Numbers of Strange Kind and Their Applications

Manindra Agrawal

IIT Kanpur

BII, Singapore 2007

Overview

Outline

1. Numbers
2. Essential Properties of Numbers
3. Numbers of Strange Kind: Finite Fields
4. Numbers of Stranger Kind: Extension Rings

Numbers

- 0, 1, -2, 6, $\frac{1}{2}$, 1.713, ...
- There are several types of numbers that we generally encounter.

NUMBERS

- 0, 1, -2, 6, $\frac{1}{2}$, 1.713, ...
- There are several types of numbers that we generally encounter.

Natural Numbers

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, \ldots$$

- Closed under addition and multiplication.
- Not closed under subtraction.

Natural Numbers

$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, \ldots$

- Closed under addition and multiplication.
- Not closed under subtraction.

Natural Numbers

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, \ldots$$

- Closed under addition and multiplication.
- Not closed under subtraction.

Integers

$$\ldots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \ldots$$

- Closed under subtraction also.
- Not closed under division.

Integers

$$\ldots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \ldots$$

- Closed under subtraction also.
- Not closed under division.

Integers

$$\ldots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \ldots$$

- Closed under subtraction also.
- Not closed under division.

Rational Numbers

All numbers of the form $\frac{a}{b}$ where a and b are integers and $b \neq 0$.

- Closed under division by non-zero numbers.
- Called a field.
- Does not contain $\pi = 3.1415\cdots$

Rational Numbers

All numbers of the form $\frac{a}{b}$ where a and b are integers and $b \neq 0$.

- Closed under division by non-zero numbers.
- Called a field.
- Does not contain $\pi = 3.1415\cdots$

Rational Numbers

All numbers of the form $\frac{a}{b}$ where a and b are integers and $b \neq 0$.

- Closed under division by non-zero numbers.
- Called a field.
- Does not contain $\pi = 3.1415\cdots$

Real Numbers

All numbers of the form $a.d_1d_2d_3d_4\cdots$ where a is an integer and d_1, d_2, d_3, d_4, $\ldots$ is a possibly infinite sequence of digits.

- Contains numbers such as π, golden ratio.
- Still closed under all the basic operations.

Real Numbers

All numbers of the form $a.d_1d_2d_3d_4\cdots$ where a is an integer and d_1, d_2, d_3, d_4, $\ldots$ is a possibly infinite sequence of digits.

- Contains numbers such as π, golden ratio.
- Still closed under all the basic operations.

Outline

Identifying Numbers

- Symbols used to represent numbers cannot always identify numbers:

$$0 + 2 = 1$$
$$1 * 3 = 4$$

- Different symbols may also represent numbers:

$$\spadesuit + \blacktriangle = \spadesuit$$
$$\bigstar + \blacktriangle = \bigstar$$
$$\spadesuit * \bigstar = \bigstar$$
$$\spadesuit * \blacktriangle = \blacktriangle$$

Identifying Numbers

- Symbols used to represent numbers cannot always identify numbers:

$$\begin{aligned} 0 + 2 &= 1 \\ 1 * 3 &= 4 \end{aligned}$$

- Different symbols may also represent numbers:

$$\begin{aligned} \spadesuit + \blacktriangle &= \spadesuit \\ \bigstar + \blacktriangle &= \bigstar \\ \spadesuit * \bigstar &= \bigstar \\ \spadesuit * \blacktriangle &= \blacktriangle \end{aligned}$$

Identifying Numbers

- "Addition" and "multiplication" operations are required for identifying numbers.
- With respect to these operations, numbers should satisfy certain properties.
- What properties should the numbers satisfy?
- It should be a minimal set of properties that are essential for our understanding of numbers.

Identifying Numbers

- "Addition" and "multiplication" operations are required for identifying numbers.
- With respect to these operations, numbers should satisfy certain properties.
- What properties should the numbers satisfy?
- It should be a minimal set of properties that are essential for our understanding of numbers.

Identifying Numbers

- "Addition" and "multiplication" operations are required for identifying numbers.
- With respect to these operations, numbers should satisfy certain properties.
- What properties should the numbers satisfy?
- It should be a minimal set of properties that are essential for our understanding of numbers.

Addition

- Numbers should be closed under addition.
- There should be an identity of addition, i.e., number 0: for every number a, $a + 0 = a$.
- It is useful to have negative numbers, i.e., for every number a there should be a number b such that $a + b = 0$.

Addition

- Numbers should be closed under addition.
- There should be an identity of addition, i.e., number 0: for every number a, $a + 0 = a$.
- It is useful to have negative numbers, i.e., for every number a there should be a number b such that $a + b = 0$.

Addition

- Numbers should be closed under addition.
- There should be an identity of addition, i.e., number 0: for every number a, $a + 0 = a$.
- It is useful to have negative numbers, i.e., for every number a there should be a number b such that $a + b = 0$.

Multiplication

- Numbers should be closed under multiplication.
- There should be an identity of multiplication, i.e., number 1: for every number a, $a * 1 = a$.
- It is useful to have closure under division, i.e., for every number a except 0, there should be a number b such that $a * b = 1$.
- Multiplication should distribute over addition, i.e., for every a, b and c, $a * (b + c) = a * b + a * c$.

Multiplication

- Numbers should be closed under multiplication.
- There should be an identity of multiplication, i.e., number 1: for every number a, $a * 1 = a$.
- It is useful to have closure under division, i.e., for every number a except 0, there should be a number b such that $a * b = 1$.
- Multiplication should distribute over addition, i.e., for every a, b and c, $a * (b + c) = a * b + a * c$.

Multiplication

- Numbers should be closed under multiplication.
- There should be an identity of multiplication, i.e., number 1: for every number a, $a * 1 = a$.
- It is useful to have closure under division, i.e., for every number a except 0, there should be a number b such that $a * b = 1$.
- Multiplication should distribute over addition, i.e., for every a, b and c, $a * (b + c) = a * b + a * c$.

Multiplication

- Numbers should be closed under multiplication.
- There should be an identity of multiplication, i.e., number 1: for every number a, $a * 1 = a$.
- It is useful to have closure under division, i.e., for every number a except 0, there should be a number b such that $a * b = 1$.
- Multiplication should distribute over addition, i.e., for every a, b and c, $a * (b + c) = a * b + a * c$.

Are There Other Kind of Numbers?

- If a set of "elements" admits two "operations" satisfying the above properties, these "elements" can be called numbers.
- And the two "operations" can be called addition and multiplication respectively.
- Do there exist such "elements" and "operations"?
- Even if they do, are they of any use?

Are There Other Kind of Numbers?

- If a set of "elements" admits two "operations" satisfying the above properties, these "elements" can be called numbers.
- And the two "operations" can be called addition and multiplication respectively.
- Do there exist such "elements" and "operations"?
- Even if they do, are they of any use?

Are There Other Kind of Numbers?

- If a set of "elements" admits two "operations" satisfying the above properties, these "elements" can be called numbers.
- And the two "operations" can be called addition and multiplication respectively.
- Do there exist such "elements" and "operations"?
- Even if they do, are they of any use?

Yes!

- There are many "strange" ways of defining numbers, addition and multiplication.
- Some of these strange numbers play a fundamental role in solving both practical and theoretical problems:
  - All the data stored in a CD/DVD is in the form of strange numbers.
  - A lot of properties of integers can be understood using strange numbers!

YES!

- There are many "strange" ways of defining numbers, addition and multiplication.
- Some of these strange numbers play a fundamental role in solving both practical and theoretical problems:
  - All the data stored in a CD/DVD is in the form of strange numbers.
  - A lot of properties of integers can be understood using strange numbers!

Yes!

- There are many "strange" ways of defining numbers, addition and multiplication.
- Some of these strange numbers play a fundamental role in solving both practical and theoretical problems:
  - All the data stored in a CD/DVD is in the form of strange numbers.
  - A lot of properties of integers can be understood using strange numbers!

YES!

- There are many "strange" ways of defining numbers, addition and multiplication.
- Some of these strange numbers play a fundamental role in solving both practical and theoretical problems:
  - All the data stored in a CD/DVD is in the form of strange numbers.
  - A lot of properties of integers can be understood using strange numbers!

Outline

Residues

- Fix r to be a positive integer, $r > 0$.
- Consider the set R_r of numbers $0, 1, \ldots, r-1$.
- Define addition operation $\oplus$ on these numbers as:

$$a \oplus b = a + b \; (mod \; r),$$

where $c \; (mod \; r)$ is the residue of c on division by r.

- Similarly, define multiplication operation $\otimes$ as:

$$a \otimes b = a * b \; (mod \; r).$$

- It is easily seen that these operations, on set R_r, satisfy all the required properties except closure under division.

Residues

- Fix r to be a positive integer, $r > 0$.
- Consider the set R_r of numbers 0, 1, $\ldots$, $r - 1$.
- Define addition operation $\oplus$ on these numbers as:

$$a \oplus b = a + b \ (mod\ r),$$

where $c\ (mod\ r)$ is the residue of c on division by r.

- Similarly, define multiplication operation $\otimes$ as:

$$a \otimes b = a * b \ (mod\ r).$$

- It is easily seen that these operations, on set R_r, satisfy all the required properties except closure under division.

Residues

- Fix r to be a positive integer, $r > 0$.
- Consider the set R_r of numbers $0, 1, \ldots, r-1$.
- Define addition operation $\oplus$ on these numbers as:

$$a \oplus b = a + b \ (mod\ r),$$

where $c \ (mod\ r)$ is the residue of c on division by r.

- Similarly, define multiplication operation $\otimes$ as:

$$a \otimes b = a * b \ (mod\ r).$$

- It is easily seen that these operations, on set R_r, satisfy all the required properties except closure under division.

RESIDUES

- Fix r to be a positive integer, $r > 0$.
- Consider the set R_r of numbers 0, 1, ..., $r - 1$.
- Define addition operation $\oplus$ on these numbers as:

$$a \oplus b = a + b \ (mod\ r),$$

  where $c \ (mod\ r)$ is the residue of c on division by r.
- Similarly, define multiplication operation $\otimes$ as:

$$a \otimes b = a * b \ (mod\ r).$$

- It is easily seen that these operations, on set R_r, satisfy all the required properties except closure under division.

Example: R_7

- $1 \oplus 6 = 0$, $5 \oplus 5 = 3$, $6 \oplus 3 = 2$ etc.
- $2 \otimes 6 = 5$, $5 \otimes 3 = 1$, $4 \otimes 4 = 2$ etc.
- $1 \oplus 6 = 0$, $2 \oplus 5 = 0$, $3 \oplus 4 = 0$; so "negative" numbers do exist!

Example: R_7

- $1 \oplus 6 = 0$, $5 \oplus 5 = 3$, $6 \oplus 3 = 2$ etc.
- $2 \otimes 6 = 5$, $5 \otimes 3 = 1$, $4 \otimes 4 = 2$ etc.
- $1 \oplus 6 = 0$, $2 \oplus 5 = 0$, $3 \oplus 4 = 0$; so "negative" numbers do exist!

Example: R_7

- $1 \oplus 6 = 0$, $5 \oplus 5 = 3$, $6 \oplus 3 = 2$ etc.
- $2 \otimes 6 = 5$, $5 \otimes 3 = 1$, $4 \otimes 4 = 2$ etc.
- $1 \oplus 6 = 0$, $2 \oplus 5 = 0$, $3 \oplus 4 = 0$; so "negative" numbers do exist!

Finite Fields

- Suppose r is a prime number.
- Then, closure under division also holds!!
- Why?
- Consider any non-zero number a from R_r.
- Consider $a \otimes 1$, $a \otimes 2$, ..., $a \otimes (r-1)$.
- None of the $a \otimes i$ is zero since $a \otimes i = a * i \ (mod\ r)$ and r is a prime greater than a and i.
- Therefore, $a \otimes i$ different for different i.
- Since there are $r-1$ numbers of the form $a \otimes i$ and $r-1$ non-zero numbers in R_r, there must be an i such that $a \otimes i = 1$.

Finite Fields

- Suppose r is a prime number.
- Then, closure under division also holds!!
- Why?
- Consider any non-zero number a from R_r.
- Consider $a \otimes 1$, $a \otimes 2$, ..., $a \otimes (r-1)$.
- None of the $a \otimes i$ is zero since $a \otimes i = a * i \ (mod\ r)$ and r is a prime greater than a and i.
- Therefore, $a \otimes i$ different for different i.
- Since there are $r-1$ numbers of the form $a \otimes i$ and $r-1$ non-zero numbers in R_r, there must be an i such that $a \otimes i = 1$.

Finite Fields

- Suppose r is a prime number.
- Then, closure under division also holds!!
- Why?
- Consider any non-zero number a from R_r.
- Consider $a \otimes 1$, $a \otimes 2$, $\ldots$, $a \otimes (r-1)$.
- None of the $a \otimes i$ is zero since $a \otimes i = a * i \ (mod\ r)$ and r is a prime greater than a and i.
- Therefore, $a \otimes i$ different for different i.
- Since there are $r-1$ numbers of the form $a \otimes i$ and $r-1$ non-zero numbers in R_r, there must be an i such that $a \otimes i = 1$.

Finite Fields

- Suppose r is a prime number.
- Then, closure under division also holds!!
- Why?
- Consider any non-zero number a from R_r.
- Consider $a \otimes 1$, $a \otimes 2$, $\ldots$, $a \otimes (r-1)$.
- None of the $a \otimes i$ is zero since $a \otimes i = a * i \ (mod\ r)$ and r is a prime greater than a and i.
- Therefore, $a \otimes i$ different for different i.
- Since there are $r-1$ numbers of the form $a \otimes i$ and $r-1$ non-zero numbers in R_r, there must be an i such that $a \otimes i = 1$.

EXAMPLE: R_7

- $1 \otimes 1 = 1$, $2 \otimes 4 = 1$, $3 \otimes 5 = 1$, $6 \otimes 6 = 1$.
- So closure under division holds: for example, $\frac{1}{6} = 6$.

Example: R_7

- $1 \otimes 1 = 1$, $2 \otimes 4 = 1$, $3 \otimes 5 = 1$, $6 \otimes 6 = 1$.
- So closure under division holds: for example, $\frac{1}{6} = 6$.

Finite Fields

- The set R_r for prime r is called a finite field.
- Finite fields are very useful.
- For example, in coding theory, finite fields are extensively used: Reed-Solomon codes are based on finite fields.
- These codes are used in storing data on a CD/DVD.

Finite Fields

- The set R_r for prime r is called a finite field.
- Finite fields are very useful.
- For example, in coding theory, finite fields are extensively used: Reed-Solomon codes are based on finite fields.
- These codes are used in storing data on a CD/DVD.

Finite Fields

- The set R_r for prime r is called a finite field.
- Finite fields are very useful.
- For example, in coding theory, finite fields are extensively used: Reed-Solomon codes are based on finite fields.
- These codes are used in storing data on a CD/DVD.

A Reed-Soloman Code

- Suppose input number is 245.
- Let $P(x) = 2x^2 \oplus 4x \oplus 5$ treating P as polynomial over R_7.
- We have $P(0) = 5$, $P(1) = 4$, $P(2) = 0$, $P(3) = 0$, $P(4) = 4$, $P(5) = 5$, and $P(6) = 3$.
- Code the number 245 as the number 5400453.

A Reed-Soloman Code

- Suppose input number is 245.
- Let $P(x) = 2x^2 \oplus 4x \oplus 5$ treating P as polynomial over R_7.
- We have $P(0) = 5$, $P(1) = 4$, $P(2) = 0$, $P(3) = 0$, $P(4) = 4$, $P(5) = 5$, and $P(6) = 3$.
- Code the number 245 as the number 5400453.

A Reed-Soloman Code

- Suppose input number is 245.
- Let $P(x) = 2x^2 \oplus 4x \oplus 5$ treating P as polynomial over R_7.
- We have $P(0) = 5$, $P(1) = 4$, $P(2) = 0$, $P(3) = 0$, $P(4) = 4$, $P(5) = 5$, and $P(6) = 3$.
- Code the number 245 as the number 5400453.

A Reed-Soloman Code

- Even if the number 5400453 gets corrupted in two digits, we can recover the number 245.
- For example, 245 can be recovered from 541056 or 240013.
- This is due to a property of polynomials over fields:

  If we start with any other number than 245 *and construct the code for that, then it will agree with the code for* 245 *at a maximum of two digits.*

- So a corrputed codeword will match the right codeword at 5 digits while it can match any wrong codeword at a maximum of 4 digits.

A Reed-Soloman Code

- Even if the number 5400453 gets corrupted in two digits, we can recover the number 245.
- For example, 245 can be recovered from 541056 or 240013.
- This is due to a property of polynomials over fields:

  If we start with any other number than 245 *and construct the code for that, then it will agree with the code for* 245 *at a maximum of two digits.*

- So a corrputed codeword will match the right codeword at 5 digits while it can match any wrong codeword at a maximum of 4 digits.

A Reed-Soloman Code

- Even if the number 5400453 gets corrupted in two digits, we can recover the number 245.
- For example, 245 can be recovered from 541056 or 240013.
- This is due to a property of polynomials over fields:

  If we start with any other number than 245 *and construct the code for that, then it will agree with the code for* 245 *at a maximum of two digits.*

- So a corrputed codeword will match the right codeword at 5 digits while it can match any wrong codeword at a maximum of 4 digits.

Finite Rings

- The set R_r for composite r is called a finite ring.
- These "numbers" are also very useful.
- For example, a fundamental problem in number theory is to find out if a given integer n is prime.
- To decide this, we study the properties of the finite ring R_n.

Finite Rings

- The set R_r for composite r is called a finite ring.
- These "numbers" are also very useful.
- For example, a fundamental problem in number theory is to find out if a given integer n is prime.
- To decide this, we study the properties of the finite ring R_n.

Finite Rings

- The set R_r for composite r is called a finite ring.
- These "numbers" are also very useful.
- For example, a fundamental problem in number theory is to find out if a given integer n is prime.
- To decide this, we study the properties of the finite ring R_n.

Outline

Polynomials Over Rings

- A polynomial in x over R_n is an expression of the form

$$a_d x^d \oplus a_{d-1} x^{d-1} \oplus \cdots \oplus a_1 x \oplus a_0$$

  where $a_i \in R_n$.
- x is a variable.
- d is the degree of the polynomial.
- We will use the notation

$$\sum_{i=0}^{d} a_i x^i$$

  to shorthand the polynomial.

Polynomials Over Rings

- A polynomial in x over R_n is an expression of the form

$$a_d x^d \oplus a_{d-1} x^{d-1} \oplus \cdots \oplus a_1 x \oplus a_0$$

  where $a_i \in R_n$.
- x is a variable.
- d is the degree of the polynomial.
- We will use the notation

$$\sum_{i=0}^{d} a_i x^i$$

  to shorthand the polynomial.

Finite Extension Rings

- Fix a degree d polynomial:

$$P = x^d \oplus a_{d-1}x^{d-1} \oplus \cdots \oplus a_1 x \oplus a_0.$$

- Let $R_{n,P}$ be the set of all polynomials in x over R_n of degree less than d.
- Define addition of elements of $R_{n,P}$ as:

$$\sum_{i=0}^{d-1} b_i x^i \oplus \sum_{i=0}^{d-1} c_i x^i = \sum_{i=0}^{d-1} (b_i \oplus c_i) x^i.$$

- Define multiplication of elements of $R_{n,P}$ as:

$$\sum_{i=0}^{d-1} b_i x^i \otimes \sum_{i=0}^{d-1} c_i x^i = \sum_{i=0}^{d-1} \sum_{j=0}^{d-1} (b_i \otimes c_j) x^{i+j}.$$

Finite Extension Rings

- Fix a degree d polynomial:

$$P = x^d \oplus a_{d-1}x^{d-1} \oplus \cdots \oplus a_1 x \oplus a_0.$$

- Let $R_{n,P}$ be the set of all polynomials in x over R_n of degree less than d.
- Define addition of elements of $R_{n,P}$ as:

$$\sum_{i=0}^{d-1} b_i x^i \oplus \sum_{i=0}^{d-1} c_i x^i = \sum_{i=0}^{d-1} (b_i \oplus c_i) x^i.$$

- Define multiplication of elements of $R_{n,P}$ as:

$$\sum_{i=0}^{d-1} b_i x^i \otimes \sum_{i=0}^{d-1} c_i x^i = \sum_{i=0}^{d-1} \sum_{j=0}^{d-1} (b_i \otimes c_j) x^{i+j}.$$

Finite Extension Rings

- Fix a degree d polynomial:

$$P = x^d \oplus a_{d-1}x^{d-1} \oplus \cdots \oplus a_1 x \oplus a_0.$$

- Let $R_{n,P}$ be the set of all polynomials in x over R_n of degree less than d.
- Define addition of elements of $R_{n,P}$ as:

$$\sum_{i=0}^{d-1} b_i x^i \oplus \sum_{i=0}^{d-1} c_i x^i = \sum_{i=0}^{d-1} (b_i \oplus c_i) x^i.$$

- Define multiplication of elements of $R_{n,P}$ as:

$$\sum_{i=0}^{d-1} b_i x^i \otimes \sum_{i=0}^{d-1} c_i x^i = \sum_{i=0}^{d-1} \sum_{j=0}^{d-1} (b_i \otimes c_j) x^{i+j}.$$

EXAMPLE: R_{7,x^3-1}

- The members of R_{7,x^3-1} are all degree zero, one, or two polynomials, a total of $7^3 = 343$ polynomials.
- $(2x^2 \oplus x) \oplus (5x^2 \oplus 3x \oplus 1) = 0x^2 \oplus 4x \oplus 1$.
- $(2x^2 \oplus x) \otimes (5x^2 \oplus 3x \oplus 1) = 3x^4 \oplus 6x^3 \oplus 2x^2 \oplus 5x^3 \oplus 3x^2 \oplus x = 3x^4 \oplus 4x^3 \oplus 5x^2 \oplus x$.
- The result is not an element of R_{7,x^3-1} since its degree is more than 2.

EXAMPLE: R_{7,x^3-1}

- The members of R_{7,x^3-1} are all degree zero, one, or two polynomials, a total of $7^3 = 343$ polynomials.
- $(2x^2 \oplus x) \oplus (5x^2 \oplus 3x \oplus 1) = 0x^2 \oplus 4x \oplus 1$.
- $(2x^2 \oplus x) \otimes (5x^2 \oplus 3x \oplus 1) = 3x^4 \oplus 6x^3 \oplus 2x^2 \oplus 5x^3 \oplus 3x^2 \oplus x = 3x^4 \oplus 4x^3 \oplus 5x^2 \oplus x$.
- The result is not an element of R_{7,x^3-1} since its degree is more than 2.

Example: R_{7,x^3-1}

- The members of R_{7,x^3-1} are all degree zero, one, or two polynomials, a total of $7^3 = 343$ polynomials.
- $(2x^2 \oplus x) \oplus (5x^2 \oplus 3x \oplus 1) = 0x^2 \oplus 4x \oplus 1$.
- $(2x^2 \oplus x) \otimes (5x^2 \oplus 3x \oplus 1) = 3x^4 \oplus 6x^3 \oplus 2x^2 \oplus 5x^3 \oplus 3x^2 \oplus x = 3x^4 \oplus 4x^3 \oplus 5x^2 \oplus x$.
- The result is not an element of R_{7,x^3-1} since its degree is more than 2.

Example: R_{7,x^3-1}

- The members of R_{7,x^3-1} are all degree zero, one, or two polynomials, a total of $7^3 = 343$ polynomials.
- $(2x^2 \oplus x) \oplus (5x^2 \oplus 3x \oplus 1) = 0x^2 \oplus 4x \oplus 1$.
- $(2x^2 \oplus x) \otimes (5x^2 \oplus 3x \oplus 1) = 3x^4 \oplus 6x^3 \oplus 2x^2 \oplus 5x^3 \oplus 3x^2 \oplus x = 3x^4 \oplus 4x^3 \oplus 5x^2 \oplus x$.
- The result is not an element of R_{7,x^3-1} since its degree is more than 2.

Finite Extension Rings

- To define multiplication correctly, we reduce the result by the polynomial P and take the remainder.
- For example, in R_{7,x^3-1} instead of

$$(2x^2 \oplus x) \otimes (5x^2 \oplus 3x \oplus 1) = 3x^4 \oplus 4x^3 \oplus 5x^2 \oplus x.$$

we define

$$(2x^2 \oplus x) \otimes (5x^2 \oplus 3x \oplus 1) = 3x \oplus 4 \oplus 5x^2 \oplus x = 5x^2 \oplus 4x \oplus 4.$$

- Now we can treat polynomials in $R_{n,P}$ as "numbers" with their addition and multiplication operations satisfying usual properties.
- $R_{n,P}$ is called a finite extension ring.

Finite Extension Rings

- To define multiplication correctly, we reduce the result by the polynomial P and take the remainder.
- For example, in R_{7,x^3-1} instead of

$$(2x^2 \oplus x) \otimes (5x^2 \oplus 3x \oplus 1) = 3x^4 \oplus 4x^3 \oplus 5x^2 \oplus x.$$

  we define

$$(2x^2 \oplus x) \otimes (5x^2 \oplus 3x \oplus 1) = 3x \oplus 4 \oplus 5x^2 \oplus x = 5x^2 \oplus 4x \oplus 4.$$

- Now we can treat polynomials in $R_{n,P}$ as "numbers" with their addition and multiplication operations satisfying usual properties.
- $R_{n,P}$ is called a finite extension ring.

Finite Extension Rings

- To define multiplication correctly, we reduce the result by the polynomial P and take the remainder.
- For example, in R_{7,x^3-1} instead of

$$(2x^2 \oplus x) \otimes (5x^2 \oplus 3x \oplus 1) = 3x^4 \oplus 4x^3 \oplus 5x^2 \oplus x.$$

  we define

$$(2x^2 \oplus x) \otimes (5x^2 \oplus 3x \oplus 1) = 3x \oplus 4 \oplus 5x^2 \oplus x = 5x^2 \oplus 4x \oplus 4.$$

- Now we can treat polynomials in $R_{n,P}$ as "numbers" with their addition and multiplication operations satisfying usual properties.
- $R_{n,P}$ is called a finite extension ring.

Finite Extension Rings

- To define multiplication correctly, we reduce the result by the polynomial P and take the remainder.
- For example, in R_{7,x^3-1} instead of

$$(2x^2 \oplus x) \otimes (5x^2 \oplus 3x \oplus 1) = 3x^4 \oplus 4x^3 \oplus 5x^2 \oplus x.$$

we define

$$(2x^2 \oplus x) \otimes (5x^2 \oplus 3x \oplus 1) = 3x \oplus 4 \oplus 5x^2 \oplus x = 5x^2 \oplus 4x \oplus 4.$$

- Now we can treat polynomials in $R_{n,P}$ as “numbers” with their addition and multiplication operations satisfying usual properties.
- $R_{n,P}$ is called a finite extension ring.

Primality Test Using Finite Extension Rings

- Given a number n, we wish to know if it is a prime number.
- The number n may be a very large number, say 200 digits long!
- Such large prime numbers are used extensively in cryptography.
- The trial division method will take a very long time on such numbers: about 10^{200} operations.
- Even on the fastest computers available, this will take more than the life of the universe!

Primality Test Using Finite Extension Rings

- Given a number n, we wish to know if it is a prime number.
- The number n may be a very large number, say 200 digits long!
- Such large prime numbers are used extensively in cryptography.
- The trial division method will take a very long time on such numbers: about 10^{200} operations.
- Even on the fastest computers available, this will take more than the life of the universe!

Primality Test Using Finite Extension Rings

- Given a number n, we wish to know if it is a prime number.
- The number n may be a very large number, say 200 digits long!
- Such large prime numbers are used extensively in cryptography.
- The trial division method will take a very long time on such numbers: about 10^{200} operations.
- Even on the fastest computers available, this will take more than the life of the universe!

Primality Test Using Finite Extension Rings

- To quickly decide if a given number n is prime, we study the finite extension ring R_{n,x^r-1}.
- It was shown by Pierre de Fermat in 17th century that if n is prime then

$$\underbrace{(x \oplus a) \otimes (x \oplus a) \otimes \cdots \otimes (x \oplus a)}_{n \text{ times}} = \underbrace{x \otimes x \otimes \cdots \otimes x}_{n \text{ times}} \oplus a$$

  for every a in R_n.
- This, however, cannot be used for quickly testing if n is prime since:
  - The property may be satisfied even if n is composite,
  - Checking if the property is satisfied is very time consuming as it requires checking for n different a's and n is large.

Primality Test Using Finite Extension Rings

- To quickly decide if a given number n is prime, we study the finite extension ring R_{n,x^r-1}.
- It was shown by Pierre de Fermat in 17th century that if n is prime then

$$\underbrace{(x \oplus a) \otimes (x \oplus a) \otimes \cdots \otimes (x \oplus a)}_{n \text{ times}} = \underbrace{x \otimes x \otimes \cdots \otimes x}_{n \text{ times}} \oplus a$$

  for every a in R_n.
- This, however, cannot be used for quickly testing if n is prime since:
  - The property may be satisfied even if n is composite,
  - Checking if the property is satisfied is very time consuming as it requires checking for n different a's and n is large.

Primality Test Using Finite Extension Rings

- To quickly decide if a given number n is prime, we study the finite extension ring R_{n,x^r-1}.
- It was shown by Pierre de Fermat in 17th century that if n is prime then

$$\underbrace{(x \oplus a) \otimes (x \oplus a) \otimes \cdots \otimes (x \oplus a)}_{n \text{ times}} = \underbrace{x \otimes x \otimes \cdots \otimes x}_{n \text{ times}} \oplus a$$

  for every a in R_n.
- This, however, cannot be used for quickly testing if n is prime since:
  - The property may be satisfied even if n is composite,
  - Checking if the property is satisfied is very time consuming as it requires checking for n different a's and n is large.

Primality Test Using Finite Extension Rings

- To quickly decide if a given number n is prime, we study the finite extension ring R_{n,x^r-1}.
- It was shown by Pierre de Fermat in 17th century that if n is prime then

$$\underbrace{(x \oplus a) \otimes (x \oplus a) \otimes \cdots \otimes (x \oplus a)}_{n \text{ times}} = \underbrace{x \otimes x \otimes \cdots \otimes x}_{n \text{ times}} \oplus a$$

  for every a in R_n.
- This, however, cannot be used for quickly testing if n is prime since:
  - The property may be satisfied even if n is composite,
  - Checking if the property is satisfied is very time consuming as it requires checking for n different a's and n is large.

Primality Test Using Finite Extension Rings

- To quickly decide if a given number n is prime, we study the finite extension ring R_{n,x^r-1}.
- It was shown by Pierre de Fermat in 17th century that if n is prime then

$$\underbrace{(x \oplus a) \otimes (x \oplus a) \otimes \cdots \otimes (x \oplus a)}_{n \text{ times}} = \underbrace{x \otimes x \otimes \cdots \otimes x}_{n \text{ times}} \oplus a$$

  for every a in R_n.
- This, however, cannot be used for quickly testing if n is prime since:
  - The property may be satisfied even if n is composite,
  - Checking if the property is satisfied is very time consuming as it requires checking for n different a's and n is large.

Primality Test Unsing Finite Extension Rings

- A few years ago, we showed that if we choose r carefully for R_{n,x^r-1} and if

$$\underbrace{(x \oplus a) \otimes (x \oplus a) \otimes \cdots \otimes (x \oplus a)}_{n \text{ times}} = \underbrace{x \otimes x \otimes \cdots \otimes x}_{n \text{ times}} \oplus a$$

  for only a few a's in R_n then n must be prime!
- This was the first fast method that guaranteed correctness.
- Earlier, there were fast methods that may go wrong occasionally.

Primality Test Unsing Finite Extension Rings

- A few years ago, we showed that if we choose r carefully for R_{n,x^r-1} and if

$$\underbrace{(x \oplus a) \otimes (x \oplus a) \otimes \cdots \otimes (x \oplus a)}_{n \text{ times}} = \underbrace{x \otimes x \otimes \cdots \otimes x}_{n \text{ times}} \oplus a$$

  for only a few a's in R_n then n must be prime!
- This was the first fast method that guaranteed correctness.
- Earlier, there were fast methods that may go wrong occasionally.

Remarks

- There are several other places where these strange numbers are useful.
- A general principle is:

  To understand the solutions of an equation defined over integers, study the solutions of the equation in R_p for primes p.

- Many problems have been solved using this principle including the famous Fermat's Last Theorem:

  There is no integer solution of the equation $x^n + y^n = z^n$ for $n \geq 3$.

Remarks

- There are several other places where these strange numbers are useful.
- A general principle is:

  To understand the solutions of an equation defined over integers, study the solutions of the equation in R_p for primes p.

- Many problems have been solved using this principle including the famous Fermat's Last Theorem:

  There is no integer solution of the equation $x^n + y^n = z^n$ for $n \geq 3$.

Remarks

- There are several other places where these strange numbers are useful.
- A general principle is:

  To understand the solutions of an equation defined over integers, study the solutions of the equation in R_p for primes p.

- Many problems have been solved using this principle including the famous Fermat's Last Theorem:

  There is no integer solution of the equation $x^n + y^n = z^n$ for $n \geq 3$.