Groups (a brief overview)

Def-n. A group is a set G with a binary operation

$$*: G \times G \to G, \quad (\star)$$

satisfying the following requirements:

(0) $a*b \in G$ $\forall a,b \in G$ (closure, follows from $\star$);

(1) $(a*b)*c = a*(b*c)$ $\forall a,b,c \in G$ (associativity);

(2) There exists an element $e \in G$: $e*g = g*e = g$ $\forall g \in G$; (identity)

(3) $\forall g \in G$ $\exists a$: $a*g = g*a = e$ (inverse of g, denoted by g^{-1}).

Remark. If $a*b = b*a$ $\forall a,b \in G$, then G is called commutative (abelian).

Examples.

(1) $(\mathbb{Z},+)$, $(\mathbb{Z}_n,+)$: $e=0$, $a^{-1}=-a$. (2) $(\mathbb{F}_p^\times, \cdot)$: $e=1$, $a^{-1}=\frac{1}{a}$.

(3) Continuous functions on an interval $[a,b]$: $C([a,b])$

Do they form a group under

(a) pointwise addition?

(b) pointwise multiplication?

(c) composition?

(a) Well, $f^{-1} = -f$, $f \pm g$ is a continuous f-n, the op-n is associative. ✓

(b) We need to set $f^{-1} = \frac{1}{f}$, but it might so happen that $f(x) = 0$ at some points $x \in \mathbb{R}$ ($f \equiv 0$ is also a continuous f-n). Clearly $\frac{1}{f(x)}$ is not continuous at x with $f(x) = 0$. Hence, not a group. Can be improved by considering the subset $Good \subset C(\mathbb{R})$

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

Then $(Good, \times)$ is a group.

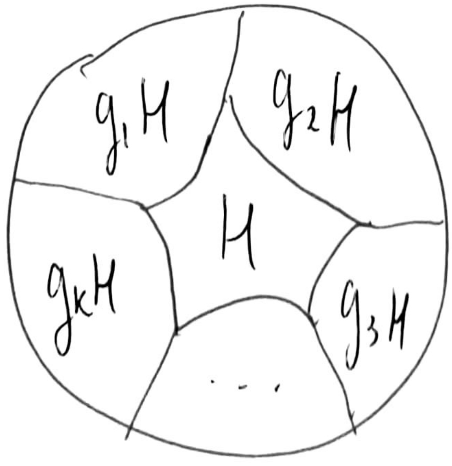
(c) Again, a problem withe the inverses. Think it over :) (bonus problem)

In this class, we focus on finite groups ($|G| < \infty$). The following theorem is a very important result on the structure of finite groups.

<u>Thm (Lagrange).</u> Let $H \subset G$ be a <u>subgroup</u> (both are finite). Then $|H|$ divides $|G|$.

Proof: for any element $g \in G$, there is a left coset of H in G given by $gH := \{gh \mid h \in H\}$.

• The left cosets g_1H and g_2H either do not intersect or coincide. Indeed, let $x \in g_1H \cap g_2H$, then $x = g_1h_1 = g_2h_2$, giving $g_2 = g_1h_1h_2^{-1}$ with $h_1h_2^{-1} \in H$. As $g_2 \in g_1H$, we get the containment $g_2H \subseteq g_1H$, and the reverse containment $g_1H \subseteq g_2H$ can be shown the same way. We conclude that $g_1H = g_2H$. It is also clear that the cardinality of any coset gH (number of elements) is equal to cardinality of H. As the number of different (nonintersecting) left cosets is equal to $\frac{|G|}{|H|}$ (G is disjoint union of such cosets), this number must be an integer. Hence, $|H|$ divides $|G|$.



$k = \frac{|G|}{|H|}$

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

A very important class of group is formed by multiplicative groups of integers modulo a number.

Def-n. Let $n \in \mathbb{Z}_{>1}$ and $\mathbb{Z}_n^\times = \{a \in \mathbb{Z}_n \mid \gcd(a,n)\} = 1\}$. The group $(\mathbb{Z}_n^\times, \times)$ is called the mult. group of integers modulo n.

Examples.

(1) $\mathbb{Z}_p^\times = \mathbb{F}_p^\times = \{1, 2, \ldots, p-1\}$

(2) $\mathbb{Z}_6^\times = \{1, 5\}$

(3) $\mathbb{Z}_8^\times = \{1, 3, 5, 7\}$

Which group is that? Is it cyclic?

Well, $3^2 \equiv 9 \equiv 1$, $5^2 \equiv 25 \equiv 1$, $1^2 \equiv 1$, $7^2 \equiv 1$. Not cyclic, has 3 elements of order 2, so must be $\mathbb{Z}_2 \times \mathbb{Z}_2$.

(4) $\mathbb{Z}_{15}^\times = \{1, 2, 4, 7, 8, 11, 13, 14\}$.

Find which 8-el-t group that is. Hint: there are the following possibilities (up to isomorphism):

$\mathbb{Z}_8$

$\mathbb{Z}_4 \times \mathbb{Z}_2$

$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

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

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

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

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.
2. $\varphi(mn) = \varphi(m)\varphi(n)$ for any m, n with $\gcd(m,n) = 1$ (multiplicativity).
3. Euler's product formula:

$n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$, then $\varphi(n) = p_1^{k_1-1}(p_1-1)p_2^{k_2-1}(p_2-1)\cdots p_s^{k_s-1}(p_s-1)$.

You will verify some of these in your homework.

Examples.

1. $20 = 2^2 \cdot 5$, so $\varphi(20) = 2^{2-1}(2-1)(5-1) = 2 \cdot 4 = 8$.
2. $225 = 3^2 \cdot 5^2$, so $\varphi(225) = 3^{2-1}(3-1)5^{2-1}(5-1) = 3 \cdot 2 \cdot 5 \cdot 4 = 120$.

<u>Thm (Gauss)</u> $\sum_{d|n} \varphi(d) = n$, where '$d|n$' means d divides n.

<u>Proof</u>: notice that $\varphi(d)$ is the number of generators of the group $\mathbb{Z}_d$. Every element in $\mathbb{Z}_n$ generates a subgroup of order $d|n$ (due to Lagrange thm). The result follows.

Another corollary of Lagrange theorem is the following result.

<u>Thm.</u> Let $a \in \mathbb{Z}_n$ and $\gcd(a,n)=1$. Then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

($\varphi(n)$ is the order of $\mathbb{Z}_n^{\times}$ and the order of an element divides the order of the group).

Integer factorization and RSA.

Our next goal is to study one of the most fundamental public key cryptosystems known as RSA (founded by Rivert, Shamir and Adleman). The following proposition is of fundamental importance for this system.

<u>Prop-n.</u> Let p and q be distinct primes and let $e \geq 1$ satisfy $\gcd(e, (p-1)(q-1)) = 1$. Then the congruence

$$x^e \equiv c \pmod{pq}$$

has the unique solution $x \equiv c^d \pmod{pq}$, where $d \equiv e^{-1} \pmod{(p-1)(q-1)}$. ($d$ exists as e and $(p-1)(q-1)$ are coprime).

<u>Proof:</u>

1. We check that $x \equiv c^d$ is a solution:

$$\varphi(pq) = (p-1)(q-1), \text{ so } c^{de} \equiv c^{\overset{\text{for some } k \in \mathbb{Z}}{1 + k\varphi(pq)}} \equiv c \cdot (c^{\varphi(pq)})^k \equiv c.$$

2. Now let's verify uniqueness. Suppose y is a different solution. Then $x^e \equiv y^e$, so $x^{ed} \equiv y^{ed}$ or (as $ed = 1 + k\varphi(pq)$ for some $k \in \mathbb{Z}$) $x \cdot (x^{\varphi(pq)})^k \equiv y (y^{\varphi(pq)})^k \Leftrightarrow x \equiv y$.

<u>Remark.</u> Now we have an algorithm for solving congruences $x^e \equiv c \pmod{pq}$ (for e with $\gcd(e, (p-1)(q-1)) = 1$).

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

Step 1. Find $d \equiv 11^{-1} \pmod{24}$.

Use extended Euclid's algorithm:
$$24 = 2\cdot 11 + 2$$
$$11 = 5\cdot 2 + 1$$
$$1 = 11 - 5\cdot 2 = 11 - 5\cdot(24 - 2\cdot 11) = 11\cdot 11 - 5\cdot 24,$$ hence

$11^{-1} \equiv 11 \pmod{24}$, so $d \equiv 11$.

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

Check: $6^{11} \equiv 6$.

Important remark. Given $n=pq$, but not the actual factors p and q, it is very hard to solve the congruence $x^e \equiv c \pmod{n}$.

Reason: we do not know $\varphi(n)$.

RSA.

We describe this PKC first, assuming Alice wants to send Bob a message.

<u>Step 1.</u> Bob chooses two distinct large primes p and q and a number e, s.t. $\gcd(e, (p-1)(q-1)) = 1$ (e is called <u>the encryption exponent</u>). He publishes $N = pq$ and e.

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

<u>Step 3.</u> Bob computes $d \equiv e^{-1} \pmod{(p-1)(q-1)}$ and recovers $m \equiv c^d$ (see the prop-n and example above).

<u>Rmk.</u> The number d is called <u>the decryption exponent</u>.

<u>Rmk.</u> In order to intercept the message, one needs to know p and q. In fact, it is sufficient to know $p+q$, since p and q are the roots of the quadratic polynomial $x^2-(p+q)x+pq$ and we already know that $pq = N$.

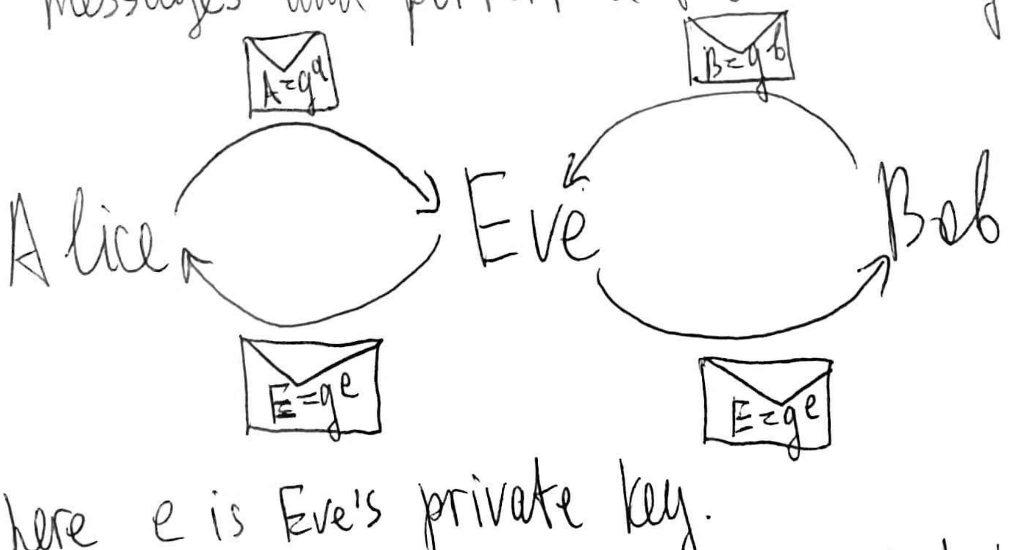
Man-in-the-Middle-Attack.

Here we briefly address some security issues related to practical implementation of RSA.

As a warm example, we describe an attack on the Diffie-Hellman key exchange.

Recall that $g \in \mathbb{F}_p^\times$, Alice chooses a secret key $a \in \mathbb{F}_p^\times$ and Bob chooses his private key $b \in \mathbb{F}_p^\times$. Then Alice sends Bob the number $A = g^a$ and Bob sends $B = g^b$ in return, so their shared key becomes $K = A^b = B^a$.

What if someone (usually named Eve) intercepted their messages and performed the following trick:



,

where e is Eve's private key.

Alice would not be able to realize that the message she received was not from Bob and obtain a shared key $K_{wrong_1} = g^{ea}$ with Eve.

Similarly, Bob would have a shared key with Eve. $K_{wrong_2} = g^{eb}$ and think that he has a common key with Alice.

Rmk. Notice that Eve did not solve the underlying DLP, but was able to intercept the whole correspondence. Moreover, neither Alice nor Bob are aware of what happened.

Next, an example of an attack on RSA.

Suppose Sherlock convinces Alice to decrypt a message using her (Alice's) private key (for example to authenticate her identity as the owner of the public key (N, e)). Moreover, assume that Sherlock has access to an encoded message c that Bob sent to Alice.

Then Sherlock chooses a random number k and sends Alice ~~an~~ a 'message' $c' \equiv k^e \cdot c \pmod{N}$.

Alice replies with $(c')^d \equiv k^{ed} \cdot c^d \equiv k \cdot m \pmod{N}$, where m is Bob's plaintext message. As Sherlock knows k^{-1} (can easily compute), he decodes m.

Again, Sherlock made no progress in solving the original hard problem (factoring N). Well, he did not need to, he has his dear Watson for that.