Modern Cryptography December 17, 2018

Homework 9

Lecturer: Daniel Slamanig, TA: Karen Klein

To get credit for this homework it must be submitted no later than Wednesday, December 12th via email to `michael.walter@ist.ac.at`, please use "MC18 Homework 9" as subject.
Please put your solutions into a single pdf file[1] and name this file Yourlastname_HW9.pdf.

1. Groups

   - Let $N \in \mathbb{Z}_{\geq 0}$ and let $G = \mathbb{Z}_N$. Prove that G is a group under the operation $a \cdot b = (a + b) \bmod N$.

     Solution: For $N = 0$, $\mathbb{Z}_N$ is the empty set, which is not a group by definition. Now, assume $N > 0$, hence, $\mathbb{Z}_N$ is not empty. To prove that $G = \mathbb{Z}_N$ is a group we have to show that all four properties are satisfied. Let $a, b, c \in \mathbb{Z}_N$.

     – *Closure:* Obviously, $a \cdot b = [a + b \bmod N] \in \mathbb{Z}_N$.

     – *Identity:* The identity element is $0 \in \mathbb{Z}_N$, since $a \cdot 0 = [a+0 \bmod N] = [a \bmod N] = a$ and $0 \cdot a = [0 + a \bmod N] = [a \bmod N] = a$.

     – *Inverse:* Define the inverse $(-a)$ of a as $(-a) := [-a \bmod N] = N - a \in \mathbb{Z}_N$. It holds: $a \cdot (-a) = [a + N - a \bmod N] = [0 \bmod N] = 0 \in \mathbb{Z}_N$ and $(-a) \cdot a = [N - a + a \bmod N] = [0 \bmod N] = 0 \in \mathbb{Z}_N$.

     – *Associativity:* $(a \cdot b) \cdot c = [[a + b \bmod N] + c \bmod N] = [[a + b \bmod N] + (a + b - [a + b \bmod N]) + c \bmod N] = [a + b + c \bmod N]$ and similarly for $a \cdot (b \cdot c)$. Note, that we used the fact that $(a + b - [a + b \bmod N])$ is a multiple of N.

     $\square$

   - List the elements of $\mathbb{Z}_{10}^*$; what is its order?; What are the orders of 3 and 9?; Is $\mathbb{Z}_{10}^*$ cyclic?

     Solution: $\mathbb{Z}_{10}^* = \{x \in \mathbb{Z}_{10} \mid \mathsf{gcd}(x, 10) = 1\} = \{1, 3, 7, 9\}$; thus, $|\mathbb{Z}_{10}^*| = 4$. Recall, $\mathsf{ord}(x) := \min\{i \in \mathbb{Z}_{>0} \mid x^i = 1 \bmod 10\}$. We have $3^1 = 3 \bmod 10$, $3^2 = 9 \bmod 10$, $3^3 = 27 = 7 \bmod 10$, $3^4 = 21 = 1 \bmod 10$; hence, $\mathsf{ord}(3) = 4$. Similarly, we get $\mathsf{ord}(9) = 2$ by computing $9^1 = 9 \bmod 10$, $9^2 = 81 = 1 \bmod 10$. Recall that a group G is cyclic if there is an element $g \in G$ such that $\mathsf{ord}(g) = |G|$. Above we saw that $\mathsf{ord}(3) = 4 = |\mathbb{Z}_{10}^*|$, thus, $\mathbb{Z}_{10}^*$ is cyclic and 3 is a generator of $\mathbb{Z}_{10}^*$. $\square$

   - Does the set $\mathbb{Z}_{15} \setminus \{0\}$ form a group under multiplication? If not, why?

     Solution: $(\mathbb{Z}_{15} \setminus \{0\}, \cdot)$ is not a group, since, e.g., $3, 5 \in \mathbb{Z}_{15} \setminus \{0\}$ but $3 \cdot 5 = [0 \bmod 15] \notin \mathbb{Z}_{15} \setminus \{0\}$, hence the closure property is not satisfied. Alternatively, one could also argue that 3 doesn't have an inverse in $\mathbb{Z}_{15} \setminus \{0\}$. $\square$

[1] If you don't know how to do it, you can use e.g. `https://www.pdfmerge.com/`

2. Extended Euclidean Algorithm:

- **[B.1 in book, 2nd edition]** Prove correctness of the extended Euclidean algorithm (extGCD).

  Solution: Recall the extended Euclidean algorithm extGCD from the book [B.10]:

Algorithm 1 extGCD

Input: $a, b \in \mathbb{N}$
Output: (d, X, Y) with $d = \mathsf{gcd}(a, b)$ and $Xa + Yb = d$
if $b|a$ **then return** $(b, 0, 1)$
else compute $q, r \in \mathbb{N}$ with $a = qb + r$ and $0 < r < b$
    $(d, X, Y) := \mathsf{extGCD}(b, r)$
    return $(d, Y, X - Yq)$

We prove correctness by an inductive argument (over the number of rounds). For the base case, let $b|a$. Then $\mathsf{gcd}(a, b) = b = 0a + 1b$, hence correctness is satisfied for the output $\mathsf{extGCD}(a, b) = (b, 0, 1)$. Now, consider the case $b \nmid a$. Let $q, r \in \mathbb{N}$ with $a = qb + r$ and $0 < r < b$. Assume the output $(d, X, Y) = \mathsf{extGCD}(b, r)$ of the previous round is correct. Then $d = \mathsf{gcd}(b, r) = \mathsf{gcd}(b, a - qb) = \mathsf{gcd}(b, a) = \mathsf{gcd}(a, b)$ and $Ya + (X - Yq)b = Xb + Y(a - qb) = Xb + Yr = d$, as required.
You can prove $\mathsf{gcd}(b, a - qb) = \mathsf{gcd}(b, a)$ more formally as follows. Let $d = \mathsf{gcd}(b, a - qb)$ and $d' = \mathsf{gcd}(b, a)$. By definition, $d|b$ and $d|(a - qb)$, hence $b = k_1 d$ and $a - qb = k_2 d$ for some $k_1, k_2 \in \mathbb{Z}$, which implies $a = (k_2 + qk_1)d$. Thus, d divides a as well as b and it follows $d \leq d'$. On the other hand, similarly to above, $b = k_1' d'$ and $a = k_2' d'$ for some $k_1', k_2' \in \mathbb{Z}$ implies $a - qb = (k_2' - qk_1')d'$, hence d' divides b as well as $a - qb$, and we can conclude $d' \leq d$. It follows that $d = d'$. □

- Use the extGCD to compute X, Y for $a = 2498$ and $b = 8712$. Illustrate all steps.

  Solution: It holds $b \nmid a$, so we compute $q_0 = 0$, $r_0 = 2498$ such that $2498 = q_0 8712 + r_0$.
  It holds $r_0 \nmid b$, so we compute $q_1 = 3$, $r_1 = 1218$ such that $8712 = q_1 2598 + r_1$.
  It holds $r_1 \nmid r_0$, so we compute $q_2 = 2$, $r_2 = 62$ such that $2498 = q_2 1218 + r_2$.
  It holds $r_2 \nmid r_1$, so we compute $q_3 = 19$, $r_3 = 40$ such that $1218 = q_3 62 + r_3$.
  It holds $r_3 \nmid r_2$, so we compute $q_4 = 1$, $r_4 = 22$ such that $62 = q_4 40 + r_4$.
  It holds $r_4 \nmid r_3$, so we compute $q_5 = 1$, $r_5 = 18$ such that $40 = q_5 22 + r_5$.
  It holds $r_5 \nmid r_4$, so we compute $q_6 = 1$, $r_6 = 4$ such that $22 = q_6 18 + r_6$.
  It holds $r_6 \nmid r_5$, so we compute $q_7 = 4$, $r_7 = 2$ such that $18 = q_7 4 + r_7$.
  It holds $r_7 \mid r_6$, so $(d, X_7, Y_7) = \mathsf{extGCD}(r_6, r_7) = (r_7, 0, 1) = (2, 0, 1)$.
  Thus, we get $(d, X_6, Y_6) = (d, Y_7, X_7 - Y_7 q_7) = (2, 1, -4)$.
  Thus, we get $(d, X_5, Y_5) = (d, Y_6, X_6 - Y_6 q_6) = (2, -4, 5)$.
  Thus, we get $(d, X_4, Y_4) = (d, Y_5, X_5 - Y_5 q_5) = (2, 5, -9)$.
  Thus, we get $(d, X_3, Y_3) = (d, Y_4, X_4 - Y_4 q_4) = (2, -9, 14)$.
  Thus, we get $(d, X_2, Y_2) = (d, Y_3, X_3 - Y_3 q_3) = (2, 14, -275)$.
  Thus, we get $(d, X_1, Y_1) = (d, Y_2, X_2 - Y_2 q_2) = (2, -275, 564)$.
  Thus, we get $(d, X_0, Y_0) = (d, Y_1, X_1 - Y_1 q_1) = (2, 564, -1967)$.

Finally, we get $(d, X, Y) = (d, Y_0, X_0 - Y_0 q_0) = (2, -1967, 564)$ and indeed it holds $-1967 \cdot 2498 + 564 \cdot 8712 = 2$.

$\square$

- Discuss how extGCD can be used to compute the multiplicative inverse.

  Solution: To compute the multiplicative inverse of $a \bmod N$, note that $a \in \mathbb{Z}_N$ is invertible if and only if $\mathsf{gcd}(a, N) = 1$. Thus, we can use extGCD to compute $X, Y \in \mathbb{Z}$ such that $Xa + YN = 1$. Since $1 = Xa + YN = Xa \bmod N$ we can deduce that $[X \bmod N] \in \mathbb{Z}_N$ is the inverse of a in $\mathbb{Z}_N^*$. $\square$

3. Euler phi function

- Let p be prime and $e \geq 1$ an integer. Show that $\varphi(p^e) = p^{e-1}(p-1)$.

  Solution: Recall,

  $$\varphi(p^e) := |\mathbb{Z}_{p^e}^*| = |\{x \in \mathbb{Z}_{p^e} \mid \mathsf{gcd}(x, p^e) = 1\}| = |\{x \in \mathbb{Z}_{p^e} \mid \mathsf{gcd}(x, p) = 1\}|.$$

  Using division with remainder, we get $\mathbb{Z}_{p^e} = \{kp + r \mid 0 \leq k < p^{e-1},\ 0 \leq r < p\}$. It holds $\mathsf{gcd}(kp + r, p) = \mathsf{gcd}(r, p)$ and since p is a prime, we have $\mathsf{gcd}(r, p) = 1$ for all $0 < r < p$. Hence, $\mathbb{Z}_{p^e}^* = \{kp + r \mid 0 \leq k < p^{e-1},\ 0 < r < p\}$ and $\varphi(p^e) = p^{e-1}(p-1)$. $\square$

- Let p, q be relatively prime. Show that $\varphi(pq) = \varphi(p) \cdot \varphi(q)$.

  Solution: For any $x \in \mathbb{Z}_{pq}$, by definition of gcd we have $\mathsf{gcd}(x, pq) = 1$ if and only if $\mathsf{gcd}(x, p) = 1$ and $\mathsf{gcd}(x, q) = 1$, i.e., $[x \bmod p] \in \mathbb{Z}_p^*$ and $[x \bmod q] \in \mathbb{Z}_q^*$. Consider the following map $f : \mathbb{Z}_{pq}^* \to \mathbb{Z}_p^* \times \mathbb{Z}_q^*$, $x \mapsto ([x \bmod p], [x \bmod q])$. We show that f is bijective. For surjectivity, let (a, b) be an arbitrary element in $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$. Since p and q are coprime, there exist $X, Y \in \mathbb{N}$ such that $Xp + Yq = 1$ and in particular $Yq = 1 \bmod p$ and $Xp = 1 \bmod q$. It follows $f([aYq + bXp \bmod pq]) = ([aYq \bmod p], [bXp \bmod q]) = (a, b)$, which proves surjectivity. For injectivity, let $x, x' \in \mathbb{Z}_{pq}^*$ such that $f(x) = f(x')$. Hence, $x = x' \bmod p$ and $x = x' \bmod q$. It follows $p|(x - x')$ and $q|(x - x')$, and since p and q are coprime we can conclude $pq|(x - x')$ as follows. Let $k_1, k_2 \in \mathbb{Z}$ such that $(x - x') = k_1 p = k_2 q$, and X, Y as above, i.e., $Xp + Yq = 1$. Multiplying this with $(x - x')$ gives $x - x' = (x - x')Xp + (x - x')Yq = k_2 q X p + k_1 p Y q = (k_2 X + k_1 Y)pq$. Thus, $(pq)|(x - x')$ and hence $x = x' \bmod pq$. This shows that f is a bijection between $\mathbb{Z}_{pq}^*$ and $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$, which proves that both sets have the same cardinality, i.e., $\varphi(pq) = |\mathbb{Z}_{pq}^*| = |\mathbb{Z}_p^* \times \mathbb{Z}_q^*| = \varphi(p)\varphi(q)$. $\square$