Osaka University Knowledge Archive

Title	Jacobian Group Arithmetic on Algebraic Curves
Author(s)	原澤, 隆一
Citation	大阪大学, 2003, 博士論文
Version Type	VoR
URL	https://hdl.handle.net/11094/337
rights	
Note	

Osaka University Knowledge Archive : OUKA

https://ir.library.osaka-u.ac.jp/

Osaka University

氏　　名	原　澤　隆　一（はら さわ りゅう いち）
博士の専攻分野の名称	博　士（理　学）
学　位　記　番　号	第　１７５０１　号
学位授与年月日	平成 15 年 3 月 25 日
学位授与の要件	学位規則第４条第１項該当 理学研究科数学専攻
学　位　論　文　名	Jacobian Group Arithmetic on Algebraic Curves **（代数曲線上のヤコビアン群演算）**
論　文　審　査　委　員	（主査） 教　授　山本　芳彦 （副査） 教　授　伊吹山知義　　教　授　日比　孝之　　助教授　鈴木　　譲 助教授　藤原　彰夫

論　文　内　容　の　要　旨

本論文は、$\mathbf{F}_q$- 有理点を１つ持つ$\mathbf{F}_q$上定義された非特異射影代数曲線のヤコビアン群の具体的かつ効率的な実現方法を提案し、その計算量を厳密に評価することを目的としている。この結果は、楕円曲線暗号、超楕円曲線暗号に替わる代数曲線暗号系の実現性に関するものである。

ヤコビアン群演算の実現性を考察する際、特別なクラスの曲線に関してはその方法が知られている：

楕円曲線

$$y^2=x^3+ax+b$$

に関しては、その自明な方法がよく知られている。また、超楕円曲線

$$y^2=x^{2g+1}+\cdots$$

においても、Cantor が具体的かつ効率的方法を提案している。この方法の特徴は、ヤコビアン群が座標環のイデアル類群と同型となることから、イデアル類群上の演算を考察しているということである。必要となる演算は全て一変数多項式環$\mathbf{F}_q[x]$上で行われており、その計算量も厳密に評価することができ、$O(g^2\log^2 q)$回のビット演算で実行され、入力サイズの２乗のオーダーとなっている。

本論文では、以下のような一変数代数関数体$F/\mathbf{F}_q$を考える（任意の一変数代数関数体は、ある非特異射影代数曲線の関数体となっていることが知られているので、記法は必要に応じて使い分けることにする）：

仮定　次数が１の素因子（Pとかく）をもつ。

今、Pの極位数がt個の自然数$\{a_1,\cdots,a_t\}$によって生成されているとし、必要ならば順序を並び替えて$\gcd(a_1,q)=1$と並べ替える。（種数の有限性より、そのようなa_1は存在する。）三浦は 1998 年に、そのような代数関数体において、そのアフィンモデルとなる、ある代数曲線$C/\mathbf{F}_q$を特徴付けた。そして、その座標環$\mathbf{F}_q[C]$のイデアル類群はもとの代数関数体のヤコビアン群と同型になるという性質をもっている。ゆえに、本論文ではこの代数曲線の座標環でのイデアル類群上の演算に関して、Cantor の方法の拡張方法を提案した。（P を無限遠点、$t=2$、$(a_1,a_2)=(2,2g+1)$としたとき、これは超楕円曲線に対応している。）

実際にイデアル類群上の演算を実行する際には、以下の２つの行程が必要となる：

・逆イデアルの計算；

・イデアルが与えられたとき、そのイデアルに属する元の中で、P の極位数に関する最小元を求める計算。

前者に関しては、

1. $\mathbf{F}_q[x]$ は単項イデアル整域（PID）（ここで、x は $(x)_\infty = a_1 P$ を満たす元）；

2. $\mathbf{F}_q(C)/\mathbf{F}_q(x)$ は有限次分離拡大；

3. 関数体 $\mathbf{F}_q(C)$ における $\mathbf{F}_q[x]$ の整閉包は座標環 $\mathbf{F}_q[C]$；

という性質から、代数的整数論を基にして、その実現方法が得ることができる。

また、後者に関しては、$\mathbf{F}_q[C]$ の $\mathbf{F}_q[x]$ 上の基底 $\{w_1, \cdots, w_{a_1}\}$ として、以下の条件を満たすものがとれることを基として、その実現方法を得ることができる：

・$-v_P(w_i) \not\equiv -v_P(w_j) \bmod a_1 (i \neq j)$.

以上の考察の下で得られた提案方式は、一変数多項式環 $\mathbf{F}_q[x]$ 上の演算のみで実行され、その計算量（本論文の主結果）は以下の通りである：

主結果　次数１の素因子を持つ一変数関数体 $F/\mathbf{F}_q$ のヤコビアン群演算は

$$O\left(\max\left\{a_1^6 g^2, a_1^8\right\} \log^2 q\right)$$

回のビット演算で実行される。

この結果より、a_1 を固定したとき、超楕円曲線の場合と同様、ヤコビアン群演算は、その入力サイズの２乗のオーダーとなっており、$a_1=2$ つまり超楕円曲線の場合が１番効率的であることもわかる。また、この提案方式の実装結果も挙げている。

論文審査の結果の要旨

原澤隆一君の論文“Jacobian Group Arithmetic on Algebraic Curves”は、有限体上定義された非特異射影代数曲線のヤコビアン群の具体的かつ効率的な実現方法を提案し、その計算量を厳密に評価するものである。次数１の素因子が存在し、極位数が有限個の自然数によって生成されるような代数関数体において、アフィン代数曲線のある標準的な形式（三浦標準形）が存在する。原澤君は、その座標環のイデアル類群がもとの代数関数体のヤコビアン群と同型になるという性質を利用し、代数曲線の座標環でのイデアル類群上の演算に関して、Cantor の方法（超楕円曲線のみに適用される）を一般化した方法を提案している。提案アルゴリズムでは、逆イデアルの演算、極位数最小のイデアル要素の探索などで従来になかった方法が導入されている。その結果、Cantor の方法と同様、種数を g、有限体サイズを q とすれば、$g \log q$ の２乗のオーダーの計算時間で演算が完結するような効率のよい優れたアルゴリズムになっている。以上のように、原澤隆一君の提出した論文は、博士（理学）の学位論文として十分価値あるものと認めるものである。