What Can Logic Do For You?

G. Eric Moorhouse

Department of Mathematics
University of Wyoming

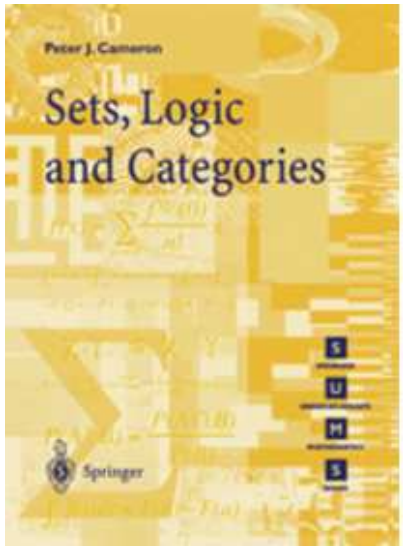
UD Seminar—6 April 2012

Useful Tools from Logic

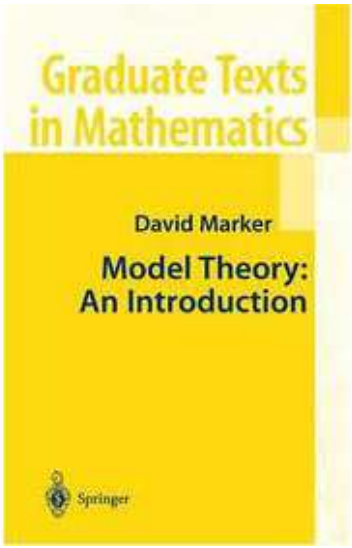
Some of the tools from mathematical logic which enjoy applications in algebra, combinatorics and number theory are

- the Compactness Theorem
- Transfinite Induction (or the Axiom of Choice, or Zorn's Lemma)
- Ultraproduct Constructions
- Back-and-Forth Constructions
- Fraïssé Limits
- Order Indiscernibles

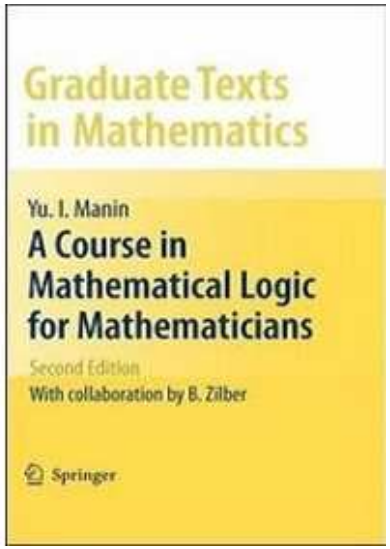
General References



P. J. Cameron



D. Marker



Y. I. Manin

Ax-Grothendieck Theorem

A map $f : \mathbb{C}^n \to \mathbb{C}^n$ is *polynomial* if

$$f(z_1, \ldots, z_n) = (f_1(z_1, \ldots, z_n), \ldots, f_n(z_1, \ldots, z_n))$$

where each $f_j(z_1, \ldots, z_n) \in \mathbb{C}[z_1, \ldots, z_n]$, i.e. each f_j is a multivariate polynomial.

Theorem (Ax (1968), Grothendieck (1966))

Let $f : \mathbb{C}^n \to \mathbb{C}^n$ be a polynomial map. If f is one-to-one, then f is onto.

James Ax
(1937-2006)

Alexander
Grothendieck
(1928-)

Ax-Grothendieck Theorem

A map $f : \mathbb{C}^n \to \mathbb{C}^n$ is *polynomial* if

$$f(z_1, \ldots, z_n) = (f_1(z_1, \ldots, z_n), \ldots, f_n(z_1, \ldots, z_n))$$

where each $f_j(z_1, \ldots, z_n) \in \mathbb{C}[z_1, \ldots, z_n]$, i.e. each f_j is a multivariate polynomial.

Theorem (Ax (1968), Grothendieck (1966))

Let $f : \mathbb{C}^n \to \mathbb{C}^n$ be a polynomial map. If f is one-to-one, then f is onto.

James Ax
(1937-2006)

Alexander
Grothendieck
(1928-)

Ax-Grothendieck Theorem

Theorem (Ax (1968), Grothendieck (1966))

Let $f : \mathbb{C}^n \to \mathbb{C}^n$ be a polynomial map. If f is one-to-one, then f is onto.

Ax's original proof uses the Compactness Theorem of first-order logic to reduce this to the case of polynomial maps $f : \mathbb{F}_q \to \mathbb{F}_q$ where the result is obvious.

Borel also gave a topological proof (1969). Rudin's analytic proof (1995) is less pretty, but avoids model theory.

Serre discussed these proofs in *How to Use Finite Fields for Problems Concerning Infinite Fields* (2009).

Ax-Grothendieck Theorem

Theorem (Ax (1968), Grothendieck (1966))

Let $f : \mathbb{C}^n \to \mathbb{C}^n$ be a polynomial map. If f is one-to-one, then f is onto.

Ax's original proof uses the Compactness Theorem of first-order logic to reduce this to the case of polynomial maps $f : \mathbb{F}_q \to \mathbb{F}_q$ where the result is obvious.

Borel also gave a topological proof (1969). Rudin's analytic proof (1995) is less pretty, but avoids model theory.

Serre discussed these proofs in *How to Use Finite Fields for Problems Concerning Infinite Fields* (2009).

Ax-Grothendieck Theorem

Theorem (Ax (1968), Grothendieck (1966))

Let $f : \mathbb{C}^n \to \mathbb{C}^n$ be a polynomial map. If f is one-to-one, then f is onto.

Ax's original proof uses the Compactness Theorem of first-order logic to reduce this to the case of polynomial maps $f : \mathbb{F}_q \to \mathbb{F}_q$ where the result is obvious.

Borel also gave a topological proof (1969). Rudin's analytic proof (1995) is less pretty, but avoids model theory.

Serre discussed these proofs in *How to Use Finite Fields for Problems Concerning Infinite Fields* (2009).

The Lefschetz Principle: Another Example

Theorem

Consider a linear system

$$(*) \qquad Ax = b$$

where $A \in \mathbb{Z}^{m \times n}$ *and* $b \in \mathbb{Z}^m$. *Then one of the following two possibilities holds:*

(i) *For all but finitely many primes p, the system (*) has a solution* $x \in \mathbb{F}_p^n$. *In this case, (*) has a solution* $x \in \mathbb{Q}^n$. *OR*

(ii) *For at most finitely many primes p, the system (*) has a solution* $x \in \mathbb{F}_p^n$. *In this case, (*) has no solution* $x \in \mathbb{Q}^n$.

It is not possible that (*) has solutions for infinitely many primes, *and* is insoluble for infinitely many primes.

The most elementary proof uses the theory of Smith Normal Forms. A short, elegant proof can be given using the Compactness Theorem.

The Lefschetz Principle: Another Example

Theorem

Consider a linear system

$$(*) \qquad Ax = b$$

where $A \in \mathbb{Z}^{m \times n}$ *and* $b \in \mathbb{Z}^m$. *Then one of the following two possibilities holds:*

(i) *For all but finitely many primes p, the system (*) has a solution* $x \in \mathbb{F}_p^n$. *In this case, (*) has a solution* $x \in \mathbb{Q}^n$. *OR*

(ii) *For at most finitely many primes p, the system (*) has a solution* $x \in \mathbb{F}_p^n$. *In this case, (*) has no solution* $x \in \mathbb{Q}^n$.

It is not possible that (*) has solutions for infinitely many primes, *and* is insoluble for infinitely many primes.

The most elementary proof uses the theory of Smith Normal Forms. A short, elegant proof can be given using the Compactness Theorem.

The Compactness Theorem of First-Order Logic

Compactness Theorem

Let Σ be a set of sentences in a first-order language L. If every finite subset $\Sigma_0 \subseteq \Sigma$ is satisfiable (i.e. has a model), then Σ is satisfiable.

Example

Let L be the language of ordered rings, with constant symbols '0','1','ε'; symbols '$+$','$\times$' denoting binary operations; the symbol '$-$' denoting a unary operation; and the symbol '$<$' denoting a binary relation. Let Σ be the infinite set consisting of

- the axioms for an ordered field; and
- for every $n \geq 1$, an axiom $0 < \underbrace{\varepsilon + \varepsilon + \cdots + \varepsilon}_{n \text{ times}} < 1$.

Every finite subset of Σ is satisfiable in $\mathbb{Q}$ or in $\mathbb{R}$; so there exist infinite ordered fields containing infinitesimals.

The Compactness Theorem of First-Order Logic

Compactness Theorem

Let Σ be a set of sentences in a first-order language L. If every finite subset $\Sigma_0 \subseteq \Sigma$ is satisfiable (i.e. has a model), then Σ is satisfiable.

Example

Let L be the language of ordered rings, with constant symbols '0','1','ε'; symbols '$+$','$\times$' denoting binary operations; the symbol '$-$' denoting a unary operation; and the symbol '$<$' denoting a binary relation. Let Σ be the infinite set consisting of

- the axioms for an ordered field; and
- for every $n \geq 1$, an axiom $0 < \underbrace{\varepsilon + \varepsilon + \cdots + \varepsilon}_{n \text{ times}} < 1$.

Every finite subset of Σ is satisfiable in $\mathbb{Q}$ or in $\mathbb{R}$; so there exist infinite ordered fields containing infinitesimals.

Ramsey's Theorem

Theorem (Finite Version)

Let $k, m, r \geq 1$. There exists $N = N(k, m, r)$ such that for every set X with $|X| \geq N$ and every k-colouring of the r-subsets of X, there is an m-subset of X, all of whose r-subsets have the same colour.

Theorem (Infinite Version)

Let $k, r \geq 1$. For every k-colouring of the r-subsets of $\mathbb{N}$, there is an infinite subset $A \subseteq \mathbb{N}$, all of whose r-subsets have the same colour.

The infinite version implies the finite one, by a compactness argument. And the infinite version is easier to state, and to prove, than the finite version.

Ramsey's Theorem

Theorem (Finite Version)

Let $k, m, r \geq 1$. There exists $N = N(k, m, r)$ such that for every set X with $|X| \geq N$ and every k-colouring of the r-subsets of X, there is an m-subset of X, all of whose r-subsets have the same colour.

Theorem (Infinite Version)

Let $k, r \geq 1$. For every k-colouring of the r-subsets of $\mathbb{N}$, there is an infinite subset $A \subseteq \mathbb{N}$, all of whose r-subsets have the same colour.

The infinite version implies the finite one, by a compactness argument. And the infinite version is easier to state, and to prove, than the finite version.

Ramsey's Theorem

Theorem (Finite Version)

Let $k, m, r \geq 1$. There exists $N = N(k, m, r)$ such that for every set X with $|X| \geq N$ and every k-colouring of the r-subsets of X, there is an m-subset of X, all of whose r-subsets have the same colour.

Theorem (Infinite Version)

Let $k, r \geq 1$. For every k-colouring of the r-subsets of $\mathbb{N}$, there is an infinite subset $A \subseteq \mathbb{N}$, all of whose r-subsets have the same colour.

The infinite version implies the finite one, by a compactness argument. And the infinite version is easier to state, and to prove, than the finite version.

Chromatic Numbers of Infinite Graphs

A *proper colouring* of a graph Γ is a colouring of the vertices such that no two adjacent vertices bear the same colour.

The *chromatic number* $\chi(\Gamma)$ is the minimum number of colours used in any proper colouring of the vertices of Γ.

Another application of the Compactness Theorem:

Theorem

Let $k \geq 1$, and let Γ be an infinite graph. If $\chi(\Gamma_0) \leq k$ for every finite subgraph $\Gamma_0 \subset \Gamma$, then $\chi(\Gamma) \leq k$.

Chromatic Numbers of Infinite Graphs

A *proper colouring* of a graph Γ is a colouring of the vertices such that no two adjacent vertices bear the same colour.

The *chromatic number* $\chi(\Gamma)$ is the minimum number of colours used in any proper colouring of the vertices of Γ.

Another application of the Compactness Theorem:

Theorem

Let $k \geq 1$, and let Γ be an infinite graph. If $\chi(\Gamma_0) \leq k$ for every finite subgraph $\Gamma_0 \subset \Gamma$, then $\chi(\Gamma) \leq k$.

Philosophical Considerations

Proofs by model-theoretic methods are sometimes shorter or more natural than alternative proofs obtained by other means.

Concern may be expressed over the liberal use of the axiom of choice (AC) in model theory. But often, proofs obtained by these methods can be rewritten so as to obtain more ‘constructive’ proofs not requiring AC.

The model-theoretic language often serves as a convenience rather than as a necessity. Its use is similar to proofs in discrete mathematics that appeal to $\mathbb{R}$ or to $\mathbb{C}$, where typically a finite extension of $\mathbb{Q}$ suffices.

Philosophical Considerations

Proofs by model-theoretic methods are sometimes shorter or more natural than alternative proofs obtained by other means.

Concern may be expressed over the liberal use of the axiom of choice (AC) in model theory. But often, proofs obtained by these methods can be rewritten so as to obtain more 'constructive' proofs not requiring AC.

The model-theoretic language often serves as a convenience rather than as a necessity. Its use is similar to proofs in discrete mathematics that appeal to $\mathbb{R}$ or to $\mathbb{C}$, where typically a finite extension of $\mathbb{Q}$ suffices.

Philosophical Considerations

Proofs by model-theoretic methods are sometimes shorter or more natural than alternative proofs obtained by other means.

Concern may be expressed over the liberal use of the axiom of choice (AC) in model theory. But often, proofs obtained by these methods can be rewritten so as to obtain more 'constructive' proofs not requiring AC.

The model-theoretic language often serves as a convenience rather than as a necessity. Its use is similar to proofs in discrete mathematics that appeal to $\mathbb{R}$ or to $\mathbb{C}$, where typically a finite extension of $\mathbb{Q}$ suffices.

Ultraproducts

Let M_α (for $\alpha \in A$) be models of some set of formulas Σ. (Think of Σ as a set of axioms satisfied by every M_α.) We take the index set A to be infinite; the models M_α need not be distinct.

The *ultraproduct construction* (details omitted) gives

$$M = \left(\prod_\alpha M_\alpha\right) \Big/ \text{ultrafilter}$$

which is also a model of Σ, often with many new and interesting properties.

An ultraproduct of infinitely many copies of $\mathbb{R}$ gives the field of *hyperreal numbers*, an ordered field containing finite, infinite and infinitesimal elements.

An ultraproduct of $\mathbb{F}_p$ (as p ranges over the primes) gives a field $\mathbb{F}$ of characteristic zero, but having a unique extension of degree k for each $k \geq 1$.

Ultraproducts

Let M_α (for $\alpha \in A$) be models of some set of formulas Σ. (Think of Σ as a set of axioms satisfied by every M_α.) We take the index set A to be infinite; the models M_α need not be distinct.

The *ultraproduct construction* (details omitted) gives

$$M = \left(\prod_\alpha M_\alpha\right) \Big/ \text{ultrafilter}$$

which is also a model of Σ, often with many new and interesting properties.

An ultraproduct of infinitely many copies of $\mathbb{R}$ gives the field of *hyperreal numbers*, an ordered field containing finite, infinite and infinitesimal elements.

An ultraproduct of $\mathbb{F}_p$ (as p ranges over the primes) gives a field $\mathbb{F}$ of characteristic zero, but having a unique extension of degree k for each $k \geq 1$.

Ultraproducts

Let M_α (for $\alpha \in A$) be models of some set of formulas Σ. (Think of Σ as a set of axioms satisfied by every M_α.) We take the index set A to be infinite; the models M_α need not be distinct.

The *ultraproduct construction* (details omitted) gives

$$M = \left(\prod_\alpha M_\alpha\right) \Big/ \text{ultrafilter}$$

which is also a model of Σ, often with many new and interesting properties.

An ultraproduct of infinitely many copies of $\mathbb{R}$ gives the field of *hyperreal numbers*, an ordered field containing finite, infinite and infinitesimal elements.

An ultraproduct of $\mathbb{F}_p$ (as p ranges over the primes) gives a field $\mathbb{F}$ of characteristic zero, but having a unique extension of degree k for each $k \geq 1$.

Ultraproducts

Let M_α (for $\alpha \in A$) be models of some set of formulas Σ. (Think of Σ as a set of axioms satisfied by every M_α.) We take the index set A to be infinite; the models M_α need not be distinct.

The *ultraproduct construction* (details omitted) gives

$$M = \left(\prod_\alpha M_\alpha\right) \Big/ \text{ultrafilter}$$

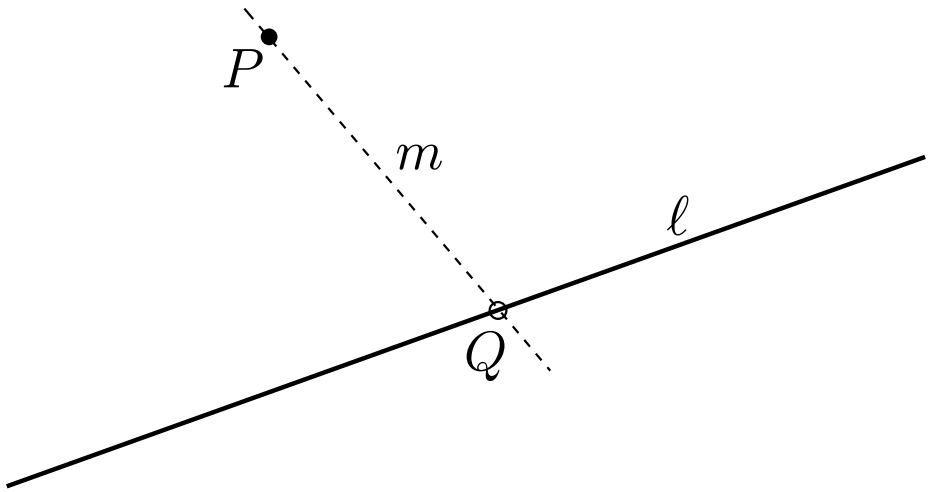
which is also a model of Σ, often with many new and interesting properties.

An ultraproduct of infinitely many copies of $\mathbb{R}$ gives the field of *hyperreal numbers*, an ordered field containing finite, infinite and infinitesimal elements.

An ultraproduct of $\mathbb{F}_p$ (as p ranges over the primes) gives a field $\mathbb{F}$ of characteristic zero, but having a unique extension of degree k for each $k \geq 1$.

Generalized Quadrangles

A *generalized quadrangle* (GQ) is a point-line incidence structure in which every non-incident point-line pair (P, ℓ) has exactly one line through P meeting ℓ:



We assume every point is on more than two lines; and every line has more than 2 points.

Semifinite Generalized Quadrangles

We say the GQ is *semifinite* if it has infinitely many points and lines, but the number of points on each line (always the same number) is finite. (*Open question: Can this happen?*)

There is no semifinite GQ with line size 3 (Cameron, 1981 . . . one paragraph).

There is no semifinite GQ with line size 4 (Brouwer, 1991 . . . three pages).

There is no semifinite GQ with line size 5 (Cherlin, 2005 . . . seven pages of model theory).

Nothing is known for line size ≥ 6. Experts differ on whether semifinite GQ's may exist at all.

Semifinite Generalized Quadrangles

We say the GQ is *semifinite* if it has infinitely many points and lines, but the number of points on each line (always the same number) is finite. (*Open question: Can this happen?*)

There is no semifinite GQ with line size 3 (Cameron, 1981 . . . one paragraph).

There is no semifinite GQ with line size 4 (Brouwer, 1991 . . . three pages).

There is no semifinite GQ with line size 5 (Cherlin, 2005 . . . seven pages of model theory).

Nothing is known for line size ≥ 6. Experts differ on whether semifinite GQ's may exist at all.

Semifinite Generalized Quadrangles

We say the GQ is *semifinite* if it has infinitely many points and lines, but the number of points on each line (always the same number) is finite. (*Open question: Can this happen?*)

There is no semifinite GQ with line size 3 (Cameron, 1981 . . . one paragraph).

There is no semifinite GQ with line size 4 (Brouwer, 1991 . . . three pages).

There is no semifinite GQ with line size 5 (Cherlin, 2005 . . . seven pages of model theory).

Nothing is known for line size ≥ 6. Experts differ on whether semifinite GQ's may exist at all.

Semifinite Generalized Quadrangles

We say the GQ is *semifinite* if it has infinitely many points and lines, but the number of points on each line (always the same number) is finite. (*Open question: Can this happen?*)

There is no semifinite GQ with line size 3 (Cameron, 1981 . . . one paragraph).

There is no semifinite GQ with line size 4 (Brouwer, 1991 . . . three pages).

There is no semifinite GQ with line size 5 (Cherlin, 2005 . . . seven pages of model theory).

Nothing is known for line size ≥ 6. Experts differ on whether semifinite GQ's may exist at all.

Semifinite Generalized Quadrangles

We say the GQ is *semifinite* if it has infinitely many points and lines, but the number of points on each line (always the same number) is finite. (*Open question: Can this happen?*)

There is no semifinite GQ with line size 3 (Cameron, 1981 . . . one paragraph).

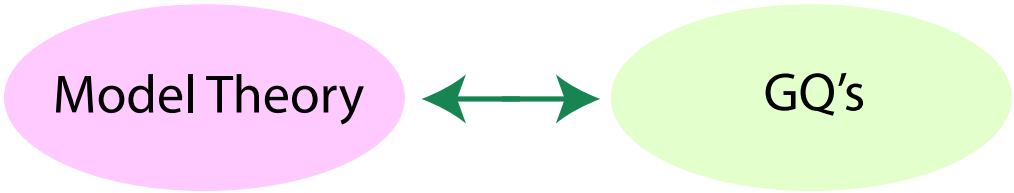
There is no semifinite GQ with line size 4 (Brouwer, 1991 . . . three pages).

There is no semifinite GQ with line size 5 (Cherlin, 2005 . . . seven pages of model theory).

Nothing is known for line size ≥ 6. Experts differ on whether semifinite GQ's may exist at all.

GQ's and Model Theory

Cherlin applied techniques of model theory to the study of GQ's.



However, the study of GQ's is also applied to model theory. GQ's arise in the investigation of the Cherlin-Zil'ber Conjecture, one of the leading open problems in model theory.

Geometric Proofs by Transfinite Induction

Consider the affine 3-space $F^3 = \{(x, y, z) : x, y, z \in F\}$ over a field F. It is easy to partition the points of F^3 into lines (e.g. using all lines parallel to a given line). The following is trickier:

Theorem

If the field F is infinite, then $F^3 \setminus \{(0, 0, 0)\}$ can be partitioned into lines.

This is not hard to prove by transfinite induction. The result fails for a finite field $|F| = q$ since $q^3 - 1$ is not divisible by the line size q.

I have used similar arguments for other geometric partition problems, e.g. partitioning all but one point of a quadratic cone into conics.

Geometric Proofs by Transfinite Induction

Consider the affine 3-space $F^3 = \{(x, y, z) : x, y, z \in F\}$ over a field F. It is easy to partition the points of F^3 into lines (e.g. using all lines parallel to a given line). The following is trickier:

Theorem

If the field F is infinite, then $F^3 \setminus \{(0, 0, 0)\}$ can be partitioned into lines.

This is not hard to prove by transfinite induction. The result fails for a finite field $|F| = q$ since $q^3 - 1$ is not divisible by the line size q.

I have used similar arguments for other geometric partition problems, e.g. partitioning all but one point of a quadratic cone into conics.

Geometric Proofs by Transfinite Induction

Consider the affine 3-space $F^3 = \{(x, y, z) : x, y, z \in F\}$ over a field F. It is easy to partition the points of F^3 into lines (e.g. using all lines parallel to a given line). The following is trickier:

Theorem

If the field F is infinite, then $F^3 \setminus \{(0, 0, 0)\}$ can be partitioned into lines.

This is not hard to prove by transfinite induction. The result fails for a finite field $|F| = q$ since $q^3 - 1$ is not divisible by the line size q.

I have used similar arguments for other geometric partition problems, e.g. partitioning all but one point of a quadratic cone into conics.

Polynomials Producing Primes

The polynomial $f(x) = x^2 - x + 41$ famously has prime values for $x = 0, 1, 2, \ldots, 40$. (Not an accident: the discriminant $D = 1 - 4 \cdot 41 = -163$ yields a quadratic extension $\mathbb{Q}[\sqrt{-163}]$ with unique factorization.)

There is *no* nonconstant polynomial $f(x) \in \mathbb{Z}[x]$ that has *only* prime values for $x \in \mathbb{Z}$.

It is not known if $f(x) = x^2 + 1$ is prime infinitely often for $x \in \mathbb{Z}$.

More generally, there is no polynomial $f(x) \in \mathbb{Z}[x]$ of degree > 1 that is known to realize infinitely many prime values for $x \in \mathbb{Z}$.

But...

Polynomials Producing Primes

The polynomial $f(x) = x^2 - x + 41$ famously has prime values for $x = 0, 1, 2, \ldots, 40$. (Not an accident: the discriminant $D = 1 - 4 \cdot 41 = -163$ yields a quadratic extension $\mathbb{Q}[\sqrt{-163}]$ with unique factorization.)

There is *no* nonconstant polynomial $f(x) \in \mathbb{Z}[x]$ that has *only* prime values for $x \in \mathbb{Z}$.

It is not known if $f(x) = x^2 + 1$ is prime infinitely often for $x \in \mathbb{Z}$.

More generally, there is no polynomial $f(x) \in \mathbb{Z}[x]$ of degree > 1 that is known to realize infinitely many prime values for $x \in \mathbb{Z}$.

But...

Polynomials Producing Primes

The polynomial $f(x) = x^2 - x + 41$ famously has prime values for $x = 0, 1, 2, \ldots, 40$. (Not an accident: the discriminant $D = 1 - 4 \cdot 41 = -163$ yields a quadratic extension $\mathbb{Q}[\sqrt{-163}]$ with unique factorization.)

There is *no* nonconstant polynomial $f(x) \in \mathbb{Z}[x]$ that has *only* prime values for $x \in \mathbb{Z}$.

It is not known if $f(x) = x^2 + 1$ is prime infinitely often for $x \in \mathbb{Z}$.

More generally, there is no polynomial $f(x) \in \mathbb{Z}[x]$ of degree > 1 that is known to realize infinitely many prime values for $x \in \mathbb{Z}$.

But...

Polynomials Producing Primes

The polynomial $f(x) = x^2 - x + 41$ famously has prime values for $x = 0, 1, 2, \ldots, 40$. (Not an accident: the discriminant $D = 1 - 4 \cdot 41 = -163$ yields a quadratic extension $\mathbb{Q}[\sqrt{-163}]$ with unique factorization.)

There is *no* nonconstant polynomial $f(x) \in \mathbb{Z}[x]$ that has *only* prime values for $x \in \mathbb{Z}$.

It is not known if $f(x) = x^2 + 1$ is prime infinitely often for $x \in \mathbb{Z}$.

More generally, there is no polynomial $f(x) \in \mathbb{Z}[x]$ of degree > 1 that is known to realize infinitely many prime values for $x \in \mathbb{Z}$.

But...

Polynomials Producing Primes

The polynomial $f(x) = x^2 - x + 41$ famously has prime values for $x = 0, 1, 2, \ldots, 40$. (Not an accident: the discriminant $D = 1 - 4 \cdot 41 = -163$ yields a quadratic extension $\mathbb{Q}[\sqrt{-163}]$ with unique factorization.)

There is *no* nonconstant polynomial $f(x) \in \mathbb{Z}[x]$ that has *only* prime values for $x \in \mathbb{Z}$.

It is not known if $f(x) = x^2 + 1$ is prime infinitely often for $x \in \mathbb{Z}$.

More generally, there is no polynomial $f(x) \in \mathbb{Z}[x]$ of degree > 1 that is known to realize infinitely many prime values for $x \in \mathbb{Z}$.

But...

Polynomials Producing Primes

For $a, b, c, \ldots, z \in \mathbb{N}$, the polynomial $P(a, b, c, \ldots, z)$ defined by

$$(k+2)\{1-[wz+h+j-q]^2-[(gk+2g+k+1)(h+j)+h-z]^2-[2n+p+q+z-e]^2-[16(k+1)^3(k+2)(n+1)^2+1-f^2]^2-[e^3(e+2)(a+1)^2+1-o^2]^2-[(a^2-1)y^2+1-x^2]^2-[16r^2y^4(a^2-1)+1-u^2]^2-[((a+u^2(u^2-a))^2-1)(n+4dy)^2+1-(x+cu)^2]^2-[n+l+v-y]^2-[(a^2-1)l^2+1-m^2]^2-[ai+k+1-l-i]^2-[p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m]^2-[q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x]^2-[z+pl(a-p)+t(2ap-p^2-1)-pm]^2\}$$

has the set of primes as its positive values (i.e. it takes on every prime value, and no other positive values).

The same is true for the values of

$$P(1+a_1^2+a_2^2+a_3^2+a_4^2,\ 1+b_1^2+b_2^2+b_3^2+b_4^2,\ \ldots,\ 1+z_1^2+z_2^2+z_3^2+z_4^2)$$

for $a_1, a_2, a_3, a_4, \ldots, z_1, z_2, z_3, z_4 \in \mathbb{Z}$.

Polynomials Producing Primes

For $a, b, c, \ldots, z \in \mathbb{N}$, the polynomial $P(a, b, c, \ldots, z)$ defined by

$$(k+2)\{1-[wz+h+j-q]^2-[(gk+2g+k+1)(h+j)+h-z]^2-[2n+p+q+z-e]^2-[16(k+1)^3(k+2)(n+1)^2+1-f^2]^2-[e^3(e+2)(a+1)^2+1-o^2]^2-[(a^2-1)y^2+1-x^2]^2-[16r^2y^4(a^2-1)+1-u^2]^2-[((a+u^2(u^2-a))^2-1)(n+4dy)^2+1-(x+cu)^2]^2-[n+l+v-y]^2-[(a^2-1)l^2+1-m^2]^2-[ai+k+1-l-i]^2-[p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m]^2-[q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x]^2-[z+pl(a-p)+t(2ap-p^2-1)-pm]^2\}$$

has the set of primes as its positive values (i.e. it takes on every prime value, and no other positive values).

The same is true for the values of

$$P(1+a_1^2+a_2^2+a_3^2+a_4^2,\ 1+b_1^2+b_2^2+b_3^2+b_4^2,\ \ldots,\ 1+z_1^2+z_2^2+z_3^2+z_4^2)$$

for $a_1, a_2, a_3, a_4, \ldots, z_1, z_2, z_3, z_4 \in \mathbb{Z}$.

Completely Enumerable Sets are Diophantine

This says less about the prime numbers than you might think.

Surprisingly, it is also true that the set $A = \{10, 10^{10}, 10^{10^{10}}, 10^{10^{10^{10}}}, \ldots\}$ is the set of positive values of some multivariate polynomial over $\mathbb{Z}$. And for the same logical reason:

MRDP Theorem (Matiyasevich, Robinson, Davis, Putnam)

Every completely enumerable set is Diophantine.

$A \subseteq \mathbb{N}$ is *completely enumerable* if is the set of values generated (eventually) by some Turing machine (or computer program) that runs forever.

$A \subseteq \mathbb{N}$ is *Diophantine* if it is the set of positive values of some multivariate polynomial over $\mathbb{Z}$.

Completely Enumerable Sets are Diophantine

This says less about the prime numbers than you might think.

Surprisingly, it is also true that the set $A = \{10, 10^{10}, 10^{10^{10}}, 10^{10^{10^{10}}}, \ldots\}$ is the set of positive values of some multivariate polynomial over $\mathbb{Z}$. And for the same logical reason:

MRDP Theorem (Matiyasevich, Robinson, Davis, Putnam)

Every completely enumerable set is Diophantine.

$A \subseteq \mathbb{N}$ is *completely enumerable* if is the set of values generated (eventually) by some Turing machine (or computer program) that runs forever.

$A \subseteq \mathbb{N}$ is *Diophantine* if it is the set of positive values of some multivariate polynomial over $\mathbb{Z}$.

Completely Enumerable Sets are Diophantine

This says less about the prime numbers than you might think.

Surprisingly, it is also true that the set $A = \{10, 10^{10}, 10^{10^{10}}, 10^{10^{10^{10}}}, \ldots\}$ is the set of positive values of some multivariate polynomial over $\mathbb{Z}$. And for the same logical reason:

MRDP Theorem (Matiyasevich, Robinson, Davis, Putnam)

Every completely enumerable set is Diophantine.

$A \subseteq \mathbb{N}$ is *completely enumerable* if is the set of values generated (eventually) by some Turing machine (or computer program) that runs forever.

$A \subseteq \mathbb{N}$ is *Diophantine* if it is the set of positive values of some multivariate polynomial over $\mathbb{Z}$.

Completely Enumerable Sets are Diophantine

Julia Robinson (1919-1985)

Yuri Matiyasevich (1947-)

MRDP Theorem (Matiyasevich, Robinson, Davis, Putnam)

Every completely enumerable set is Diophantine.

Hilbert's Tenth Problem asked for an algorithm for determining whether a given multivariate integer polynomial has integer solutions.

Corollary

No such algorithm exists.

Completely Enumerable Sets are Diophantine

Julia Robinson (1919-1985)

Yuri Matiyasevich (1947-)

MRDP Theorem (Matiyasevich, Robinson, Davis, Putnam)

Every completely enumerable set is Diophantine.

Hilbert's Tenth Problem asked for an algorithm for determining whether a given multivariate integer polynomial has integer solutions.

Corollary

No such algorithm exists.

Independence Results

Gödel's Incompleteness Theorem

There exist statements which are true for $\mathbb{N}$, but which can neither be proved nor disproved using Peano's axioms.

The earliest explicit example of such a result (Paris and Harrington, 1977) is a slightly strengthened form of the Finite Ramsey Theorem.

Gödel's Theorem applies to all other available axioms for $\mathbb{N}$.

Theorem (Matiyasevich)

For every choice of axioms for $\mathbb{N}$, there exists a Diophantine equation which has no solutions in $\mathbb{N}$, but for which this cannot be proved using the chosen axioms.

Independence Results

Gödel's Incompleteness Theorem

There exist statements which are true for $\mathbb{N}$, but which can neither be proved nor disproved using Peano's axioms.

The earliest explicit example of such a result (Paris and Harrington, 1977) is a slightly strengthened form of the Finite Ramsey Theorem.

Gödel's Theorem applies to all other available axioms for $\mathbb{N}$.

Theorem (Matiyasevich)

For every choice of axioms for $\mathbb{N}$, there exists a Diophantine equation which has no solutions in $\mathbb{N}$, but for which this cannot be proved using the chosen axioms.

Independence Results

Gödel's Incompleteness Theorem

There exist statements which are true for $\mathbb{N}$, but which can neither be proved nor disproved using Peano's axioms.

The earliest explicit example of such a result (Paris and Harrington, 1977) is a slightly strengthened form of the Finite Ramsey Theorem.

Gödel's Theorem applies to all other available axioms for $\mathbb{N}$.

Theorem (Matiyasevich)

For every choice of axioms for $\mathbb{N}$, there exists a Diophantine equation which has no solutions in $\mathbb{N}$, but for which this cannot be proved using the chosen axioms.