Advanced Computer Algebra: The resultant and gcd computation

Marc Moreno Maza
University of Western Ontario

CS424 / CS 556 – Winter 2005

January 7, 2008

1 Coefficients growth in the Euclidean Algorithm over $\mathbb{Q}[x]$

We saw in the first chapter that running the Euclidean Algorithm in $\mathbb{Q}[x]$ can lead to a significant expression swell. Let us try to estimate how coefficients grow. That is, we want to estimate the maximal space needed to store one coefficient of an intermediate polynomial. Let N be the number of bits of a machine word.

Definition 1 *For an integer $a \in \mathbb{Z}$ we define $\lambda(a)$ the* length *of a as the minimum number of words to encode a. Hence for $a \neq 0$ we have*

$$\lambda(a) = \lfloor \log_2(a)/N \rfloor + 1 \quad \text{and} \quad \lambda(0) = 0 \tag{1}$$

For a rational number $a = b/c$ with $b, c \in \mathbb{Z}$ and $\gcd(c, d) = 1$ we define $\lambda(a)$, the length *of a, as the maximum among $\lambda(b)$ and $\lambda(c)$.*

Definition 2 *For a polynomial $a \in \mathbb{Q}[x]$ of degree $n \geq 0$ such that all coefficients have denominator b and such that the numerators $a_n, a_{n-1}, \ldots, a_1, a_0$ have gcd 1 then we define the* length *of a as*

$$\lambda(a) = \max(\lambda(b), \max_{0 \leq i \leq n}(\lambda(a_i))) \tag{2}$$

Remark 1 A polynomial $a \in \mathbb{Q}[x]$ of degree $n \geq 0$ can be represented with

$$\lambda(a)\,(2 + \deg(a)) \tag{3}$$

words.

Proposition 1 *Let a, b be univariate polynomials over $\mathbb{Z}$ in x. Then we have*

1. $\lambda(a+b) \;\leq\; \max(\lambda(a), \lambda(b)) + 1.$
2. $\lambda(ab) \;\leq\; \lambda(a) + \lambda(b) + \lambda(\min(\deg(a), \deg(b)) + 1).$

Proof $\triangleright$ See [GG99]. $\triangleleft$

Proposition 2 *Let a, b be univariate polynomials over $\mathbb{Z}$ in x. We assume that a and b are monic and that $\deg(a) = \deg(b) + 1$ holds. Let q and r be the quotient and the remainder of a w.r.t. b. Then we have*

$$\lambda(r) \;\leq\; \lambda(a) + 2\lambda(b) + 3 \tag{4}$$

Proof $\triangleright$ We define

$$a \;=\; x^n + a_{n-1}x^{n-1} + \cdots + a_0 \quad \text{and} \quad b \;=\; x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_0 \tag{5}$$

It is not hard to see that

$$q \;=\; x + a_{n-1} - b_{n-2} \tag{6}$$

Then

$$\lambda(q) \;\leq\; \max(\lambda(a), \lambda(b)) + 1 \tag{7}$$

Thus

$$\lambda(bq) \;\leq\; \max(\lambda(a), \lambda(b)) + 1 + \lambda(b) + \lambda(\deg(q) + 1) \tag{8}$$

Recall that

$$r \;=\; a - bq \tag{9}$$

Since $\lambda(bq) \geq \lambda(a)$ we obtain

$$\begin{aligned} \lambda(r) \;&\leq\; \max(\lambda(a), \lambda(b)) + 1 + \lambda(b) + \lambda(\deg(q) + 1) + 1 \\ &\leq\; \lambda(a) + 2\lambda(b) + 3 \end{aligned} \tag{10}$$

Indeed $\max(\lambda(a), \lambda(b)) \;\leq\; \lambda(a) + \lambda(b)$ and $\lambda(\deg(q) + 1) \;=\; \lambda(2) \;\leq\; 1$. $\triangleleft$

Remark 2 A similar result as Proposition 2 holds for monic polynomials $a, b \in \mathbb{Q}[x]$ such that $\deg(a) = \deg(b) + 1$. See [GG99]. These results provide us with an exponential upper bound for the coefficient of the gcd computed by the Euclidean Algorithm. But in fact a polynomial bound can be established. Moreover there is an efficient modular approach for computing gcds in $\mathbb{Q}[x]$ and $\mathbb{Z}[x]$ as we shall see in the next sections.

2 Relation between gcds in $\mathbb{Q}[x]$ and $\mathbb{Z}[x]$. Polynomial gcds in non Euclidean domains.

Remark 3 The Euclidean Algorithm does not apply to $\mathbb{Z}[x]$ since $\mathbb{Z}[x]$ is not an Euclidean domain. However the concept of a polynomial gcd is well defined in $\mathbb{Z}[x]$ since $\mathbb{Z}[x]$ is a Unique Factorization Domain, as we shall review.

If we transport the computation of a gcd from $\mathbb{Z}[x]$ to $\mathbb{Q}[x]$ we should be careful. For instance with

$$f \;=\; 2x^2+2 \quad \text{and} \quad g \;=\; 6x+2. \tag{11}$$

In $\mathbb{Q}[x]$ their normalized gcd will be 1 whereas their expected gcd in $\mathbb{Z}[x]$ is 2.

Notation 1 Let R be a commutative ring with identity element. Every element $a \in R$ can be written

$$a \;=\; \mathrm{lu}(a)\ \mathrm{normal}(a) \tag{12}$$

where $\mathrm{normal}(a)$ stands for a canonical representative of the class of the elements associate with a and where $\mathrm{lu}(a)$ is a unit. Observe that a is a unit iff $\mathrm{normal}(a)$ is 1.

For $R = \mathbb{Z}$ we will take $\mathrm{normal}(a) =\mid a \mid$. For $R = \mathbf{k}[x]$ we will take $\mathrm{normal}(a) = a/\mathrm{lc}(a)$.

Remark 4 A nonzero nonunit $p \in R$ is *reducible* if there are two nonunits $c, d \in R$ such that $p = c\,d$, otherwise p is *irreducible*. Units are neither reducible nor irreducible. A nonzero nonunit $p \in R$ is *prime* if for every $c, d \in R$ we have we have

$$(p \mid cd) \quad \Rightarrow \quad (p \mid c \text{ or } p \mid d) \tag{13}$$

Observe that a prime is irreducible.

Assume from now on that R is a Unique Factorization Domain (UFD). This means that R is an integral domain such that

- every irreducible is a prime
- every nonzero nonunit $a \in R$ can be written as a product of irreducible elements in a unique way up to reordering and multiplication by units.

This leads to a natural formula for gcds, but not to an algorithm. However we assume that all gcds (for which we have an algorithm or not) are normalized. Hence we assume that gcds are **uniquely defined**.

Definition 3 *Let R be a UFD and $f = f_n x^n + \cdots + f_1 x + f_0$ be a univariate polynomial over R of positive degree. The* content *of f, denoted* $\mathrm{cont}(f)$ *is the gcd of its coefficients $f_n, \ldots, f_1, f_0$. By convention the content of a constant polynomial $f_0 \in R$ is* $\mathrm{normal}(f_0)$*. Observe that* $\mathrm{cont}(f)$ *is uniquely defined in any case.*

The polynomial $f \in R[x]$ is primitive *if* $\mathrm{cont}(f) = 1$*. The* primitive part *of $f \in R[x]$ is the polynomial* $\mathrm{pp}(f) \in R[x]$ *such that*

$$p \;=\; \mathrm{cont}(f)\mathrm{pp}(f). \tag{14}$$

Proposition 3 *If R is a UFD, for $f \in R[x]$ and $c \in R$ we have*

$$\mathrm{cont}(c\,f) \;=\; c\;\mathrm{cont}(f) \quad \text{and} \quad \mathrm{pp}(c\,f) \;=\; c\;\mathrm{pp}(f) \tag{15}$$

Theorem 1 (Gauss Lemma) *If R is a UFD, the product of two primitive polynomials in $R[x]$ is primitive.*

Proof ▷ Let R be a UFD. Let $f, g \in R[x]$ be primitive. Let $p \in R$ be a prime. Then, the residue class ring $D = R/p$ is an integral domain. It follows (this is a classical result) that $D[x]$ is an integral domain too. By hypothesis $f \mod p$ and $g \mod p$ are not zero. Hence $fg \mod p$ is not zero too. This shows that p cannot divide $\mathrm{cont}(fg)$. Finally we have proved that no primes divide $\mathrm{cont}(fg)$ and thus $\mathrm{cont}(fg) = 1$. ◁

Corollary 1 *Let R be a UFD. Let $f, g \in R[x]$. Then we have*

$$\mathrm{cont}(fg) \;=\; \mathrm{cont}(f)\,\mathrm{cont}(g) \quad \text{and} \quad \mathrm{pp}(fg) \;=\; \mathrm{pp}(f)\,\mathrm{pp}(g). \tag{16}$$

Proof ▷ Let $h = \mathrm{pp}(fg)$ and $h^* = \mathrm{pp}(f)\,\mathrm{pp}(g)$. By Gauss Lemma, the polynomial h^* is primitive. By definition of the content and the primitive part of a polynomial, we have

$$\begin{array}{rcl} fg & = & \mathrm{cont}(f)\,\mathrm{pp}(f)\,\mathrm{cont}(g)\,\mathrm{pp}(g) \\ & = & \mathrm{cont}(f)\,\mathrm{cont}(g)\,h^*. \end{array} \tag{17}$$

Then since h^* is primitive, with Proposition 3, we get

$$\begin{array}{rcl} \mathrm{cont}(fg) & = & \mathrm{cont}(\mathrm{cont}(f)\,\mathrm{cont}(g)\,h^*) \\ & = & \mathrm{cont}(f)\,\mathrm{cont}(g). \end{array} \tag{18}$$

◁

Theorem 2 (Gauss) *If R is a UFD, then so is $R[x]$.*

Proof $\triangleright$ See [GG99]. $\triangleleft$

Corollary 2 *Let R be $\mathbb{Z}$ or a field. Then $R[x_1, \ldots, x_n]$ is a UFD.*

Proof $\triangleright$ This is a direct consequence of Theorem 2. $\triangleleft$

Corollary 3 *Let R be a UFD with field of fractions K. Let $f, g \in R[x]$ be univariate polynomials over R and let h be their normalized gcd in $R[x]$. Then the following properties hold.*

1. *The prime elements of $R[x]$ are the primes of R plus the primitive polynomials in $R[x]$ that are irreducible in $K[x]$.*
2. $\mathrm{cont}(h) = \gcd(\mathrm{cont}(f), \mathrm{cont}(g))$ *in R.*
3. $\mathrm{pp}(h) = \gcd(\mathrm{pp}(f), \mathrm{pp}(g))$ *in $R[x]$.*
4. $h = \gcd(\mathrm{cont}(f), \mathrm{cont}(g)) \gcd(\mathrm{pp}(f), \mathrm{pp}(g))$
5. *$h/\mathrm{lc}(h)$ is the monic gcd of f and g in $K[x]$.*

Proof $\triangleright$ See [GG99]. $\triangleleft$

Remark 5 From Corollary 3 we can derive an algorithm for computing the normalized gcd h of $f, g \in R[x]$ by means of a polynomial gcd computation in $K[x]$ and gcd computations in R. We define

$$c = \gcd(\mathrm{cont}(f), \mathrm{cont}(g)) \tag{19}$$

To compute the primitive part of $\gcd_{R[x]}(f, g)$ we can assume that f and g are divided out by their contents. Let ν be the monic gcd of f and g in $K[x]$. We have

$$\nu \ = \ h/\mathrm{lc}(h) \tag{20}$$

Since h divides f and g in $R[x]$ then $\mathrm{lc}(h)$ divides $\mathrm{lc}(f)$ and $\mathrm{lc}(g)$ in R. Hence $\mathrm{lc}(h)$ divides $\gcd(\mathrm{lc}(f), \mathrm{lc}(g))$. We define

$$b = \gcd(\mathrm{lc}(f), \mathrm{lc}(g)) \tag{21}$$

Since $h = \mathrm{lc}(h)\ \nu$ lies in $R[x]$ and since $\mathrm{lc}(h)$ divides b we have

$$b\,\nu \in R[x] \tag{22}$$

Finally we obtain

$$h \ = \ c \ \ \mathrm{pp}(b\,\nu) \tag{23}$$

Remark 6 It follows from Corollary 3 and Remark 5 that if we have an algorithm for computing gcds in some UFD R then we have an algorithm to compute gcds in $R[x_1, \ldots, x_n]$. Of course this method based on the Euclidean Algorithm may not be the most efficient one.

In fact for computing gcds in $\mathbb{Z}[x]$ (and more generally over $\mathbb{Z}[x_1, \ldots, x_n]$) the modular methods (to be described shortly) are much more efficient than going through $\mathbb{Q}[x]$ and the Euclidean Algorithm.

The simplest approach would be

- to chose a large prime p
- then to compute the gcd $\overline{h}$ of f and g in $\mathbb{Z}/\langle p \rangle \mathbb{Z}[x]$ (rather than $\mathbb{Z}[x]$)
- and to *recover* the gcd h of f and g in $\mathbb{Z}[x]$ from $\overline{h}$.

This could work provided that

- $\overline{h}$ is the modular image of h and that
- we have a *reasonable* bound for the coefficients of h.

The next section introduces a powerful tool to control modular images of polynomial gcds.

3 The resultant

For univariate polynomials f, g over a field the following lemma says that it is possible to find polynomials s, t such that $sf + tg = 0$, $\deg(s) < \deg(g)$, $\deg(t) < \deg(f)$ if and only if $\gcd(f, g) \neq 1$.

Lemma 1 *Let $f, g \in \mathbf{k}[x]$ be nonzero polynomials over the field $\mathbf{k}$. Then the following statements are equivalent.*

- $\gcd(f, g) \neq 1$
- *There exist polynomials $s, t \in R[x] \setminus \{0\}$ such that*

$$sf + tg \ = \ 0, \quad \deg(s) < \deg(g) \quad \text{and} \quad \deg(t) < \deg(f) \tag{24}$$

PROOF $\triangleright$ Let $h = \gcd(f, g)$. If $h \neq 1$ then $\deg(h) \geq 1$ and a *solution* is

$$(s, t) \;=\; (g/h, -f/h) \tag{25}$$

Conversely, let (s, t) be a solution. Assume that f and g are coprime. Then $sf = -tg$ would imply $f \mid t$. This is impossible since $t \neq 0$ and $\deg(t) < \deg(f)$. Hence f and g are not coprime and $\gcd(f, g) \neq 1$ holds. $\triangleleft$

Remark 7 Given $f, g \in \mathbf{k}[x]$ nonzero polynomials of degrees n, m respectively we consider the map

$$\phi : \begin{array}{lcl} \mathbf{k}[x] \times \mathbf{k}[x] & \rightarrow & \mathbf{k}[x] \\ (s, t) & \longmapsto & sf + tg \end{array} \tag{26}$$

For $d \in \mathbb{N} \setminus \{0\}$ we define

$$P_d \;=\; \{p \in \mathbf{k}[x] \;\mid\; \deg(p) < d\} \tag{27}$$

with the convention that

$$P_0 \;=\; \{0\} \tag{28}$$

The restriction of ϕ to $P_m \times P_n \;\rightarrow\; P_{n+m}$ is a linear map ϕ_0 between vector spaces of finite dimension.

Proposition 4 *Let $f, g \in \mathbf{k}[x]$ nonzero polynomials of degrees n, m such that $n + m > 0$. Then we have:*

- $\gcd(f, g) = 1 \quad \Longleftrightarrow \quad \phi_0$ *is an isomorphism.*
- *If $\gcd(f, g) = 1$ then the Bézout coefficients (u, v) computed by the Extended Euclidean Algorithm form the unique solution in $P_m \times P_n$ of the equation*

$$\phi_0(u, v) \;=\; 1 \tag{29}$$

PROOF $\triangleright$ From Lemma 1 we deduce that the kernel of ϕ_0 is reduced to $\{0\}$ iff $\gcd(f, g) = 1$. Since both $P_m \times P_n$ and P_{n+m} have dimension $n + m$ this proves the first claim. The second claim is a consequence of the first one. $\triangleleft$

Remark 8 Let's carry on with f, g nonzero univariate polynomials in x of degrees n, m such that $n + m > 0$. However let us relax the hypothesis on the coefficient ring by assuming that it is just a commutative ring R with identity element. Let us write:

$$f \;=\; f_n x^n + \cdots + f_0 \quad \text{and} \quad g \;=\; g_m x^m + \cdots + g_0 \tag{30}$$

The natural basis for $P_m \times P_n$ consists of the $(x^i, 0)$ for $0 \leq i < m$ followed by the $(0, x^j)$ for $0 \leq j < m$. On this basis ϕ_0 is represented by the following matrix

$$\begin{pmatrix}
f_0 & 0 & \cdots & 0 & g_0 & 0 & \cdots & 0 \\
f_1 & f_0 & \ddots & \vdots & g_1 & g_0 & \ddots & \vdots \\
f_2 & f_1 & \ddots & 0 & g_2 & g_1 & \ddots & 0 \\
\vdots & & \ddots & f_0 & \vdots & & \ddots & g_0 \\
 & \vdots & & f_1 & & \vdots & & g_1 \\
f_n & & & & g_m & & & \\
0 & f_n & & \vdots & 0 & g_m & & \vdots \\
\vdots & \ddots & \ddots & & \vdots & \ddots & \ddots & \\
0 & \cdots & 0 & f_n & 0 & \cdots & 0 & g_m
\end{pmatrix} \tag{31}$$

where all entries outside of the *parallelograms* are equal to zero.

Definition 4 *The above square matrix of order $n + m$ is denoted* $\mathrm{Sylv}(f, g)$ *and called the* Sylvester matrix *of f and g. Its determinant is called the* resultant *of f and g denoted by* $\mathrm{res}(f, g)$. *We make the following conventions.*

- *If $n = m = 0$ (and still nonzero polynomials) we define* $\mathrm{res}(f, g) = 1$.
- *If $f = 0$ or $f \in R[x] \setminus R$ then* $\mathrm{res}(f, 0) = \mathrm{res}(0, f) = 0$.
- *If $f \in R \setminus \{0\}$ then* $\mathrm{res}(f, 0) = \mathrm{res}(0, f) = 1$.

Proposition 5 *Let $f, g \in \mathbf{k}[x]$ be nonzero univariate polynomials over a field $\mathbf{k}$. Then the following statements are equivalent*

1. $\gcd(f, g) = 1$.
2. $\mathrm{res}(f, g) \neq 0$.
3. *there do not exist any $s, t \in \mathbf{k}[x] \setminus \{0\}$ such that*

$$sf + tg = 0, \quad \deg(s) < \deg(g) \quad \text{and} \quad \deg(t) < \deg(f). \tag{32}$$

PROOF $\triangleright$ This follows from Proposition 4 and the fact that $\text{res}(f, g)$ is a determinant of the linear map ϕ_0. $\triangleleft$

Proposition 6 *Let $f, g \in R[x]$ be nonzero univariate polynomials over a UFD R. Then we have*

$$\gcd(f, g) \in R \qquad \Longleftrightarrow \qquad \text{res}(f, g) \neq 0. \tag{33}$$

PROOF $\triangleright$ This follows from the adaptation of the results of Lemma 1 and Proposition 4 to the case where the ground ring is a UFD (and in particular an integral domain) instead of a field. $\triangleleft$

Proposition 7 *Let $f, g \in R[x]$ be nonzero univariate polynomials over an integral domain R. Then there exist nonzero $s, t \in R[x]$ such that*

$$sf + tg = \text{res}(f, g), \quad \deg(s) < \deg(g) \quad \text{and} \quad \deg(t) < \deg(f). \tag{34}$$

PROOF $\triangleright$ Let $\mathbf{k}$ be the field of fractions of R. If $\text{res}(f, g) = 0$ then we know that there exist $s, t \in \mathbf{k}[x] \setminus \{0\}$ such that

$$sf + tg = 0, \quad \deg(s) < \deg(g) \quad \text{and} \quad \deg(t) < \deg(f). \tag{35}$$

Then the claim follows by cleaning up the denominators.

If $\text{res}(f, g) \neq 0$ then f and g are coprime in $\mathbf{k}[x]$. Then there exists $u, v \in \mathbf{k}[x]$ with stated degree bounds such that $uf + vg = 1$ holds in $\mathbf{k}[x]$. Observe that

- The coefficients of u, v are in fact the unique solution of a linear system whose matrix is the Sylvester $\text{Sylv}(f, g)$ matrix of f and g.
- These coefficients can be computed by the Cramer's rule.
- Hence each of these coefficients is the quotient of a determinant of a submatrix of $\text{Sylv}(f, g)$ by $\text{res}(f, g)$.

Then the polynomials $s = \text{res}(f, g)\ u$ and $t = \text{res}(f, g)\ v$ have coefficients in R and we have the desired relations. $\triangleleft$

4 Lucky and unlucky modular reductions

Let $f, g \in R[x]$ be nonzero polynomials for an Euclidean domain R. Let $p \in R$ be a prime. We denote by $a \longmapsto \overline{a}$ the reduction modulo p. We know from the previous section that

$$\gcd(f, g) \in R \qquad \Longleftrightarrow \qquad \operatorname{res}(f, g) \neq 0 \tag{36}$$

The formula of the resultant of f and g shows that $\operatorname{res}(f, g)$ is a multivariate polynomial expression in the coefficients of f and g. Hence we might be tempted to say

- $\overline{\operatorname{res}(f, g)} = \operatorname{res}(\overline{f}, \overline{g})$.
- $\overline{f}$ and $\overline{g}$ are coprime in $R/p[x]$ iff p does not divide $\operatorname{res}(f, g)$.

Example 1 Consider $R = \mathbb{Z}$, $p = 2$, $f = x + 2$ and $g = x$. Then we have

$$\operatorname{res}(f, g) = -2 \equiv 0 \mod 2 \quad \text{and} \quad \operatorname{res}(\overline{f}, \overline{g}) = 0 \tag{37}$$

as expected. **But** when $f = 4x^3 - x$ and $g = 2x + 1$ we have

$$\operatorname{res}(f, g) = 0 \quad \text{and} \quad \operatorname{res}(\overline{f}, \overline{g}) = \operatorname{res}(x, 1) = 1 \tag{38}$$

The reason for this unexpected behavior in the last example is that the Sylvester matrix of $\overline{f} = x$ and $\overline{g} = 1$ is

$$\left(\begin{array}{c} 1 \end{array} \right) \tag{39}$$

and thus is not the reduction modulo 2 of the Sylvester matrix of f and g which is

$$\left(\begin{array}{cccc} 4 & 2 & 0 & 0 \\ 0 & 1 & 2 & 0 \\ -1 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 \end{array} \right) \tag{40}$$

In other words the res operation for $\overline{f}$ and $\overline{g}$ is not the reduction modulo 2 of the res operation for f and g. This is because the res operation depends on the degrees of its input polynomials. Fortunately this nuisance disappears when p does not divide at least one of the leading coefficients.

Lemma 2 *Let R be a commutative ring with identity element. Let $f, g \in R[x]$ be nonzero polynomials. Let r be their resultant. Let I be an ideal if R and let denote by $a \longmapsto \overline{a}$ the reduction modulo I. Assume that*

$$\overline{\mathrm{lc}(f)} \neq 0 \tag{41}$$

Then we have

$$\overline{r} = 0 \qquad \Longleftrightarrow \qquad \mathrm{res}(\overline{f}, \overline{g}) = 0 \tag{42}$$

Moreover, if R/I is a UFD, then we have

$$\overline{r} = 0 \qquad \Longleftrightarrow \qquad \deg(\gcd(\overline{f}, \overline{g})) > 0 \tag{43}$$

Proof $\triangleright$ Let us write:

$$f \;=\; f_n x^n + \cdots + f_0 \quad \text{and} \quad g \;=\; g_m x^m + \cdots + g_0 \tag{44}$$

with $f_n \neq 0$ and $g_m \neq 0$. If $n = 0$ then $\mathrm{Sylv}(f, g)$ and $\mathrm{Sylv}(\overline{f}, \overline{g})$ are both diagonal with f on the diagonal. Then in that case

$$\overline{r} \;=\; \overline{f^m} \;=\; \overline{f}^m \;=\; \mathrm{res}(\overline{f}, \overline{g})^m \tag{45}$$

If $n > 0$ we distinguish two cases. If $\overline{g} = 0$ then $\mathrm{res}(\overline{f}, \overline{g}) = 0$ (by Definition 4). Moreover each g-column of $\mathrm{Sylv}(f, g)$ is zero modulo I such that $\overline{r} = 0$ too. From now on assume $\overline{g} \neq 0$ and let i be the smallest index such that $\overline{g_{m-i}} \neq 0$ holds.

$$\mathrm{Sylv}(f, g) \;=\; \left(\begin{array}{ccccccccc}
f_0 & & & & & g_0 & & & \\
\vdots & \ddots & & & & \vdots & & & \\
f_{n-i} & & f_0 & & & \vdots & \ddots & & \\
\vdots & \ddots & \vdots & \ddots & & g_{m-i} & \ddots & \ddots & g_0 \\
f_n & & f_{n-i} & & f_0 & \vdots & & \ddots & \vdots \\
 & \ddots & \vdots & \ddots & \vdots & g_m & \ddots & & \vdots \\
 & & f_n & & f_{n-i} & & & \ddots & g_{m-i} \\
 & & & \ddots & \vdots & & & & \vdots \\
 & & & & f_n & & & & g_m
\end{array} \right) \tag{46}$$

By exchanging the f-*zone* with the g-*zone* we have also

$$\mathrm{res}(f,g) \;=\; (-1)^{nm} \begin{vmatrix} g_0 & & & & f_0 & & & & \\ \vdots & & & & \vdots & \ddots & & & \\ \vdots & \ddots & & & f_{n-i} & & f_0 & & \\ g_{m-i} & \ddots & \ddots & g_0 & \vdots & \ddots & \vdots & \ddots & \\ \vdots & & \ddots & \vdots & f_n & & f_{n-i} & & f_0 \\ g_m & \ddots & & \vdots & & \ddots & \vdots & \ddots & \vdots \\ & & \ddots & g_{m-i} & & & f_n & & f_{n-i} \\ & & & \vdots & & & & \ddots & \vdots \\ & & & g_m & & & & & f_n \end{vmatrix} \tag{47}$$

Let M be the submatrix obtained from $\mathrm{Sylv}(g,f)$ by deleting the last i rows and the last i columns. Observe that we have

$$\overline{\mathrm{res}(f,g)} \;=\; (-1)^{nm}\, \overline{\det(M)}\; \overline{f_n}^{\,i} \tag{48}$$

Since

$$\overline{\det(M)} \;=\; \det(\overline{M}) \;=\; \mathrm{res}(\overline{f},\overline{g}) \tag{49}$$

we obtain

$$\overline{\mathrm{res}(f,g)} \;=\; (-1)^{nm}\, \mathrm{res}(\overline{f},\overline{g})\; \overline{\mathrm{lc}(f)}^{\,i} \tag{50}$$

This shows that we have

$$\overline{r} = 0 \qquad \Longleftrightarrow \qquad \mathrm{res}(\overline{f},\overline{g}) = 0 \tag{51}$$

and the first claim of the lemma is proved. The second claim follows from Proposition 6. $\triangleleft$

Theorem 3 *Let $f, g \in R[x]$ be nonzero polynomials for an Euclidean Domain R. Let $p \in R$ be a prime. Let*

$$h = \gcd(f,g), \qquad e = \deg(h). \qquad \text{and} \qquad \alpha = \mathrm{lc}(h) \tag{52}$$

Assume that p does not divide

$$b \;=\; \gcd(\mathrm{lc}(f), \mathrm{lc}(g)) \tag{53}$$

Finally let

$$e^* \;=\; \deg(\gcd(\overline{f},\overline{g})) \tag{54}$$

Then we have

1. *α divides b*

2. $e^* \geq e$

3. $e^* = e \quad \Longleftrightarrow \quad \overline{\alpha}\ \gcd(\overline{f}, \overline{g}) = \overline{h} \quad \Longleftrightarrow \quad p \not| \operatorname{res}(f/h, g/h)$

PROOF $\triangleright$ Since in $R[x]$

$$h \mid f \quad \text{and} \quad h \mid g \tag{55}$$

we have in R

$$\operatorname{lc}(h) \mid \operatorname{lc}(f) \quad \text{and} \quad \operatorname{lc}(h) \mid \operatorname{lc}(g). \tag{56}$$

Therefore

$$\alpha \ = \ \operatorname{lc}(h) \mid \gcd(\operatorname{lc}(f), \operatorname{lc}(g)) \ = \ b \tag{57}$$

and the first claim is proved. Consider now the cofactors of f and g in $R[x]$

$$u \ = \ f/h \quad \text{and} \quad v \ = \ g/h. \tag{58}$$

Then we have

$$\overline{u}\,\overline{h} \ = \ \overline{f} \quad \text{and} \quad \overline{v}\,\overline{h} \ = \ \overline{g} \tag{59}$$

which shows that

$$\overline{h} \mid \gcd(\overline{f}, \overline{g}) \tag{60}$$

and implies that

$$\deg(\overline{h}) \ \leq \ \deg(\gcd(\overline{f}, \overline{g})) \tag{61}$$

Since p does not divide b, it cannot not divide α neither. Hence the leading coefficient of $\overline{h}$ is $\overline{\alpha}$ and we have

$$\deg(\overline{h}) \ = \ \deg(h) \tag{62}$$

Therefore

$$e \ = \ \deg(h) \ \leq \ \deg(\gcd(\overline{f}, \overline{g})) \ = \ e^* \tag{63}$$

and the second claim is proved.

Now consider the case where $e = e^*$. Since $\overline{h}$ divides $\gcd(\overline{f}, \overline{g})$ and since $\gcd(\overline{f}, \overline{g})$ is monic (as a gcd over the field R/p) there exists a unit β such that

$$\overline{h} \ = \ \beta \gcd(\overline{f}, \overline{g}) \tag{64}$$

Since the leading coefficient of $\overline{h}$ is $\overline{\alpha}$ we have in fact

$$\beta \; = \; \overline{\alpha} \tag{65}$$

Therefore we have the following equivalence

$$e \; = \; e^* \qquad \Longleftrightarrow \qquad \overline{h} \; = \; \overline{\alpha} \, \gcd(\overline{f}, \overline{g}) \tag{66}$$

It remains to prove that

$$\overline{\alpha} \, \gcd(\overline{f}, \overline{g}) = \overline{h} \quad \Longleftrightarrow \quad p \not| \mathrm{res}(f/h, g/h) \tag{67}$$

Observe that p cannot divide both $\mathrm{lc}(u)$ and $\mathrm{lc}(v)$. If this was the case then from Relation (59) (and since p does not divide $\alpha = \mathrm{lc}(h)$) p would divide $\mathrm{lc}(f)$ and $\mathrm{lc}(g)$, and thus b. A contradiction. Therefore we can assume that p does not divide $\mathrm{lc}(u)$. By applying Lemma 2 we obtain

$$\overline{\mathrm{res}(u, v)} = 0 \qquad \Longleftrightarrow \qquad \mathrm{res}(\overline{u}, \overline{v}) = 0 \tag{68}$$

By applying Proposition 5 this leads to

$$p \; | \; \mathrm{res}(u, v) \qquad \Longleftrightarrow \qquad \gcd(\overline{u}, \overline{v}) \neq 1 \tag{69}$$

From Relation (59) we have

$$\gcd(\overline{f}, \overline{g}) \; = \; \gcd(\overline{u}, \overline{v}) \; \overline{h}/\overline{\alpha} \tag{70}$$

Therefore

$$p \quad \not| \; \mathrm{res}(u, v) \qquad \Longleftrightarrow \qquad \gcd(\overline{f}, \overline{g}) \; = \; 1 \; \times \; \overline{h}/\overline{\alpha} \tag{71}$$

This concludes the proof of the theorem. $\triangleleft$

Definition 5 *Let $f, g \in R[x]$ be nonzero polynomials for an Euclidean domain R. Let $h \in R[x]$ be* $\gcd(f, g)$. *A prime element $p \in R$ is said* lucky *if p does not divide* $\mathrm{res}(f/h, g/h)$ *otherwise it is said* unlucky*.*

Example 2 Consider $f = 12x^3 - 28x^2 + 20x - 4$, $g = -12x^2 + 10x - 2$ and $p = 17$. We have the following computation in AXIOM (where we do not display types)

```
N := NonNegativeInteger

   (1)  NonNegativeInteger

Z := Integer

   (2)  Integer

U := UnivariatePolynomial(x,Z)

   (3)  UnivariatePolynomial(x,Integer)

f: U := 12*x^3 -28*x^2 +20*x - 4

           3      2
   (4)  12x  - 28x  + 20x - 4

g: U := -12*x^2 +10*x -2

             2
   (5)  - 12x  + 10x - 2

resultant(f,g)

   (6)  0

h: U := gcd(f,g)

   (7)  6x - 2

r: Z := resultant(exquo(f,h),exquo(g,h))

   (8)  2

K17 := PrimeField(17)

   (9)  PrimeField 17
```

```
r :: K17


   (10)  2

U17 := UnivariatePolynomial(x,K17)

   (11)  UnivariatePolynomial(x,PrimeField 17)

f17: U17 := f :: U17

            3     2
   (12)  12x  + 6x  + 3x + 13

g17: U17 := g :: U17

           2
   (13)  5x  + 10x + 15

h17: U17 := h ::U17

   (14)  6x + 15

c17 := gcd(f17,g17)

   (15)  x + 11

h17 - (leadingCoefficient(h17)) * c17

   (16)  0
```

Example 3 Consider $f = x^4 - 3x^2 + 2x$, $g = x^3 - 1$ and $p = 13$. We have the following computation in AXIOM (where we do not display types) The variables `N, Z, U` are defined as above.

```
f: U := x^4 -3*x^3 + 2*x
```

```
         4     3
   (4)  x  - 3x  + 2x

g: U := x^3  -1

         3
   (5)  x  - 1

resultant(f,g)

   (6)  0

h: U := gcd(f,g)

   (7)  x - 1

r: Z := resultant(exquo(f,h),exquo(g,h))

   (8)  9

K3 := PrimeField(3)

   (9)  PrimeField 3

r :: K3

   (10)  0

U3 := UnivariatePolynomial(x,K3)

   (11)  UnivariatePolynomial(x,PrimeField 3)

f3: U3 := f :: U3

          4
   (12)  x  + 2x

g3: U3 := g :: U3
```

```
          3
   (13)  x  + 2

h3: U3 := h ::U3

   (14)  x + 2

c3 := gcd(f3,g3)

          3
   (15)  x  + 2

exquo(c3, h3)

          2
   (16)  x  + x + 1
```

5 Mignotte's factor bound

Definition 6 *Let $f = \Sigma_{0 \leq i \leq n} \, f_i x^i$ be a univariate polynomial over $\mathbb{C}$. The* 2-norm *of f is defined by*

$$\|f\|_2 \;=\; \left(\Sigma_{0 \leq i \leq n} \, |f_i|^2\right)^{1/2} \tag{72}$$

where $|z|$ denotes the square root of the product of z by its conjugate $\overline{z}$.

Remark 9 Given $f = \Sigma_{0 \leq i \leq n} \, f_i x^i$ we shall compute a bound B such that for any $h \in \mathbb{C}[x]$ we have

$$h \;|\; f \quad \Rightarrow \quad \|h\|_2 \;\leq\; B \tag{73}$$

One could hope that $B = \|f\|_2$ would work. Unfortunately there are some counter-examples. Though they are very rare, there are infinitely many of them.

```
(2) -> factor(x^105 - 1)
```

(2)

$$(x - 1)(x^2 + x + 1)(x^4 + x^3 + x^2 + x + 1)$$

*

$$(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$$

*

$$(x^8 - x^7 + x^5 - x^4 + x^3 - x + 1)$$

*

$$(x^{12} - x^{11} + x^9 - x^8 + x^6 - x^4 + x^3 - x + 1)$$

*

$$x^{24} - x^{23} + x^{19} - x^{18} + x^{17} - x^{16} + x^{14} - x^{13}$$

$$+ x^{12} - x^{11} + x^{10} - x^8 + x^7 - x^6 + x^5 - x + 1$$

*

$$x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - 2x^{41} - x^{40}$$

$$- x^{39} + x^{36} + x^{35} + x^{34} + x^{33}$$

$$+ x^{32} + x^{31} - x^{28} - x^{26} - x^{24} - x^{22} - x^{20}$$

$$+ x^{17} + x^{16} + x^{15} + x^{14} + x^{13}$$

$$+ x^{12} - x^9 - x^8 - 2x^7 - x^6 - x^5 + x^2 + x + 1$$

Type: Factored Polynomial Integer

Worse than that: for every $B > 0$ there exist infinitely many n such that there exists a polynomial h dividing $x^n - 1$ and satisfying $\|h\|_2 > B$. See [GG99] for more details.

Lemma 3 *For $f \in \mathbb{C}[x]$ and $z \in \mathbb{C}$ we have*

$$\|(x-z)f\|_2 \;=\; \|(\overline{z}\,x - 1)f\|_2 \tag{74}$$

PROOF $\triangleright$ Let $f = \Sigma_{0 \leq i \leq n}\; f_i x^i$ and define $f_{-1} = f_{n+1} = 0$. We calculate

$$\begin{array}{rcl}
\|(x-z)f\|_2^2 & = & \Sigma_{0\leq i\leq n+1}\;|f_{i-1} - zf_i|^2 \\
& = & \Sigma_{0\leq i\leq n+1}\;(f_{i-1} - zf_i)\left(\overline{f_{i-1} - zf_i}\right) \\
& = & \|f\|_2^2(1+\mid z\mid^2) + \Sigma_{0\leq i\leq n+1}\;\left(-f_{i-1}\,\overline{zf_i} - zf_i\overline{f_{i-1}}\right) \\
& = & \|f\|_2^2(\mid z\mid^2+1) + \Sigma_{0\leq i\leq n+1}\;\left(-z\,\overline{f_{i-1}}\,f_i - \overline{z}\,f_{i-1}\,\overline{f_i}\right) \\
& = & \Sigma_{0\leq i\leq n+1}\;(\overline{z}f_{i-1} - f_i)(z\overline{f_{i-1}} - \overline{f_i}) \\
& = & \Sigma_{0\leq i\leq n+1}\;|\overline{z}f_{i-1} - f_i|^2 \\
& = & \|(\overline{z}\,x - 1)f\|_2
\end{array} \tag{75}$$

$\triangleleft$

Definition 7 Let $z_1, \ldots, z_n$ be the complex roots of the polynomial

$$f \;=\; \Sigma_{0\leq i\leq n}\; f_i x^i \;=\; f_n\; \Pi_{1\leq i\leq n}\;(x - z_i) \tag{76}$$

We define the *measure* of the polynomial f by

$$M(f) \;= \mid f_n \mid\; \Pi_{1\leq i\leq n}\; \max(1, \mid z_i \mid) \tag{77}$$

Remark 10 For $f, g \in \mathbb{C}[x]$ the following statements are easy to prove:

1. $M(f) \;\geq\; \mathrm{lc}(f)$.
2. $M(fg) \;=\; M(f)\,M(g)$.

The following theorem of Landau (1905) relates $M(f)$ and $\|f\|_2$.

Theorem 4 (Landau) *For any $f \in \mathbb{C}[x]$ we have*

$$M(f) \;\leq\; \|f\|_2 \tag{78}$$

PROOF $\triangleright$ We arrange the roots $z_1, \ldots, z_n$ of f such that

$$| z_1 |, \ldots, | z_k | > 1 \quad \text{and} \quad | z_{k+1} |, \ldots, | z_n | \leq 1 \tag{79}$$

Therefore

$$M(f) = | f_n \cdot z_1 \cdots z_k | \tag{80}$$

Let

$$\begin{aligned} g &= f_n \, \Pi_{1 \leq j \leq k}(\overline{z_j} z - 1) \Pi_{k < j \leq n}(x - z_j) \\ &= g_n x^n + \cdots + g_0 \end{aligned} \tag{81}$$

We calculate

$$\begin{aligned} M(f)^2 &= | f_n \cdot z_1 \cdots z_k |^2 \\ &= | f_n \cdot \overline{z_1} \cdots \overline{z_k} |^2 \\ &= | g_n |^2 \\ &\leq \|g\|_2^2 \\ &= \|\tfrac{g}{\overline{z_1} x - 1}(x - z_1)\|_2^2 \\ &= \cdots \\ &= \|\tfrac{g}{(\overline{z_1} x - 1) \cdots (\overline{z_k} x - 1)}(x - z_1) \cdots (x - z_k)\|_2^2 \\ &= \|f\|_2^2 \end{aligned} \tag{82}$$

where we made repeated use of Lemma 3. $\triangleleft$

Remark 11 Given $f = \Sigma_{0 \leq i \leq n} \, f_i x^i$ it is convenient to use the 1-norm

$$\|f\|_1 = \Sigma_{0 \leq i \leq n} \; | f_i | \tag{83}$$

and the ∞-norm

$$\|f\|_\infty = \max{}_{0 \leq i \leq n}(| f_i |) \tag{84}$$

The following inequalities are classical.

$$\|f\|_\infty \leq \|f\|_2 \leq \|f\|_1 \leq (n+1)\,\|f\|_\infty \quad \text{and} \quad \|f\|_2 \leq (n+1)^{1/2}\,\|f\|_\infty \tag{85}$$

Theorem 5 *Let $f = \Sigma_{0 \leq i \leq n} \, f_i x^i$ and $h = \Sigma_{0 \leq i \leq m} \, h_i x^i$ be two polynomials such that h divides f. Then we have*

$$\|h\|_2 \leq \|h\|_1 \leq 2^m \, M(h) \leq \left|\frac{h_m}{f_n}\right| 2^m \, \|f\|_2 \tag{86}$$

PROOF $\triangleright$ Let us write

$$h \;=\; h_n \; \Pi_{1 \leq i \leq m} \; (x - u_i) \tag{87}$$

where $u_1, \ldots, u_m \in \mathbb{C}$ are the roots of h and thus among the roots of f. Observe that the coefficient h_i of h (in the term of degree i)

- is a sum of products, where each product consists of $m-i$ factors, each of these factors being a root of h.
- Hence each of these factors is bounded by $M(h)$.
- Moreover there are $\left(\begin{array}{c} m \\ i \end{array} \right)$ of these factors. Indeed, in order to build one of these factors, one needs to choose i roots among the m of h.

So for $i = 0 \cdots m$ we have

$$\mid h_i \mid \leq \left(\begin{array}{c} m \\ i \end{array} \right) M(h) \tag{88}$$

This implies

$$\begin{array}{rcl} \|h\|_1 & = & \Sigma_{0 \leq i \leq m} \;\; \mid h_i \mid \\ & \leq & M(h) \; \Sigma_{0 \leq i \leq m} \left(\begin{array}{c} m \\ i \end{array} \right) \\ & = & M(h) \; (1+1)^m \\ & = & M(h) \; 2^m \end{array} \tag{89}$$

Now observe that the measures of h and f satisfy

$$M(h) \;\leq\; \left| \frac{h_m}{f_n} \right| M(f) \tag{90}$$

Relations (89) and (90) together we Theorem 4 leads to

$$\|h\|_2 \;\leq\; \|h\|_1 \;\leq\; M(h)\; 2^m \;\leq\; \left| \frac{h_m}{f_n} \right| M(f) \; 2^m \;\leq\; \left| \frac{h_m}{f_n} \right| \|f\|_2 \; 2^m \tag{91}$$

The theorem is proved. $\triangleleft$

Corollary 4 (Mignotte's bound) *Let $f, g, h \in \mathbb{Z}[x]$ be univariate polynomials with degrees n, m, k respectively. If the product $g\,h$ divides f in $\mathbb{Z}[x]$ then we have*

$$\|g\|_\infty \, \|h\|_\infty \;\leq\; \|g\|_2 \, \|h\|_2 \;\leq\; \|g\|_1 \, \|h\|_1 \;\leq\; 2^{m+k} \, \|f\|_2 \;\leq\; (n{+}1)^{1/2} \, 2^{m+k} \, \|f\|_\infty \tag{92}$$

Proof $\triangleright$ The first, the second and the fourth above inequalities follow directly from the classical relations between the norms $\| \cdot \|_1$, $\| \cdot \|_2$ and $\| \cdot \|_\infty$ given in Remark 11. So the only inequality to prove is

$$\|g\|_1 \, \|h\|_1 \ \leq \ 2^{m+k} \, \|f\|_2. \tag{93}$$

From Theorem 5 (that essentially relates the 1-norm of a polynomial with its measure) we have

$$\|g\|_1 \ \leq \ 2^m \, M(g) \quad \text{and} \quad \|h\|_1 \ \leq \ 2^k \, M(h). \tag{94}$$

From the elementary properties of the measure of a polynomial given in Remark 10 we have

$$M(g) \, M(h) \ \leq \ M(f). \tag{95}$$

By virtue of Landau's inequality (Theorem 4) we have

$$M(f) \ \leq \ \|f\|_2. \tag{96}$$

Putting all these relations together leads to

$$\|g\|_1 \, \|h\|_1 \ \leq \ 2^{m+k} \, M(g) \, M(h) \ \leq \ 2^{m+k} \, M(f) \ \leq \ 2^{m+k} \, \|f\|_2. \tag{97}$$

The corollary is proved. $\triangleleft$

Remark 12 Applying Corollary 4 to $g = 1$ and keeping f, g as before leads to the following bound for every coefficient of every factor h of f.

$$\|h\|_\infty \ \leq \ (n+1)^{1/2} \, 2^n \, \|f\|_\infty \tag{98}$$

6 Modular Gcd Algorithms in $\mathbb{Z}[x]$

Remark 13 Algorithm 1 computes the gcd h of two primitive polynomials $f, g \in \mathbb{Z}[x]$. Before proving this algorithm, let us check that all its computations are well defined. Consider an iteration of the loop. We assume that we have a source of primes large enough. Given a prime p from this source the following polynomials are computed

- $\overline{f} = f \mod p$ and $\overline{g} = g \mod p$ which implies that the each coefficient c of $\overline{f}$ or $\overline{g}$ is the range $[-\frac{p-1}{2}, \frac{p-1}{2}]$

- ν the (monic) gcd of $\overline{f}$ and $\overline{g}$ in $\mathbb{Z}/\langle p\rangle[x]$ (same remark for the coefficients of ν)

- $w \in Z[x]$ such that $w \equiv b\,\nu \mod p$ (same remark for the coefficients of w)

- f^* is $q \mod p$ where q is the quotient in the division of $b\,f$ by ν

- g^* is $q \mod p$ where q is the quotient in the division of $b\,g$ by ν

The only points to clarify are the equalities $f^*\,w \equiv b\,f \mod p$ and $g^*\,w \equiv b\,g \mod p$. They hold since w is the gcd $\overline{f}$ and $\overline{g}$ which implies that w divides $b\,f \mod p$ and $b\,g \mod p$.

Algorithm 1

Input: primitive polynomials $f, g \in \mathbb{Z}[x]$ such that $\deg(f) = n \geq \deg(g) \geq 1$ and $\|f\|_\infty, \|g\|_\infty \leq A$.

Output: $h = \gcd(f, g) \in \mathbb{Z}[x]$

$b := \gcd(\mathrm{lc}(f), \mathrm{lc}(g))$
$B := (n+1)^{1/2}\, 2^n\, A\, b$
repeat
  choose a prime p such that $2\,B < p$
  $\overline{f} := f \mod p$
  $\overline{g} := g \mod p$
  compute ν the monic gcd of $\overline{f}$ and $\overline{g}$ in $\mathbb{Z}/\langle p\rangle[x]$
  compute w such that $w \equiv b\,\nu \mod p$
  compute f^* such that $f^*\,w \equiv b\,f \mod p$
  compute g^* such that $g^*\,w \equiv b\,g \mod p$
until $\|f^*\|_1\,\|w\|_1 \leq B$ **and** $\|g^*\|_1\,\|w\|_1 \leq B$
return normal(pp(w))

Proof $\triangleright$ It is sufficient to see that

$$\|f^*\|_1\,\|w\|_1 \leq B \quad \text{and} \quad \|g^*\|_1\,\|w\|_1 \leq B \tag{99}$$

both hold iff normal(pp(w)) $= h$. If the conditions hold then

$$\|f^* w\|_\infty \leq \|f^* w\|_1 \leq \|f^*\|_1\,\|w\|_1 \leq B < p/2 \tag{100}$$

Moreover from the algorithm computations we have

$$\|b\,f\|_{\infty} \; < \; p/2 \tag{101}$$

and

$$f^{*}\,w \; \equiv \; b\,f \quad \bmod p \tag{102}$$

Relations (100) and (101) imply that every coefficient c of $f^{*}\,w - b\,f$ satisfies $-p < c < p$. Whereas Relation (102) tells us that every coefficient c of $f^{*}\,w - b\,f$ is a multiple of p. Therefore we have

$$f^{*}\,w \; = \; b\,f \tag{103}$$

Similarly we have

$$g^{*}\,w \; = \; b\,g \tag{104}$$

This implies that w divides $\gcd(b\,f, b\,g)$. Hence the primitive part of w divides that of $\gcd(b\,f, b\,g)$ which is h. On the other hand

- w and ν have the same degree since $w \equiv b\,\nu \mod p$ holds and since p does not divide b.
- ν has degree equal or greater to that of h by virtue of Theorem 3.

Therefore $\mathrm{pp}(w)$ and h have the same degree and are in fact equal up to a sign. Conversely assume that normal(pp(w)) is h. Recall that w and ν have the same degree. Then the polynomials ν and h have the same degree too. Hence by virtue of Theorem 3 we have

$$\overline{\alpha}\,\nu \; = \; \overline{h} \tag{105}$$

where $\alpha = \mathrm{lc}(h)$. Since α divides b let β be such that $b = \alpha\,\beta$. Hence we have

$$w \; \equiv \; \beta\,h \; \equiv \; b\,\nu \quad \bmod p \tag{106}$$

Now by construction we have

$$\|w\|_{\infty} \; < \; p/2 \tag{107}$$

Moreover Corollary 4 states that

$$\|h\|_{\infty} \; \leq \; (n+1)^{1/2}\,2^{n}\,\|f\|_{\infty} \tag{108}$$

which implies

$$\|\beta\, h\|_\infty \;\leq\; B \;<\; p/2. \tag{109}$$

Relations (105), (106) and (107) imply

$$w \;=\; \beta\, h \tag{110}$$

Since h divides f and g we deduce from Relation (109) that w divides $b\, f$ and $b\, g$. Hence there exist polynomials $\widehat{f}$ and $\widehat{g}$ such that

$$\widehat{f}\, w \;=\; b\, f \quad \text{and} \quad \widehat{g}\, w \;=\; b\, g \tag{111}$$

Corollary 4 applied to $(\widehat{f}, w)$ (as factors of $b\, f$) and $(\widehat{g}, w)$ (as factors of $b\, g$) shows to

$$\|\widehat{f}\|_1\, \|w\|_1 \;\leq\; B \quad \text{and} \quad \|\widehat{g}\|_1\, \|w\|_1 \;\leq\; B \tag{112}$$

Finally, it follows from the way f^* and g^* are computed that we have in fact

$$\widehat{f} \;=\; f^* \quad \text{and} \quad \widehat{g} \;=\; g^* \tag{113}$$

and we proved that Relation (99) holds! $\lhd$

Remark 14 During the proof of Algorithm 1 between Relation (105) and Relation (110) we have established the following proposition which will lead to an improved algorithm.

Proposition 8 *Let f, g, h, p, ν, w be as in Algorithm 1. Let α be the lading coefficient of h. Then we have*

$$\deg(h) \;=\; \deg(\nu) \quad \Rightarrow \quad h \;=\; \mathrm{pp}(w). \tag{114}$$

PROOF $\rhd$ From Theorem 3 and $\deg(h) \;=\; \deg(\nu)$ we derive Relation (105). Together with the fact that α divides b and the definition of w this leads to Relation (106). Then Relations (105), (106) and (107) imply Relation (110) which shows $h \;=\; \mathrm{pp}(w)$. $\lhd$

Remark 15 From Theorem 3 we know that there are only a finite number of prime p for which the relation $\deg(h) \;=\; \deg(\nu)$ does not hold Moreover for those prime such $\deg(h) \;\neq\; \deg(\nu)$ the polynomial w has a higher degree than h. Hence we can simply Algorithm 1 into Algorithm 2. as follows.

Algorithm 2

Input: primitive polynomials $f, g \in \mathbb{Z}[x]$ such that $\deg(f) = n \geq \deg(g) \geq 1$ and $\|f\|_\infty, \|g\|_\infty \leq A$.

Output: $h = \gcd(f, g) \in \mathbb{Z}[x]$

$b := \gcd(\mathrm{lc}(f), \mathrm{lc}(g))$
$B := (n+1)^{1/2}\, 2^n\, A\, b$
repeat
  choose a prime p such that $2\,B < p$
  $\overline{f} := f \mod p$
  $\overline{g} := g \mod p$
  compute ν the monic gcd of $\overline{f}$ and $\overline{g}$ in $\mathbb{Z}/\langle p \rangle[x]$
  compute w such that $w \equiv b\,\nu \mod p$
  $w := \mathrm{normal}(\mathrm{pp}(w))$
until $w \mid f$ **and** $w \mid g$
return w

Remark 16 We aim now to realize the following improvements.

- We woulk like to use a CRA scheme which would allow us to work with small primes and thus to take advantage of machine integer arithmetic.
- We know that the bound B is most of the times very pessimistic. So we would like to try to exit before the bound is reached.
- We would like also to add optimizations like: when the modular gcd has degree 0 then h is 1.

This leads to Algorithm 3

Algorithm 3

Input: primitive polynomials $f, g \in \mathbb{Z}[x]$.

Output: $h = \gcd(f, g) \in \mathbb{Z}[x]$

$b := \gcd(\mathrm{lc}(f), \mathrm{lc}(g))$
$d := \min(\deg(f), \deg(g))$
$(m, g_m) := (1, 0)$
repeat
  choose a prime machine integer p such that $p \not| (m\, b)$
  $\overline{f} := f \mod p$
  $\overline{g} := g \mod p$
  compute g_p the monic gcd of $\overline{f}$ and $\overline{g}$ in $\mathbb{Z}/\langle p\rangle[x]$
  $g_p := b\, g_p$ in $\mathbb{Z}/\langle p\rangle[x]$
    with coefficients in $[-\frac{p-1}{2}, \frac{p-1}{2}]$
  if $\deg(g_p) = 0$ **then return** 1
  if $\deg(g_p) > d$ **then iterate** { unlucky reduction }
  if $\deg(g_p) < d$ **then** { previous reductions were unlucky }
    $(m, g_m, d) := (1, 0, \deg(g_p))$
  $w := \mathsf{combine}(p, m)(g_p, g_m)$
    with coefficients in $[-\frac{m\,p-1}{2}, \frac{m\,p-1}{2}]$
  $h := \mathrm{pp}(w)$
  if $h \mid f$ **and** $h \mid g$ **then return** h
  $(m, g_m) := (m\,p, w)$

7 A modular Gcd Algorithm in $\mathbb{Z}[x_1, \ldots, x_n]$

Algorithm 3 can be adapted to the case of more than one variable provided that we have a gcd algorithm in polynomial rings of the form $\mathbb{Z}/\langle p\rangle[x_1, \ldots, x_n]$. Algorithm 4 computes the gcd of two polynomials $f, g \in \mathbb{Z}[x_1, \ldots, x_n]$ with this assumption. Observe that Algorithm 4 takes as input any couple of multivariate polynomials over $\mathbb{Z}$, primitive or not.

Algorithm 4 relies also on the following technical assumptions.

- $f \in \mathbb{Z}[x_1, \ldots, x_n] \longmapsto \mathrm{content}_{\mathbb{Z}}(f)$ computes the content of a multivariate polynomial over $\mathbb{Z}$, that is **the** gcd of its coefficients. We make the same conventions as for the univariate case. See Definition 3.

- $(f \in \mathbb{Z}[x_1, \ldots, x_n], c \in R) \longmapsto f$ `exquo` c is the **exact** division of a polynomial by an integer. That is, assuming that c divides f, the value returned by f `exquo` c is the polynomial g such that $f = c\, g$.

- We need to specify what the *leading coefficient* and the *degree* of a multivariate polynomial are. To do so, we view polynomials as linear combinations of monomials with coefficients in $\mathbb{Z}$. To decide which is the leading monomial (and thus which is the leading coefficient) we assume that the variables are totally ordered, say $x_1 > \cdots > x_n$. Then to order monomials we use the lexicographic ordering induced by $x_1 > \cdots > x_n$.

- $f \in \mathbb{Z}[x_1, \ldots, x_n] \longmapsto \mathrm{lc}_{lex}(f)$ returns the leading coefficient of f w.r.t. the lexicographic ordering induced by $x_1 > \cdots > x_n$.

- $f \in \mathbb{Z}[x_1, \ldots, x_n] \longmapsto \deg_{lex}(f)$ returns the degreeof f w.r.t. the lexicographic ordering induced by $x_1 > \cdots > x_n$. That is the exponent vector of the leading monomial of f.

Algorithm 4

Input: $f, g \in \mathbb{Z}[x_1, \ldots, x_n]$.

Output: $h = \gcd(f, g) \in \mathbb{Z}[x]$

$(c_f, c_g) := (\mathrm{content}_{\mathbb{Z}}(f), \mathrm{content}_{\mathbb{Z}}(g))$
$c := \gcd_{\mathbb{Z}}(c_f, c_g)$
$(f, g) := (f \ \mathsf{exquo}\ c_f, g \ \mathsf{exquo}\ c_g)$
$b := \gcd(\mathrm{lc}_{lex}(f), \mathrm{lc}_{lex}(g))$
$d := \min(\deg_{lex}(f), \deg_{lex}(g))$
$(m, g_m) := (1, 0)$
repeat
  choose a prime machine integer p such that $p \not| (m\, b)$
  $\overline{f} := f \mod p$
  $\overline{g} := g \mod p$
  compute g_p the monic gcd of $\overline{f}$ and $\overline{g}$ in $\mathbb{Z}/\langle p\rangle[x_1, \ldots, x_n]$
  $g_p := b\, g_p$ in $\mathbb{Z}/\langle p\rangle[x]$
    with coefficients in $[-\frac{p-1}{2}, \frac{p-1}{2}]$
  if $\deg_{lex}(g_p) = 0$ **then return** 1
  if $\deg_{lex}(g_p) > d$ **then iterate** { unlucky reduction }
  if $\deg(g_p) < d$ **then** { previous reductions were unlucky }
    $(m, g_m, d) := (1, 0, \deg_{lex}(g_p))$
  $w := \mathsf{combine}(p, m)(g_p, g_m)$
    with coefficients in $[-\frac{m\,p-1}{2}, \frac{m\,p-1}{2}]$
  $h := c\ \mathrm{pp}(w)$
  if $\mathrm{pp}(w) \mid f$ **and** $\mathrm{pp}(w) \mid g$ **then return** h
  $(m, g_m) := (m\,p, w)$

Observations.

- The assumption of primtive input polynomials has been relaxed. However by dividing f and g by their contents, we turn back to the *primitive case*.
- The $\mathsf{combine}(p, m)(g_p, g_m)$ is in fact a series of CRA: one per monomial. Remember the case of the fast multication in $\mathbb{Z}[x]$ based on the FFT.
- Note that the result computed by the Chinese remainder algorithm (CRA) must be expressed in the symmetric range of the integers mod-

ulo $m\,p$ so that negative integer coefficients in w can be reconstructed as well as positive ones.

- The termination test can be improved in the sense that it may not be worth trying it before a certain amount of modular gcd have been computed. In practice, one could wait for the following stabilization condition
$$g_m = w \tag{115}$$
which will necessarily happen.

See [KM99] for more details and proofs.

8 A modular Gcd Algorithm in $E[x]$ with E Euclidean

We present now another generalization of Algorithm 3: the case of univariate polynomials over an Euclidean domain E with an Euclidean size δ. This idea appears in [KM99]. We need two assumptions for E.

First we assume that we have access to the stream of unassociated primes $p_1, p_2, p_3, \ldots,$ such that $\delta(p_1) < \delta(p_1 p_2) < \delta(p_1 p_2 p_3) < \cdots$. Indeed the recovery of an element a in E from $a \mod m = p_1 \cdots p_n$ requires sufficiently large m.

Secondly, we assume the avialability of a mapping scs from $E \times E \setminus \{0\}$ to E, called a *symmetric canonical simplifier*, such that we have the following properties.

Simplification. Any element $a \in E$ must satisfy $a \equiv \mathsf{scs}(a, m)$ for any $m \in E \setminus \{0\}$. More formally:
$$(\forall\; a \in E)(\forall\; m \in E \setminus \{0\}) \;\; a \;\equiv\; \mathsf{scs}(a, m). \tag{116}$$

Canonicity. For any $m \in E \setminus \{0\}$, any two elements $a, b \in E$ equivalent modulo m must satisfy $\mathsf{scs}(a, m) = \mathsf{scs}(b, m)$. More formally:
$$(\forall\; a, b \in E)(\forall\; m \in E \setminus \{0\}) \;\; (a \;\equiv\; b) \quad\Longleftrightarrow\quad (\mathsf{scs}(a, m) \;=\; \mathsf{scs}(b, m)). \tag{117}$$

Recoverage = symmetry. All elements of a bounded degree are recovered by the simplifier if the modulus is sufficiently large.

$$(\forall\, B > 0)(\exists\, M \in \mathbb{N})(\forall\, (a, m) \in E \times E \backslash \{0\}) \left\{ \begin{array}{l} \delta(m) \geq M(B) \\ \delta(a) < B \end{array} \right. \Rightarrow \mathsf{scs}(a, m) = a. \tag{118}$$

Algorithm 5

Input: $f, g \in E[x]$.

Output: $h = \gcd(f, g) \in E[x]$

$(c_f, c_g) := (\mathrm{content}_E(f), \mathrm{content}_E(g))$
$c := \gcd_E(c_f, c_g)$
$(f, g) := (f \ \mathsf{exquo}\ c_f, g \ \mathsf{exquo}\ c_g)$
$b := \gcd(\mathrm{lc}(f), \mathrm{lc}(g))$
$d := \min(\deg(f), \deg(g))$
$(m, g_m) := (1, 0)$
repeat
  choose a prime p such that $p \not| (m\, b)$
  $\overline{f} := f \mod p$
  $\overline{g} := g \mod p$
  compute g_p the monic gcd of $\overline{f}$ and $\overline{g}$ in $E/\langle p \rangle[x]$
  $g_p := \mathsf{scs}(b\, g_p, p)$ in $\mathbb{Z}/\langle p \rangle[x]$
  if $\deg(g_p) = 0$ **then return** 1
  if $\deg(g_p) > d$ **then iterate** { unlucky reduction }
  if $\deg(g_p) < d$ **then** { previous reductions were unlucky }
    $(m, g_m, d) := (1, 0, \deg(g_p))$
  $w := \mathsf{combine}(p, m)(g_p, g_m)$
  $w := \mathsf{scs}(w, m\, p)$
  $h := c\ \mathrm{pp}(w)$
  if $\mathrm{pp}(w) \mid f$ **and** $\mathrm{pp}(w) \mid g$ **then return** h
  $(m, g_m) := (m\, p, w)$

See [KM99] for more details.

9 Gcd Algorithms in $\mathbf{k}[x_1, \ldots, x_n]$ where $\mathbf{k}$ is a field

For $n = 2$ use the previous section, since $\mathbf{k}[x_1]$ is an Euclidean domain. Of course this requires some additional explanations. For $n > 2$ use evaluation-interpolation in order to reduce to the case $n = 2$. Again, some details would need to be added.

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. 2e 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.

[KM99] E. Kaltofen and M. Monagan. On the genericity of the modular polynomial gcd algorithm. In *Proc. ISSAC 1999*. ACM Press, 1999.