Last time, we spoke about Euclidean domains. A key fact is that polynomials form a Euclidean domain; we can ‘divide’ polynomials with remainder. In class, I showed how this is done; this is much easier to ‘show’ than to ‘tell’, so I won’t write it here. (If you weren’t in class, the book has a description...)

We argued last time that everything we proved before about unique factorization is grounded in the existence of division with remainder. It is tempting to hope that, if we have a good notion of division with remainder (that is, if we are in a Euclidean domain), it will follow that unique factorization holds. This is indeed the case!

The rest of this section will be devoted to proving that we do indeed have unique factorization in every Euclidean domain. The proofs will be very reminiscent of the first section of the course. Throughout, we will illustrate with examples drawn from polynomials over \( \mathbb{R} \), but it should be stressed that this is just for illustrative purposes; everything we do works for any Euclidean domain we like.

**Definition 8.** Let \( R \) be a domain, and let \( a, b \in R \) be nonzero. We say \( a \) divides \( b \), and write \( a|b \), if there is some \( x \) such that \( ax = b \). We say that \( a \) and \( b \) are associates if \( a|b \) and \( b|a \). (In this case, \( b = xa \) and \( a = yb \) for some \( x, y \in R \), so \( b = xyb \) so \( (xy - 1)b = 0 \), so \( xy = 1 \)—this last step uses the domain property. Thus \( x \) is a unit, so \( b \) a multiple of \( a \) by a unit, and vice versa.)

**Definition 9.** Let \( R \) be a domain, and let \( a, b \in R \). We say that a \( c \in R \) is a highest common factor of \( a \) and \( b \) iff:

- \( c|a \) and \( c|b \)
- If \( d \in R \) such that \( d|a \) and \( d|b \) then \( d|c \).

Note that we say ‘a’ highest common factor, rather than ‘the’; if you multiply an hcf by a unit, the result will still be an hcf. Any two hcfs will always be associates, though.

It is not always the case that there is an hcf, but in a Euclidean domain, we can carry out the Euclidean algorithm, by repeatedly using the division-with-remainder property. Here is the general way the Euclidean algorithm works, with a general case on the left and a polynomial example on the right. Note that the general case looks just like the general case for the natural numbers, although now all the letters stand for elements of our general Euclidean domain, not for natural numbers.

We will write \( f \) for our Euclidean size function.

- Write \( a = q_1b + r_1 \). (\( f(r_1) \leq f(b) \)) \[ x^6 - x = (x^2)(x^4 - x) + (x^3 - x) \]
- Write \( b = q_2r_1 + r_2 \). (\( f(r_2) < f(r_1) \)) \[ x^4 - x = (x)(x^3 - x) + (x^2 - x) \]
- Write \( r_1 = q_3r_2 + r_3 \). (\( f(r_3) < f(r_2) \))

...Keep going until \( r_{n-1} = q_{n+1}r_n + r_{n+1} \) with \( r_{n+1} = 0 \). \[ x^3 - x = (x + 1)(x^2 - x) + 0. \]

Output \( r_n \). Answer is \( x^2 - x \).

**Proposition 10.** Euclid’s algorithm will always eventually stop. When it stops, the output is an hcf of \( a \) and \( b \).

**Proof.** Since \( f(b) > f(r_1) > f(r_2) > \cdots > f(r_j) \), it can last at most \( f(b) \) steps, so it will indeed stop. Also, we have \( r_n|r_{n-1} \) (last line). So \( r_n|r_{n-2} \) (second to last line); so \( r_n|r_i \) for all \( i \) (technically, by induction). The first two rows then say \( r_n|b \) and \( r_n|a \). On the other hand, if \( d|a \) and \( d|b \) then \( d|r_1 \) (by the first line). Then \( d|r_2 \) (second line) and (again, technically by induction) \( d|r_i \) for all \( i \) in particular, \( d|r_n \).

**Proposition 11.** Let \( R \) be a Euclidean domain, and let \( a, b \in R \), with hcf \( h \). Then we can find elements of \( R \), \( x, y \) with \( ax + by = h \).

**Proof.** Again, looking at the output of Euclid; \( r_n \) is a linear combination of \( r_{n-1} \) and \( r_{n-2} \) (penultimate line). Then \( r_n \) is a linear combination of \( r_{n-2}, r_{n-3} \) (substitute for \( r_{n-1} \) using antepenultimate line). Use induction again; get \( r_n \) is a l.c. of \( a \) and \( b \).
**Definition 12.** Suppose $R$ is a ring. An element $t$ is prime if whenever $t|ab$ for $a, b \in R$, we may conclude that $t|a$ or $t|b$.

**Proposition 13.** In a Euclidean domain, every irreducible element is prime. That is, if $R$ is a Euclidean domain, $p \in R$ is irreducible, and $p|ab$. Then $p|a$ or $p|b$.

*Proof.* Suppose $p \nmid a$. Want to show $p|b$. But $\gcd(a, p) = 1$, so $1 = ax + py$. Multiply by $b$: $b = bax + pby$. $p$ divides RHS, so it divides $b$.  

\qed