Polynomials over Zp

Reading

- Section 10.2

Practice Problems

10.2 1–4, 7, 8
10.2 (Optional) 9–13, 15. These problems concern the quadratic formula.

Notes

Polynomials over Zn

Polynomials over $\mathbb{Z}_n$ are defined similarly to real-valued polynomials, except for the fact that all numbers and operations come from $\mathbb{Z}_n$. For instance we can write:

$$\bar{3}\bar{x}^2 + \bar{4}\bar{x} + \bar{1}$$

Where all elements are considered modulo 7. We will omit the bars for simplicity.

Given such a polynomial $f(x)$, we can evaluate it at any point of $\mathbb{Z}_n$, by replacing x by that value and then carrying out the computations. For instance in the example above, let's compute the value of f at all points:

x	$f(x)$
0	$3 \cdot 0^2 + 4 \cdot 0 + 1 = 1$
1	$3 \cdot 1^2 + 4 \cdot 1 + 1 = 8 = 1$
2	$3 \cdot 2^2 + 4 \cdot 2 + 1 = 21 = 0$
3	$3 \cdot 3^2 + 4 \cdot 3 + 1 = 40 = 5$
4	$3 \cdot 4^2 + 4 \cdot 4 + 1 = 65 = 2$
5	$3 \cdot 5^2 + 4 \cdot 5 + 1 = 3(-2)^2 - 4 \cdot 2 + 1 = 5$
6	$3 \cdot 6^2 + 4 \cdot 6 + 1 = 3(-1)^2 - 4 \cdot 1 + 1 = 0$

So this polynomial takes the values 0, 1, 2 and 5. Notice also that there are two points x for which $f(x) = 0$.

Many familiar algebraic properties hold. In particular, it makes sense to multiply polynomials together, or to add them, and evaluating the polynomials at a point gives the same result before and after.

An important property of polynomials is **polynomial division**:

> If $f(x)$, $g(x)$ are polynomials, and the leading coefficient of $g(x)$ is invertible, then there are (unique) polynomials $q(x)$ and $k(x)$ where the degree of $k(x)$ is

less than the degree of $g(x)$ and:

$$f(x) = q(x)g(x) + k(x)$$

A special important case of this is when $g(x) = x - a$. Then we have:

$$f(x) = q(x)(x - a) + f(a)$$

As a consequence, a polynomial $f(x)$ has a as a root if any only if it is perfectly divisible by $x - a$.

Dividing by $x - a$ uses the familiar method of **synthetic division**[1], which is the same way in which a computer would in fact evaluate a polynomial.

Roots of a polynomial

One important consideration is the number of roots/zeros of a polynomial. For instance we can see in the example above that there are two roots, namely 2 and 6. Could there be more? We will answer the question shortly. But first, suppose we were working modulo 8, and let us repeat the evaluations above:

x	$f(x)$
0	$3 \cdot 0^2 + 4 \cdot 0 + 1 = 1$
1	$3 \cdot 1^2 + 4 \cdot 1 + 1 = 8 = 0$
2	$3 \cdot 2^2 + 4 \cdot 2 + 1 = 21 = 5$
3	$3 \cdot 3^2 + 4 \cdot 3 + 1 = 40 = 0$
4	$3 \cdot 4^2 + 4 \cdot 4 + 1 = 65 = 1$
5	$3 \cdot 5^2 + 4 \cdot 5 + 1 = 96 = 0$
6	$3 \cdot 6^2 + 4 \cdot 6 + 1 = 133 = 5$
7	$3 \cdot 7^2 + 4 \cdot 7 + 1 = 176 = 0$

So you see that modulo 8, this polynomial has 4 zeros! It is a polynomial of degree 2, and yet it has 4 zeros.

Let's try to understand how this might be possible. First let's start with the solution $a = 1$. This means that our polynomial is divisible by $x - 1$, and in fact it is easy to see that:

$$3x^2 + 4x + 1 = (3x + 7)(x - 1)$$

Now we look for other solutions. In a real variable case, we could say the following: If a is another solution, then we must have:

$$0 = 3a^2 + 4a + 1 = (3a + 7)(a - 1)$$

[1] http://en.wikipedia.org/wiki/Synthetic_division

Since $a-1$ is non-zero, it must mean that $3a+7=0$, and solving for a we find the unique other solution.

In $\mathbb{Z}_8$ this is no longer the case! $(3a+7)(a-1)$ might equal 0 without either factor equaling 0, because we can have zero-divisors. For example when $a=5$ we have $3a+7=22=-2$ and $a-1=4$, and therefore $(3a+7)(a-1)=-2\cdot 4=0$.

This problem only occurs because of the presence of zero-divisors in $\mathbb{Z}_8$. This is in fact the only obstacle. We have the following theorem:

> If p is prime and $f(x)$ is a polynomial over $\mathbb{Z}_p$ of degree d, then $f(x)$ has at most d distinct roots in $\mathbb{Z}_p$.
>
> This is true more generally when we use values from a field ($\mathbb{Z}_p$ in this instance).

Let us prove this theorem.

- Say a is a root of $f(x)$.
- Then we can write $f(x)=g(x)(x-a)$ where $g(x)$ has degree $d-1$.
- If $b\neq a$ is a root of $f(x)$ then:
  - $g(b)(b-a)=0$.
  - In the absence of zero-divisors, $g(b)=0$.
  - So b is a root of $g(x)$.
- So any root of $f(x)$ different from a must be a root of $g(x)$.
- But by induction, since $g(x)$ is of degree $d-1$, it has at most $d-1$ roots.
- Adding a to that list, we see that $f(x)$ has at most d roots.
- All we need is to take care of the base case. A polynomial of degree 0 is just a constant $c\neq 0$, and it has 0 roots.

Roots of unity

There is a special polynomial whose roots we will be interested in, namely x^m-1.

> The roots of the polynomial x^m-1 are called the m-th *roots of unity*.
>
> They are the solutions to the equation $x^m=1$.

In $\mathbb{Z}_p$ it is easy to describe the solutions:

> If p is a prime and $m\in\mathbb{N}$, consider the equation $x^m=1$ in $\mathbb{Z}_p$.
>
> 1. If $m|(p-1)$, then there are exactly m solutions.
> 2. For any m, then there are exactly $\gcd(m,p-1)$ solutions.

Let us prove this:

- We start with the case where $m = p - 1$.
  - Fermat's theorem tells us that all numbers $1, 2, \ldots, p-1$ are roots.
- Now for other cases with $m | p - 1$.
  - We start with $p - 1 = km$.
  - This allows us to factor $x^{p-1} - 1 = (x^m)^k - 1$, using the formula for $y^k - 1 = y^{k-1} + y^{k-2} + \cdots + y^1 + 1$:

$$(x^m)^k - 1 = (x^m - 1)((x^m)^{k-1} + (x^m)^{k-2} + \cdots + (x^m)^1 + 1)$$

  - Note that the left-hand-side has exactly $p - 1$ distinct solutions.
  - Each one of these solutions must also solve one of the two factors on the right.
  - The one factor can have at most m solutions, while the other can have at moat $m(k-1) = mk - m$ roots.
  - This adds up to exactly $mk = p - 1$.
  - Since that's how many solutions we must have, it must be the case that $x^m - 1$ indeed has exactly m roots.
- For the second part:
  - Let $d = \gcd(m, p-1)$.
  - If $x^m = 1$ then $x^d = 1$ as well.
    * That is because $d = a \cdot m + b(p-1)$.
    * So $x^d = (x^m)^a (x^{p-1})^b = 1$.
  - Conversely if $x^d = 1$, then since d divides m we also have $x^m = 1$.
  - So the roots of $x^m - 1$ are the same as the roots of $x^d - 1$.
  - And we know that $x^d - 1$ has exactly $d - 1$ roots.