Polynomial Division, Remainder,GCD

Lecture 7

Division with remainder, integers

- p divided by s to yield quotient q and remainder r: 100 divided by 3

- p = s*q + r
- 100 = 3*33 + 1

- by some measure r is less than s: 0<r<s

Division with remainder, polynomials

- p(x) divided by s(x) to yield quotient q(x) and remainder r(x):
- p = s*q + r
- by some measure (degree in x, usually) r<s
- notice there is an asymmetry if we have several variables..

Example (this is typeset from Macsyma)

quotient, remainder

$$\text{divide}\left((x+1)^3, x+1\right) = \left\{x^2 + 2\,x + 1, 0\right\}$$

Long division: In detail

$$
\begin{array}{r|l}
 & x^2 + 2x \quad +1 \\
\hline
x+1 \;) & x^3+3x^2+3x+1 \\
 & x^3+\ x^2 \\
\hline
 & \quad 2x^2+3x \\
 & \quad 2x^2+2x \\
\hline
 & \qquad x+1 \\
 & \qquad x+1 \\
\hline
 & \qquad 0
\end{array}
$$

That was lucky: Divisible AND we could represent quotient and remainder over Z[x].

- Consider this minor variation -- the divisor is not monic (coefficient 1) : $2x+1$ instead of $x+1$. This calculation needs Q[x] to allow us to do the division...

Long division: In detail

$$
\begin{array}{rl}
 & \tfrac{1}{2}x^2 + \tfrac{5}{4}x \quad + \tfrac{7}{8} \\
\cline{2-2}
{\color{red}2}x+1 & \big)\, x^3 + \quad 3x^2 + \quad 3x \quad + 1 \\
 & x^3 + \tfrac{1}{2}x^2 \\
\cline{2-2}
 & \quad \tfrac{5}{2}x^2 + 3x \\
 & \quad \tfrac{5}{2}x^2 + \tfrac{5}{4}x \\
\cline{2-2}
 & \qquad \tfrac{7}{4}x + 1 \\
 & \qquad \tfrac{7}{4}x + \tfrac{7}{8} \\
\cline{2-2}
 & \qquad \tfrac{1}{8}
\end{array}
$$

Macsyma writes it out this way

$$\mathrm{divide}\left((x+1)^3, 2\,x+1\right) = \left\{\frac{4\,x^2+10\,x+7}{8}, \frac{1}{8}\right\}$$

$$\mathrm{ratexpand}\,(\%) = \left\{\frac{x^2}{2}+\frac{5\,x}{4}+\frac{7}{8}, \frac{1}{8}\right\}$$

In general that denominator gets nasty:

- 5^4 is 625.

$$\operatorname{divide}\left((x+1)^4, 5\,x+1\right) =$$

$$\left\{\frac{125\,x^3+475\,x^2+655\,x+369}{625}, \frac{256}{625}\right\}$$

Symbols (other indeterminates) are worse

$$\mathsf{divide}\left((x+1)^3, a\,x+b\right) =$$

$$\left\{\frac{a^2\,x^2+\left(3\,a^2-a\,b\right)\,x+b^2-3\,a\,b+3\,a^2}{a^3}, -\frac{b^3-3\,a\,b^2+3\,a^2\,b-a^3}{a^3}\right\}$$

Pseudo-remainder.. Pre-multiplying by power of leading coefficient... a^3

$$\text{divide}\left(\boxed{a^3}\,(x+1)^3,\; a\,x+b\right) =$$

$$\left\{a^2\,x^2+\left(3\,a^2-a\,b\right)\,x+b^2-3\,a\,b+3\,a^2,\, -b^3+3\,a\,b^2-3\,a^2\,b+a^3\right\}$$

note: we are doing arithmetic in Z[a,b][x]
not Q(a,b)[x].

Order of variables matters too.

- Consider x^2+y^2 divided by $x+y$, main variable x.
- Quotient is $x-y$, remainder $2y^2$. That is,
- $x^2+y^2 = (x-y)(x+y) + 2y^2$.

- Now consider main variable y
- Quotient is $y-x$, remainder $2x^2$. That is,
- $x^2+y^2 = (-x+y)(x+y) + 2x^2$.

Some activitives (Gröbner Basis reduction) divide by several polynomials

- P divided by s_1, s_2, ... to produce
- $P= q_1s_1+1_2s_2+...$ (not necessarily unique)

Euclid's algorithm (generalized to polynomials): Polynomial remainder sequence

- P_1, P_2 input polynomials
- P_3 is remainder of divide(P_1,P_2)
- .... P_n is remainder of divide(P_{n-2},P_{n-1})
- If P_n is zero, the GCD is P_{n-1}

- At least, an associate of the GCD. It could have some extraneous factor (remember the a^3?)

How bad could this be? (Knuth, vol 2 4.6.1)

$$x^8 + x^6 - 3\,x^4 - 3\,x^3 + 8\,x^2 + 2\,x - 5$$

$$3\,x^6 + 5\,x^4 - 4\,x^2 - 9\,x + 21,$$

$$-\frac{5\,x^4 - x^2 + 3}{9}$$

$$-\frac{117\,x^2 + 225\,x - 441}{25}$$

$$\frac{233150\,x - 307500}{19773}$$

$$-\frac{1288744821}{543589225}$$

Euclid's alg.
over Q

Making the denominators disappear by premultiplication....

$$x^8 + x^6 - 3\,x^4 - 3\,x^3 + 8\,x^2 + 2\,x - 5$$

$$3\,x^6 + 5\,x^4 - 4\,x^2 - 9\,x + 21$$

$$-15\,x^4 + 3\,x^2 - 9$$

$$-585\,x^2 - 1125\,x + 2205$$

$$307500 - 233150\,x$$

$$143193869$$

Euclid's alg. over Z, using pseudoremainders

Compute the content of each polynomial

1 $$x^8 + x^6 - 3\,x^4 - 3\,x^3 + 8\,x^2 + 2\,x - 5$$

1 $$3\,x^6 + 5\,x^4 - 4\,x^2 - 9\,x + 21,$$

1/9 $$-\frac{5\,x^4 - x^2 + 3}{9}$$

9/25 $$-\frac{117\,x^2 + 225\,x - 441}{25}$$

50/ 19773 $$\frac{233150\,x - 307500}{19773}$$

1288744821/ 543589225 $$-\frac{1288744821}{543589225}$$

Euclid's alg. over Q. Each coefficient is reduced... not much help.

Better but costlier, divide by the content

$$x^8 + x^6 - 3x^4 - 3x^3 + 8x^2 + 2x - 5$$

$$3x^6 + 5x^4 - 4x^2 - 9x + 21$$

$$-5x^4 + x^2 - 3$$

$$-13x^2 - 25x + 49$$

$$4663x - 6150$$

$$-1$$

Euclid's alg. over Q, content removed: primitive PRS

Some Alternatives

- Do computations over Q, but make each polynomial MONIC, eg. $p_2 = x^6 + 5/3x^4 + \ldots$
- (this does not gain much, if anything. recall that in general the leading coefficient will be a polynomial. Carrying around $1/(a^3+b^3)$ is bad news.
- Do computations in a finite field (in which case there is no coefficient growth, but the answer may be bogus)

Sample calculation mod 13 drops some coefficients!

$x^8+x^6-3x^4-3x^3-5x^2+2x-5$

$3x^6+5x^4-4x^2+4x-5$

$-2x^4+3x^2+4$

$6x-5$ was $585x^2$ ... but $585|13$

$5x-2$

0

... bad result suggests $5x-2$ is the *gcd*, but $5x-2$ is not a factor of p_1 or p_2

This modular approach is actually better than this...

In reality, the choice of 13 is easily avoidable, and there are plenty of "lucky" primes which will tell us the GCD is 1

e.g. prime 3571 gives,

$X^8+x^6-3x^4-3x^3-5x^2+2x-5$

$3x^6+5x^4-4x^2+4x-5$

x^4+714x^2+1429

$281x^2-9x+589$ or $x^2+826x+1095$

$x+1152$

376647 or 1 if monic.

Another Alternative: the subresultant PRS

- Do computations where a (guaranteed) divisor not much smaller than the content can be removed at each stage (subresultant PRS)
- In our example, the subresultant's last 2 lines are
  - 9326x-12300
  - 260708 (actually the subres PRS is usually better; our example was an abnormal remainder sequence)

The newest thought: Heuristic GCD, the idea is to evaluate

- In our example,
- $p_1(1234567)$=539656376132193465471586118557521938924302235 2699
- $p_2(1234567)$=106220719596340106386606195083119480 74
- the integer GCD is 1
- Can we conclude that if the GCD is h(x), that h(1234567)=1 ?

The GCD papers, selected, online in /readings. Recent "reviews"

- M. Monagan, A. Wittkopf:
- On the design and implementation of Brown's Algorithm (GCD) over the integers and number fields. Proc. ISSAC 2000 p 225-233
- http://portal.acm.org/citation.cfm?doid=345542.345639
- or the class directory, monagan.pdf
- P. Liao, R. Fateman:
- Evaluation of the heuristic polynomial GCD Proc ISSAC 1995 p 240-247
- http://doi.acm.org/10.1145/220346.220376
- or this directory, liao.pdf

The GCD papers, selected, online in /readings. Classics.

- G.E. Collins:
- Subresultants and reduced polynomial remainder sequences
- JACM Jan 1967
- http://doi.acm.org/10.1145/321371.321381
- or this directory, collins.pdf

- W.S Brown:
- The Subresultant PRS algorithm
- ACM TOMS 1978
- brown.pdf

The GCD papers, selected, online in /readings. The sparse GCDs

- J. Moses and D.Y.Y. Yun
- The EZ GCD algorithm
- 1973 Proc. SYMSAC
- moses-yun.pdf
- R. Zippel: SPMOD in Zippel's text. Or PhD

The GCD papers, selected, online in /readings. The sparse GCDs

- E. Kaltofen:

Greatest common divisors of polynomials given by straight-line programs

JACM 1988.

http://doi.acm.org/10.1145/42267.45069

kaltofen.pdf