Modern Cryptology (236506) – Exercise no. 1

Submission in singles on 05/11/2012.

5 bonus points will be given to two-sided printed submissions.

- The purpose of the first part of this exercise is to remind you some basic properties of groups. No additional material is required. Questions marked with # are not for submission.
- Text files for the last questions are available in the course website.

Recall that a group \((S, \oplus)\) is a set \(S\) with a binary operation \(\oplus\) defined on \(S\) for which the following properties hold:

I Closure: For all \(a, b \in S\) it holds that \(a \oplus b \in S\).

II Identity: There is an element \(e \in S\) such that \(e \oplus a = a \oplus e = a\) for all \(a \in S\).

III Associativity: \((a \oplus b) \oplus c = a \oplus (b \oplus c)\) for all \(a, b, c \in S\).

IV Inverses: For each \(a \in S\) there exists an element \(b \in S\) such that \(a \oplus b = b \oplus a = e\).

Let \(a\) be an element in a group and let \(a^{-1}\) denote the (unique) inverse of \(a\). Then, for every integer \(k\) we define:

\[
a^k \overset{\text{def}}{=} \begin{cases} 
\bigoplus_{i=1}^{k} a = a \oplus a \oplus \ldots \oplus a, & \text{if } k > 0; \\
e, & \text{if } k = 0; \\
(a^{-1})^{-k}, & \text{if } k < 0.
\end{cases}
\]

# Prove:

(a) The identity element \(e\) in the group is unique.

(b) Every element \(a\) has a single inverse.

Let \(m, n\) be integers (not necessarily positive). Prove:

(c) \(a^m \oplus a^n = a^{m+n}\).

(d) \((a^n)^n = a^{nm}\).

The order of a group, denoted by \(|S|\), is the number of elements in \(S\). If the order of a group is a finite number, the group is said to be a finite group.

The order of an element \(a\) in a group is the smallest integer \(k\) such that \(a^k = e\), or infinity if no such \(k\) exists.

Let \((S, \oplus)\) be a finite group, and let \(S' \subseteq S\). If \((S', \oplus)\) is also a group, then \((S', \oplus)\) is called a subgroup of \((S, \oplus)\). We will sometimes denote the subgroup only by \(S'\), omitting the operation sign.

A subgroup \(S' \subseteq S\) is called trivial if \(S' = \{e\}\) or \(S' = S\). Otherwise, it is called nontrivial.
Let \((S, \oplus)\) be a finite group.

(a) Let \(a \in S\). Prove that the order of \(a\) in \(S\) is finite.

(b) Prove that if \(S'\) is any non-empty subset of \(S\) such that \(a \oplus b \in S'\) for all \(a, b \in S'\), then \((S', \oplus)\) is a subgroup of \((S, \oplus)\).

If a group \((S, \oplus)\) satisfies the commutative law \(a \oplus b = b \oplus a\) for all \(a, b \in S\) then it is called an Abelian group.

Let \(g\) be an element of a finite group \((S, \oplus)\), define the set \(\langle g \rangle \overset{\text{def}}{=} \{g^k : k \geq 1\}\). A group of the form \((\langle g \rangle, \oplus)\) is called a cyclic group.

1. Let \((S, \oplus)\) be a finite group, and let \(g \in S\).

(a) Prove that \((\langle g \rangle, \oplus)\) is indeed a group, and that it is Abelian.

(b) Show that without the assumption that \(S\) is finite, \(\langle g \rangle\) is not necessarily a group.

(c) How should the definition of the set \(\langle g \rangle\) be generalized so that \((\langle g \rangle, \oplus)\) will be a subgroup even when \(S\) is infinite?

2. Let \(+_n\) denote addition modulo \(n\) (e.g., \(5+_3 6 = (5+6) \mod 3 = 2\)). Let \(\mathbb{Z}_n = \{0, 1, \ldots, n-1\}\).

(a) Prove that \((\mathbb{Z}_n, +_n)\) is a finite Abelian group for every natural number \(n\).

(b) Give an example of a group of the form \(\mathbb{Z}_n\) with a nontrivial subgroup.

(c) Give an example of a group of the form \(\mathbb{Z}_n\) that does not have a nontrivial subgroup.

Can you characterize all the groups that holds this property?

3. A group \((S, \oplus)\) is cyclic if there exists an element \(g \in S\) that “generates” the group; that is, \(S = \langle g \rangle\), where \(\langle g \rangle\) is defined as in 1c. (Such an element is referred to as a generator.)

(a) Give an example of a finite cyclic group.

(b) Give an example of a finite group that is not cyclic.

In both cases you should prove that the given group is indeed cyclic (resp. non-cyclic).

4. Let \(a\) and \(b\) be two positive integers. We denote by \(\gcd(a, b)\) the greatest common divisor of \(a\) and \(b\); i.e, \(d = \gcd(a, b)\) if \(d\) is the greatest integer that divides both \(a\) and \(b\). The Euclidean algorithm computes the gcd as follows:

\[
\begin{align*}
\text{input: } & a > b > 0 \\
r_{-1} & \leftarrow a \\
r_0 & \leftarrow b \\
\text{for } i = 1, 2, \ldots \text{ till } r_i = 0 \\
r_i & \leftarrow r_{i-2} \mod r_{i-1} \\
\text{output } & r_{i-1}
\end{align*}
\]

Let \(a\) be your 9-digit id number. Use the Euclidean algorithm to compute \(\gcd(a, 3600)\). Write all the intermediate values of the \(r_i\)’s.
5. The Euclidean algorithm can be extended so that not only \( \gcd(a, b) \) is found but also \( x, y \in \mathbb{Z} \) such that \( x \cdot a + y \cdot b = \gcd(a, b) \).

(a) Similar to \( +_n \), we define \( \cdot_n \) to be multiplication modulo \( n \). Show that \((\mathbb{Z}_n, \cdot_n)\) is not a group.

(b) In order to make a group out of \((\mathbb{Z}_n, \cdot_n)\) we “remove the offending elements”. Define \( \mathbb{Z}_n^* \) to be \( \{a \in \mathbb{Z}_n | \gcd(a, n) = 1\} \) and show that \((\mathbb{Z}_n^*, \cdot_n)\) is a group (hint: use the extended Euclidean algorithm on \( a, n \)).

(c) (Bonus - 5 points) Give a pseudo-code for the extended algorithm (there is no need to prove its correctness).

6. Solve the following Vigenere cipher. Explain the techniques you use, describe the steps of your solution and show some partial results.

```
IGJAT QLYCE NQZAO CLJIE RNTOJ RLVMR GQBCM CESIW ENGHB
XLXEM DRATI ICPPM VRQWI SXJSY MNLKO SHMCX HRAAN IZQER
NNOEM PPPER DGUIT QLTHI NFUEM MGPHA IGUNP SESIV TUBUH
LEELE NGLBP ZPLRH BRYOW IOMCQ EVJAT ENSMP DNADT LPHEW
APUIM HTYXL IFXIO KQZQF YGUET ILMYX WRYOW IOHMX HNYOW
IESEX WNFMP VPELE NYBVF MLHYQ YNANB FPWPI EJVTI EWZI
TUN TU LPHMR GRQSF VLALW OSUEB ZPYGS VRGEE LPCER DZREE
KLCEP LNAPP I
```

7. Solve the following substitution cipher. Explain the techniques you use, describe the steps of your solution and show some partial results.

```
DPGJD OORNW WNKMD BDCWJ NAMEK NRWBW DCIDN CKGJC NKAQC
WLGEK EBXSI GDYJ GWCDD NAGEK AKDAL DNINR WBBDC IDNBG
KNGGE KAKDA LDNIN RBBD CIDNB KNGM DBDXK BGDNA RBBBD
CIDNA IANGO IFKEI LKZKN GEWJT EEEKD ANKZK CBKKN EILED
ZINTE ILORI NTDCD JNADO QADRQ NNWRK ARWBB DCIDN BWLJP
EGEDG EKEDA TWNKG WGEKW CACO RCWLL BKZKC DOGIL KGBWP
WLXOD INGBJ KCTKD NGGWM BKCMF WCKQJ BKAGW DALIG GEDGG
EKAKD ALDKN ZKNU IBGKA MEIPE WQPWJ CBKEK NOWNB TKCAI
AIGMD BBGIO OLWCK QCJBG CDGIN TGWGC RGWDX XKDOA ICKPG
ORGWL DFWCL DFWCG EKOWN TNDAY WNRBS JDACW NPWLL DANKC
MEWOW WHKAD OIQGO KIYIG IHEKE KCRQW NADIN AIBGC KBBBDN
AMKNG FJLXI NTWJG GEKMI NAWMQ QEBW QQIPK KDPEG ILKRW
BBDCI DNYJO OIAKE IBMDR XDBGB KCTKD NGGWM BKGW BXKDH
GWEIL DYWJG IGEK AKDLN DNINR WBBBD IDNBG KNGM DBILX
ORNWG KDBRG WOIJK MIGEE KKSZK AIBGJ CYKAW CCMEW MDBNW
GKDRB GWOIZ KIMEG KIKEK CDNAM EWWNG EKADR RBBD CIDNP
DLKYD PHMDB GINHK CINTM IGEGE KQDJP KGGED GQKAT DBWOI
NKING WGEKB GWZKE KEDAB DCGK AYJIO AINTM EIOKR WBBDC
IDNMD BINGE KEWBX IGDOF WBKXE EKOOK C
```