Mathematics 4300 – Foundations of Algebra – Fall 1999

12. Polynomials with Integer Coefficients. Gauss's Lemma states that when a polynomial with integer coefficients factors in $\mathbf{Q}[x]$, then the factors can also be chosen to have integer coefficients. We use this to prove Eisenstein's criterion, which enables us to find lots of prime polynomials in $\mathbf{Q}[x]$ of all degrees. We end this section with a discussion of number fields, and some new "integers" where unique factorization may or may not be true.

We start with a familiar test for rational roots of a polynomial.

Rational Roots Test: Suppose $f(x) \in \mathbf{Q}[x]$ is of the form:

$$f(x) = a_d x^d + a_{d-1}x^{d-1} + ... + a_0$$

where all the coefficients $a_0, ..., a_d$ are **integers**.

Then if $r \in \mathbf{Q}$ is a root of $f(x)$ and if $r = \frac{b}{m}$ is written in lowest terms (i.e. b and m are chosen so that $\gcd(b, m) = 1$) then $b|a_0$ and $m|a_d$.

Proof: $r = \frac{b}{m}$ is a root if:

$$a_d \left(\frac{b}{m}\right)^d + a_{d-1}\left(\frac{b}{m}\right)^{d-1} + ... + a_1\left(\frac{b}{m}\right) + a_0 = 0.$$

If we clear denominators by multiplying through by m^d, we get:

$$a_d b^d + a_{d-1}b^{d-1}m + ... + a_1 b m^{d-1} + a_0 m^d = 0$$

from which we may conclude that $b|a_0 m^d$. But $\gcd(b, m) = 1$ implies that $\gcd(b, m^d) = 1$ which implies that $b|a_0$. Similarly $m|a_d b^d$, and $\gcd(b, m) = 1$ implies that $\gcd(b^d, m) = 1$ which implies that $m|a_d$.

Example: To check that $f(x) = 2x^4 + x + 3$ has no rational roots, we only need to notice that $1, -1, 3, -3, \frac{1}{2}, -\frac{1}{2}, \frac{3}{2}, -\frac{3}{2}$ are the only possible rational roots, by the rational root test, but:

$$f(1) = 6, f(-1) = 4, f(3) = 168, f(-3) = 162$$

$$f(\frac{1}{2}) = \frac{29}{8}, f(-\frac{1}{2}) = \frac{21}{8}, f(\frac{3}{2}) = \frac{109}{8}, f(-\frac{3}{2}) = \frac{101}{8}$$

But this doesn't tell us when a polynomial of degree four or more is prime!

Gauss's Lemma: If $f(x) \in \mathbf{Q}[x]$ is a polynomial as above, with integer coefficients, and if $f(x)$ is reducible, i.e.

$$f(x) = g(x)h(x) \text{ with } g(x), h(x) \in \mathbf{Q}[x]$$

then there are polynomials $\widetilde{g}(x)$ and $\widetilde{h}(x)$ of the same degrees as $g(x)$ and $h(x)$ respectively, and with **integer** coefficients such that:

$$f(x) = \widetilde{g}(x)\widetilde{h}(x)$$

Proof: The coefficients of $g(x)$ and $h(x)$ are all rational numbers. This means that there are natural numbers m and n so that $mg(x)$ and $nh(x)$ are polynomials with **integer** coefficients. (Take m to be the least common multiple of the denominators of the coefficients of $g(x)$, and similarly for n). Let $g_0(x) = mg(x)$ and $h_0(x) = nh(x)$. Then we have:

$$mnf(x) = g_0(x)h_0(x)$$

a factorization of $mnf(x)$ as a product of polynomials with integer coefficients. Of course, this isn't what we want. But now suppose p is a prime, and $p|mn$. Then p divides all the coefficients of $mnf(x)$, so:

$$0 = g_0(x)h_0(x) \in \mathbf{F}_p[x]$$

when we think of $g_0(x)$ and $h_0(x)$ as polynomials with coefficients in $\mathbf{F}_p$. But of course, this implies that $g_0(x) = 0$ or $h_0(x) = 0$, thought of as a polynomial in $\mathbf{F}_p[x]$. That is, p either divides all the coefficients of $g_0(x)$ or it divides all the coefficients of $h_0(x)$. **So divide the polynomial by p and continue.** That is, if p divides all the coefficients of $g_0(x)$, then $g_1(x) = \frac{1}{p}g_0(x)$ still has integer coefficients, and likewise for $h_1(x)$. After we divide through by all the primes dividing mn, we are left with the desired factorization:

$$f(x) = \widetilde{g}(x)\widetilde{h}(x)$$

Example: Starting with $x^2 - 1 = (\frac{3}{2}x - \frac{3}{2})(\frac{2}{3}x + \frac{2}{3})$, we clear denominators taking $m = 2$ and $n = 3$, and we get:

$$6(x^2 - 1) = (3x - 3)(2x + 2)$$

Dividing through by $p = 2$, we get:

$$3(x^2 - 1) = (3x - 3)(x + 1)$$

and dividing through by $p = 3$, we get:

$$x^2 - 1 = (x - 1)(x + 1)$$

the factorization with integer coefficients that we were looking for.

An Application: Suppose that $f(x) \in \mathbf{Q}[x]$ has integer coefficients, and suppose that p is a prime not dividing the leading coefficient a_d. Then if $f(x)$ is prime in $\mathbf{F}_p[x]$, it is also prime in $\mathbf{Q}[x]$.

Proof: If $f(x) = g(x)h(x)$ in $\mathbf{Q}[x]$, then we may use Gauss's Lemma to replace $g(x)$ and $h(x)$ by $\tilde{g}(x)$ and $\tilde{h}(x)$ with **integer** coefficients. Now think of $\tilde{g}(x)$ and $\tilde{h}(x)$ as polynomials in $\mathbf{F}_p[x]$. We know $f(x)$ has degree d in $\mathbf{F}_p[x]$ because p doesn't divide a_d. Now if $f(x)$ is prime in $\mathbf{F}_p[x]$, then it follows that $\tilde{g}(x)$ or $\tilde{h}(x)$ must be a constant and the other has degree d. But if $\tilde{g}(x)$ has degree d in $\mathbf{F}_p[x]$, then it must have had degree d to start with, and then $h(x)$ is a constant. Similarly, if $\tilde{h}(x)$ has degree d in $\mathbf{F}_p[x]$, then $g(x)$ must have been a constant. Putting this all together, we see that there is no factorization of $f(x)$ as a product of polynomials of smaller degrees. That is, $f(x)$ is prime in $\mathbf{Q}[x]$.

Example: $x^3 + x + 1$ is irreducible in $\mathbf{F}_2[x]$. It follows that the polynomials:

$$3x^3 + 6x^2 + 7x + 5, \quad 5x^3 + 9x - 1, \quad 17x^3 - 2x^2 - 21x - 39$$

and indeed any polynomial of the form:

$$(\text{odd})x^3 + (\text{even})x^2 + (\text{odd})x + (\text{odd})$$

is prime in $\mathbf{Q}[x]$.

Remark: This is a nice way to find lots of prime polynomials in $\mathbf{Q}[x]$ with integer coefficients starting with a prime polynomial in $\mathbf{F}_p[x]$. Unfortunately, we've seen that it is pretty hard to find prime polynomials in $\mathbf{F}_p[x]$ of large degrees (try to find a prime polynomial of degree 7 in $\mathbf{F}_2[x]$(!)) So we'll move on to one final method for checking primeness of polynomials.

Eisenstein's Criterion: Suppose

$$f(x) = a_d x^d + a_{d-1} x^{d-1} + ... + a_1 x + a_0$$

is a polynomial with integer coefficients, and suppose p is a prime number with the following properties:

(i) p divides $a_0, a_1, ..., a_{d-1}$.

(ii) p does not divide a_d.

(iii) p^2 does not divide a_0.

Then $f(x)$ is prime in $\mathbf{Q}[x]$.

Proof: If $f(x) = g(x)h(x)$, then by Gauss's Lemma, $f(x) = \widetilde{g}(x)\widetilde{h}(x)$ where $\widetilde{g}(x)$ and $\widetilde{h}(x)$ have integer coefficients. We have $f(x) = a_d x^d \in \mathbf{F}_p[x]$ when we think of it as a polynomial in $\mathbf{F}_p[x]$. This is a consequence of properties (i) and (ii) above. Thus $\widetilde{g}(x) = b_m x^m$ and $\widetilde{h}(x) = c_n x^n$ when thought of as polynomials in $\mathbf{F}_p[x]$ (by unique factorization). If m and n are both positive, this means that p divides the constant terms of both $\widetilde{g}(x)$ and $\widetilde{h}(x)$. This is impossible by property (iii) since it would imply that p^2 divides the contant term of $f(x)$. Thus either $m = 0$ or $n = 0$, which is to say either $n = d$ or $m = d$, telling us as before that either $g(x)$ is a constant or else $h(x)$ is a constant. In other words, $f(x)$ is prime!

Example: $x^d - 2$ is always prime in $\mathbf{Q}[x]$.

This is because 2 divides all the coefficients (including the zeroes) except for the coefficient of x^d, and 2^2 does not divide the constant.

Definition: A **number field** is a field which is also a finite dimensional vector space over $\mathbf{Q}$.

Example: (a) A $p(x)$-clock is a number field when $p(x) \in \mathbf{Q}[x]$ is prime. Then as we've seen, the dimension of the number field is the degree of $p(x)$.

(b) Suppose F is a number field of dimension n and $p(x)$ is a prime polynomial of degree d in $F[x]$. Then the $p(x)$-clock is a field which is a d-dimensional vector space over F. But then the $p(x)$-clock is an nd-dimensional vector space over $\mathbf{Q}$, so it is itself a number field.

Definition: Number fields which are contained in $\mathbf{C}$ are called **embedded** number fields. An identification of a number field F with an embedded number field is called a **complex embedding** of F.

Example and Notation: If $\alpha \in \mathbf{C}$, let

$$\mathbf{Q}[\alpha] = \{a_d\alpha^d + a_{d-1}\alpha^{d-1} + ... + a_1\alpha + a_0 \in \mathbf{C}\}$$

where $a_0, ..., a_d$ are any rational numbers. That is, $\mathbf{Q}[\alpha]$ are the complex numbers that are polynomials in α. If α is a root of a (prime) polynomial $p(x) \in \mathbf{Q}[x]$, then $\mathbf{Q}[\alpha]$ is a field, because it can be identified with the $p(x)$-clock F by identifying x with α, so that x^2 is identified with α^2, etc. Such an identification is an embedding of the $p(x)$-clock, and all the embeddings of the $p(x)$-clock are obtained by taking x to the complex roots of $p(x)$.

Example: (a) The $x^2 + 1$-clock over $\mathbf{Q}$ has two embeddings:

$$x \mapsto i \text{ or } \ x \mapsto -i$$

identifying the clock with $\mathbf{Q}[i]$ in two different ways.

(b) The $x^3 - 2$-clock over $\mathbf{Q}$ has three embeddings:

$$x \mapsto (\sqrt[3]{2}; 0), \ x \mapsto (\sqrt[3]{2}; \frac{2\pi}{3}) \text{ and } x \mapsto (\sqrt[3]{2}; \frac{4\pi}{3})$$

corresponding to the three complex cube roots of 2. Here the embedded number fields $\mathbf{Q}[\alpha]$ are different (e.g. only the first is contained in $\mathbf{R}$).

The **Gaussian Integers** are the numbers of the form:

$$\mathbf{Z}[i] = \{a + bi \text{ where } a, b \in \mathbf{Z}\}$$

with multiplication as complex numbers, so that $\mathbf{Z}[i] \subset \mathbf{Q}[i]$.

Division with Remainders: Given $a + bi$ and $c + di$, there is a quotient Gaussian integer $p + qi$ and a remainder Gaussian integer $r + si$ such that:

$$a + bi = (p + qi)(c + di) + (r + si) \text{ and } r^2 + s^2 < c^2 + d^2$$

Idea of Proof: Divide $a + bi$ by $c + di$ as complex numbers:

$$\frac{a + bi}{c + di} = x + yi$$

and take p to be the closest integer to x and q to be the closest integer to y. Since $|p - x| \leq \frac{1}{2}$ and $|q - y| \leq \frac{1}{2}$, it follows that $r^2 + s^2 < c^2 + d^2$.

Example:

$$\frac{4+14i}{1+2i} = \frac{(4+14i)(1-2i)}{5} = \frac{1}{5}(32+6i)$$

so $p = 6$, $q = 1$, and:

$$4 + 14i = (6+i)(1+2i) + (0+i) \text{ and } 1^2 < 1^2 + 2^2 = 5$$

Euclid's Algorithm: Run division with remainders repeatedly!

The GCD is the last remainder term in Euclid's algorithm.

Primes are the Gaussian integers which cannot be factored as products of Gaussian integers with smaller values for $a^2 + b^2$.

Unique Factorization: Every Gaussian integer is uniquely expressed as a product of finitely many primes.

So Gaussian integers behave a lot like ordinary integers!

On the other hand, the "unlucky integers":

$$\mathbf{Z}[\sqrt{-13}] = \{a + b\sqrt{-13} \text{ with } a, b \in \mathbf{Z}\}$$

does not behave a lot like the ordinary integers!

Primes in $\mathbf{Z}[\sqrt{-13}]$ are numbers $a + b\sqrt{-13}$ that cannot be factored as:

$$a + b\sqrt{-13} = (p + q\sqrt{-13})(c + d\sqrt{-13})$$

with $p^2 + 13q^2$ and $c^2 + 13d^2$ both less than $a^2 + 13b^2$.

It is not hard to check that $2, 7, 1 + \sqrt{-13}$ and $1 - \sqrt{-13}$ are all primes, and:

$$(2)(7) = 14 = (1 + \sqrt{-13})(1 - \sqrt{-13})$$

so that the unlucky integers do not have unique factorization!!

Exercises:

1. Decide whether the following polynomials are prime in $\mathbf{Q}[x]$ or not. If not, factor them completely. If prime, explain how you came to that conclusion (Eisenstein's criterion, rational root test or application of Gauss's Lemma)

(a) $x^3 + 2x + 4$

(b) $x^4 + 3x + 3$

(c) $27x^3 + 29x^2 + 35$

(d) $2x^9 + 3x^6 + 6x^3 + 21$

(e) $16x^3 + 35x + 65$

(f) $x^6 + 3x^4 + 3x^2 + 1$

2. Suppose $f(x) = x^{p-1} + x^{p-2} + ... + x + 1$ and p is a prime number. Prove that $f(x)$ is prime in $\mathbf{Q}[x]$.

(Hint: Apply Eisenstein's criterion to the polynomial $f(x+1)$.)

3. If $f(x)$ is prime in $\mathbf{Q}[x]$, prove that the complex roots of $f(x)$ are all different. That is, if $f(x)$ has degree d, then it has d distinct complex roots.

(Hint: If $(x-r)^2$ divides $f(x)$, show that $\gcd(f(x), f'(x)) \neq 1$)

4. Use Euclid's algorithm to find $\gcd(25 + 35i, 17 + 34i)$.

5. (a) If $(a + bi) = (p + qi)(c + di)$, show that $a^2 + b^2 = (p^2 + q^2)(c^2 + d^2)$.

(b) Which of the following prime numbers remain prime in $\mathbf{Z}[i]$?

$$(i)\ 3\ \ (ii)\ 5\ \ (iii)\ 7\ \ (iv)\ 11\ \ (v)\ 13\ \ (vi)\ 17$$

(c) Show that $2, 7, 1 + \sqrt{-13}$ and $1 - \sqrt{-13}$ are all prime in $\mathbf{Z}[\sqrt{-13}]$.