2.4 Clock Arithmetic and Finite Fields.

We want to think about roots of prime polynomials in $\mathbb{Q}[x]$. An appropriate first question is: "How do we know there are any interesting prime polynomials?" The rational roots test tells us there are lots of polynomials with no rational roots, but that doesn't tell us the polynomials are prime! We'll find prime polynomials using finite fields, which are constructed with "clock arithmetic."

Fix a natural number n.

Definition: Integers a and b are **equivalent mod** n, written:

$$a \equiv b \pmod{n}$$

if n divides $a - b$.

First of all, equivalence mod n is an equivalence relation (see §1.2):

(i) Reflexive:

$a \equiv a \pmod{n}$ because $a - a = 0$ and n divides 0.

(ii) Symmetric:

If $a \equiv b \pmod{n}$, then n divides $a - b$, which means $a - b = dn$ for some d, and then $b - a = (-d)n$ so $b \equiv a \pmod{n}$.

(iii) Transitive:

If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ then $a - b = dn$ and $b - c = en$, so $a - c = (a - b) + (b - c) = (d + e)n$ and so $a \equiv c \pmod{n}$.

Definition: We let $[a]$ be the equivalence class of $a \pmod{n}$.

Remark: There are n different equivalence classes:

$$\mathbb{Z}_n = \{[0], [1], [2], ..., [n-2], [n-1]\}$$

since we can always divide by n to get a remainder between 0 and $n - 1$, and two different remainders are never equivalent.

Definition of "clock" addition and multiplication in $\mathbb{Z}_n$:

$$[a] + [b] = [a + b] \quad \text{and} \quad [a][b] = [ab]$$

These are well-defined: If $a - a' = dn$ and $b - b' = en$ then:

$$(a + b) - (a' + b') = (a - a') + (b - b') = (d + e)n$$

so addition is well-defined, and:

$$(ab) - (a'b') = (a - a')b + a'(b - b') = dnb + a'en = (db + a'e)n$$

so multiplication is well-defined!

With these definitions, it is obvious that:

(a) Clock addition is associative and commutative.

(b) $[0]$ is the additive identity and $[-a]$ is the additive inverse of $[a]$.

(c) Clock multiplication is distributive, associative and commutative.

(d) $[1]$ is the multiplicative identity.

but there is no cancellation law unless n is a **prime**.

Example: If $n = 12$ (the "usual" clock on the wall), then:

$$[3][4] = [12] = 0$$

so the cancellation law doesn't hold! (See Exercise 6-1) In other words, 12-clock arithmetic isn't an integral domain (see §2.2). However:

Proposition 2.4.1. *p-clock arithmetic is a* **field***:*

$$\mathbb{Z}_p := \{0 = [0], 1 = [1], ..., [p-1]\}$$

if p is a prime number.

Proof: Because of (a)-(d) above, we just need to find multiplicative inverses of everything (except 0). We use Propositions 2.2.2 and 2.2.4. Namely, if $[a] \neq [0]$, then p does not divide a and Proposition 2.2.4 says that 1 is a gcd of a and p. Then Proposition 2.2.2 says:

$$1 = up + va$$

for some integers u, v. But $1 - va = up$ tells us $1 \equiv va \pmod{p}$ and so:

$$1 = [1] = [va] = [v][a]$$

That is, $[v]$ is the multiplicative inverse of $[a]$!

Examples:

(a) $\mathbb{Z}_2 = \{0, 1\}$ and $[1] + [1] = [2] = [0]$. Just as before! (See §2.1)

(b) $\mathbb{Z}_3 = \{0, 1, [2]\}$ and $[2] = -1$ in this field. (Compare with Exercise 5-5)

(c) $\mathbb{Z}_5 = \{0, 1, [2], [3], [4]\}$ with the following "+" and "×" tables:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

So there are fields with any prime p number of elements. We will later see how to find fields with any **prime power** p^n number of elements.

Now that we know $\mathbb{Z}_p$ is a field, we can consider $\mathbb{Z}_p[x]$, the set of polynomials with coefficients in $\mathbb{Z}_p$. Rather surprisingly, these polynomials will help us to find prime polynomials in $\mathbb{Q}[x]$. What's the connection? If we start with a polynomial with integer coefficients:

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

we can take the equivalence classes of the coefficients to get:

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

(putting brackets around $f(x)$ is just a device to shorten the notation). Each $[f(x)]$ is called **the reduction mod p** of $f(x)$. For example:

$$[px^2 + px + p] = [p]x^2 + [p]x + [p] = [0]x^2 + [0]x + [0] = 0$$

Another example: $[x^2 + x - 3] = x^2 + x = (x + [1])(x) \in \mathbb{Z}_3[x]$ shows that the reduced polynomial can factor when the original doesn't. On the other hand, if $f(x)$ factors, then:

$$[f(x)] = [g(x)h(x)] = [g(x)][h(x)]$$

because it makes no difference whether we take the reduction mod p before or after multiplying the polynomials!

Gauss's Lemma: If $f(x)$ is a polynomial with integer coefficients and

$$f(x) = g(x)h(x) \in \mathbb{Q}[x]$$

then there is a rational number $\frac{a}{b}$ so that $\frac{a}{b}g(x)$ and $\frac{b}{a}h(x)$ both have **integer** coefficients, and of course:

$$f(x) = \left(\frac{a}{b}g(x)\right)\left(\frac{b}{a}h(x)\right)$$

Proof: Since the coefficients of $g(x)$ and $h(x)$ are rational numbers, we can clear the denominators by multiplying through by some pair of natural numbers m and n so that $mg(x)$ and $nh(x)$ are polynomials with **integer** coefficients. Then:

$$mnf(x) = (mg(x))\,(nh(x))$$

is a product of polynomials with integer coefficients. Of course, this isn't what we want. But now suppose p is a prime and p divides mn. Then p divides all the coefficients of $mnf(x)$ and so $mnf(x)$ reduces to the zero polynomial mod p. But that means:

$$0 = [mg(x)][nh(x)] \in \mathbb{Z}_p[x]$$

Since $\mathbb{Z}_p[x]$ is an integral domain (see §2.2), it has a cancellation law, which tells us that **either** $[mg(x)] = 0$ or $[nh(x)] = 0$ (Exercise 6-1). So p divides all the coefficients of $mg(x)$ or of $nh(x)$. **Now divide through by p and continue.** That is, if p divides all the coefficients of $mg(x)$, change it to $\frac{m}{p}g(x)$, otherwise change $h(x)$ to $\frac{n}{p}h(x)$. This gives us two polynomials with integer coefficients whose product is $\frac{mn}{p}f(x)$. We can keep doing this, dividing either m or n on the right by by each of the primes that divide mn to finally get:

$$f(x) = \left(\frac{m}{p_1 \cdots p_d} g(x)\right)\left(\frac{n}{q_1 \cdots q_e} h(x)\right)$$

with $mn = p_1 \cdots p_d \cdot q_1 \cdots q_e$ and each of the polynomials on the right side has integer coefficients!

Example: Starting with a “silly’ factorization $x^2 - 1 = (\frac{3}{2}x - \frac{3}{2})(\frac{2}{3}x + \frac{2}{3})$, clear denominators taking $m = 2$ and $n = 3$ to get:

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

Dividing through by $p = 2$ gives:

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

and dividing through by $p = 3$ gives:

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

the factorization with integer coefficients.

Proposition 2.4.2. *Suppose*

$$f(x) = a_d x^d + ... + a_0 \in \mathbb{Q}[x]$$

has integer coefficients, and that p is a prime that doesn’t divide a_d. Then if $[f(x)]$ is prime in $\mathbb{Z}_p[x]$, it follows that $f(x)$ is prime in $\mathbb{Q}[x]$.

Proof: Since we assume p doesn’t divide a_d, the reduced polynomial $[f(x)]$ is a polynomial of degree d in $\mathbb{Z}_p[x]$. If $f(x) = g(x)h(x)$, then Gauss’ lemma says $g(x)$ and $h(x)$ can be replaced by polynomials with integer coefficients (without changing their degrees) and then: $[f(x)] = [g(x)][h(x)]$. But if $[f(x)]$ is prime, then $[g(x)]$ (or $[h(x)]$) must have degree d, and then $g(x)$ (or $h(x)$) must have had degree d. So $f(x)$ is prime!

Example: $x^4 + x + 1 = [x^4 + x + 1]$, is prime in $\mathbb{Z}_2[x]$ (Exercise 5.4). It follows that this polynomial, as well as each of the polynomials:

$$3x^4 + 2x^2 + 6x^2 + 7x + 5, \quad 5x^4 + 9x - 1, \quad 17x^4 - 2x^3 - 21x - 39$$

and indeed any polynomial with integer coefficients of the form:

$$(\text{odd})x^4 + (\text{even})x^3 + (\text{even})x^2 + (\text{odd})x + (\text{odd})$$

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

Remark: This gives us infinitely many prime polynomials in $\mathbb{Q}[x]$ with integer coefficients starting with a single prime polynomial in $\mathbb{Z}_p[x]$. We know that there are prime polynomials of larger and larger degrees in $\mathbb{Z}_p[x]$, by Euclid's theorem, so we know there are prime polynomials in $\mathbb{Q}[x]$ of larger and larger degrees. But it can be hard to use this to check whether a **given** polynomial is prime! For example, is $x^n - 2$ prime? It certainly isn't prime in $\mathbb{Z}_2[x]$. Is it prime in $\mathbb{Z}_3[x]$? In $\mathbb{Z}_5[x]$?

Eisenstein's Criterion: If

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

is a polynomial with integer coefficients, and p is a prime such that:

(i) p divides each of the coefficients $a_{d-1}, a_{d-2}, ..., a_1, a_0$.

(ii) p doesn't divide a_d.

(iii) p^2 doesn't divide a_0.

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

Proof: If $f(x) = g(x)h(x)$, then by Gauss's Lemma we can assume $g(x)$ and $h(x)$ have integer coefficients. Properties (i) and (ii) above tell us that $[f(x)] = [a_d]x^d \in \mathbb{Z}_p[x]$ since all the other coefficients are divisible by p. But then it follows from the unique factorization in the fundamental theorem of arithmetic (§2.2) that $[g(x)] = [b_m]x^m$ and $[h(x)] = [c_n]x^n$. If m and n are both positive, this means in particular that p divides the constant terms of both $g(x)$ and $h(x)$. But this would imply that p^2 divides the contant term of $f(x)$, violating (iii). Thus either $m = 0$ or $n = 0$, which is to say either $n = d$ or $m = d$, telling us that either $g(x)$ or $h(x)$ has degree d, hence $f(x)$ is prime!

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

Use the criterion for $p = 2$. (This also shows that every $x^n - p$ is prime.)

Remark: Eisenstein's criterion was designed to prove that a certain kind of polynomial, the "cyclotomic" polynomial is prime. Namely:

Corollary 2.4.3. *If p is a prime number, then:*

$$f(x) = x^{p-1} + x^{p-2} + ... + x + 1 = \frac{x^p - 1}{x - 1}$$

is a prime polynomial.

Proof: Obviously Eisenstein's criterion doesn't apply to $f(x)$. Instead, we will apply it to the polynomial $f(x + 1)$. Notice that any factorization of $f(x)$:

$$f(x) = g(x)h(x)$$

gives a factorization of $f(x + 1)$:

$$f(x + 1) = g(x + 1)h(x + 1)$$

and vice versa, so that if we want to see that $f(x)$ is prime, we may instead prove that $f(x + 1)$ is prime!

By Exercise 5-1, we know that:

$$(x+1)^p = x^p + \frac{p!}{(p-1)!1!}x^{p-1} + \frac{p!}{(p-2)!2!}x^{p-2} + ... + \frac{p!}{1!(p-1)!}x + 1$$

from which we get:

$$f(x+1) = \frac{(x+1)^p - 1}{(x+1)-1} = x^{p-1} + \frac{p!}{(p-1)!1!}x^{p-2} + ... + \frac{p!}{2!(p-2)!}x + \frac{p!}{1!(p-1)!}$$

But now Eisenstein's criterion does apply!

(i) p divides $p!$ (of course), which we can rewrite as:

$$p! = \left(\frac{p!}{(p-n)!n!}\right)(p-n)!n!$$

and as long as $p-n$ and n are both less than p, then p cannot divide $(p-n)!n!$ because p is bigger than all the prime factors. So p divides:

$$\frac{p!}{(p-n)!n!}$$

which are all the coefficients of $f(x+1)$ (except the first one).

(ii) The leading coefficient of $f(x+1)$ is 1 and p doesn't divide 1.

(iii) The last coefficient is $\frac{p!}{1!(p-1)!} = p$, and p^2 doesn't divide p.

So Eisenstein's criterion applies, and $f(x+1)$ (and $f(x)$) is prime.

Examples: (a) $(p=3)$: $f(x) = x^2 + x + 1$ is prime and:

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

(b) $(p=5)$: $f(x) = x^4 + x^3 + x^2 + x + 1$ is prime and:

$$f(x+1) = x^4 + 5x^3 + 10x^2 + 10x + 5$$

(c) On the other hand, $f(x) = x^3 + x^2 + x + 1 = (x+1)(x^2+1)$ and:

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

(What went wrong? Well, 4 isn't a prime, so Eisenstein's criterion fails!)

In fact, one can prove that:

$$x^{n-1} + x^{n-2} + ... + x + 1$$

is **only** a prime polynomial when n is a prime number.

2.4.1 Clock Arithmetic and Finite Fields Exercises

8-1 Write addition and multiplication tables for the following fields:

(a) $\mathbb{Z}_7$ (b) $\mathbb{Z}_{11}$ (c) $\mathbb{Z}_{13}$

8-2 (a) Prove that if n isn't prime, then $\mathbb{Z}_n$ isn't a domain.

(b) Prove that if 1 is a gcd of a and n, then $[a]$ has a multiplicative inverse in $\mathbb{Z}_n$ (and we'll call $[a]$ a unit even when $\mathbb{Z}_n$ isn't a domain).

(c) Find every unit in $\mathbb{Z}_{48}$ and its multiplicative inverse.

(d) Find the multiplicative inverse of $[1027]$ in $\mathbb{Z}_{20317}$.

8-3 Prove that if n isn't a prime number, then:

$$x^{n-1} + x^{n-2} + ... + 1 \text{ isn't a prime polynomial}$$

8-4 Decide whether the following polynomials are prime in $\mathbb{Q}[x]$ or not. If not, factor them. If prime, explain how you came to that conclusion
(Eisenstein's criterion, rational root test or Proposition 2.4.2)

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

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

(c) $x^4 + 3x^3 + 9$

(d) $x^4 + 6x^2 + 9$

(e) $x^5 + 5x^4 + 10x^3 + 10x^2 + 5x + 1$

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

(g) $x^6 + x^3 + 1$

8-5 For which primes p is $[x^2 + 1] \in \mathbb{Z}_p[x]$ prime? For example:

In $\mathbb{Z}_2[x]$, it isn't prime: $[x + 1]^2 = [x^2 + 1]$.

In $\mathbb{Z}_3[x]$, it is prime (Exercises 6).

In $\mathbb{Z}_5[x]$, it isn't prime: $[x - 2][x - 3] = [x^2 - 5x + 6] = [x^2 + 1]$.

What about in $\mathbb{Z}_7[x], \mathbb{Z}_{11}[x], \mathbb{Z}_{13}[x], \mathbb{Z}_{17}[x], \mathbb{Z}_{19}[x]$?

Do you see a pattern?