Fermat の最終定理と楕円曲線　関連年表

	Fermat の最終定理	楕円曲線ほか
1637 頃?	Fermat　余白書き込み	
1659 以前	Fermat　4 次の場合	$y^2 = x^3 - x$
1749		Euler　$\zeta(1-k)$ の値
1753	Euler　3 次の場合	$x^3 + y^3 = 1$
1757		Euler　楕円積分の加法公式
1796		Gauss　正 17 角形の作図
1797		Gauss　レムニスケートの等分
1800		Gauss　j 不変量
1825	Legendre　5 次の場合	
1825		Abel　5 次方程式の非可解性
1827		Abel　楕円関数論
1832		Galois　Galois 理論
1850	Kummer　円分体	
1857		Riemann　Riemann 面
1859		Riemann　ζ 関数
		Eisenstein　Eisenstein 級数
		Kronecker　合同関係式
		Weierstrass　$\wp$ 関数
1877		Dedekind　楕円モジュラー関数
1914		Mordell　有限生成
1937		Hecke　Hecke 作用素
1930?-52		Hasse-Weil　L 関数
1955-64?		谷山・志村　楕円曲線の保型性
1963?		Birch−Swinnerton-Dyer　BSD 予想
1977		Mazur　等分点
1983		Faltings　Mordell 予想
1986	Frey　Frey 曲線	$y^2 = x(x - a^\ell)(x - b^\ell)$
1987	Ribet　Fermat の最終定理を	谷山・志村予想に帰着
1994	Wiles(-Taylor) 証明	
1999		Breuil-Conrad-Diamond-Taylor
		谷山・志村予想を証明

参考文献

フェルマーの最終定理

[1] 足立 恒雄、フェルマーの大定理が解けた！、講談社ブルーバックス、1995.

[2] 加藤 和也、解決！フェルマーの最終定理、日本評論社、1995.

[3] サイモン・シン、フェルマーの最終定理　(青木薫訳)、新潮社、2000.

数学史

[4] 高木 貞治、近世数学史談、岩波文庫 青 939-1、1995.

[5] F. クライン、19 世紀の数学　(石井省吾・渡辺 弘訳)、共立出版、1995.

[6] アンドレ・ヴェイユ、数論　歴史からのアプローチ　(足立 恒雄・三宅克哉訳)、日本評論社、1987.

入門書

[7] 藤崎源二郎・森田康夫・山本芳彦、数論への出発（増補版)、日本評論社、2004.

[8] 加藤 和也・黒川 信重・斎藤 毅、数論 I　Fermat の夢と類体論，岩波書店、2005.

[9] 森田康夫、整数論、東京大学出版会、1999.

[10] J. シルバーマン-J. テイト，楕円曲線論入門 (足立恒雄、木田雅成、小松啓一、田谷久雄 訳) シュプリンガー・フェアラーク東京. 1995.

専門書

[11] J.-P. セール、数論講義（彌永 健一訳)，岩波書店、1979.

[12] 岩澤 健吉、代数函数論　増補版，岩波書店、1973.

[13] 斎藤 毅、Fermat 予想１，岩波講座　現代数学の展開、2000，同２，近刊予定.

http://www.ms.u-tokyo.ac.jp/~t-saito/ce/surijoho.pdf
http://faculty.ms.u-tokyo.ac.jp/users/surijoho/

Fermat の最終定理

n を 3 以上の整数とする．方程式 $x^n + y^n = z^n$ の整数解 $(x, y, z) = (a, b, c)$ は，自明なものしかない．つまり，a, b, c のどれかは 0 であるものしかない．

n が 4 の場合と，3 以上の素数 ℓ の場合とに帰着される．

楕円曲線

方程式 $y^2 = x^3 + ax + b$ で定義される曲線．ただし，右辺の 3 次式は重根をもたない，つまり $4a^3 + 27b^2 \neq 0$.

Fermat

$y^2 = x^3 - x$ の解は $(x, y) = (0, 1), (\pm 1, 1)$ しかない．これから n が 4 の場合がしたがう．

Euler

$n = 3$ の場合を証明.

曲線 $y^2 = x^3 - x$ や，$x^3 + y^3 = 1$ は楕円曲線.

Gauss

$\cos \dfrac{2\pi}{17}, \sin \dfrac{2\pi}{17}$ は，2 次方程式を解く操作を 4 回繰り返すことによって得られる．

逆三角関数　弧の長さ

$$\mathrm{Arcsin} x = \int_0^x \frac{1}{\sqrt{1 - x^2}} dx.$$

曲線 $x^2 + y^2 = 1$ のパラメータ表示 $(x, y) = (\cos\theta, \sin\theta)$.

レムニスケート $(x^2 + y^2)^2 = 2(x^2 - y^2)$ の弧の長さ：楕円積分

$$\int_0^x \frac{1}{\sqrt{1 - x^4}} dx.$$

楕円曲線 $x^4 + y^2 = 1$ のパラメータ表示.

レムニスケートの 5 等分点の座標は，2 次方程式を解く操作を繰り返すことで得られる．

楕円曲線の加法：$P, Q \in E$ をむすぶ直線と E の第 3 の交点 R をとり，それの x 軸に関して対称な点を $P + Q$ とおく．

Abel

一般の 5 次方程式には，根号を開く操作を何度繰り返しても解けないものがある．

Galois

一般の方程式が解けるかどうかは，その方程式の Galois 群で判定できる．

Kummer

方程式 $x^n + y^n = z^n$ を $(x + y)(x + \zeta y)(x + \zeta^2 y) \cdots (x + \zeta^{n-1} y) = z^n$ とみて，2 通りの分解と考える．素因数分解がなりたたないことに基づく困難を研究.

素数 $\ell \geq 3$ が Bernoulli 数 $B_k, (1 \leq k \leq \ell - 3, \text{偶数})$ の分子をわらなければ，その ℓ について Fermat の最終定理がなりたつ．Bernoulli 数 B_r は

$$\frac{x}{e^x - 1} = \sum_{r=0}^{\infty} \frac{B_r}{r!} x^r$$

で定まる有理数.

Mordell

$E(\mathbb{Q})$ は有限生成 Abel 群をなす．$E(\mathbb{Q})$ の有限個の元 $P_1, \ldots, P_n$ で，$E(\mathbb{Q})$ の任意の元 P が $P_1, \ldots, P_n$ に加法を繰り返すことで得られるようなものがある．

Mordell 予想：種数が 2 以上の代数曲線 X の有理点は有限個しかない。1983 年 Faltings が証明.

Frey

$x^\ell + y^\ell = z^\ell$ の整数解 $(x, y, z) = (a, b, c)$ があったとして，楕円曲線 $y^2 = x(x - a^\ell)(x - b^\ell)$ を考え、この楕円曲線が異常な性質をもつことを示す.

谷山・志村

有理数係数の方程式で定義される楕円曲線は，L 関数を通じて，保型形式と結びついている.

Hasse-Weil

楕円曲線の L 関数．$E : y^2 = x^3 + ax + b,\ (a, b \in \mathbb{Z})$ 楕円曲線．$p \nmid 2(4a^3 + 27b^2)$：素数．$E(\mathbb{F}_p) = \{(x, y) | y^2 \equiv x^3 + ax + b \bmod p\}$ に一点 O を付け加えたもの．$a_p(E) = p + 1 - \sharp E(\mathbb{F}_p)$ とおく.

$$L(E, s) = \prod_p (1 - a_p(E)p^{-s} + p^{1-2s})^{-1} \times \cdots.$$

Re $s > \frac{3}{2}$ で絶対収束.

志村・谷山予想.

$L(E, s) = \sum_{n=1}^{\infty} a_n n^{-s}$ とおくと，巾級数 $\sum_{n=0}^{\infty} a_n q^n$ は保型形式である.

志村・谷山予想 $\Rightarrow$ $L(E, s)$ は s の整関数.

Riemann

Riemann ゼータ関数．素数分布.

$$\zeta(s) = \prod_p (1 - p^{-s})^{-1} = \sum_{n=1} \frac{1}{n^s}.$$

Riemann 面．楕円積分 $\int \frac{dx}{\sqrt{f(x)}}$ の逆関数を，複素平面の 2 重被覆面 $y^2 = f(x)$ のパラメータ表示として考察.

保型形式

巾級数 $\sum_{n=0}^{\infty} a_n q^n$ で，保型性とよばれるある条件をみたすもの.

例：$\Delta(q) = q \prod_{n=1}^{\infty} (1 - q^n)^{24}$.　$f_{11}(q) = q \prod_n (1 - q^n)^2 (1 - q^{11n})^2$.

Eisenstein 級数：$k \geq 2$　偶数

$$E_k(q) = 1 + \frac{2}{\zeta(1 - k)} \sum_n \sigma_{k-1}(n) q^n.$$

$\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}$. $\zeta(1-k) = -\dfrac{B_r}{r}$,

$$\zeta(-1) = -\frac{1}{12}, \quad \zeta(-3) = \frac{1}{120}, \quad \zeta(-5) = -\frac{1}{252}, \dots$$

$$\Delta = \left(\frac{1}{12}E_4\right)^3 - \left(\frac{1}{216}E_6\right)^2$$

右辺は 3 次式 $4x^3 - \dfrac{1}{12}E_4 x + \dfrac{1}{216}E_6$ の判別式.

$$G_k(\tau) = \sum_{(n,m)\neq(0,0)} \frac{1}{(n+m\tau)^k}$$

$k \geq 4$　偶数とすると,

$$G_k(\tau) = \frac{(2\pi i)^k}{(k-1)!}\zeta(1-k)E_k(e^{2\pi i\tau}).$$

Ribet

谷山・志村が Frey 曲線についてなりたてば，Fermat の最終定理は正しい．つまり，Frey 曲線は志村・谷山予想に矛盾する.

Wiles

Frey 曲線を含む楕円曲線の集合について，志村・谷山予想を証明．したがって，Ribet の定理とあわせて Fermat の最終定理を証明.