

The Division Algorithm

Our work on Friday should convince us that quite frequently we can treat polynomials like numbers in performing arithmetic with them. Perhaps the following is not incredibly surprising:

Theorem (3.46: Division Algorithm). Let R be a commutative ring, and let $f(x), g(x) \in R[x]$ such that the leading coefficient of $f(x)$, $LT(f)$, is a unit.

1. There are polynomials $q(x), r(x) \in R[x]$ such that $g(x) = q(x)f(x) + r(x)$ and either $r(x) = 0$ or $\deg(r) < \deg(f)$.
2. If R is an integral domain, then q and r are unique.

Proof. What happens if $f(x)|g(x)$?

If this isn't the case, then consider the nonzero polynomial $r(x)$ of least degree having the form $g(x) - q(x)f(x)$. (The minimum is taken over all possible qs !)

Write $f(x) = s_0 + s_1x + \cdots + s_nx^n$ and $r(x) = t_0 + t_1x + \cdots + t_mx^m$. What two possibilities do our computations from Friday suggest for the polynomial

$$h(x) = r(x) - \frac{LT(r)}{LT(f)}f(x)?$$

What happens if $h(x) = 0$? (*Hint:* compute $g = qf + r$.)

What happens if $h(x) \neq 0$ but $\deg(h) < \deg(r)$? (*Hint:* can you write h in the form $g - q'f$?)

I'll leave the proof of the second part of the theorem as an exercise for you. (It's also given on page 254 of your text.)

Definitions. Not surprisingly, we can call $q(x)$ the _____ and $r(x)$ the _____ of the Division Algorithm.

Usually we reserve this terminology for the case in which R is a field, since then these polynomials are unique. For the time being let us assume we're in that case and replace R with k .

Given $f(x) \in k[x]$, any element $a \in k$ is called a _____ of f if $f(a) = _ _$.

Question. Let $a \in k$. Suppose you want to divide $f(x) \in k[x]$ by the linear polynomial $x - a$. What's the remainder in this case?

From your answer to this last fact, we immediately get the following

Proposition (3.49). Let k be a field and let $f(x) \in k[x]$ and $a \in k$. Then a is a root of f if and only if $(x - a) | f(x)$ in $k[x]$.

Proof.

Theorem (3.50). If k is a field and $f(x) \in k[x]$ then $f(x)$ has at most n roots in k .

Proof.

Example. Can you find a ring R and a polynomial $f(x) \in R[x]$ such that $f(x)$ has *more* than $\deg(f)$ roots in R ?

Homework. Here are a few more homework problems that are mostly computational and investigate the roots of some simple polynomials over finite fields. None of these problems are committee problems. They are all due on *Friday, February 6th*.

1. Find every root of the polynomial $x^2 + a$ in \mathbb{Z}_7 , for each $a \in \mathbb{Z}_7$, in turn.
2. Let $P = \{3, 5, 7, 11, 13, 17, 19, 23\}$ be the collection of the first 8 odd primes.
 - (a) For each $p \in P$ find all roots of the polynomial $f(x) = x^2 + 1$ in \mathbb{Z}_p .
 - (b) Do you notice a pattern?
3. Let P be as above.
 - (a) For each $p \in P$ find all roots of the polynomial $g(x) = x^2 - 2$ in \mathbb{Z}_p .
 - (b) **(Extra Credit.)** Do you notice a pattern? (*Hint:* This is one's *really* tough to see with such a small amount of data!)