ETH Zürich, D-INFK
HS 2017, 13. November 2017

Prof. Ueli Maurer
Marta Mularczyk

Diskrete Mathematik
Solution 9

9.1 The group $\mathbb{Z}_m^*$

a) The order of the group $\langle \mathbb{Z}_{36}^*; \odot \rangle$ is $\varphi(36)$. By Lemma 5.12, $\varphi(36) = (2-1) \cdot 2^{2-1} \cdot (3-1) \cdot 3^{2-1} = 2 \cdot 2 \cdot 3 = 12$.

The group consists of all numbers in $\mathbb{Z}_{36}$ which are relatively prime with 36. Hence, $\mathbb{Z}_{36}^* = \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\}$.

b) By the Lagrange's Theorem, it follows that for any $a \in \mathbb{Z}_{11}^*$ we have $\mathrm{ord}(a) \in \{1, 2, 5, 10\}$. If a is a generator of $\mathbb{Z}_{11}^*$, then a has the order $10 = \varphi(11)$. This happens if and only if $a^2 \neq 1$ and $a^5 \neq 1$. By trying all the possibilities, we get that $2, 6, 7, 8$ are the generators of $\mathbb{Z}_{11}^*$.

The following lemma allows to solve this exercise for any group $\mathbb{Z}_m^*$, potentially even for very large m. We can prove the following lemma:

Lemma 1. Let g be a generator of $\mathbb{Z}_m^*$. Then the set of all generators of $\mathbb{Z}_m^*$ is

$$A = \{g^i \mid 1 \leq i < \varphi(m) \ \wedge \ \mathsf{gcd}(i, \varphi(m)) = 1\}$$

Proof: Let h be a generator of $\mathbb{Z}_m^*$. Since g is a generator, there exists a $1 \leq i < \varphi(m)$ such that $h = g^i$. Let $d = \gcd(i, \varphi(m))$. Then we have $h^{\frac{\varphi(m)}{d}} = (g^i)^{\frac{\varphi(m)}{d}} = g^{\varphi(m)\frac{i}{d}} = 1$. But since h is a generator, we must have $d = 1$. Therefore, every generator of $\mathbb{Z}_m^*$ is in A.

Let further $h \in A$. This means that there exists $1 \leq i < \varphi(m)$ such that $h = g^i$ und $\gcd(i, \varphi(m)) = 1$. It follows that $1 = h^{\mathrm{ord}(h)} = g^{i \cdot \mathrm{ord}(h)}$. Since g is a generator, $i \cdot \mathrm{ord}(h)$ is a multiple of $\varphi(m)$. Since $\gcd(i, \varphi(m)) = 1$, $\mathrm{ord}(h)$ is also a multiple of $\varphi(m)$. Hence, h is a generator of $\mathbb{Z}_m^*$. □

With the above lemma, it is enough to find one generator, namely 2. All the other generators can be computed as 2^i for $1 \leq i < \varphi(m)$.

c) Let $f : \mathbb{Z}_{nm}^* \to \mathbb{Z}_n^* \times \mathbb{Z}_m^*$ be defined as $f(x) = (R_n(x), R_m(x))$. We prove that f is an isomorphism. To this end, we first prove two lemmas.

Lemma 1. Let m and n be relatively prime. The function $f : \mathbb{Z}_{nm} \to \mathbb{Z}_n \times \mathbb{Z}_m$, defined as $f(x) = (R_n(x), R_m(x))$ is an injection.

Proof. Let $x \in \mathbb{Z}_{nm}$. By Lemma 4.17, $x \equiv_n R_n(x)$ and $x \equiv_m R_m(x)$. By the Chinese Remainder Theorem, we have that for any $(a, b) \in \mathbb{Z}_n \times \mathbb{Z}_m$, there exists exactly one $x \in \mathbb{Z}_{nm}$ such that $x \equiv_n a$ and $x \equiv_m b$. Hence, f is an injection. □

Lemma 2. Let n and m be integers. For any $a \in \mathbb{Z}$ we have

$$\gcd(a, nm) = 1 \implies \gcd(a, n) = 1 \wedge \gcd(a, m) = 1$$

Proof. Let $a \in \mathbb{Z}$ and assume that $\gcd(a, nm) = 1$. Let $\gcd(a, n) = d$ and $\gcd(a, m) = e$. From this we have $d \mid n$ and $e \mid m$. It follows that $d \mid nm$ and $e \mid nm$. Therefore, since d and e also divide a, d and e are both common divisors of a and nm. But by assumption that $\gcd(a, nm) = 1$, we get $d = e = 1$. □

With the above lemmas, we can now prove the statement.

We first show that f is well defined, that is, that $f(x) \in \mathbb{Z}_n^* \times \mathbb{Z}_m^*$ for all $x \in \mathbb{Z}_{nm}^*$. Let $x \in \mathbb{Z}_{nm}^*$. Then we have $\gcd(x, nm) = 1$. By **Lemma 2.**, it follows that $\gcd(x, n) = 1$ and $\gcd(x, m) = 1$. By Lemma 4.2, we have $\gcd(R_n(x), n) = 1$ and $\gcd(R_m(x), m) = 1$. Hence, $f(x) \in \mathbb{Z}_n^* \times \mathbb{Z}_m^*$.

Next we show that f is a bijection. By **Lemma 1.**, f is injective. Thus, $|f(\mathbb{Z}_{nm}^*)| = |\mathbb{Z}_{nm}^*|$. Since f is well defined, we have $f(\mathbb{Z}_{nm}^*) \subseteq \mathbb{Z}_n^* \times \mathbb{Z}_m^*$. By Lemma 5.12, we have $|\mathbb{Z}_{nm}^*| = |\mathbb{Z}_n^* \times \mathbb{Z}_m^*|$ and, thus, $f(\mathbb{Z}_{nm}^*) = \mathbb{Z}_n^* \times \mathbb{Z}_m^*$. Therefore, f is surjective.

Finally, we show that f is a homomorphism. Let $a, b \in \mathbb{Z}_{nm}^*$. By Lemma 4.18, we have

$$f(a \odot b) = (R_n(a \odot b), R_m(a \odot b)) \overset{Lem\ 4.18}{=} \big(R_n(R_n(a)R_n(b)), R_m(R_m(a)R_m(b))\big) = f(a) \odot f(b).$$

Hence, f is indeed an isomorphism.

d) The goal is to construct an isomorphism $\varphi : \mathbb{Z}_{15}^* \to \mathbb{Z}_{20}^*$. We will proceed in three steps, where we construct three isomorphisms: $\alpha : \mathbb{Z}_{15}^* \to \mathbb{Z}_3^* \times \mathbb{Z}_5^*$, $\beta : \mathbb{Z}_3^* \times \mathbb{Z}_5^* \to \mathbb{Z}_4^* \times \mathbb{Z}_5^*$ and $\gamma : \mathbb{Z}_4^* \times \mathbb{Z}_5^* \to \mathbb{Z}_{20}^*$. We then define φ as the composition of these isomorphisms: $\varphi = \gamma \circ \beta \circ \alpha$.

To construct α, we use Subtask a) and define $\alpha : a \mapsto (R_3(a), R_5(a))$. Further, let f be the isomorphism $f : \mathbb{Z}_{20}^* \to \mathbb{Z}_4^* \times \mathbb{Z}_5^*$, defined by $f : a \mapsto (R_4(a), R_5(a))$. We set $\gamma = f^{-1}$ (γ can be computed efficiently using the Chinese Remainder Theorem).

What is left is to find the isomorphism β. Note first that the function $g : \mathbb{Z}_3^* \to \mathbb{Z}_4^*$ defined by $g(1) = 1$ and $g(2) = 3$ is an isomorphism. The function g is trivially bijective. We also have $g(1 \odot 1) = 1 = g(1) \odot g(1)$, $g(2 \odot 1) = 3 = g(2) \odot g(1)$, $g(1 \odot 2) = 3 = g(1) \odot g(2)$ and $g(2 \odot 2) = 1 = g(2) \odot g(2)$. Therefore, g is also a homomorphism. Therefore, β defined by $\beta\big((a, b)\big) = \big(g(a), b\big)$ is an isomorphism.

Alternatively, one can find an isomorphism ψ using trial and error. However, in such case one has to prove that ψ is indeed an isomorphism.

9.2 RSA attack

First, consider the case when n_1, n_2 and n_3 are not relatively prime. Without loss of generality, assume that $\gcd(n_1, n_2) > 1$. We can now use the Extended GCD algorithm to compute $p = \gcd(n_1, n_2)$ and this way efficiently factorize n_1. This allows us to compute the secret key of Alice and decrypt c_1.

Secondly, assume that n_1, n_2 and n_3 are relatively prime. Consider the following system of congruence equations:

$$\begin{aligned} x &\equiv c_1 \pmod{n_1} \\ x &\equiv c_2 \pmod{n_2} \\ x &\equiv c_3 \pmod{n_3} \end{aligned}$$

Let $N = n_1 n_2 n_3$. Using the Chinese Remainder Theorem, we can efficiently find the solution x_0 to the above system of equations, such that $0 \le x_0 < N$.

Notice now that m^3 is also a solution to the system of equations, because $c_i \equiv m^3 \pmod{n_i}$ for $i \in \{1, 2, 3\}$. Moreover, since $0 \le m < n_i$ for $i \in \{1, 2, 3\}$, we have $0 \le m^3 < n_1 \cdot n_2 \cdot n_3 =$

N. Since by the Chinese Remainder Theorem x_0 is unique in $\{0,\ldots,N-1\}$, it follows that $x_0 = m^3$.

What is left is to compute the cube root of x_0 over $\mathbb{Z}$, which can be done efficiently.

Note: This attack is also possible for $e > 3$. However, for given e one needs e ciphertexts, each encrypted for a different recipient.

9.3 Elementary properties of rings

a) We have

$$(-a)b + ab \overset{\text{distrib.}}{=} (-a+a)b \overset{\text{def. inverse}}{=} 0b \overset{\text{Lemma 5.17 (i)}}{=} 0.$$

(1 Point)

Therefore, $(-a)b$ is the additive inverse of ab, which means that $(-a)b = -ab$. *(1 Point)*

b) We have

$$\begin{aligned}(-a)(-b) + (-(ab)) &\overset{\text{a)}}{=} (-a)(-b) + (-a)b \overset{\text{distrib.}}{=} (-a)(-b+b)\\ &\overset{\text{def. inverse}}{=} (-a)0 \overset{\text{Lemma 5.17 (i)}}{=} 0.\end{aligned}$$

(2 Points)

Therefore, $(-a)(-b)$ is the additive inverse of ab, which means that $(-a)(-b) = ab$. *(1 Point)*

9.4 Properties of commutative rings

a) From $a|b$ it follows that $\exists d\ b = ad$ and, thus, $bc = (ad)c = a(dc)$. Hence, $a|bc$.

b) From $a|b$ it follows that $\exists d\ b = ad$ and from $a|c$ it follows that $\exists e\ c = ae$. By the distributive law, we have $b + c = ad + ae = a(d+e)$. Hence, $a|(b+c)$.

9.5 System of linear equations

In order to solve the system of equations, we can use Gaussian elimination over F. The system can be expressed as the following matrix:

$$\begin{bmatrix} A & B & B & A \\ 1 & A & 1 & 0 \\ B & B & 1 & 1 \end{bmatrix}$$

First of all, we multiply the first row by the multiplicative inverse of A, namely by B. We obtain:

$$\begin{bmatrix} 1 & A & A & 1 \\ 1 & A & 1 & 0 \\ B & B & 1 & 1 \end{bmatrix}$$

Note first that in F every element is its own additive inverse. Therefore, subtraction (formally, it means adding the inverse of an element) is the same operation as addition.

We can now eliminate the variable x from the second row, by subtracting the first row. That is, we add the first row to the second row and obtain $\begin{bmatrix}0, & 0, & B, & 1\end{bmatrix}$. We can also eliminate x from the third row by adding the first row multiplied by B:

$$\begin{bmatrix}B + (B \cdot 1), & B + (B \cdot A), & 1 + (B \cdot A), & 1 + (B \cdot 1)\end{bmatrix} = \begin{bmatrix}0, & A, & 0, & A\end{bmatrix}$$

After swapping the third and the second row, we now get the following matrix:

$$\begin{bmatrix} 1 & A & A & 1 \\ 0 & A & 0 & A \\ 0 & 0 & B & 1 \end{bmatrix}$$

We multiply the second row by the multiplicative inverse of A and get and the third row by the multiplicative inverse of B and get:

$$\begin{bmatrix} 1 & A & A & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & A \end{bmatrix}$$

From the second and third rows we have $z = A$ and $y = 1$. Further, from the first row we get $x = 1 - (A \cdot y) - (A \cdot z) = 1 + A \cdot (y + z) = 1 + A \cdot B = 0$. Hence, the solution is $x = 0$, $y = 1$ and $z = A$.