Manuel Kauers
RISC-Linz

Hagenberg, January 7, 2003

Computer Algebra Exercises
Solution 5

Ex. (22) We are about to compute the bivariate gcd of f and g where

$$f(x,y) = y^6 + xy^5 + x^3y - xy + x^4 - x^2$$
$$g(x,y) = xy^5 - 2y^5 + x^2y^4 - 2xy^4 + xy^2 + x^2y.$$

Let's take y as main variable, i.e. let's write

$$f(x,y) = y^6 + xy^5 + (x^3 - x)y + (x^4 - x^2)$$
$$g(x,y) = (x-2)y^5 + (x^2 - 2x)y^4 + xy^2 + x^2y.$$

We find $M := 1 + \min(\deg_y(f), \deg_y(g)) = 5$.

r	$f(x,r)$	$g(x,r)$	gcd	g
1	$x^4 + x^3 - x^2 + 1$	$-2x^2 - 2$	$x+1$	$x+1$
2	$x^4 + 2x^3 - x^2 + 30x + 64$	$18x^2 + 4x - 64$	$x+2$	$x+y$
3	$x^4 + 3x^3 - x^2 + 240x + 729$	$84x^2 + 90x - 486$	$x+3$	$x+y$
4	$x^4 + 4x^3 - x^2 + 1\,020x + 4\,096$	$260x^2 + 528x - 2\,048$	$x+4$	$x+y$
5	$x^4 + 5x^3 - x^2 + 3\,120x + 15\,625$	$630x^2 + 1\,900x - 6\,250$	$x+5$	$x+y$

We verify that $x + y \mid f(x,y)$ and $x + y \mid g(x,y)$ and thus find

$$\gcd(f(x,y), g(x,y)) = x + y.$$

Ex. (26)

```
squarefree := proc(poly, p)
local a, Da, l, i, j, l1, l2, r, f, g, trash;

  a := poly; Da := diff(a, x) mod p;
  g := Gcd(a, Da) mod p; r := [];

  if a = 0 or degree(a) = 0 then
    r := [[a,1]];
  elif g = 1 or g = a then
     if Da = 0 then
       l := sf1(subs(x=x^(1/p), a), p);
       for f in l do
         r := [op(r), [f[1], f[2] * p]];
       od;
     else
       r := [[a,1]];
     fi;
  else
```

```
    l1 := sf1(Quo(a, g, x, 'trash') mod p, p); l2 := sf1(g, p);
    l := [[1,i] $ i=1..(max(l1[j][2] $j=1..nops(l1)) +
                        max(l2[j][2] $j=1..nops(l2)))];
    for i from 1 to nops(l1) do
      for j from 1 to nops(l2) do
        g := Gcd(l1[i][1], l2[j][1]) mod p;
        if not g = 1 then
          l1[i][1] := Quo(l1[i][1], g, x, 'trash') mod p;
          l2[j][1] := Quo(l2[j][1], g, x, 'trash') mod p;
          l[l1[i][2] + l2[j][2]][1] := l[l1[i][2] + l2[j][2]][1] * g;
        fi;
      od;
      l[l1[i][2]][1] := l[l1[i][2]][1] * l1[i][1];
    od;
    for j from 1 to nops(l2) do
      l[l2[j][2]][1] := l[l2[j][2]][1] * l2[j][1];
    od;
    for f in l do
      if not f[1] = 1 then
        r := [op(r), f];
      fi;
    od;
  fi;
  r;
end;
```

Using this procedure, we obtain

```
>> squareFree(x^7+x^5+x^4+x^3+x^2+1, 3);
```

$$(x+2)^2(x+1)^5$$

and indeed

```
>> expand(%) mod 3;
```

$$x^7 + x^5 + x^4 + x^3 + x^2 + 1$$

Ex. (27) Let $a(x) = x^6 + 2x^4 + x^2 + 2$.

a) Squarefree decomposition of a in $\mathbb{Q}[x]$:

$$\gcd(a, a') = \gcd(x^6 + 2x^4 + x^2 + 2, 6x^5 + 8x^3 + 2x) = 1,$$

so a is already squarefree and we are done.

b) Squarefree decomposition of a in $\mathbb{Z}_5[x]$.

$$\gcd(a, a') = \gcd(x^6 + 2x^4 + x^2 + 2, x^5 + 3x^3 + 2x) = x^2 + 2$$

We apply the decomposition algorithm recursively to $a_1 := x^2 + 2$ and $a_2 := a/(x^2 + 2)$. By

$$\gcd(a_1, a_1') = \gcd(x^2 + 2, 2x) = 1,$$
$$\gcd(a_2, a_2') = \gcd(x^4 + 1, 4x^3) = 1.$$

we see that both a_1 and a_2 are squarefree. For the combination of the two results, we note that

$$\gcd(a_1, a_2) = \gcd(x^2 + 2, x^4 + 1) = x^2 + 2,$$

such that by $(x^4 + 1)/(x^2 + 2) = x^2 + 3$ we finally get

$$a = (x^2 + 3) \cdot (x^2 + 2)^2$$

as square free decomposition of a in $\mathbb{Z}_5[x]$.

Ex. (28) In order to factor $a(x) = a^6 + 2x^4 + x^2 + 2 \in \mathbb{Z}_5[x]$, we have to factor both square free parts separately (cf. Ex. 27).

First, we factor $a_1(x) = x^2 + 3$: By

$$1 \bmod x^2 + 3 = 1$$
$$x^5 \bmod x^2 + 3 = 4x$$

we obtain

$$Q - I = \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 3 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

and hence $\text{Rank}(Q - I) = 2 - 1 = 1$, such that $x^2 + 3$ is irreducible in $\mathbb{Z}_5[x]$.

Analogously, we factor $a_2(x) = x^2 + 2$: By

$$1 \bmod x^2 + 2 = 1$$
$$x^5 \bmod x^2 + 2 = 4x$$

such that $x^2 + 3$ must also be irreducible.

Putting things together, we obtain the factorization $a(x) = (x^2+3)\cdot(x^2+2)^2$.

Ex. (29) Factor $a(x) = x^6 + 2x^4 + x^2 + 2$ over $\mathbb{Q}$ by Berlekamp-Hensel assuming that the coefficients are bounded by 10. By Exercise 27, we know that a is squarefree over $\mathbb{Z}[x]$.

First, we have to choose a prime p such that a is squarefree in $\mathbb{Z}_p[x]$. The exercise text suggests to take $p = 5$, but this is impossible since $a \bmod 5$ is not squarefree, see Exercise 27. We take $p = 3$ instead, which is possible because

$$\gcd(a, a') = \gcd(x^6 + 2x^4 + x^2 + 2, 2x^3 + 2x) = 1$$

in $\mathbb{Z}_3[x]$ such that a must be squarefree there.

In the next step, we have to factor a in $\mathbb{Z}_3[x]$ by the Berlekamp algorithm:

$$1 \bmod a = 1$$
$$x^3 \bmod a = x^3$$
$$x^6 \bmod a = x^4 + 2x^2 + 1$$
$$x^9 \bmod a = x$$
$$x^{12} \bmod a = x^4$$
$$x^{15} \bmod a = x^5 + 2x^3 + x$$

leads to

$$Q - I = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} - I = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 2 & 0 & 2 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$
$$\rightsquigarrow \begin{pmatrix} 0 & 1 & 0 & 2 & 0 & 2 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix},$$

such that the $\ker(Q - I)$ has the basis

$$\{1, x^3 + x, x^4, x^5 + x\}.$$

The first polynomial in the basis is trivial, the second one yields two factors:

$$\gcd(a, x^3 + x - 1) = x^3 + x + 2,$$
$$\gcd(a, x^3 + x - 2) = x^3 + x + 1.$$

But we expect four factors, so we proceed and obtain

$$\gcd(x^3 + x + 2, x^4 - 1) = x + 1,$$
$$\gcd(x^3 + x + 2, x^4 - 2) = x^2 + 2x + 2,$$
$$\gcd(x^3 + x + 1, x^4 - 1) = x + 2,$$
$$\gcd(x^3 + x + 1, x^4 - 2) = x^2 + x + 2.$$

These are the four irreducible factors of a in $\mathbb{Z}_3[x]$, i.e.

$$a(x) = (x + 1)(x + 2)(x^2 + 2x + 2)(x^2 + x + 2)$$

in $\mathbb{Z}_3[x]$.

We are interested in a factorization of a in $\mathbb{Z}[x]$, so it remains to “lift” the above result to a factorisation in $\mathbb{Z}_{3^3}[x]$ (we make use of the knowledge that all coefficients are bounded by 10, cf. Exercise sheet). Let $a_1 = x + 1$, $a_2 = x + 2$, $a_3 = x^2 + 2x + 2$ and $a_4 = x^2 + x + 2$ and

$$a_2^* = \prod_{k=2}^{4} a_k = (x + 2)(x^2 + 2x + 2)(x^2 + x + 2) = x^5 + 2x^4 + x + 2,$$
$$a_3^* = \prod_{k=3}^{4} a_k = (x^2 + 2x + 2)(x^2 + x + 2) = x^5 + 2x^4 + x + 2,$$
$$a_4^* = \prod_{k=4}^{4} a_k = (x^2 + x + 2) = x^5 + 2x^4 + x + 2.$$

We compute the v_i to

$$
\begin{aligned}
1 &= (x^4+x^3+2x^2+x)\cdot\underbrace{(x+1)}_{=a_1}+2\cdot\underbrace{(x^5+2x^4+x+2)}_{=a_2^*} \\
x^4+x^3+2x^2+x &= (x^7+2x^6+x^5+2x^4+x^3+x)(x+2) \\
&\quad + (2x^4+2x^3+x^2+2x)(x^4+1) \\
&= (x^2+1)\cdot(x+2)+1\cdot(x^4+1) \\
x^4+1 &= (x^3+x^2+x+1)\cdot(x^2+2x+2) \\
&\quad + (2x^3+x^2+2x+1)\cdot(x^2+x+2) \\
&= (2x+1)(x^2+2x+2)+(x+1)(x^2+x+2),
\end{aligned}
$$

i.e. we obtain

$$(v_1,v_2,v_3,v_4)=(2,1,x+1,2x+1).$$

Set $k:=1$ and $(\bar{a}_1,\bar{a}_2,\bar{a}_3,\bar{a}_4):=(a_1,a_2,a_3,a_4)$. We now lift from $3=3^k$ to $3^{k+1}=9$.

$$
\begin{aligned}
\tilde{d} &= a-\prod_{i=1}^{r}\bar{a}_i \bmod p^2 = 3x^5+3x^4+6x^3+3x^2+3x \\
d &= \tilde{d}/p^1 = x^5+x^4+2x^3+x^2+x+1. \\
\bar{a}_1 &= \bar{a}_1+3\cdot(d\cdot b_1 \bmod a_1) = x+4 \\
\bar{a}_2 &= \bar{a}_2+3\cdot(d\cdot b_2 \bmod a_2) = x+5 \\
\bar{a}_3 &= \bar{a}_3+3\cdot(d\cdot b_3 \bmod a_3) = x^2+5x+8 \\
\bar{a}_4 &= \bar{a}_4+3\cdot(d\cdot b_4 \bmod a_4) = x^2+4x+8.
\end{aligned}
$$

Now, for $k:=2$ we lift from $9=3^k$ to $3^{k+1}=27$.

$$
\begin{aligned}
\tilde{d} &= a-\prod_{i=1}^{r}\bar{a}_i \bmod p^3 = 9x^5+18x^3+9x+18 \\
d &= \tilde{d}/9 = x^5+2x^3+x+2. \\
\bar{a}_1 &= \bar{a}_1+9\cdot(d\cdot b_1 \bmod a_1) = x+22 \\
\bar{a}_2 &= \bar{a}_2+9\cdot(d\cdot b_2 \bmod a_2) = x+5 \\
\bar{a}_3 &= \bar{a}_3+9\cdot(d\cdot b_3 \bmod a_3) = x^2+5x+26 \\
\bar{a}_4 &= \bar{a}_4+9\cdot(d\cdot b_4 \bmod a_4) = x^2+22x+26.
\end{aligned}
$$

Centering the representation around 0, we obtain

$$(\bar{a}_1,\bar{a}_2,\bar{a}_3,\bar{a}_4)=(x-5,x+5,x^2+5x-1,x^2-5x-1)$$

as result of the lifting process.

It remains to combine these factors to factors of a. None of the $\bar{v}_i$ is a factor of a by itself, but

$$\bar{a}_1\cdot\bar{a}_2 = x^2+2 \bmod 27$$

is a factor:

$$a=(x^2+2)(x^4+1).$$

This removes $\bar{a}_1$ and $\bar{a}_2$ from the candidate list. It remains to combine factors of $x^4 + 1$ out of $\bar{a}_3$ and $\bar{a}_4$. In fact, we already get

$$\bar{a}_3 \cdot \bar{a}_4 = x^4 + 1 \bmod 27.$$

Putting things together, we finally have the factorization

$$a = (x^2 + 2) \cdot (x^4 + 1).$$

Ex. (30) $\boxed{\textbf{to be}}$