Cryptographic passports & biometrics, summer 2009

Michael Nüsken, Konstantin Ziegler

2. Exercise sheet
Hand in solutions until Monday, 27 April 2009.

Any claim needs a proof or argument.

Exercise 2.1 (Tool: Groups). (6 points)

Consider the *additive group* $\mathbb{Z}_N^+ := (\mathbb{Z}_N, +)$ of the ring $\mathbb{Z}_N = (\mathbb{Z}_N, +, \cdot)$ of integers modulo N and for a prime p the *unit group* $\mathbb{Z}_p^\times := (\mathbb{Z}_p^\times, \cdot)$ of the ring $\mathbb{Z}_p = (\mathbb{Z}_p, +, \cdot)$ of integers modulo N. Compute (fast):

(i) $17 + 13$ in $\mathbb{Z}_{21}^+$.

(ii) $17 \cdot 13$ in $\mathbb{Z}_{67}^\times$. $\boxed{1}$

(iii) -5 in $\mathbb{Z}_{15}^+$. $\boxed{1}$

(iv) 5^{-1} in $\mathbb{Z}_{19}^\times$. $\boxed{2}$

(v) $17 \cdot 5 := \underbrace{5 + \cdots + 5}_{17}$ in $\mathbb{Z}_{12}^+$. (Note that there is *no* multiplication available!) $\boxed{1}$

(vi) $5^{17} := \underbrace{5 \cdot \ldots \cdot 5}_{17}$ in $\mathbb{Z}_{19}^\times$. $\boxed{1}$

Exercise 2.2 (Tool: Euclid). (6 points)

Consider the integers modulo 42.

(i) Decide whether $a = 10$ and $b = 11$ have a multiplicate inverses in $(\mathbb{Z}_{42}, \times)$. $\boxed{2}$

(ii) Compute an integer k, s.t. $\boxed{2}$

$$17 \cdot k = 5 \text{ in } \mathbb{Z}_{42}.$$

(iii) Compute an integer k, s.t. $\boxed{2}$

$$17^k = 5 \text{ in } \mathbb{Z}_{42}.$$

Exercise 2.3 (Tool: Groups). (9 points)

In this exercise you will get comfortable with the concept of a group. Always remember: Don't PANIC. Which of the following sets, together with the given operation form a group? Check for each property (Proper, Associative, Neutral, Inverse, Commutative) if it is well-defined, and if so if it is fulfilled or not:

1 (i) $(\mathbb{Z}, -)$: The integers $\mathbb{Z}$ with subtraction.

1 (ii) $(\mathbb{N} \setminus \{0\}, \hat{\ })$: The positive integers $\mathbb{N} \setminus \{0\}$ with exponentiation.

1 (iii) $(\mathbb{B}, \vee)$: The set $\mathbb{B} := \{\top, \bot\}$ with operation $\vee$ (the logical OR), defined as:

$\vee$	$\top$	$\bot$
$\top$	$\top$	$\top$
$\bot$	$\top$	$\bot$

1 (iv) $(4\mathbb{Z}+1, \cdot)$: The set $4\mathbb{Z}+1 := \{z \in \mathbb{Z} \mid z = 1 \text{ in } \mathbb{Z}_4\}$ with multiplication.

2 (v) The elliptic curve $E \colon y^2 = x^3 + x$ has four points over $\mathbb{F}_3$. Namely we have $E = \{(0,0), (-1,1), (-1,-1), \mathcal{O}\}$. We define an addition on E via the following table:

$+$	$\mathcal{O}$	$(0,0)$	$(-1,1)$	$(-1,-1)$
$\mathcal{O}$	$\mathcal{O}$	$(0,0)$	$(-1,1)$	$(-1,-1)$
$(0,0)$	$(0,0)$	$\mathcal{O}$	$(-1,-1)$	$(-1,1)$
$(-1,1)$	$(-1,1)$	$(-1,-1)$	$(0,0)$	$\mathcal{O}$
$(-1,-1)$	$(-1,-1)$	$(-1,1)$	$\mathcal{O}$	$(0,0)$

1 (vi) $(\mathcal{S}(\mathbb{Z}_{13}), \circ)$: The set $\mathcal{S}(\mathbb{Z}_{13}) := \{f : \mathbb{Z}_{13} \to \mathbb{Z}_{13} \mid f \text{ bijective}\}$ with concatenation $\circ$.

1 (vii) $(\mathrm{GL}(\mathbb{Z}_{13}), \cdot)$: The set $\mathrm{GL}(\mathbb{Z}_{13})$ of all invertible 2×2-matrices having entries from $\mathbb{Z}_{13}$ and matrix multiplication $\cdot$ as operation.

1 (viii) $(\mathbb{Z}_3^2, \square)$: The set $\mathbb{Z}_3^2 := \{(a,b) \mid a \in \mathbb{Z}_3, b \in \mathbb{Z}_3\}$ with the following operation $\square$:

$$\square\colon \begin{array}{ccc} \mathbb{Z}_3^2 \times \mathbb{Z}_3^2 & \longrightarrow & \mathbb{Z}_3^2, \\ (a,b),(c,d) & \longmapsto & (ac+bd, ad+bc) \end{array}$$