

楕円曲線の数論幾何 (第 3 回)

楕円曲線の有理点は(見かけ以上に)難しい

楕円曲線の有理点の座標の分子や分母はかなり大きくなることもある. 楕円曲線

$$y^2 = x^3 + 877x$$

は無限個の有理点を持つが, $(0, 0)$ 以外の有理点のうち, x 座標の分子・分母の絶対値が最も小さいものは

$$x = \frac{375494528127162193105504069942092792346201}{6215987776871505425463220780697238044100}$$

$$y = \frac{256256267988926809388776834045513089648669153204356603464786949}{490078023219787588959802933995928925096061616470779979261000}$$

である (ブレムネール - キャッセルズ (1984 年))

楕円曲線の方程式 $y^2 = x^3 + ax + b$ (a, b は整数, $4a^3 + 27b^2 \neq 0$) が与えられたとき, その有理点を全て求める方法は知られていない. 有理点の個数が有限個か無限個かを判定する方法も知られていない. もし BSD 予想 (バーチ - スイナートン = ダイアー予想) が正しければ, それを使って計算する方法は知られている (マニンのアルゴリズム).

階数 28 以上の楕円曲線

エルキースは 2006 年に楕円曲線

$$y^2 + xy + y = x^3 - x^2 - 20067762415575526585033208209338542750930230312178956502x + 34481611795030556467032985690390720374855944359319180361266008296291939448732243429$$

が 28 個の独立な有理点を持つことを示し, 「世界記録」を更新した.

$$P_1 = (-2124150091254381073292137463, 259854492051899599030515511070780628911531)$$

$$P_2 = (2334509866034701756884754537, 18872004195494469180868316552803627931531)$$

$$P_3 = (-1671736054062369063879038663, 251709377261144287808506947241319126049131)$$

$$P_4 = (2139130260139156666492982137, 36639509171439729202421459692941297527531)$$

$$P_5 = (1534706764467120723885477337, 85429585346017694289021032862781072799531)$$

$$P_6 = (-2731079487875677033341575063, 262521815484332191641284072623902143387531)$$

$$P_7 = (2775726266844571649705458537, 12845755474014060248869487699082640369931)$$

$$P_8 = (1494385729327188957541833817, 88486605527733405986116494514049233411451)$$

$$P_9 = (1868438228620887358509065257, 59237403214437708712725140393059358589131)$$

$$P_{10} = (2008945108825743774866542537, 47690677880125552882151750781541424711531)$$

$P_{11} = (2348360540918025169651632937, 17492930006200557857340332476448804363531)$
 $P_{12} = (-1472084007090481174470008663, 246643450653503714199947441549759798469131)$
 $P_{13} = (2924128607708061213363288937, 28350264431488878501488356474767375899531)$
 $P_{14} = (5374993891066061893293934537, 286188908427263386451175031916479893731531)$
 $P_{15} = (1709690768233354523334008557, 71898834974686089466159700529215980921631)$
 $P_{16} = (2450954011353593144072595187, 4445228173532634357049262550610714736531)$
 $P_{17} = (2969254709273559167464674937, 32766893075366270801333682543160469687531)$
 $P_{18} = (2711914934941692601332882937, 2068436612778381698650413981506590613531)$
 $P_{19} = (20078586077996854528778328937, 2779608541137806604656051725624624030091531)$
 $P_{20} = (2158082450240734774317810697, 34994373401964026809969662241800901254731)$
 $P_{21} = (2004645458247059022403224937, 48049329780704645522439866999888475467531)$
 $P_{22} = (2975749450947996264947091337, 33398989826075322320208934410104857869131)$
 $P_{23} = (-2102490467686285150147347863, 259576391459875789571677393171687203227531)$
 $P_{24} = (311583179915063034902194537, 168104385229980603540109472915660153473931)$
 $P_{25} = (2773931008341865231443771817, 12632162834649921002414116273769275813451)$
 $P_{26} = (2156581188143768409363461387, 35125092964022908897004150516375178087331)$
 $P_{27} = (3866330499872412508815659137, 121197755655944226293036926715025847322531)$
 $P_{28} = (2230868289773576023778678737, 28558760030597485663387020600768640028531)$

授業中に使う補題

補題 a, b を整数とする. 文字 n, m に関する多項式

$$F = n^4 - 2an^2m^2 - 8bnm^3 + a^2m^4, \quad G = 4n^3m + 4anm^3 + 4bm^4$$

を考える. このとき, n, m に関する整数係数の 3 次斉次多項式 f_1, f_2, g_1, g_2 で,

$$f_1F + g_1G = 4(4a^3 + 27b^2)m^7, \quad f_2F + g_2G = 4(4a^3 + 27b^2)n^7$$

をみたすものが存在する.

(証明) $f_1 = 12n^2m + 16am^3, f_2 = 4(4a^3 + 27b^2)n^3 - 4a^2bn^2m + 4a(3a^3 + 22b^2)nm^2 + 12b(a^3 + 8b^2)m^3, g_1 = -3n^3 + 5anm^2 + 27bm^3, g_2 = a^2bn^3 + a(5a^3 + 32b^2)n^2m + 2b(13a^3 + 96b^2)nm^2 - 3a^2(a^3 + 8b^2)m^3$ とおけばよい. $\square$

系 a, b を $4a^3 + 27b^2 \neq 0$ をみたす整数とする. n, m を 0 でない整数で, 互いに素と仮定する. このとき, $d = \gcd\{n^4 - 2ax^2m^2 - 8bnm^3 + a^2m^4, 4n^3m + 4anm^3 + 4bm^4\}$ は $4(4a^3 + 27b^2)$ の約数である. ($\gcd\{s, t\}$ は s, t の最大公約数を表す.)

(証明) 補題より, d は $\gcd\{4(4a^3 + 27b^2)m^7, 4(4a^3 + 27b^2)n^7\}$ の約数である. m, n は互いに素なので, $\gcd\{4(4a^3 + 27b^2)m^7, 4(4a^3 + 27b^2)n^7\} = 4(4a^3 + 27b^2)$ である. $\square$