The electronic health card, summer 2008

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

3. Exercise sheet
Hand in solutions until Monday, 5 May 2008.

Exercise 3.1 (Science). (7+1 points)

(i) Count the number of elements in $\mathbb{Z}_4^\times$, in $\mathbb{Z}_9^\times$, and in $\mathbb{Z}_{25}^\times$, respectively. $\boxed{1}$
Do you recognize a pattern? Can you prove your guess? $\boxed{+1}$

(ii) Prove that there are exactly 40 invertible elements in $\mathbb{Z}_{100}$. $\boxed{1}$

(iii) Prove with the help of Euler's theorem and Fermat's little theorem that we have the equation $\boxed{2}$

$$3^{3^{160}} = 3 \text{ in } \mathbb{Z}_{101}.$$

(iv) Prove that we have the equation $\boxed{3}$

$$3^{2^{160}} = 3^{76} \text{ in } \mathbb{Z}_{101}.$$

Exercise 3.2 (Visual Chinese Remainder Theorem). (4+2 points)

(i) Consider $21 = 3 \cdot 7$ and, as we did in the course, produce a table indicating the relation betweeen $\mathbb{Z}_{21}$ and $\mathbb{Z}_7 \times \mathbb{Z}_3$. $\boxed{1}$

(ii) Pick two elements $x, y \in \mathbb{Z}_{21}$ (to make it interesting: the sum of the representing integers shall be larger than 21). First, add them in $\mathbb{Z}_{21}$ and then map to $\mathbb{Z}_7 \times \mathbb{Z}_3$. Second, map both to $\mathbb{Z}_7 \times \mathbb{Z}_3$ and add afterwards. What do you observe? $\boxed{1}$

(iii) Pick two elements $x, y \in \mathbb{Z}_{21}$ (to make it interesting: the product of the representing integers shall be larger than 21). First, multiply them in $\mathbb{Z}_{21}$ and then map to $\mathbb{Z}_7 \times \mathbb{Z}_3$. Second, map both to $\mathbb{Z}_7 \times \mathbb{Z}_3$ and multiply afterwards. What do you observe? $\boxed{1}$

(iv) Mark all the invertible elements in $\mathbb{Z}_7$, $\mathbb{Z}_3$, and $\mathbb{Z}_{21}$. Do you note a relationship? $\boxed{1}$

Now consider $a, b \in \mathbb{Z}_{\geq 2}$ coprime.

(v) Suppose you are given $x \bmod ab, y \bmod ab \in \mathbb{Z}_{ab}$. Prove that $\boxed{+2}$

$$(xy \bmod a, xy \bmod b) = ((x \bmod a) \cdot (y \bmod a), (x \bmod b) \cdot (y \bmod b)) .$$

(You might want to do, say, the first component first.) For short: the map $\mathbb{Z}_{ab} \to \mathbb{Z}_a \times \mathbb{Z}_b,\ x \bmod ab \mapsto (x \bmod a, x \bmod b)$ preserves the multiplication.

Exercise 3.3 (Touching $\mathbb{F}_4$). (4+4 points)

Consider polynomials of degree less than 2 over the field $\mathbb{F}_2$. Define addition and multiplication of them modulo the polynomial $X^2 + X + 1$.

$\boxed{1}$ (i) Write down the complete list of elements.

$\boxed{1}$ (ii) Write down the addition table.

$\boxed{2}$ (iii) Write down the multiplication table.

We can now consider polynomials over $\mathbb{F}_4$: $T^2 + T + 1$ is such a polynomial.
$\boxed{+4}$ Factor it (over $\mathbb{F}_4$).

Exercise 3.4 (Computing in $\mathbb{F}_{256}$). (0+4 points)

Let M be your student id. Let

$$a = M \operatorname{rem} 256, b = (M \operatorname{quo} 256) \operatorname{rem} 256, \text{ and } c = (a + b) \operatorname{rem} 256$$

Now interpret a, b and c as elementes of $\mathbb{F}_{256} = \mathbb{F}_2[X]/\left\langle X^8 + X^4 + X^3 + X + 1 \right\rangle$, just as in AES. Compute in $\mathbb{F}_{256}$

$\boxed{+1}$ (i) $a + b$ (Attention! Usually the result will not be c!),

$\boxed{+1}$ (ii) $a \cdot b$, and

$\boxed{+2}$ (iii) $1/a$ (or $1/b$ in case $a = 0$).

Note: If $x = x_1 \cdot 256 + x_0$, $0 \leq x_0 < 256$, then $x \operatorname{quo} 256 = x_1$ and $x \operatorname{rem} 256 = x_0$.