Computing with polynomials over algebraic number fields

Michael Monagan

Department of Mathematics, Simon Fraser University

Bordeaux, July 12, 2022

The GCD problem in $K[x]$ and $K[x_1, x_2, \ldots, x_n]$

Let $K = \mathbb{Q}(\alpha_1, \alpha_2, ..., \alpha_k)$ be an algebraic number field and let A and B be polynomials over K.

Problem: How can we compute $\gcd(A, B)$ in $K[x]$? in $K[x_1, x_2, ..., x_n]$?
Application: Trager's algorithm for factoring polynomials over K.
Do not use the Euclidean algorithm in $K[x]$! Why?

The GCD problem in $K[x]$ and $K[x_1, x_2, \ldots, x_n]$

Let $K = \mathbb{Q}(\alpha_1, \alpha_2, ..., \alpha_k)$ be an algebraic number field and let A and B be polynomials over K.

Problem: How can we compute $\gcd(A, B)$ in $K[x]$? in $K[x_1, x_2, ..., x_n]$?
Application: Trager's algorithm for factoring polynomials over K.
Do not use the Euclidean algorithm in $K[x]$! Why?

Smedley 1989 $(k = 1)$ uses single point evaluation.
Let $m(z)$ be the M.P. for α_1. Replace α_1 by an integer b and compute mod $m(b)$.

Langemyr 1989 $(k = 1)$ for α_1 an algebraic integer.
Compute $\gcd(A, B)$ modulo primes $p_1, p_2, p_3, \ldots$ and apply the CRT.

Encarnacion 1995 $(k = 1)$ uses rational number reconstruction.

van Hoeij and Monagan 2002 $(k \geq 1)$ generalizes Encarnacion

Javadi 2007 $(k \geq 1, n \geq 1)$ uses Zippel's sparse polynomial interpolation.

Rational number reconstruction

```
> p1,p2 := 10^4+7,10^4+9;
```

$$p1, p2 := 10007, 10009$$

```
> u1 := 101/103 mod p1;
```

$$u1 := 1264$$

```
> u2 := 101/103 mod p1;
```

$$u2 := 2236$$

```
> um := chrem([u1,u2],[p1,p2]);
```

$$um := 95297925$$

```
> iratrecon(um,p1*p2);
```

$$\frac{101}{103}$$

Paul Wang 1981, Wang+Guy+Davenport 1982, Monagan 2004

Computing in $K = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_k)$

How do we represent elements of $K = \mathbb{Q}(\alpha_1, \alpha_2, ..., \alpha_k)$?

Build K as a sequence of k quotients.

> Set $K_0 = \mathbb{Q}$.
> For $i = 1$ to k do
> > Let $m_i(z_i)$ be the minimal polynomial for α_i over K_{i-1} and let $d_i = \deg(m_i, z_i)$.
> > Set $K_i = K_{i-1}[z_i]/\langle m_i \rangle$.

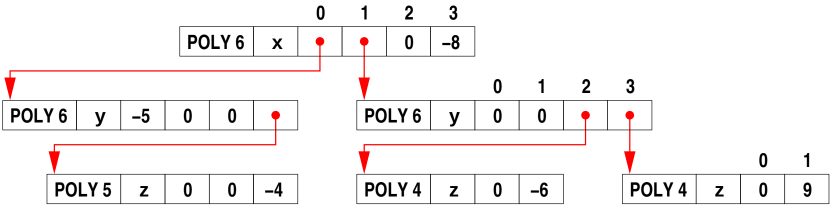
We have $K_k \simeq K$ and $\dim(K : \mathbb{Q}) = \prod_{i=1}^{k} d_i = d$.

Method 1 : Compute in $\mathbb{Q}[z_1, \ldots, z_k]/\langle m_1, \ldots, m_k \rangle$ using Groebner bases.
Method 2 : Compute in K_k using univariate polynomial arithmetic.

Pari's Dense Recursive Polynomial Data Structure

Use $\mathbb{Q}[x, y, z] \simeq \mathbb{Q}[z][y][x]$!

Pari's representation for $-5 - 4\,z^2y^3 - 6\,zy^2x + 9\,zy^3x - 8\,x^3$



Richard Fateman [2003] Comparing the speed of programs for sparse polynomial multiplication. *SIGSAM Bulletin*, **37**(1):4–15.

I was inspired by this and used dense recursive polynomials for GCDs in $K[x]$ in Maple.

Method 2: Using Recursive Quotients

```
> f := rpoly( 3*x^2+5*y^2, [x,y] );
```

$$3x^2 + 5y^2$$

```
> lprint(f);
POLYNOMIAL([0, [x, y], []], [[0, 0, 5], 0, [3]])
```

```
> m1,m2 := z^3-2,y^2-3*z-1;
```

$$m1, m2 := z^3 - 2,\ y^2 - 3\,z - 1$$

```
> f := rpoly( 2*x^2 + 3*y*x + 5*z, [x,y,z], [m1,m2] );
```

$$2x^2 + 3yx + 5z \mod \langle y^2 - 3z - 1, z^3 - 2 \rangle$$

```
> getring(f);
```

$$[0, [x, y, z], [\,[[-1, -3], 0, [1]], [-2, 0, 0, 1]\,]]$$

Maple demo of RECDEN
Monagan and van Hoeij 2002

Benchmark for $\dim(K : \mathbb{Q}) = 32$

```
? x+y+z+u+w;    /* Henri, is there a better way to force x>y>z>u>w ? */
? p = 2^25-855; /* p = 2^31-399; p = 2^62-923; */
? m1 = w^2+w+1;
? m2 = u^4-u*w-2;
? m3 = z^2-z*u-4;
? m4 = y^2-3*y*z-u;
/* K = Z/pZ[y,z,u,w]/<m1,m2,m3,m4>  */
? zero = Mod(Mod(Mod(Mod(Mod(0,p),m1),m2),m3),m4);
? g = x+2*u*y+5*z+4*w*u+3 + zero;
? a = x+y*w+6*z+7*w*u+8 + zero;
? b = x+y*z+9*y*u+2*w+2 + zero;
? n = 7; /* n = 3, 4, 7, 15, 31, 61, 127 */
? aa = g*a^n; bb = g*b^n;
? monicgcd = (a,b) -> {G = gcd(a,b); G/pollead(G)};
? for( i=1, 100, H=monicgcd(aa,bb) );
? ##
  ***   last result: cpu time 4,360 ms, real time 4,373 ms.
? liftall(H)
%276 = x + (2*u*y + (5*z + (4*w*u + 3)))
```

Table: Timings in CPU seconds for $k = 4 (k = 1)$ with $[K : \mathbb{Q}] = 32$.

$p = 2^{25} - 855$

n	Pari	Magma	Maple	ipgcd - C code
3	1.178(0.0301)	0.36(0.087)	0.11(0.045)	0.067(0.0155)
7	4.371(0.0691)	1.10(0.159)	0.30(0.101)	0.257(0.0484)
15	16.66(0.1821)	3.36(0.471)	0.97(0.275)	0.972(0.1617)
31	64.29(0.5507)	11.52(1.711)	3.25(0.799)	3.652(0.579)
61	239.1(1.754)	38.80(6.160)	11.1(2.616)	13.37(2.046)
127	STACK(6.734)	158.2(26.36)	45.28(10.23)	56.11(8.403)

$p = 2^{62} - 923$

n	Pari	Magma	Maple	ipgcd - C code
3	1.307(0.0722)	1.37(0.230)	1.535(BUG)	0.097(0.0234)
7	4.910(0.1870)	3.90(0.597)	5.184(BUG)	0.369(0.0760)
15	18.71(0.5320)	12.04(1.755)	18.34(BUG)	1.378(0.2609)
31	72.56(1.703)	40.26(5.830)	66.38(BUG)	5.264(0.948)
61	268.3(5.632)	148.4(19.85)	231.5(BUG)	19.12(3.375)
127	STACK(22.09)	662.0(79.40)	954.3(BUG)	77.84(13.95)

Why is $k = 1$ field extension so much faster than $k = 4$ extensions?

Use a primitive element from K modulo p

Input $K = \mathbb{Q}[z_1, \ldots, z_k]/\langle m_1(z_1), \ldots, m_k(z_k)\rangle$.

Let $d = \prod_{i=1}^{k} \deg(m_i, z_i)$.
repeat
Pick non-zero $c_i \in \mathbb{Z}$ and set $\gamma = \sum_{i=1}^{k} c_i z_i$.
Let $m(z)$ be the minimal polynomial for γ over $\mathbb{Q}$.
until $\deg(m, z) = d$. // This means $\mathbb{Q}[z]/\langle m(z)\rangle \simeq K$
Compute an isomorphism $\varphi : K \to \mathbb{Q}[z]/m(z)$.

Example $K = \mathbb{Q}[x, y]/\langle x^2 - 2, y^2 - 3\rangle$ with $c_1 = c_2 = 1, \gamma = x + y$,

$m = z^4 - 10z^2 + 1, \quad \varphi(1) = 1, \quad \varphi(x) = \frac{9}{2}z - \frac{1}{2}z^3, \quad \varphi(y) = -\frac{11}{2}z + \frac{1}{2}z^3$

and $\varphi(xy) = \varphi(x)\varphi(y) = \frac{1}{2}z^2 + \frac{7}{2}$.

Do this modulo a prime p to avoid large fractions!

How do we compute $m(z)$ and φ mod p ?

Method 1: Groebner bases

```
> B := [x^2-2,y^2-3,z-(1*x+1*y)];
```

$$[x^2 - 2, y^2 - 3, z - x - y]$$

```
> G := Groebner[Basis](B,plex(x,y,z));  # x > y > z
```

$$G \ := \ [z^4 - 10z^2 + 1, z^3 + 2y - 11z, -z^3 + 2x + 9z]$$

```
> phi(x) = solve(G[3],x), phi(y) = solve(G[2],y);
```

$$\phi(x) = -\frac{9}{2}z + \frac{1}{2}z^3, \ \phi(y) = \frac{11}{2}z - \frac{1}{2}z^3$$

```
> Groebner[Basis](B,plex(z,x,y));  # z > x > y
```

$$[y^2 - 3, x^2 - 2, z - x - y]$$

We can use FGLM (Faugere, Gianni, Lazard, Miola)! Costs $O(kd^3)$.

Method 2: Linear Algebra

K is a vector space over $\mathbb{Q}$ of dimension $d = \dim(K : \mathbb{Q})$.
Let $m(z) = z^d + \sum_{i=0}^{d-1} x_i z^i$ where $x_i \in \mathbb{Q}$.
Pick non-zero $c_i \in \mathbb{Z}$ and let $\gamma = \sum_{i=1}^{k} c_i z_i$.
Then

$$m(\gamma) = 0 \implies A = \begin{bmatrix} \vdots & \vdots & \vdots & \dots & \vdots \\ 1 & \gamma & \gamma^2 & \dots & \gamma^{d-1} \\ \vdots & \vdots & \vdots & \dots & \vdots \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} \vdots \\ -\gamma^d \\ \vdots \end{bmatrix} = b$$

Compute A then A^{-1} then $x = A^{-1} b$ all modulo p.
Costs $O(d^3) + O(d^3) + O(d^2)$ arithmetic operations in $\mathbb{Z}/p\mathbb{Z}$.

Method 3: Iterated Resultants

Use the subresultant algorithm to eliminate z_k then z_{k-1}, ... then z_1 from $z - \gamma$ where $\gamma = \sum_{i=1}^{k} c_i z_i$.
Example $K = \mathbb{Q}[x, y]/\langle x^2 - 2, y^2 - 3\rangle$ with $\gamma = x + y$.

SubresultantAlgorithm($z - x - y,\ x^2 - 2,\ x$) in $R[z][x]$ where $R = \mathbb{Q}[y]/(y^2 - 3)$.
Output: $x^2 - 2,\ z - x - y,\ -2zy + z^2 + 1$.

SubresultantAlgorithm($-2zy + z^2 + 1,\ y^2 - 3,\ y$) in $\mathbb{Q}[z][y]$.
Output: $y^2 - 3,\ -2zy + z^2 + 1,\ z^4 - 10z^2 + 1$.

Set $m(z) = z^4 - 10z^2 + 1$ and $L = \mathbb{Q}[z]/\langle m(z)\rangle$.

Solve $-2zy + z^2 + 1$ for y over L (invert $-2z$ in L)) to get $\varphi(y)$
Solve $z - x - \varphi(y)$ for x over L to get $\varphi(x)$.

Use evaluation/interpolation on z ?
What can go wrong mod p ?
Cost ?

Using Method 2: Linear Algebra (column phigcd)

Table: Timings in CPU seconds for $k = 4 (k = 1)$ with $[K : \mathbb{Q}] = 32$.

$p = 2^{25} - 855$

n	Pari	Magma	Maple	ipgcd	phigcd(%phi)
3	1.178(0.0301)	0.36(0.087)	0.11(0.045)	0.067(0.0155)	0.081(77.8%)
7	4.371(0.0691)	1.10(0.159)	0.30(0.101)	0.257(0.0484)	0.117(59.3%)
15	16.66(0.1821)	3.36(0.471)	0.97(0.275)	0.972(0.1617)	0.238(26.2%)
31	64.29(0.5507)	11.52(1.711)	3.25(0.799)	3.652(0.579)	0.672(9.3%)
61	239.1(1.754)	38.80(6.160)	11.1(2.616)	13.37(2.046)	2.197(2.9%)
127	STACK(6.734)	158.2(26.36)	45.28(10.23)	56.11(8.403)	8.717(0.7%)

$p = 2^{62} - 923$

n	Pari	Magma	Maple	ipgcd	phigcd(%phi)
3	1.307(0.0722)	1.37(0.230)	1.535(BUG)	0.097(0.0234)	0.100(69.3%)
7	4.910(0.1870)	3.90(0.597)	5.184(BUG)	0.369(0.0760)	0.159(44.2%)
15	18.71(0.5320)	12.04(1.755)	18.34(BUG)	1.378(0.2609)	0.356(29.8%)
31	72.56(1.703)	40.26(5.830)	66.38(BUG)	5.264(0.948)	1.082(6.6%)
61	268.3(5.632)	148.4(19.85)	231.5(BUG)	19.12(3.375)	3.635(2.0%)
127	STACK(22.09)	662.0(79.40)	954.3(BUG)	77.84(13.95)	14.63(1.0%)

Computing in $K \mod p$: How to divide by p?

How do we compute $C(x) = A(x) \times B(x)$ in $\mathbb{Z}/p\mathbb{Z}[x]$?
Let $A = \sum_{i=0}^{da} a_i x^i$, $B = \sum_{i=0}^{db} b_i x^i$, $C = \sum_{i=0}^{dc} c_i x^i$.

$$c_k = \sum_{i=\max(k,k-db)}^{\min(k,da)} (a_i \times b_{k-i} \mod p)$$

The hardware integer $\div p$ instruction is very expensive compare with $\times$.
1994 T. Granlund and P. Montgomery replaces the division by p with 2 multiplications and ....

$$c_k = \left(\sum_{i=\max(k,k-db)}^{\min(k,da)} (a_i \times b_{k-i} \mod 2^{64} p) \right) \mod p$$

```
ULONG[2] z; z[0] = 0; z[1] = 0;
while( i<m ) {
    zfma(z,a[i],b[k-i]); i++;
    zfma(z,a[i],b[k-i]); i++;
    if( z[1]>=p ) z[1] -= p;  // if( z>p*2^64 ) z = z - p*2^64;
}
```

Computing in $K \mod p$: How to divide by $m_1(z)$?

How do we compute $C(x) = A(x) \times B(x)$ in $R[x]$ where $R = \mathbb{Q}[z_1]/m_1(z_1) \mod p$.

$$c_k = \left(\sum_{i=\max(k,k-db)}^{\min(k,da)} a_i(z_1) \times b_{k-i}(z_1) \right) \quad \text{mod } m_1(z_1)$$

$T =$

0	1	2	3	4	5	6

$\div$

1	0	-10	0	1

$= m_1(z)$

I've coded (in C Henri!) $+, -, \times$ and inverse in $K \mod p$ to run in-place for $k \geq 1$ for $p < 2^{63}$.
Also $+, -, \times, \div, \gcd$ in $K[x] \mod p$ for $k \geq 1$ for $p < 2^{63}$.
I use a dense representation for $K \mod p$, for example, for $K = \mathbb{Q}[y,z]/\langle z^3 - 2, y^2 - 3z - 1\rangle$

I store $3z^1 + 5z^2y^1$ as

1	1	0	3	ϕ	2	0	0	5

Thank you.

Benchmark - Magma code

```
Magma V2.26-12    Thu Jun 16 2022 15:48:32 on cecm-maple [Seed = 3928172896]
Type ? for help.  Type <Ctrl>-D to quit.
> p := 2^25-855; // p := 2^31-399; p := 2^62-923;
> Fp := FiniteField(p);
> P1<z> := PolynomialRing(Fp); m1 := z^2+z+1; K1<z>,phi1 := quo<P1|m1>;
> P2<y> := PolynomialRing(K1); m2 := y^4-y*z-2; K2<y>,phi2 := quo<P2|m2>;
> P3<x> := PolynomialRing(K2); m3 := x^2-x*y-4; K3<x>,phi3 := quo<P3|m3>;
> P4<w> := PolynomialRing(K3); m4 := w^2-3*x*w-y; K4<w>,phi4 := quo<P4|m4>;
> P<u> := PolynomialRing(K4);
> g := u+2*w*z+5*x+4*y*z+3;
> a := u+w*y+6*x+7*y*z+8;
> b := u+w*x+9*w*z+2*y+2;
> n := 3; // 4, 7, 15, 31, 61, 127
> a := a^n*g;
> b := b^n*g;
> time for i := 1 to 100 do h := Gcd(a,b); end for;
Time: 0.480
> h;
u + 2*z*w + 5*x + 4*z*y + 3
```

Benchmark - Maple code

```
> kernelopts(opaquemodules=false):
> RD := Algebraic:-RecursiveDensePolynomials:
> p := 2^25-855:  # p := 2^31-399; p := 2^62-923;
> m1 := z^2+z+1:
> m2 := y^4-y*z-2:
> m3 := x^2-x*y-4:
> m4 := w^2-3*w*x-y:
> R := ( [u,w,x,y,z], [m4,m3,m2,m1], p ):
> g := RD:-rpoly( u+2*w*z+5*x+4*y*z+3, R ):
> aa := RD:-rpoly( u+w*y+6*x+7*y*z+8, R ):
> bb := RD:-rpoly( u+w*x+9*w*z+2*y+2, R ):
> n := 3:  # 3, 4, 7, 15, 31, 61, 127
> a := RD:-mulrpoly(g,RD:-powrpoly(aa,n)):
> b := RD:-mulrpoly(g,RD:-powrpoly(bb,n)):
> CodeTools[Usage]( to 100 do h := RD:-gcdrpoly(a,b) od ):
memory used=2.12MiB, alloc change=0 bytes, cpu time=40.00ms, real time=41.00ms, gc time=0ns
> RD:-rpoly(h); # check
                         2 w z + 4 y z + u + 5 x + 3
```