cryptosystems, known as RSA (after Rivest, Shamir and Adleman, who also 'invented' Alice and Bob). A technical lemma will be in the core of this cryptosystem.

Lemma. Let $p \neq q$ be prime numbers and $e \geq 1$ an integer, s.t. $\gcd(e, (p-1)(q-1)) = 1$. Then the congruence

$$x^e \equiv C \pmod{pq} \quad (\star)$$

has unique solution $x \equiv C^d \pmod{pq}$, $d \equiv e^{-1} \pmod{(p-1)(q-1)}$.

Pf: notice that $|\mathbb{Z}_{pq}^{\times}| = \varphi(pq) = (p-1)(q-1)$. We check that

$$C^{de} \equiv C^{1+k(p-1)(q-1)} \equiv C \cdot \left(C^{(p-1)(q-1)}\right)^k \equiv C \cdot 1 \equiv C \pmod{pq},$$ thus

$x \equiv C^d$ is a sol-n.

Let $x = a$ and $x = b$ be sol-ns of $(\star)$, then $a^e \equiv b^e \equiv C$, hence $a^{ed} \equiv a \equiv b \equiv b^{ed}$, so the sol-n is unique.

Example. $p=5, q=7, e=11$, i.e. we are given the congruence $x^{11} \equiv c \pmod{35}$. Let's pick $c=6$.

Step 1. Find $d \equiv 11^{-1} \pmod{24}$ $(24=(5-1)(7-1))$.
Using extended Euclid's algorithm we get

$$24 = 11 \cdot 2 + 2$$
$$11 = 5 \cdot 2 + 1$$

and $1 = 11 - 5 \cdot 2 = 11 - 5 \cdot (24 - 11 \cdot 2) = 11 \cdot 11 - 5 \cdot 24$,

so $11 \cdot 11 \equiv 1 \pmod{24}$ with $11^{-1} = 11$.

Step 2. The solution is $x \equiv c^d \equiv 6^{11} \equiv (6^2)^5 \cdot 6 \equiv 1 \cdot 6 \equiv 6 \pmod{35}$

2 3 **Rmk.** Given $n=pq$, but not the factors p and q, it is very hard to solve the congruence $x^e \equiv c \pmod{n}$ if $p, q \gg 0$.

RSA.

We describe how Alice can send an encrypted message to Bob and Bob recovers it.

Step 1. Bob chooses two large primes $p \neq q$ and a number e with $\gcd(e, (p-1)(q-1)) = 1$ (e is called an *encryption exponent*). He publishes $n = pq$ and e.

Step 2. Alice sends her plaintext message $m \in \mathbb{Z}_N$ encrypted via $c \equiv m^e \pmod{N}$

Step 3. Bob computes the decryption exponent $d \equiv e^{-1} \pmod{(p-1)(q-1)}$ and recovers the original message as

$$m \equiv c^d.$$

Rmk. In order to successfully intercept the message, one needs to know p, q. In fact, it is sufficient to know $p+q$, as $(x-p)(x-q) = x^2 - (p+q)x + \underbrace{n}_{=pq}$, so p and q can be recovered as roots.

Example of an attack on RSA.

Suppose Eve convinces Bob to decrypt a message (for instance to confirm his knowledge of p and q). Let's assume that Eve has access to the encrypted message $c \equiv m^e$ that Alice sent to Bob. Then Eve chooses a random number $k \in \mathbb{Z}_n$ and sends Bob the message $c' \equiv k^e \cdot c \pmod N$. Bob replies with the message $(c')^d \equiv k^{ed} \cdot c^d \equiv km \pmod N$ from which Eve easily recovers Alice's message m (as Eve knows k and therefore k^{-1}).