Vanishing Polynomials and Polynomial Functions

Matvey Borodin, Ethan Liu, Justin Zhang
Mentor: James Coykendall

MIT PRIMES USA

October 15-16, 2022
MIT PRIMES Conference

Rings

Definition (Ring)

A **ring** is a set A with operation $+$ and $\times$ such that:

- A is closed under $+$ and $\times$.
- $+$ is commutative and has inverses (so $-$ exists).
- There is an additive identity (denoted 0).
- Both operations are associative.
- The distributive law holds ($(a+b) \times c = a \times c + b \times c$).

We will be working with commutative rings (so $\times$ is commutative).

Vanishing Polynomials

Definition (Polynomial)

A **polynomial** $F(x)$ in a polynomial ring $R[x]$ is a formal sum

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

for some nonnegative integer n, where each $a_i \in R$ and x is an indeterminate.

Definition (Vanishing polynomial)

A **vanishing polynomial** $F(x) \in R[x]$ is a polynomial such that $F(a) = 0$ for all $a \in R$. By definition, 0 itself is a vanishing polynomial.

Simple Vanishing Polynomials

Example

Consider the polynomial $F(x) = x^2 + x$ over $\mathbb{Z}_2$. Notice that $F(0) = 0$ and $F(1) = 2 = 0$.

Example

Consider the ring $R = \Pi_{n=1}^{\infty} \mathbb{Z}_2$. Notice that $x^2 + x$ is vanishing in this ring as well.

Example

Over the ring $\mathbb{Z}_6$, the polynomial $x(x-1)(x-2)(x-3)(x-4)(x-5)$ clearly vanishes; however, the lower degree $x(x-1)(x-2)$ and $3(x-1)(x-2)$ also vanish.

Polynomial Functions

Definition (Polynomial function)

A **polynomial function** $f : R \to R$ is a function on R for which there exists a polynomial $F(x) \in R[x]$ such that $f(r) = F(r)$ for all $r \in R$.

Polynomials are denoted with uppercase letters while polynomial functions are denoted with lowercase letters.
Thus, $F(x)$ is a polynomial but $f(x)$ is a polynomial function.

Polynomial Functions

Example

Over $\mathbb{Z}_6$, $F(x) = x^2 + 1$ is a polynomial while the mapping induced, namely f which maps $0 \to 1, 1 \to 2, 2 \to 5, 3 \to 4, 4 \to 5, 5 \to 2$, is a polynomial function.

Ideal of Vanishing Polynomials

Definition (Ideal)

A subring $S \subseteq R$ is an **ideal** if $rs \in S$ for all $r \in R$ and $s \in S$.

Lemma (Well-known)

Vanishing polynomials form an ideal.

Vanishing Polynomials Over $\mathbb{Z}_n$

Theorem (Singmaster, 1974)

Any element of the ideal of vanishing polynomials over $\mathbb{Z}_n$ is of the form

$$G(x) = F(x)B_s(x) + \sum_{k=0}^{s-1} a_k \cdot \frac{n}{\gcd(k!, n)} \cdot B_k(x)$$

where $B_k(x) = (x+1)(x+2)\dots(x+k)$ with $B_0(x) = 1$, and s is the smallest integer such that $n \mid s!$. $F(x)$ is a polynomial which is uniquely defined based on $G(x)$, and a_k's are integers also uniquely defined in the range $0 \leq a_k < \gcd(k!, n)$.

Vanishing Polynomials Over $\mathbb{Z}_n$

Definition

A polynomial $P(x)$ is **integer valued** if for all integers n, $P(n)$ is an integer.

- Any vanishing polynomial $F(x)$ corresponds to an integer valued polynomial $G(x) = F(x)/n$.
- Conversely, in order for an integer-valued polynomial $G(x)$ to correspond to a polynomial $F(x) = nG(x)$, all resulting coefficients in $F(x)$ must be integers.

Vanishing Polynomials Over $\mathbb{Z}_n$

$\binom{x}{k} = \frac{x(x-1)\cdots(x-k+1)}{k!}$ denotes the "choose" function.

Lemma (Well-known)

Any integer-valued polynomial can be uniquely expressed as a linear sum with integer coefficients of functions of the form $\binom{x}{k}$.

By the lemma, every such $G(x)$ can be uniquely represented as a sum $G(x) = \sum_{k=1}^{m} c_k \binom{x}{k}$. Thus, every vanishing polynomial $F(x)$ over $\mathbb{Z}_n$ can be uniquely represented as

$$F(x) = \sum_{k=1}^{m} nc_k \binom{x}{k},$$

where $c_k, m \in \mathbb{Z}$.

Vanishing Polynomials Over $\mathbb{Z}_n$

Theorem (Borodin, Liu, Zhang, 2022)

If any term in the summation $\sum_{k=1}^{m} nc_k \binom{x}{k}$ has a non-integer coefficient then the resulting polynomial cannot have integer coefficients.

- $nc_k \binom{x}{k}$ has integer coefficients $\implies k! \mid nc_k$.
- The smallest such c_k is $k!/\gcd(n, k!)$ and any greater c_k would be a multiple of this, so any valid c_k can be written as $a_k \cdot (k!/\gcd(n, k!))$ for integer $0 \leq a_k < \gcd(n, k!)$ (any a_k outside this range is redundant in $\mathbb{Z}_n$).
- If we define s to be the smallest integer such that $n \mid s!$, any polynomial $n \cdot a_k \frac{k!}{\gcd(k!, n)} \binom{x}{k}$, where $k \geq s$, is a polynomial multiple of $\binom{x}{s}$.

Vanishing Polynomials Over $\mathbb{Z}_n$

- If we define s to be the smallest integer such that $n \mid s!$, any polynomial $n \cdot a_k \frac{k!}{\gcd(k!,n)} \binom{x}{k}$, where $k \geq s$, is a polynomial multiple of $\binom{x}{s}$.
- Therefore we have arrived at Singmaster's formulation, except with $B_k(x)$ written in the form $\binom{x}{k} \cdot k!$.

Theorem (Singmaster 1974)

Any element of the ideal of vanishing polynomials over $\mathbb{Z}_n$ is of the form

$$G(x) = F(x)B_s(x) + \sum_{k=0}^{s-1} a_k \cdot \frac{n}{\gcd(k!, n)} \cdot B_k(x)$$

where $B_k(x) = (x+1)(x+2)\ldots(x+k)$ with $B_0(x) = 1$, and s is the smallest integer such that $n \mid s!$. $F(x)$ is a polynomial which is uniquely defined based on $G(x)$, and a_k's are integers also uniquely defined in the range $0 \leq a_k < \gcd(k!, n)$.

Vanishing Polynomials Over $\mathbb{Z}_n$

Corollary

The generating set for the ideal of vanishing polynomials over $\mathbb{Z}_n$ is

$$\left\{ \frac{n}{\gcd(k!, n)} \cdot B_k(x) \mid k \in \mathbb{Z}_{\geq 0} \right\}$$

for either definition of $B_k(x)$.

- If k is less than the smallest prime divisor of n, the only element in the above set is the zero polynomial.
- We can immediately find the degree of the minimal degree monic vanishing polynomial and minimal degree non-monic vanishing polynomial, which would be s and the smallest prime factor of n, respectively.
- The minimal degree non-monic polynomial must be unique up to multiplication by a constant since the generating set only contains a single nonzero polynomial of that degree or lower.

Vanishing Polynomials Over $\mathbb{Z}_n$

Corollary

The generating set for the ideal of vanishing polynomials over $\mathbb{Z}_n$ is

$$\left\{ \frac{n}{\gcd(k!, n)} \cdot B_k(x) \mid k \in \mathbb{Z}_{\geq 0} \right\}$$

for either definition of $B_k(x)$.

- Many of the elements in the generating set are redundant.
- In particular, if we have two polynomials $a \cdot \binom{x}{i} \cdot i!$ and $a \cdot \binom{x}{j} \cdot j!$ for some integer a, and $i < j$ then the polynomial containing j is a polynomial multiple of the other and therefore redundant in a generating set.
- Therefore, in order to minimize our generating set we can remove any polynomials $(n/\gcd(k!, n))\binom{x}{k} \cdot k!$ for which k is not the minimal integer which gives the same value of $\gcd(k!, n)$.

Quotient Rings

Definition (Quotient)

A **quotient of a ring** R **by an ideal** I is a partitioning of the ring R into cosets of the form $r_1 + I$, $r_2 + I$, $r_3 + I$, $\ldots$, which form a ring under $(a + I) + (b + I) = ((a + b) + I)$ and $(a + I) \times (b + I) = ((a \times b) + I)$.

Quotient Rings

Example

$5\mathbb{Z}$ is the ideal generated by 5 consisting of all integer multiples of 5. The quotient $\mathbb{Z}/5\mathbb{Z}$ is summarized in the following table:

Representative	Coset
0	$0 + 5\mathbb{Z} = \{\dots, -5, 0, 5, 10, \dots\}$
1	$1 + 5\mathbb{Z} = \{\dots, -4, 1, 6, 11, \dots\}$
2	$2 + 5\mathbb{Z} = \{\dots, -3, 2, 7, 12, \dots\}$
3	$3 + 5\mathbb{Z} = \{\dots, -2, 3, 8, 13, \dots\}$
4	$4 + 5\mathbb{Z} = \{\dots, -1, 4, 9, 14, \dots\}$

Vanishing Polynomials Over General Rings

$(y) = \{ay : a \in R\}$, the ideal generated by y.

Definition

For a $y \in R$ such that $R/(y)$ is finite and creates the cosets $a_1 + (y), a_2 + (y), \ldots, a_k + (y)$ we define

$$F_y(x) = (x - a_1)(x - a_2)\ldots(x - a_k).$$

Lemma (Borodin, Liu, Zhang, 2022)

Given nonzero $y_1 y_2 = 0$, the polynomials

$$G(x) = y_2 F_{y_1}(x)$$

and

$$H(x) = F_{y_1}(x) F_{y_2}(x)$$

are vanishing.

Vanishing Polynomials Over General Rings

Theorem (Borodin, Liu, Zhang, 2022)

Given nonzero $y_1 y_2 \dots y_m = 0$ and an indexing set N such that if $i \in N$ then $R/(y_i)$ is finite and M containing all other indices the polynomial

$$H(x) = \prod_{j \in M} y_j \cdot \prod_{i \in N} F_{y_i}(x)$$

is vanishing.

Vanishing Polynomials Over General Rings

Note that we often get duplicate terms which can be removed.

Example

Over $\mathbb{Z}_{35}$, we get the vanishing polynomial

$$G(x) = (x)(x-1)(x-2)(x-3)(x-4) \cdot \\ (x)(x-1)(x-2)(x-3)(x-4)(x-5)(x-6)$$

which can be reduced to

$$G(x) = (x)(x-1)(x-2)(x-3)(x-4)(x-5)(x-6).$$

Vanishing Polynomials Over General Rings

Some duplicate terms cannot be removed.

Example

Consider the polynomial $(x)(x-1)\cdot(x)(x-1)$ over the ring $\mathbb{Z}_4$ using the zero divisors $2\cdot 2 = 0$. These duplicate terms cannot be removed since $(x)(x-1)$ is not vanishing over $\mathbb{Z}_4$.

Precise description of when terms can be removed is more complicated.

Vanishing Polynomials Over General Rings

This method allows us to find vanishing polynomials not only for finite rings but also for infinite ones.

Example

- Consider $R = \prod_{n=1}^{\infty} \mathbb{Z}_2$.
- $(0, 1, 1, 1, 1 \ldots) \cdot (1, 0, 0, 0, 0 \ldots) = 0$.
- $R/((0, 1, 1, 1, 1 \ldots)) \cong \mathbb{Z}_2$ so it is finite.
- $(1, 0, 0, 0, 0 \ldots)(x - (0, 0, 0, 0, 0 \ldots))(x - (1, 0, 0, 0, 0 \ldots))$ is vanishing.
- $(0, 0, 0, 0, 0 \ldots)$ and $(1, 0, 0, 0, 0 \ldots)$ can be replaced by any representatives from the corresponding cosets.

Vanishing Polynomials Over General Rings

Theorem (Borodin, Liu, Zhang, 2022)

If $R = \mathbb{Z}_n$, this description is sufficient to give a generating set of all vanishing polynomials if we take $y_1 \cdot \ldots \cdot y_k = n$ to be the prime factorization of n.

Proof sketch.

Number theoretic proof from before uses the fact that $x(x-1)(x-2)\ldots(x-k)$ is divisible by $\gcd(n, k!)$. Now we can instead use a product of $F_{y_i}(x)$'s where y_i's multiply to $\gcd(n, k!)$ to achieve the same result. Removing duplicates gives the desired degree. □

Vanishing Polynomials Over Product Rings

We now have a classification of vanishing polynomials for $\mathbb{Z}_n$.

- How to extend to more general rings?
- Extend to direct products of rings of integers modulo a number.

Definition (Direct Product)

The **direct product** $A \times B$ of rings A and B is the set of elements $(a, b)|a \in A, b \in B$ such that

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$

where $a_1 + a_2$ is the sum of a_1 and a_2 in A. Similarly,

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 \cdot a_2, b_1 \cdot b_2).$$

Vanishing Polynomials Over Product Rings

Example

Consider the two elements $a = (0, 1)$ and $b = (1, 0)$ in $\mathbb{Z}_2 \times \mathbb{Z}_2$. We have

$$a + b = (1, 1) \text{ and } ab = (0, 0).$$

Notice that $\mathbb{Z}_4$ is not the same as $\mathbb{Z}_2 \times \mathbb{Z}_2$: in $\mathbb{Z}_4$, the identity added to itself gives $1 + 1 = 2$, while in $\mathbb{Z}_2 \times \mathbb{Z}_2$ it gives $(1, 1) + (1, 1) = (0, 0)$, the zero element.

Vanishing Polynomials Over Product Rings

Besides extending above results, what can direct product be used for?

- Any finite ring can be decomposed into prime power order rings.
- Very small set of distinct prime power order rings for any given prime power.

Vanishing Polynomials Over Product Rings

Lemma (Well-known)

Let R be the direct product of k rings $R_1, \ldots, R_k$. Then, we have

$$R[x] \cong R_1[x] \times \cdots \times R_k[x].$$

Theorem (Borodin, Liu, Zhang, 2022)

Let R be the direct product of k rings $R_1, \ldots, R_k$. Then, the ring of polynomial functions on R has the same ring structure as the direct product of the rings of polynomial functions on $R_1, \ldots, R_k$.

Vanishing Polynomials Over Product Rings

Example

Consider $R = \mathbb{Z}_2 \times \mathbb{Z}_2$.
We can then express any element of $R[x]$ as an element of $\mathbb{Z}_2[x] \times \mathbb{Z}_2[x]$ and vice versa.

R[x]	$\mathbb{Z}_2[x] \times \mathbb{Z}_2[x]$
(1,0)x	(x,0)
$(1,0)x^4 + (0,1)x^3 + (1,1)x$	$(x^4 + x, x^3 + x)$
$(1,0)x^3 + (1,1)x^2 + (0,1)x$	$(x^3 + x^2, x^2 + x)$

Notice that all vanishing polynomials in $R[x]$ correspond to pairs of vanishing polynomials in $\mathbb{Z}_2[x] \times \mathbb{Z}_2[x]$.

Vanishing Polynomials Over Product Rings

Example

We now apply this theorem to find the set of polynomial functions over $\mathbb{Z}_2 \times \mathbb{Z}_2$.

(a,b)	0	1	x	x+1
0	(0,0)	(1,0)	(1,0)x	(1,0)x + (1,0)
1	(0,1)	(1,1)	(1,0)x + (0,1)	(1,0)x + (1,1)
x	(0,1)x	(0,1)x + (1,0)	(1,1)x	(1,1)x + (1,0)
x+1	(0,1)x + (0,1)	(0,1)x + (1,1)	(1,1)x + (0,1)	(1,1)x + (1,1)

The set of polynomial functions over $\mathbb{Z}_2 \times \mathbb{Z}_2$ is

$$
\begin{aligned}
&(0,0), (1,0), (0,1), (1,1),\\
&(1,0)x, (1,0)x + (1,0), (1,0)x + (0,1), (1,0)x + (1,1)\\
&(0,1)x, (0,1)x + (1,0), (0,1)x + (0,1), (0,1)x + (1,1)\\
&(1,1)x, (1,1)x + (1,0), (1,1)x + (0,1), (1,1)x + (1,1).
\end{aligned}
$$

Acknowledgements

We would like to express our sincere thanks to our mentor, Prof. Jim Coykendall for his continuous guidance and support throughout this project.

We would also like to thank Dr. Felix Gotti, Dr. Tanya Khovanova, and the rest of the MIT PRIMES program for making this project possible.

Finally, we would like to thank our parents, family, and friends for supporting us throughout our endeavors.

References

[1] Gert-Martin Greuel, Frank Seelisch, and Oliver Wienand. "The Gröbner basis of the ideal of vanishing polynomials". In: *Journal of Symbolic Computation* 46.5 (2011). Groebner Bases and Applications, pp. 561–570.

[2] Donald J. Newman. *A Problem Seminar*. Springer New York, 1982.

[3] Ivan Morton Niven and Leroy J. Warren. "A generalization of Fermat's theorem". In: 1957.

[4] David Singmaster. "On polynomial functions (mod m)". In: *Journal of Number Theory* 6.5 (1974), pp. 345–352.

[5] Ernst Specker, Norbert Hungerbühler, and Micha Wasem. "The Ring of Polyfunctions over $\mathbb{Z}/n\mathbb{Z}$". In: (2021).