Cryptology, homework sheet 2
Due: 22 September 2016, 10:45 for students of 2MMC10 and
06 October 2016, 10:45 for students following the MasterMath course.

2MMC10: Please hand in your homework in groups of two or three. To submit your homework, place it on the table of the lecturer *before* the lecture.

Mastermath: Instructions on how to submit will follow. Please team up in groups of 2 or 3.

Please write the names and student numbers on the homework sheet. Please indicate your home university and study direction.
This time one-line answers using a computer algebra system do *not* count. But it is a good moment to familiarize yourself with some system(s) so that you know how to solve similar problems for real life examples and to verify your answers. You may use a computer algebra system to compute subresults, such as f div g and $f \cdot g$. See below for a description of the Extended Greatest Common Divisor Algorithm (XGCD).

1. Compute the extended gcd of 155 and 649 using XGCD.

2. Compute the extended gcd of $f(x) = x^5 + 3x^3 + x^2 + 2x + 1$ and $g(x) = x^4 - 5x^3 - 5x^2 - 5x - 6$ in $\mathbb{Q}[x]$ using XGCD.

3. Consider the residue classes of $\mathbb{F}_2[x]$ modulo $f(x) = x^n + 1$ for some positive integer $n > 1$, i.e. $R = \mathbb{F}_2[x]/(x^n + 1)$. Note that R can be represented as
$$R = \left\{ a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1} \mid a_i \in \mathbb{F}_2 \right\}.$$
Show that R is not a field.
Hint: Find a non-zero element that is not invertible.

4. Let K be a field of characteristic p, where p is prime. Show that for any integer $n \geq 0$ one has
$$(a+b)^{p^n} = a^{p^n} + b^{p^n}$$
for all $a, b \in K$.
Hint: You can use the binomial theorem and use proof by induction.

5. Use the Rabin test (see below) to prove that $x^4 + x + 1$ is irreducible over $\mathbb{F}_2$. You should be able to do this exercise by hand. Please document the results of all steps in the algorithm and show how they were obtained.

Here is a description of XGCD. This description assumes that the input elements f, g live in some ring R in which the greatest common divisor is defined. We will usually use the XGCD on integers or polynomials. If the inputs are integers you can ignore the part the leading coefficient.

Algorithm 1 (Extended Euclidean algorithm)
IN: $f, g \in R$
OUT: $d, u, v \in R$ *with* $d = uf + vg$

1. $a \leftarrow [f, 1, 0]$
2. $b \leftarrow [g, 0, 1]$
3. `repeat`
   (a) $c \leftarrow a - (a[1] \operatorname{div} b[1])b$
   (b) $a \leftarrow b$
   (c) $b \leftarrow c$

   `while` $b[1] \neq 0$
4. $l \leftarrow LC(a[1])$, $a \leftarrow a/l$ */*LC = leading coefficient, this only applies to polynomials*/*
5. $d \leftarrow a[1]$, $u \leftarrow a[2]$, $v \leftarrow a[3]$
6. `return` d, u, v

In this algorithm, div denotes division with remainder. The first component of c is thus easier written as $c[1] \leftarrow a[1] \bmod b[1]$ but by operating on the whole vector we get to update the values leading to u and v, too. At each step we have

$$a[1] = a[2]f + a[3]g \text{ and } b[1] = b[2]f + b[3]g.$$

To see this, note that this holds trivially for the initial conditions. If it holds for both a and b then also for c since it computes a linear relation of both vectors. So each update maintains the relation and eventually when $b[1] = 0$, we have that $a[1]$ holds the previous remainder, which is the gcd of f and g. If the inputs are polynomials, at the end the gcd is made monic by dividing by the leading coefficient $LC(a[1])$.

Example 2 *Let* $R = \mathbb{R}[x]$ *and* $f(x) = x^5 + 3x^3 - x^2 - 4x + 1$, $g(x) = x^4 - 8x^3 + 8x^2 + 8x - 9$. *So at first we have* $a = [f, 1, 0], b = [g, 0, 1]$.

We have $(a[1] \operatorname{div} b[1]) = x + 8$ *and so end the first round with*

$$\begin{aligned} a &= [g, 0, 1], \\ b &= [59x^3 - 73x^2 - 59x + 73, 1, -x - 8]. \end{aligned}$$

Indeed $b[1] = f(x) + (-x - 8)g(x)$.

With these new values we have $(a[1] \operatorname{div} b[1]) = 1/59x - 399/3481$ *and so the second round ends with*

$$\begin{aligned} a &= [59x^3 - 73x^2 - 59x + 73, 1, -x - 8], \\ b &= [2202/3481x^2 - 2202/3481, -1/59x + 399/3481, 1/59x^2 + 73/3481x + 289/3481]. \end{aligned}$$

In the third round we have $(a[1] \operatorname{div} b[1]) = 205379/2202x - 254113/2202$ *and obtain*

$$\begin{aligned} a &= [2202/3481x^2 - 2202/3481, -1/59x + 399/3481, 1/59x^2 + 73/3481x + 289/3481], \\ b &= [0, 3481/2202x^2 - 13924/1101x + 10443/734, -3481/2202x^3 - 6962/1101x + 3481/2202]. \end{aligned}$$

Since $b[1] = 0$ *the loop terminates. We have* $LC(a[1]) = 2202/3481$ *and thus normalize to*

$$a = [x^2 - 1, -59/2202x + 133/734, 59/2202x^2 + 73/2202x + 289/2202].$$

We check that indeed

$$\begin{aligned} x^2 - 1 = {} & (-59/2202x + 133/734)(x^5 + 3x^3 - x^2 - 4x + 1) + \\ & (59/2202x^2 + 73/2202x + 289/2202)(x^4 - 8x^3 + 8x^2 + 8x - 9). \end{aligned}$$

Here is a formal statement of the Rabin test:

Lemma 3 (Rabin test)
The polynomial $f(x) \in \mathbb{F}_q[x]$ *of degree* $\deg(f) = m$ *is irreducible if and only if*

$$f(x) | x^{q^m} - x$$

and for all primes $d < m$ *dividing* m *one has*

$$\gcd(f(x), x^{q^d} - x) = 1.$$