The Binomial Theorem without middle terms: Putting prime numbers to work in algebra

Tom Marley

University of Nebraska-Lincoln

April 8, 2016

Rings!

RING

THEORY

Modular Arithmetic

Modular Arithmetic

Clock arithmetic:

Modular Arithmetic

Clock arithmetic:

- 8 (o'clock) + 5 (hours) = 1 (o'clock)

Modular Arithmetic

Clock arithmetic:

- 8 (o'clock) + 5 (hours) = 1 (o'clock)
- 8 (hours) + 5 (o'clock) = 1 (o'clock)

Modular Arithmetic

Clock arithmetic:

- 8 (o'clock) + 5 (hours) = 1 (o'clock)
- 8 (hours) + 5 (o'clock) = 1 (o'clock)

So in clock arithmetic, we can simply write:

$$8 + 5 = 1.$$

Modular Arithmetic

Clock arithmetic:

- 8 (o'clock) + 5 (hours) = 1 (o'clock)
- 8 (hours) + 5 (o'clock) = 1 (o'clock)

So in clock arithmetic, we can simply write:

$$8 + 5 = 1.$$

We can also subtract: $4 - 6 =$

Modular Arithmetic

Clock arithmetic:

- 8 (o'clock) + 5 (hours) = 1 (o'clock)
- 8 (hours) + 5 (o'clock) = 1 (o'clock)

So in clock arithmetic, we can simply write:

$$8 + 5 = 1.$$

We can also subtract: $4 - 6 = 10$.

Modular Arithmetic

Clock arithmetic:

- 8 (o'clock) + 5 (hours) = 1 (o'clock)
- 8 (hours) + 5 (o'clock) = 1 (o'clock)

So in clock arithmetic, we can simply write:

$$8 + 5 = 1.$$

We can also subtract: $4 - 6 = 10.$

As well as multiply: 4×7

Modular Arithmetic

Clock arithmetic:

- 8 (o'clock) + 5 (hours) = 1 (o'clock)
- 8 (hours) + 5 (o'clock) = 1 (o'clock)

So in clock arithmetic, we can simply write:

$$8 + 5 = 1.$$

We can also subtract: $4 - 6 = 10.$

As well as multiply: $4 \times 7 = 28$

Modular Arithmetic

Clock arithmetic:

- 8 (o'clock) + 5 (hours) = 1 (o'clock)
- 8 (hours) + 5 (o'clock) = 1 (o'clock)

So in clock arithmetic, we can simply write:

$$8 + 5 = 1.$$

We can also subtract: $4 - 6 = 10$.

As well as multiply: $4 \times 7 = 28 = 4$.

General rule:

Modular Arithmetic

Clock arithmetic:

- 8 (o'clock) + 5 (hours) = 1 (o'clock)
- 8 (hours) + 5 (o'clock) = 1 (o'clock)

So in clock arithmetic, we can simply write:

$$8 + 5 = 1.$$

We can also subtract: $4 - 6 = 10$.

As well as multiply: $4 \times 7 = 28 = 4$.

General rule:

Divide by 12 and take remainder.

The integers modulo n

We denote this number system by $\mathbb{Z}_{12}$, "the integers modulo 12".

The integers modulo n

We denote this number system by $\mathbb{Z}_{12}$, "the integers modulo 12". But there is nothing special about a clock with 12 hours.

The integers modulo n

We denote this number system by $\mathbb{Z}_{12}$, "the integers modulo 12".
But there is nothing special about a clock with 12 hours.
For example, a day on Neptune lasts about 16 hours.

The integers modulo n

We denote this number system by $\mathbb{Z}_{12}$, "the integers modulo 12".
But there is nothing special about a clock with 12 hours.
For example, a day on Neptune lasts about 16 hours.

We can do arithmetic in $\mathbb{Z}_{16}$ in the same way:

$$10 + 10 = 20$$

The integers modulo n

We denote this number system by $\mathbb{Z}_{12}$, "the integers modulo 12".
But there is nothing special about a clock with 12 hours.
For example, a day on Neptune lasts about 16 hours.

We can do arithmetic in $\mathbb{Z}_{16}$ in the same way:

$$10 + 10 = 20 = 4$$

The integers modulo n

We denote this number system by $\mathbb{Z}_{12}$, "the integers modulo 12".
But there is nothing special about a clock with 12 hours.
For example, a day on Neptune lasts about 16 hours.

We can do arithmetic in $\mathbb{Z}_{16}$ in the same way:

$$10 + 10 = 20 = 4$$

$$7 - 13 = -6$$

The integers modulo n

We denote this number system by $\mathbb{Z}_{12}$, "the integers modulo 12".
But there is nothing special about a clock with 12 hours.
For example, a day on Neptune lasts about 16 hours.

We can do arithmetic in $\mathbb{Z}_{16}$ in the same way:

$$10 + 10 = 20 = 4$$
$$7 - 13 = -6 = 10$$

The integers modulo n

We denote this number system by $\mathbb{Z}_{12}$, "the integers modulo 12".
But there is nothing special about a clock with 12 hours.
For example, a day on Neptune lasts about 16 hours.

We can do arithmetic in $\mathbb{Z}_{16}$ in the same way:

$$10 + 10 = 20 = 4$$
$$7 - 13 = -6 = 10$$
$$5 \times 7 = 35$$

The integers modulo n

We denote this number system by $\mathbb{Z}_{12}$, "the integers modulo 12".
But there is nothing special about a clock with 12 hours.
For example, a day on Neptune lasts about 16 hours.

We can do arithmetic in $\mathbb{Z}_{16}$ in the same way:

$$10 + 10 = 20 = 4$$
$$7 - 13 = -6 = 10$$
$$5 \times 7 = 35 = 3$$

Similarly for $\mathbb{Z}_n$ for any integer $n \geq 1$.

Ring axioms

In number systems like $\mathbb{Z}_n$, many of the familiar axioms from arithmetic hold: For example:

Ring axioms

In number systems like $\mathbb{Z}_n$, many of the familiar axioms from arithmetic hold: For example:

$$a + b = b + a \qquad \text{(commutativity of addition)}$$

Ring axioms

In number systems like $\mathbb{Z}_n$, many of the familiar axioms from arithmetic hold: For example:

$$a + b = b + a \qquad \text{(commutativity of addition)}$$

$$ab = ba \qquad \text{(commutative of multiplication)}$$

Ring axioms

In number systems like $\mathbb{Z}_n$, many of the familiar axioms from arithmetic hold: For example:

$$a + b = b + a \qquad \text{(commutativity of addition)}$$

$$ab = ba \qquad \text{(commutative of multiplication)}$$

$$a(b + c) = ab + ac \qquad \text{(distributive property)}$$

Ring axioms

In number systems like $\mathbb{Z}_n$, many of the familiar axioms from arithmetic hold: For example:

$$a + b = b + a \qquad \text{(commutativity of addition)}$$

$$ab = ba \qquad \text{(commutative of multiplication)}$$

$$a(b + c) = ab + ac \qquad \text{(distributive property)}$$

Ring axioms

In number systems like $\mathbb{Z}_n$, many of the familiar axioms from arithmetic hold: For example:

$$a + b = b + a \qquad \text{(commutativity of addition)}$$
$$ab = ba \qquad \text{(commutative of multiplication)}$$
$$a(b + c) = ab + ac \qquad \text{(distributive property)}$$

Number systems that satisfy these axioms (and a couple more) are called Rings.

Ring axioms

In number systems like $\mathbb{Z}_n$, many of the familiar axioms from arithmetic hold: For example:

$$a + b = b + a \qquad \text{(commutativity of addition)}$$
$$ab = ba \qquad \text{(commutative of multiplication)}$$
$$a(b + c) = ab + ac \qquad \text{(distributive property)}$$

Number systems that satisfy these axioms (and a couple more) are called Rings.

One can also subtract in rings, but not necessarily divide.

Ring axioms

In number systems like $\mathbb{Z}_n$, many of the familiar axioms from arithmetic hold: For example:

$$a + b = b + a \qquad \text{(commutativity of addition)}$$
$$ab = ba \qquad \text{(commutative of multiplication)}$$
$$a(b + c) = ab + ac \qquad \text{(distributive property)}$$

Number systems that satisfy these axioms (and a couple more) are called Rings.

One can also subtract in rings, but not necessarily divide.
For example, in $\mathbb{Z}_{12}$ we have: $6 \times 3 = 6 \times 9$.

Ring axioms

In number systems like $\mathbb{Z}_n$, many of the familiar axioms from arithmetic hold: For example:

$$a + b = b + a \qquad \text{(commutativity of addition)}$$
$$ab = ba \qquad \text{(commutative of multiplication)}$$
$$a(b + c) = ab + ac \qquad \text{(distributive property)}$$

Number systems that satisfy these axioms (and a couple more) are called Rings.

One can also subtract in rings, but not necessarily divide.
For example, in $\mathbb{Z}_{12}$ we have: $6 \times 3 = 6 \times 9$.
However: $3 \neq 9$ in $\mathbb{Z}_{12}$.

Polynomial and power series rings

There are many examples of rings out there in addition to $\mathbb{Z}_n$:

Polynomial and power series rings

There are many examples of rings out there in addition to $\mathbb{Z}_n$:

- $\mathbb{Z}$ (the integers)
- $\mathbb{R}$ (the real numbers)
- $\mathbb{C}$ (the complex numbers)

Polynomial and power series rings

There are many examples of rings out there in addition to $\mathbb{Z}_n$:

- $\mathbb{Z}$ (the integers)
- $\mathbb{R}$ (the real numbers)
- $\mathbb{C}$ (the complex numbers)

It's easy to create new rings from old. One way is to consider all polynomials in a variable x with coefficients from a given ring R:

$$R[x] := \{a_0 + a_1 x + \cdots + a_n x^n \mid a_i \in R \ \forall \ i, \ n \geq 0\}.$$

Polynomial and power series rings

There are many examples of rings out there in addition to $\mathbb{Z}_n$:

- $\mathbb{Z}$ (the integers)
- $\mathbb{R}$ (the real numbers)
- $\mathbb{C}$ (the complex numbers)

It's easy to create new rings from old. One way is to consider all polynomials in a variable x with coefficients from a given ring R:

$$R[x] := \{a_0 + a_1 x + \cdots + a_n x^n \mid a_i \in R \ \forall \ i, \ n \geq 0\}.$$

We can also consider all power series in x with coefficients from R:

$$R[[x]] := \{\sum_{i=0}^{\infty} a_i x^i \mid a_i \in R \ \forall \ i\}.$$

Polynomials and power series (cont.)

We can iterate these processes:

- $R[x, y] := (R[x])[y]$
- $R[x, y, z] := (R[x, y])[z]$
- $R[[x, y]] := (R[[x]])[[y]]$

Polynomials and power series (cont.)

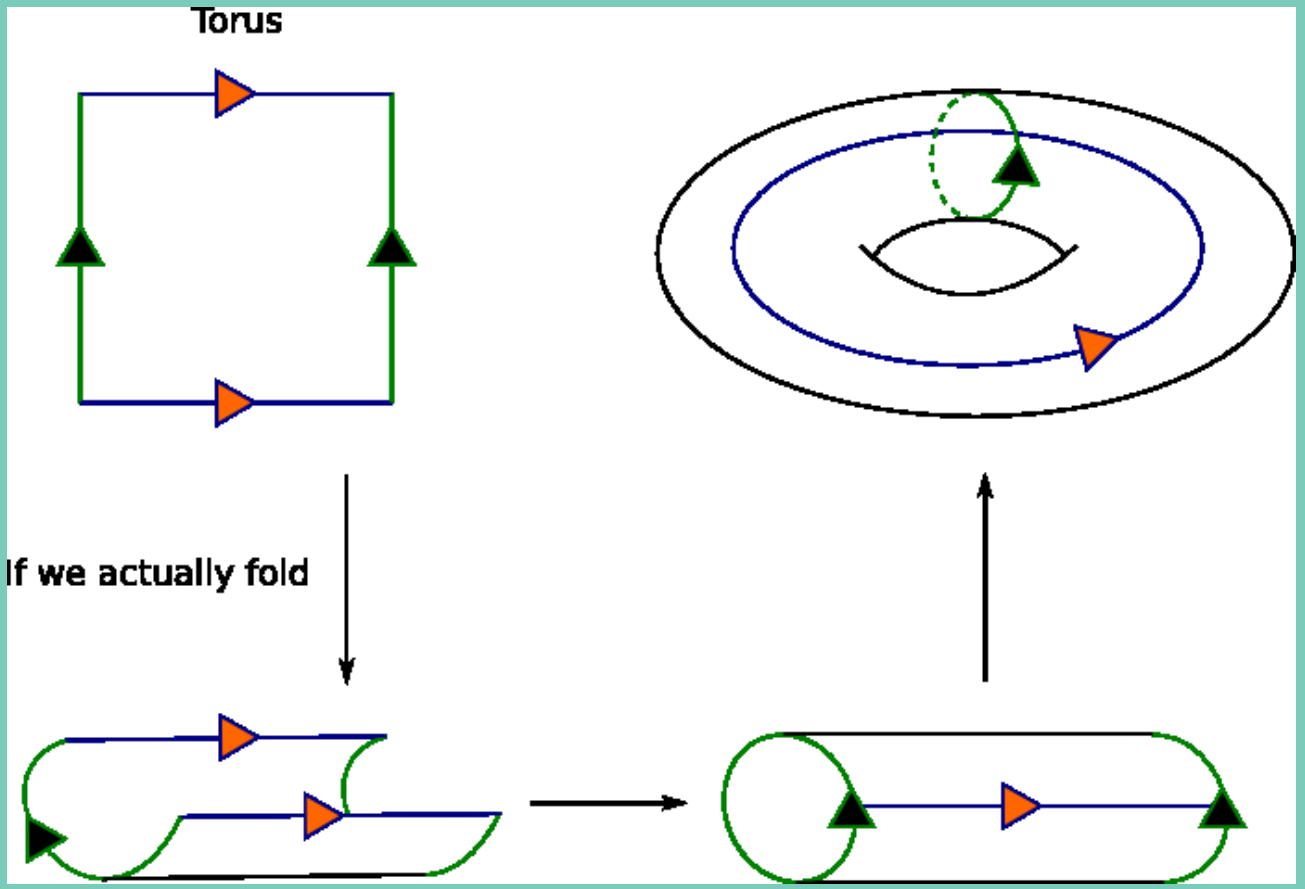
We can iterate these processes:

- $R[x, y] := (R[x])[y]$
- $R[x, y, z] := (R[x, y])[z]$
- $R[[x, y]] := (R[[x]])[[y]]$

For example, in $\mathbb{Z}[[x, y]]$, we have:

$$(1 - xy) \cdot (1 + xy + x^2y^2 + \cdots + x^iy^i + \cdots) = 1.$$

Quotient spaces



Quotient rings

Given a ring R and elements $f, g \in R$, we can form a quotient ring from R by identifying f and g; or equivalently, by identifying $h = f - g$ and 0. We write this quotient ring as $R/(h)$.

Quotient rings

Given a ring R and elements $f, g \in R$, we can form a quotient ring from R by identifying f and g; or equivalently, by identifying $h = f - g$ and 0. We write this quotient ring as $R/(h)$.

More generally, given $f_1, \ldots, f_n \in R$, the quotient ring obtained by identifying $f_1 = 0, \ldots, f_n = 0$ is written:

$$R/(f_1, \ldots, f_n).$$

Quotient rings

Given a ring R and elements $f, g \in R$, we can form a quotient ring from R by identifying f and g; or equivalently, by identifying $h = f - g$ and 0. We write this quotient ring as $R/(h)$.

More generally, given $f_1, \ldots, f_n \in R$, the quotient ring obtained by identifying $f_1 = 0, \ldots, f_n = 0$ is written:

$$R/(f_1, \ldots, f_n).$$

For example: $\mathbb{Z}/(n) \cong$

Quotient rings

Given a ring R and elements $f, g \in R$, we can form a quotient ring from R by identifying f and g; or equivalently, by identifying $h = f - g$ and 0. We write this quotient ring as $R/(h)$.

More generally, given $f_1, \ldots, f_n \in R$, the quotient ring obtained by identifying $f_1 = 0, \ldots, f_n = 0$ is written:

$$R/(f_1, \ldots, f_n).$$

For example: $\mathbb{Z}/(n) \cong \mathbb{Z}_n$

Quotient rings

Given a ring R and elements $f, g \in R$, we can form a quotient ring from R by identifying f and g; or equivalently, by identifying $h = f - g$ and 0. We write this quotient ring as $R/(h)$.

More generally, given $f_1, \ldots, f_n \in R$, the quotient ring obtained by identifying $f_1 = 0, \ldots, f_n = 0$ is written:

$$R/(f_1, \ldots, f_n).$$

For example: $\mathbb{Z}/(n) \cong \mathbb{Z}_n$ and $\mathbb{R}[x]/(x^2 + 1) \cong$

Quotient rings

Given a ring R and elements $f, g \in R$, we can form a quotient ring from R by identifying f and g; or equivalently, by identifying $h = f - g$ and 0. We write this quotient ring as $R/(h)$.

More generally, given $f_1, \ldots, f_n \in R$, the quotient ring obtained by identifying $f_1 = 0, \ldots, f_n = 0$ is written:

$$R/(f_1, \ldots, f_n).$$

For example: $\mathbb{Z}/(n) \cong \mathbb{Z}_n$ and $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$.

Quotient rings

Given a ring R and elements $f, g \in R$, we can form a quotient ring from R by identifying f and g; or equivalently, by identifying $h = f - g$ and 0. We write this quotient ring as $R/(h)$.

More generally, given $f_1, \ldots, f_n \in R$, the quotient ring obtained by identifying $f_1 = 0, \ldots, f_n = 0$ is written:

$$R/(f_1, \ldots, f_n).$$

For example: $\mathbb{Z}/(n) \cong \mathbb{Z}_n$ and $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$.

To invert an element $a \in R$, just consider the ring:

$$R[x]/(ax - 1).$$

What are rings good for?

What are rings good for?

They're *precious*!

What are rings good for?

They're *precious*!

Applications of ring theory:

What are rings good for?

They're *precious*!

Applications of ring theory:

- Cryptography

What are rings good for?

They're *precious*!

Applications of ring theory:

- Cryptography
- Error-correcting codes

What are rings good for?

They're *precious*!

Applications of ring theory:

- Cryptography
- Error-correcting codes
- 3D animation

What are rings good for?

They're *precious*!

Applications of ring theory:

- Cryptography
- Error-correcting codes
- 3D animation
- Communication networks

What are rings good for?

They're *precious*!

Applications of ring theory:

- Cryptography
- Error-correcting codes
- 3D animation
- Communication networks
- Number theory, algebraic geometry, invariant theory

The Binomial Theorem

Let p be a (positive) prime integer. For the remainder of this talk, we'll restrict our attention to rings of the form

$$R = \mathbb{Z}_p[[x_1, \ldots, x_n]]/(f_1, \ldots, f_r).$$

The Binomial Theorem

Let p be a (positive) prime integer. For the remainder of this talk, we'll restrict our attention to rings of the form

$$R = \mathbb{Z}_p[[x_1, \ldots, x_n]]/(f_1, \ldots, f_r).$$

Consider the Binomial Theorem in such rings:

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^{p-i} b^i$$

The Binomial Theorem

Let p be a (positive) prime integer. For the remainder of this talk, we'll restrict our attention to rings of the form

$$R = \mathbb{Z}_p[[x_1, \ldots, x_n]]/(f_1, \ldots, f_r).$$

Consider the Binomial Theorem in such rings:

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^{p-i} b^i$$

$$= a^p + pa^{p-1}b + \frac{p(p-1)}{2} a^{p-2}b^2 + \frac{p(p-1)((p-2)}{6} a^{p-3}b^3 +$$

The Binomial Theorem

Let p be a (positive) prime integer. For the remainder of this talk, we'll restrict our attention to rings of the form

$$R = \mathbb{Z}_p[[x_1, \ldots, x_n]]/(f_1, \ldots, f_r).$$

Consider the Binomial Theorem in such rings:

$$\begin{aligned}(a+b)^p &= \sum_{i=0}^{p} \binom{p}{i} a^{p-i} b^i \\ &= a^p + pa^{p-1}b + \frac{p(p-1)}{2} a^{p-2}b^2 + \frac{p(p-1)((p-2)}{6} a^{p-3}b^3 + \\ &= a^p + b^p\end{aligned}$$

Fermat's (Little) Theorem

Fermat's Theorem

Let p be a prime. Then $a^p = a$ for any $a \in \mathbb{Z}_p$.

Fermat's (Little) Theorem

Fermat's Theorem

Let p be a prime. Then $a^p = a$ for any $a \in \mathbb{Z}_p$.

Proof

The theorem clearly holds when $a = 0$ and $a = 1$. Suppose $a^p = a$ for some $a \in \mathbb{Z}_p$.

Fermat's (Little) Theorem

Fermat's Theorem

Let p be a prime. Then $a^p = a$ for any $a \in \mathbb{Z}_p$.

Proof

The theorem clearly holds when $a = 0$ and $a = 1$. Suppose $a^p = a$ for some $a \in \mathbb{Z}_p$. Then

$$(a+1)^p = a^p + 1^p$$

Fermat's (Little) Theorem

Fermat's Theorem

Let p be a prime. Then $a^p = a$ for any $a \in \mathbb{Z}_p$.

Proof

The theorem clearly holds when $a = 0$ and $a = 1$. Suppose $a^p = a$ for some $a \in \mathbb{Z}_p$. Then

$$\begin{aligned}(a+1)^p &= a^p + 1^p \\ &= a + 1.\end{aligned}$$

A special subring

Key Observation

The set

$$R^p := \{a^p \mid a \in R\}$$

is a subring of R.

A special subring

Key Observation

The set

$$R^p := \{a^p \mid a \in R\}$$

is a subring of R.

Proof

First observe $0 = 0^p$ and $1 = 1^p$, so $0, 1 \in R^p$.

A special subring

Key Observation

The set

$$R^p := \{a^p \mid a \in R\}$$

is a subring of R.

Proof

First observe $0 = 0^p$ and $1 = 1^p$, so $0, 1 \in R^p$. Now let $a^p, b^p \in R^p$. Then $a^p + b^p = (a+b)^p \in R^p$ and $a^p b^p = (ab)^p \in R^p$.

A special subring

Key Observation

The set

$$R^p := \{a^p \mid a \in R\}$$

is a subring of R.

Proof

First observe $0 = 0^p$ and $1 = 1^p$, so $0, 1 \in R^p$. Now let $a^p, b^p \in R^p$. Then $a^p + b^p = (a+b)^p \in R^p$ and $a^p b^p = (ab)^p \in R^p$. Finally, $-(a^p) = (-a)^p \in R^p$.

A special subring

Key Observation

The set

$$R^p := \{a^p \mid a \in R\}$$

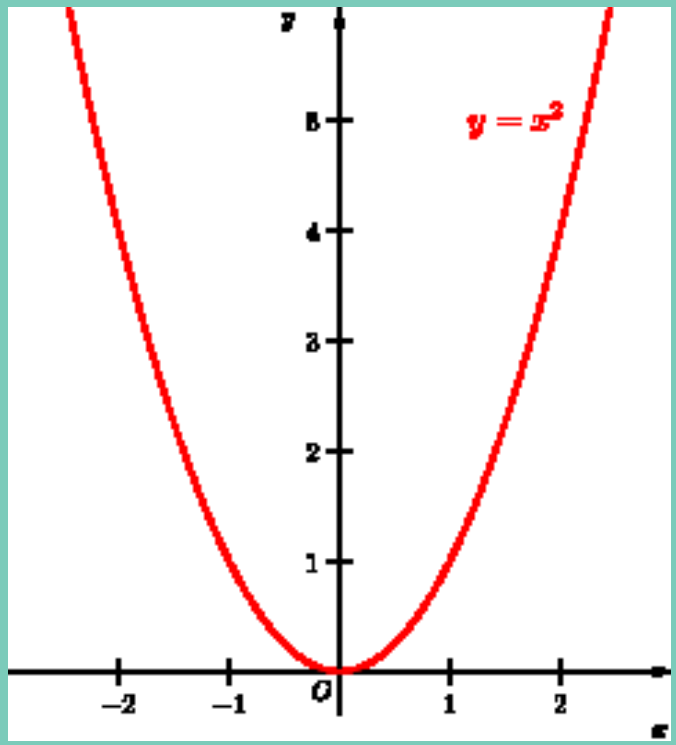
is a subring of R.

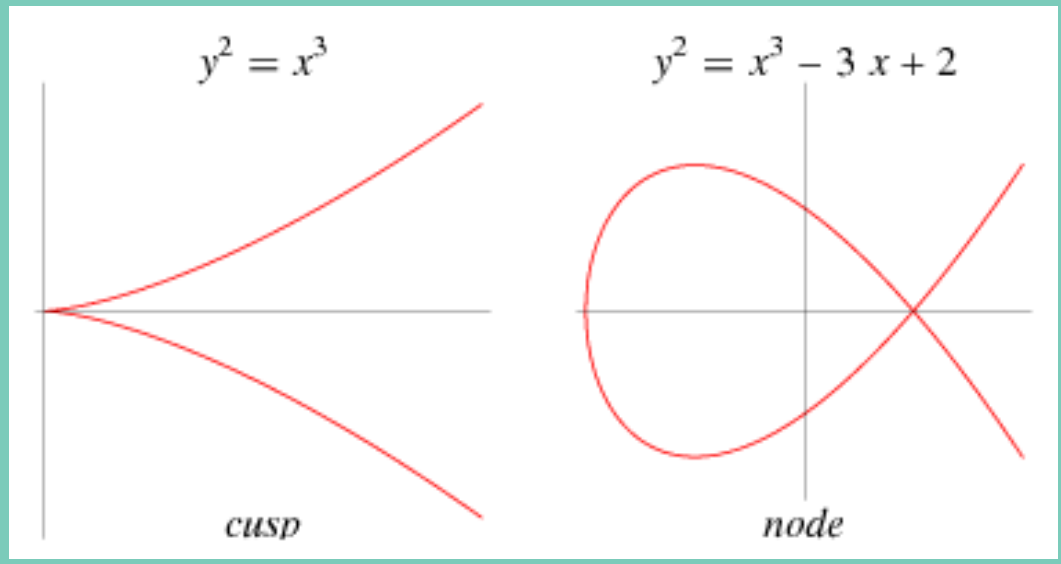
Proof

First observe $0 = 0^p$ and $1 = 1^p$, so $0, 1 \in R^p$. Now let $a^p, b^p \in R^p$. Then $a^p + b^p = (a+b)^p \in R^p$ and $a^p b^p = (ab)^p \in R^p$. Finally, $-(a^p) = (-a)^p \in R^p$.

The relationship between the ring R and the subring R^p provides important clues about the structure of R.

Curve singularities





Coordinate rings

For the parabola:

$$\mathbb{R}[[x, y]]/(y - x^2) \cong \mathbb{R}[[x, x^2]]$$

Coordinate rings

For the parabola:

$$\begin{aligned}\mathbb{R}[[x,y]]/(y-x^2) &\cong \mathbb{R}[[x,x^2]] \\ &\cong \mathbb{R}[[x]].\end{aligned}$$

Coordinate rings

For the parabola:

$$\begin{aligned}\mathbb{R}[[x,y]]/(y-x^2) &\cong \mathbb{R}[[x,x^2]] \\ &\cong \mathbb{R}[[x]].\end{aligned}$$

For the cusp: $\mathbb{R}[[x,y]]/(y^2-x^3) \cong \mathbb{R}[[t^2,t^3]]$.

Coordinate rings

For the parabola:

$$\begin{aligned}\mathbb{R}[[x,y]]/(y-x^2) &\cong \mathbb{R}[[x,x^2]] \\ &\cong \mathbb{R}[[x]].\end{aligned}$$

For the cusp: $\mathbb{R}[[x,y]]/(y^2-x^3) \cong \mathbb{R}[[t^2,t^3]]$.

For the node:

$$\mathbb{R}[[x,y]]/(y^2-x^3-x^2) \cong \mathbb{R}[[x,y]]/(y^2-x^2(x+1))$$

Coordinate rings

For the parabola:

$$\begin{aligned}\mathbb{R}[[x,y]]/(y-x^2) &\cong \mathbb{R}[[x,x^2]] \\ &\cong \mathbb{R}[[x]].\end{aligned}$$

For the cusp: $\mathbb{R}[[x,y]]/(y^2-x^3) \cong \mathbb{R}[[t^2,t^3]]$.

For the node:

$$\begin{aligned}\mathbb{R}[[x,y]]/(y^2-x^3-x^2) &\cong \mathbb{R}[[x,y]]/(y^2-x^2(x+1)) \\ &\cong \mathbb{R}[[x,y]]/((y-cx)(y+cx)).\end{aligned}$$

where $c=\sqrt{x+1}=1+\frac{1}{2}x-\frac{1}{8}x^2+\cdots$.

Smoothness

Definition

Let $f(x, y) = 0$ define a curve C. We say C is smooth or nonsingular at the origin if its coordinate ring $k[[x, y]]/(f)$ is isomorphic to a polynomial ring in one variable. Otherwise, C is singular at the origin.

Smoothness

Definition

Let $f(x, y) = 0$ define a curve C. We say C is smooth or nonsingular at the origin if its coordinate ring $k[[x, y]]/(f)$ is isomorphic to a polynomial ring in one variable. Otherwise, C is singular at the origin.

Remark

If $k = \mathbb{R}$ then C is smooth at $(0, 0)$ if and only if $\frac{\partial f}{\partial x}$ and $\frac{\partial f}{\partial y}$ don't both vanish at the origin. That is, C is smooth at $(0, 0)$ if and only if there is a unique well-defined tangent line to C at the origin.

An illustrative example

Question

Given a ring $R = \mathbb{Z}_p[[x_1, \ldots, x_d]]/(f_1, \ldots, f_r)$, how can we decide if R is smooth at the origin? That is, how can we tell if $R \cong \mathbb{Z}_p[[y_1, \ldots, y_s]]$?

An illustrative example

Question

Given a ring $R = \mathbb{Z}_p[[x_1, \ldots, x_d]]/(f_1, \ldots, f_r)$, how can we decide if R is smooth at the origin? That is, how can we tell if $R \cong \mathbb{Z}_p[[y_1, \ldots, y_s]]$?

Consider $R = \mathbb{Z}_p[[x]]$.

An illustrative example

Question

Given a ring $R = \mathbb{Z}_p[[x_1, \ldots, x_d]]/(f_1, \ldots, f_r)$, how can we decide if R is smooth at the origin? That is, how can we tell if $R \cong \mathbb{Z}_p[[y_1, \ldots, y_s]]$?

Consider $R = \mathbb{Z}_p[[x]]$. Then $R^p = \mathbb{Z}_p[[x^p]]$.

An illustrative example

Question

Given a ring $R = \mathbb{Z}_p[[x_1, \ldots, x_d]]/(f_1, \ldots, f_r)$, how can we decide if R is smooth at the origin? That is, how can we tell if $R \cong \mathbb{Z}_p[[y_1, \ldots, y_s]]$?

Consider $R = \mathbb{Z}_p[[x]]$. Then $R^p = \mathbb{Z}_p[[x^p]]$.

Note that every element in $f \in R$ can be written uniquely in the form:

$$f = c_0 + c_1 x + c_2 x^2 + \cdots + c_{p-1} x^{p-1}$$

for some $c_0, \ldots, c_{p-1} \in R^p$.

An illustrative example

Question

Given a ring $R = \mathbb{Z}_p[[x_1, \ldots, x_d]]/(f_1, \ldots, f_r)$, how can we decide if R is smooth at the origin? That is, how can we tell if $R \cong \mathbb{Z}_p[[y_1, \ldots, y_s]]$?

Consider $R = \mathbb{Z}_p[[x]]$. Then $R^p = \mathbb{Z}_p[[x^p]]$.

Note that every element in $f \in R$ can be written uniquely in the form:

$$f = c_0 + c_1 x + c_2 x^2 + \cdots + c_{p-1} x^{p-1}$$

for some $c_0, \ldots, c_{p-1} \in R^p$.

For example, let $p = 3$ and $f = 2 + x + 2x^3 + x^4 + 2x^5 + x^7$.

An illustrative example

Question

Given a ring $R = \mathbb{Z}_p[[x_1, \ldots, x_d]]/(f_1, \ldots, f_r)$, how can we decide if R is smooth at the origin? That is, how can we tell if $R \cong \mathbb{Z}_p[[y_1, \ldots, y_s]]$?

Consider $R = \mathbb{Z}_p[[x]]$. Then $R^p = \mathbb{Z}_p[[x^p]]$.

Note that every element in $f \in R$ can be written uniquely in the form:

$$f = c_0 + c_1 x + c_2 x^2 + \cdots + c_{p-1} x^{p-1}$$

for some $c_0, \ldots, c_{p-1} \in R^p$.

For example, let $p = 3$ and $f = 2 + x + 2x^3 + x^4 + 2x^5 + x^7$. Then

$$f = (2 + 2x^3) \cdot 1 + (1 + x^3 + x^6)x + (2x^3)x^2.$$

An illustrative example, cont.

Thus $R = \mathbb{Z}_p[[x]]$ has a basis over $R^p = \mathbb{Z}_p[[x^p]]$. Namely,

$$\{1, x, x^2, \ldots, x^{p-1}\}.$$

An illustrative example, cont.

Thus $R = \mathbb{Z}_p[[x]]$ has a basis over $R^p = \mathbb{Z}_p[[x^p]]$. Namely,

$$\{1, x, x^2, \ldots, x^{p-1}\}.$$

The same holds for $R = \mathbb{Z}_p[[x_1, \ldots, x_d]]$.

An illustrative example, cont.

Thus $R = \mathbb{Z}_p[[x]]$ has a basis over $R^p = \mathbb{Z}_p[[x^p]]$. Namely,

$$\{1, x, x^2, \ldots, x^{p-1}\}.$$

The same holds for $R = \mathbb{Z}_p[[x_1, \ldots, x_d]]$.

Now consider the coordinate ring of the cusp over $\mathbb{Z}_2$:
$R = \mathbb{Z}_2[[x, y]]/(y^2 - x^3) \cong \mathbb{Z}_2[[t^2, t^3]]$.

An illustrative example, cont.

Thus $R = \mathbb{Z}_p[[x]]$ has a basis over $R^p = \mathbb{Z}_p[[x^p]]$. Namely,

$$\{1, x, x^2, \ldots, x^{p-1}\}.$$

The same holds for $R = \mathbb{Z}_p[[x_1, \ldots, x_d]]$.

Now consider the coordinate ring of the cusp over $\mathbb{Z}_2$:
$R = \mathbb{Z}_2[[x, y]]/(y^2 - x^3) \cong \mathbb{Z}_2[[t^2, t^3]]$.
Then

$$R^2 \cong \mathbb{Z}_2[[t^4, t^6]].$$

An illustrative example, cont.

Thus $R = \mathbb{Z}_p[[x]]$ has a basis over $R^p = \mathbb{Z}_p[[x^p]]$. Namely,

$$\{1, x, x^2, \ldots, x^{p-1}\}.$$

The same holds for $R = \mathbb{Z}_p[[x_1, \ldots, x_d]]$.

Now consider the coordinate ring of the cusp over $\mathbb{Z}_2$:
$R = \mathbb{Z}_2[[x, y]]/(y^2 - x^3) \cong \mathbb{Z}_2[[t^2, t^3]]$.
Then

$$R^2 \cong \mathbb{Z}_2[[t^4, t^6]].$$

Does R have a basis over R^2?

An illustrative example, cont.

Thus $R = \mathbb{Z}_p[[x]]$ has a basis over $R^p = \mathbb{Z}_p[[x^p]]$. Namely,

$$\{1, x, x^2, \ldots, x^{p-1}\}.$$

The same holds for $R = \mathbb{Z}_p[[x_1, \ldots, x_d]]$.

Now consider the coordinate ring of the cusp over $\mathbb{Z}_2$:
$R = \mathbb{Z}_2[[x, y]]/(y^2 - x^3) \cong \mathbb{Z}_2[[t^2, t^3]]$.
Then

$$R^2 \cong \mathbb{Z}_2[[t^4, t^6]].$$

Does R have a basis over R^2? No!

An illustrative example, cont.

Thus $R = \mathbb{Z}_p[[x]]$ has a basis over $R^p = \mathbb{Z}_p[[x^p]]$. Namely,

$$\{1, x, x^2, \ldots, x^{p-1}\}.$$

The same holds for $R = \mathbb{Z}_p[[x_1, \ldots, x_d]]$.

Now consider the coordinate ring of the cusp over $\mathbb{Z}_2$:
$R = \mathbb{Z}_2[[x, y]]/(y^2 - x^3) \cong \mathbb{Z}_2[[t^2, t^3]]$.
Then

$$R^2 \cong \mathbb{Z}_2[[t^4, t^6]].$$

Does R have a basis over R^2? No!

Suppose $\{1, t^2\}$ is part of the basis.

An illustrative example, cont.

Thus $R = \mathbb{Z}_p[[x]]$ has a basis over $R^p = \mathbb{Z}_p[[x^p]]$. Namely,

$$\{1, x, x^2, \ldots, x^{p-1}\}.$$

The same holds for $R = \mathbb{Z}_p[[x_1, \ldots, x_d]]$.

Now consider the coordinate ring of the cusp over $\mathbb{Z}_2$:
$R = \mathbb{Z}_2[[x, y]]/(y^2 - x^3) \cong \mathbb{Z}_2[[t^2, t^3]]$.
Then

$$R^2 \cong \mathbb{Z}_2[[t^4, t^6]].$$

Does R have a basis over R^2? No!

Suppose $\{1, t^2\}$ is part of the basis. Then

$$t^6 \cdot 1 + t^4 \cdot t^2 = 0.$$

Kunz's Theorem

Theorem (Ernst Kunz, 1969)

R has a basis over R^p if and only if $R \cong \mathbb{Z}_p[[x_1, \ldots, x_r]]$.

Kunz's Theorem

Theorem (Ernst Kunz, 1969)

R has a basis over R^p if and only if $R \cong \mathbb{Z}_p[[x_1, \ldots, x_r]]$.

That is, a curve, surface, solid, etc. over $\mathbb{Z}_p$ is smooth at the origin if and only if its coordinate ring R has a basis over R^p.

Kunz's Theorem

Theorem (Ernst Kunz, 1969)

R has a basis over R^p if and only if $R \cong \mathbb{Z}_p[[x_1, \ldots, x_r]]$.

That is, a curve, surface, solid, etc. over $\mathbb{Z}_p$ is smooth at the origin if and only if its coordinate ring R has a basis over R^p.

Kunz's Theorem is in some sense the very beginning of the story of the study of singularities over $\mathbb{Z}_p$. This continues to be a very active area of research today.

Kunz's Theorem

Theorem (Ernst Kunz, 1969)

R has a basis over R^p if and only if $R \cong \mathbb{Z}_p[[x_1, \ldots, x_r]]$.

That is, a curve, surface, solid, etc. over $\mathbb{Z}_p$ is smooth at the origin if and only if its coordinate ring R has a basis over R^p.

Kunz's Theorem is in some sense the very beginning of the story of the study of singularities over $\mathbb{Z}_p$. This continues to be a very active area of research today.

Theorem (Avramov-Hochster-Iyengar-Yao, 2012)

If there exists any nonzero R-module which has a finite basis over R^p then $R \cong \mathbb{Z}_p[[x_1, \ldots, x_r]]$.

Thank you!

Thank you!