Security on the Internet, summer 2007
MICHAEL NÜSKEN

5. Exercise sheet
Hand in solutions until Thursday, 10 Mai 2007.

Any claim needs a proof or an argument.

Exercise 5.1 (The group of invertible elements). (12+4 points)

List the elements of and count the group

(i) $\mathbb{Z}_2^\times$, (iii) $\mathbb{Z}_4^\times$, (v) $\mathbb{Z}_8^\times$, (vii) $\mathbb{Z}_{12}^\times$,

(ii) $\mathbb{Z}_3^\times$, (iv) $\mathbb{Z}_5^\times$, (vi) $\mathbb{Z}_{10}^\times$, (viii) $\mathbb{Z}_{15}^\times$.

(ix) Consider all previous examples as vertices of a graph, arrange them nicely and draw green lines when the moduli divide and no other vertex fits inbetween. [If, say, you have the nodes $\mathbb{Z}_3$, $\mathbb{Z}_9$, $\mathbb{Z}_{18}$ it is enough to draw a line from $\mathbb{Z}_3$ to $\mathbb{Z}_9$ and one from $\mathbb{Z}_9$ to $\mathbb{Z}_{18}$. The connection $\mathbb{Z}_3$ to $\mathbb{Z}_{18}$ is already represented by the two lines.] $\boxed{2}$

(x) Add blue lines similarly when the sizes of the multiplicative groups divide. $\boxed{2}$

(xi) Explain how this continues... $\boxed{+4}$

Exercise 5.2 (Remainders). (5+1 points)

Consider rings $\mathbb{Z}_{mn}$ with the following pairs (m, n). In each case make a table with $\mathbb{Z}_m$ on one axis and $\mathbb{Z}_n$ on the other, then write each number $a \in \mathbb{Z}_{mn}$ at position $(a \operatorname{mod} m, a \operatorname{mod} n)$ as in this example:

$\mathbb{Z}_2 \backslash \mathbb{Z}_3$	0	1	2
0	0	4	2
1	3	1	5

(i) $(m, n) = (2, 4)$, (iii) $(m, n) = (4, 6)$,

(ii) $(m, n) = (3, 5)$, (iv) $(m, n) = (3, 8)$.

(v) In which of the previous cases do the numbers fill the entire table? When do they not collide? $\boxed{1}$

(vi) Give a simple criterion on (m, n) to tell when the numbers fill the table. $\boxed{+1}$

Exercise 5.3 (MuPAD and finite rings). (8+4 points)

The computer algebra system MuPAD is able to handle all these things. It is installed on the b-it computers and you can download it from the MuPAD webpage and ask for a 30-day trial key at the webpage `http://www.mupad.de/download/`.

$\boxed{1}$ (i) Try this:

```
F5:=Dom::GaloisField(5);
a:=F5(3);
b:=F5(-1);
a+b;
a*b;
1/a;

F2:=Dom::GaloisField(2);
FX:=Dom::UnivariatePolynomial( X, F2 );
m:=FX(X^8+X^4+X^3+X+1);
f:=FX(X^6+X^2+1);
g:=FX(X^3+X+1);
f+g;
f*g;
gcd(f,g);
(f*g) mod m;
divide(f*g, m, Rem);
```

Hint: if you mark a word and press F2 you get help on the marked part. (You can also type `?divide` to get help.)

$\boxed{4}$ (ii) Use MuPAD to find the complete factorization of $X^i - 1 \in \mathbb{F}_2[X]$ for each $i \in \mathbb{N}'_{<16}$.

$\boxed{3}$ (iii) Look at the result to see for which degrees an irreducible factor occurs in the above list. [For automating this task consider the MuPAD help on `Factored`, further `map` and `{op(`*expression*`)}` may be helpful.]

$\boxed{+4}$ (iv) Use `Dom::AlgebraicExtension` to define $\mathbb{F}_{256}$. Check your solution of Exercise 4.4. [Also `Dom::GaloisField` allows the definition of $\mathbb{F}_{256}$ with a given polynomial. Can you spot differences?]