University of Wyoming
Math 3200—Spring 2012
Polynomials
$f(X,Y)\in\mathbb{Z}[X,Y]$
$x=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$
Department of Mathematics

The Division Algorithm for Polynomials

Handout Monday March 5, 2012

Let F be a field (such as $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$, or $\mathbb{F}_p$ for some prime p). This will allow us to divide by any nonzero scalar. (For some of the following, it is sufficient to choose a ring of constants; but in order for the Division Algorithm for Polynomials to hold, we need to be able to divide constants.) For much of the following, you can pretend that $F=\mathbb{R}$.

Recall that a *polynomial* in x is an expression of the form

$$f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n$$

where x is a symbol and $a_0,a_1,\dots,a_n\in F$. We say that a_k is the *coefficient* of x^k, for $k=0,1,2,\dots,n$. Let $F[x]$ denote the set of all polynomials in x, with coefficients in F. (Thus, for example, $\mathbb{R}[x]$ is the set of polynomials in x with real coefficients.) The *zero polynomial,* denoted by 0, is the polynomial whose coefficients are all zero. Two polynomials $f(x)$ and $g(x)$ are the *same,* denoted $f(x)=g(x)$, if their corresponding coefficients are the same; for example,

$$1-2x+5x^3=5x^3-2x+1=1-2x+0x^2+5x^3=0x^4+5x^3+0x^2-2x+1.$$

In particular, we write $f(x)=0$ if and only if all coefficients of $f(x)$ are zero, thus for example, $x^2-1\neq 0$. If $p(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n\neq 0$, the *degree* of $p(x)$, denoted by $\deg p(x)$, is the largest k such that $a_k\neq 0$. For example, $\deg(1-2x+5x^3)=3$, $\deg(2x-0x^2)=1$, $\deg(-8)=0$. We define $\deg 0=-\infty$ so that the following proposition holds universally for all polynomials $f(x),g(x)$, with the obvious conventions for adding $-\infty$.

Proposition 1. If $f(x),g(x)\in F[x]$ then $\deg\big(f(x)g(x)\big)=\deg f(x)+\deg g(x)$.

Proof. If either of the two polynomials $f(x),g(x)$ is zero, then $f(x)g(x)=0$ and the desired equality holds, with both sides equal to $-\infty$ by convention. We may therefore assume $f(x)$ and $g(x)$ are nonzero polynomials. Now

$$f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n;\quad g(x)=b_0+b_1x+b_2x^2+\cdots+b_mx^m$$

where $n=\deg f(x)$ and $m=\deg g(x)$; in particular, $a_n\neq 0$ and $b_m\neq 0$. Thus

$$f(x)g(x)=a_0b_0+(a_0b_1+a_1b_0)x+\cdots+a_nb_mx^{n+m}$$

where the last term is the unique term of highest degree in $f(x)g(x)$, with coefficient $a_n b_m \neq 0$; thus

$$\deg\big(f(x)g(x)\big) = n + m = \deg f(x) + \deg g(x).$$

□

We say that $f(x)$ *divides* $g(x)$ in $F[x]$, denoted $f(x) \mid g(x)$, if $g(x) = m(x)f(x)$ for some $m(x) \in F[x]$. The following is obviously analogous to the Division Algorithm for Integers. We omit the proof, which we take to be evident from the usual algorithm of long division.

Theorem 2 (Division Algorithm for Polynomials). Let $f(x), d(x) \in F[x]$ such that $d(x) \neq 0$. Then there exist unique polynomials $q(x), r(x) \in F[x]$ such that

$$f(x) = q(x)d(x) + r(x), \qquad \deg r(x) < \deg d(x)\,.$$

As usual 'unique' means that there is only one pair of polynomials $(q(x), r(x))$ satisfying the conclusions of the theorem. We call $q(x)$ and $r(x)$ the quotient and remainder, respectively. Note that $a(x) \mid b(x)$ if and only if $r(x) = 0$. Note that the Division Algorithm holds in $F[x]$ for any field F; it does not hold in $\mathbb{Z}[x]$, the set of polynomials in x with integer coefficients.

A *zero* or *root* of $f(x)$ is a number a such that $f(a) = 0$. An important consequence of the Division Algorithm is the fact (made explicit by the following theorem) that roots of polynomials correspond to linear factors.

Theorem 3. Let $f(x) \in F[x]$ and $a \in F$. Then $f(a) = 0$ if and only if $(x-a) \mid f(x)$.

Proof. If $(x - a) \mid f(x)$ then $f(x) = (x - a)m(x)$ for some $m(x) \in F[x]$, and so $f(a) = 0m(a) = 0$.

Conversely, suppose $f(a) = 0$. By the Division Algorithm, we may write $f(x) = (x-a)q(x) + r(x)$ for some $q(x), r(x) \in F[x]$ where $r(x)$ has degree less than 1 (the degree of $x - a$). If $r(x) = 0$ then we would have $(x - a) \mid f(x)$, and so we would be done. So let's assume instead that $r(x) \neq 0$, in which case $\deg r(x) = 0$, so $r = r(x)$ is a nonzero constant. Substituting a for x gives $0 = f(a) = 0m(a) + r$, so $r = 0$. This contradiction proves that in fact $(x - a) \mid f(x)$. □

This argument extends to multiple roots:

Theorem 4. If $f(x) \in F[x]$ has distinct roots $a_1, a_2, \ldots, a_n$, then $f(x)$ is divisible by $(x-a_1)(x-a_2)\cdots(x-a_n)$. In particular, either $f(x) \neq 0$ or $\deg f(x) \geq n$.

Proof. Suppose $f(x)$ has at least n distinct roots $a_1, a_2, \ldots, a_n$. By Theorem 3, we have $f(x) = (x-a_1)g(x)$ for some $g(x) \in F[x]$. Substituting a_2 for x gives $0 = f(a_2) = (a_2 - a_1)g(a_2)$ where $a_2 - a_1 \neq 0$ since the n roots are distinct. Therefore $g(a_2) = 0$, and by Theorem 3 we have $g(x) = (x-a_2)h(x)$ for some $h(x) \in F[x]$. Thus $f(x) = (x-a_1)(x-a_2)h(x)$. Continuing in this way, we eventually obtain $f(x) = (x-a_1)(x-a_2)(x-a_3)\cdots(x-a_n)m(x)$ for some $m(x) \in F[x]$. □

Corollary 5. A nonzero polynomial $f(x) \in F[x]$ of degree n cannot have more than n distinct roots.

The notion of gcd for integers, generalizes to polynomials as follows. Given two polynomials $f(x), g(x) \in F[x]$, not both zero, we define the *greatest common divisor* (denoted $\gcd(f(x), g(x))$ to be the unique monic polynomial of highest degree dividing both $f(x)$ and $g(x)$. Here '*monic*' means 'having leading coefficient 1'. Consider the following example:

The divisors of $f(x) = 2x^2 - \frac{1}{2} = 2\big(x+\frac{1}{2}\big)\big(x-\frac{1}{2}\big)$ are all polynomials of the form

$$c; \quad c\big(x+\tfrac{1}{2}\big); \quad c\big(x-\tfrac{1}{2}\big); \quad c\big(x+\tfrac{1}{2}\big)\big(x-\tfrac{1}{2}\big)$$

where c is an arbitrary nonzero constant. The divisors of $g(x) = 2x^2 - 3x + 1 = (2x-1)(x-1) = 2\big(x-\frac{1}{2}\big)\big(x-1\big)$ are

$$c; \quad c\big(x-\tfrac{1}{2}\big); \quad c\big(x-1\big); \quad c\big(x-\tfrac{1}{2}\big)\big(x-1\big)$$

where c is an arbitrary nonzero constant. The common divisors of $f(x)$ and $g(x)$ have the form

$$c; \quad c\big(x-\tfrac{1}{2}\big)$$

where c is an arbitrary nonzero constant. The polynomials of highest degree dividing both $f(x)$ and $g(x)$ have the form $c\big(x-\frac{1}{2}\big)$ where c is a nonzero constant. In order that the greatest common divisor of $f(x)$ and $g(x)$ be well-defined, we choose $c = 1$ so that the answer is monic; thus

$$\gcd\big(f(x), g(x)\big) = \gcd(2x^2 - \tfrac{1}{2}\,,\ 2x^2 - 3x + 1\big) = x - \tfrac{1}{2}\,.$$

The computation of $\gcd(f(x), g(x))$ does not require knowing how to factorize polynomials; instead, we use Euclid's Algorithm, just as we did with integers. This algorithm, in its extended form, also expresses $\gcd(f(x),g(x))$ as a 'polynomial-linear combination' of $f(x)$ and $g(x)$:

Theorem 6 (Euclid's Algorithm for Polynomials). Let $f(x),g(x)\in F[x]$ be polynomials, not both zero. Then there exist polynomials $r(x),s(x)\in F[x]$ such that

$$r(x)f(x)+s(x)g(x)=\gcd\big(f(x),g(x)\big).$$

For example, we compute the gcd of the polynomials $f(x)=5x^3+2x^2+3x-10$, $g(x)=x^3+2x^2-5x+2\in\mathbb{Q}[x]$. The steps are almost the same as when computing the gcd of two integers. We proceed to repeatedly apply the Division Algorithm:

$$\begin{aligned}f(x)&=5g(x)+(-8x^2+28x-20)\\ g(x)&=\big(-\tfrac{1}{8}x-\tfrac{11}{16}\big)(-8x^2+28x-20)+\big(\tfrac{47}{4}x-\tfrac{47}{4}\big)\\ -8x^2+28x-20&=\tfrac{4}{47}\big(-8x+20\big)\big(\tfrac{47}{4}x-\tfrac{47}{4}\big)+0\end{aligned}$$

At this point we might want to say that $gcd(f(x),g(x))=\frac{47}{4}x-\frac{47}{4}=\frac{47}{4}(x-1)$ (the last nonzero remainder). However observe that the much simpler polynomial $x-1$ divides both $f(x)$ and $g(x)$. We choose the gcd to be *monic*, i.e. its leading coefficient should be 1. So in this case $gcd(f(x),g(x))=x-1$ and the extended form of the algorithm allows us to write this as a polynomial-linear combination of $f(x)$ and $g(x)$:

$$\begin{aligned}\tfrac{47}{4}x-\tfrac{47}{4}&=g(x)-\big(-\tfrac{1}{8}x-\tfrac{11}{16}\big)(-8x^2+28x-20);\\ x-1&=\tfrac{4}{47}g(x)+\big(\tfrac{1}{94}x+\tfrac{11}{188}\big)(-8x^2+28x-20)\\ &=\tfrac{4}{47}g(x)+\big(\tfrac{1}{94}x+\tfrac{11}{188}\big)\big(f(x)-5g(x)\big)\\ &=\big(\tfrac{1}{94}x+\tfrac{11}{188}\big)f(x)+\big(-\tfrac{5}{94}x-\tfrac{39}{188}\big)g(x).\end{aligned}$$

Ugly fractions like this are to be expected when working over $\mathbb{Q}$. Life is much easier working over $\mathbb{F}_p$, when coefficients are more simply expressed as elements of $\{0,1,2,\ldots,p-1\}$. Consider what happens to the preceding example over $\mathbb{F}_7$:

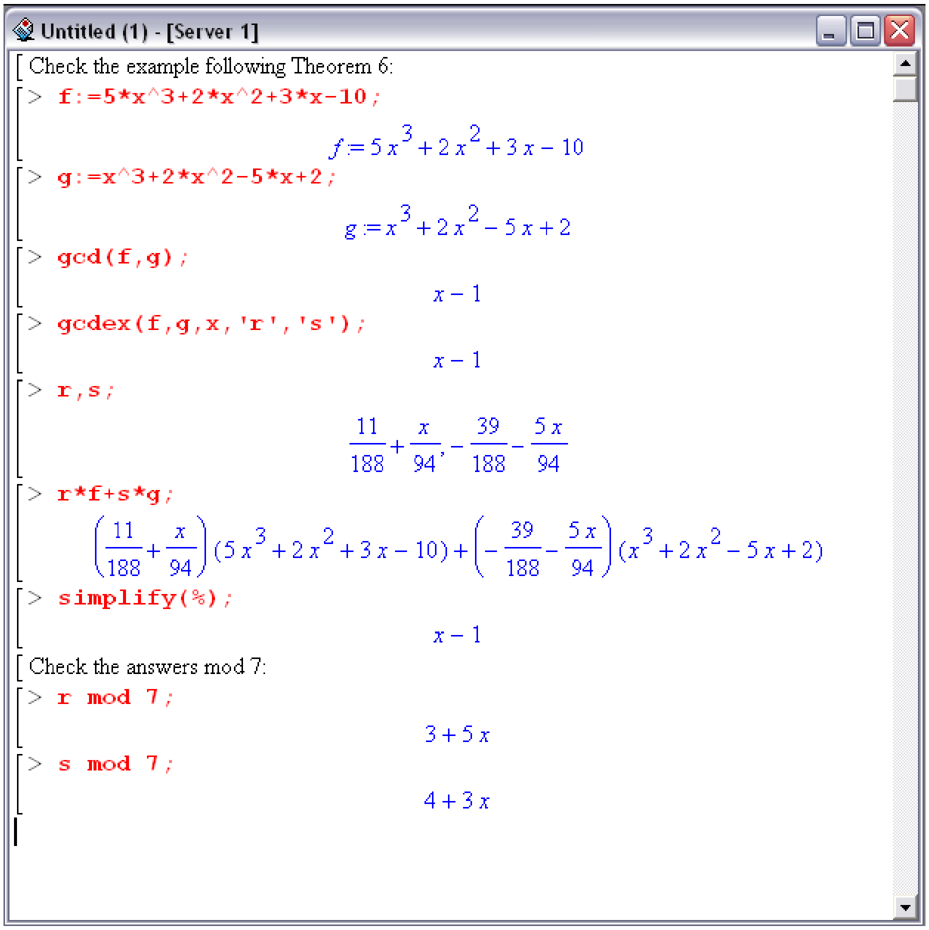
$$\begin{aligned}f(x)&=5x^3+2x^2+3x+4,\\ g(x)&=x^3+2x^2+2x+2;\end{aligned}$$

$$\begin{aligned}f(x)&=5g(x)+(6x^2+1)\\ g(x)&=(6x+5)(6x^2+1)+(3x+4)\\ 6x^2+1&=5(6x+1)(3x+4)+0\end{aligned}$$

so from $3x+4 = 3(x+6)$ we obtain $\gcd(f(x), g(x)) = x+6$ over $\mathbb{F}_7$. The extended version of Euclid's Algorithm over $\mathbb{F}_7$ is also not hard:

$$\begin{aligned} 3x+4 = 3(x+6) &= g(x) - (6x+5)(6x^2+1); \\ x+6 &= 5g(x) + (5x+3)(6x^2+1) \\ &= 5g(x) + (5x+3)(f(x) - 5g(x)) \\ &= (5x+3)f(x) + (3x+4)g(x). \end{aligned}$$

It is important to understand how this works (and to be prepared to perform simpler versions of this on a test) in the same way that we expect you to be able (in principle) to perform arithmetic (including multiplication and division of large integers). However, there is no additional benefit in repeatedly performing such operations by hand once the principles are mastered. For this we may use Maple:



Check the example following Theorem 6:

```
> f:=5*x^3+2*x^2+3*x-10;
```

$$f := 5\,x^3 + 2\,x^2 + 3\,x - 10$$

```
> g:=x^3+2*x^2-5*x+2;
```

$$g := x^3 + 2\,x^2 - 5\,x + 2$$

```
> gcd(f,g);
```

$$x - 1$$

```
> gcdex(f,g,x,'r','s');
```

$$x - 1$$

```
> r,s;
```

$$\frac{11}{188} + \frac{x}{94},\ -\frac{39}{188} - \frac{5\,x}{94}$$

```
> r*f+s*g;
```

$$\left(\frac{11}{188} + \frac{x}{94}\right)(5\,x^3 + 2\,x^2 + 3\,x - 10) + \left(-\frac{39}{188} - \frac{5\,x}{94}\right)(x^3 + 2\,x^2 - 5\,x + 2)$$

```
> simplify(%);
```

$$x - 1$$

Check the answers mod 7:

```
> r mod 7;
```

$$3 + 5\,x$$

```
> s mod 7;
```

$$4 + 3\,x$$

The analog of prime numbers, for polynomials, is the concept of an *irreducible polynomial*. A polynomial $p(x) \in F[x]$ of degree ≥ 1 is *irreducible* if its only divisors are c and $cp(x)$ where c is a nonzero constant. The concept of irreducibility depends on the choice of field F; for example, $x^2 - 2$ is irreducible over $\mathbb{Q}$, but not over $\mathbb{R}$ where it factors as

$\big(x+\sqrt{2}\,\big)\big(x-\sqrt{2}\,\big)$. The polynomial x^2+1 is irreducible over $\mathbb{Q}$ and over $\mathbb{R}$, but not over $\mathbb{C}$ where it factors as $(x+i)(x-i)$, $i=\sqrt{-1}$. Recall Euclid's Lemma for Integers, which states that a prime p divides a product of two integers ab, iff $p\,\big|\,a$ or $p\,\big|\,b$. (As usual, this is an inclusive 'or': we allow the possibility that both a and b are divisible by p.) This fact extends to polynomials, with the same proof.

Theorem 7 (Euclid's Lemma). Let $p(x)\in F[x]$ be irreducible, and consider two polynomials $f(x),g(x)\in F[x]$. If $f(x)g(x)$ is divisible by $p(x)$, then $p(x)\,\big|\,f(x)$ or $p(x)\,\big|\,g(x)$.

Proof. Suppose that $p(x)\nmid f(x)$; we must prove that $p(x)\,\big|\,g(x)$. Since $p(x)\nmid f(x)$ where $p(x)$ is irreducible, we have $\gcd(p(x),f(x))=1$. By Euclid's Algorithm, there exist $r(x),s(x)\in F[x]$ such that

$$1=r(x)p(x)+s(x)f(x).$$

Then

$$g(x)=[g(x)r(x)]p(x)+s(x)[f(x)g(x)]$$

is divisible by $p(x)$ as required. □

A consequence of Euclid's Lemma is the fact that every polynomial has an essentially unique factorization into irreducible factors. By 'essentially unique', we mean the factorization is unique except for constant scalar multiples. If we factor out the coefficient of the leading term, and then use only monic irreducible factors, then the factorization is unique. This is the analogue (for polynomials) of the Fundamental Theorem of Arithmetic (the fact that every positive integer has a unique factorization as a product of primes).

HOMEWORK #3 Due Mon March 19, 10:01 am

Solutions for this homework will be posted moments after the deadline, and further submissions will not be accepted beyond that time. Submit solutions in class, or to the departmental office (the secretary will put them in my mailbox), or by sliding under my office door, or by email. (Remember never to submit homework *outside* my door.) Solutions should be done by hand, but may be checked using Maple or other software (Sage, etc.).

1. Show that there *do not* exist polynomials $q(x),r(x)\in\mathbb{Z}[x]$ such that $x^2-3x+4=(3x+1)q(x)+r(x)$ and $r(x)$ is a constant. Conclude that the Division Algorithm does not hold in $\mathbb{Z}[x]$.

2. Show that there *do* exist polynomials $q(x), r(x) \in \mathbb{Q}[x]$ such that $x^2 - 3x + 4 = (3x+1)q(x) + r(x)$ and $r(x)$ is a constant. (This is an example of the Division Algorithm in $\mathbb{Q}[x]$. The Division Algorithm holds for $F[x]$, where F is any field, such as $\mathbb{R}$, $\mathbb{Q}$ or $\mathbb{F}_p$.)

3. Consider the polynomials $f(x), d(x) \in \mathbb{F}_5[x]$ given by

$$\begin{aligned} f(x) &= x^4 + 2x^3 + 4x^2 + x + 3; \\ d(x) &= 2x^2 + x + 3. \end{aligned}$$

Find the quotient $q(x)$ and remainder $r(x)$ when $f(x)$ is divided by $d(x)$. Express your answers for $q(x)$ and $r(x)$ in simplified form using coefficients $0, 1, 2, 3, 4$.

4. Consider the polynomials $f(x), g(x) \in \mathbb{F}_7[x]$ given by

$$\begin{aligned} f(x) &= x^5 + x + 1; \\ g(x) &= x^4 + x^2 + 1. \end{aligned}$$

Determine $\gcd(f(x), g(x))$ and find $r(x), s(x) \in \mathbb{F}_7[x]$ such that

$$r(x)f(x) + s(x)g(x) = \gcd\big(f(x), g(x)\big).$$