

## Re: GCD of multivariate polynomials

**Source:** <http://sci.tech-archive.net/Archive/sci.math.symbolic/2004-11/0026.html>

---

**From:** Richard Fateman (*fateman\_at\_cs.berkeley.edu*)

**Date:** 11/05/04

Date: Fri, 05 Nov 2004 16:04:21 GMT

Mitch Harris wrote:

> *Gagan Raj Gupta* wrote:

>

>> *I wish to know if there is a way to compute the GCD of 2 multivariate*

>> *polynomials.*

1. Yes, there is a way.

Now for the questions you did NOT ask..

2. Just about any computer algebra system has such a capability, which is necessary to simplify ratios of polynomials to simplest form.

3. There are public open-source programs with this capability.

4. It is a well-studied problem, and you can find simple programs or far more elaborate programs that are efficient for large cases.

5. The names Reduced, Subresultant, Modular, EZGCD, Heuristic, Sparse, will be found if you Google for the subject.

6. If you are writing such a program, I recommend you NOT start with an exponential time

procedure (Buchberger's algorithm) and hope that the special case of GCD will come out faster. You can write such a program more directly. Assuming you already know how to represent polynomials

in several variables over the integers, and can add, multiply, and compute remainders, a decent GCD program, say subresultant, can fit on half a page. A useful treatment can be found in Knuth's

Art of Computer programming Volume 2. I think that the 'details'

you find in Cox et al, and books on Groebner bases will not address the computational task, but only the mathematical implications. If that is what you want, fine.

RJF

>>

>> *For eg, the gcd of  $abcd + abe + c^2d + ec + ecd + e^2$  and*

>>  *$abgh + abk + abl + cgh + ck + cl$  is  $ab + c + e$ .*

>>

>> *I constructed this by doing  $(ab + c + e)(cd + e)$  and  $(ab + c + e)(gh + k)$ .*

>

>

> *(I think you meant  $abgh + abk + cgh + egh + ck + ek$ )*

>

sci.math.symbolic: Re: GCD of multivariate polynomials

- > *Yes, it's possible. As with (plain old) integers, factoring is –not–*
- > *the most efficient method (in general) for computing the gcd.*
- >
- > *What does work is a more generalized Euclidean gcd algorithm (divide*
- > *the "larger" by the "smaller", repeat with the remainder, stop when*
- > *you get to 0, the remainder before you get 0 is the gcd).*
- >