Computations Modulo Regular Chains

Xin Li, Marc Moreno Maza and Wei Pan
(University of Western Ontario)

ISSAC 2009, Seoul
July 30, 2009

Background

A historical application of the resultant is to compute the intersection of two plane curves. Up to details, there are two steps:

- eliminate one variable by computing a resultant,
- compute a GCD modulo this resultant.

Example (From MCA, Chapter 6)

Let $P = \left(y^2+6\right)(x-1) - y\left(x^2+1\right)$ and $Q = \left(x^2+6\right)(y-1) - x\left(y^2+1\right)$

- $\mathrm{res}(P, Q, y) = 2\,\left(x^2 - x + 4\right)(x-2)^2(x-3)^2$.
- $\gcd(P, Q, x-2=0) = (y-2)(y-3)$.
- $\gcd(P, Q, x-3=0) = (y-2)(y-3)$.
- $\gcd(P, Q, x^2-x+4=0) = (2\,x-1)\,y - 7 - x$.

Regular GCD

- Let $\mathbb{B}$ be a commutative ring with units. Let $P, Q \in \mathbb{B}[y]$ be non-constant with regular leading coefficients.
- $G \in \mathbb{B}[y]$ is a *regular GCD* of P, Q if we have:
  - (*i*) $\mathrm{lc}(G, y)$ is a regular element of $\mathbb{B}$,
  - (*ii*) $G \in \langle P, Q \rangle$ in $\mathbb{B}[y]$,
  - (*iii*) $\deg(G, y) > 0 \quad \Rightarrow \quad \mathrm{prem}(P, G, y) = \mathrm{prem}(Q, G, y) = 0$.

Regular GCD

- Let $\mathbb{B}$ be a commutative ring with units. Let $P, Q \in \mathbb{B}[y]$ be non-constant with regular leading coefficients.
- $G \in \mathbb{B}[y]$ is a *regular GCD* of P, Q if we have:
  - (*i*) $\mathrm{lc}(G, y)$ is a regular element of $\mathbb{B}$,
  - (*ii*) $G \in \langle P, Q \rangle$ in $\mathbb{B}[y]$,
  - (*iii*) $\deg(G, y) > 0 \quad \Rightarrow \quad \mathrm{prem}(P, G, y) = \mathrm{prem}(Q, G, y) = 0$.
- In practice $\mathbb{B} = \mathbf{k}[x_1, \ldots, x_n]/\mathrm{sat}(T)$, with T being a regular chain.

Regular GCD

- Let $\mathbb{B}$ be a commutative ring with units. Let $P, Q \in \mathbb{B}[y]$ be non-constant with regular leading coefficients.
- $G \in \mathbb{B}[y]$ is a *regular GCD* of P, Q if we have:
  - (*i*) $\mathrm{lc}(G, y)$ is a regular element of $\mathbb{B}$,
  - (*ii*) $G \in \langle P, Q \rangle$ in $\mathbb{B}[y]$,
  - (*iii*) $\deg(G, y) > 0 \quad \Rightarrow \quad \mathrm{prem}(P, G, y) = \mathrm{prem}(Q, G, y) = 0$.
- In practice $\mathbb{B} = \mathbf{k}[x_1, \ldots, x_n]/\mathrm{sat}(T)$, with T being a regular chain.
- Such a regular GCD may not exist. However one can compute $\mathcal{I}_i = \mathrm{sat}(T_i)$ and non-zero polynomials G_i such that

$$\sqrt{\mathcal{I}} = \cap_{i=0}^{e} \sqrt{\mathcal{I}_i} \quad \text{and} \quad G_i \quad \text{regular GCD of} \quad P, Q \bmod \mathcal{I}_i$$

Regularity test

- Regularity test is a fundamental operation:

$$\mathrm{Regularize}(p, \mathcal{I}) \quad \longmapsto \quad (\mathcal{I}_1, \ldots, \mathcal{I}_e)$$

  such that:

$$\sqrt{\mathcal{I}} = \cap_{i=0}^{e} \sqrt{\mathcal{I}_i} \quad \text{and} \quad p \in \mathcal{I}_i \text{ or } p \text{ regular modulo } \mathcal{I}_i$$

- Regularity test reduces to regular GCD computation.

Related work

- This notion of a regular GCD was proposed in (M. M. 2000)
- In previous work (Kalkbrener 1993) and (Rioboo & M. M. 1995), other regular GCDs modulo regular chains were introduced, but with limitations.
- In other work (Wang 2000), (Yang etc. 1995) and (Jean Della Dora, Claire Dicrescenzo, Dominique Duval 85), related techniques are used to construct triangular decompositions.
- Regular GCDs modulo regular chains generalize GCDs over towers of field extentions for which specialized algorithms are available, (van Hoeij and Monagan 2002 & 2004).

Overview

- We study the relations between subresultants and regular GCDs. We insist on the case where $\mathrm{sat}(T)$ is not radical.

Overview

- We study the relations between subresultants and regular GCDs. We insist on the case where $\mathrm{sat}(T)$ is not radical.
- We present a new algorithm to compute regular GCDs.
    - Compute subresultant chains over the base field (typically $\mathbb{Z}/p\mathbb{Z}[\mathbf{x}]$)
    - Discover GCDs in a bottom-up manner.

Overview

- We study the relations between subresultants and regular GCDs. We insist on the case where $\mathrm{sat}(T)$ is not radical.
- We present a new algorithm to compute regular GCDs.
  - Compute subresultant chains over the base field (typically $\mathbb{Z}/p\mathbb{Z}[\mathbf{x}]$)
  - Discover GCDs in a bottom-up manner.
- This allows us to apply fast polynomial arithmetic over the base field and to make the computations as lazy as possible.

Overview

- We study the relations between subresultants and regular GCDs. We insist on the case where $\mathrm{sat}(T)$ is not radical.
- We present a new algorithm to compute regular GCDs.
  - Compute subresultant chains over the base field (typically $\mathbb{Z}/p\mathbb{Z}[\mathbf{x}]$)
  - Discover GCDs in a bottom-up manner.
- This allows us to apply fast polynomial arithmetic over the base field and to make the computations as lazy as possible.
- In most cases, our new code outperforms the other packages by several orders of magnitude.

Regular Chain

- Let $T \subset \mathbf{k}[x_1 < \cdots < x_n] \setminus \mathbf{k}$ be a triangular set, hence the polynomials of T have pairwise distinct main variables.
- $\mathrm{mvar}(T) := \{\mathrm{mvar}(t) \mid t \in T\}$ and $\mathrm{init}(t) := \mathrm{lc}(t, \mathrm{mvar}(t))$ for all $t \in T$.
- T_v is the polynomial of T with main variable v and $T_{<v} = \{t \in T \mid \mathrm{mvar}(t) < v\}$.
- The saturated ideal of T is the ideal of $\mathbf{k}[x_1 < \cdots < x_n]$ defined by
$$\mathrm{sat}(T) := \langle T \rangle : h^\infty,$$
where h is the product of initials in T.
- T is a regular chain if for each $v \in \mathrm{mvar}(T)$ the initial of T_v is regular modulo $\mathrm{sat}(T_{<v})$.

Subresultants

- Let $P, Q \in \mathbb{B}[y]$ with $p = \deg(P) \geq \deg(Q) = q > 0$.
- For $0 \leq d < q$ let $S_d = S_d(P, Q)$ be the d-th *subresultant* of P and Q. Let $s_d = \mathrm{coeff}(S_d, x^d)$. If $s_d = 0$ we say S_d is defective, otherwise we say S_d is non-defective.
- Let $d = q-1, \ldots, 1$. Assume S_d, S_{d-1} nonzero, with resp. degrees d and e. Assume s_d regular in $\mathbb{B}$. Then we have

$$\mathrm{lc}(S_{d-1})^{d-e-1} S_{d-1} = {s_d}^{d-e-1} S_e.$$

- Moreover, there exists $C_d \in \mathbb{B}[X]$ such that we have:

$$(-1)^{d-1} \mathrm{lc}(S_{d-1}) s_e S_d + C_d S_{d-1} = {s_d}^2 S_{e-1}.$$

  In addition $S_{d-2} = S_{d-3} = \cdots = S_{e+1} = 0$ also holds.
- (Yap 1993) (Ducos 1997) (El Kahoui, 2003)

Regular GCDs (1/6)

- Let $P, Q \in \mathbf{k}[\mathbf{x}][y]$ with $\mathrm{mvar}(P) = \mathrm{mvar}(Q) = y$.
- Define $R = \mathrm{res}(P, Q, y)$.
- Let $T \subset \mathbf{k}[x_1, \ldots, x_n]$ be a regular chain such that
  - $R \in \mathrm{sat}(T)$,
  - $\mathrm{init}(P)$ and $\mathrm{init}(Q)$ are regular modulo $\mathrm{sat}(T)$.
- $\mathbb{A} = \mathbf{k}[x_1, \ldots, x_n]$ and $\mathbb{B} = \mathbf{k}[x_1, \ldots, x_n]/\mathrm{sat}(T)$.
- For $0 \leq j \leq \mathrm{mdeg}(Q)$, we write S_j for the j-th subresultant of P, Q in $\mathbb{A}[y]$.

Regular GCDs (2/6)

- Let $1 \leq d \leq q$ such that $S_j \in \mathrm{sat}(T)$ for all $0 \leq j < d$.

Lemma

If $\mathrm{lc}(S_d, y)$ is regular modulo $\mathrm{sat}(T)$, then S_d is non-defective over $\mathbf{k}[\mathbf{x}]$.

- Consequently, S_d is the last nonzero subresultant over $\mathbb{B}$, and it is also non-defective over $\mathbb{B}$.
- If $\mathrm{lc}(S_d, x_n)$ is not regular modulo $\mathrm{sat}(T)$ then S_d may be defective over $\mathbb{B}$.

Regular GCDs (3/6)

- Let $1 \leq d \leq q$ such that $S_j \in \mathrm{sat}(T)$ for all $0 \leq j < d$.

Lemma

If $\mathrm{lc}(S_d, y)$ is in $\mathrm{sat}(T)$, then S_d is nilpotent modulo $\mathrm{sat}(T)$.

- Up to sufficient splitting of $\mathrm{sat}(T)$, S_d will vanish on all the components of $\mathrm{sat}(T)$.
- The above two lemmas completely characterize the last non-zero subresultant of P and Q over $\mathbb{B}$.

Regular GCDs (4/6)

Example

- Consider P and Q in $\mathbb{Q}[x_1, x_2][y]$:

$$P = x_2^2 y^2 - x_1^4 \text{ and } Q = x_1^2 y^2 - x_2^4.$$

- We have:

$$S_1 = x_1^6 - x_2^6 \text{ and } R = (x_1^6 - x_2^6)^2.$$

- Let $T = \{R\}$. Then we observe:
  - The last subresultant of P, Q modulo $\mathrm{sat}(T)$ is S_1, which is a defective one.
  - S_1 is nilpotent modulo $\mathrm{sat}(T)$.
- P and Q do not admit a regular GCD over $\mathbb{Q}[x_1, x_2]/\mathrm{sat}(T)$.

Regular GCDs (5/6)

- Let $1 \leq d \leq q$ such that $S_j \in \mathrm{sat}(T)$ for all $0 \leq j < d$.

Proposition

Assume

- $\mathrm{lc}(S_d, y)$ *is regular modulo* $\mathrm{sat}(T)$*,*
- $\mathrm{sat}(T)$ *is radical.*

Then, S_d *is a regular GCD of* P, Q *modulo* $\mathrm{sat}(T)$*.*

Regular GCDs (5/6)

- Let $1 \leq d \leq q$ such that $S_j \in \mathrm{sat}(T)$ for all $0 \leq j < d$.

Proposition

Assume

- $\mathrm{lc}(S_d, y)$ *is regular modulo* $\mathrm{sat}(T)$,
- $\mathrm{sat}(T)$ *is radical.*

Then, S_d *is a regular GCD of* P, Q *modulo* $\mathrm{sat}(T)$.

Recall that S_d regular GCD of P, Q modulo $\mathrm{sat}(T)$ means

(*i*) $\mathrm{lc}(S_d, y)$ is a regular element of $\mathbb{B}$,

(*ii*) $S_d \in \langle P, Q \rangle$ in $\mathbb{B}[y]$,

(*iii*) $\deg(S_d, y) > 0 \quad \Rightarrow \quad \mathrm{prem}(P, S_d, y) = \mathrm{prem}(Q, S_d, y) = 0$.

Regular GCDs (5/6)

- Let $1 \leq d \leq q$ such that $S_j \in \mathrm{sat}(T)$ for all $0 \leq j < d$.

Proposition

Assume

- $\mathrm{lc}(S_d, y)$ *is regular modulo* $\mathrm{sat}(T)$,
- $\mathrm{sat}(T)$ *is radical.*

Then, S_d *is a regular GCD of* P, Q *modulo* $\mathrm{sat}(T)$.

Proposition

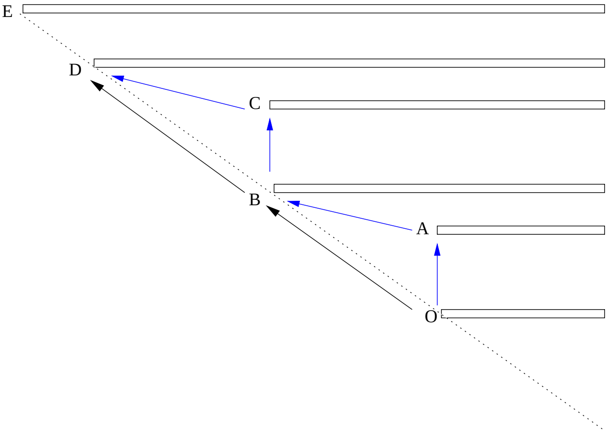
Assume

- $\mathrm{lc}(S_d, y)$ *is regular modulo* $\mathrm{sat}(T)$,
- *for all* $d < k \leq q$, $\mathrm{coeff}(S_k, y^k)$ *is either* 0 *or regular modulo* $\mathrm{sat}(T)$.

Then, S_d *is a regular GCD of* P, Q *modulo* $\mathrm{sat}(T)$.

Regular GCDs (6/6)

- Assume that the subresultants S_j for $1 \le j < q$ are computed.
- Then one can compute a regular GCD of P, Q modulo $\mathrm{sat}(T)$ by performing a bottom-up search.



Complexity Estimates

We assume that the the base field **k** supports FFT.

- Let $x_{n+1} := y$. Define $d_i := \max(\deg(P, x_i), \deg(Q, x_i))$. Define $b_i := 2d_i d_{n+1}$ and $B := (b_1 + 1) \cdots (b_n + 1)$.

Complexity Estimates

We assume that the the base field **k** supports FFT.

- Let $x_{n+1} := y$. Define $d_i := \max(\deg(P, x_i), \deg(Q, x_i))$. Define $b_i := 2d_i d_{n+1}$ and $B := (b_1 + 1) \cdots (b_n + 1)$.
- We compute S_j for $1 \leq j < \mathrm{mdeg}(Q)$ via FFT on an n-dim. grid of points not cancelling $\mathrm{init}(P)$ and $\mathrm{init}(Q)$ in

$$O(d_{n+1} B \log(B) + d_{n+1}^2 B) \quad \text{where} \quad B \in O(2^n d_{n+1}^n d_1 \ldots d_n).$$

Complexity Estimates

We assume that the the base field **k** supports FFT.

- Let $x_{n+1} := y$. Define $d_i := \max(\deg(P, x_i), \deg(Q, x_i))$. Define $b_i := 2d_i d_{n+1}$ and $B := (b_1 + 1) \cdots (b_n + 1)$.
- We compute S_j for $1 \leq j < \mathrm{mdeg}(Q)$ via FFT on an n-dim. grid of points not cancelling $\mathrm{init}(P)$ and $\mathrm{init}(Q)$ in

$$O(d_{n+1} B \log(B) + d_{n+1}^2 B) \quad \text{where} \quad B \in O(2^n d_{n+1}^n d_1 \ldots d_n).$$

- Then $\mathrm{res}(P, Q, y) = S_0$ is interpolated in time $O(B \log(B))$.

Complexity Estimates

We assume that the the base field **k** supports FFT.

- Let $x_{n+1} := y$. Define $d_i := \max(\deg(P, x_i), \deg(Q, x_i))$. Define $b_i := 2d_i d_{n+1}$ and $B := (b_1 + 1) \cdots (b_n + 1)$.
- We compute S_j for $1 \leq j < \mathrm{mdeg}(Q)$ via FFT on an n-dim. grid of points not cancelling $\mathrm{init}(P)$ and $\mathrm{init}(Q)$ in

$$O(d_{n+1} B \log(B) + d_{n+1}^2 B) \quad \text{where} \quad B \in O(2^n d_{n+1}^n d_1 \ldots d_n).$$

- Then $\mathrm{res}(P, Q, y) = S_0$ is interpolated in time $O(B \log(B))$.
- If $\mathrm{sat}(T)$ is radical, a regular GCD is interpolated within $O(d_{n+1} B \log(B))$; otherwise $O(d_{n+1}^2 B \log(B))$.

Complexity Estimates

We assume that the the base field **k** supports FFT.

- Let $x_{n+1} := y$. Define $d_i := \max(\deg(P, x_i), \deg(Q, x_i))$. Define $b_i := 2 d_i d_{n+1}$ and $B := (b_1 + 1) \cdots (b_n + 1)$.
- We compute S_j for $1 \leq j < \mathrm{mdeg}(Q)$ via FFT on an n-dim. grid of points not cancelling $\mathrm{init}(P)$ and $\mathrm{init}(Q)$ in

$$O(d_{n+1} B \log(B) + d_{n+1}^2 B) \quad \text{where} \quad B \in O(2^n d_{n+1}^n d_1 \ldots d_n).$$

- Then $\mathrm{res}(P, Q, y) = S_0$ is interpolated in time $O(B \log(B))$.
- If $\mathrm{sat}(T)$ is radical, a regular GCD is interpolated within $O(d_{n+1} B \log(B))$; otherwise $O(d_{n+1}^2 B \log(B))$.
- If a regular GCD is expected to have degree 1 in y all computations fit in $O\tilde{~}(d_{n+1} B)$.

Regularity Test

T a normalized zero-dimensional regular chain. Q a polynomial with initial regular modulo $\mathrm{sat}(T)$.

RegularizeDim0(Q, T) ==

(1) $Results := []$; $v := \mathrm{mvar}(Q)$

(2) $R := \mathrm{res}(Q, T_v, v)$

(3) **for** $D \in$ RegularizeDim0(R, $T_{<v}$) **do**

(4) $\quad s :=$ NormalForm(R, D)

(5) $\quad$ **if** $s \neq 0$ **then**

(7) $\quad\quad Results := \{\{D \cup \{T_v\} \cup T_{>v}\}\} \cup Results$

(8) $\quad$ **else for** $(g, E) \in$ RegularGcd(Q, T_v, D) **do**

(9) $\quad\quad g :=$ NormalForm(g, E)

(11) $\quad\quad Results := \{\{E \cup \{g\} \cup T_{>v}\}\} \cup Results$

(12) $\quad\quad c :=$ NormalForm($\mathrm{quo}(T_v, g)$, E)

(13) $\quad\quad$ **if** $\deg(c, v) > 0$ **then**

(14) $\quad\quad\quad Results :=$ RegularizeDim0(q, $E \cup c \cup T_{>}v$) $\cup$ $Results$

(15) **return** $Results$

Experimentation in Maple

$d_1 = d_2$	Lex-Basis	Solve	Triang.	FastTriang.
4	0.020	0.040	0.152	0.020
7	0.020	0.580	0.424	0.016
10	0.064	3.892	0.680	0.020
13	0.136	16.557	1.424	0.024
16	0.232	55.939	2.324	0.032
22	0.552	416.466	13.972	0.044
25	0.804	1116.045	22.346	0.048
28	1.124	2162.271	58.695	0.056

Table: Bivariate solving. 32-bit Characterisitic. Generic input

Experimentation in Maple

$d_1 = d_2$	Lex-Basis	Solve	Triang	FTriang
5	0.014	0.080	0.616	0.016
8	0.152	3.004	3.200	0.048
11	0.908	44.407	10.049	0.124
14	6.837	246.839	25.902	0.428
17	36.581	1266.958	55.014	0.938
20	156.245	6296.301	92.662	1.740
23	627.551	21758.120	222.897	2.625

Table: Bivariate solving. 32-bit Characteristic. Highly non-equiprojectable systems

Experimentation Magma vs our Code

$d_1 = d_2$	Lex-GB (Magma)	Triang (Magma)	FastTriang (Maple)
5	0.010	0.010	0.016
8	0.040	0.070	0.048
11	0.190	0.360	0.124
14	0.730	1.210	0.428
17	2.170	3.300	0.938
20	5.510	7.810	1.740
23	12.430	17.220	2.625

Table: Bivariate solving. Highly non-equiprojectable case.

Experimentation Magma vs our Code

d_1	d_2	d_3	Regularize	Fast Regularize	Magma
2	2	3	0.032	0.004	0.010
3	4	6	0.160	0.016	0.020
4	6	9	0.404	0.024	0.060
5	8	12	>100	0.129	0.330
6	10	15	>100	0.272	1.300
7	12	18	>100	0.704	5.100
8	14	21	>100	1.276	14.530
9	16	24	>100	5.836	40.770
10	18	27	>100	9.332	107.280
11	20	30	>100	15.904	229.950
12	22	33	>100	33.146	493.490

Table: Random dense input. 3-variable case.

Conclusions

- We have given sufficient conditions for a subresultant S_d of P, Q to be a regular GCD modulo $\mathrm{sat}(T)$.

Conclusions

- We have given sufficient conditions for a subresultant S_d of P, Q to be a regular GCD modulo $\mathrm{sat}(T)$.
- We have insisted on the non-radical case. In particular, in the long version of the paper in the `CoRR` repository.

Conclusions

- We have given sufficient conditions for a subresultant S_d of P, Q to be a regular GCD modulo $\mathrm{sat}(T)$.
- We have insisted on the non-radical case. In particular, in the long version of the paper in the `CoRR` repository.
- We have derived a bottom-up algorithm, which permits efficient implementation techniques.

Conclusions

- We have given sufficient conditions for a subresultant S_d of P, Q to be a regular GCD modulo $\mathrm{sat}(T)$.
- We have insisted on the non-radical case. In particular, in the long version of the paper in the `CoRR` repository.
- We have derived a bottom-up algorithm, which permits efficient implementation techniques.
- Our implementation `Maple13:-RegularChains:-FastArithmeticTools` for dense polynomials over $\mathbb{Z}/p\mathbb{Z}$ often outperforms related packages by several orders of magnitude.
- See also the poster *Balanced Dense Multiplication on Multi-cores* for the latest development in the dense case.

Thank you!

Example: Bivariate System Solving

- Let $P, Q \in \mathbb{Z}/p\mathbb{Z}[x_1, x_2]$. Assume $\deg(P, x_2) \geq \deg(Q, x_2) > 0$ and $R = \mathrm{res}(P, Q, x_2) \notin \mathbb{Z}/p\mathbb{Z}$ and $\gcd(\mathrm{lc}(P, x_2), \mathrm{lc}(Q, x_2)) = 1$.
- Assume P, Q admits a regular GCD G modulo $\langle R \rangle$. Then we have
$$V(P, Q) = V(R, G).$$
- Hence $V(P, Q)$ can be decomposed at the cost of computing R that is $O^{\sim}(d_2^2 d_1)$ operations in $\mathbb{Z}/p\mathbb{Z}$.
- The assumptions can be relaxed and in the worst case the running time is $O^{\sim}(d_2^3 d_1)$.

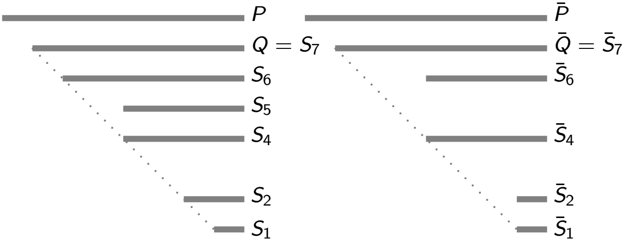


Figure: A possible configuration of the subresultant chain of P and Q. On the left, P and Q have five nonzero subresultants over $\mathbf{k}[\mathbf{X}]$, four of which are non-defective and one of which is defective. Let T be a regular chain in $\mathbf{k}[\mathbf{X}]$ such that $\mathrm{lc}(P)$ and $\mathrm{lc}(Q)$ are regular modulo $\mathrm{sat}(T)$. Further, we assume that $\mathrm{lc}(S_1)$ and $\mathrm{lc}(S_4)$ are regular modulo $\mathrm{sat}(T)$, however, $\mathrm{lc}(S_6)$ is in $\mathrm{sat}(T)$. The right hand side is a possible configuration of the subresultant chain of $\bar{P}$ and $\bar{Q}$. In this case, S_1 is a regular gcd of P and Q modulo $\mathrm{sat}(T)$.