Rick Staals and Erwin van Duijnhoven (0716184, 0719562)

2WC09- Cryptography 1

Homework sheet 4

October 2, 2013

The input is two elements f and g. The steps of the algorithm is given in the form of a table containing a and b as in Algorithm 1. The answers are given as d, u and v as in Algorithm 1, i.e. $d = \gcd(f, g)$, and $d = u \cdot f + v \cdot g$. In exercise 3 and 4, the last step (4 in both cases) is the normalization step, i.e. $a \leftarrow \frac{a}{l}$ with $l = LC(a[1])$, the leading coefficient of $a[1]$.

Question 1

Compute the extended gcd of 155 *and* 649 *using Algorithm 1.*

Step	a	b
0	[155,1,0]	[649,0,1]
1	[649,0,1]	[155,1,0]
2	[155,1,0]	[29,-4,1]
3	[29,-4,1]	[10,21,-5]
4	[10,21,-5]	[9,-46,11]
5	[9,-46,11]	[1,67,-16]
6	[1,67,-16]	[0,-649,155]

So $d = 1, u = 67$ and $v = -16$.

Question 2

Compute the extended gcd of 5007 *and* 6891 *using Algorithm 1.*

Step	a	b
0	[5007,1,0]	[6891,0,1]
1	[6891,0,1]	[5007,1,0]
2	[5007,1,0]	[1884,-1,1]
3	[1884,-1,1]	[1239,3,-2]
4	[1239,3,-2]	[645,-4,3]
5	[645,-4,3]	[594,7,-5]
6	[594,7,-5]	[51,-11,8]
7	[51,-11,8]	[33,128,-93]
8	[33,128,-93]	[18,-139,101]
9	[18,-139,101]	[15,267,-194]
10	[15,267,-194]	[3,-406,295]
11	[3,-406,295]	[0,2297,-1669]

So $d = 3, u = -406$ and $v = 295$.

Question 3

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 Algorithm 1.*

Step	a	b
0	$[x^5+3x^3+x^2+2x+1,1,0]$	$[x^4-5x^3-5x^2-5x-6,0,1]$
1	$[x^4-5x^3-5x^2-5x-6,0,1]$	$[33x^3+31x^2+33x+31,1,-x-5]$
2	$[33x^3+31x^2+33x+31,1,-x-5]$	$[-\frac{458x^2}{1089}-\frac{458}{1089},\frac{196}{1089}-\frac{x}{33},\frac{x^2}{33}-\frac{31x}{1089}+\frac{109}{1089}]$
3	$[-\frac{458x^2}{1089}-\frac{458}{1089},\frac{196}{1089}-\frac{x}{33},\frac{x^2}{33}-\frac{31x}{1089}+\frac{109}{1089}]$	$[0,-\frac{1089\left(x^2-5x-6\right)}{458},\frac{1089\left(x^3+2x+1\right)}{458}]$
4	$[x^2+1,\frac{1}{458}\left(33x-196\right),-\frac{1}{458}\left(33x^2-31x+109\right)]$	$[0,-\frac{1089\left(x^2-5x-6\right)}{458},\frac{1089\left(x^3+2x+1\right)}{458}]$

So $d = x^2+1, u = \frac{1}{458}\left(33x-196\right)$ and $v = -\frac{1}{458}\left(33x^2-31x+109\right)$.

Question 4

Compute the extended gcd of $f(x) = x^{11}+x^9+x^7+x^4+x^3+x+1$ *and* $g(x) = x^8+x^5+x^4+x^3+x+1$ *in* $\mathbb{F}_2[x]$ *using Algorithm 1.*

Step	a	b
0	$[x^{11}+x^9+x^7+x^4+x^3+x+1,1,0]$	$[x^8+x^5+x^4+x^3+x+1,0,1]$
1	$[x^8+x^5+x^4+x^3+x+1,0,1]$	$[x^3+x^2+x,1,x^3+x+1]$
2	$[x^3+x^2+x,1,x^3+x+1]$	$[x^2+x+1,x^5+x^4+x,x^8+x^7+x^6+x^2+x+1]$
3	$[x^2+x+1,x^5+x^4+x,x^8+x^7+x^6+x^2+x+1]$	$[0,x^6+x^5+x^2+1,x^9+x^8+x^7+x^2+1]$
4	$[x^2+x+1,x^5+x^4+x,x^8+x^7+x^6+x^2+x+1]$	$[0,x^6+x^5+x^2+1,x^9+x^8+x^7+x^2+1]$

So $d = x^2+x+1, u = x^5+x^4+x$ and $v = x^8+x^7+x^6+x^2+x+1$.