Exercise 6.1 (Chinese Remainder Theorem). (8 points) To investigate the structure of rings \((\mathbb{Z}_N, +, \cdot)\) with composite \(N\) it is useful to pick a suitable factorization \(N = ab\) and look at the set \(\mathbb{Z}_a \times \mathbb{Z}_b\) consisting of all pairs \((x, y)\) with \(x \in \mathbb{Z}_a\) and \(y \in \mathbb{Z}_b\). We define addition and multiplication on \(\mathbb{Z}_a \times \mathbb{Z}_b\) componentwise.

(i) Consider \(20 = 5 \cdot 4\) and look at the map \(\pi_1 : \mathbb{Z}_{20} \to \mathbb{Z}_4\) which maps an integer \(0, 1, \ldots, 19 \in \mathbb{Z}_{20}\) to its remainder modulo 4. Prove that for any two elements \(a, b \in \mathbb{Z}_{20}\) the following holds:

\[
\pi_1(a + b) = \pi_1(a) + \pi_1(b)\]

and

\[
\pi_1(a \cdot b) = \pi_1(a) \cdot \pi_1(b).\]  

(†)

Fill out a table with rows indexed by \(\mathbb{Z}_4\) and columns indexed by \(\mathbb{Z}_5\).

Note: a map having the properties \(†\) is called a ring homomorphism.

(ii) Pick two elements \(x, y \in \mathbb{Z}_{20}\) (to make it interesting: the sum of the representing integers shall be larger than 20). First, add them in \(\mathbb{Z}_{20}\) and then map to \(\mathbb{Z}_5 \times \mathbb{Z}_4\). Second, map both to \(\mathbb{Z}_5 \times \mathbb{Z}_4\) and add afterwards. What do you observe?

(iii) Pick two elements \(x, y \in \mathbb{Z}_{20}\) (to make it interesting: the product of the representing integers shall be larger than 20). First, multiply them in \(\mathbb{Z}_{20}\) and then map to \(\mathbb{Z}_5 \times \mathbb{Z}_4\). Second, map both to \(\mathbb{Z}_5 \times \mathbb{Z}_4\) and multiply afterwards. What do you observe?

(iv) Mark all the invertible elements in \(\mathbb{Z}_5, \mathbb{Z}_4,\) and \(\mathbb{Z}_{20}\). What is their relationship?

(v) Revisit the previous four questions under the factorization \(20 = 2 \cdot 10\).

Now consider two relatively prime positive integers \(a, b \in \mathbb{Z}_{\geq 2}\).
(i) Let $x$ be any integer and suppose $x \pmod{ab}$ is invertible. Prove that $x \pmod{a}$ and $x \pmod{b}$ are also invertible.

(ii) Assume that an integer $y$ is invertible modulo $a$ and modulo $b$. Prove that $y$ is then invertible modulo $ab$.

(iii) Conclude that there is a bijection between $\mathbb{Z}^\times_{ab}$ and $\mathbb{Z}^\times_a \times \mathbb{Z}^\times_b$.


**Exercise 6.2** (Orders, generators and the Diffie-Hellman key exchange). (10 points)

Let $G$ be a finite multiplicative commutative group and $g \in G$ an element. We define the subgroup generated by $g$ as

$$\langle g \rangle = \{1, g, g^2, g^3, \ldots \}$$

and the order of $g$ as $\# \langle g \rangle$.

(i) Prove that $\langle g \rangle$ is a group.

An element $g \in G$ that generates all of $G$, i.e. $\langle g \rangle = G$, is called a generator of $G$.

(i) Does every group have a generator?

**Alice** and **Bob** want to agree on a common key over an insecure channel. To do so, they want to perform a Diffie-Hellman key exchange in the group $\mathbb{Z}^\times_{20443}$. Please, help them:

(i) Find a generator for the group $\mathbb{Z}^\times_{20443}$. You can use the following theorem:

**Theorem 6.3.** An element $g \in \mathbb{Z}^\times_p$ is a generator of $\mathbb{Z}^\times_p$ if and only if

$$g^{(p-1)/t} \neq 1 \pmod{p}$$

for all prime divisors $t$ of $p - 1$. 
(ii) Next, ALICE chooses as her secret key $a = 257$ and BOB chooses as his secret key $b = 1280$. Both have to compute their public keys $A = g^a$ and $B = g^b$, respectively. Compute both using as few multiplications and squarings as possible. (Hint: Repeated Squaring.)

(iii) The values of $A$ and $B$ are sent over the insecure channel. ALICE computes as common key $k_{\text{ALICE}} = B^a$, while BOB computes $k_{\text{BOB}} = A^b$. Prove that $k_{\text{ALICE}} = k_{\text{BOB}}$.

(iv) Formulate the problem, that a passive attacker is facing. (What does she know and what does she want to compute?)

(v) Assume an active attacker in the middle of the communication channel. He can read and modify any messages sent over the channel. How can he trick ALICE and BOB into establishing a common key with him?