A digression to describe RSA encryption

Alice wants to be able to have Bob send her secret messages (as some $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$), while Eve is eavesdropping (!?) (on both the set-up and the message transmissions)

STEP 1:

Alice picks two huge random primes p, q keeping them secret, (~10^{1000})

but then computes $n = p \cdot q$ and publishes n.

She also picks a randomly chosen encryption exponent $\bar{e} \in \left(\mathbb{Z}/(p-1)(q-1)\right)^{\times}$,

and publishes e as an integer in range $1, 2, \ldots, (p-1)(q-1)$,

keeping $(p-1)(q-1)$ secret.

She lastly computes the decryption exponent $\bar{d} = \bar{e}^{-1}$ in $\left(\mathbb{Z}/(p-1)(q-1)\right)^{\times}$,

but keeps it secret.

STEP 2:

When Bob wants to send Alice $\bar{x}$ in $(\mathbb{Z}/pq\mathbb{Z})^{\times} = (\mathbb{Z}/n\mathbb{Z})^{\times}$,

he computes $\bar{y} := \bar{x}^{e}$ and sends $\bar{y}$ to Alice publicly instead.

STEP 3:

Alice decrypts $\bar{y}$ by computing

$$\bar{y}^{d} = (\bar{x}^{e})^{d} = \bar{x}^{de} = \bar{x}^{1+k(p-1)(q-1)} = \bar{x}^{1}\left(\bar{x}^{(p-1)(q-1)}\right)^{k} = \bar{x}^{1} \cdot \bar{1} = \bar{x}$$

(for some $k \in \mathbb{Z}$, since $\bar{d} = \bar{e}^{-1}$ in $(\mathbb{Z}/(p-1)(q-1)\mathbb{Z})^{\times}$)

(by Euler's Thm, since $\varphi(n) = \varphi(pq) = (p-1)(q-1)$)

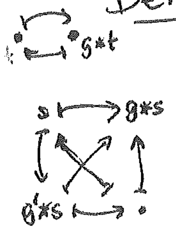
10/15/18 >

Crucial points

- Every computation Alice or Bob must do need to be achievable quickly, meaning at worst in # of steps at most a polynomial in # of digits of p or q ($= \log(p), \log(q)$)
  (Math 5248 discusses these computational issues)
- Eve would need to either factor n into $p \cdot q$ (only slow, exponential algorithms known !)
  or compute $\sqrt[e]{\bar{y}} = \bar{x}$ in $\mathbb{Z}/n\mathbb{Z}$ (same story !)

§6.7 Group operations / actions

Groups were made to *operate* or *act* on things, as symmetries!



DEF'N: A group G *operates/acts* on a set S if we specify a rule

$$G \times S \longrightarrow S \qquad (g, s) \longmapsto g*s$$

with
$$\begin{cases} 1*s = s & \forall s \in S \\ (gh)*s = g*(h*s) & \forall g,h \in G,\ s \in S \end{cases}$$

(Often we suppress the $*$, writing gs or $g(s)$)

Writing $s \sim s'$ if $\exists g \in G$ with $g(s) = s'$,

this is an equiv. relation:

$s \sim s$ since $s = 1*s$

$s \sim s' \Rightarrow s' \sim s$ since $g(s) = s'$
$\Rightarrow g^{-1} g(s) = g^{-1} s'$, where $g^{-1}g(s) = 1(s) = s$

$s \sim s',\ s' \sim s'' \Rightarrow s \sim s''$ since $g_1(s) = s'$, $g_2(s') = s''$
$\Rightarrow g_2 g_1(s) = g_2(s') = s''$

The equivalence classes are called the *orbits* of G on S,

written $\mathcal{O}_s = \{s' \in S : s' \sim s,$ i.e. $\exists g \in G$ with $s' = g(s)\}$

or $s \sim s' \Leftrightarrow \mathcal{O}_s = \mathcal{O}_{s'}$. If there is *only one* orbit $\mathcal{O}_s = S$, then one calls the G-action S *transitive*.

EXAMPLES: ① $G = S_n$ = symmetric group acts on $S := \{1, 2, \ldots, n\}$ via

$$G \times S \longrightarrow S$$
$$S_n \times \{1, 2, \ldots, n\} \mapsto \{1, 2, \ldots, n\}$$
$$(p, i) \longmapsto p(i) \ (=: p*i)$$

with only one orbit, i.e. transitively,

since for any $i, j \in \{1, 2, \ldots, n\}$ $\exists\, p \in S_n$ with $p(i) = j$.

But $G=S_n$ also acts on $S := \{\text{ordered pairs } (i,j) : i,j \in \{1,2,\dots,n\}\}$
$= \{1,2,\dots,n\} \times \{1,2,\dots,n\}$

via $p * (i,j) := (p(i), p(j))$

and then there are two orbits $\{(i,i) : i=1,\dots,n\} = \mathcal{O}_{(1,1)}$, $\{(i,j) : i \neq j\} = \mathcal{O}_{(1,2)}$, so it is not a transitive action.

e.g. $n=4$

$$S = \left\{\begin{matrix} (1,1), & (1,2), & (1,3), & (1,4), \\ (2,1), & (2,2), & (2,3), & (2,4), \\ (3,1), & (3,2), & (3,3), & (3,4), \\ (4,1) & (4,2), & (4,3), & (4,4) \end{matrix}\right\}$$

$= \mathcal{O}_{(1,2)} = \mathcal{O}_{(1,3)} = \dots = \mathcal{O}_{(4,3)}$

$\mathcal{O}_{(1,1)} = \mathcal{O}_{(2,2)} = \dots$

e.g. $(14) * (1,1) = (4,4)$

$\begin{pmatrix} 1234 \\ 3241 \end{pmatrix} * (1,3) = (3,4)$

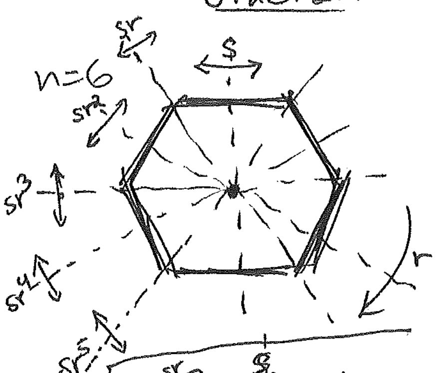
10/17/2018>

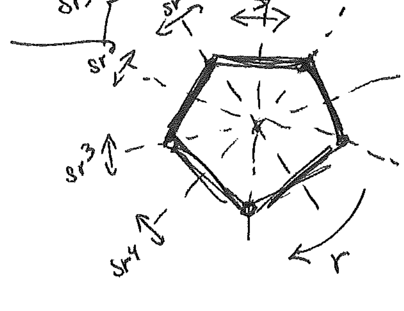
② $D_n :=$ (linear) symmetries of a regular n-sided polygon
dihedral group of order $2n$

$= \{n \text{ rotations } e, r, r^2, \dots, r^{n-1}\} \sqcup \{n \text{ reflections } s, sr, sr^2, \dots, sr^{n-1}\}$

r = rotation through $\frac{2\pi}{n}$ clockwise

$= \langle r \rangle \sqcup s\langle r \rangle$





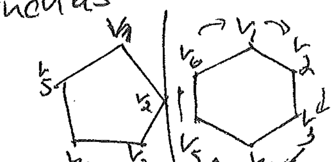
$C_n \cong \langle r \rangle \cong (\mathbb{Z}/n\mathbb{Z})^+$, $\langle r \rangle \lhd D_n$

$srs^{-1} = srs = r^{-1} = r^{n-1}$

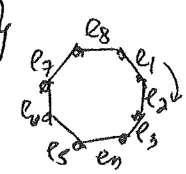
$sr^ks^{-1} = r^{-k}$

$G = D_n$ acts on various sets transitively such as

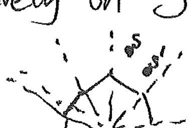
$S = \{\text{vertices } v_1, \dots, v_n \text{ of the } n\text{-gon}\}$
$\mathcal{O}_{v_1} = \mathcal{O}_{v_2} = \dots = \mathcal{O}_{v_n}$



or $S = \{\text{edges } e_1, \dots, e_n \text{ of the } n\text{-gon}\}$
$\mathcal{O}_{e_1} = \mathcal{O}_{e_2} = \dots = \mathcal{O}_{e_n}$



but G also acts nontransitively on $S = \mathbb{R}^2$, since there are infinitely many orbits $\mathcal{O}_s$:



$\mathcal{O}_s \neq \mathcal{O}_{s'}$