数理解析研究所講究録
1091 巻 1999 年 9-17

θ-合同数と楕円曲線

菅 真紀子 (Makiko KAN)
お茶の水女子大学 人間文化研究科

§1. θ-合同数の紹介と主な結果

3 辺の長さが有理数であるような直角三角形の面積となりうる自然数 n を合同数と呼びます。自然数の合同性と楕円曲線論には密接な関係があり、ある自然数が合同か否かを調べることは、$\mathbf{Q}$ 上定義された対応する楕円曲線の Mordell-Weil rank が正か否かを調べることと同値となります。楕円曲線論の研究の進展により、合同数については もう既にいくつかの興味深い結果が得られています。例えば、Birch-Swinnerton-Dyer 予想を仮定すれば、8 を法として 5,6,7 に合同な自然数は全て合同数であるということが知られています。また、Birch-Swinnerton-Dyer 予想を仮定しなくても、素因子数が少ないいくつかの合成数についてはその合同性・非合同性が確認されています [1, 11, 12]。

[9] の中で、Fujiwara は合同数の概念を次のように拡張しました。θ を $0<\theta<\pi$ なる実数とします。この θ について、1 つの角の大きさが θ で 3 辺の長さが有理数となるような三角形のことを "θ-有理三角形" と呼ぶことにします。ここで、この様な三角形については $\cos\theta$ の値が必ず有理数として得られるという事に注意しなくてはいけません。その値を $\cos\theta=s/r,\ r,s\in\mathbf{Z}, gcd(r,s)=1, r>0$ と置きます。更に、この θ によって一意的に定まる α_θ の値を $\sqrt{r^2-s^2}$ とします。すると、従来の合同数の拡張判、θ-合同数は次の様に定義されます。

定義. n を自然数とする。$n\alpha_\theta$ がある θ-有理三角形の面積となりうる時、n は θ-合同数であるという。

この報告の中では、常に θ は $0<\theta<\pi$ なる実数で $\cos\theta$ が有理数となるものとします。また、三角形の各辺を整数倍することによってその面

積は2乗倍されますから、一般性を失うことなく自然数 n は square-free であると仮定します。

$\theta=\pi/2$ の時には $\alpha_{\pi/2}=1$ となり、$\pi/2$-合同数は従来の意味での合同数と同じになります。このことから、θ-合同数の定義は従来の合同数の自然な拡張となっている事が分かります。
自然数 n と、上で与えた θ、つまりは自然数のペア (r,s) に対して、楕円曲線 $E_{n,\theta}$ を $y^2=x(x+(r+s)n)(x-(r-s)n)$ で与えます。

定理 (Fujiwara, [9]). n を自然数とする。この時
(1) n が θ-合同数であることの必要十分条件は $E_{n,\theta}$ が位数3以上の有理点を持つことである。
(2) $n\neq 1,2,3,6$ である時、n が θ-合同数であることの必要十分条件は $E_{n,\theta}(\mathbf{Q})$ が正の Mordell-Weil rank を持つことである。

注. θ-合同数に対応する楕円曲線全体を $\mathbf{Q}$ 上同型で割った族を考えます。するとその族は $\mathbf{Q}$ 上3つの一次因子に完全分解される楕円曲線の族、つまり Mordell-Weil 群の 2-torsion part $E(\mathbf{Q})[2]$ が $\mathbf{Z}/2\mathbf{Z}\oplus\mathbf{Z}/2\mathbf{Z}$ の形であるもの全体の族となります。

$$\begin{aligned}\{\ E_{n,\theta}\ \}/\cong_{\mathbf{Q}} &= \{y^2=(x-A)(x-B)(x-C)\ :\ \text{楕円曲線},\ A,B,C\in\mathbf{Q}\}/\cong_{\mathbf{Q}}\\ &= \{E/\mathbf{Q}\ :\ E(\mathbf{Q})[2]\cong\mathbf{Z}/2\mathbf{Z}\oplus\mathbf{Z}/2\mathbf{Z}\}/\cong_{\mathbf{Q}}\end{aligned}$$

このような楕円曲線族はコンピューター計算をする時に便利であったり、modular であることが証明されていたりで [6]、比較的扱いやすい対象であると言えます。

この定理から、楕円曲線 $E_{n,\theta}$ は θ-合同数についての重要な情報を私達に与えてくれるということが分かります。この様な流れの中で、24を法として $5,7,19$ に合同な素数は $\pi/3$-合同でないことが確かめられています [9]。
今回得られた主な結果は次の通りです。

補題. 自然数 n が θ-合同数であるなら n は $pq(p+q)(2rq-(r-s)p)$, $p,q\in\mathbf{N}, gcd(p,q)=1$ の square free part となっている。逆に、このような p,q で表される式の square-free part は θ-合同数である。

注. 上の補題を用いると$\pi/2$-合同数に関する既成の結果がいくつか導き出されます。例えば、整数m_1, m_2, $m_1m_2 > 1, gcd(m_1, m_2) = 1$について$\frac{1}{2}m_1m_2(m_1^2 + m_2^2)$は$\pi/2$-合同数であることが知られています(定理2.1,[14])。補題で$p = a^2 - b^2, q = b^2$, $a, b \in \mathbf{N}, a > b, gcd(a, b) = 1$とすれば$pq(p+q)(p+2q) = a^2b^2(a^2+b^2)(a^2-b^2) \equiv (a^2+b^2)(a^2-b^2) \pmod{\mathbf{Q}^{*2}}$となります。再び$m_1 = a+b$, $m_2 = a-b$ (a, bが共に奇数ならそれぞれ$2m_1, 2m_2$)と置き直すと上の結果が得られます[9]。また、任意のθ-についてθ-合同数は8を法とした各剰余類に無限個ずつ存在することも補題から得られます[9]。これも[3]の定理3を一般化した結果となっています。

例. (1) $\theta = \pi/2$について$p = 1, q = 1$を取ると6は$\pi/2$-合同となる。実際、6は3辺の長さが3,4,5である直角三角形の面積となっている。
(2) $\theta = 2\pi/3$について$p = 61991193600 = 2^{10} \cdot 3^2 \cdot 5^2 \cdot 7^2 \cdot 17^2 \cdot 19$, $q = 18357811081 = 157^2 \cdot 863^2$を取ると19は$2\pi/3$-合同となる。実際、$19\sqrt{3}$は3辺の長さが544/105, 1995/136, 254659/14280であるような$2\pi/3$-有理三角形の面積となっている。

命題. $p > 3$を素数、$E_{p,\frac{\pi}{3}}, E_{p,\frac{2\pi}{3}}$はそれぞれ$\theta = \pi/3, 2\pi/3$とその素数$p$に対応する楕円曲線とする。この時、これらの曲線のMordell-Weil-rank $rankE(\mathbf{Q})$とShafarevich-Tate群$\text{Ш}(E/\mathbf{Q})$は次の性質を満たす。

$$rankE_{p,\frac{\pi}{3}}(\mathbf{Q}) + dim_2\text{Ш}(E_{p,\frac{\pi}{3}}/\mathbf{Q})[2]$$

$$= \begin{cases} 0 & for \quad p \equiv 5, 7, 19 \ (mod \ 24) \\ 1 & for \quad p \equiv 11, 13, 17, 23 \ (mod \ 24) \\ 2 & for \quad p \equiv 1 \ (mod \ 24) \end{cases}$$

$$rankE_{p,\frac{2\pi}{3}}(\mathbf{Q}) + dim_2\text{Ш}(E_{p,\frac{2\pi}{3}}/\mathbf{Q})[2]$$

$$= \begin{cases} 0 & for \quad p \equiv 7, 11 \ (mod \ 24) \\ 1 & for \quad p \equiv 5, 17, 19, 23 \ (mod \ 24) \\ 2 & for \quad p \equiv 1, 13 \ (mod \ 24). \end{cases}$$

この命題は、2-decsentと呼ばれる手法をもとにHenselの補題などを駆使して楕円曲線のSelmer群の構造を調べる事によって得られました。上の

結果はMordell-Weil-rankに明確な上限を与えています。

定理. p を素数とする。p が 24 を法として 7, 11 又は 13 に合同なら p は $\frac{2\pi}{3}$-合同数ではない。また、p が 24 を法として 23 に合同な素数なら p は $\frac{2\pi}{3}$-合同数である。

非合同性は上の命題から直接得られます。ただ、$p \equiv 13 \pmod{24}$ の場合に関してだけは $E_{p,2\pi/3}$の定義方程式をちょっと変形させる工夫を要しました。この場合に限って非自明なShafarevich-Tate群が確認されますから、Hasseの原理を満たさないような不定方程式を副産物として得る事が出来ます。合同性の証明については、もう少し複雑ですので次節で詳しく触れることにします。

従来の合同数からθ-合同数へ拡張するに当たって、その性質を明らかにするのに様々な壁があります。例えば、$\pi/2$-合同数に対応する楕円曲線は虚数乗法を持つのですが、θ-合同数に対応する楕円曲線は一般に虚数乗法を持ちません。そこで、Coats-Wilesの定理([4])など虚数乗法を持つ楕円曲線に限った結果を適応することは一般には不可能になります。しかし、Coats-Wilesの結果に関して言えば、Kolyvaginによって「虚数乗法を持つ」という条件は「modularである」へと大きく弱められましたから[13](そして私達が扱う楕円曲線は全てmodularでしたから)、その壁は取り除かれました。Kolyvaginの定理は合同性に関する必要条件を解析的手法によって与えてくれるものでしたが、十分条件で効果的なものは余り得られていません。しかし、θを$\pi/3, 2\pi/3$に制限して考えた時、まだ解かれていない、しかし正しいであろうと思われるいくつかの予想やコンピューターを使っての数値実験によって、合同性に関する予想をたてることが出来ます。

例えばFreyは、任意の楕円曲線 $E/\mathbf{Q}$ についてTate-Shafarevich群 $\text{Ш}(E/\mathbf{Q})$の2-primary partが有限であるという仮定のもと、$dim_2\text{Ш}(E/\mathbf{Q})[2] =$ 偶数 であることを示しました([7])。$\text{Ш}(E/\mathbf{Q})$ は有限であろうという予想がありますから、上の命題から次のような予想をたてることが出来ます。またこれは、Birch-Swinnerton-Dyer予想を仮定した上でのコンピューター実験によってもある程度確認されています。

予想. p を素数とする。p が 24 を法として 11, 13, 17, 23 に合同ならば p は$\frac{\pi}{3}$-合同数である。また、p が 24 を法として 5, 17, 19, 23 に合同ならば p は$\frac{2\pi}{3}$-合同数である。

§2. 合同性の証明

非合同性に比べて合同性を示すことは余り簡単ではありません。実際、楕円曲線の Mordell-Weil rank が正であることを確認する汎用な手段は、具体的な有理点をコンピューター頼みに探す以外みつかっていません。

この節では Heegner point という概念を用いて、どの様に定理の合同性部分を示したかを説明します。まず 1 つ注を与えて置きます。

注. 楕円曲線 $E : y^2 = x^3 + ax^2 + bx$ の n-twist $E^{(n)}$、つまり Eと $\mathbf{Q}(\sqrt{n})$ 上同型であるような楕円曲線 $E^{(n)}$は $y^2 = x^3 + anx^2 + bn^2x$ という形で表されます。(ここでは $\mathbf{Q}$ 上同型である楕円曲線族は同一視しています。) θ-合同数に関した場合、楕円曲線 $E_{n,\theta}$は $E_{1,\theta}$の n-twist となっています。さらに $E_{n,\pi-\theta}$は $E_{n,\theta}$の (-1)-twist となっています。特に $E_{n,2\pi/3}$は $E_{1,\pi/3}$の $(-n)$-twist です。

次に Birch の [1] にある定理を 1 つ引用します。この論文において、Heegner point の概念は初めて紹介されました。

定理 (Birch, [1]). p を 4 を法として 3 と合同な素数で、$p = 96T^2 - S^2$が $\mathbf{Z}$ で可解であるようなものとする。すると、有限個を除いたほとんどの p について楕円曲線 $E : Y^2 = (X-1)(X^2-4)$ の $(-p)$-twist $E^{(-p)}$は無限位数の $\mathbf{Q}$ 有理点を持つ。

Birch の定理の中で扱っている楕円曲線 Eは$\pi/3$-合同に関する楕円曲線 $E_{1,\pi/3}$と $\mathbf{Q}$ 上同型です。また、上の注で見たように $E_{p,2\pi/3}$は $E_{1,\pi/3}$の $(-p)$-twist となっています。ですから、この定理は $2\pi/3$-合同であるような素数 p をいくつか与えてくれそうに見えます。この段階で残された課題は、$p = 96T^2 - S^2$が $\mathbf{Z}$ で可解となる p の条件を知ること、p の有限個の例外が具体的に何なのかを知ることとなります。[1] によると、例外は $H^*/\Gamma_0(24)$ の model J_{24} から Fricke の 4 次曲線 C_{24} ([1, 7]) への

写像がうまく作れるか否かに依存して生じるようです。より詳しく見るためにFrickeの仕事について再考し、私たちのケースへの適応を試みます。

$\Gamma_0(24)=\left\{\begin{pmatrix} a & b \\ c & d\end{pmatrix}\in SL_2(\mathbf{Z}) : c\equiv 0 \pmod{24}\right\}$、$H$は上半平面Im(z)>0とします。すると$\Gamma_0(24)$は$H^*=H\cup\mathbf{Q}$上線型分数変換の形で作用します。$F_0(24)$を14個の頂点$0,\pm1/12,\pm1/8,\pm1/6,\pm1/4,\pm1/3,\pm1/2,\infty$を持ち、12個の半円周、2本の垂直線によって囲まれた14角形の形をした、$\Gamma_0(24)$に関する基本領域であるとします。この領域の各辺は、$\Gamma_0(24)$のある要素によって虚軸対称に移されますから、尖点は$0,1/12,1/8,1/6,1/4,1/3,1/2,\infty$の8つとなります(p458,[8])。$j$を$\Gamma_0(1)=SL_2(\mathbf{Z})$に関するmodular invariant、$j_{24}(z)=j(24z)$とすると、$j$と$j_{24}$は$\Gamma_0(24)$の作用によって不変となっています。実際$\gamma=\begin{pmatrix} a & b \\ c & d\end{pmatrix}\in\Gamma_0(24)$とすると、$\gamma(j(z),j_{24}(z))=(j(\gamma z),j_{24}(\gamma z))=(j(\frac{az+b}{cz+d}),j(24\cdot\frac{az+b}{cz+d}))=(j(z),j(\frac{a\cdot 24z+24b}{c/24\cdot 24z+d}))=(j(z),j(\begin{pmatrix} a & 24b \\ c/24 & d\end{pmatrix}\cdot 24z))=(j(z),j_{24}(z))$となり、不変である事が確かめられます。また、$j$と$j_{24}$はmodular equationと呼ばれる代数等式$F_{24}(j,j_{24})=0$を満たす事が知られていて、曲線$J_{24}:F_{24}(u,v)=0$は$X_0(24):=H^*/\Gamma_0(24)$の1つのmodelとなっています。それに伴い、$(j,j_{24})$は$X_0(24)$から$J_{24}$への正則写像、つまりは$F_0(24)$から$J_{24}$への写像とみなされます。$(j,j_{24})$を$F_0(24)$から$J_{24}$への写像とみなした時、その過程で特異点が生じ得ることに注意しなくてはいけません。特にここではzを基本領域内の虚二次数と仮定して、zが特異点を生じる場合の特性を考察します。

J_{24}がz上で特異性を持つとすると、ある$z'\in F_0(24)$が存在して、zとz'は$F_0(24)$の点として異なるけれども曲線$J_0(24)$上の点として同じもの$(j(z),j_{24}(z))=(j(z'),j_{24}(z'))$を与えてしまいます。つまり、$a,b,c,d,A,B,C,D\in\mathbf{Z}$, $ad-bc=AD-BC=1$で、しかし$a=A, 24b=B, c=24C, d=D$という関係ではないものについて$\frac{24az+24b}{cz+d}=\frac{24Az+B}{24Cz+D}$が成り立ちます。これは行列$M=\begin{pmatrix} 24A & B \\ 24C & D\end{pmatrix}^{-1}\begin{pmatrix} 24a & 24b \\ c & d\end{pmatrix}=\begin{pmatrix} aD-\frac{Bc}{24} & bD-\frac{Bd}{24} \\ -24aC+Ac & -24bC+Ad\end{pmatrix}\in SL_2(\mathbf{Q})$が$F_0(24)$上ellipticである事を意味します。(すなわち、Mは$F_0(24)$でただ二つの固定点z, $-\bar{z}$を持つということです。) Elliptic element Mは$|trM|<2$を満足するという事が一般に知られていますから、ここでは$|aD-\frac{Bc}{24}-24bC+Ad|<2$です。計算によって、この条件は$-2304\leq\Delta(z)<0$という$z$の判別式に関する条件に帰着されます。

一方Frickeは[8]の中で$\tau(z)$と$\sigma(z)$という2つのmodular関数を紹介

しました。$\tau(z), \sigma(z)$ は主に次のような性質を持ちます: $\tau(z) \in \mathbf{Q}(j(z), j_{24}(z))$、$\tau(z)$ は $j(z)$ と $j_{24}(z)$ について対称、$\sigma(z)/(j(z) - j_{24}(z)) \in \mathbf{Q}(\tau(z))$、$\sigma^2(z) = f(\tau(z)) = \tau^4(z) - 12\tau^3(z) + 32\tau^2(z) - 24\tau(z) + 4$ (p459 [8], [1])。W を $Wz = -1/24z$ なる involution とします。ここで W は j と j_{24} を入れ替える事に注意をします; $W(j(z), j_{24}(z)) = (j(Wz), j_{24}(Wz)) = j(-1/24z), j(-1/z)) = (j(\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} 24z), j(\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} z)) = (j_{24}(z), j(z))$。$\tau(z)$ は j と j_{24} について対称でしたから W-不変で、したがって $F_0(24)/W$ 上の関数とみなす事が出来ます。一方 $\sigma(z)$ は W で $-\sigma(z)$ に写ります。さらに W は $F_0(24) \cap \{z : |z| \geq \sqrt{6}/12\}$ を $F_0(24) \cap \{z : |z| \leq \sqrt{6}/12\}$ に bijective に写すことが分かります。特に $|z| = \sqrt{6}/12$ 上、z を虚軸対称な点に写します。すると $F_0(24)$ から Fricke の 4 次曲線 $C_{24} : \sigma^2 = \tau^4 - 12\tau^3 + 32\tau^2 - 24\tau + 4$ への写像を次のように与えることが出来ます。

$$
\begin{array}{rcccl}
(\tau, \sigma) & : & F_0(24) & \longrightarrow & C_{24} \\
 & & z & \longmapsto & \begin{cases} (\tau(z), \sigma(z) = \sqrt{f(\tau(z))}) & |z| > \sqrt{6}/12 \text{ 又は } \\ & |z| = \sqrt{6}/12, \mathrm{Re}(z) \geq 0 \\ (\tau(z), \sigma(z) = -\sqrt{f(\tau(z))}) & \text{その他の場合} \end{cases}
\end{array}
$$

ここで $\sqrt{f(\tau)}$ についてはどちらか一方の branch を選べば良い事とします。このようにして、私たちは可換図式

$$
\begin{array}{ccc}
 & z \in F_0(24) \backslash \left\{ \begin{array}{l} z \in F_0(24) : \\ (j(z), j_{24}(z)) \text{ は } J_{24} \text{上特異点} \end{array} \right\} & \\
\swarrow & & \searrow \\
\pi : \; J_{24} \backslash \{ \text{特異点} \} & \longrightarrow & C_{24} \\
(j(z), j_{24}(z)) & \longmapsto & (\tau(z), \sigma(z))
\end{array}
$$

を得ることができます。そして、この図式は $J_{24} \backslash \{$ 特異点 $\}$ から C_{24} への well-defined map π を導き出します。

[1] の定理 1 より、$-p = S^2 - 96T^2$ が整数解 (S, T) をもつならば J_{24} は $\mathbf{Q}(\sqrt{-p})$-有理点 $(j(\omega), j_{24}(\omega))$ を持ちます。ここで ω は $\omega = \frac{S + \sqrt{-p}}{48T}$ なる虚二次数で、$\Delta(\omega) = -p$, $\overline{j_{24}(\omega)} = j(\omega)$ なるものです。(この ω が Heegner point。) 計算により、$-p = S^2 - 96T^2$ が整数解 (S, T) を持つような必要十分条件は $p \equiv 23 \pmod{24}$ であることが簡単に確かめられます。すると、もし $\Delta(\omega) = -p < -2304$ ならば写像 π は $(j(\omega), j_{24}(\omega))$ を

$(\tau(\omega), \sigma(\omega))$, $\tau(\omega) \in \mathbf{Q}$, $\sigma(\omega) \in \mathbf{Q}(\sqrt{-p})\backslash\mathbf{Q}$ へと写します ([1])。

$(\tau, \sigma) \mapsto (\tau, \sigma/\sqrt{-p})$ によって得られる C_{24}の $(-p)$-twist を $C_{24}^{(-p)}$ とすると、$(\tau(\omega), \sigma(\omega)/\sqrt{-p})$ は $C_{24}^{(-p)}$の $\mathbf{Q}$ 有理点です。[1] の補題 2 は、もし $C_{24}^{(-p)}$が有理点を持つならばその Jacobi 曲線は $\mathbf{Q}$ 上 正の Mordell-Weil-rank を持つと主張しています。そして、その Jacobi 曲線は Birch の定理における楕円曲線 $E^{(-p)}$、すなわち私たちの呼ぶところの $E_{p,\frac{2\pi}{3}}$ と $\mathbf{Q}$ 上同型です。[1] において、写像 π が $\omega = \frac{S+\sqrt{-p}}{48T} \in F_0(24)$ 上 well-defined なら ω は確かに非自明な有理点を私たちの楕円曲線に与えることが示されています。$J_{24}\backslash\{$ 特異点 $\}$ の中では π は well-defined となりますから、これは $p > 2304$ なる素数について主定理の結果を与えてくれることとなります。

$p \equiv 23 \pmod{24}$ なる素数で、$23 \leq p < 2304$ の範囲にあるような 42 個については、[10] の定理 7.3 とコンピューター計算によって $E_{p,\frac{2\pi}{3}}$が正の rank 1 を持つことが確認されました。ということで、全ての $p \equiv 23 \pmod{24}$ なる素数について主定理は確かめられたことになります。

例. 23 は $2\pi/3$-合同である。実際、$23\sqrt{3}$ は 3 辺の長さが$\frac{14}{5}$, $\frac{230}{7}$, $\frac{1202}{35}$ であるような $2\pi/3$-有理三角形の面積となっている。更に 2039 も $2\pi/3$-合同である。実際、$2039\sqrt{3}$ は 3 辺の長さが$\frac{891339311078695734731 98}{70311443271560150011 79}$, $\frac{28673006566142229174807962}{4456696555393478673659 9}$, $\frac{2036193258877906366441529848343726435356779132 02}{3133567670331061034744344902646726065474502 21}$ であるような $2\pi/3$-有理三角形の面積となっている。

参考文献

[1] Birch,B.J., Elliptic Curves and Modular Functions, Symposia Math. 4, 1970, 27-32.

[2] Birch,B.J., Heegner Points of Elliptic Curves, Symposia Mathematica XV, 1973, 441-445.

[3] Chahal, J. S., On an Identity of Desboves, Proc. Japan Acad., 60,

Ser. A, 1984, 105-108.

[4] Coats,J.,Wiles,A., On the Conjecture of Birch and Swinnerton-Dyer, Invent. Math. 39, 1977, 223-251.

[5] Cornell,G.,Silverman,J.H.,Stevens,G.(editors), *Modular Forms and Fermat's Last Theorem*, Springer-Verlag, New York-Berlin-Heidelberg, 1997.

[6] Diamond,F., Kramer,K., Modularity of a family of elliptic curves, Math. Research Letters 2, 1995, 299-305.

[7] Frey, G., Some Aspects of the Theory of Elliptic Curves over Number Fields, Exposition.Math. 4, 1986, 35-66.

[8] Fricke,R., *Lehrbuch der Algebra III* , Braunschweig, 1928.

[9] Fujiwara,M., θ-congruent numbers, Number Theory, ed. by Győry, Pethő, Sós Walter de Gruyter, 1997, 235-241.

[10] Gross,B., Zagier,D., Heegner Points and Derivatives of L-series, Invent. Math. 84, 1986, 225-320.

[11] Heegner,K., Diophantine Analysis und Modulfunktionen, Math.Z. 56, 1952, 227-253.

[12] Monsky,P., Mock Heegner Points and Congruent Numbers, Math.Zeitschrift 204, 1990, 45-68.

[13] Kolyvagin,V.A., Finiteness of $E(\mathbf{Q})$ and $\text{Ш}(E/\mathbf{Q})$ for a subclass of Weil curves, (Russian) Izv. Akad. Nauk. Ser. Mat. 52, 1988, no 6., 1154-1180; translation in Math USSR Izv. 33 no. 3, 1989, 473-499.

[14] Serf, P., Congruent numbers and elliptic curves, in Computational Number Theory, Pethō, Pohst, Williams, Zimmer, eds., Walter de Gruyter, 1991, 227-238.

[15] Silverman, J. H., *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York-Berlin-Heidelberg, 1986.

[16] Wiman, A., Über den Rang von Kurven $y^2 = x(x+a)(x+b)$, Acta. math. 76, 1944, 225-251.