CO 480 Lecture 19

Adrien-Marie Legendre

July 11th, 2017

July 11th...

1686 - Leibniz published his work on the Fundamental Theorem of Calculus in the scientific journal Acta eruditorum.

1700 - Prince Elector Frederick I signed into being the Brandenburg Electorate Society of Sciences (later the Royal Prussian Society) and named Gottfried Leibniz its President for life. Exists today as the Berlin-Brandenburg Academy of Sciences and Humanities.

Final Comment on Sophie Germain

- Sophie Germain did have a grand plan to prove Fermat's Last Theorem which basically amounted to showing that the variables x, y, z had infinitely many primes.
- This plan sadly never materialized. In fact Libri showed that if $x^n + y^n + z^n \equiv 0 \mod p$, then for p sufficiently large, this will always have solutions [Dic17].

Today: Adrien-Marie Legendre

- "All the truths of mathematics are linked to each other, and all means of discovering them are equally admissible." (Legendre) https://www.goodreads.com/author/quotes/7309675.Adrien_Marie_Legendre
- "Our colleague has often expressed the desire that, in speaking of him, it would only be the matter of his works, which are, in fact, his entire life" [OR].

(Wikimedia Commons)

Controversy with Picture

- Many sources including [Bur91] and [Smi58] do not have the correct picture of Legendre.
- In 2009, [Dur09] noted that the picture often associated with Legendre is actually a Politician named Louis Legendre!
- Even his name is spelt differently than written (he usually wrote Le Gendre)

he is known chiefly for his geometry,[1] a work which had a generous reception in various countries and which justly ranks as one of the best textbooks ever written upon the subject. In it he sought to rearrange the propositions of Euclid, separating the theorems from the problems and simplifying the proofs, without lessening the rigor of the ancient methods of treatment. To Legendre is largely due the abandoning of Euclid as a textbook in American schools.

ADRIEN-MARIE LEGENDRE
After a lithograph by Delpech

In higher mathematics Legendre is known for his works on the theory of numbers[2] and on elliptic functions.[3] He is also known for his treatises on the calculus, higher geometry, mechanics, astronomy, and physics. To him is due the first satisfactory treatment of the method of least squares,[4] although Gauss had already discovered the method. In his theory of numbers appears the law of quadratic reciprocity which Gauss called the "gem of arithmetic." The treatise on elliptic functions appeared almost simultaneously with the works by Abel and Jacobi on the same subjects; and although Legendre had spent thirty years on the theory, he

Picture

Figure 2. L. Legendre pictured with Montagnards (lower left and inset).

Wikipedia Wars

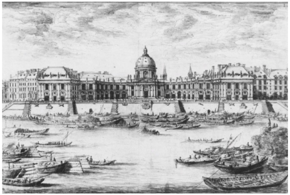
	Date/Time	Thumbnail	Dimensions	User	Comment
current	**07:21, 8 November 2010**		160 × 200 (7 KB)	MER-C (talk I contribs)	w:Adrien-Marie Legendre#Portrait debacle
	11:57, 29 October 2010		363 × 450 (26 KB)	Deevrod (talk I contribs)	Reverted to version as of 21:59, 4 March 2009 (rvv vandalism)
	09:31, 14 November 2009		160 × 200 (7 KB)	Pieter Kuiper (talk I contribs)	This is the real A-M Legendre
	21:59, 4 March 2009		363 × 450 (26 KB)	RayAYang (talk I contribs)	{{Information IDescription= {{enI1=Adrien-Marie Legendre (1752-1833), French mathematician}} ISource=Bibliotheque Nationale, Paris IAuthor=lithograph by F.-S. Delpech after a portrait by Z. Belliard IDate=19th century IPermission= Iother_versions= }} <!--

Life of Legendre

- Never wanted much if anything written about himself. Cared more for his work.
- Born September 18th, 1752.
- Believed to be born in Paris [Wei84, p.322], though Ball claims Toulouse [Bal60, p. 346] but is the only reference of such a claim and [OR] suggests that he might have been born in Toulouse and then moved to Paris where he lived most of his life.
- Died January 10th, 1833 in Paris.
- Not much is known of his childhood though he was born to a rich family

Legendre's Life

- Throughout his life, Legendre wanted little mention of himself.
- In his 1798 Essai, "It appears… that Euler had a special inclination towards such investigations and that he took them up with a kind of passionate addiction, as happens to nearly all those who concern themselves with them" [Wei84, p.325].
- Born to a wealthy family and given exceptional education in mathematics and physics.
- Legendre studied at the Collège Mazarin (aka Collège des Quatre-Nations) in Paris where he defended his thesis [more of a plan of research] at age 18.



Etching by Israel Silvestre, circa 1670 (Wikipedia Commons).

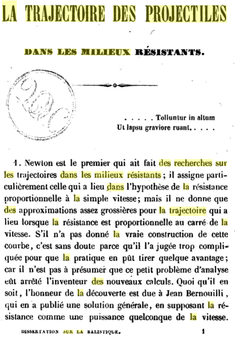
Notes on Collège Mazarin

- Opened in 1688
- Funded by estate of Cardinal Mazarin (died in 1661)
- Named the College of four nations for the distribution of students as desired to be included by Mazarin.
- Notable students: d'Alembert, chemist Lavoisier, Legendre.

Legendre Wealth

- From sources [OR][Wei84], it is clear that Legendre didn't need work and could focus primarily on his research in his early years.
- He held a teaching position at the Ècole Militaire from 1775-1780 [Wei84, p. 324]. (Laplace was also there teaching).
- Following this he took 2 years off to study [Bur91, p. 571].
- In 1782, Legendre submitted to the Berlin Academy of Science, and won, a prize for his submission on the problem of describing the path taken by cannonballs and bombs [oEB].

Recherches sur la trajectoire des projectiles dans les milieux rsistants



LA TRAJECTOIRE DES PROJECTILES

DANS LES MILIEUX RÉSISTANTS.

. . . . . Tolluntur in altum
Ut lapsu graviore ruant. . . . .

1. Newton est le premier qui ait fait des recherches sur les trajectoires dans les milieux résistants; il assigne particulièrement celle qui a lieu dans l'hypothèse de la résistance proportionnelle à la simple vitesse; mais il ne donne que des approximations assez grossières pour la trajectoire qui a lieu lorsque la résistance est proportionnelle au carré de la vitesse. S'il n'a pas donné la vraie construction de cette courbe, c'est sans doute parce qu'il l'a jugée trop compliquée pour que la pratique en pût tirer quelque avantage; car il n'est pas à présumer que ce petit problème d'analyse eût arrêté l'inventeur des nouveaux calculs. Quoi qu'il en soit, l'honneur de la découverte est due à Jean Bernouilli, qui en a publié une solution générale, en supposant la résistance comme une puissance quelconque de la vitesse.

DISSERTATION SUR LA BALISTIQUE. 1

Legendre's Career Starts to Blossom

- Lagrange who was the Berlin Academy mailed Laplace for more information on the young Legendre [OR] [Wei84, p. 324].
- The Académie des Science made Legendre an adjoint member in 1783 [oEB] and an adjunct in 1785 [Wei84, p. 324-325].
- Was a fellow in the Royal Society and was part of a committee int he early 1790s that eventually established the metric system [Wei84, p. 325].

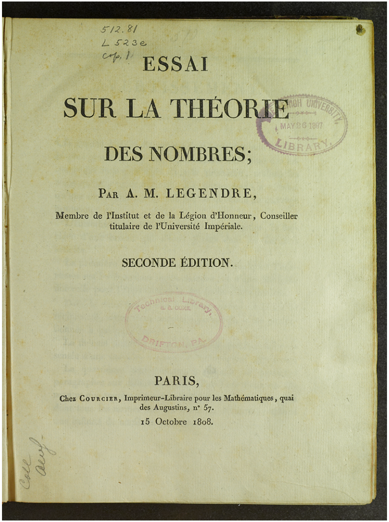
Middle Years

- Legendre was around his 40s when the French Revolution (1787-1794) was taking place.
- The Revolution was not kind to Legendre and he managed to lose most of his family's wealth during this time [oEB].
- Still, Legendre married Marguerite-Claudine Couhin in 1793 who helped straighten out his life. (Note: all academies were closed in 1793).
- As mentioned last week, Legendre was an *examinateur* for École Polytechnique from 1799-1815.

Work in Number Theory

- In 1785, Legendre produced his first work in number theory, a 134 page essay titled *Recherches d'analyse indéterminée* [Wei84, p. 326].
- Note: By this point, Euler was dead and Lagrange was no longer working on number theory; Gauss claimed it was "an excellent memoir" [Wei84, p. 326]
- His celebrated work was in 1798 called *Essai Sur le Théorie des Nombres*

Book - Essai Sur le Théorie des Nombres


512.81
L523e
cop.1

ESSAI

SUR LA THÉORIE

DES NOMBRES;

PAR A. M. LEGENDRE,

Membre de l'Institut et de la Légion d'Honneur, Conseiller titulaire de l'Université Impériale.

SECONDE ÉDITION.

PARIS,

Chez COURCIER, Imprimeur-Libraire pour les Mathématiques, quai des Augustins, n° 57.

15 Octobre 1808.

Legendre Symbol

- One of the highlights of the book was the invention and the first use of the Legendre symbol.
- Throughout, let p be an odd prime.
- Note that for nonzero a, if $x^2 \equiv a \mod p$, we say that a is a *quadratic residue* and otherwise, we say a is a *quadratic non-residue*.
- In class, we mentioned that $a^{(p-1)/2}$ is equivalent to 0 or ± 1 when reduced modulo p.
- It is cumbersome when you want to talk about the values as obtained from the previous theorem.
- Legendre decided to invent a new notation that would help to quickly represent the idea as expressed here.

Definition of the Legendre Symbol

Legendre Symbol

Let p be an odd prime number and a an integer. The *Legendre symbol* is a function of a and p defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \text{ and } p \nmid a, \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p, \\ 0 & \text{if } a \equiv 0 \pmod{p}. \end{cases}$$

Properties

- The Legendre symbol is multiplicative and in fact it is a completely multiplicative function. That is, if a and b are integers then $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.
- Translated, if $x^2 \equiv a \mod p$ has a solution and $x^2 \equiv b \mod p$ has a solution, then $x^2 \equiv ab \mod p$ also has a solution.
- Further, if exactly one of the above doesn't have a solution, then the third of the group also doesn't have a solution.
- However, if $x^2 \equiv a \mod p$ does not have a solution and $x^2 \equiv b \mod p$ does not have a solution, then $x^2 \equiv ab \mod p$ **does** have a solution!
- If $a \equiv b \mod p$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
- For an integer a coprime with p, $\left(\frac{a^2}{p}\right) = 1$.

Evaluating some values

Determine the value of $\binom{12}{5}$.

Evaluating some values

Determine the value of $\left(\frac{12}{5}\right)$.

Solution: Notice that $\left(\frac{12}{5}\right) = \left(\frac{2}{5}\right)$ and the squares modulo 5 are $0, 1$ and 4. Since 2 is not a quadratic residue, we have that $\left(\frac{2}{5}\right) = -1$.

Reframing Euler's Criterion

Recall Euler's Criterion:

Euler's Criterion

Let a be an integer not divisible by a prime p. If there is a solution to $x^2 \equiv a \mod p$ then $a^{(p-1)/2} \equiv 1 \mod p$. Also, if $x^2 \equiv a \mod p$ does not have a solution then $a^{(p-1)/2} \equiv -1 \mod p$.

Reframing Euler's Criterion

Recall Euler's Criterion:

Euler's Criterion

Let a be an integer not divisible by a prime p. If there is a solution to $x^2 \equiv a \mod p$ then $a^{(p-1)/2} \equiv 1 \mod p$. Also, if $x^2 \equiv a \mod p$ does not have a solution then $a^{(p-1)/2} \equiv -1 \mod p$.

We can reframe this as:

Euler's Criterion

Let p be an odd prime and a an integer. Then

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \mod p.$$

Note: You can use this to prove the multiplicative nature of the Legendre symbol.

Another example

Determine the value of $\left(\frac{-1}{17}\right)$.

Another example

Determine the value of $\left(\frac{-1}{17}\right)$.

Solution: From Euler's Criterion, it suffices to evaluate $(-1)^{(17-1)/2} = (-1)^8 = 1$.

Exploratory Question Part 1

Examine when the following equations are solvable. Can you make any conjectures about $\left(\frac{-1}{p}\right)$?

$$x^2 \equiv -1 \mod 3$$
$$x^2 \equiv -1 \mod 5$$
$$x^2 \equiv -1 \mod 7$$
$$x^2 \equiv -1 \mod 11$$
$$x^2 \equiv -1 \mod 13$$
$$x^2 \equiv -1 \mod 17$$

The Value $\left(\frac{-1}{p}\right)$

The Legendre Symbol $\left(\frac{-1}{p}\right)$

For an odd prime p, $\left(\frac{-1}{p}\right) = 1$ if and only if $p \equiv 1 \mod 4$.

The Value $\left(\frac{-1}{p}\right)$

The Legendre Symbol $\left(\frac{-1}{p}\right)$

For an odd prime p, $\left(\frac{-1}{p}\right) = 1$ if and only if $p \equiv 1 \mod 4$.

Proof By Euler's Criterion,

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{if } p \equiv 1 \mod 4 \\ -1 & \text{if } p \equiv 3 \mod 4 \end{cases}$$

Exploratory Question Part 2

Examine when the following equations are solvable. Can you make any conjectures about $\left(\frac{2}{p}\right)$? (Hint: Modulo 4 isn't enough this time!)

$$x^2 \equiv 2 \mod 3$$
$$x^2 \equiv 2 \mod 5$$
$$x^2 \equiv 2 \mod 7$$
$$x^2 \equiv 2 \mod 11$$
$$x^2 \equiv 2 \mod 13$$
$$x^2 \equiv 2 \mod 17$$
$$x^2 \equiv 2 \mod 19$$
$$x^2 \equiv 2 \mod 23$$
$$x^2 \equiv 2 \mod 29$$
$$x^2 \equiv 2 \mod 31$$

The Value $\left(\frac{2}{p}\right)$

The Legendre Symbol $\left(\frac{2}{p}\right)$

For an odd prime p, $\left(\frac{2}{p}\right) = 1$ if and only if $p \equiv 1 \mod 8$ or $p \equiv 7 \mod 8$.

The Value $\left(\frac{2}{p}\right)$

The Legendre Symbol $\left(\frac{2}{p}\right)$

For an odd prime p, $\left(\frac{2}{p}\right) = 1$ if and only if $p \equiv 1 \mod 8$ or $p \equiv 7 \mod 8$.

Proof Notice that Euler's Criterion alone isn't going to work in this case because $2^{(p-1)/2}$ is complicated to evaluate modulo p.

Proof Continued

Do an example with $p = 11$.

Proof Continued

Do an example with $p = 11$.

Idea: Look at the product of even numbers $2 \cdot 4 \cdot ... \cdot (p-1)$. This is

$$2 \cdot 4 \cdot ... \cdot (p-1) = 2^{(p-1)/2}(1)(2)...((p-1)/2) = 2^{(p-1)/2}(\frac{p-1}{2})!$$

Left Hand Side Simplification

$$2 \cdot 4 \cdot ... \cdot (p-1) = 2^{(p-1)/2}(1)(2)...((p-1)/2) = 2^{(p-1)/2}(\tfrac{p-1}{2})!$$

Now, change the left hand side so that all the values are between $-(p-1)/2+1$ and $(p-1)/2$. For example,

$$\begin{aligned} p-1 &\equiv -1 \mod p \\ p-3 &\equiv -3 \mod p \\ &\vdots \\ p-k &\equiv -k \mod p \end{aligned}$$

This, the left hand side is also

$$2 \cdot 4 \cdot ... \cdot (p-1) \equiv (-1)^k (\tfrac{p-1}{2})!$$

for some positive integer k, the number of numbers we flipped above.

Number of Flips

We flipped once for each of the even numbers from $p-k$ to $p-1$ where k is the odd integer satisfying:

$$\frac{p-1}{2} \leq k \leq \frac{p-1}{2} + 1$$

The above value is $k = \frac{p-1}{2} + 1$ when $1 + 4\ell$ for some integer ℓ giving $\frac{p-1}{4} = \ell$ total flips and $k = \frac{p-1}{2}$ when $p = 3 + 4\ell$ for some integer ℓ giving $\frac{k+1}{2} = \ell + 1$ number of flips.

Hence

Thus, the value of $(-1)^k$ is 1 if k is even and -1 if k is odd.

When $p = 1 + 4\ell$, the total number of flips is ℓ meaning $\left(\frac{2}{p}\right) = 1$ when $p = 1 + 4\ell$ with ℓ even (ie when $p \equiv 1 \mod 8$) and $\left(\frac{2}{p}\right) = -1$ when $p = 1 + 4\ell$ with ℓ odd (ie when $p \equiv 5 \mod 8$).

When $p = 3 + 4\ell$, the total number of flips is $\ell + 1$ meaning $\left(\frac{2}{p}\right) = 1$ when $p = 3 + 4\ell$ with ℓ odd (ie when $p \equiv 7 \mod 8$) and $\left(\frac{2}{p}\right) = -1$ when $p = 3 + 4\ell$ with ℓ even (ie when $p \equiv 3 \mod 8$).

This completes the proof.

Exploratory Question Part 3

Examine when the following equations are solvable. Can you make any conjectures about the relationships between $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$?

$$x^2 \equiv 3 \mod 5$$
$$x^2 \equiv 5 \mod 3$$
$$x^2 \equiv 3 \mod 7$$
$$x^2 \equiv 7 \mod 3$$
$$x^2 \equiv 7 \mod 5$$
$$x^2 \equiv 5 \mod 7$$
$$x^2 \equiv 5 \mod 13$$
$$x^2 \equiv 13 \mod 5$$

Quadratic Reciprocity

Quadratic Reciprocity

Let p and q be two odd primes. Then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)/2 \cdot (q-1)/2}$$

Quadratic Reciprocity

- Euler conjectures this result and Legendre attempted a proof in his book *Théorie des Nombres* [Leg09, p. 214-226].
- Proof was corrected by Gauss in his book *Disquisitiones Arithmeticae* (See section 4, particularly around pages 88-89 in [Gau86]).
- Gauss also mentions why Legendre's proof is inadequate [Gau86, p. 104-106, 349-352, Art. 151, 296, 297]
- The key missing fact is that in a given arithmetic progression (under mild conditions), there exists infinitely many primes, a result first proved by Dirichlet in 1837. (Legendre needed there to be one prime in any AP not necessarily infinitely many).

Quadratic Reciprocity

Of the cases Legendre did prove, he used the following theorem which he derived from case work using infinite descent(!)

Legendre's Theorem

Let a, b, c be three integers not all of the same sign and such that abc is a squarefree integer. Then the equation

$$ax^2 + by^2 + cz^2 = 0$$

has a solution in integers x, y and z not all 0 if and only if $-bc$, $-ca$ and $-ab$ are all quadratic residues modulo $|a|$, $|b|$ and $|c|$ respectively.

Legendre and Fermat's Last Theorem

- We've already discussed Sophie Germain's work on FLT for exponents less than 100.
- Legendre extended her work to include all primes less than 200 (so that $x^n + y^n = z^n$ has a solution implies that n divides the variables).
- On July 11th, 1825, Dirichlet presented a proof to deal with $n = 5$ using arithmetic in $\mathbb{Q}(\sqrt{5})$. The proof work if 10 divided one of the variables.
- Legendre in September of 1825, after reading this proof resolved the final case when 5 divided one of the variables and 2 divided the other. (Legendre needed two separate cases).
- Dirichlet eventually unified the two subcases sometime after September 1825.

Legendre and the Prime Number Theorem

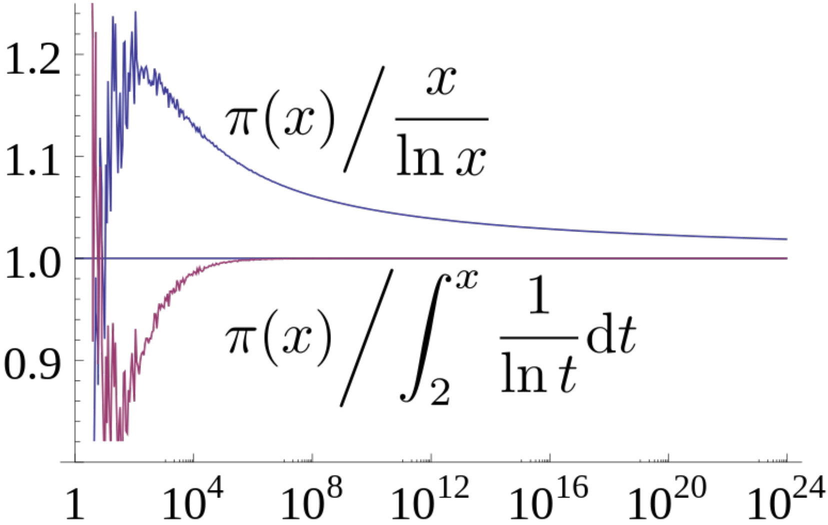
Legendre conjectured that the number of primes less than x (often denoted by $\pi(x)$) is roughly well approximated for $x \leq 10^6$ by [Leg09]

$$\pi(x) \approx \frac{x}{\log x - 1.08366}$$

With this guess being vastly improved by Gauss later:

$$\pi(x) \approx \int_2^x \frac{dt}{\log t}$$

Prime Number Theorem



Other Works of Legendre

- He spend a large deal of time studying elliptic integrals in 1786 (the foundation of modern day elliptic curves) [oEB].
- He also spent time as many of his predecessors on celestial mechanics.
- Legendre's work *Eléments de géomeétrie* in 1795 was one of the best sellers in France, selling over 100,000 copies [Bur91, p.575].
- One of his goals was to try to prove the parallel postulate (which we now consider to be an axiom).

Final Days

- In 1824, Legendre refused to support the government's candidate for the National Institute resulting in a loss of pension and final years of poverty.
- Died on January 10th, 1833.
- He and his wife are buried in the village of Auteuil. Left estate to the village.
- His name is one of the 72 scientists etched in the Eiffel Tower (see below).

References I

W. W. Rouse Ball, *A short account of the history of mathematics*, Dover Publications, Inc., New York, 1960. MR 0112798

David M. Burton, *The history of mathematics*, second ed., W. C. Brown Publishers, Dubuque, IA, 1991, An introduction. MR 1223776

L. E. Dickson, *Fermat's last theorem and the origin and nature of the theory of algebraic numbers*, Ann. of Math. (2) **18** (1917), no. 4, 161–187. MR 1503597

Peter Duren, *Changing faces: the mistaken portrait of Legendre*, Notices Amer. Math. Soc. **56** (2009), no. 11, 1440–1443. MR 2590729

Carl Friedrich Gauss, *Disquisitiones arithmeticae*, Springer-Verlag, New York, 1986, Translated and with a preface by Arthur A. Clarke, Revised by William C. Waterhouse, Cornelius Greither and A. W. Grootendorst and with a preface by Waterhouse. MR 837656

Adrien-Marie Legendre, *Essai sur la théorie des nombres*, Cambridge Library Collection, Cambridge University Press, Cambridge, 2009, Reprint of the second (1808) edition. MR 2859036

References II

The Editors of Encyclopaedia Britannica, *Adrien-marie legendre*, https://www.britannica.com/print/article/334981, visited 2017-06-28.

J. J. O'Connor and E.F. Robertson, *Adrien-marie legendre*, http://www-groups.dcs.st-and.ac.uk/~history/Biographies/Legendre.html, visited 2017-06-28.

David Eugene Smith, *History of mathematics. Vol. I. General survey of the history of elementary mathematics*, Dover Publications, Inc., New York, N. Y., 1958. MR 0091896

André Weil, *Number theory*, Birkhäuser Boston, Inc., Boston, MA, 1984, An approach through history, From Hammurapi to Legendre. MR 734177