Honors Day 2010
It's Fundamental, My Dear Gauss

Steven F. Bellenot

Department of Mathematics
Florida State University

Honors Day
Florida State University, Tallahassee, FL
Apr 2, 2010

Math, It's Fundamental

- But it is not easy
- There is no royal road
- There is no math pill
- Skills are not FCAT-able
- But it is a human activity

Math, It's Fundamental

- But it is not easy
- There is no royal road
- There is no math pill
- Skills are not FCAT-able
- But it is a human activity

Math, It's Fundamental

- But it is not easy
- There is no royal road
- There is no math pill
- Skills are not FCAT-able
- But it is a human activity

- But it is not easy
- There is no royal road
- There is no math pill
- Skills are not FCAT-able
- But it is a human activity

Math, It's Fundamental

- But it is not easy
- There is no royal road
- There is no math pill
- Skills are not FCAT-able
- But it is a human activity

Fundamental Theorems

- Fundamental Theorem of Arithemetic
- Each integer $n > 1$ has a unique prime factorialization
$$n = p_1 p_2 \cdots p_k$$
with $p_1 \leq p_2 \cdots \leq p_k$
- Fundamental Theorem of Algebra
- Each non-constant polynomial has a root
- Fundamental Theorem of Calculus
- Part I: If $f(t)$ is continuous,
$$F(x) = \int_a^x f(t)\, dt$$
then $F'(x) = f(x)$

Fundamental Theorems

- Fundamental Theorem of Arithmetic
- Each integer $n > 1$ has a unique prime factorialization

$$n = p_1 p_2 \cdots p_k$$

with $p_1 \leq p_2 \cdots \leq p_k$

- Fundamental Theorem of Algebra
- Each non-constant polynomial has a root
- Fundamental Theorem of Calculus
- Part I: If $f(t)$ is continuous,

$$F(x) = \int_a^x f(t)\, dt$$

then $F'(x) = f(x)$

Fundamental Theorems

- Fundamental Theorem of Arithemetic
- Each integer $n > 1$ has a unique prime factorialization

$$n = p_1 p_2 \cdots p_k$$

  with $p_1 \leq p_2 \cdots \leq p_k$
- Fundamental Theorem of Algebra
- Each non-constant polynomial has a root
- Fundamental Theorem of Calculus
- Part I: If $f(t)$ is continuous,

$$F(x) = \int_a^x f(t)\,dt$$

  then $F'(x) = f(x)$

Fundamental Theorems

- Fundamental Theorem of Arithemetic
- Each integer $n > 1$ has a unique prime factorialization

$$n = p_1 p_2 \cdots p_k$$

with $p_1 \leq p_2 \cdots \leq p_k$

- Fundamental Theorem of Algebra
- Each non-constant polynomial has a root
- Fundamental Theorem of Calculus
- Part I: If $f(t)$ is continuous,

$$F(x) = \int_a^x f(t)\,dt$$

then $F'(x) = f(x)$

Fundamental Theorems

- Fundamental Theorem of Arithemetic
- Each integer $n > 1$ has a unique prime factorialization

$$n = p_1 p_2 \cdots p_k$$

with $p_1 \leq p_2 \cdots \leq p_k$

- Fundamental Theorem of Algebra
- Each non-constant polynomial has a root
- Fundamental Theorem of Calculus
- Part I: If $f(t)$ is continuous,

$$F(x) = \int_a^x f(t)\,dt$$

then $F'(x) = f(x)$

Fundamental Theorems

- Fundamental Theorem of Arithemetic
- Each integer $n > 1$ has a unique prime factorialization

$$n = p_1 p_2 \cdots p_k$$

  with $p_1 \leq p_2 \cdots \leq p_k$
- Fundamental Theorem of Algebra
- Each non-constant polynomial has a root
- Fundamental Theorem of Calculus
- Part I: If $f(t)$ is continuous,

$$F(x) = \int_a^x f(t)\, dt$$

  then $F'(x) = f(x)$

Fundamental Theorem of Arithmetic

Euclid's Elements ($\approx$ 300 bce) contains a proof. Three of the 13 books, VII, VIII and IX are about number theory. (But Euclid had no notation for the product of more than 3 numbers.)

Known to the Egyptian Ahmes ($\approx$ 1550 bce?) who copied a earlier source:

Directions for Knowing All Dark Things ($\approx$ 1650 bce) (discovered in 2002).

Some people say Gauss gave the first full and correct proof in Disquisitiones Arithmeticae. (written 1798 when Gauss was 21, published in 1801)

Fundamental Theorem of Arithmetic

Euclid's Elements ($\approx$ 300 bce) contains a proof. Three of the 13 books, VII, VIII and IX are about number theory. (But Euclid had no notation for the product of more than 3 numbers.)
Known to the Egyptian Ahmes ($\approx$ 1550 bce?) who copied a earlier source:
Directions for Knowing All Dark Things ($\approx$ 1650 bce) (discovered in 2002).
Some people say Gauss gave the first full and correct proof in Disquisitiones Arithmeticae. (written 1798 when Gauss was 21, published in 1801)

Euclid's Elements ($\approx$ 300 bce) contains a proof. Three of the 13 books, VII, VIII and IX are about number theory. (But Euclid had no notation for the product of more than 3 numbers.)
Known to the Egyptian Ahmes ($\approx$ 1550 bce?) who copied a earlier source:
Directions for Knowing All Dark Things ($\approx$ 1650 bce)
(discovered in 2002).
Some people say Gauss gave the first full and correct proof in Disquisitiones Arithmeticae. (written 1798 when Gauss was 21, published in 1801)

Euclid's Elements ($\approx$ 300 bce) contains a proof. Three of the 13 books, VII, VIII and IX are about number theory. (But Euclid had no notation for the product of more than 3 numbers.)
Known to the Egyptian Ahmes ($\approx$ 1550 bce?) who copied a earlier source:
Directions for Knowing All Dark Things ($\approx$ 1650 bce) (discovered in 2002).
Some people say Gauss gave the first full and correct proof in Disquisitiones Arithmeticae. (written 1798 when Gauss was 21, published in 1801)

Fundamental Theorem of Arithmetic

Euclid's Elements ($\approx$ 300 bce) contains a proof. Three of the 13 books, VII, VIII and IX are about number theory. (But Euclid had no notation for the product of more than 3 numbers.)

Known to the Egyptian Ahmes ($\approx$ 1550 bce?) who copied a earlier source:

Directions for Knowing All Dark Things ($\approx$ 1650 bce) (discovered in 2002).

Some people say Gauss gave the first full and correct proof in Disquisitiones Arithmeticae. (written 1798 when Gauss was 21, published in 1801)

Euclid's Elements ($\approx$ 300 bce) contains a proof. Three of the 13 books, VII, VIII and IX are about number theory. (But Euclid had no notation for the product of more than 3 numbers.)
Known to the Egyptian Ahmes ($\approx$ 1550 bce?) who copied a earlier source:
Directions for Knowing All Dark Things ($\approx$ 1650 bce) (discovered in 2002).
Some people say Gauss gave the first full and correct proof in Disquisitiones Arithmeticae. (written 1798 when Gauss was 21, published in 1801)

Proof

Existence:
By Strong induction:
Suppose n is first integer for which existence fails. Then n cannot be prime, so $n = mk$ with $m, k < n$. But both m and k are products of primes, so n is also a product of primes.

One Cryptography Method depends on it being very hard to find m and k

Uniqueness:
Euclid's lemma: If p is prime and $p|ab$, then $p|a$ or $p|q$.

Proof

Existence:
By Strong induction:
Suppose n is first integer for which existence fails. Then n cannot be prime, so $n = mk$ with $m, k < n$. But both m and k are products of primes, so n is also a product of primes.

One Cryptography Method depends on it being very hard to find m and k

Uniqueness:
Euclid's lemma: If p is prime and $p|ab$, then $p|a$ or $p|q$.

Proof

Existence:
By Strong induction:
Suppose n is first integer for which existence fails. Then n cannot be prime, so $n = mk$ with $m, k < n$. But both m and k are products of primes, so n is also a product of primes.

One Cryptography Method depends on it being very hard to find m and k

Uniqueness:
Euclid's lemma: If p is prime and $p|ab$, then $p|a$ or $p|q$.

Uniqueness Proof Cont

Suppose not:
find the smallest counterexample with

$$p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m$$

If follows that $p_i \neq q_j$,
or we could cancel from both sides yielding a smaller counterexample.
We can assume $p_1 < q_1$.
By Euclid's lemma $p_1 | q_j$ for some j.
Which implies q_j is not prime.
A contradiction, so there is no counterexample.

Uniqueness Proof Cont

Suppose not:
find the smallest counterexample with

$$p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m$$

If follows that $p_i \neq q_j$,
or we could cancel from both sides yielding a smaller counterexample.
We can assume $p_1 < q_1$.
By Euclid's lemma $p_1 | q_j$ for some j.
Which implies q_j is not prime.
A contradiction, so there is no counterexample.

Uniqueness Proof Cont

Suppose not:
find the smallest counterexample with

$$p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m$$

If follows that $p_i \neq q_j$,
or we could cancel from both sides yielding a smaller counterexample.
We can assume $p_1 < q_1$.
By Euclid's lemma $p_1 | q_j$ for some j.
Which implies q_j is not prime.
A contradiction, so there is no counterexample.

Uniqueness Proof Cont

Suppose not:
find the smallest counterexample with

$$p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m$$

If follows that $p_i \neq q_j$,
or we could cancel from both sides yielding a smaller counterexample.
We can assume $p_1 < q_1$.
By Euclid's lemma $p_1 | q_j$ for some j.
Which implies q_j is not prime.
A contradiction, so there is no counterexample.

Uniqueness Proof Cont

Suppose not:
find the smallest counterexample with

$$p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m$$

If follows that $p_i \neq q_j$,
or we could cancel from both sides yielding a smaller counterexample.
We can assume $p_1 < q_1$.
By Euclid's lemma $p_1 | q_j$ for some j.
Which implies q_j is not prime.
A contradiction, so there is no counterexample.

Uniqueness Proof Cont

Suppose not:
find the smallest counterexample with

$$p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m$$

If follows that $p_i \neq q_j$,
or we could cancel from both sides yielding a smaller counterexample.
We can assume $p_1 < q_1$.
By Euclid's lemma $p_1 | q_j$ for some j.
Which implies q_j is not prime.
A contradiction, so there is no counterexample.

Uniqueness Proof Cont

Suppose not:
find the smallest counterexample with

$$p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m$$

If follows that $p_i \neq q_j$,
or we could cancel from both sides yielding a smaller counterexample.
We can assume $p_1 < q_1$.
By Euclid's lemma $p_1 | q_j$ for some j.
Which implies q_j is not prime.
A contradiction, so there is no counterexample.

Fundamental Theorem of Calculus, Part I

- James Gregory (1638-1675) proved a restricted version
- Isaac Barrow (1630-1677) proved a general version, geometric proof without using limits.
- Isaac Newton (1643-1727) Barrow's student, developed limits and wanted to call the subject:
  the science of fluents and fluxions
- Gottfried Leibniz (1646-1716) developed limits and gave Calculus its name. Who won the calculus wars?

Fundamental Theorem of Calculus, Part I

- James Gregory (1638-1675) proved a restricted version
- Isaac Barrow (1630-1677) proved a general version, geometric proof without using limits.
- Isaac Newton (1643-1727) Barrow's student, developed limits and wanted to call the subject:
  the science of fluents and fluxions
- Gottfried Leibniz (1646-1716) developed limits and gave Calculus its name. Who won the calculus wars?

Fundamental Theorem of Calculus, Part I

- James Gregory (1638-1675) proved a restricted version
- Isaac Barrow (1630-1677) proved a general version, geometric proof without using limits.
- Isaac Newton (1643-1727) Barrow's student, developed limits and wanted to call the subject:
  the science of fluents and fluxions
- Gottfried Leibniz (1646-1716) developed limits and gave Calculus its name. Who won the calculus wars?

Fundamental Theorem of Calculus, Part I

- James Gregory (1638-1675) proved a restricted version
- Isaac Barrow (1630-1677) proved a general version, geometric proof without using limits.
- Isaac Newton (1643-1727) Barrow's student, developed limits and wanted to call the subject:
  the science of fluents and fluxions
- Gottfried Leibniz (1646-1716) developed limits and gave Calculus its name. Who won the calculus wars?

Fundamental Theorem of Calculus, Part I

- James Gregory (1638-1675) proved a restricted version
- Isaac Barrow (1630-1677) proved a general version, geometric proof without using limits.
- Isaac Newton (1643-1727) Barrow's student, developed limits and wanted to call the subject:
  the science of fluents and fluxions
- Gottfried Leibniz (1646-1716) developed limits and gave Calculus its name. Who won the calculus wars?

Fundamental Theorem of Calculus, Part 2

- Second part Fund Thm: If F is an anti-derivative of f then,

$$\int_a^b f(t)\,dt = F(b) - F(a)$$

(Newton-Leibniz Axiom)

- the 2nd part is stronger as f does not have to be continuous. $F(x) = x^2 \sin(1/x)$ and $F'(x) = f(x) = x \sin(1/x) - cos(1/x)$ but $F'(0) = 0$.
- Current textbooks use Riemann integration Riemann (1826-1866) was a student of Gauss.

Fundamental Theorem of Calculus, Part 2

- Second part Fund Thm: If F is an anti-derivative of f then,

$$\int_a^b f(t)\,dt = F(b) - F(a)$$

  (Newton-Leibniz Axiom)

- the 2nd part is stronger as f does not have to be continuous. $F(x) = x^2 \sin(1/x)$ and $F'(x) = f(x) = x \sin(1/x) - cos(1/x)$ but $F'(0) = 0$.
- Current textbooks use Riemann integration Riemann (1826-1866) was a student of Gauss.

Fundamental Theorem of Calculus, Part 2

- Second part Fund Thm: If F is an anti-derivative of f then,

$$\int_a^b f(t)\,dt = F(b) - F(a)$$

  (Newton-Leibniz Axiom)

- the 2nd part is stronger as f does not have to be continuous. $F(x) = x^2 \sin(1/x)$ and $F'(x) = f(x) = x \sin(1/x) - cos(1/x)$ but $F'(0) = 0$.
- Current textbooks use Riemann integration Riemann (1826-1866) was a student of Gauss.

Fundamental Theorem of Calculus, Part 2

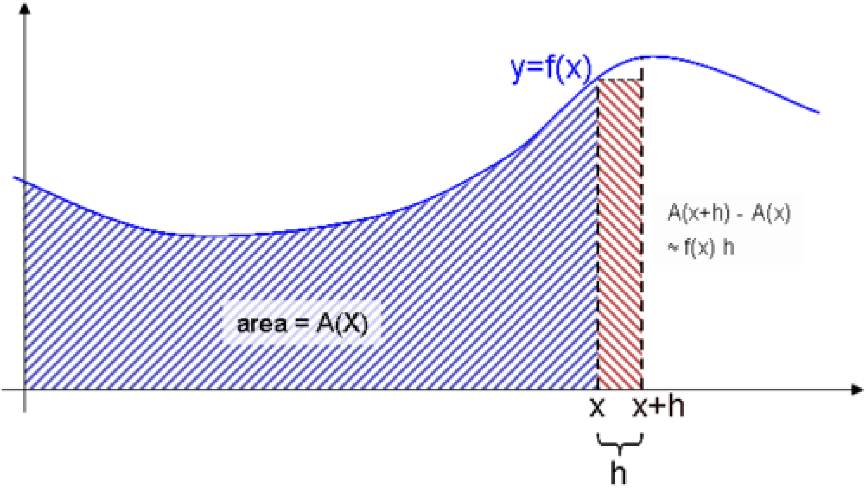
- Second part Fund Thm: If F is an anti-derivative of f then,

$$\int_a^b f(t)\,dt = F(b) - F(a)$$

(Newton-Leibniz Axiom)

- the 2nd part is stronger as f does not have to be continuous. $F(x) = x^2 \sin(1/x)$ and $F'(x) = f(x) = x \sin(1/x) - cos(1/x)$ but $F'(0) = 0$.
- Current textbooks use Riemann integration Riemann (1826-1866) was a student of Gauss.

Proof of Part I



Fundamental Theorem of Algebra

Every non-constant polynomial with complex coefficients has a complex root.

Known in some form to Rother 1608 (may have n solutions) and Girard 1629 (has n solutions, but not all polynomials). Many attempted proofs: D'Alembert 1746 Euler 1749, de Foncenex 1759, Lagrange 1772, Laplace 1795 assumed the existence of a root and then showed it was a complex number. Gauss 1799 gave a geometric proof in his PhD thesis. Argand 1806 and Gauss 1816 are rigorous by today's standards. Weierstrass 1891 gave a constructive proof.

Fundamental Theorem of Algebra

Every non-constant polynomial with complex coefficients has a complex root.
Known in some form to Rother 1608 (may have n solutions) and Girard 1629 (has n solutions, but not all polynomials).
Many attempted proofs: D'Alembert 1746 Euler 1749, de Foncenex 1759, Lagrange 1772, Laplace 1795 assumed the existence of a root and then showed it was a complex number.
Gauss 1799 gave a geometric proof in his PhD thesis. Argand 1806 and Gauss 1816 are rigorous by today's standards.
Weierstrass 1891 gave a constructive proof.

Every non-constant polynomial with complex coefficients has a complex root.
Known in some form to Rother 1608 (may have n solutions) and Girard 1629 (has n solutions, but not all polynomials).
Many attempted proofs: D'Alembert 1746 Euler 1749, de Foncenex 1759, Lagrange 1772, Laplace 1795 assumed the existence of a root and then showed it was a complex number.
Gauss 1799 gave a geometric proof in his PhD thesis. Argand 1806 and Gauss 1816 are rigorous by today's standards.
Weierstrass 1891 gave a constructive proof.

Fundamental Theorem of Algebra

Every non-constant polynomial with complex coefficients has a complex root.

Known in some form to Rother 1608 (may have n solutions) and Girard 1629 (has n solutions, but not all polynomials).

Many attempted proofs: D'Alembert 1746 Euler 1749, de Foncenex 1759, Lagrange 1772, Laplace 1795 assumed the existence of a root and then showed it was a complex number.

Gauss 1799 gave a geometric proof in his PhD thesis. Argand 1806 and Gauss 1816 are rigorous by today's standards.

Weierstrass 1891 gave a constructive proof.

Fundamental Theorem of Algebra

Every non-constant polynomial with complex coefficients has a complex root.
Known in some form to Rother 1608 (may have n solutions) and Girard 1629 (has n solutions, but not all polynomials).
Many attempted proofs: D'Alembert 1746 Euler 1749, de Foncenex 1759, Lagrange 1772, Laplace 1795 assumed the existence of a root and then showed it was a complex number.
Gauss 1799 gave a geometric proof in his PhD thesis. Argand 1806 and Gauss 1816 are rigorous by today's standards.
Weierstrass 1891 gave a constructive proof.

Neither Algebra nor Fundamental?

Almost all proofs require some analysis and the fastest proofs use analytic function theory. A proof must use the completeness of the reals.

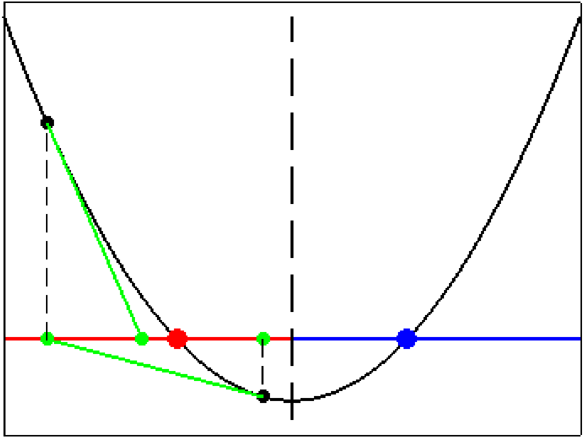
Nor is the theorem fundamental for modern algebra. There are other fundamental theorems in algebra: FT of Galois, FT on homomorphisms, FT of finitely generated abelian groups.

Neither Algebra nor Fundamental?

Almost all proofs require some analysis and the fastest proofs use analytic function theory. A proof must use the completeness of the reals.

Nor is the theorem fundamental for modern algebra. There are other fundamental theorems in algebra: FT of Galois, FT on homomorphisms, FT of finitely generated abelian groups.

Newton's Method



Constructive Proof

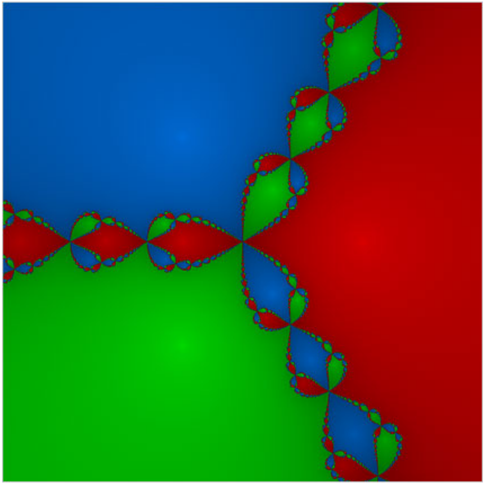
Start almost anywhere z_0 in the complex plane, repeat Newton's method

$$z_{n+1} = z_n - P(z_n)/P'(z_n)$$

and the sequence (z_n) will converge to a root of $P(z)$
If $P(z) = z^3 - 1$ with roots 1, $\exp(2\pi i/3) = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ and $\exp(-2\pi i/3) = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$, then

$$z_{n+1} = (2z_n^3 + 1)/3z_n^2$$

Degree 3 implies Chaos



Other Fundamental Theorems

Ordinary Differential Equations: one might call the existence and unqueness of solutions fundamental but we don't.

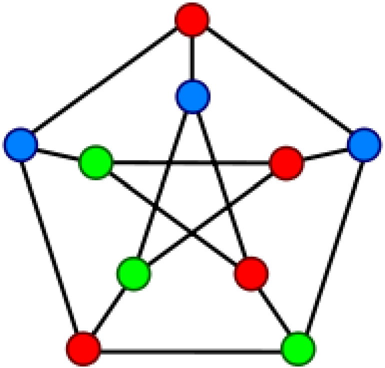
Strang (1993) declared a theorem to be the Fundamental Theorem of Linear Algebra.

Other Fundamental Theorems

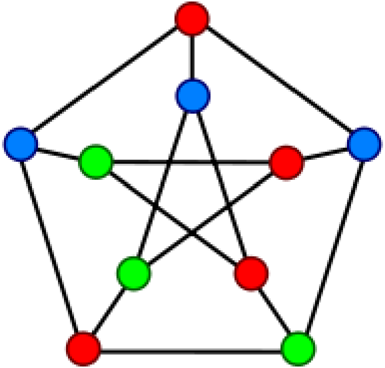
Ordinary Differential Equations: one might call the existence and unqueness of solutions fundamental but we don't.

Strang (1993) declared a theorem to be the Fundamental Theorem of Linear Algebra.

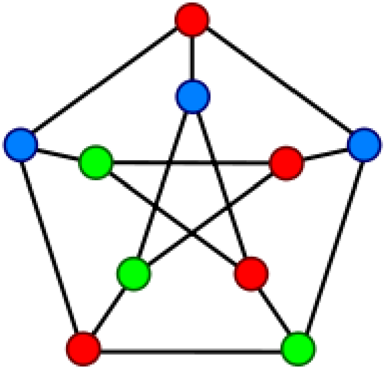
Graph Theory



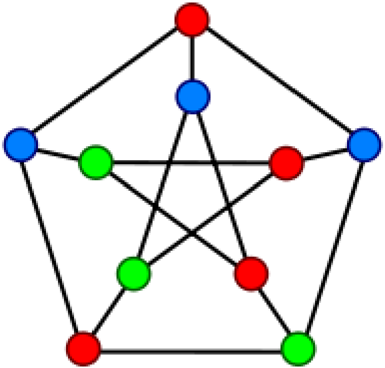
The color points are **vertices**, the connecting lines are are **edges**. The degree of a vertex is the number of incident edges. Here each vertex has degree 3. This graph is the Petersen graph, the figure shows it can be 3-colored, adjacent vertices have different colors. The web is just one big graph.



The color points are **vertices**, the connecting lines are are **edges.**The degree of a vertex is the number of incident edges. Here each vertex has degree 3. This graph is the Petersen graph, the figure shows it can be 3-colored, adjacent vertices have different colors. The web is just one big graph.



The color points are **vertices**, the connecting lines are are **edges.**The degree of a vertex is the number of incident edges. Here each vertex has degree 3. This graph is the Petersen graph, the figure shows it can be 3-colored, adjacent vertices have different colors. The web is just one big graph.



The color points are **vertices**, the connecting lines are are **edges.**The degree of a vertex is the number of incident edges. Here each vertex has degree 3. This graph is the Petersen graph, the figure shows it can be 3-colored, adjacent vertices have different colors. The web is just one big graph.

The Handshaking Lemma

$$\sum_{v \in V} deg(v) = 2|E|$$

The sum of the degrees of the vertices is equal to twice the number of edges.

Proof: (Euler 1736) double counting. Count (v, e) where v is incident to e, two ways. Vertex v belongs to $deg(v)$ pairs while edge e belongs to 2 pairs, one for each vertex.

This is the first paper on Graph Theory. It could easily be elected to being the fundamental theory of graph theory (or topology).

The Handshaking Lemma

$$\sum_{v \in V} deg(v) = 2|E|$$

The sum of the degrees of the vertices is equal to twice the number of edges.

Proof: (Euler 1736) double counting. Count (v, e) where v is incident to e, two ways. Vertex v belongs to $deg(v)$ pairs while edge e belongs to 2 pairs, one for each vertex.

This is the first paper on Graph Theory. It could easily be elected to being the fundamental theory of graph theory (or topology).

The Handshaking Lemma

$$\sum_{v \in V} deg(v) = 2|E|$$

The sum of the degrees of the vertices is equal to twice the number of edges.

Proof: (Euler 1736) double counting. Count (v, e) where v is incident to e, two ways. Vertex v belongs to $deg(v)$ pairs while edge e belongs to 2 pairs, one for each vertex.

This is the first paper on Graph Theory. It could easily be elected to being the fundamental theory of graph theory (or topology).

There is always an even number of odd vertices. (Proof: the RHS, $2|E|$ is even, the LHS would be odd if there were an odd number of vertices of odd degree.)

In a honor's ceremony, people shake hands, and an even number of people must have shaken an odd number of others peoples hands.

Where is Gauss?

The Handshaking Lemma

There is always an even number of odd vertices. (Proof: the RHS, $2|E|$ is even, the LHS would be odd if there were an odd number of vertices of odd degree.)

In a honor's ceremony, people shake hands, and an even number of people must have shaken an odd number of others peoples hands.

Where is Gauss?

The Handshaking Lemma

There is always an even number of odd vertices. (Proof: the RHS, $2|E|$ is even, the LHS would be odd if there were an odd number of vertices of odd degree.)

In a honor's ceremony, people shake hands, and an even number of people must have shaken an odd number of others peoples hands.

Where is Gauss?

The Handshaking Lemma

There is always an even number of odd vertices. (Proof: the RHS, $2|E|$ is even, the LHS would be odd if there were an odd number of vertices of odd degree.)

In a honor's ceremony, people shake hands, and an even number of people must have shaken an odd number of others peoples hands.

Where is Gauss?

PhD Defenses

1. SF Bellenot
2. RC James (one of two advisors)
3. AD Michal
4. M Bocher
5. Felix Klein
6. J Plucker (one of two advisors)
7. CL Gerling
8. **Gauss**

PhD Defenses

1. SF Bellenot
2. RC James (one of two advisors)
3. AD Michal
4. M Bocher
5. Felix Klein
6. J Plucker (one of two advisors)
7. CL Gerling
8. **Gauss**

PhD Defenses

1. SF Bellenot
2. RC James (one of two advisors)
3. AD Michal
4. M Bocher
5. Felix Klein
6. J Plucker (one of two advisors)
7. CL Gerling
8. **Gauss**

PhD Defenses

1. SF Bellenot
2. RC James (one of two advisors)
3. AD Michal
4. M Bocher
5. Felix Klein
6. J Plucker (one of two advisors)
7. CL Gerling
8. **Gauss**

1. SF Bellenot
2. Melvin Henriksen (Chairman of HMC) in 1960's
3. Artur Rosenthal in the 1950's
4. Richard Dedekind around 1909
5. **Gauss** – Dedekind's major professor 1851

Just Handshakes

1. SF Bellenot
2. Melvin Henriksen (Chairman of HMC) in 1960's
3. Artur Rosenthal in the 1950's
4. Richard Dedekind around 1909
5. **Gauss** – Dedekind's major professor 1851

Just Handshakes

1. SF Bellenot
2. Melvin Henriksen (Chairman of HMC) in 1960's
3. Artur Rosenthal in the 1950's
4. Richard Dedekind around 1909
5. **Gauss** – Dedekind's major professor 1851