1　楕円曲線の有理点

1.1　2 次曲線の有理点

• 方程式 $X^2+Y^2=Z^2$ の整数解。

方程式 $x^2+y^2=1$ の有理数解。

解 $P=(a,b)\neq Q=(-1,0)$ と、有理数の間に 1 対 1 対応。

P に対し、直線 PQ の傾きを対応。

有理数 t に対し、直線 $y=t(x+1)$ と円 $x^2+y^2=1$ の 2 交点のうち Q でないほうを対応。

$$(a,b)=\left(\frac{1-t^2}{1+t^2},\frac{2t}{1+t^2}\right).$$

• 一般に、2 次曲線 $x^2-ay^2=b$ が 1 つ有理点をもてば、この方法で無限個の有理点が構成できる。

• 全くもたないこともある。例 $x^2+y^2=3$。

$x'=2^nx, y'=2^ny$ が整数になるような最小の整数 n をとる．すると x',y' の少なくともどちらかは奇数．x' が奇数とすると，x' を 4 でわったあまりは 1，y' を 4 でわったあまりは 0 か 1．したがって，$x'^2+y'^2=3\cdot 2^{2n}$ を 4 でわったあまりが 1 か 2 となり矛盾．

• 一般に $ax^2+by^2=1$ が有理点をもつかどうかは，簡単な判定法が知られている．(「数論講義」参照)

• 方程式 $x^2-2y^2=\pm 1$ の整数解。$(a,b),(a',b')$ が解なら $a''+b''\sqrt{2}=(a+b\sqrt{2})(a'+b'\sqrt{2})$ とおくと (a'',b'') も解．$(1,1)$ が解．$(1+\sqrt{2})^2=3+2\sqrt{2}$ だから $(3,2)$ も解．

一般解 $a+b\sqrt{2}=\pm(1+\sqrt{2})^n$.

1.2　楕円曲線の有理点

$E=E_{a,b}$ を方程式 $y^2=x^3+ax+b$ (a,b は有理数) で定義された楕円曲線とする．

• Mordell：E の有理点 $P_1,\ldots,P_n$ で次の性質をもつものが存在する．

$P_1,\ldots,P_n$ から出発して，

2 点を結んで第 3 の交点をとる，

接線を引いてもう 1 つの交点をとる，

x 軸に対して対称な点をとる，

という操作を繰り返すことにより，E のすべての有理点が得られる．

• より現代的な定式化：$E(\mathbb{Q})$ は有限生成 Abel 群.

E の有理点 $P_1,\ldots,P_r$ と，E の有理点の有限集合 $E(\mathbb{Q})_{\mathrm{tors}}$ で，次の性質をもつものが存在する．

E の任意の有理点 P に対し，整数 $n_1,\ldots,n_r$ と $Q\in E(\mathbb{Q})_{\mathrm{tors}}$ で，$P=n_1P_1+\cdots+n_rP_r+Q$ をみたすものがただ 1 つ存在する．さらに $E(\mathbb{Q})_{\mathrm{tors}}$ は加法で閉じている．

$E(\mathbb{Q})_{\rm tors}$: ねじれ部分.

• Mazur: $E(\mathbb{Q})_{\rm tors}$ の元の個数は $1 \sim 10, 12, 16$ のどれか.

• $P_1, \dots, P_r$：自由部分の基底.

r：現代の数学の最大の問題の１つ。

r がいくらでも大きくなるか？

• Birch−Swinnerton-Dyer 予想.

$L(E,s)$：E の L 関数．本来は $s > \frac{3}{2}$ の範囲で，次の式で定義

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

志村・谷山予想が証明されていることから，すべての s で定義されている．$s = 1$ での Taylor 展開：

$$L(E,s) = a_n(s-1)^n + a_{n+1}(s-1)^{n+1} + \cdots .$$

ただし $a_n \neq 0$.

BSD 予想：$r = n$.

$n \leq 1$ なら確かめられている。（Kolyvagin, 1986?）

p 進類似

1.3　おまけ

曲線 $x^3 + y^3 = 1$ が確かに楕円曲線であること。$x = \dfrac{x'}{y'+1}, y = \dfrac{y'-1}{y'+1}$ とおいて，分母を払うと

$$x'^3 + (y'-1)^3 = (y'+1)^3$$

移項して

$$x'^3 = 6y'^2 + 2.$$

さらに移項して、

$$\left(\frac{y'}{6}\right)^2 = \left(\frac{x'}{6}\right)^3 - \frac{1}{108}.$$

どうやって、変換を思いつくか．同次座標で書くと、$X^3 + Y^3 = Z^3$.

点 $(0,1) = (0:1:1)$ が無限遠点に、

直線 $Y = Z$ が無限遠直線 $Z' = 0$ に、

2 等分点をとおる直線 $Y + Z = 0$ が、$Y' = 0$ に、

直線 $X = 0$ が $X' = 0$ に

なるように，$X = X', 2Y' = Y + Z, 2Z' = Z - Y$ と変換する．すると $X = X', Y = Y' - Z', Z = Y' + Z'$ だから上の式になる．