Summaries, March 17 and 19

Factoring Polynomials.

We consider the problem of factoring a given polynomial

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

with rational coefficients.

First, we may as well clear the denominators. So we can suppose that f has integer coefficients. The cost of doing this is that, whereas with rational coefficients we aan assume that f is *monic*, i.e., that $a_n = 1$, we can't do this if we want integer coefficients. However, if a polynomial

$$g(x) = b_r x^r + \cdots + b_0$$

divides f in $\mathbb{Q}[x]$, then if we make it primitive, the quotient will have integer coefficients too. This was discussed before. So at the cost of working with nonmonic polynomials, we can stay with integers.

(Recall that g is primitive if b_i are integers for all i, they have no common divisor, and b_r is positive.)

The simplest case is that g has degree 1, $g = b_1 x + b_0$. Then if g divides f, b_1 divides a_n and b_0 divides a_0. Since a_n and a_0 have finitely many intger divisors, there are finitely many linear polynomials to check for dividing f. Of course we prefer not to do such a check.

It is harder to decide if f has a divisor g of degree 2.

Reduction modulo p

The homomorphism $\mathbb{Z}[x] \xrightarrow{\pi} \mathbb{F}_p[x]$, p a prime integer, is a useful tool for studying divisibility. We denote the image $\pi(f)$ by $\overline{f}$ as usual:

$$\overline{f}(x) = \overline{a}_n x^n + \cdots + \overline{a}_0$$

If f factors, $f = gh$, then $\overline{f} = \overline{g}\overline{h}$, and provided that p doesn't divide the leading coefficient a_n of f, $\overline{g}$ and $\overline{h}$ will have the same degrees as g and h, respectively. So if we factor $\overline{f}$, we will, among other things, know the degrees of possible factors of f. This is helpful because there are finitely many polynomials of a given degree in $\mathbb{F}_p[x]$, so factoring of $\overline{f}$ can be done in finitely many steps.

The simplest application is to show that a polynomial f is irreducible. If we suspect that f is irreducible, we can reduce modulo som prime p. If $\overline{f}$ turns out to be irreducible, then we will have proved that f is irreducible.

Let's take the prime $p = 2$. There are two rules making computation modulo 2 particularly simple. Let R be a ring R of characteristi 2, i.e., in which $1+1 = 0$. Then, first, if a is in R, then, then $a+a = a(1+1) = 0$, so $a = -a$. This means that we can bring an element a that appears on one side of any equation to the other side without changing it. Second, if a and b are in R, then $(a+b)^2 = a^2 + b^2$ becauseth cross term $2ab$ is zero.

OK: Let's list the irrducible polynomials in $\mathbb{F}_2[x]$. First, in degree 1 there are two polynmials x and $x+1$, and obviously, both are irreducible. We use the "sieve method" to find the irrducible polynomials of degree 2. The polynomials of degree 2 are:

$$x^2, x^2 + x, x^2 + 1, x^2 + x + 1$$

The first two have 0 as root, and not irreducible. The third one $x^2 + 1$ has root 1, also not irreducible. The last one, $x^2 + x + 1$ doesn't have 0 or 1 as root. it is the only irreducible polynomial of degree 2.

We see here two necessary conditions that a polynomial must satisfy in order to be irreducible: The constant coefficient must be 1. If it is 0, then 0 is a root, and there must be an odd number of monomials with coefficient 1. If the number of those monomials is even, then 1 is a root.

Any reducible polynomial of degree 5 or less must have a linear factor or an irreducible quadratic factor. If it is made up of an odd number of monomials including 1 and is irreducible, it must be divisible by $x^2 + x + 1$. And it isn't hard to check divibility by that polynomial.

One way to can make that check easily is to look at the quotient ring $K = \mathbb{F}_2[x]/I$, where I is the principal ideal generated by $g = x^2 + x + 1$. Since g has degree 2, the residues of $0, 1, x, x^2$ form a basis for K, which is therefore a vector space of dimension 4 over the field $\mathbb{F}_2$. Let's use the same notation $0, 1, x, x^2$ forthe

residues. Since the residue of x^2+x+1 is zero, $x^2 = x+1$ in K. Since g is irreducible, K is a finite domain, and therefore a field. The multiplicative group $K^\times$ of nonzeo elements of K has order 3. It is a cyclic group. generated by any element different from 1, for example by x (more precisely, its residue). Then the powers of x run through the group $K^\times$:

$$1, x, x^2 = x+1, x^3 = 1, x^4 = x, x^5 = x+1, ...$$

Now to check whether a polynmial such as $f = x^5 + x^3 + x^2 + x + 1$ is irreducible in $\mathbb{F}_2[x]$, we look at its residue $\overline{f}$ in $\mathbb{F}_2[x]/I$. Working modulo g, we substitute the values of the powers, obtaining $\overline{f} = (x+1) + 1 + (x+1) + x + 1$. We cancel pairs of xs and pairs of 1s, and are left with x. Therefore $\overline{f}$ isn't zero and f isn't divisible by x^2+x+1. Since it has an odd number of terms and 1 appears, f is an irreducible element of $\mathbb{F}_2[x]$. Of course, there are otherways to do this.

the Eisenstein Criterion

It is easiest to understand this by going through an example. Let $f = x^5 + 3x^3 - 6x^2 + 3$. Reducing modulo 3, we get the polynomial $\overline{f} = x^5$ in $\mathbb{F}_3[x]$. Now suppose that f were reducible, say $f = gh$, where $g = x^2 + b_1x + b_0$ and $h = x^3 + \cdots + c_0$. Then in $\mathbb{F}_5[x]$, we will have $\overline{f} = \overline{g}\overline{h}$, and since $\overline{f} = x^6$, $\overline{g} = x^2$ and $\overline{h} = x^3$. Therefore the coefficients b_1, b_0, and c_2, c_1, c_0 are all divisible by 3. The constant term of f is the product b_0c_0. So it must be divisible by 3^2. Since the constant term is 3, this is a contradiction. So we can't have $f = gh$.

The principle at work here is the Eisenstein Criterion: Let $f(x) = a_nx^2 + \cdots + a_0$ be an integer polynomial and let p be a prime integer. Suppose that

- p doesn't divide a_n,
- p divides all other coefficients $a_{n-1}, ..., a_0$, and
- p^2 doesn't divide a_0.

Then f is irreducible in $\mathbb{Z}[x]$ and in $\mathbb{Q}[x]$.

The proof is the same as the one given in the example.

The Eisenstein Criterion doesn't apply often, but it is very useful when it does apply. Its most important application is to prove that the *cyclotomic polynomial* $\phi(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible when p is a prime. (When p is not a prime, this polynomial won't be irreducible.) The cyclotomic polynomial is the result of dividing $x^p - 1$ by $x - 1$:

$$x^p - 1 = (x-1)(x^{p-1} + \cdots + x + 1) = (x-1)\phi(x)$$

To prove that $\phi(x)$ is irreducible, we substitute $x = y + 1$ into this equation:

$$(y+1)^p - 1 = y\phi(y+1)$$

If $\phi(x)$ factors, so does $\phi(y+1)$. So it suffices to prove that $\phi(y+1)$ is irreducible. We expand the left side of the equation:

$$(y+1)^p - 1 = \big(y^p + \binom{p}{1}y^{p-1} + \cdots \binom{p}{p-1}y + 1\big) - 1$$

Dividing both sides of the equation by y,

$$y^{p-1} + \binom{p}{1}y^{p-2} + \cdots \binom{p}{p-1} = \phi(y+1)$$

Now, $\binom{p}{i}$ is divisible by p for every $i = 1, ..., p-1$. The reason is that $\binom{p}{i} = \frac{p!}{i!(p-i)!}$. In this fraction, the numerator is divisible by p but the denominator is not. The hypotheses of the Eisenstein Criterion are satisfied, so $\phi(y+1)$ and $\phi(x)$ are irreducible.

March 19: Imaginary Quadratic Number Fields

a particular case We look at the ring $R = \mathbb{Z}[\delta]$, with $\delta = \sqrt{-5}$. The elements of R have the form $a + b\delta$ with $a, b \in \mathbb{Z}$.

The example

$$2 \cdot 3 = 6 = (1 + \delta)(1 - \delta)$$

shows that factoring in R isn't unique. It is easy to check that the factors $2, 3, 1 + \delta$ and $1 - \delta$ are irreducible, and that they aren't associates. The method of handling arithmetic in such a ring was one of the important developments in number theory in the 19th century.

an aside Let R be a principal ideal domain, and suppose that we have two factorizations in R, say $au = bv$. To reconcile the two sides, we would look for a common divisor of a and b. Their greatest common divisor in R is the element d that generates the ideal $aR + bR$. Then we would have $a = da'$ and $b = db'$ with a', b' in R. We'd cancel d from both sides of the equation $da'u = db'v$ and we left with a smaller pair of factorizations $a'u = b'v$ to reconcile.

Now: Our ring $R = \mathbb{Z}[delta]$ isn't a principal ideal domain, and there is no element (other than ± 1) that divides both 2 and $1 + \delta$. However, there is an *ideal* that contains the two elements, namely the ideal I that is generated by the two elements: $2R + (1+\delta)R$. The elements of this ideal are combinations $r \cdots 2 + r' \cdot (1+\delta)$ with r and r' in R.

Let's write the ideal of a ring R that is generated by some elements $a_1, ..., a_k$ using parnthesis, as $(a_1, ..., a_r)$. The elements of $(a_1, ..., a_r)$ are combinations $r_1a_1 + \cdots + r_ka_k$ with coefficients r_i in R. With this notation, the ideal I is $(2, 1 + \delta)$. Let's denote this ideal by A.

You will be able to check that the elements of the ideal $\overline{A} = (2, 1 - \delta)$ are the complex conjugates of the elements of A. The ring R is equal to its complex onjugate, so the conjugateof an ideal is an ideal. Similarly we can consider the ideals $B = (3, 1 + \delta)$, and $\overline{B} = (3, 1 - \delta)$.

We need to define the *product ideal*. If I an J are ideals of a ring R, the notation IJ stands for the set of elements of R that are finite sums of products $x_1y_1 + \cdots + x_ny_n$ with x_i in I and y_i in J, and arbitrary n. It doesn't consist only of the products themselves.

If I is generated by $a_1, ..., a_k$, $I == (a_1, ..., a_k)$, and $J = (b_1, ..., bb_\ell)$, the product IJ will be generated by the $k\ell$ products $\{a_ib_j\}$.

Going back to our four ideals $A, \overline{A}, B, \overline{B}$, we form the product $AB = (2, 1+\delta)(3, 1+\delta)$. It is generaated by the four products:

$$AB = (6, 2(1 + \delta), 3(1 + \delta), (1 + \delta)^2)$$

We don't need to evaluate $(1 + \delta)^2$. What we see is that all four of the generators for AB are divisible by $1 + \delta$. Therefore the principal ideal $(1 + \delta)$ conntains AB. Moreover, $1 + \delta$ is the difference of the third and second generators of AB, so it is in AB, and therefore $(1 + \delta) \subset AB$. Putting these two conclusions together, we find that $AB = (1 + \delta)$. Similarly, one. So finds that $\overline{AB} = (1 - \delta)$, $\overline{A}A = (2)$, and $\overline{B}B = (3)$. So

$$(\overline{A}A)(\overline{B}B) = (2)(3) = (6) = (1 + \delta)(1 - \delta) = (AB)(\overline{AB})$$

So uniqueness of factoring is saved by looking at ideals.