Foundations of Computer Algebra: Hensel lifting

Marc Moreno Maza
University of Western Ontario
CS 424 / CS 556 – Winter 2006

January 7, 2008

1 Linear Diophantine Equations

Definition 1 *Let R be a commutative ring with identity element. A* linear Diophantine equation *over R is an equation of the form*

$$f_1 s_1 + \cdots + f_n s_n = a \tag{1}$$

where $f_1, \ldots, f_n, a$ are given in R and where $s_1, \ldots, s_n$ are unknowns in R.

Theorem 1 *Let R be an Euclidean domain and let $f, g, h, a \in R$ such that $h = \gcd(f, g)$. We consider the linear Diophantine equation*

$$sf + tg = a. \tag{2}$$

Then the following hold

(i) Equation (2) has a solution if and only if h divides a.

(ii) If $h \neq 0$ and if $(s_0, t_0) \in R^2$ is a solution of Equation (2) then every other solution is of the form

$$(s_0 + r\frac{g}{h}, t_0 - r\frac{f}{h}) \quad \text{where} \quad r \in R. \tag{3}$$

(*iii*) *If $R = F[x]$ where F is a field, $h \neq 0$, and if Equation (2) is solvable, and if we have*

$$\deg f + \deg g - \deg h > \deg a \tag{4}$$

then there is a unique solution $(s_0, t_0) \in R^2$ of Equation (2) such that

$$\deg s_0 < \deg g - \deg h \ \text{ and } \ \deg t_0 < \deg f - \deg h. \tag{5}$$

PROOF $\rhd$ First we prove (*i*). If $(s_0, t_0) \in R^2$ is a solution of Equation (2), then h which divides $s_0 f + t_0 g$, divides also a. Conversly, we assume that $h = \gcd(f, g)$ divides a. The claim is trivial if $h = 0$. (Indeed, this implies $f = g = 0$ and also $a = 0$.) Otherwise, let $(s_0, t_0) \in R^2$ be computed by the Extended Euclidean Algorithm applied to (f, g), such that we have $s_0 f + t_0 g = h$. Then $(s, t) = (s_0 a/h, t_0 a/h)$ is a solution of Equation (2).

Now we prove (*ii*). Assume $h \neq 0$ and let $(s_0, t_0) \in R^2$ is a solution of Equation (2). Since $h \neq 0$, then f/h and g/h are coprime. Let (s, t) be in R^2. Then we have

$$\begin{array}{lll}
sf + tg = a & \Longleftrightarrow & (s - s_0)f + (t - t_0)g = 0 \\
 & \Longleftrightarrow & (s - s_0)(f/h) = -(t - t_0)(g/h) \\
 & \Longleftrightarrow & (s - s_0)(f/h) = (t_0 - t)(g/h) \\
 & \Longleftrightarrow & (g/h) \mid (s - s_0) \ \text{ and } \ (f/h) \mid (t_0 - t) \\
 & \Longleftrightarrow & (\exists r \in R)\ (s - s_0) = r(g/h) \ \text{ and } \ (t_0 - t) = r(f/h) \\
 & \Longleftrightarrow & (\exists r \in R)\ s = s_0 + r(g/h) \ \text{ and } \ t = t_0 - r(f/h).
\end{array}$$

Finally, we prove (*iii*). Let $(s_1, t_1) \in R^2$ be a solution of Equation (2). Let q and t_0 be the quotient and the remainder of t_1 w.r.t. f/h. Hence we have

$$t_1 = f/hq + t_0 \ \text{ and } \ \deg t_0 < \deg f - \deg h. \tag{6}$$

We define

$$s_0 = s_1 + qg/h. \tag{7}$$

Observe that

$$(s_0, t_0) = (s_1, t_1) + q(g/h, -f/h)$$

solves Equation (2) too. By Relation (6) and by hypothesis we have

$$\deg(t_0 g) < \deg f + \deg g - \deg h \ \text{ and } \ \deg a < \deg f + \deg g - \deg h$$

leading to

$$\deg s_0 + \deg f = \deg s_0 f = \deg(a - t_0 g) < \deg f + \deg g - \deg h.$$

Therefore we have

$$\deg t_0 < \deg f - \deg h \ \text{ and } \ \deg s_0 < \deg g - \deg h.$$

This proves the existence. Let us prove the unicity. Let (s, t) be a solution of Equation (2). We know that there exists $r \in R$ such that $s = s_0 + rg/h$. Since $\deg s_0 < \deg g - \deg h$ holds, if $r \neq 0$, we have

$$\deg s \geq \deg(g/h) = \deg g - \deg h.$$

This implies the uniquemess. $\triangleleft$

Theorem 2 *Let R be a commutative ring with identity element and let $p \in R$. ...*

2 Linear Hensel Lifting

Theorem 3 *Let R be a commutative ring with identity element. Let f, g_0, h_0 be univariate polynomials in $R[x]$ and let $m \in R$. We assume that the following relation holds*

$$f \ \equiv \ g_0 \, h_0 \mod m \tag{8}$$

We assume also that g_0 and h_0 are relatively prime modulo m, that is there exists $s, t \in R$ such that

$$s g_0 + t h_0 \ \equiv \ 1 \mod m \tag{9}$$

Then, for every integer ℓ there exist $g^{(\ell)}, h^{(\ell)} \in R[x]$ such that we have

1. $f \ \equiv \ g^{(\ell)} h^{(\ell)} \mod m^{\ell}$,
2. $g_0 \ \equiv \ g^{(\ell)} \mod m$.

Proof $\triangleright$ We apply Theorem **??** with

$$\mathcal{I} = \langle m \rangle, \ n = 1, \ r = 2, \ f_1(x_1, x_2) = x_1 x_2 - f. \tag{10}$$

Thus we have

$$U \ = \ (u_{11} \ u_{12}) \ = \ (g_0 \ h_0) \tag{11}$$

Observe that this matrix is left-invertible modulo m if and only if g_0, h_0 are relatively prime modulo m. Indeed, the matrix U is left-invertible modulo m iff there exists a matrix

$$U^{-1} = \begin{pmatrix} s \\ t \end{pmatrix}$$

such that $U\,U^{-1} \;\equiv\; (1) \mod m$, that is

$$sg_0 + th_0 \;\equiv\; 1 \mod m \tag{12}$$

We prove now the claim of the theorem. Assume we have computed $g^{(\ell)}, h^{(\ell)} \in R$ such that $f \;\equiv\; g^{(\ell)}h^{(\ell)} \mod m^\ell$ and $g \;\equiv\; g^{(\ell)} \mod m$ hold. We want to compute $g^{(\ell+1)}, h^{(\ell+1)} \in R$. Let v be such that

$$f_1(g^{(\ell)}, h^{(\ell)}) = g^{(\ell)}h^{(\ell)} - f = vm^\ell \tag{13}$$

We look for $g_\ell, h_\ell \in R$ such that

$$g^{(\ell+1)} = g^{(\ell)} + g_\ell m^\ell \;\text{ and }\; h^{(\ell+1)} = h^{(\ell)} + h_\ell m^\ell \tag{14}$$

Following the proof of Theorem **??** we are led to solve the equation

$$v + g_\ell h_0 + h_\ell g_0 \equiv\; 0 \mod m \tag{15}$$

A solution of this equation is

$$\begin{pmatrix} g_\ell \\ h_\ell \end{pmatrix} = \begin{pmatrix} -sv \\ -tv \end{pmatrix} \tag{16}$$

This proves the claim of the theorem. $\triangleleft$

Remark 1 The proof of Theorem 3 provides a solution (g_ℓ, h_ℓ) to Equation (15). It is desirable to add constraints such that Equation (15) has a unique soulution. In particular, one would like to guarantee that for every integer ℓ the polynomials $g^{(\ell)}$ and g_0 have the same degree. As we shall see now, this problem was solved, in fact, by our preliminary study of *Linear Diophantine Equations.*

Theorem 4 *Let R be a commutative ring with identity element. Let f, g_0, h_0 be univariate* **monic** *polynomials in $R[x]$. Let $m \in R$ be such that R/m is a field. We assume that the following relation holds*

$$f \;\equiv\; g_0\, h_0 \mod m \tag{17}$$

and that g_0 and h_0 are relatively prime modulo m. Then, for every integer ℓ there exist **unique monic** *polynomials $g^{(\ell)}, h^{(\ell)} \in R[x]$ such that we have*

1. $f \equiv g^{(\ell)}h^{(\ell)} \mod m^{\ell}$,

2. $g_0 \equiv g^{(\ell)} \mod m$,

3. $h_0 \equiv h^{(\ell)} \mod m$.

Proof $\triangleright$ By induction on $\ell \geq 1$. The clain is clear for $\ell = 1$. So let us assume it is true for $\ell \geq 1$ and consider monic polynomials $g^{(\ell+1)}, h^{(\ell+1)} \in R[x]$ satisfying

$$f \equiv g^{(\ell+1)}h^{(\ell+1)} \mod m^{\ell+1} \tag{18}$$

and

$$g_0 \equiv g^{(\ell+1)} \mod m \text{ and } h_0 \equiv h^{(\ell+1)} \mod m. \tag{19}$$

Such polynomials $g^{(\ell+1)}, h^{(\ell+1)}$ exist by Theorem 3. (The fact that they can be chosen monic is left to the reader as an exercise.) Observe that we have

$$f \equiv g^{(\ell+1)}h^{(\ell+1)} \mod m^{\ell} \tag{20}$$

So the induction hypothesis leads to

$$g^{(\ell)} \equiv g^{(\ell+1)} \mod m^{\ell} \text{ and } h^{(\ell)} \equiv h^{(\ell+1)} \mod m^{\ell} \tag{21}$$

Hence there exist polynomials $q_g, q_h \in (R/m)[x]$ such that

$$g^{(\ell+1)} = g^{(\ell)} + m^{\ell} q_g \text{ and } h^{(\ell+1)} = h^{(\ell)} + m^{\ell} q_h. \tag{22}$$

Since f, g_0, h_0 are given to be monic, it is easy to prove that for $k \geq 1$ we have

$$\deg q_g < \deg g_0 \text{ and } \deg q_h < \deg h_0 \tag{23}$$

In addition, observe that combining Equation (18) and Equation (22) we obtain

$$f \equiv g^{(\ell)}h^{(\ell)} + \left(g^{(\ell)}q_h + h^{(\ell)}q_g\right) m^{\ell} \mod m^{\ell+1} \tag{24}$$

The induction hypothesis shows that $f - g^{(\ell)}h^{(\ell)}$ is a multiple of m^{ℓ}. Then we obtain

$$g_0 q_h + h_0 q_g \equiv \frac{f - g^{(\ell)}h^{(\ell)}}{m^{\ell}} \mod m. \tag{25}$$

By Theorem 1 and Equation (23), the Equation (25) has a unique solution. $\triangleleft$

3 Quadratic Hensel Lifting

Let R be a commutative ring with identity element. Let f, g, h be univariate polynomials in $R[x]$ and let $m \in R$. We assume that the following relation holds

$$f \equiv g\,h \mod m \tag{26}$$

We aim to lift this factorization modulo m into a factorization modulo m^2. Hence we want to compute $\widehat{g}$ and $\widehat{h}$ such that

$$f \equiv \widehat{g}\,\widehat{h} \mod m^2 \tag{27}$$

We will refer to this problem as the *factorization lifting problem.* To do so we will assume that we are given two polynomials s and t such that

$$sg + th \equiv 1 \mod m \tag{28}$$

Hence we will say that g and h are coprime modulo m. When R/m is a field then we can compute s and t by applying the Extended Euclidean Algorithm in $R[x]/m$.

Proposition 1 *A solution to the factorization lifting problem of Equation 27 is given by*

$$\widehat{g} = g + t\,e \quad \text{and} \quad \widehat{h} = h + s\,e \quad \text{where} \quad e = f - g\,h \tag{29}$$

PROOF $\triangleright$ We have the following relations.

$$\begin{array}{rcll} f - \widehat{g}\widehat{h} & = & f - (g + t\,e)\,(h + s\,e) & \\ & = & f - g\,h - g\,s\,e - h\,t\,e - s\,t\,e^2 & \\ & = & e - (s\,g + t\,h)\,e - s\,t\,e^2 & \\ & = & (1 - s\,g + t\,h)\,e - s\,t\,e^2 & \\ & \equiv & (1 - s\,g + t\,h)\,e - s\,t\,e^2 & \mod m^2 \end{array} \tag{30}$$

By hypothesis

$$e \equiv 0 \mod m \qquad \text{and} \qquad (1 - s\,g + t\,h) \equiv 0 \mod m \tag{31}$$

Hence both $(1 - s\,g + t\,h)\,e$ and e^2 are mutiple of m^2. It follows that

$$f - \widehat{g}\widehat{h} \equiv 0 \mod m^2 \tag{32}$$

$\triangleleft$

Remark 2 Observe that Proposition 1 works also if f, g, h are constants of R. In other words, f, g, h do not need to be polynomials! The factorization lifting problem and its solution by Proposition 1 are valid in any commutative ring with identity element. But for this solution to be an algorithm one needs to be able to compute the Bézout coefficients s and t.

Example 1 Consider $f = x^4 - 1$, $g = x - 2$, $h = x^3 + 2\,x^2 - x - 2$ and $m = 5$. We have the following computation in AXIOM

```
N := NonNegativeInteger


   (1)  NonNegativeInteger
                                                  Type: Domain

Z := Integer


   (2)  Integer
                                                    Type: Domain

U := UnivariatePolynomial(x,Z)


   (3)  UnivariatePolynomial(x,Integer)
                                                    Type: Domain

m: Z := 5


   (4)  5
                                                   Type: Integer

f: U := x^4 - 1


         4
   (5)  x  - 1
```

```
                    Type: UnivariatePolynomial(x,Integer)

g: U := x - 2


   (6)  x - 2
                    Type: UnivariatePolynomial(x,Integer)

h: U := x^3 + 2 *x^2 -x -2


         3     2
   (7)  x  + 2x  - x - 2
                    Type: UnivariatePolynomial(x,Integer)

e := f - g*h


          2
   (8)  5x  - 5
                    Type: UnivariatePolynomial(x,Integer)

K5 := PrimeField(5)


   (9)  PrimeField
                                         Type: Domain

U5 := UnivariatePolynomial(x,K5)


   (10)  UnivariatePolynomial(x,PrimeField 5)
                                          Type: Domain

f5: U5 := f :: U5


          4
```

```
   (11)  x  + 4
                    Type: UnivariatePolynomial(x,PrimeField 5)

g5: U5 := g :: U5


   (12)  x + 3
                    Type: UnivariatePolynomial(x,PrimeField 5)

h5: U5 := h ::U5


          3     2
   (13)  x  + 2x  + 4x + 3
                     Type: UnivariatePolynomial(x,PrimeField 5)

res := extendedEuclidean(g5,h5)

                   2
   (14)  [coef1= 2x  + 3x + 4,coef2= 3,generator= 1]

s5: U5 := res.coef1


           2
   (15)  2x  + 3x + 4
                     Type: UnivariatePolynomial(x,PrimeField 5)

t5: U5 := res.coef2


   (16)  3
                     Type: UnivariatePolynomial(x,PrimeField 5)

g_^ := g + t5 :: U * e


            2
```

```
   (17)  15x  + x - 17
                            Type: UnivariatePolynomial(x,Integer)
```

```
h_^ := h + s5 :: U * e
```

```
              4      3      2
   (18)  10x  + 16x  + 12x  - 16x - 22
                            Type: UnivariatePolynomial(x,Integer)
```

```
factor(f -  g_^  * h_^ )
```

```
                              4      3     2
   (19)  - 25(x - 1)(x + 1)(6x  + 10x  + 7x  - 10x - 15)
                   Type: Factored UnivariatePolynomial(x,Integer)
```

Remark 3 We see with Example 1 that the degrees of $\widehat{g}$ and $\widehat{h}$ are higher that those of g and h. In particular

$$\deg \widehat{g} + \deg \widehat{h} \ > \ \deg f \tag{33}$$

which may not look satisfactory! To overcome this problem we need to use division with remainder in $R[x]$. We will take advantage of the following.

Proposition 2 *Let a and b be in $R[x]$ such that b is monic. Let q and r be the quotient and the remainder of a w.r.t. b. Let m be in R. If $a \equiv 0 \mod m$ then*

$$q \equiv 0 \mod m \quad \text{and} \quad r \equiv 0 \mod m \tag{34}$$

also hold.

PROOF $\triangleright$ There exists $a^* \in R[x]$ such that $a = m\, a^*$. Let q^* and r^* be the quotient and the remainder of a^* w.r.t. b. Then we have

$$a^* \ = \ q^*\, b + r^* \quad \text{and} \quad \deg r^* \ < \ \deg b \tag{35}$$

Hence we have

$$a = m\,q^*\,b + m\,r^* \quad \text{and} \quad \deg\,(m\,r^*) < \deg b \tag{36}$$

Since the quotient and the remainder of a w.r.t. b are unique we have

$$q = m\,q^* \quad \text{and} \quad r = m\,r^* \tag{37}$$

$\triangleleft$

Definition 2 *Let f, g, h, s, t be polynomials in $R[x]$ and let $m \in R$. We say that (f, g, h, s, t) is a* liftable quintet *modulo m if the following conditions hold*

- $f \equiv g\,h \mod m$,
- $s\,g + t\,h \equiv 1 \mod m$,
- *h is monic,*
- $\deg f = \deg g + \deg h$,
- $\deg s < \deg h$,
- $\deg t < \deg g$.

Algorithm 1

Input: $f, g, h, s, t \in R[x]$ and $m \in R$ such that (f, g, h, s, t) is a liftable quintet modulo m.

Output: $g^*, h^*, s^*, t^* \in R[x]$ such that (f, g^*, h^*, s^*, t^*) is a liftable quintet modulo m^2 such that $u^* \equiv u \mod m$ for $u = g, h, s, t$ and $\deg g^* = \deg g$ and $\deg h^* = \deg h$.

$e := f - g\,h \mod m^2$
$(q,\, r) := \mathsf{divisionWithRemainder}(s\,e,\, h)$
$(q,\, r) := (q \mod m^2,\, r \mod m^2)$
$g^* := (g + t\,e + q\,g) \mod m^2$
$h^* := (h + r) \mod m^2$
$b := (s\,g^* + t\,h^* - 1) \mod m^2$
$(c,\, d) := \mathsf{divisionWithRemainder}(s\,b,\, h^*)$
$(c,\, d) := (c \mod m^2,\, d \mod m^2)$
$s^* := s - d \mod m^2$
$t^* := t - t\,b - c\,g^* \mod m^2$
return (g^*, h^*, s^*, t^*)

Theorem 5 *Algorithm 1 works correctly. Let $n = \deg f$. If $R = \mathbb{Z}$ and all input polynomials have max-norm less than m^2 then it requires $\mathcal{O}(\mathbf{M}(n)\,\mathbf{M}(\log m))$ word operations.*

Proof $\triangleright$ We shall prove the following claims about g^* and h^*:

1. $f - g^*\,h^* \equiv 0 \mod m^2$,
2. $g^* \equiv g \mod m$,
3. $h^* \equiv h \mod m$,
4. h^* monic and of the same degree as h,
5. g^* of the same degree as g.

We calculate modulo m^2:

$$\begin{aligned} f - g^* h^* &\equiv f - (g + te + qg)(h + se - qh) \\ &= f - gh - gse + gqh - teh - tese + teqh - qgh - qgse + qgqh \\ &= f - gh - gse - teh - tese + teqh - qgse + qgqh \\ &= e - (sg + th)e - ste^2 + qe(th + sg) + ghq^2 \\ &= (1 - sg - th)(f - gh) - ste^2 + qe(th + sg) + ghq^2 \end{aligned} \tag{38}$$

By assumption we have

- $1 - sg - th \ \equiv 0 \mod m$
- $f - gh \ \equiv 0 \mod m$

Moreover

$$e \ \equiv 0 \mod m \quad \text{and} \quad se \equiv qh + r \mod m^2 \tag{39}$$

by Proposition 2 imply

$$q \ \equiv 0 \mod m \tag{40}$$

This leads to

$$f - g^* h^* \ \equiv \ 0 \mod m^2. \tag{41}$$

Now the relation defining g^*

$$g^* \ = \ (q + t\, e + q\, g) \mod m^2 \tag{42}$$

together with $e \ \equiv \ 0 \mod m$ and $q \ \equiv \ 0 \mod m$ imply

$$g^* \ \equiv \ g \mod m \tag{43}$$

Similarly we have

$$h^* \ \equiv \ h \mod m \tag{44}$$

Now observe that by definition of r we have

$$\deg r \ < \ \deg h \tag{45}$$

Then since

$$h^* \ = \ (h + r) \mod m^2 \tag{46}$$

we obtain

$$h \text{ monic} \quad \text{and} \quad \deg h \ = \ \deg h^* \tag{47}$$

These last relations together with

$$f \equiv g^* h^* \mod m^2 \tag{48}$$

imply

$$\begin{array}{rcl} \deg g^* & = & \deg f - \deg h^* \\ & = & \deg f - \deg h \\ & = & \deg g \end{array} \tag{49}$$

This concludes this proof. We refer to Theorem 15.11 in [GG99] for the other claims of the theorem. $\triangleleft$

Example 2 Consider $f = x^4 - 1$, $g = x - 2$, $h = x^3 + 2\,x^2 - x - 2$ and $m = 5$. Using Proposition 1 we computed

$$\widehat{g} = 15x^2 + x - 17 \quad \text{and} \quad \widehat{h} = 10x^4 + 16x^3 + 12x^2 - 16x - 22 \tag{50}$$

Now using the improved formula of Algorithm 1 we have the following AXIOM session

```
N := NonNegativeInteger


   (1)  NonNegativeInteger
                                                   Type: Domain

Z := Integer


   (2)  Integer
                                                   Type: Domain

U := UnivariatePolynomial(x,Z)


   (3)  UnivariatePolynomial(x,Integer)
                                                   Type: Domain

m: Z := 5
```

```
   (4)  5
                                                        Type: Integer
```

```
f: U := x^4 - 1
```

```
         4
   (5)  x  - 1
                      Type: UnivariatePolynomial(x,Integer)
```

```
g: U := x - 2
```

```
   (6)  x - 2
                      Type: UnivariatePolynomial(x,Integer)
```

```
h: U := x^3 + 2 *x^2 -x -2
```

```
         3     2
   (7)  x  + 2x  - x - 2
                      Type: UnivariatePolynomial(x,Integer)
```

```
e := f - g*h
```

```
          2
   (8)  5x  - 5
                      Type: UnivariatePolynomial(x,Integer)
```

```
K5 := PrimeField(5)
```

```
   (9)  PrimeField 5
                                                         Type: Domain
```

```
U5 := UnivariatePolynomial(x,K5)
```

```
   (10)  UnivariatePolynomial(x,PrimeField 5)
                                                   Type: Domain

f5: U5 := f :: U5


          4
   (11)  x  + 4
              Type: UnivariatePolynomial(x,PrimeField 5)

g5: U5 := g :: U5


   (12)  x + 3
              Type: UnivariatePolynomial(x,PrimeField 5)

h5: U5 := h ::U5


          3     2
   (13)  x  + 2x  + 4x + 3
              Type: UnivariatePolynomial(x,PrimeField 5)

res := extendedEuclidean(g5,h5)


                  2
   (14)  [coef1= 2x  + 3x + 4,coef2= 3,generator= 1]
Type: Record(coef1: UnivariatePolynomial(x,PrimeField 5),
coef2: UnivariatePolynomial(x,PrimeField 5),
generator: UnivariatePolynomial(x,PrimeField 5))

s5: U5 := res.coef1


           2
```

```
   (15)  2x  + 3x + 4
              Type: UnivariatePolynomial(x,PrimeField 5)

s: U := s5 :: U


           2
   (16)  2x  + 3x + 4
                   Type: UnivariatePolynomial(x,Integer)

t5: U5 := res.coef2


   (17)  3
              Type: UnivariatePolynomial(x,PrimeField 5)

t: U := t5 :: U


   (18)  3
                   Type: UnivariatePolynomial(x,Integer)

R25 := IntegerMod(25)


   (19)  IntegerMod 25
                                            Type: Domain

U25 := UnivariatePolynomial(x,R25)


   (20)  UnivariatePolynomial(x,IntegerMod 25)
                                            Type: Domain

e25 := f::U25 - g::U25 * h::U25


           2
```

```
   (21)  5x  + 20
             Type: UnivariatePolynomial(x,IntegerMod 25)

e : U := e25 :: U


          2
   (22)  5x  + 20
                   Type: UnivariatePolynomial(x,Integer)

res := monicDivide(s*e, h)


                                                2
   (23)  [quotient= 10x - 5,remainder= 80x  + 75x + 70]
Type: Record(quotient: UnivariatePolynomial(x,Integer),
             remainder: UnivariatePolynomial(x,Integer))

q25: U25 := res.quotient :: U25


   (24)  10x + 20
             Type: UnivariatePolynomial(x,IntegerMod 25)

r25: U25 := res.remainder :: U25


          2
   (25)  5x  + 20
             Type: UnivariatePolynomial(x,IntegerMod 25)

g_* := (g::U25 + t::U25 * e25 + q25 * (g::U25)) :: U


   (26)  x + 18
                   Type: UnivariatePolynomial(x,Integer)

h_* := (h::U25 + r25) :: U
```

```
           3     2
   (27)  x  + 7x  + 24x + 18
                   Type: UnivariatePolynomial(x,Integer)
```

```
(f - g_* * h_*) :: U25
```

```
   (28)  0
               Type: UnivariatePolynomial(x,IntegerMod 25)
```

Theorem 6 *Let R be a commutative ring with identity element, an element $m \in R$ which is not a zero divisor, an integer $\ell \in \mathbb{N}$ and nonzero univariate polynomials $g, h, g^*, h^*, s, t \in R[x]$ such that*

1. $sg + th \equiv 1 \mod m$
2. *the leading coefficients of g and h are not zero divisors modulo m*
3. *the polynomials g and g^* have the same leading coefficients, the same degree and coincide modulo m*
4. *the polynomials h and h^* have the same leading coefficients, the same degree and coincide modulo m*
5. $gh \ \equiv \ g^* h^* \mod m^\ell$

Then we have

$$g \equiv g^* \mod m^\ell \quad \text{and} \quad h \equiv h^* \mod m^\ell \tag{51}$$

Proof $\triangleright$ We assume to the contrary that

$$g \not\equiv g^* \mod m^\ell \quad \text{or} \quad h \not\equiv h^* \mod m^\ell \tag{52}$$

Let $1 \leq i < \ell$ be maximal such that m^i both divides $g^* - g$ and $h^* - h$. Thus there exist polynomials $u, v \in R[x]$ such that

$$g^* - g \ = \ u\, m^i \quad \text{and} \quad h^* - h \ = \ v\, m^i \tag{53}$$

and also m does not divide u or v. We may assume that m does not divide u. Now we have

$$\begin{aligned} 0 &\equiv g^*h^* - gh \mod m^\ell \\ &= g^*(h^* - h) + h(g^* - g) \\ &= g^*v\, m^i + hu\, m^i \end{aligned} \tag{54}$$

This means that m^ℓ divides $g^*v\, m^i + hu\, m^i$. In other words there exist $w \in R[x]$ such that

$$(g^*v + hu)m^i \;=\; m^\ell\, w \tag{55}$$

Since m is not a zero divisor in R we have

$$(g^*v + hu) \;=\; m^{\ell - i}\, w \tag{56}$$

which implies

$$g^*v + hu \equiv 0 \mod m \tag{57}$$

Recall also that we have

$$th \equiv 1 - sg \mod m \tag{58}$$

and

$$g^* \equiv g \mod m \quad \text{and} \quad h^* \equiv h \mod m \tag{59}$$

Therefore we obtain the following calculation modulo m

$$\begin{aligned} 0 &\equiv t(g^*v + hu) \\ &\equiv tg^*v + thu \\ &\equiv tg^*v + (1 - sg)u \\ &\equiv (tv - su)g + u \end{aligned} \tag{60}$$

This shows that g divides u modulo m. However from $g^* - g \;=\; u\, m^i$ together with the facts that g^* and g have same leading coefficient and degree shows that

$$\deg u \;<\; \deg g \tag{61}$$

Since the leading coefficient of g is not a zero divisor modulo m we must have

$$u \equiv 0 \mod m \tag{62}$$

A contradiction. Therefore the theorem is proved. $\lhd$

References

[BL82] Bruno Buchberger and Rüdiger Georg Konrad Loos. *Algebraic Simplification*, pages 11–43. Springer Verlag, Wien–New York, 1982.

[DST93] J. Davenport, Y. Siret, and E. Tournier. *Calcul Formel*. Masson, 1993. 2^e édition révisée.

[GCL92] K.O. Geddes, S.R. Czapor, and G. Labahn. *Algorithms for Computer Algebra*. Kluwer Academic Publishers, 1992.

[GG99] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, 1999.