Evoluzione del significato di algebra e del suo linguaggio. Quale algebra per i vari livelli scolastici?

Alberto Facchini
Università di Padova

Paderno del Grappa, 30 agosto 2013

Come si colloca l'algebra all'interno della matematica

Un primo punto di vista è:

Come si colloca l'algebra all'interno della matematica

Un primo punto di vista è:

La matematica pura è organizzata in quattro capitoli principali, che sono l'algebra, la teoria dei numeri, la geometria e l'analisi matematica.

Come si colloca l'algebra all'interno della matematica

Un primo punto di vista è:

La matematica pura è organizzata in quattro capitoli principali, che sono l'algebra, la teoria dei numeri, la geometria e l'analisi matematica.

Un secondo punto di vista, un po' più raffinato, è invece:

La matematica

Nel XXI secolo, la matematica è organizzata in:

La matematica

Nel XXI secolo, la matematica è organizzata in:

- un capitolo zero, la teoria degli insiemi, su cui poggia tutto il resto;

La matematica

Nel XXI secolo, la matematica è organizzata in:

- un capitolo zero, la teoria degli insiemi, su cui poggia tutto il resto;
- i primi due capitoli sono l'algebra e la topologia

La matematica

Nel XXI secolo, la matematica è organizzata in:

- un capitolo zero, la teoria degli insiemi, su cui poggia tutto il resto;
- i primi due capitoli sono l'algebra e la topologia — l'algebra studia gli insiemi su cui sono definite operazioni,

La matematica

Nel XXI secolo, la matematica è organizzata in:

- un capitolo zero, la teoria degli insiemi, su cui poggia tutto il resto;
- i primi due capitoli sono l'algebra e la topologia — l'algebra studia gli insiemi su cui sono definite operazioni, la topologia studia gli insiemi su cui sono definiti concetti quali la distanza e la continuità;

La matematica

Nel XXI secolo, la matematica è organizzata in:

- un capitolo zero, la teoria degli insiemi, su cui poggia tutto il resto;
- i primi due capitoli sono l'algebra e la topologia — l'algebra studia gli insiemi su cui sono definite operazioni, la topologia studia gli insiemi su cui sono definiti concetti quali la distanza e la continuità;
- su questi due capitoli poggia tutto il resto della matematica

La matematica

Nel XXI secolo, la matematica è organizzata in:

- un capitolo zero, la teoria degli insiemi, su cui poggia tutto il resto;
- i primi due capitoli sono l'algebra e la topologia — l'algebra studia gli insiemi su cui sono definite operazioni, la topologia studia gli insiemi su cui sono definiti concetti quali la distanza e la continuità;
- su questi due capitoli poggia tutto il resto della matematica (geometria algebrica, analisi matematica, geometria differenziale, trigonometria, analisi funzionale, teoria delle categorie, combinatorica, statistica matematica, ottimizzazione, teoria del controllo, calcolo delle probabilità,...)

. . . e cosa fa l'algebra?

. . . e cosa fa l'algebra?

Essenzialmente l'algebra fa calcoli simili a quelli dell'aritmetica, ma con oggetti matematici che non sono necessariamente numeri

. . . e cosa fa l'algebra?

Essenzialmente l'algebra fa calcoli simili a quelli dell'aritmetica, ma con oggetti matematici che non sono necessariamente numeri (possono essere numeri, ma anche lettere — indeterminate, variabili —, vettori, espressioni, proposizioni, movimenti, matrici, polinomi, funzioni, permutazioni,. . .)

. . . e cosa fa l'algebra?

Essenzialmente l'algebra fa calcoli simili a quelli dell'aritmetica, ma con oggetti matematici che non sono necessariamente numeri (possono essere numeri, ma anche lettere — indeterminate, variabili —, vettori, espressioni, proposizioni, movimenti, matrici, polinomi, funzioni, permutazioni,. . .)

Quindi l'algebra studia le operazioni sugli insiemi.

. . . e cosa fa l'algebra?

Essenzialmente l'algebra fa calcoli simili a quelli dell'aritmetica, ma con oggetti matematici che non sono necessariamente numeri (possono essere numeri, ma anche lettere — indeterminate, variabili —, vettori, espressioni, proposizioni, movimenti, matrici, polinomi, funzioni, permutazioni,. . .)

Quindi l'algebra studia le operazioni sugli insiemi.

Un'*operazione* su un insieme A è un'applicazione (funzione) $A \times A \to A$.

George Boole (1815-1864)

Si ha infatti un vero giro di boa in matematica quando George Boole a metà del XIX secolo comincia ad usare la notazione matematica, che fino ad allora era stata usata per denotare numeri (quantità) e oggetti geometrici (punti, rette, piani, superfici, angoli,...), anche per denotare proposizioni, insiemi arbitrari e loro elementi.

George Boole (1815-1864)

Si ha infatti un vero giro di boa in matematica quando George Boole a metà del XIX secolo comincia ad usare la notazione matematica, che fino ad allora era stata usata per denotare numeri (quantità) e oggetti geometrici (punti, rette, piani, superfici, angoli,...), anche per denotare proposizioni, insiemi arbitrari e loro elementi.

Successivamente le proprietà strutturali di questi oggetti matematici non numerici sono state astratte, fino a definire le strutture algebriche che studiamo oggi, quali gruppi, monoidi, anelli, campi, algebre, algebre di Lie,...

L'algebra oggi

L'algebra oggi

- Gruppi

L'algebra oggi

- Gruppi
- Campi e polinomi

L'algebra oggi

- Gruppi
- Campi e polinomi
- Anelli commutativi

L'algebra oggi

- Gruppi
- Campi e polinomi
- Anelli commutativi
- Algebra lineare e multilineare; teoria delle matrici

L'algebra oggi

- Gruppi
- Campi e polinomi
- Anelli commutativi
- Algebra lineare e multilineare; teoria delle matrici
- Anelli e algebre associativi e non associativi
- Teoria delle categorie
- Algebra omologica
- K-teoria

L'algebra oggi

- Gruppi
- Campi e polinomi
- Anelli commutativi
- Algebra lineare e multilineare; teoria delle matrici
- Anelli e algebre associativi e non associativi
- Teoria delle categorie
- Algebra omologica
- K-teoria

Si usano molto pesantemente metodi algebrici anche in

- Teoria algebrica dei numeri e
- Geometria algebrica

Come si è evoluta l'algebra nei millenni

Breve storia dell'algebra

Le radici dell'algebra affondano nell'antica Babilonia (Iraq, Mesopotamia).

Come si è evoluta l'algebra nei millenni

Breve storia dell'algebra

Le radici dell'algebra affondano nell'antica Babilonia (Iraq, Mesopotamia). La matematica assiro-babilonese era incredibilmente sviluppata. Stiamo parlando della matematica sviluppata in Mesopotamia innanzitutto dai sumèri (2600 a. C.) fino alla caduta di Babilonia (539 a.C). Di questo periodo restano numerosissime tavole di argilla, che ci testimoniano che

Come si è evoluta l'algebra nei millenni

a Babilonia si usava la:

- Notazione posizionale - introdotta in Europa solo nel medioevo. La notazione posizionale era estesa anche a valori frazionari e permetteva di eseguire facilmente calcoli a precisione indefinita.

Come si è evoluta l'algebra nei millenni

a Babilonia si usava la:

- Notazione posizionale - introdotta in Europa solo nel medioevo. La notazione posizionale era estesa anche a valori frazionari e permetteva di eseguire facilmente calcoli a precisione indefinita.
- Numerazione a base 60 - agevolava i calcoli pratici, dato che 60 ha più divisori di 10 (le dieci dita...) Ancora oggi si usa per i gradi degli angoli, per il tempo e per le coordinate geografiche.

Come si è evoluta l'algebra nei millenni

a Babilonia si usava la:

- Notazione posizionale - introdotta in Europa solo nel medioevo. La notazione posizionale era estesa anche a valori frazionari e permetteva di eseguire facilmente calcoli a precisione indefinita.
- Numerazione a base 60 - agevolava i calcoli pratici, dato che 60 ha più divisori di 10 (le dieci dita...) Ancora oggi si usa per i gradi degli angoli, per il tempo e per le coordinate geografiche.
- Teorema di Pitagora - e lo utilizzavano per la risoluzione dei problemi.

Come si è evoluta l'algebra nei millenni

a Babilonia si usava la:

- Notazione posizionale - introdotta in Europa solo nel medioevo. La notazione posizionale era estesa anche a valori frazionari e permetteva di eseguire facilmente calcoli a precisione indefinita.
- Numerazione a base 60 - agevolava i calcoli pratici, dato che 60 ha più divisori di 10 (le dieci dita...) Ancora oggi si usa per i gradi degli angoli, per il tempo e per le coordinate geografiche.
- Teorema di Pitagora - e lo utilizzavano per la risoluzione dei problemi.
- Uso di algoritmi - ad esempio conoscevano almeno un algoritmo per il calcolo della radice quadrata.

Come si è evoluta l'algebra nei millenni

- Uso di tabelle - per evitare i calcoli ripetitivi venivano prodotte tabelle, famosa quella dei reciproci che permetteva di evitare le difficili operazioni di divisione sostituendole con operazioni di moltiplicazione.

Come si è evoluta l'algebra nei millenni

- Uso di tabelle - per evitare i calcoli ripetitivi venivano prodotte tabelle, famosa quella dei reciproci che permetteva di evitare le difficili operazioni di divisione sostituendole con operazioni di moltiplicazione.
- Tabelle logaritmiche - i logaritmi sono stati inventati in Europa da Nepero nel 1600 circa. I babilonesi usavano tavole analoghe più di due millenni prima.

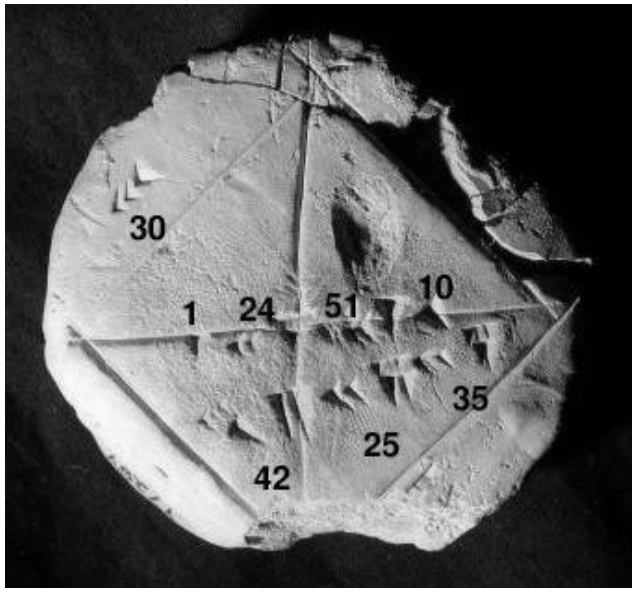
Come si è evoluta l'algebra nei millenni

- Uso di tabelle - per evitare i calcoli ripetitivi venivano prodotte tabelle, famosa quella dei reciproci che permetteva di evitare le difficili operazioni di divisione sostituendole con operazioni di moltiplicazione.
- Tabelle logaritmiche - i logaritmi sono stati inventati in Europa da Nepero nel 1600 circa. I babilonesi usavano tavole analoghe più di due millenni prima.
- Avevano un sistema aritmetico avanzato che mediante algoritmi e tabelle permetteva loro di risolvere problemi che oggi trattiamo mediante equazioni di grado uno o due. Sapevano risolvere alcune equazioni di terzo grado (tabelle).

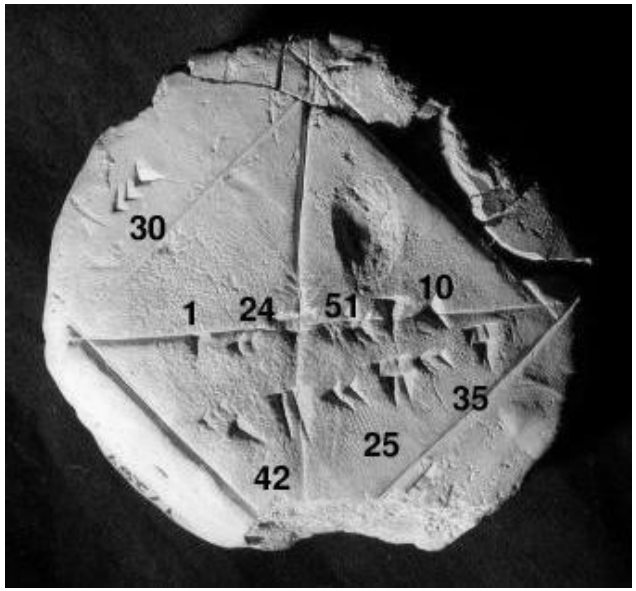
Come si è evoluta l'algebra nei millenni

- Uso di tabelle - per evitare i calcoli ripetitivi venivano prodotte tabelle, famosa quella dei reciproci che permetteva di evitare le difficili operazioni di divisione sostituendole con operazioni di moltiplicazione.
- Tabelle logaritmiche - i logaritmi sono stati inventati in Europa da Nepero nel 1600 circa. I babilonesi usavano tavole analoghe più di due millenni prima.
- Avevano un sistema aritmetico avanzato che mediante algoritmi e tabelle permetteva loro di risolvere problemi che oggi trattiamo mediante equazioni di grado uno o due. Sapevano risolvere alcune equazioni di terzo grado (tabelle).
- Solo soluzioni reali positive.

Esempio: la tavoletta YBC 7289 (1800-1600 a. C.)

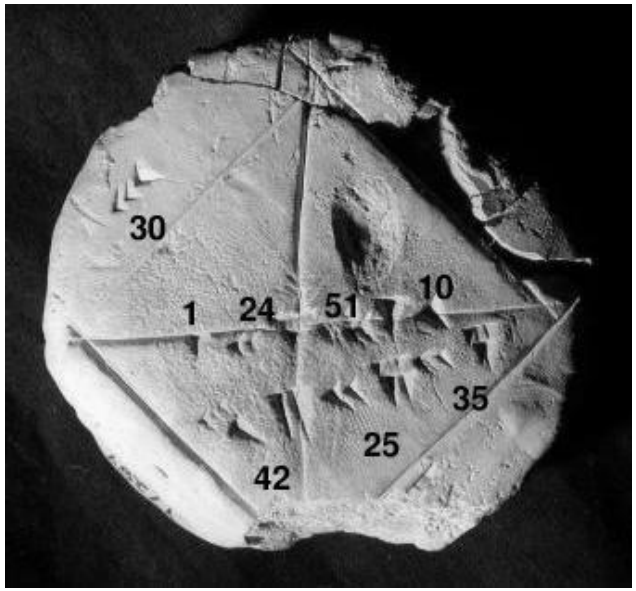


Esempio: la tavoletta YBC 7289 (1800-1600 a. C.)



La radice quadrata di 2 è $1,41421\ldots$. Quindi un quadrato di lato 30 ha diagonale $42,4263\ldots$.

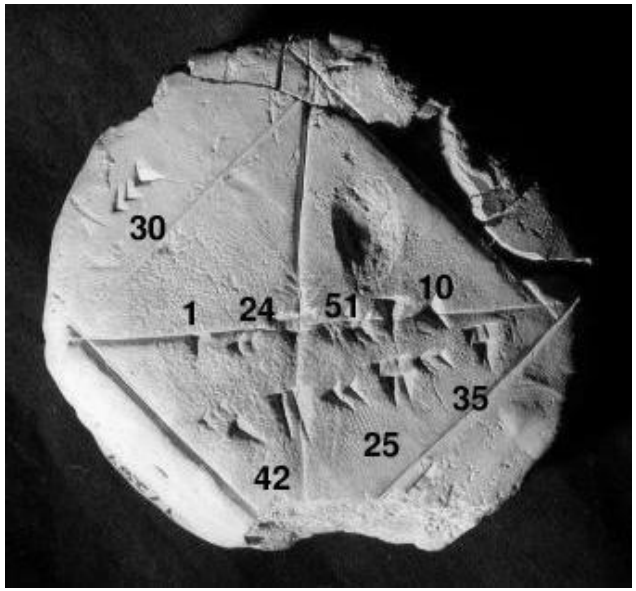
Esempio: la tavoletta YBC 7289 (1800-1600 a. C.)



La radice quadrata di 2 è $1,41421\ldots$. Quindi un quadrato di lato 30 ha diagonale $42,4263\ldots$.

$$(1,24,51,10)_{60} = 1 + \frac{24}{60} + \frac{51}{60^2} + \frac{24}{60^3} = 1,41421296\ldots$$

Esempio: la tavoletta YBC 7289 (1800-1600 a. C.)



La radice quadrata di 2 è $1,41421\ldots$. Quindi un quadrato di lato 30 ha diagonale $42,4263\ldots$.

$$(1,24,51,10)_{60} = 1 + \frac{24}{60} + \frac{51}{60^2} + \frac{24}{60^3} = 1,41421296\ldots$$

$$(42,25,35)_{60} = 42 + \frac{25}{60} + \frac{35}{60^2} = 42,4263\ldots$$

Altro esempio: come calcolavano le radici quadrate (metodo di "Newton")

Dato $\alpha > 0$, per calcolare $\sqrt{\alpha}$, definiamo induttivamente una sequenza $x_0, x_1, x_2, \ldots$ prendendo come x_0 un qualunque reale positivo (quanto più è vicino alla radice, tanto migliore è la convergenza dell'algoritmo), e poi poniamo, per ogni $n \geq 0$,

$$x_{n+1} = \frac{1}{2}\left(x_n + \frac{\alpha}{x_n}\right).$$

Altro esempio: come calcolavano le radici quadrate (metodo di "Newton")

Dato $\alpha > 0$, per calcolare $\sqrt{\alpha}$, definiamo induttivamente una sequenza $x_0, x_1, x_2, \ldots$ prendendo come x_0 un qualunque reale positivo (quanto più è vicino alla radice, tanto migliore è la convergenza dell'algoritmo), e poi poniamo, per ogni $n \geq 0$,

$$x_{n+1} = \frac{1}{2}\left(x_n + \frac{\alpha}{x_n}\right).$$

Se ne ricava che $\lim_{n\to\infty} x_n = \sqrt{\alpha}$.

Altro esempio: come calcolavano le radici quadrate (metodo di "Newton")

Dato $\alpha > 0$, per calcolare $\sqrt{\alpha}$, definiamo induttivamente una sequenza $x_0, x_1, x_2, \ldots$ prendendo come x_0 un qualunque reale positivo (quanto più è vicino alla radice, tanto migliore è la convergenza dell'algoritmo), e poi poniamo, per ogni $n \geq 0$,

$$x_{n+1} = \frac{1}{2}\left(x_n + \frac{\alpha}{x_n}\right).$$

Se ne ricava che $\lim_{n\to\infty} x_n = \sqrt{\alpha}$.

Questo è un algoritmo a convergenza quadratica, ossia il numero di cifre corrette raddoppia (circa) ad ogni passo.

La differenza:

Per risolvere le equazioni di primo e di secondo grado, i babilonesi usavano metodi algoritmici, mentre gli egiziani dello stesso periodo e i greci e i cinesi del primo millennio avanti Cristo usavano metodi geometrici.

La differenza:

Per risolvere le equazioni di primo e di secondo grado, i babilonesi usavano metodi algoritmici, mentre gli egiziani dello stesso periodo e i greci e i cinesi del primo millennio avanti Cristo usavano metodi geometrici.

Non avevano il concetto di teorema.

Diofanto di Alessandria (III sec. d. C.)

Diofanto di Alessandria (III sec. d. C.)

"Il padre dell'algebra".

Diofanto di Alessandria (III sec. d. C.)

"Il padre dell'algebra".
Importanti passi avanti nella notazione matematica.

Diofanto di Alessandria (III sec. d. C.)

"Il padre dell'algebra".
Importanti passi avanti nella notazione matematica.
La prima persona ad usare notazione e simbolismo algebrici.

Diofanto di Alessandria (III sec. d. C.)

"Il padre dell'algebra".
Importanti passi avanti nella notazione matematica.
La prima persona ad usare notazione e simbolismo algebrici.
Prima di lui tutti scrivevano le equazioni completamente.

Brahmagupta, matematico e astronomo indiano (598-668 d. C.)

Brahmagupta, matematico e astronomo indiano (598-668 d. C.)

Due importanti trattati di matematica e astronomia:

Brahmagupta, matematico e astronomo indiano (598-668 d. C.)

Due importanti trattati di matematica e astronomia: Il Brāhmasphuṭasiddhānta (Dottrina di Brahma correttamente stabilita) (628), trattato teorico

Brahmagupta, matematico e astronomo indiano (598-668 d. C.)

Due importanti trattati di matematica e astronomia: Il Brāhmasphuṭasiddhānta (Dottrina di Brahma correttamente stabilita) (628), trattato teorico, e il Khaṇḍakhādyaka, testo più pratico.

Brahmagupta, matematico e astronomo indiano (598-668 d. C.)

Due importanti trattati di matematica e astronomia: Il Brāhmasphuṭasiddhānta (Dottrina di Brahma correttamente stabilita) (628), trattato teorico, e il Khaṇḍakhādyaka, testo più pratico.
Brahmagupta è stato il primo a fare i calcoli con lo zero e a considerare zero un numero come gli altri.

Brahmagupta, matematico e astronomo indiano (598-668 d. C.)

Due importanti trattati di matematica e astronomia: Il Brāhmasphuṭasiddhānta (Dottrina di Brahma correttamente stabilita) (628), trattato teorico, e il Khaṇḍakhādyaka, testo più pratico.
Brahmagupta è stato il primo a fare i calcoli con lo zero e a considerare zero un numero come gli altri. Prima soluzione aritmetica completa dell'equazione di secondo grado (incluse soluzioni negative e nulle).

Brahmagupta, matematico e astronomo indiano (598-668 d. C.)

Due importanti trattati di matematica e astronomia: Il Brāhmasphuṭasiddhānta (Dottrina di Brahma correttamente stabilita) (628), trattato teorico, e il Khaṇḍakhādyaka, testo più pratico.
Brahmagupta è stato il primo a fare i calcoli con lo zero e a considerare zero un numero come gli altri. Prima soluzione aritmetica completa dell'equazione di secondo grado (incluse soluzioni negative e nulle).
No dimostrazioni.

Brahmagupta, matematico e astronomo indiano (598-668 d. C.)

Due importanti trattati di matematica e astronomia: Il Brāhmasphuṭasiddhānta (Dottrina di Brahma correttamente stabilita) (628), trattato teorico, e il Khaṇḍakhādyaka, testo più pratico.
Brahmagupta è stato il primo a fare i calcoli con lo zero e a considerare zero un numero come gli altri. Prima soluzione aritmetica completa dell'equazione di secondo grado (incluse soluzioni negative e nulle).
No dimostrazioni. In versi.
È da una traduzione di questi testi che i matematici arabi accettarono il sistema decimale.

L'atto di nascita dell'algebra

L'atto di nascita dell'algebra

Muḥammad ibn Mūsā al-Khwārizmī
Persiano (ora Uzbekistan), 780-850 circa.

L'atto di nascita dell'algebra

Al-Kitāb al-mukhtaṣar fī ḥisāb al-jabr wa-l-muqābala.

L'atto di nascita dell'algebra

Al-Kitāb al-mukhtaṣar fī ḥisāb al-jabr wa-l-muqābala.
Libro succinto sul calcolo per completamento e bilanciamento

L'atto di nascita dell'algebra

Al-Kitāb al-mukhtaṣar fī ḥisāb al-jabr wa-l-muqābala.
Libro succinto sul calcolo per completamento e bilanciamento

jabr = completamento, trasposizione, restaurazione

L'atto di nascita dell'algebra

Al-Kitāb al-mukhtaṣar fī ḥisāb al-jabr wa-l-muqābala.
Libro succinto sul calcolo per completamento e bilanciamento

jabr = completamento, trasposizione, restaurazione

Le parole jabr e muqābala furono usate da al-Khwārizmī per designare le due operazioni fondamentali di base per risolvere le equazioni. Jabr era portare dall'altra parte dell'equazione cambiando di segno. Muqābala era il cancellare termini uguali da entrambi i membri di un'equazione.

L'atto di nascita dell'algebra

Al-Kitāb al-mukhtaṣar fī ḥisāb al-jabr wa-l-muqābala.
Libro succinto sul calcolo per completamento e bilanciamento

jabr = completamento, trasposizione, restaurazione

Le parole jabr e muqābala furono usate da al-Khwārizmī per designare le due operazioni fondamentali di base per risolvere le equazioni. Jabr era portare dall'altra parte dell'equazione cambiando di segno. Muqābala era il cancellare termini uguali da entrambi i membri di un'equazione.

Oggi al-jabr = algebra

Al-Kitāb al-mukhtaṣar fī ḥisāb al-jabr wa-l-muqābala

Una pagina dell'Al-Kitāb al-mukhtaṣar fī ḥisāb al-jabr wa-l-muqābala.

Al-Kitāb al-mukhtaṣar fī ḥisāb al-jabr wa-l-muqābala

Stabilisce l'algebra come disciplina matematica indipendente dalla geometria e dall'artimetica.

Al-Kitāb al-mukhtaṣar fī ḥisāb al-jabr wa-l-muqābala

Stabilisce l'algebra come disciplina matematica indipendente dalla geometria e dall'artimetica.

Molti dei suoi metodi derivano dalla matematica islamica araba, ma il contributo di al-Khwārizmī fu fondamentale.

Al-Kitāb al-mukhtaṣar fī ḥisāb al-jabr wa-l-muqābala

Stabilisce l'algebra come disciplina matematica indipendente dalla geometria e dall'artimetica.

Molti dei suoi metodi derivano dalla matematica islamica araba, ma il contributo di al-Khwārizmī fu fondamentale.

Sono state traduzioni medioevali del libro di al-Khwārizmī che hanno portato in Europa il sistema di numerazione posizionale decimale e lo zero, nel XI secolo, grazie alla scuola di traduttori di Toledo.

Al-Kitāb al-mukhtaṣar fī ḥisāb al-jabr wa-l-muqābala

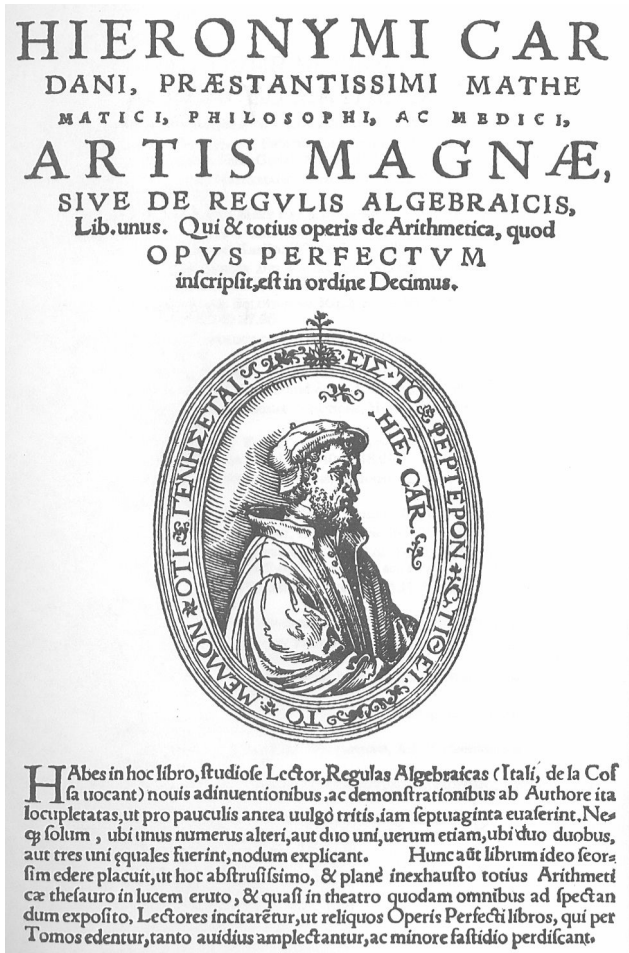
Stabilisce l'algebra come disciplina matematica indipendente dalla geometria e dall'artimetica.

Molti dei suoi metodi derivano dalla matematica islamica araba, ma il contributo di al-Khwārizmī fu fondamentale.

Sono state traduzioni medioevali del libro di al-Khwārizmī che hanno portato in Europa il sistema di numerazione posizionale decimale e lo zero, nel XI secolo, grazie alla scuola di traduttori di Toledo. Poi il sistema decimale è stato propagandato da Leonardo Fibonacci (1170-1250 ca), detto anche Leonardo Pisano, probabilmente il più grande matematico del periodo, nel suo *Liber Abaci*.

Girolamo Cardano (Pavia 1501 - Roma 1576)

Pubblica nel 1545 *Artis Magnae, sive de regulis algebraicis liber unus* (Libro uno della Grande Arte, ossia delle regole algebriche).



HIERONYMI CAR
DANI, PRÆSTANTISSIMI MATHE
MATICI, PHILOSOPHI, AC MEDICI,
ARTIS MAGNÆ,
SIVE DE REGVLIS ALGEBRAICIS,
Lib. unus. Qui & totius operis de Arithmetica, quod
OPVS PERFECTVM
inscripsit, est in ordine Decimus.

HAbes in hoc libro, studiose Lector, Regulas Algebraicas (Itali, de la Cosa uocant) nouis adinuentionibus, ac demonstrationibus ab Authore ita locupletatas, ut pro pauculis antea uulgò tritis, iam septuaginta euaserint. Neq; solum, ubi unus numerus alteri, aut duo uni, uerum etiam, ubi duo duobus, aut tres uni æquales fuerint, nodum explicant. Hunc aũt librum ideo seorsim edere placuit, ut hoc abstrusissimo, & planè inexhausto totius Arithmeticæ thesauro in lucem eruto, & quasi in theatro quodam omnibus ad spectandum exposito, Lectores incitarẽtur, ut reliquos Operis Perfecti libros, qui per Tomos edentur, tanto auidius amplectantur, ac minore fastidio perdiscant.

Ars Magna (1545)

Contiene le formule per la soluzione dell'equazione di terzo grado (in realtà dovuta a Niccolò Fontana Tartaglia) e di quella di quarto grado (in realtà dovuta a Lodovico Ferrari).

Ars Magna (1545)

Contiene le formule per la soluzione dell'equazione di terzo grado (in realtà dovuta a Niccolò Fontana Tartaglia) e di quella di quarto grado (in realtà dovuta a Lodovico Ferrari).

Sempre Cardano introduce i coefficienti binomiali.

Ars Magna (1545)

Contiene le formule per la soluzione dell'equazione di terzo grado (in realtà dovuta a Niccolò Fontana Tartaglia) e di quella di quarto grado (in realtà dovuta a Lodovico Ferrari).

Sempre Cardano introduce i coefficienti binomiali.

Nello stesso periodo appaiono i numeri complessi (Rafael Bombelli, Bologna 1526 - Roma 1572).

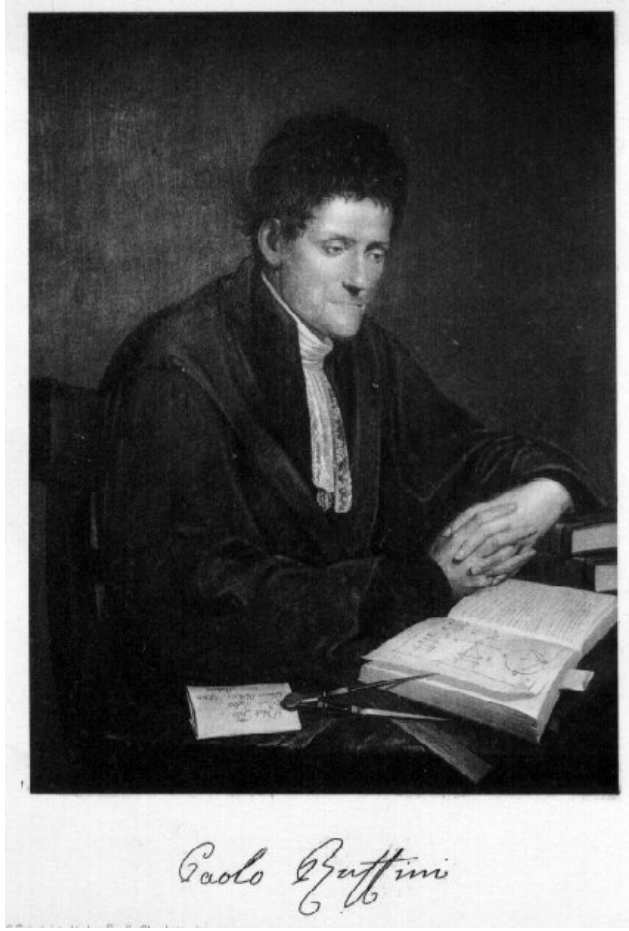
Il determinante

L'idea fu sviluppata dal matematico giapponese Kowa Seki nel 17-esimo secolo, e indipendentemente dieci anni dopo da Gottfried Leibniz. Lo scopo era quello di risolvere sistemi di equazioni lineari usando le matrici (algebra lineare).

Le permutazioni

Studiate da Joseph-Louis Lagrange (Torino 1736 - Parigi 1813) nel suo articolo *Réflexions sur la résolution algébrique des équations* (1770).

Paolo Ruffini (Valentano (VT) 1765 - Modena 1822)



Paolo Ruffini (Valentano (VT) 1765 - Modena 1822)

- *La teoria generale delle equazioni in cui è provato che la soluzione algebrica di equazioni di grado maggiore di 4 è impossibile* (1799).

Paolo Ruffini (Valentano (VT) 1765 - Modena 1822)

- *La teoria generale delle equazioni in cui è provato che la soluzione algebrica di equazioni di grado maggiore di 4 è impossibile* (1799).
- Il primo a sviluppare la teoria dei gruppi di permutazioni, sempre nel contesto della soluzione delle equazioni algebriche.

Tardo ottocento: nasce l'algebra astratta

La maggior parte dei gruppi studiati nel primo stadio dello sviluppo della teoria dei gruppi erano "concreti"

Tardo ottocento: nasce l'algebra astratta

La maggior parte dei gruppi studiati nel primo stadio dello sviluppo della teoria dei gruppi erano "concreti", nel senso che erano gruppi di numeri, gruppi di permutazioni, di matrici o di trasformazioni.

Tardo ottocento: nasce l'algebra astratta

La maggior parte dei gruppi studiati nel primo stadio dello sviluppo della teoria dei gruppi erano "concreti", nel senso che erano gruppi di numeri, gruppi di permutazioni, di matrici o di trasformazioni. Nel tardo ottocento incominciò a prendere piede l'idea di gruppo astratto.

Tardo ottocento: nasce l'algebra astratta

La maggior parte dei gruppi studiati nel primo stadio dello sviluppo della teoria dei gruppi erano "concreti", nel senso che erano gruppi di numeri, gruppi di permutazioni, di matrici o di trasformazioni. Nel tardo ottocento incominciò a prendere piede l'idea di gruppo astratto.

Così incominciò a svilupparsi l'algebra astratta, motivata dall'interesse di risolvere le equazioni, inizialmente focalizzata in quello che ora chiamiamo teoria di Galois e in questioni di costruibilità.

Gruppo (astratto)

Insieme G su cui è definita un'operazione $*$ tale che:

Gruppo (astratto)

Insieme G su cui è definita un'operazione $*$ tale che:

- $x * (y * z) = (x * y) * z$ per ogni $x, y, z \in G$;

Gruppo (astratto)

Insieme G su cui è definita un'operazione $*$ tale che:

- $x * (y * z) = (x * y) * z$ per ogni $x, y, z \in G$;
- esiste un elemento $e \in G$ tale che $e * x = x * e = x$ per ogni $x \in G$;

Gruppo (astratto)

Insieme G su cui è definita un'operazione $*$ tale che:

- $x * (y * z) = (x * y) * z$ per ogni $x, y, z \in G$;
- esiste un elemento $e \in G$ tale che $e * x = x * e = x$ per ogni $x \in G$;
- per ogni $x \in G$ esiste $y \in G$ tale che $x * y = y * x = e$.

Gruppo (astratto)

Insieme G su cui è definita un'operazione $*$ tale che:

- $x * (y * z) = (x * y) * z$ per ogni $x, y, z \in G$;
- esiste un elemento $e \in G$ tale che $e * x = x * e = x$ per ogni $x \in G$;
- per ogni $x \in G$ esiste $y \in G$ tale che $x * y = y * x = e$.

(La classificazione dei gruppi semplici finiti, cioè privi di sottogruppi normali non banali, è uno dei più significativi teoremi del XX secolo. Si tratta di risultati pubblicati soprattutto tra il 1955 e il 1983; risultano esserci 30 tipi basici di gruppi semplici finiti.)

Ogni sottogruppo H di un gruppo G determina una partizione di G in classi laterali

Siano G un gruppo

Ogni sottogruppo H di un gruppo G determina una partizione di G in classi laterali

Siano G un gruppo, H un sottogruppo di G

Ogni sottogruppo H di un gruppo G determina una partizione di G in classi laterali

Siano G un gruppo, H un sottogruppo di G, g un elemento di G.

Ogni sottogruppo H di un gruppo G determina una partizione di G in classi laterali

Siano G un gruppo, H un sottogruppo di G, g un elemento di G. La *classe laterale sinistra di g modulo H* è il sottoinsieme

$$gH := \{ gh \mid h \in H \}$$

di G.

Ogni sottogruppo H di un gruppo G determina una partizione di G in classi laterali

Siano G un gruppo, H un sottogruppo di G, g un elemento di G. La *classe laterale sinistra di g modulo H* è il sottoinsieme

$$gH := \{ gh \mid h \in H \}$$

di G.

Le classi laterali sinistre modulo un sottogruppo H fissato di G formano una partizione $\{ gH \mid g \in G \}$ di G.

Gruppi ciclici finiti

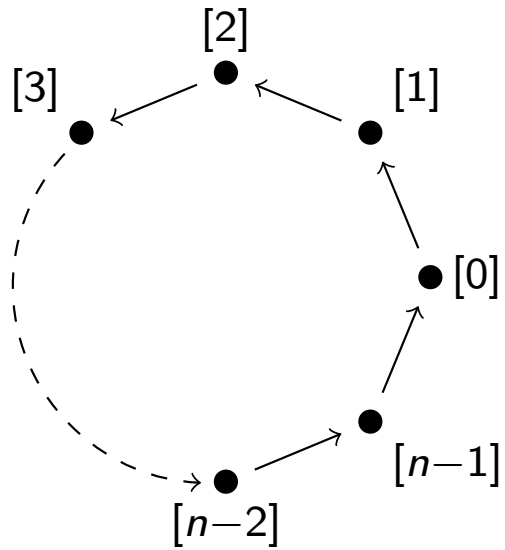
Sono i gruppi G, finiti (cioè con un numero finito di elementi), per i quali esiste un elemento $g \in G$, detto un *generatore* di G, tale che $G = \{ g^t \mid t \in \mathbb{Z} \}$.

Gruppi ciclici finiti

Ogni gruppo ciclico è isomorfo ad un quoziente di $\mathbb{Z}$.

Gruppi ciclici finiti

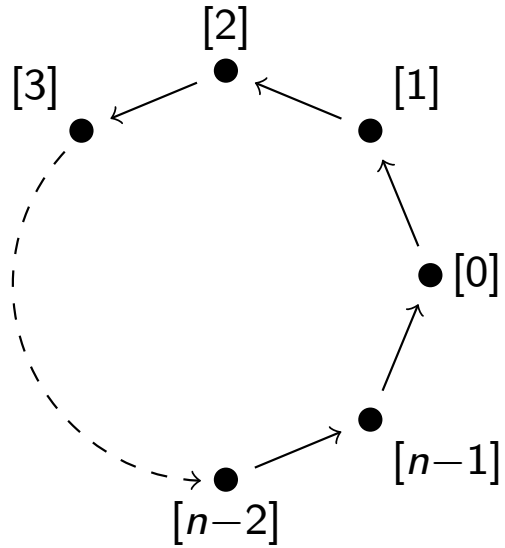
Ogni gruppo ciclico è isomorfo ad un quoziente di $\mathbb{Z}$. In particolare, un gruppo ciclico finito con n elementi è isomorfo a $\mathbb{Z}/n\mathbb{Z}$, la cui rappresentazione più naturale è quella della seguente figura:



Il gruppo ciclico con n elementi $\mathbb{Z}/n\mathbb{Z}$.

Gruppi ciclici finiti

Ogni gruppo ciclico è isomorfo ad un quoziente di $\mathbb{Z}$. In particolare, un gruppo ciclico finito con n elementi è isomorfo a $\mathbb{Z}/n\mathbb{Z}$, la cui rappresentazione più naturale è quella della seguente figura:



Il gruppo ciclico con n elementi $\mathbb{Z}/n\mathbb{Z}$.

Ecco perchè sono stati chiamati *ciclici*: i suoi elementi si dispongono naturalmente in un cerchio, un ciclo. Hanno cioè una struttura "periodica".

Richard Dedekind (1831-1916) e Leopold Kronecker (1823-1891), matematici tedeschi

Iniziarono a scoprire le profonde connessioni tra algebra, teoria dei numeri (teoria algebrica dei numeri) e geometria (geometria algebrica).

Richard Dedekind (1831-1916) e Leopold Kronecker (1823-1891), matematici tedeschi

Iniziarono a scoprire le profonde connessioni tra algebra, teoria dei numeri (teoria algebrica dei numeri) e geometria (geometria algebrica).

Iniziarono lo studio dei primi anelli, anche questi "concreti", sottoanelli di $\mathbb{C}$, quindi tutti anelli necessariamente commutativi.

Adolf Abraham Halevi Fraenkel (Monaco di Baviera 1891, Gerusalemme 1965), matematico israeliano nato in Germania

Definizione di anello astratto (1914).

Adolf Abraham Halevi Fraenkel (Monaco di Baviera 1891, Gerusalemme 1965), matematico israeliano nato in Germania

Definizione di anello astratto (1914).

Insieme R su cui sono definite due operazioni $+$ e $\cdot$ di modo che:

Adolf Abraham Halevi Fraenkel (Monaco di Baviera 1891, Gerusalemme 1965), matematico israeliano nato in Germania

Definizione di anello astratto (1914).

Insieme R su cui sono definite due operazioni $+$ e $\cdot$ di modo che:

- R è un gruppo rispetto all'operazione $+$;

Adolf Abraham Halevi Fraenkel (Monaco di Baviera 1891, Gerusalemme 1965), matematico israeliano nato in Germania

Definizione di anello astratto (1914).

Insieme R su cui sono definite due operazioni $+$ e $\cdot$ di modo che:

- R è un gruppo rispetto all'operazione $+$;
- $x + y = y + x$ per ogni $x, y \in R$;

Adolf Abraham Halevi Fraenkel (Monaco di Baviera 1891, Gerusalemme 1965), matematico israeliano nato in Germania

Definizione di anello astratto (1914).

Insieme R su cui sono definite due operazioni $+$ e $\cdot$ di modo che:

- R è un gruppo rispetto all'operazione $+$;
- $x + y = y + x$ per ogni $x, y \in R$;
- $x(yz) = (xy)z$ per ogni $x, y, z \in R$;

Adolf Abraham Halevi Fraenkel (Monaco di Baviera 1891, Gerusalemme 1965), matematico israeliano nato in Germania

Definizione di anello astratto (1914).

Insieme R su cui sono definite due operazioni $+$ e $\cdot$ di modo che:

- R è un gruppo rispetto all'operazione $+$;
- $x + y = y + x$ per ogni $x, y \in R$;
- $x(yz) = (xy)z$ per ogni $x, y, z \in R$;
- $x(y + z) = xy + xz$ e $(y + z)x = yx + zx$ per ogni $x, y, z \in R$.

Altre strutture algebriche: semigruppi, monoidi,...

Un *semigruppo* è un insieme S su cui è definita un'operazione $*$ tale che $x * (y * z) = (x * y) * z$ per ogni $x, y, z \in S$.

Altre strutture algebriche: semigruppi, monoidi,...

Un *semigruppo* è un insieme S su cui è definita un'operazione $*$ tale che $x * (y * z) = (x * y) * z$ per ogni $x, y, z \in S$.

Appaiono definiti per la prima volta da Jean Armand Marie Joseph de Séguier in "Élements de la Théorie des Groupes Abstraits" (1904).

Altre strutture algebriche: semigruppi, monoidi,...

Un *semigruppo* è un insieme S su cui è definita un'operazione $*$ tale che $x * (y * z) = (x * y) * z$ per ogni $x, y, z \in S$.

Appaiono definiti per la prima volta da Jean Armand Marie Joseph de Séguier in "Élements de la Théorie des Groupes Abstraits" (1904). Primi risultati non-banali ottenuti nel 1928 da Anton Suschkewitsch, che determina la struttura dei semigruppi semplici finiti.

Altre strutture algebriche: semigruppi, monoidi,...

Un *semigruppo* è un insieme S su cui è definita un'operazione $*$ tale che $x * (y * z) = (x * y) * z$ per ogni $x, y, z \in S$.

Appaiono definiti per la prima volta da Jean Armand Marie Joseph de Séguier in "Élements de la Théorie des Groupes Abstraits" (1904). Primi risultati non-banali ottenuti nel 1928 da Anton Suschkewitsch, che determina la struttura dei semigruppi semplici finiti.

Categorie: Samuel Eilenberg e Saunders MacLane, General Theory of Natural Equivalences, Trans. Amer. Math. Soc., 1945.

I monoidi

Un *monoide* è un semigruppo M dotato di identità, cioè di un elemento $e \in M$ tale che $ex = xe = x$ per ogni $x \in M$.

I monoidi

Un *monoide* è un semigruppo M dotato di identità, cioè di un elemento $e \in M$ tale che $ex = xe = x$ per ogni $x \in M$.

Esempio. L'insieme $\mathbb{N}_0$ dei numeri naturali $0, 1, 2, 3, \ldots$ è un monoide commutativo sia rispetto all'addizione che rispetto alla moltiplicazione.

Anche per i monoidi si hanno le classi laterali

Siano M un monoide

Anche per i monoidi si hanno le classi laterali

Siano M un monoide, S un sottomonoide di M

Anche per i monoidi si hanno le classi laterali

Siano M un monoide, S un sottomonoide di M, x un elemento di M.

Anche per i monoidi si hanno le classi laterali

Siano M un monoide, S un sottomonoide di M, x un elemento di M. La *classe laterale sinistra di x modulo S* è il sottoinsieme

$$xS := \{ xs \mid s \in S \}$$

di M.

Anche per i monoidi si hanno le classi laterali

Siano M un monoide, S un sottomonoide di M, x un elemento di M. La *classe laterale sinistra di x modulo S* è il sottoinsieme

$$xS := \{ xs \mid s \in S \}$$

di M.

Le classi laterali sinistre $\{ xS \mid x \in M \}$ di un monoide M modulo un sottomonoide S fissato non formano però in generale una partizione di M.

Monoidi ciclici finiti

Sono i monoidi M, finiti (cioè con un numero finito di elementi), per i quali esiste un elemento $x \in M$, detto un *generatore* di M, tale che $M = \{ x^t \mid t \in \mathbb{N}_0 \}$.

Monoidi ciclici finiti

Ogni monoide ciclico finito M è isomorfo ad un monoide quoziente additivo $\mathbb{N}_0/\sim_{t,\ell}$ per qualche $t, \ell \in \mathbb{N}_0$, $\ell \geq 1$. Qui $\sim_{t,\ell}$ è la relazione di equivalenza su $\mathbb{N}_0$ definita ponendo, per ogni $x, y \in \mathbb{N}_0$,

$$x \sim_{t,\ell} y \text{ se } \begin{cases} x = y \\ \text{oppure} \\ x \geq t,\ y \geq t \text{ e } x \equiv y \pmod{\ell}. \end{cases}$$

Congruenze sul monoide additivo $\mathbb{N}_0$

È possibile dimostrare che le equivalenze $\sim_{t,\ell}$ sono tutte e sole le congruenze sul monoide additivo $\mathbb{N}_0$ diverse dalla relazione di eguaglianza $=$, ossia tutte e sole le relazioni di equivalenza $\sim$ su $\mathbb{N}_0$ tali che $x \sim y$ implica $x + z \sim y + z$ per ogni $x, y, z \in \mathbb{N}_0$, oltre all'eguaglianza $=$.

Congruenze sul monoide additivo $\mathbb{N}_0$

È possibile dimostrare che le equivalenze $\sim_{t,\ell}$ sono tutte e sole le congruenze sul monoide additivo $\mathbb{N}_0$ diverse dalla relazione di eguaglianza $=$, ossia tutte e sole le relazioni di equivalenza $\sim$ su $\mathbb{N}_0$ tali che $x \sim y$ implica $x + z \sim y + z$ per ogni $x, y, z \in \mathbb{N}_0$, oltre all'eguaglianza $=$.

Se $\sim$ è una relazione di equivalenza su un insieme A e $a \in A$, denotiamo con $[a]_\sim$ la classe di equivalenza di a modulo $\sim$, cioè l'insieme degli elementi $b \in A$ con $a \sim b$.

Congruenze sul monoide additivo $\mathbb{N}_0$

È possibile dimostrare che le equivalenze $\sim_{t,\ell}$ sono tutte e sole le congruenze sul monoide additivo $\mathbb{N}_0$ diverse dalla relazione di eguaglianza $=$, ossia tutte e sole le relazioni di equivalenza $\sim$ su $\mathbb{N}_0$ tali che $x \sim y$ implica $x + z \sim y + z$ per ogni $x, y, z \in \mathbb{N}_0$, oltre all'eguaglianza $=$.

Se $\sim$ è una relazione di equivalenza su un insieme A e $a \in A$, denotiamo con $[a]_\sim$ la classe di equivalenza di a modulo $\sim$, cioè l'insieme degli elementi $b \in A$ con $a \sim b$. Allora

$$\mathbb{N}_0/{\sim_{t,\ell}} = \{[0]_{\sim_{t,\ell}}, [1]_{\sim_{t,\ell}}, \ldots, [t + \ell - 1]_{\sim_{t,\ell}}\}$$

Congruenze sul monoide additivo $\mathbb{N}_0$

È possibile dimostrare che le equivalenze $\sim_{t,\ell}$ sono tutte e sole le congruenze sul monoide additivo $\mathbb{N}_0$ diverse dalla relazione di eguaglianza $=$, ossia tutte e sole le relazioni di equivalenza $\sim$ su $\mathbb{N}_0$ tali che $x \sim y$ implica $x + z \sim y + z$ per ogni $x, y, z \in \mathbb{N}_0$, oltre all'eguaglianza $=$.

Se $\sim$ è una relazione di equivalenza su un insieme A e $a \in A$, denotiamo con $[a]_\sim$ la classe di equivalenza di a modulo $\sim$, cioè l'insieme degli elementi $b \in A$ con $a \sim b$. Allora

$$\mathbb{N}_0/{\sim_{t,\ell}} = \{[0]_{\sim_{t,\ell}}, [1]_{\sim_{t,\ell}}, \ldots, [t+\ell-1]_{\sim_{t,\ell}}\},$$

e gli elementi $[0]_{\sim_{t,\ell}}$, $[1]_{\sim_{t,\ell}}$, $\ldots$, $[t+\ell-1]_{\sim_{t,\ell}}$ di $\mathbb{N}_0/{\sim_{t,\ell}}$ sono a due a due distinti. In particolare $\mathbb{N}_0/{\sim_{t,\ell}}$ è un monoide ciclico con esattamente $t + \ell$ elementi.

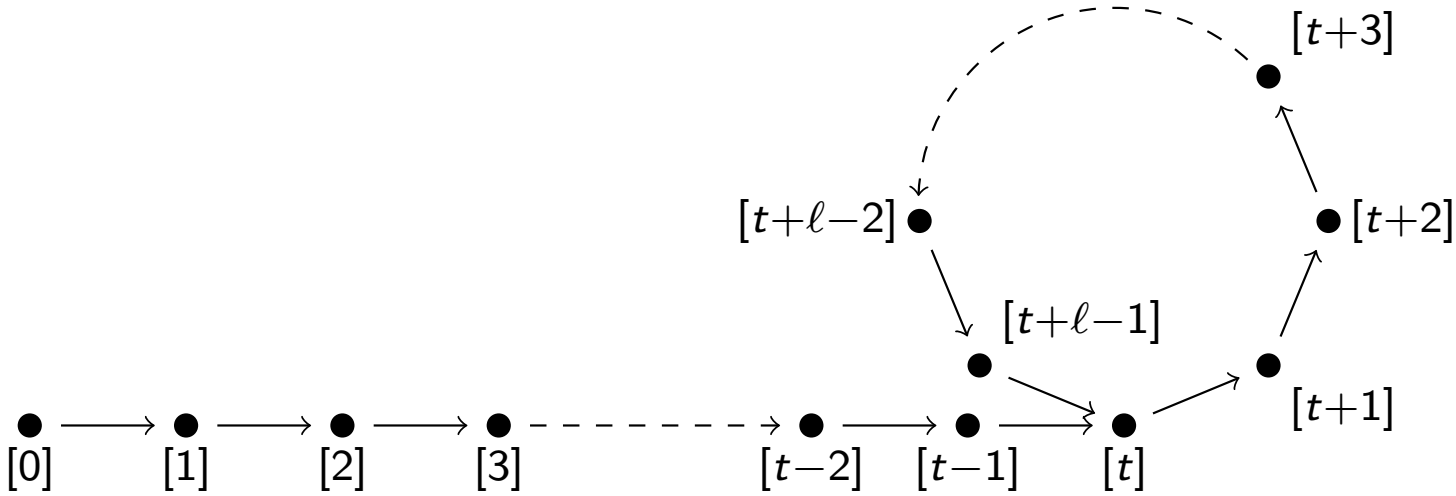
Il monoide additivo $\mathbb{N}_0/\sim_{t,\ell}$

Gli elementi di $\mathbb{N}_0/\sim_{t,\ell}$ sono

$$[0]_{\sim_{t,\ell}} = \{0\},$$
$$[1]_{\sim_{t,\ell}} = \{1\},$$
$$[2]_{\sim_{t,\ell}} = \{2\},$$
$$\vdots$$
$$[t-2]_{\sim_{t,\ell}} = \{t-2\},$$
$$[t-1]_{\sim_{t,\ell}} = \{t-1\},$$
$$[t]_{\sim_{t,\ell}} = \{t, t+\ell, t+2\ell, t+3\ell, \dots\},$$
$$[t+1]_{\sim_{t,\ell}} = \{t+1, t+1+\ell, t+1+2\ell, t+1+3\ell, \dots\},$$
$$\vdots$$
$$[t+\ell-2]_{\sim_{t,\ell}} = \{t+\ell-2, t+\ell-2+\ell, t+\ell-2+2\ell, t+\ell-2+3\ell, \dots$$
$$[t+\ell-1]_{\sim_{t,\ell}} = \{t+\ell-1, t+\ell-1+\ell, t+\ell-1+2\ell, t+\ell-1+3\ell, \dots$$

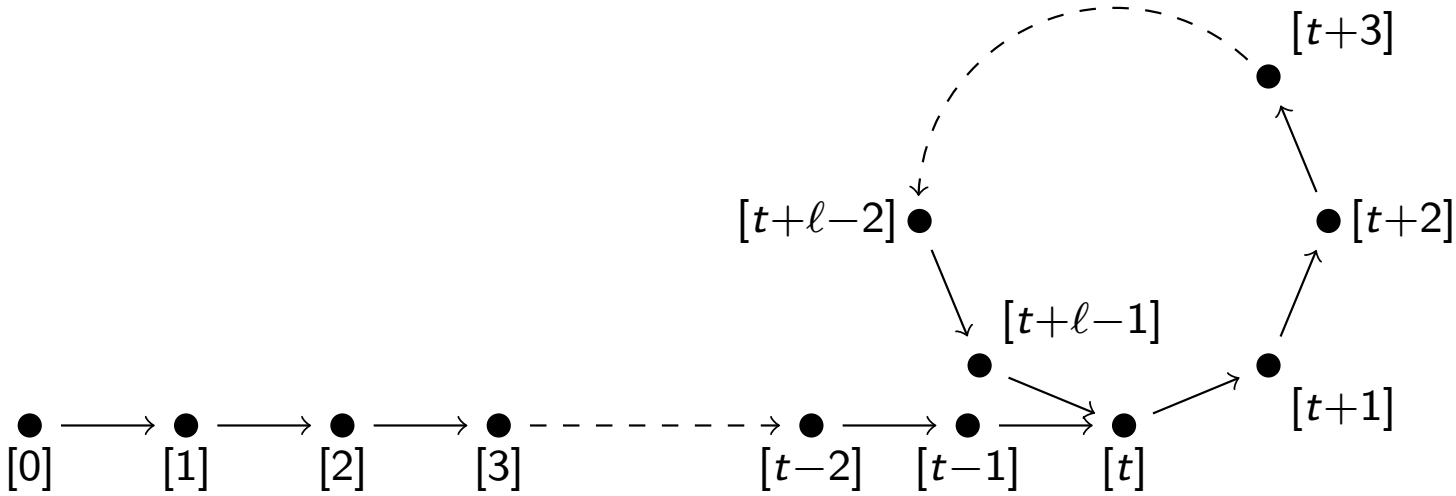
Il monoide additivo $\mathbb{N}_0/\sim_{t,\ell}$

La rappresentazione di $\mathbb{N}_0/\sim_{t,\ell}$ analoga a quella di $\mathbb{Z}/n\mathbb{Z}$ come ciclo è la seguente:



Il monoide additivo $\mathbb{N}_0/\sim_{t,\ell}$

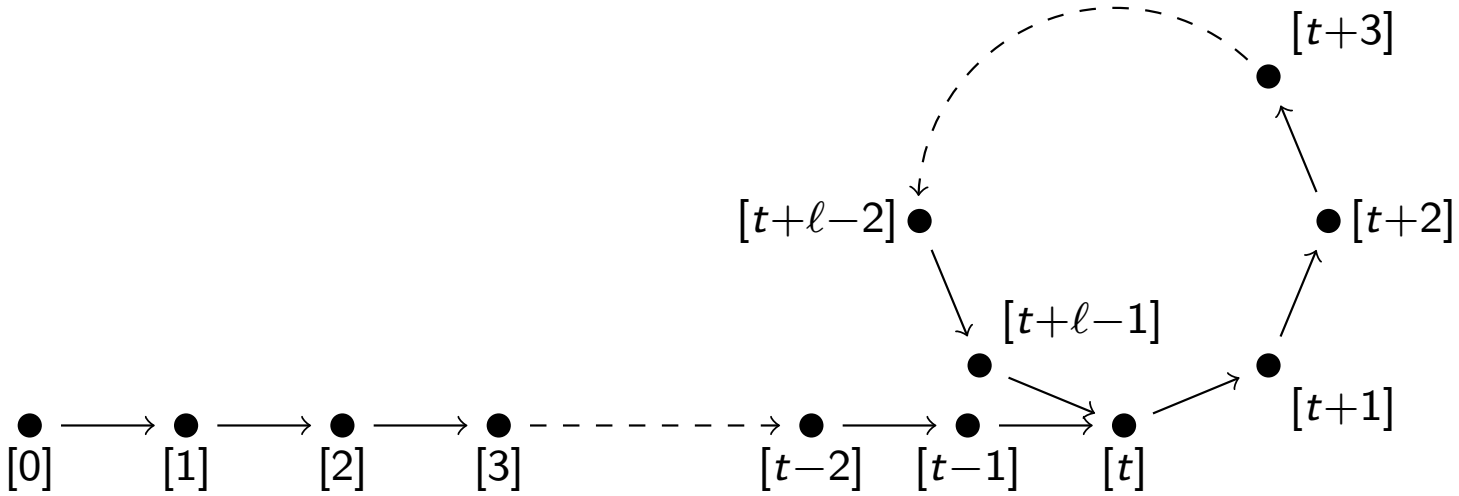
La rappresentazione di $\mathbb{N}_0/\sim_{t,\ell}$ analoga a quella di $\mathbb{Z}/n\mathbb{Z}$ come ciclo è la seguente:



cioè $\mathbb{N}_0/\sim_{t,\ell}$ è periodico da un certo punto in poi.

Il monoide additivo $\mathbb{N}_0/\sim_{t,\ell}$

La rappresentazione di $\mathbb{N}_0/\sim_{t,\ell}$ analoga a quella di $\mathbb{Z}/n\mathbb{Z}$ come ciclo è la seguente:



cioè $\mathbb{N}_0/\sim_{t,\ell}$ è periodico da un certo punto in poi. Consiste di un ciclo di lunghezza ℓ preceduto da una coda di lunghezza t che comincia in $[0]_{\sim_{t,\ell}}$.

. . . periodici da un certo punto in poi, come i razionali. . .

Sia α un numero reale, che supporremo positivo per semplicità.

. . . periodici da un certo punto in poi, come i razionali. . .

Sia α un numero reale, che supporremo positivo per semplicità. Sappiamo tutti che α si può scrivere in notazione decimale come

$$\alpha = d_N d_{N-1} \dots d_1 d_0, d_{-1} d_{-2} d_{-3} \dots$$

dove ogni $d_N, d_{N-1}, \dots, d_1, d_0, d_{-1}, d_{-2}, \dots$ è una delle dieci cifre $0, 1, 2, \dots, 8, 9$.

. . . periodici da un certo punto in poi, come i razionali. . .

Sia α un numero reale, che supporremo positivo per semplicità. Sappiamo tutti che α si può scrivere in notazione decimale come

$$\alpha = d_N d_{N-1} \dots d_1 d_0, d_{-1} d_{-2} d_{-3} \dots$$

dove ogni $d_N, d_{N-1}, \dots, d_1, d_0, d_{-1}, d_{-2}, \dots$ è una delle dieci cifre $0, 1, 2, \dots, 8, 9$. Inoltre α è un numero razionale se e solo se i d_i sono periodici da un certo punto in poi.

I monoidi ciclici finiti sono periodici da un certo punto in poi, come i numeri razionali...

Quindi sia la rappresentazione decimale dei numeri razionali che i monoidi ciclici finiti sono periodici da un certo punto in poi.

I monoidi ciclici finiti sono periodici da un certo punto in poi, come i numeri razionali...

Quindi sia la rappresentazione decimale dei numeri razionali che i monoidi ciclici finiti sono periodici da un certo punto in poi. C'è una relazione tra questi due fatti?

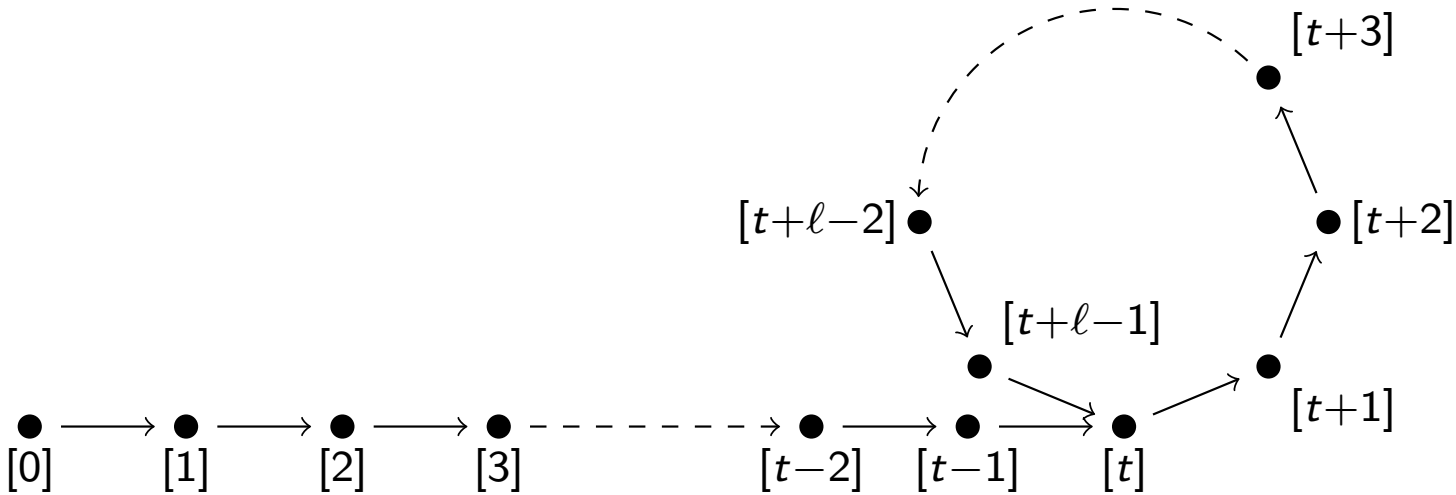
Relazione tra i monoidi ciclici finiti e i numeri razionali

Sì, e si vede in due passi:

Relazione tra i monoidi ciclici finiti e i numeri razionali

Sì, e si vede in due passi:

(1) Non solo i monoidi ciclici finiti S sono del tipo



ma anche tutte le classi laterali xS, dove S è sottomonoide ciclico finito di un monoide M e $x \in M$, sono dello stesso tipo.

Relazione tra i monoidi ciclici finiti e i numeri razionali

(2) Fisso $\alpha = m/n$ razionale, dove m ed n sono interi positivi.

Relazione tra i monoidi ciclici finiti e i numeri razionali

(2) Fisso $\alpha = m/n$ razionale, dove m ed n sono interi positivi. Quando si scrive α in notazione decimale, per determinare le cifre $a_1, a_2, a_3, \ldots$ di α dopo la virgola, si procede con una successione di divisioni euclidee, come segue:

$$m = na_0 + r_0$$
$$10r_0 = na_1 + r_1$$
$$10r_1 = na_2 + r_2$$
$$\vdots$$
$$10r_{i-1} = na_i + r_i$$
$$\vdots$$

Relazione tra i monoidi ciclici finiti e i numeri razionali

(2) Fisso $\alpha = m/n$ razionale, dove m ed n sono interi positivi. Quando si scrive α in notazione decimale, per determinare le cifre $a_1, a_2, a_3, \ldots$ di α dopo la virgola, si procede con una successione di divisioni euclidee, come segue:

$$m = na_0 + r_0$$
$$10r_0 = na_1 + r_1$$
$$10r_1 = na_2 + r_2$$
$$\vdots$$
$$10r_{i-1} = na_i + r_i$$
$$\vdots$$

Gli elementi $\overline{r_0}, \overline{r_1}, \overline{r_2}, \ldots$ di $\mathbb{Z}/n\mathbb{Z}$ sono gli elementi della classe laterale $\overline{m}\langle\overline{10}\rangle$ di $\overline{m}$ modulo il sottomodulo ciclico del monoide moltiplicativo $\mathbb{Z}/n\mathbb{Z}$ generato da $\overline{10}$.

Relazione tra i monoidi ciclici finiti e i numeri razionali

(2) Fisso $\alpha = m/n$ razionale, dove m ed n sono interi positivi. Quando si scrive α in notazione decimale, per determinare le cifre $a_1, a_2, a_3, \ldots$ di α dopo la virgola, si procede con una successione di divisioni euclidee, come segue:

$$m = na_0 + r_0$$
$$10r_0 = na_1 + r_1$$
$$10r_1 = na_2 + r_2$$
$$\vdots$$
$$10r_{i-1} = na_i + r_i$$
$$\vdots$$

Gli elementi $\overline{r_0}, \overline{r_1}, \overline{r_2}, \ldots$ di $\mathbb{Z}/n\mathbb{Z}$ sono gli elementi della classe laterale $\overline{m}\langle\overline{10}\rangle$ di $\overline{m}$ modulo il sottomodulo ciclico del monoide moltiplicativo $\mathbb{Z}/n\mathbb{Z}$ generato da $\overline{10}$. Quindi gli elementi $\overline{r_i} \in \mathbb{Z}/n\mathbb{Z}$ sono periodici da un certo punto in poi.

Relazione tra i monoidi ciclici finiti e i numeri razionali

Dato che $0 \leq r_i < n$ per ogni $i \geq 0$, anche la successione $r_0, r_1, r_2, \ldots$ è periodica da un certo punto in poi.

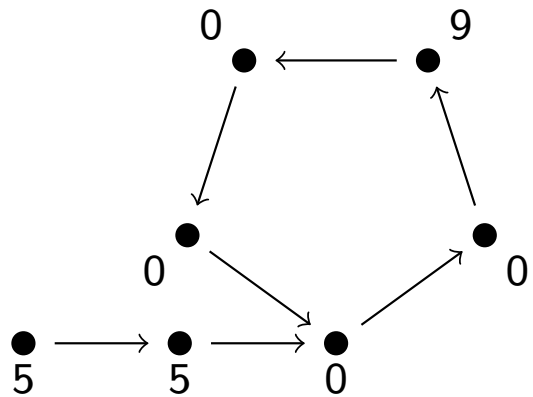
Relazione tra i monoidi ciclici finiti e i numeri razionali

Dato che $0 \leq r_i < n$ per ogni $i \geq 0$, anche la successione $r_0, r_1, r_2, \ldots$ è periodica da un certo punto in poi.

Ma $10r_{i-1} = na_i + r_i$ per ogni $i \geq 1$, e quindi anche la sequenza $a_0, a_1, a_2, \ldots$ è periodica da un certo punto in poi.

Quindi, come per i monoidi, ogni numero razionale tra 0 e 1 può essere scritto come un monoide con una coda

Per esempio, il numero razionale
$\alpha := 122241/222220 = 0.55\overline{00900}$ si può rappresentare come



Scrivendo il numero $\frac{1}{n}$ in forma decimale...

Fissiamo un intero $n \geq 2$.

Scrivendo il numero $\frac{1}{n}$ in forma decimale...

Fissiamo un intero $n \geq 2$. Scriviamo $\frac{1}{n}$ in notazione decimale:

$$\frac{1}{n} = 0, a_1 a_2 \dots a_t \overline{a_{t+1} \dots a_{t+\ell}}$$

Scrivendo il numero $\frac{1}{n}$ in forma decimale...

Fissiamo un intero $n \geq 2$. Scriviamo $\frac{1}{n}$ in notazione decimale:

$$\frac{1}{n} = 0, a_1 a_2 \dots a_t \overline{a_{t+1} \dots a_{t+\ell}}$$

Quindi $\frac{1}{n}$ ha una *parte intera*, che è 0

Scrivendo il numero $\frac{1}{n}$ in forma decimale...

Fissiamo un intero $n \geq 2$. Scriviamo $\frac{1}{n}$ in notazione decimale:

$$\frac{1}{n} = 0, a_1 a_2 \dots a_t \overline{a_{t+1} \dots a_{t+\ell}}$$

Quindi $\frac{1}{n}$ ha una *parte intera*, che è 0, un *antiperiodo* composto da $t \geq 0$ cifre

Scrivendo il numero $\frac{1}{n}$ in forma decimale...

Fissiamo un intero $n \geq 2$. Scriviamo $\frac{1}{n}$ in notazione decimale:

$$\frac{1}{n} = 0, a_1 a_2 \dots a_t \overline{a_{t+1} \dots a_{t+\ell}}$$

Quindi $\frac{1}{n}$ ha una *parte intera*, che è 0, un *antiperiodo* composto da $t \geq 0$ cifre, e un *periodo* composto di $\ell \geq 1$ cifre.

Scrivendo il numero $\frac{1}{n}$ in forma decimale...

Fissiamo un intero $n \geq 2$. Scriviamo $\frac{1}{n}$ in notazione decimale:

$$\frac{1}{n} = 0, a_1 a_2 \dots a_t \overline{a_{t+1} \dots a_{t+\ell}}$$

Quindi $\frac{1}{n}$ ha una *parte intera*, che è 0, un *antiperiodo* composto da $t \geq 0$ cifre, e un *periodo* composto di $\ell \geq 1$ cifre. Non è difficile dimostrare che t ed ℓ hanno le seguenti proprietà:

Scrivendo il numero $\frac{1}{n}$ in forma decimale...

Fissiamo un intero $n \geq 2$. Scriviamo $\frac{1}{n}$ in notazione decimale:

$$\frac{1}{n} = 0, a_1 a_2 \dots a_t \overline{a_{t+1} \dots a_{t+\ell}}$$

Quindi $\frac{1}{n}$ ha una *parte intera*, che è 0, un *antiperiodo* composto da $t \geq 0$ cifre, e un *periodo* composto di $\ell \geq 1$ cifre. Non è difficile dimostrare che t ed ℓ hanno le seguenti proprietà:

(1) Il numero razionale $\frac{1}{n}$ non può essere scritto in notazione decimale con meno cifre, cioè nella forma $0, a'_1 \dots \overline{\dots a'_j}$ con $j < t + \ell$.

Scrivendo il numero $\frac{1}{n}$ in forma decimale...

Fissiamo un intero $n \geq 2$. Scriviamo $\frac{1}{n}$ in notazione decimale:

$$\frac{1}{n} = 0, a_1 a_2 \dots a_t \overline{a_{t+1} \dots a_{t+\ell}}$$

Quindi $\frac{1}{n}$ ha una *parte intera*, che è 0, un *antiperiodo* composto da $t \geq 0$ cifre, e un *periodo* composto di $\ell \geq 1$ cifre. Non è difficile dimostrare che t ed ℓ hanno le seguenti proprietà:

(1) Il numero razionale $\frac{1}{n}$ non può essere scritto in notazione decimale con meno cifre, cioè nella forma $0, a'_1 \dots \overline{\dots a'_j}$ con $j < t + \ell$.

(2) Il sottomonoide ciclico del monoide moltiplicativo $\mathbb{Z}/n\mathbb{Z}$ generato dalla classe residua di 10 modulo n è isomorfa al monoide $\mathbb{N}_0/\sim_{t,\ell}$.

Scrivendo il numero $\frac{1}{n}$ in forma decimale...

(3) I numeri t ed ℓ dipendono essenzialmente dalla fattorizzazione di n in primi.

Scrivendo il numero $\frac{1}{n}$ in forma decimale...

(3) I numeri t ed ℓ dipendono essenzialmente dalla fattorizzazione di n in primi. Più precisamente, fattorizziamo n come

$$n = 2^{e_2} 5^{e_5} \prod_{p \in P} p^{e_p},$$

dove e_2 e e_5 sono interi non-negativi, P è un insieme finito di numeri primi diversi da 2 e 5, ed e_p è un intero positivo per ogni $p \in P$.

Scrivendo il numero $\frac{1}{n}$ in forma decimale...

(3) I numeri t ed ℓ dipendono essenzialmente dalla fattorizzazione di n in primi. Più precisamente, fattorizziamo n come

$$n = 2^{e_2} 5^{e_5} \prod_{p \in P} p^{e_p},$$

dove e_2 e e_5 sono interi non-negativi, P è un insieme finito di numeri primi diversi da 2 e 5, ed e_p è un intero positivo per ogni $p \in P$. Allora t è uguale al più grande tra e_2 ed e_5, ed ℓ è un divisore del minimo comune multiplo dei numeri $p^{e_p} - p^{e_p - 1}$, con p in P.

Scrivendo il numero $\frac{1}{n}$ in forma decimale...

(4) Il più piccolo numero naturale che in notazione decimale può essere scritto nella forma $99\ldots900\ldots0$ ed è divisibile per n è

$$\underbrace{99\ldots9}_{\ell \text{ volte}}\underbrace{00\ldots0}_{t \text{ volte}}.$$

Scrivendo il numero $\frac{1}{n}$ in forma decimale...

(4) Il più piccolo numero naturale che in notazione decimale può essere scritto nella forma $99\ldots900\ldots0$ ed è divisibile per n è

$$\underbrace{99\ldots9}_{\ell \text{ volte}}\underbrace{00\ldots0}_{t \text{ volte}}.$$

Inoltre i numeri naturali della forma $99\ldots900\ldots0$ divisibili per n sono tutti i numeri della forma

$$\underbrace{99\ldots9}_{a \text{ volte}}\underbrace{00\ldots0}_{b \text{ volte}},$$

dove a è multiplo di ℓ e $b \geq t$.

Scrivendo il numero $\frac{1}{n}$ in forma decimale...

(5) La sequenza $r_0, r_1, r_2, r_3 \ldots$ di interi vista prima (i resti delle divisioni) è tale che:

Scrivendo il numero $\frac{1}{n}$ in forma decimale...

(5) La sequenza $r_0, r_1, r_2, r_3 \ldots$ di interi vista prima (i resti delle divisioni) è tale che:

(a) $r_0 = 1$;

Scrivendo il numero $\frac{1}{n}$ in forma decimale...

(5) La sequenza $r_0, r_1, r_2, r_3 \ldots$ di interi vista prima (i resti delle divisioni) è tale che:

(a) $r_0 = 1$;

(b) per ogni $i, j \in N$, $r_i = r_j$ se e solo se $i \sim_{t,\ell} j$, di modo che i $t + \ell$ interi $r_0 = 1, r_1, \ldots, r_{t+\ell-1}$ sono tra loro a due a due distinti;

Scrivendo il numero $\frac{1}{n}$ in forma decimale...

(5) La sequenza $r_0, r_1, r_2, r_3 \ldots$ di interi vista prima (i resti delle divisioni) è tale che:

(a) $r_0 = 1$;

(b) per ogni $i, j \in N$, $r_i = r_j$ se e solo se $i \sim_{t,\ell} j$, di modo che i $t + \ell$ interi $r_0 = 1, r_1, \ldots, r_{t+\ell-1}$ sono tra loro a due a due distinti;

(c) gli interi r_i sono tali che $0 \leq r_i \leq n - 1$ per ogni $i \geq 0$;

Scrivendo il numero $\frac{1}{n}$ in forma decimale...

(5) La sequenza $r_0, r_1, r_2, r_3 \ldots$ di interi vista prima (i resti delle divisioni) è tale che:

(a) $r_0 = 1$;

(b) per ogni $i, j \in N$, $r_i = r_j$ se e solo se $i \sim_{t,\ell} j$, di modo che i $t + \ell$ interi $r_0 = 1, r_1, \ldots, r_{t+\ell-1}$ sono tra loro a due a due distinti;

(c) gli interi r_i sono tali che $0 \leq r_i \leq n - 1$ per ogni $i \geq 0$;

(d) per ogni $i \geq 0$, l'intero r_i è il resto della divisione euclidea di 10^i per n;

Scrivendo il numero $\frac{1}{n}$ in forma decimale...

(5) La sequenza $r_0, r_1, r_2, r_3 \ldots$ di interi vista prima (i resti delle divisioni) è tale che:

(a) $r_0 = 1$;

(b) per ogni $i, j \in N$, $r_i = r_j$ se e solo se $i \sim_{t,\ell} j$, di modo che i $t + \ell$ interi $r_0 = 1, r_1, \ldots, r_{t+\ell-1}$ sono tra loro a due a due distinti;

(c) gli interi r_i sono tali che $0 \leq r_i \leq n - 1$ per ogni $i \geq 0$;

(d) per ogni $i \geq 0$, l'intero r_i è il resto della divisione euclidea di 10^i per n;

(e) un intero positivo $m = d_N d_{N-1} \ldots d_1 d_0$, scritto in notazione decimale, è divisibile per n se e solo se $\sum_{i=0}^{N} r_i d_i$ è divisibile per n.

Scrivendo il numero $\frac{1}{n}$ in forma decimale...

(5) La sequenza $r_0, r_1, r_2, r_3 \ldots$ di interi vista prima (i resti delle divisioni) è tale che:

(a) $r_0 = 1$;

(b) per ogni $i, j \in N$, $r_i = r_j$ se e solo se $i \sim_{t,\ell} j$, di modo che i $t + \ell$ interi $r_0 = 1, r_1, \ldots, r_{t+\ell-1}$ sono tra loro a due a due distinti;

(c) gli interi r_i sono tali che $0 \leq r_i \leq n - 1$ per ogni $i \geq 0$;

(d) per ogni $i \geq 0$, l'intero r_i è il resto della divisione euclidea di 10^i per n;

(e) un intero positivo $m = d_N d_{N-1} \ldots d_1 d_0$, scritto in notazione decimale, è divisibile per n se e solo se $\sum_{i=0}^{N} r_i d_i$ è divisibile per n. Questo è il criterio di divisibilità per n.

Esempio: criteri di divisibilità

Esempio: $n = 3$**.**

Esempio: criteri di divisibilità

Esempio: $n = 3$**.**
Fissiamo un intero $n \geq 2$*. Scriviamo* $\frac{1}{n}$ *in notazione decimale:*

$$\frac{1}{n} = 0, a_1 a_2 \dots a_t \overline{a_{t+1} \dots a_{t+\ell}}$$

Quindi $\frac{1}{n}$ *ha una* parte intera, *che è* 0*, un* antiperiodo *composto da* $t \geq 0$ *cifre, e un* periodo *composto di* $\ell \geq 1$ *cifre.*

Esempio: criteri di divisibilità

Esempio: $n = 3$**.**
Fissiamo un intero $n \geq 2$*. Scriviamo* $\frac{1}{n}$ *in notazione decimale:*

$$\frac{1}{n} = 0, a_1 a_2 \dots a_t \overline{a_{t+1} \dots a_{t+\ell}}$$

Quindi $\frac{1}{n}$ *ha una* parte intera, *che è* 0, *un* antiperiodo *composto da* $t \geq 0$ *cifre, e un* periodo *composto di* $\ell \geq 1$ *cifre.*

In questo caso $n = 3$ e $\frac{1}{3} = 0, \overline{3}$.

Esempio: criteri di divisibilità

Esempio: $n = 3$**.**
Fissiamo un intero $n \geq 2$*. Scriviamo* $\frac{1}{n}$ *in notazione decimale:*

$$\frac{1}{n} = 0, a_1 a_2 \dots a_t \overline{a_{t+1} \dots a_{t+\ell}}$$

Quindi $\frac{1}{n}$ *ha una* parte intera, *che è* 0, *un* antiperiodo *composto da* $t \geq 0$ *cifre, e un* periodo *composto di* $\ell \geq 1$ *cifre.*

In questo caso $n = 3$ e $\frac{1}{3} = 0, \overline{3}$. Quindi $\frac{1}{3}$ ha parte intera 0, non ha antiperiodo e quindi $t = 0$, e periodo 3 di $\ell = 1$ cifra. Quindi $t = 0$ e $\ell = 1$ in questo caso $n = 3$.

Esempio: $n = 3$.

Allora:

(1) Il numero $\frac{1}{n}$ *non può essere scritto in notazione decimale con meno cifre, cioè nella forma* $0, a'_1 \ldots \overline{\ldots . a'_j}$ *con* $j < t + \ell$.

Esempio: $n = 3$.

Allora:

(1) Il numero $\frac{1}{n}$ *non può essere scritto in notazione decimale con meno cifre, cioè nella forma* $0, a'_1 \ldots\ldots \overline{a'_j}$ *con* $j < t + \ell$.

In questo caso $\frac{1}{3}$ non può essere scritto in notazione decimale con meno di una cifra dopo la virgola, cioè nella forma $0, a'_1 \ldots\ldots \overline{a'_j}$ con $j < 1$.

Esempio: $n = 3$.

(2) Il sottomonoide ciclico del monoide moltiplicativo $\mathbb{Z}/n\mathbb{Z}$ *generato dalla classe residua di* 10 *modulo n è isomorfo al monoide* $\mathbb{N}_0/\sim_{t,\ell}$.

Esempio: $n = 3$.

(2) Il sottomonoide ciclico del monoide moltiplicativo $\mathbb{Z}/n\mathbb{Z}$ *generato dalla classe residua di* 10 *modulo n è isomorfo al monoide* $\mathbb{N}_0/\sim_{t,\ell}$.

In questo caso, il sottomonoide ciclico del monoide moltiplicativo $\mathbb{Z}/3\mathbb{Z}$ generato dalla classe residua di 10 modulo 3, cioè il sottomonoide ciclico del monoide $\mathbb{Z}/3\mathbb{Z}$ generato da $\overline{10} = \overline{1}$, è il sottomonoide banale di $\mathbb{Z}/3\mathbb{Z}$ consistente solo dell'unità $\overline{1}$, che è isomorfo al monoide $\mathbb{N}_0/\sim_{0,1}$, che ha $0 + 1 = 1$ elementi.

Esempio: $n = 3$.

(3) I numeri t ed ℓ dipendono essenzialmente dalla fattorizzazione di n in primi. Più precisamente, fattorizziamo n come

$$n = 2^{e_2} 5^{e_5} \prod_{p \in P} p^{e_p},$$

dove e_2 e e_5 sono interi non-negativi, P è un insieme finito di numeri primi diversi da 2 e 5, ed e_p è un intero positivo per ogni $p \in P$. Allora t è uguale al più grande tra e_2 ed e_5, ed ℓ è un divisore del minimo comune multiplo dei numeri $p^{e_p} - p^{e_p - 1}$, con p in P.

Esempio: $n = 3$.

(3) I numeri t ed ℓ dipendono essenzialmente dalla fattorizzazione di n in primi. Più precisamente, fattorizziamo n come

$$n = 2^{e_2} 5^{e_5} \prod_{p \in P} p^{e_p},$$

dove e_2 e e_5 sono interi non-negativi, P è un insieme finito di numeri primi diversi da 2 e 5, ed e_p è un intero positivo per ogni $p \in P$. Allora t è uguale al più grande tra e_2 ed e_5, ed ℓ è un divisore del minimo comune multiplo dei numeri $p^{e_p} - p^{e_p - 1}$, con p in P.

In questo caso 3 si fattorizza solo come 3, quindi $e_2 = 0$, $e_5 = 0$, $P = \{3\}$, $e_3 = 1$, $t = 0$ è uguale al più grande tra $e_2 = 0$ ed $e_5 = 0$, ed $\ell = 1$ è un divisore del minimo comune multiplo dei numeri $p^{e_p} - p^{e_p - 1}$, con p in P, cioè di $3^{e_3} - 3^{e_3 - 1} = 3 - 1 = 2$.

Esempio: $n = 3$.

(4) Il più piccolo numero naturale che in notazione decimale può essere scritto nella forma $99\ldots900\ldots0$ *ed è divisibile per n è* $\underbrace{99\ldots9}_{\ell \text{ volte}}\underbrace{00\ldots0}_{t \text{ volte}}$. *Inoltre i numeri naturali della forma* $99\ldots900\ldots0$ *divisibili per n sono tutti e soli i numeri della forma* $\underbrace{99\ldots9}_{a \text{ volte}}\underbrace{00\ldots0}_{b \text{ volte}}$, *dove* ℓ *divide a 3* $b \geq t$.

Esempio: $n = 3$.

(4) Il più piccolo numero naturale che in notazione decimale può essere scritto nella forma $99\ldots900\ldots0$ *ed è divisibile per n è* $\underbrace{99\ldots9}_{\ell \text{ volte}}\underbrace{00\ldots0}_{t \text{ volte}}$. *Inoltre i numeri naturali della forma* $99\ldots900\ldots0$ *divisibili per n sono tutti e soli i numeri della forma* $\underbrace{99\ldots9}_{a \text{ volte}}\underbrace{00\ldots0}_{b \text{ volte}}$, *dove* ℓ *divide a 3 b* $\geq t$.

In questo caso il più piccolo numero naturale della forma $99\ldots900\ldots0$ divisibile per 3 è $9 = \underbrace{99\ldots9}_{1 \text{ volta}}\underbrace{00\ldots0}_{0 \text{ volte}}$.

Esempio: $n = 3$.

(4) Il più piccolo numero naturale che in notazione decimale può essere scritto nella forma $99\ldots900\ldots0$ *ed è divisibile per n è* $\underbrace{99\ldots9}_{\ell \text{ volte}}\underbrace{00\ldots0}_{t \text{ volte}}$. *Inoltre i numeri naturali della forma* $99\ldots900\ldots0$ *divisibili per n sono tutti e soli i numeri della forma* $\underbrace{99\ldots9}_{a \text{ volte}}\underbrace{00\ldots0}_{b \text{ volte}}$, *dove* ℓ *divide a 3* $b \geq t$.

In questo caso il più piccolo numero naturale della forma $99\ldots900\ldots0$ divisibile per 3 è $9 = \underbrace{99\ldots9}_{1 \text{ volta}}\underbrace{00\ldots0}_{0 \text{ volte}}$. Inoltre i numeri naturali della forma $99\ldots900\ldots0$ divisibili per 3 sono tutti e soli i numeri della forma $\underbrace{99\ldots9}_{a \text{ volte}}\underbrace{00\ldots0}_{b \text{ volte}}$, dove 1 divide a, e quindi $a \geq 1$ è arbitrario, e $b \geq 0$.

Esempio: $n = 3$.

(5) La sequenza $r_0, r_1, r_2, r_3 \ldots$ di interi vista prima è tale che:

(a) $r_0 = 1$;

(b) *per ogni $i, j \in N$, $r_i = r_j$ se e solo se $i \sim_{t,\ell} j$, di modo che i $t + \ell$ interi $r_0 = 1, r_1, \ldots, r_{t+\ell-1}$ sono tra loro distinti;*

(c) *gli interi r_i sono tali che $0 \leq r_i \leq n - 1$ per ogni $i \geq 0$;*

(d) *l'intero r_i è il resto della divisione euclidea di 10^i per n per ogni $i \geq 0$;*

(e) *un intero positivo $m = d_N d_{N-1} \ldots d_1 d_0$, scritto in notazione decimale, è divisibile per n se e solo se $\sum_{i=0}^{N} r_i d_i$ è divisibile per n (criterio di divisibilità per n).*

Esempio: $n = 3$.

(5) La sequenza $r_0, r_1, r_2, r_3 \ldots$ di interi vista prima è tale che:

(a) $r_0 = 1$;

(b) *per ogni $i, j \in N$, $r_i = r_j$ se e solo se $i \sim_{t,\ell} j$, di modo che i $t + \ell$ interi $r_0 = 1, r_1, \ldots, r_{t+\ell-1}$ sono tra loro distinti;*

(c) *gli interi r_i sono tali che $0 \leq r_i \leq n - 1$ per ogni $i \geq 0$;*

(d) *l'intero r_i è il resto della divisione euclidea di 10^i per n per ogni $i \geq 0$;*

(e) *un intero positivo $m = d_N d_{N-1} \ldots d_1 d_0$, scritto in notazione decimale, è divisibile per n se e solo se $\sum_{i=0}^{N} r_i d_i$ è divisibile per n (criterio di divisibilità per n).*

In questo caso $n = 3$, per (d), la sequenza dei resti $r_0, r_1, r_2, r_3 \ldots$ è la sequenza $1, 1, 1, 1, \ldots$. Un intero positivo $m = d_N d_{N-1} \ldots d_1 d_0$, scritto in notazione decimale, è divisibile per 3 se e solo se $\sum_{i=0}^{N} r_i d_i = \sum_{i=0}^{N} d_i$ è divisibile per 3.

Esempio: $n = 3$.

(5) La sequenza $r_0, r_1, r_2, r_3 \ldots$ di interi vista prima è tale che:

(a) $r_0 = 1$;

(b) *per ogni $i, j \in N$, $r_i = r_j$ se e solo se $i \sim_{t,\ell} j$, di modo che i $t + \ell$ interi $r_0 = 1, r_1, \ldots, r_{t+\ell-1}$ sono tra loro distinti;*

(c) *gli interi r_i sono tali che $0 \leq r_i \leq n - 1$ per ogni $i \geq 0$;*

(d) *l'intero r_i è il resto della divisione euclidea di 10^i per n per ogni $i \geq 0$;*

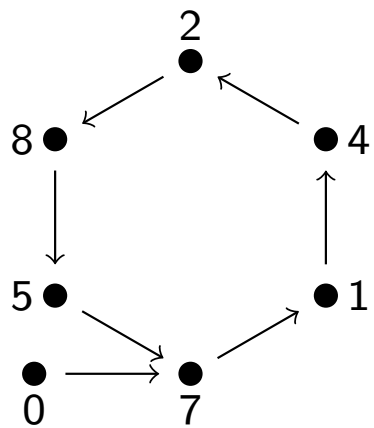
(e) *un intero positivo $m = d_N d_{N-1} \ldots d_1 d_0$, scritto in notazione decimale, è divisibile per n se e solo se $\sum_{i=0}^{N} r_i d_i$ è divisibile per n (criterio di divisibilità per n).*

In questo caso $n = 3$, per (d), la sequenza dei resti $r_0, r_1, r_2, r_3 \ldots$ è la sequenza $1, 1, 1, 1, \ldots$. Un intero positivo $m = d_N d_{N-1} \ldots d_1 d_0$, scritto in notazione decimale, è divisibile per 3 se e solo se $\sum_{i=0}^{N} r_i d_i = \sum_{i=0}^{N} d_i$ è divisibile per 3. È il solito criterio di divisibilità per 3.

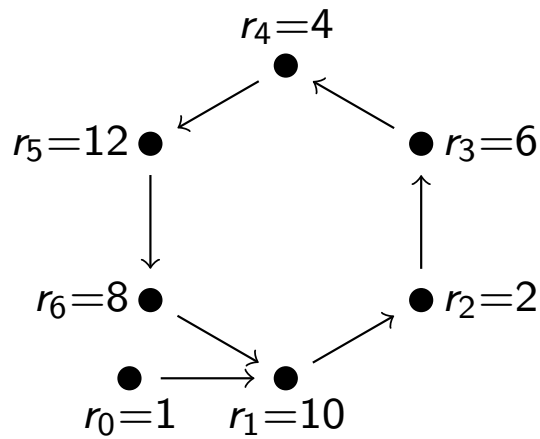
Esempio: $n = 14$.

Per $n = 14$, si ha $\frac{1}{14} = 0.0\overline{714285}$, di modo che $\frac{1}{14}$ si può rappresentare come in (a). In questo caso $t = 1$ and $\ell = 6$ ($t = 1$ è la lunghezza dell'antiperiodo 0, e $\ell = 6$ è la lunghezza del periodo 714285). Il criterio di divisibilità per 14 corrisponde alla sequenza $r_0 = 1, r_1, r_2, r_3 \ldots$ dei resti, che consiste di 1 e poi di $10, 2, 6, 4, 12, 8$ che si ripetono ciclicamente come in (b).

(a)



(b)



Esempio: $n = 14$.

14 divide 9999990 (6 nove e uno zero, e infatti $9999990 = 14 \cdot 714285$), e questo è il più piccolo numero della forma $99\ldots900\ldots0$ divisibile per 14.

Esempio: $n = 14$.

14 divide 9999990 (6 nove e uno zero, e infatti $9999990 = 14 \cdot 714285$), e questo è il più piccolo numero della forma $99\ldots900\ldots0$ divisibile per 14.

Si ha $14 = 2 \cdot 7$, e quindi $e_2 = 1,\ e_5 = 0$, $P = \{7\}$, $e_7 = 1$, $t = 1$ è uguale al più grande tra $e_2 = 1$ ed $e_5 = 0$, ed $\ell = 6$ è un divisore del minimo comune multiplo dei numeri $p^{e_p} - p^{e_p - 1}$, con p in P, cioè di $7^{e_7} - 7^{e_7 - 1} = 7 - 1 = 6$.

Un'ultima applicazione dell'algebra astratta

La prova del nove.

Un'ultima applicazione dell'algebra astratta

La prova del nove. Perchè funziona?

Un'ultima applicazione dell'algebra astratta

La prova del nove. Perchè funziona?

La prova del nove funziona per l'addizione, la sottrazione, la moltiplicazione (le tre operazioni su un anello) tra interi, per la divisione euclidea, funziona anche per le operazioni con la virgola, e anche per le radici quadrate, cubiche,...

La prova del nove

Facciamo un esempio con una divisione euclidea. Dividiamo 87325 per 475. Troviamo un quoto di 183 e un resto di 400

La prova del nove

Facciamo un esempio con una divisione euclidea. Dividiamo 87325 per 475. Troviamo un quoto di 183 e un resto di 400:

$$87325 = 475 \cdot 183 + 400.$$

La prova del nove

Facciamo un esempio con una divisione euclidea. Dividiamo 87325 per 475. Troviamo un quoto di 183 e un resto di 400:

$$87325 = 475 \cdot 183 + 400.$$

Controlliamo se abbiamo fatto giusto con la prova del nove.

La prova del nove

Facciamo un esempio con una divisione euclidea. Dividiamo 87325 per 475. Troviamo un quoto di 183 e un resto di 400:

$$87325 = 475 \cdot 183 + 400.$$

Controlliamo se abbiamo fatto giusto con la prova del nove. Facendo la somma delle cifre troviamo a sinistra 7 e a destra $7 \cdot 3 + 4$, ossia 7, come desiderato e la prova del nove ci dice che probabilmente la divisione fatta è corretta.

La prova del nove

Facciamo un esempio con una divisione euclidea. Dividiamo 87325 per 475. Troviamo un quoto di 183 e un resto di 400:

$$87325 = 475 \cdot 183 + 400.$$

Controlliamo se abbiamo fatto giusto con la prova del nove. Facendo la somma delle cifre troviamo a sinistra 7 e a destra $7 \cdot 3 + 4$, ossia 7, come desiderato e la prova del nove ci dice che probabilmente la divisione fatta è corretta.

Perchè probabilmente?

La prova del nove

Facciamo un esempio con una divisione euclidea. Dividiamo 87325 per 475. Troviamo un quoto di 183 e un resto di 400:

$$87325 = 475 \cdot 183 + 400.$$

Controlliamo se abbiamo fatto giusto con la prova del nove. Facendo la somma delle cifre troviamo a sinistra 7 e a destra $7 \cdot 3 + 4$, ossia 7, come desiderato e la prova del nove ci dice che probabilmente la divisione fatta è corretta.

Perchè probabilmente? Con quale probabilità?

La prova del nove

Facciamo un esempio con una divisione euclidea. Dividiamo 87325 per 475. Troviamo un quoto di 183 e un resto di 400:

$$87325 = 475 \cdot 183 + 400.$$

Controlliamo se abbiamo fatto giusto con la prova del nove. Facendo la somma delle cifre troviamo a sinistra 7 e a destra $7 \cdot 3 + 4$, ossia 7, come desiderato e la prova del nove ci dice che probabilmente la divisione fatta è corretta.

Perchè probabilmente? Con quale probabilità? Perchè la prova del nove funziona (abbastanza bene)?

La prova del nove

Tutto si basa nell'applicare all'identità che voglio verificare ($87325 = 475 \cdot 183 + 400$) l'omomorfismo canonico di anelli $\pi : \mathbb{Z} \to \mathbb{Z}/9\mathbb{Z}$, $x \in \mathbb{Z} \mapsto \overline{x} = x + 9\mathbb{Z} \in \mathbb{Z}/9\mathbb{Z}$.

La prova del nove

Tutto si basa nell'applicare all'identità che voglio verificare ($87325 = 475 \cdot 183 + 400$) l'omomorfismo canonico di anelli $\pi : \mathbb{Z} \to \mathbb{Z}/9\mathbb{Z}$, $x \in \mathbb{Z} \mapsto \overline{x} = x + 9\mathbb{Z} \in \mathbb{Z}/9\mathbb{Z}$.

In $\mathbb{Z}/9\mathbb{Z}$ si ha che $\overline{1} = \overline{10} = \overline{100} = \overline{1000} = \ldots$, e quindi per un numero decimale $d_N d_{N-1} \ldots d_1 d_0$ si ha che $\overline{d_N d_{N-1} \ldots d_1 d_0} = \overline{\sum_{i=0}^{N} d_i 10^i} = \overline{\sum_{i=0}^{N} d_i}$. Quindi in $\mathbb{Z}/9\mathbb{Z}$ ogni numero è uguale alla somma delle sue cifre in notazione decimale. Dato che in $\mathbb{Z}/9\mathbb{Z}$ si ha $\overline{7} = \overline{7 \cdot 3 + 4}$, cioè $\overline{87325 = 475 \cdot 183 + 400}$, è probabile che in $\mathbb{Z}$ si abbia proprio $87325 = 475 \cdot 183 + 400$ con una probabilità di $1 - \frac{1}{9} = 88, \overline{8}\%$ (perchè $\mathbb{Z}/9\mathbb{Z}$ ha nove elementi).

La prova del nove

Tutto si basa nell'applicare all'identità che voglio verificare ($87325 = 475 \cdot 183 + 400$) l'omomorfismo canonico di anelli $\pi : \mathbb{Z} \to \mathbb{Z}/9\mathbb{Z}$, $x \in \mathbb{Z} \mapsto \overline{x} = x + 9\mathbb{Z} \in \mathbb{Z}/9\mathbb{Z}$.

In $\mathbb{Z}/9\mathbb{Z}$ si ha che $\overline{1} = \overline{10} = \overline{100} = \overline{1000} = \ldots$, e quindi per un numero decimale $d_N d_{N-1} \ldots d_1 d_0$ si ha che $\overline{d_N d_{N-1} \ldots d_1 d_0} = \overline{\sum_{i=0}^{N} d_i 10^i} = \overline{\sum_{i=0}^{N} d_i}$. Quindi in $\mathbb{Z}/9\mathbb{Z}$ ogni numero è uguale alla somma delle sue cifre in notazione decimale. Dato che in $\mathbb{Z}/9\mathbb{Z}$ si ha $\overline{7} = \overline{7 \cdot 3 + 4}$, cioè $\overline{87325 = 475 \cdot 183 + 400}$, è probabile che in $\mathbb{Z}$ si abbia proprio $87325 = 475 \cdot 183 + 400$ con una probabilità di $1 - \frac{1}{9} = 88,\overline{8}\%$ (perchè $\mathbb{Z}/9\mathbb{Z}$ ha nove elementi).

In base $b \geq 2$, il tutto funziona similmente, e si ha la prova del $b-1$. Usando $\mathbb{Z}/(b-1)\mathbb{Z}$, si vede che la prova del $b-1$ ha una probabilità di funzionare di $\frac{b-2}{b-1}$.