

Re: euclidean algorithm over $\mathbb{Q}[i]$

Source: <http://sci.tech-archive.net/Archive/sci.math.symbolic/2006-12/msg00065.html>

- *From:* "Jeremy Watts" <stevie4545@xxxxxxxxxxx>
 - *Date:* Sun, 17 Dec 2006 10:18:00 GMT
-

"Chip Eastham" <hardmath@xxxxxxxxxx> wrote in message
<news:1166276481.508680.8020@xx>

Jeremy Watts wrote:

"Chip Eastham" <hardmath@xxxxxxxxxx> wrote in message
<news:1166245043.467094.262880@xx>

G. A. Edgar wrote:

In article
<[62tgh.6569\\$Dr3.1078@xxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:62tgh.6569$Dr3.1078@xxxxxxxxxxxxxxxxxxxxxxxxxxx)>,
Jeremy Watts
<stevie4545@xxxxxxxxxxx> wrote:

how does the euclidean
algorithm proceed for
numbers in $\mathbb{Q}[i]$? my

knowledge

of abstract algebra's basic to
say the least so i hope i am
using

the

correct term. i mean for
complex numbers with
rational real &

complex

parts

Re: euclidean algorithm over $\mathbb{Q}[i]$

ie. of form $a/b + c/d$ i a,b,c,d
in \mathbb{Z}

i'm sure i have seen this
somewhere but cant find
reference to it

anywhere.

thanks

$\mathbb{Q}[i]$ is a field, so greatest common divisors
are easy.

Any nonzero element divides any other
nonzero element.

$\mathbb{Z}[i]$, the Gaussian integers, may be what you
remember seeing.

--

G. A. Edgar

<http://www.math.ohio-state.edu/~edgar/>

And if the OP is interested in the Gaussian integers $\mathbb{Z}[i]$,
it is helpful to bear in mind that a Euclidean domain is
possessed of a norm. The "remainder" term is to have
norm less than the divisor in each application of the
division algorithm. Of course $\mathbb{Z}[i]$ is not an ordered ring,
so its important to pick the remainder to have minimum
norm as its defining characteristic.

The norm of $z = a + bi$ is $a^2 + b^2$ in $\mathbb{Z}[i]$.

More discussion here:

yes of course, thank you both. the reason i'm asking this is because

i've

written a pretty simplistic algorithm in java that carries out

polynomial

Re: euclidean algorithm over $\mathbb{Q}[i]$

GCD, just using polynomial long division and the euclidean algorithm.

i've been comparing the output with what 'wims' gives

<http://wims.unice.fr/wims/wims.cgi?session=XKF67EF2A7.1&+lang=en&+module=too>

1%2Farithmetic%2Fbezout.en

and they agree, apart from the final value for the gcd. which i assume 'wims' is getting somehow by avoiding intermediate 'coefficient swell'.

i

have read that if you use 'pseudo division' rather than standard long division you can get around this problem when working in the rationals

Are you using the Euclidean algorithm to compute GCD's of univariate polynomials over $\mathbb{Q}[i]$?

Hi Chip, yes i am using the Euclidean algorithm to compute gcd's of univariate polynomials over $\mathbb{Z}, \mathbb{Z}[i]$ and $\mathbb{Q}[i]$

The statement that "they agree, apart from the final value for the gcd" is a bit unsettling! I would assume normalization to monic polynomials resolves any ambiguity, and you are asking if there is strategic advantage to using 'pseudo division' to avoid large sized intermediate results.

when you say 'normalization to a monic' what do you mean by that? sorry if that sounds a bit basic. is this what 'pseudo division' does?

I assume that Gauss's content lemma goes through in $\mathbb{Z}[i]$ and that one can choose instead to compute the GCD in polynomials with (Gaussian) integer coefficients. Another ingredient that comes to mind is the possibility of evaluating the polynomials at some points in $\mathbb{Z}[i]$ and using the GCD of resulting Gaussian integers to interpolate a "candidate" polynomial GCD, something known as a "heuristic GCD algorithm" as cited here:

<http://www-fourier.ujf-grenoble.fr/~parisse/publi/gcdheu.pdf>

Re: euclidean algorithm over $\mathbb{Q}[i]$

Re: euclidean algorithm over $\mathbb{Q}[i]$

regards, chip