(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2009 年 9 月 3 日(03.09.2009)

PCT

(10) 国際公開番号
WO 2009/107650 A2

(51) 国際特許分類:
G09C 1/00 (2006.01)

(21) 国際出願番号: PCT/JP2009/053395

(22) 国際出願日: 2009 年 2 月 25 日(25.02.2009)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2008-043462 2008 年 2 月 25 日(25.02.2008) JP

(71) 出願人 (米国を除く全ての指定国について): 国立大学法人 岡山大学(NATIONAL UNIVERSITY CORPORATION OKAYAMA UNIVERSITY) [JP/JP]; 〒7008530 岡山県岡山市北区津島中一丁目１番１号 Okayama (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 野上保之 (NOGAMI, Yasuyuki) [JP/JP]; 〒7008530 岡山県岡山市津島中三丁目１番１号 国立大学法人岡山大学大学院自然科学研究科内 Okayama (JP). 森川良孝(MORITAKA, Yoshitaka) [JP/JP]; 〒7008530 岡山県岡山市津島中三丁目１番１号 国立大学法人岡山大学大学院自然科学研究科内 Okayama (JP). 加藤英洋(KATO, Hidehiro) [JP/JP]; 〒7008530 岡山県岡山市津島中三丁目１番１号 国立大学法人岡山大学大学院自然科学研究科内 Okayama (JP). 赤根正剛 (AKANE, Masataka) [JP/JP]; 〒7008530 岡山県岡山市津島中三丁目１番１号 国立大学法人岡山大学大学院自然科学研究科内 Okayama (JP).

(74) 代理人: 松尾憲一郎 (MATSUO, Kenichiro); 〒8100042 福岡県福岡市中央区赤坂１丁目１０番１７号 しんくみ赤坂ビル７階 Fukuoka (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 第１７条(2)(a)に基づく宣言；要約なし； 国際調査機関により点検されていない発明の名称。

(54) **Title**: SCALAR MULTIPLICATION METHOD, RAISING METHOD, RECORDING MEDIUM WHERE SCALAR MULTIPLICATION PROGRAM IS RECORDED, AND RECORDING MEDIUM WHERE RAISING METHOD PROGRAM IS RECORDED

(54) 発明の名称: スカラー倍算の演算方法、べき乗算の演算方法、スカラー倍算の演算プログラムを記録した記録媒体及びべき乗算の演算プログラムを記録した記録媒体

(57) **Abstract**:

(57) 要約:

WO 2009/107650 A2

明 細 書

スカラー倍算の演算方法、べき乗算の演算方法、スカラー倍算の演算プログラムを記録した記録媒体及びべき乗算の演算プログラムを記録した記録媒体

技術分野

[0001] 本発明は、有理点Qのスカラーn倍算のnを少なくともt－1進展開することによりスカラー倍算の演算を高速化したスカラー倍算の演算方法及びその演算プログラムを記録した記録媒体、及び元Aのn乗算のnを少なくとも(q－r)進展開することによりべき乗算の演算を高速化したべき乗算の演算方法及びその演算プログラムを記録した記録媒体に関する。

背景技術

[0002] 昨今、インターネットなどの電気通信回線を利用した情報ネットワーク技術が高度に発展し、インターネットによって様々な情報を取得するだけでなく、インターネットバンキングや行政機関への電子申請などのような各種のサービスが提供されてきている。

[0003] このようなサービスを利用する場合には、サービスの利用者が、成りすましや架空の人間などではなく、適正な利用者であることを確認するための認証処理が必要であり、信頼性の高い認証方法として、公開鍵と秘密鍵を用いる公開鍵暗号をベースとした電子認証技術がよく利用されている。

[0004] しかしながら、公開鍵暗号方式の電子認証では、公開鍵あるいは秘密鍵が漏洩した場合には直ちに公開鍵と秘密鍵を変更する必要があり、公開鍵及び秘密鍵の管理を慎重に行わなければならないとともに、必要に応じて新たな公開鍵と秘密鍵の設定登録作業が生じるという繁雑さがあるため、最近では、利用者の氏名やメールアドレスのように利用者特有のIDを用いて電子認証を行うIDベース暗号が用いられることが多くなっている。

[0005] また、電子認証を行う認証装置によって利用者の個人認証を行った場合には、認証装置に利用者ごとの履歴が蓄積されることとなり、この履歴情報自体が利用者の個人情報であって、最近では、この履歴情報が漏洩することによる個人情報の漏洩のおそれが指摘されている。

[0006] そこで、認証装置では利用者の個人情報を利用して認証を行うのではなく、複数の利用者をひとまとまりのグループとして、このグループに所属していることを示すグループ署名を用いることにより、利用者を特定することなく認証を行うことによって、認証装置に個人情報が蓄積されることなく認証を可能としたグループ署名技術が提案されている。

[0007] このようなIDベース暗号やグループ署名における所用の演算には、楕円曲線上の有理点の双線形写像を用いるペアリングと呼ばれる手法が用いられている。ペアリングとは、たとえば、Pを素体F_q上の有理点、Qをk次拡大体F_q^k上の有理点として、PとQとを入力して拡大体F_q^{*k}の元zが出力されるとき、a倍のPと、b倍のQを入力するとzのab乗が出力される演算である。なお、ここで、「k」を埋込み次数と呼び、「F_q^{*k}」は、正しくは、以下の表示であるが、表示の制限上、「F_q^{*k}」と表示している。

[0008] [数1]

$$F^*_{q^k}$$

[0009] IDベース暗号における暗号化あるいは復号の処理や、グループ署名における認証処理では、できるだけ短時間で実行されることが求められている。特に、ペアリングに基づく暗号方式などにおいてはスカラー倍算及びべき乗算が数多く実行されているため、これらの演算を高速に実行することが求められている。

[0010] そのため、従来より、スカラー倍算やべき乗算をバイナリ法やWindow法などを用いて高速化することが行われている。

[0011] また、拡大体の元$A \in F_q^k$のべき乗A^nを演算する場合には、フロベニウス写像$\phi_q : A \rightarrow A^q$を用いることによって演算回数を削減することにより高速化を図ることも行われている。

[0012] また、スカラー倍算においても、写像を利用することにより演算回数を削減して高速化を図る手法が提案されている(例えば、特許文献1、特許文献2参照。)。

特許文献1:特開2004－271792号公報

特許文献2:特開2007－41461号公報

発明の開示

発明が解決しようとする課題

[0013] しかしながら、写像を利用して高速化を図る周知の高速化手段では、スカラー倍算におけるスカラーn、またはべき乗算における乗数nが位数qを大きく上回る場合(n＞＞q)にはきわめて有効であるもの、有限体F_qの位数qより大きく上回ることのないスカラーn及び乗数nに対しては、高速化手段を用いずに直接的にスカラー倍算及びべき乗算を実行した場合と比較して顕著な効果が見いだせないものであった。

[0014] 特に、IDベース暗号における暗号化あるいは復号の処理や、グループ署名における認証処理においては、スカラーnを用いたスカラー倍算あるいは乗数nを用いたべき乗算が必要な場合に、スカラーnあるいは乗数nが、有限体F_qの位数qより大きく上回ることのない場合が多く、周知の高速化手段を用いても効果的な高速化が期待できなかった。

[0015] 本発明者らはこのような現状に鑑み、スカラーnあるいは乗数nが有限体F_qの位数qより大きく上回ることのない場合であっても、スカラー倍算あるいはべき乗算を高速に実行できる演算方法の研究開発を行って、本発明を成すに至ったものである。

課題を解決するための手段

[0016] 本発明のスカラー倍算の演算方法では、

楕円曲線を$E/F_q = x^3 + ax + b - y^2 = 0$, $a \in F_q$, $b \in F_q$とし、

$E(F_q)$を有限体F_qで定義される楕円曲線の有理点が成す加法群、

$E(F_q^k)$を有限体F_qの拡大体F_q^kで定義される楕円曲線の有理点が成す加法群、

ϕ_qを有限体F_qに関する有理点のフロベニウス自己準同型写像、

tをフロベニウス自己準同型写像ϕ_qのトレース、

rを$E(F_q)$の位数$\#E(F_q) = q + 1 - t$を割り切る素数位数、

E[r]を位数が素数rである有理点の集合、

[j]を有理点をj倍する写像、

Gを

$$G = E[r] \cap \mathrm{Ker}(\phi_q - [q])$$

を満たす$E(F_q^k)$に含まれる有理点の集合として、

非負整数nに対するGの有理点Qのスカラーn倍算を、CPU及び記憶手段を備え

た電子計算機により演算するスカラー倍算の演算方法において、

CPUが、前記非負整数nの値、前記トレースtの値、及び、$Q \in G \subset E(F_q^k)$により表される有理点Qの値を入力して前記記憶手段に記憶する入力ステップと、

CPUが、演算結果Zを記憶する前記記憶手段を初期化する初期化ステップと、

Gの有理点Qに対し、

$$\phi_q(Q) = [q]Q = [t-1]Q$$

が成り立つことにより、

CPUが、s＝t－1として、前記nをs進展開した次式に基づいて、

[数2]

$$n = \sum_i c[i]s^i, 0 \le c[i] \le s.$$

c[i]←n％s及びn←(n-c[i])/sにより表される代入演算をi＝0から所定回繰り返し行って各係数c[i]及び非負整数nの値を前記記憶手段に記憶する展開ステップと、

CPUが、前記記憶手段から前記有理点Q及び前記係数c[i]を読み出して、Q[i]＝c[i]Qにより表される演算をi＝0から所定回繰り返し行って各Q[i]の値を前記記憶手段に記憶する演算ステップと、

CPUが、t-1に換えて有理点に対するフロベニウス自己準同型写像ϕ_qを用いて表される次式のスカラー倍算nQに基づいて、

[数3]

$$nQ = \sum_i \phi_q^i(Q[i]).$$

前記記憶手段からQ[i]及び演算結果Zを読み出し、$Z \leftarrow Z + \phi_q^i(Q[i])$により表される代入演算をi＝0から所定回繰り返し行ってスカラー倍算の演算結果Zを前記記憶手段に記憶する合成ステップと、

を有するものである。

[0017] さらに、本発明のスカラー倍算の演算方法では、

前記楕円曲線の有限体F_qの位数q、$\#E(F_q)$を割り切る素数位数r、フロベニウス自己準同型写像ϕ_qのトレースtが、整数変数χを用いてそれぞれq(χ)、r(χ)、t(χ)で与えられている場合に、

CPUが、前記q(χ)、r(χ)、t(χ)の各値を入力して前記記憶手段に記憶する補助入力ステップと、

CPUが、前記記憶手段からr(χ)及びt(χ)の値を読み出して、前記s(χ)＝t(χ)－1として、r(χ)をs(χ)進展開した次式に基づいて、

[数4]

$$r(\chi)=\sum_{i=0}^{\lceil \deg r(\chi)/\deg s(\chi)\rceil} D_i(\chi)s(\chi)^i, 0\le \deg(D_i(\chi))<\deg(s(\chi)).$$

$D_i(\chi)\leftarrow r(\chi)\%s(\chi)$及び$r(\chi)\leftarrow(r(\chi)-D_i(\chi))/s(\chi)$により表される代入演算をi＝0からi<「degr(χ)/degs(χ)」まで繰り返し行って、各係数$D_i(\chi)$及びr(χ)の値を前記記憶手段に記憶する補助展開ステップと、

CPUが、前記記憶された係数$D_i(\chi)$のうち、deg($D_i(\chi)$)が最大のものを$D_{dmax}(\chi)$として抽出し、前記記憶手段に記憶する補助抽出ステップと、

CPUが、前記記憶手段から$D_{dmax}(\chi)$、$D_i(\chi)$、Qの値を読み出して、

$$\phi_q^{dmax}([D_{dmax}(\chi)]Q)=\Sigma\,\phi_q^{i}([D_i(\chi)]Q)-\phi_q^{dmax}([D_{dmax}(\chi)]Q)$$
$$=[f(\phi_q,\chi)]Q$$

となる多項式$f(\phi_q,\chi)$を用い、$\phi_q^{k}Q=Q$に基づいて

$$[D_{dmax}(\chi)]Q=[f(\phi_q,\chi)\phi_q^{-dmax}]Q=[h(\phi_q,\chi)]Q$$

となる多項式$h(\phi_q,\chi)$を特定し、前記多項式$h(\phi_q,\chi)$の値を前記記憶手段に記憶する補助特定ステップと、

CPUが、前記s進展開をχ＝aとしてs＝D_{dmax}(a)からなるD_{dmax}(a)進展開に置換え、前記D_{dmax}(a)に換えて前記多項式$h(\phi_q,a)$を用いるステップと、を有するものである。

[0018] しかも、本発明のスカラー倍算の演算方法では、

前記係数$D_i(\chi)$において最高次数dmaxとなる係数$D_i(\chi)$が複数存在する場合に、

前記補助入力ステップは、CPUが、r(χ)｜m(χ)を満たすm(χ)の値を入力して前記記憶手段に記憶するステップを更に含み、

CPUが、deg($D_i(\chi)$)の最高次数dmaxの項であるχ^{dmax}の係数を$T_{dmax}(\phi_q)$として、前記記憶手段から係数$D_i(\chi)$を読み出し、前記記憶手段に$T(\phi_q,\chi)$及び$U(\phi_q,\chi)$

を初期値を0として割り当て、$\deg(D_i(\chi))=\mathrm{dmax}$となる場合に$T(\phi_q,\chi)\leftarrow T(\phi_q,\chi)+D_i(\chi)\phi_q^i$、その他の場合に$U(\phi_q,\chi)\leftarrow U(\phi_q,\chi)+D_i(\chi)\phi_q^i$により表される代入演算をi＝0からi<「degr(χ)/degs(χ)」まで繰り返し行って、$T(\phi_q,\chi)$及び$U(\phi_q,\chi)$の値を前記記憶手段に記憶し、最高次数係数$T_{\mathrm{dmax}}(\phi_q)$を特定する第2の補助特定ステップと、

CPUが、前記記憶手段からm(χ)及びR(χ)の値を読み出して、r(χ)｜m(χ)を満たす最小次数の多項式m(χ)を用いて

$$V(\phi_q)\mid m(\phi_q),\gcd(T_{\mathrm{dmax}}(\phi_q),V(\phi_q))=1$$

を満たす$V(\phi_q)$を、$W(\phi_q)\leftarrow\gcd(T_{\mathrm{dmax}}(\phi_q),m(\phi_q))$及び$V(\phi_q)\leftarrow W(\phi_q)$により表される代入演算を行って特定し、前記$V(\phi_q)$の値を前記記憶手段に記憶する第3の補助特定ステップと、

CPUが、前記記憶手段から$V(\phi_q)$及び$m(\phi_q)$の値を読み出して、

$$g(\phi_q)V(\phi_q)\equiv v(\mathrm{mod}\ m(\phi_q))$$

を満たす整数のスカラーv及び$g(\phi_q)$を拡張ユークリッドの互除法により特定し、前記スカラーv及び$g(\phi_q)$の値を前記記憶手段に記憶する第4の補助特定ステップと、

前記補助特定ステップに換えて、CPUが、前記記憶手段から$T_{\mathrm{dmax}}(\phi_q)$、$\chi^{\mathrm{dmax}}$、$D_i(\chi)$、Qの各値を読み出して、

$$[T_{\mathrm{dmax}}(\phi_q)\chi^{\mathrm{dmax}}]Q=\Sigma\phi_q^i([D_i(\chi)]Q)-[T_{\mathrm{dmax}}(\phi_q)\chi^{\mathrm{dmax}}]Q$$
$$=[f(\phi_q,\chi)]Q$$

となる多項式$f(\phi_q,\chi)$と、前記$g(\phi_q)$を用い、$\phi_q^k Q=Q$に基づいて、

$$[v\chi^{\mathrm{dmax}}]Q=[g(\phi_q)f(\phi_q,\chi)]Q=[h(\phi_q,\chi)]Q$$

となる多項式$h(\phi_q,\chi)$を特定し、前記多項式$h(\phi_q,\chi)$の値を前記記憶手段に記憶する第5の補助特定ステップと、

CPUが、前記記憶手段から前記$h(\phi_q,\chi)$の値を読み出して、

この$h(\phi_q,\chi)$のϕ_qに関する定数項$h(0,\chi)$が、

$$[v\chi^{\mathrm{dmax}}-h(0,\chi)]Q=[h(\phi_q,\chi)-h(0,\chi)]Q$$

を満たすことを用いて、

$\chi=a$として、$s'=va^{\mathrm{dmax}}-h(0,a)$及び$h'(\phi_q)=h(\phi_q,a)-h(0,a)$により表される演算

を行ってs'、h'(ϕ_q)の値を前記記憶手段に記憶し、

t-1進展開した前記nをD_{dmax}(a)進展開する換わりにva^{dmax}－h(0,a)進展開して、va^{dmax}－h(0,a)の換わりにh(ϕ_q,a)－h(0,a)を用いるステップと、を有するものである。

[0019] また、本発明のべき乗算の演算方法では、

F_q^kを位数qの有限体F_qのk次拡大体、

HをF_q^kの素数位数rの部分乗法群、

ϕ_qを有限体F_qに関する元のフロベニウス自己準同型写像として、

非負整数nに対するHの元Aのn乗算を行うべき乗算を、CPU及び記憶手段を備えた電子計算機により演算する演算方法において、

CPUが、前記非負整数nの値、前記位数qの値、前記F_q^kの素数位数rの値、A∈H⊂F_q^kにより表される元Aの値を入力して前記記憶手段に記憶する入力ステップと、

CPUが、演算結果Zを記憶する前記記憶手段を初期化する初期化ステップと、

CPUが、前記位数q、前記元Aの値を前記記憶手段から読み出して、前記qとrの差分をs＝q－rとし、T[j]←A及びA←A*Aにより表される代入演算を、j＝0からj<「$\log_2$ s」まで繰り返して行って前記T[j]及び前記Aの値を前記記憶手段に記憶する第1の演算ステップと、

CPUが、前記記憶手段から前記n及び差分sの値を読み出して、差分sにより展開した次式に基づいて、

[数5]

$$n = \sum_i c[i]s^i, 0 \le c[i] \le s.$$

c[i]←n%s及びn←(n-c[i])/sにより表される代入演算をi＝0から所定回繰り返して行い、各係数c[i]及び非負整数nの値を前記記憶手段に記憶する展開ステップと、

CPUが、前記記憶手段からc[i]及び前記nの値を読み出して、A[i]＝$A^{c[i]}$に基づいて、A[i]＝1に初期化し、c[i]&1である場合にA[i]←A[i]*T[j]、c[i]←c[i]/2により表される代入演算を、i＝0から所定回繰り返して行い、前記記憶手段にA[i]及びc[i]の値を記憶する第2の演算ステップと、

CPUが、前記記憶手段から各A[i]を読み出し、次式に基づいて、

[数6]

$$A^n = \prod_i \phi_q^i(A[i]).$$

Z←Z＊ϕ_q^i(A[i])により表されるべき乗演算を、i＝0から所定回繰り返して行い、計算結果Zとして前記記憶手段に記憶する合成ステップと、を有するものである。

[0020] さらに、本発明のべき乗算の演算方法では、

X^{Y}はX^{Y}であることを表すこととし、

前記位数q、前記素数位数r、前記sが、整数変数χを用いてそれぞれq(χ)、r(χ)、s(χ)で与えられている場合に、

CPUが、前記q(χ)、r(χ)、s(χ)の各値を入力して前記記憶手段に記憶する補助入力ステップと、

CPUが、前記記憶手段からr(χ)及びs(χ)を読み出して、前記s(χ)を用いて前記r(χ)をs(χ)進展開した次式に基づいて、

[数7]

$$r(\chi) = \sum_{i=0}^{\lceil \deg r(\chi)/\deg s(\chi) \rceil} D_i(\chi)s(\chi)^i, 0 \le \deg(D_i(\chi)) < \deg(s(\chi)).$$

D_i(χ)←r(χ)%s(χ)及びr(χ)←(r(χ)-D_i(χ))/s(χ)により表される代入演算を、i＝0からi<「degr(χ)/degs(χ)」まで繰り返して行い、前記係数D_i(χ)及びr(χ)を前記記憶手段に記憶する補助展開ステップと、

CPUが、前記記憶された係数D_i(χ)のうち、deg(D_i(χ))が最大のものをD_{dmax}(χ)として抽出し、前記記憶手段に記憶する補助抽出ステップと、

CPUが、前記記憶手段から前記D_{dmax}(χ)、D_i(χ)、qの値を読み出して、

(A^{D_{dmax}(χ)})^{q^{dmax}}＝A^{Σ$_{i\neq dmax}$－D_i(χ)q^i}＝A^{f(q,χ)}

となる多項式f(q,χ)を用い、ϕ_q^k(A)＝Aに基づいて

A^{D_{dmax}(χ)}＝A^{Σ$_{i\neq dmax}$－D_i(χ)q^i－q^{dmax}}＝A^{h(q,χ)}

となる多項式h(q,χ)を特定し、前記多項式h(q,χ)の値を前記記憶手段に記憶する補助特定ステップと、

CPUが、前記s進展開した前記nを、χ＝aとしてs＝D_{dmax}(a)からなるD_{dmax}(a)進展

開に置き換え、前記$D_{dmax}(a)$に換えて前記多項式h(q,a)を用いるステップと、を有するものである。

[0021] しかも、本発明のべき乗算の演算方法では、

前記係数$D_i(\chi)$において最高次数dmaxとなる係数$D_i(\chi)$が複数存在する場合に、

前記補助記憶ステップは、CPUが、$r(\chi) \mid m(\chi)$を満たす$m(\chi)$の値を入力して前記記憶手段に記憶するステップを更に含み、

CPUが、$\deg(D_i(\chi))$の最高次数dmaxの項であるχ^{dmax}の係数を$T_{dmax}(q)$として、前記記憶手段から係数$D_i(\chi)$を読み出し、前記記憶手段に$T(q,\chi)$及び$U(q,\chi)$を初期値を0として割り当て、$\deg(D_i(\chi))=dmax$となる場合に$T(q,\chi) \leftarrow T(q,\chi)+D_i(\chi)q^i$、その他の場合に$U(q,\chi) \leftarrow U(q,\chi)+D_i(\chi)q^i$により表される代入演算をi＝0からi<「$\deg r(\chi)/\deg s(\chi)$」まで繰り返して行って$T(q,\chi)$及び$U(q,\chi)$の値を前記記憶手段に記憶し、最高次数係数$T_{dmax}(q)$を特定する第2の補助特定ステップと、

CPUが、前記記憶手段から$m(\chi)$及び$R(\chi)$の値を読み出して、$r(\chi) \mid m(\chi)$を満たす最小次数の多項式$m(\chi)$を用いて

$$V(q) \mid m(q), \gcd(T_{dmax}(q), V(q)) = 1$$

を満たすV(q)を、$W(q) \leftarrow \gcd(T_{dmax}(q), m(q))$及び$V(q) \leftarrow W(q)$により表される演算を行って特定し、前記V(q)の値を前記記憶手段に記憶する第3の補助特定ステップと、

CPUが、前記記憶手段からV(q)及びm(q)の値を読み出して、

$$g(q)V(q) \equiv v \pmod{m(q)}$$

を満たす整数のスカラーv及びg(q)を拡張ユークリッドの互除法により特定し、前記スカラーv及びg(q)の値を前記記憶手段に記憶する第4の補助特定ステップと、

前記補助特定ステップに換えて、CPUが、前記記憶手段から$T_{dmax}(q)$、χ^{dmax}、$D_i(\chi)$、Qの各値を読み出して、

$$A\hat{}\{T_{dmax}(q)\chi^{dmax}\} = A\hat{}\{\Sigma D_i(\chi)q^i - T_{dmax}(q)\chi^{dmax}\}$$
$$= A\hat{}\{f(q,\chi)\}$$

となる多項式$f(q,\chi)$と、前記g(q)を用い、$\phi_q^k(A)=A$に基づいて、

$$A\hat{}\{v\chi^{dmax}\} = A\hat{}\{g(q)f(q,\chi)\} = A\hat{}\{h(q,\chi)\}$$

となる多項式h(q,χ)を特定し、前記多項式h(q,χ)の値を前記記憶手段に記憶する第5の補助特定ステップと、

CPUが、前記記憶手段から前記h(q,χ)の値を読み出して、

このh(q,χ)のqに関する定数項h(0,χ)が、

$A\hat{}\{v\chi^{dmax}-h(0,\chi)\}=A\hat{}\{h(q,\chi)-h(0,\chi)\}$

を満たすことを用いて、

χ＝aとして、$s'=va^{dmax}-h(0,a)$及び$h'(q)=h(q,a)-h(0,a)$により表される演算を行ってs'、h'(q)の値を前記記憶手段に記憶し、s進展開した前記nをD_{dmax}(a)進展開する換わりに$va^{dmax}-h(0,a)$進展開して、$va^{dmax}-h(0,a)$の換わりにh(q,a)－h(0,a)を用いるステップと、を有するものである。

[0022] また、本発明のスカラー倍算の演算プログラムを記録した電子計算機読取可能な記録媒体では、

楕円曲線を$E/F_q=x^3+ax+b-y^2=0$, $a\in F_q$, $b\in F_q$とし、

$E(F_q)$を有限体F_qで定義される楕円曲線の有理点が成す加法群、

$E(F_q^k)$を有限体F_qの拡大体F_q^kで定義される楕円曲線の有理点が成す加法群、

ϕ_qを有限体F_qに関する有理点のフロベニウス自己準同型写像、

tをフロベニウス自己準同型写像ϕ_qのトレース、

rを$E(F_q)$の位数$\#E(F_q)=q+1-t$を割り切る素数位数、

E[r]を位数が素数rである有理点の集合、

[j]を有理点をj倍する写像、

Gを

$G=E[r]\cap Ker(\phi_q-[q])$

を満たす$E(F_q^k)$に含まれる有理点の集合として、

非負整数nに対するGの有理点Qのスカラーn倍算を、CPU及び記憶手段を備えた電子計算機に実行させるためのスカラー倍算の演算プログラムにおいて、

電子計算機に、

前記非負整数nの値、前記トレースtの値、及び、$Q\in G\subset E(F_q^k)$により表される有理点Qの値を入力して前記記憶手段に記憶する入力手順と、

演算結果Zを記憶する前記記憶手段を初期化する初期化手順と、

Gの有理点Qに対し、

$\phi_q(Q)=[q]Q=[t-1]Q$

が成り立つことにより、

s＝t－1として、前記nをs進展開した次式に基づいて、

[数8]

$$n=\sum_i c[i]s^i, 0\le c[i]\le s.$$

c[i]←n％s及びn←(n-c[i])/sにより表される代入演算をi＝0から所定回繰り返し行って各係数c[i]及び非負整数nの値を前記記憶手段に記憶する展開手順と、

前記記憶手段から前記有理点Q、非負整数n、及び前記c[i]の値を読み出して、Q[i]＝c[i]Qにより表される演算をi＝0から所定回繰り返し行って各Q[i]の値を前記記憶手段に記憶する演算手順と、

t-1に換えて有理点に対するフロベニウス自己準同型写像ϕ_qを用いて表される次式のスカラー倍算nQに基づいて、

[数9]

$$nQ=\sum_i \phi_q^i(Q[i]).$$

前記記憶手段からQ[i]及び演算結果Zを読み出し、Z←Z+ϕ_q^i(Q[i])により表される代入演算をi＝0から所定回繰り返し行ってスカラー倍算の演算結果Zを前記記憶手段に記憶する合成手順と、を実行させるものである。

[0023] さらに、本発明のスカラー倍算の演算プログラムを記録した電子計算機読取可能な記録媒体では、

前記楕円曲線の有限体F_qの位数q、$\#E(F_q)$を割り切る素数位数r、フロベニウス自己準同型写像ϕ_qのトレースtが、整数変数χを用いてそれぞれq(χ)、r(χ)、t(χ)で与えられている場合に、電子計算機に、

前記q(χ)、r(χ)、t(χ)の各値を入力して前記記憶手段に記憶する補助入力手順と、

前記記憶手段からr(χ)及びt(χ)の値を読み出して、前記s(χ)＝t(χ)－1として

、r(χ)をs(χ)進展開した次式に基づいて、

[数10]

$$r(\chi)=\sum_{i=0}^{\lceil \deg r(\chi)/\deg s(\chi)\rceil} D_i(\chi)s(\chi)^i, 0\le \deg(D_i(\chi))<\deg(s(\chi)).$$

$D_i(\chi)\leftarrow r(\chi)\%s(\chi)$及び$r(\chi)\leftarrow(r(\chi)-D_i(\chi))/s(\chi)$により表される代入演算をi＝0からi<「degr(χ)/degs(χ)」まで繰り返し行って、各係数$D_i(\chi)$及びr(χ)の値を前記記憶手段に記憶する補助展開手順と、

前記記憶された係数$D_i(\chi)$のうち、deg($D_i(\chi)$)が最大のものを$D_{dmax}(\chi)$として抽出し、前記記憶手段に記憶する補助抽出手順と、

前記記憶手段から$D_{dmax}(\chi)$、$D_i(\chi)$、Qの値を読み出して、

$$\phi_q^{dmax}([D_{dmax}(\chi)]Q)=\Sigma\,\phi_q^{i}([D_i(\chi)]Q)-\phi_q^{dmax}([D_{dmax}(\chi)]Q)$$
$$=[f(\phi_q,\chi)]Q$$

となる多項式$f(\phi_q,\chi)$を用い、$\phi_q^{k}Q=Q$に基づいて

$$[D_{dmax}(\chi)]Q=[f(\phi_q,\chi)\phi_q^{-dmax}]Q=[h(\phi_q,\chi)]Q$$

となる多項式$h(\phi_q,\chi)$を特定し、前記多項式$h(\phi_q,\chi)$の値を前記記憶手段に記憶する補助特定手順と、

前記s進展開をχ＝aとしてs＝D_{dmax}(a)からなるD_{dmax}(a)進展開に置換え、前記D_{dmax}(a)に換えて前記多項式$h(\phi_q,a)$を用いる手順と、を実行させるものである。

[0024] しかも、本発明のスカラー倍算の演算プログラムを記録した電子計算機読取可能な記録媒体では、

前記係数$D_i(\chi)$において最高次数dmaxとなる係数$D_i(\chi)$が複数存在する場合に、

前記補助入力手順は、r(χ)｜m(χ)を満たすm(χ)の値を入力して前記記憶手段に記憶する手順を更に含み、

電子計算機に、

deg($D_i(\chi)$)の最高次数dmaxの項であるχ^{dmax}の係数を$T_{dmax}(\phi_q)$として、前記記憶手段から係数$D_i(\chi)$を読み出し、前記記憶手段に$T(\phi_q,\chi)$及び$U(\phi_q,\chi)$を初期値を0として割り当て、deg($D_i(\chi)$)=dmaxとなる場合に$T(\phi_q,\chi)\leftarrow T(\phi_q,\chi)+D_i(\chi)\phi_q^{i}$、

その他の場合に$U(\phi_q,\chi)\leftarrow U(\phi_q,\chi)+D_i(\chi)\phi_q^i$により表される代入演算をi＝0からi＜「degr(χ)/degs(χ)」まで繰り返し行って、$T(\phi_q,\chi)$及び$U(\phi_q,\chi)$の値を前記記憶手段に記憶し、最高次数係数$T_{dmax}(\phi_q)$を特定する第2の補助特定手順と、

前記記憶手段からm(χ)及びR(χ)の値を読み出して、r(χ)｜m(χ)を満たす最小次数の多項式m(χ)を用いて

$$V(\phi_q)\mid m(\phi_q),\gcd(T_{dmax}(\phi_q),V(\phi_q))=1$$

を満たす$V(\phi_q)$を、$W(\phi_q)\leftarrow\gcd(T_{dmax}(\phi_q),m(\phi_q))$及び$V(\phi_q)\leftarrow W(\phi_q)$により表される代入演算を行って特定し、前記$V(\phi_q)$の値を前記記憶手段に記憶する第3の補助特定手順と、

CPUが、前記記憶手段から$V(\phi_q)$及び$m(\phi_q)$の値を読み出して、

$$g(\phi_q)V(\phi_q)\equiv v(\mathrm{mod}\ m(\phi_q))$$

を満たす整数のスカラーv及び$g(\phi_q)$を拡張ユークリッドの互除法により特定し、前記スカラーv及び$g(\phi_q)$の値を前記記憶手段に記憶する第4の補助特定手順と、

前記補助特定手順に換えて、CPUが、前記記憶手段から$T_{dmax}(\phi_q)$、χ^{dmax}、$D_i(\chi)$、Qの各値を読み出して、

$$[T_{dmax}(\phi_q)\chi^{dmax}]Q=\Sigma\,\phi_q^i([D_i(\chi)]Q)-[T_{dmax}(\phi_q)\chi^{dmax}]Q$$
$$=[f(\phi_q,\chi)]Q$$

となる多項式$f(\phi_q,\chi)$と、前記$g(\phi_q)$を用い、$\phi_q^k Q=Q$に基づいて、

$$[v\chi^{dmax}]Q=[g(\phi_q)f(\phi_q,\chi)]Q=[h(\phi_q,\chi)]Q$$

となる多項式$h(\phi_q,\chi)$を特定し、前記多項式$h(\phi_q,\chi)$の値を前記記憶手段に記憶する第5の補助特定手順と、

前記記憶手段から前記$h(\phi_q,\chi)$の値を読み出して、

この$h(\phi_q,\chi)$のϕ_qに関する定数項$h(0,\chi)$が、

$$[v\chi^{dmax}-h(0,\chi)]Q=[h(\phi_q,\chi)-h(0,\chi)]Q$$

を満たすことを用いて、

χ＝aとして、$s'=va^{dmax}-h(0,a)$及び$h'(\phi_q)=h(\phi_q,a)-h(0,a)$により表される演算を行ってs'、$h'(\phi_q)$の値を前記記憶手段に記憶し、

t−1進展開した前記nをD_{dmax}(a)進展開する換わりに$va^{dmax}-h(0,a)$進展開して、va^{dmax}

－h(0,a)の換わりにh(ϕ_q,a)－h(0,a)を用いる手順と、を実効させるためのスカラー倍算の演算プログラムを記録した電子計算機読取可能な記録媒体とした。

[0025] また、本発明のべき乗算の演算プログラムを記録した記録媒体では、

F_q^kを位数qの有限体F_qのk次拡大体、

HをF_q^kの素数位数rの部分乗法群、

ϕ_qを有限体F_qに関する元のフロベニウス自己準同型写像として、

非負整数nに対するHの元Aのn乗算を行うべき乗算を、CPU及び記憶手段を備えた電子計算機により実行させるための演算プログラムにおいて、電子計算機に、

前記非負整数nの値、前記位数qの値、前記F_q^kの素数位数rの値、$A \in H \subset F_q^k$により表される元Aの値を入力して前記記憶手段に記憶する入力手順と、

演算結果Zを記憶する前記記憶手段を初期化する初期化手順と、

前記位数q、前記元Aの値を前記記憶手段から読み出して、前記qとrの差分をs＝q－rとし、T[j]←A及びA←A*Aにより表される代入演算を、j＝0からj<「$\log_2 s$」まで繰り返し行って前記T[j]及び前記Aの値を前記記憶手段に記憶する第1の演算手順と、

前記記憶手段から前記n及び差分sの値を読み出して、差分sにより展開した次式に基づいて、

[数11]

$$n = \sum_i c[i]s^i, 0 \le c[i] \le s.$$

c[i]←n%s及びn←(n-c[i])/sにより表される代入演算をi＝0から所定回繰り返して行い、各係数c[i]及び非負整数nの値を前記記憶手段に記憶する展開手順と、

前記記憶手段からc[i]及び前記nの値を読み出して、$A[i]=A^{c[i]}$に基づいて、A[i]＝1に初期化し、c[i]&1である場合にA[i]←A[i]*T[j]、c[i]←c[i]/2により表される代入演算を、i＝0から所定回繰り返して行い、前記記憶手段にA[i]及びc[i]の値を記憶する第2の演算手順と、

前記記憶手段から各A[i]を読み出し、次式に基づいて、

[数12]

$$A^n = \prod_i \phi_q^i(A[i]).$$

Z←Z＊ϕ_q^i(A[i])により表されるべき乗演算を、i＝0から所定回繰り返して行い、計算結果Zとして前記記憶手段に記憶する合成手順と、を実行させるためのべき乗算の演算プログラムを記録した電子計算機読取可能な記録媒体とした。

[0026] さらに、本発明のべき乗算の演算プログラムを記録した記録媒体では、

X^{Y}はX^Yであることを表すこととし、

前記位数q、前記素数位数r、前記sが、整数変数χを用いてそれぞれq(χ)、r(χ)、s(χ)で与えられている場合に、電子計算機に、

前記q(χ)、r(χ)、s(χ)の各値を入力して前記記憶手段に記憶する補助入力手順と、

前記記憶手段からr(χ)及びs(χ)を読み出して、前記s(χ)を用いて前記r(χ)をs(χ)進展開した次式に基づいて、

[数13]

$$r(\chi)=\sum_{i=0}^{\lfloor \deg r(\chi)/\deg s(\chi)\rfloor} D_i(\chi)s(\chi)^i, 0\le \deg(D_i(\chi))<\deg(s(\chi)).$$

$D_i(\chi)$←r(χ)%s(χ)及びr(χ)←(r(χ)-D_i(χ))/s(χ)により表される代入演算を、i＝0からiく「degr(χ)/degs(χ)」まで繰り返して行い、前記係数$D_i(\chi)$及びr(χ)を前記記憶手段に記憶する補助展開手順と、

前記記憶された係数$D_i(\chi)$のうち、deg($D_i(\chi)$)が最大のものを$D_{dmax}(\chi)$として抽出し、前記記憶手段に記憶する補助抽出手順と、

前記記憶手段から前記$D_{dmax}(\chi)$、$D_i(\chi)$、qの値を読み出して、

$(A^{D_{dmax}(\chi)})^{q^{dmax}}=A^{\Sigma_{i\neq dmax}-D_i(\chi)q^i}=A^{f(q,\chi)}$

となる多項式f(q,χ)を用い、$\phi_q^k(A)=A$に基づいて

$A^{D_{dmax}(\chi)}=A^{\Sigma_{i\neq dmax}-D_i(\chi)q^i-q^{dmax}}=A^{h(q,\chi)}$

となる多項式h(q,χ)を特定し、前記多項式h(q,χ)の値を前記記憶手段に記憶する補助特定手順と、

前記s進展開した前記nを、χ＝aとしてs＝D_{dmax}(a)からなるD_{dmax}(a)進展開に置き換え、前記D_{dmax}(a)に換えて前記多項式h(q,a)を用いる手順と、を実行させるためのべき乗算の演算プログラムを記録した電子計算機読取可能な記録媒体とした。

[0027] しかも、本発明のべき乗算の演算プログラムを記録した記録媒体では、前記係数$D_i(\chi)$において最高次数dmaxとなる係数$D_i(\chi)$が複数存在する場合に、

前記補助記憶手順は、$r(\chi) \mid m(\chi)$を満たす$m(\chi)$の値を入力して前記記憶手段に記憶する手順を更に含み、

電子計算機に、

$deg(D_i(\chi))$の最高次数dmaxの項であるχ^{dmax}の係数を$T_{dmax}(q)$として、前記記憶手段から係数$D_i(\chi)$を読み出し、前記記憶手段に$T(q,\chi)$及び$U(q,\chi)$を初期値を0として割り当て、$deg(D_i(\chi))=dmax$となる場合に$T(q,\chi) \leftarrow T(q,\chi)+D_i(\chi)q^i$、その他の場合に$U(q,\chi) \leftarrow U(q,\chi)+D_i(\chi)q^i$により表される代入演算をi＝0からi<「$degr(\chi)/degs(\chi)$」まで繰り返して行って$T(q,\chi)$及び$U(q,\chi)$の値を前記記憶手段に記憶し、最高次数係数$T_{dmax}(q)$を特定する第2の補助特定手順と、

前記記憶手段から$m(\chi)$及び$R(\chi)$の値を読み出して、$r(\chi) \mid m(\chi)$を満たす最小次数の多項式$m(\chi)$を用いて

$$V(q) \mid m(q), gcd(T_{dmax}(q), V(q)) = 1$$

を満たす$V(q)$を、$W(q) \leftarrow gcd(T_{dmax}(q), m(q))$及び$V(q) \leftarrow W(q)$により表される演算を行って特定し、前記$V(q)$の値を前記記憶手段に記憶する第3の補助特定手順と、

前記記憶手段から$V(q)$及び$m(q)$の値を読み出して、

$$g(q)V(q) \equiv v \pmod{m(q)}$$

を満たす整数のスカラーv及び$g(q)$を拡張ユークリッドの互除法により特定し、前記スカラーv及び$g(q)$の値を前記記憶手段に記憶する第4の補助特定手順と、

前記補助特定手順に換えて、前記記憶手段から$T_{dmax}(q)$、χ^{dmax}、$D_i(\chi)$、Qの各値を読み出して、

$$\hat{A}\{T_{dmax}(q)\chi^{dmax}\} = \hat{A}\{\Sigma D_i(\chi)q^i - T_{dmax}(q)\chi^{dmax}\}$$
$$= \hat{A}\{f(q,\chi)\}$$

となる多項式$f(q,\chi)$と、前記$g(q)$を用い、$\phi_q^k(A)=A$に基づいて、

$$\hat{A}\{v\chi^{dmax}\} = \hat{A}\{g(q)f(q,\chi)\} = \hat{A}\{h(q,\chi)\}$$

となる多項式$h(q,\chi)$を特定し、前記多項式$h(q,\chi)$の値を前記記憶手段に記憶する第5の補助特定手順と、

CPUが、前記記憶手段から前記h(q,χ)の値を読み出して、

このh(q,χ)のqに関する定数項h(0,χ)が、

$A\hat{}\{v\chi^{dmax}-h(0,\chi)\}=A\hat{}\{h(q,\chi)-h(0,\chi)\}$

を満たすことを用いて、

χ＝aとして、s'＝va^{dmax}－h(0,a)及びh'(q)＝h(q,a)－h(0,a) により表される演算を行ってs'、h'(q)の値を前記記憶手段に記憶し、s進展開した前記nをD_{dmax}(a)進展開する換わりにva^{dmax}－h(0,a)進展開して、va^{dmax}－h(0,a)の換わりにh(q,a)－h(0,a)を用いる手順と、を実行させるためのべき乗算の演算プログラムを記録した電子計算機読取可能な記録媒体とした。

発明の効果

[0028] 本発明は、フロベニウス自己準同型写像ϕ_q用いて演算回数を削減するものであって、特に、スカラー倍算の場合には、Gの有理点Qに対し、

$\phi_q(Q)=[q]Q=[t-1]Q$

が成り立つことにより、また、べき乗算の場合には、qとrの差分をs＝q－rとし、Hの非零元Aに対し、

$\phi_q(A)=A^q=A^s$

が成り立つことにより、スカラーnをt-1進展開、またはべき数nをs進展開して、t-1に換えて有理点に対するフロベニウス自己準同型写像ϕ_qを用い、またはsに換えて元に対するフロベニウス自己準同型写像ϕ_qを用いることにより、スカラー倍算におけるスカラーn、またはべき乗算における乗数nが位数qを大きく上回ることのない場合でも、演算回数を削減可能として演算速度を向上させることができる。

[0029] 特に、ペアリングをベースとしたIDベース暗号やグループ署名などでは、ペアリングフレンドリ曲線と呼ばれるペアリングを利用可能な楕円曲線が用いられ、このペアリングフレンドリ曲線を用いる場合には、整数変数χを用いて位数q(χ)、＃$E(F_q)$を割り切る素数位数r(χ)、フロベニウス自己準同型写像ϕ_qのトレースt(χ)があらかじめ与えられており、スカラー倍算の場合には、r(χ)をt(χ)－1進展開するとともに、このt(χ)－1進展開の際に導入した係数$D_i(\chi)$のうちでもっとも次数の高い係数$D_i(\chi)$を$D_{dmax}(\chi)$とし、この$D_{dmax}(\chi)$を多項式$h(\phi_q,\chi)$に置き換えることにより演算回数をさらに

削減し、また、べき乗算の場合には、$r(\chi)$を$s(\chi)=q(\chi)-r(\chi)$進展開するとともに、この$s(\chi)$進展開の際に導入した係数$D_i(\chi)$のうちでもっとも次数の高い係数$D_i(\chi)$を$D_{dmax}(\chi)$とし、この$D_{dmax}(\chi)$を多項式$h(\phi_q,\chi)$に置き換えることにより演算回数をさらに削減し、それぞれ演算速度を向上させることができる。

[0030] しかも、最高次数dmaxとなる$D_i(\chi)$が複数存在する場合には、$r(\chi)\mid m(\chi)$を満たす最小次数の多項式$m(\chi)$を用いて

$$V(q)\mid m(q),\gcd(T_{dmax}(q),V(q))=1$$

を満たす$V(q)$を特定するとともに、

$$g(q)V(q)\equiv v(\mathrm{mod}\ m(q))$$

を満たす整数のスカラーvを用い、スカラー倍算の場合には、t-1進展開したスカラーnを$D_{dmax}(\chi)$進展開する換わりに$v\chi^{dmax}-h(0,\chi)$進展開して、$v\chi^{dmax}-h(0,\chi)$の換わりに$h(q,\chi)-h(0,\chi)$を用いることにより演算回数をさらに削減し、また、べき乗算の場合には、s進展開したべき数nを$D_{dmax}(\chi)$進展開する換わりに$v\chi^{dmax}-h(0,\chi)$進展開して、$v\chi^{dmax}-h(0,\chi)$の換わりに$h(q,\chi)-h(0,\chi)$を用いることにより演算回数をさらに削減し、それぞれ演算速度を向上させることができる。

図面の簡単な説明

[0031] [図1]スカラー倍算の演算プログラム及びべき乗算の演算プログラムを備えた電子計算機の説明図。

[図2]スカラー倍算の演算プログラムのフローチャートである。

[図3]スカラー倍算の演算プログラムのフローチャートである。

[図4]$D_{dmax}(\chi)$及び多項式$h(\phi_q,\chi)$を求める補助プログラムのフローチャートである。

[図5]スカラー倍算の演算プログラムのフローチャートである。

[図6]多項式$h(\phi_q,\chi)$及び$v\chi^{dmax}-h(0,\chi)$を求める補助プログラムのフローチャートである。

[図7]べき乗算の演算プログラムのフローチャートである。

[図8]べき乗算の演算プログラムのフローチャートである。

[図9]$D_{dmax}(\chi)$及び多項式$h(q,\chi)$を求める補助プログラムのフローチャートである

。

[図10]べき乗算の演算プログラムのフローチャートである。

[図11]多項式h(q, χ)及びvχ^{dmax}－h(0, χ)を求める補助プログラムのフローチャートである。

符号の説明

[0032] 10 電子計算機

11 CPU

12 記憶装置

13 メモリ装置

14 バス

15 入出力制御部

20 電気通信回線

30 クライアント装置

発明を実施するための最良の形態

[0033] 本発明は、スカラー倍算の演算の高速化及びべき乗算の演算の高速化を目的としたものであり、スカラー倍算とべき乗算というように演算自体は異なるが、高速化のための手法は同じであり、それぞれ同じように演算回数が削減されることにより、演算の高速化を可能としているものである。最初にスカラー倍算について説明し、次いでべき乗算について説明する。

[0034] まず、楕円曲線をE／F_q ＝x^3＋ax＋b－y^2＝0, a∈F_q, b∈F_qとし、

$E(F_q)$:有限体F_qで定義される楕円曲線の有理点が成す加法群

$E(F_q^k)$:有限体F_qの拡大体F_q^kで定義される楕円曲線の有理点が成す加法群

ϕ_q:有限体F_qに関する有理点のフロベニウス自己準同型写像

t:フロベニウス自己準同型写像ϕ_qのトレース

r:$E(F_q)$の位数＃$E(F_q)$＝q＋1－tを割り切る素数位数

E[r]:位数が素数rである有理点の集合

[j]:有理点をj倍する写像

G:G＝E[r]∩Ker(ϕ_q－[q])を満たす$E(F_q^k)$に含まれる有理点の集合

と定義する。

[0035] そして、非負整数nに対するGの有理点Qのスカラーn倍算、すなわちnQを演算する。なお、本実施形態で想定するスカラー倍算はペアリングの演算の際に行われるものであり、一般的にスカラーnは位数rを大きく超えるものではない。

[0036] また、$r=q+1-t$であることから、$0\equiv q+1-t \pmod r$である。

[0037] ここで、スカラーnをt－1進展開すると、スカラーnが位数rを大きく超えるものではないことから、

$$n=C_1(t-1)+C_0$$

または、

$$n=(t-1)^2+C_1(t-1)+C_0$$

となる。

[0038] $\phi_q(Q)=[q]Q=[t-1]Q$であるので、$n=C_1(t-1)+C_0$の場合、nQは以下のようになる。

$$\begin{aligned} nQ&=[C_1(t-1)+C_0]Q \\ &=[C_1q]Q+[C_0]Q \\ &=\phi_q([C_1]Q)+[C_0]Q \end{aligned}$$

[0039] また、$n=(t-1)^2+C_1(t-1)+C_0$場合には、nQは以下のようになる。

$$\begin{aligned} nQ&=[(t-1)^2+C_1(t-1)+C_0]Q \\ &=[q][q]Q+[C_1q]Q+[C_0]Q \\ &=\phi_q(\phi_q(Q))+\phi_q([C_1]Q)+[C_0]Q \end{aligned}$$

[0040] ここで、C_1及びC_0はt－1と同程度あるいはそれよりも小さくなり、しかも有理点のフロベニウス自己準同型写像を用いることができることによって演算回数を削減できる。したがって、スカラー倍算を高速化することができる。

[0041] また、通常、ペアリングの演算を行う場合には、既知のペアリングフレンドリ曲線が用いられており、特に、整数変数χを用いて位数$q(\chi)$、$\#E(F_q)$を割り切る素数位数$r(\chi)$、フロベニウス自己準同型写像ϕ_qのトレース$t(\chi)$があらかじめ与えられていることが多い。

[0042] ここで、$[r]Q=[q+1-t]Q=O$であることを考慮しながら、$r(\chi)$を$t(\chi)-1$で剰余を

とる。すなわち、$r(\chi)$を、

$$[r(\chi)]Q=\Sigma[D_i(\chi)(t(\chi)-1)^i]Q=\Sigma\ \phi_q^i([D_i(\chi)]Q)$$

と$t(\chi)-1$進展開して、$D_i(\chi)$のうちでもっとも次数の高いものを$D_{dmax}(\chi)$とする。

[0043] そして、

$$\phi_q^{dmax}([D_{dmax}(\chi)]Q)=\Sigma\ \phi_q^i([D_i(\chi)]Q)-\phi_q^{dmax}([D_{dmax}(\chi)]Q)$$
$$=[f(\phi_q,\chi)]Q$$

として定義されるϕ_qとχを変数とする2変数の多項式$f(\phi_q,\chi)$を導入する。

[0044] さらに、$\phi_q^k Q=Q$に基づいて、

$$[D_{dmax}(\chi)]Q=[f(\phi_q,\chi)\phi_q^{-dmax}]Q=[h(\phi_q,\chi)]Q$$

として定義されるϕ_qとχを変数とする2変数の多項式$h(\phi_q,\chi)$を導入する。すなわち、この多項式$h(\phi_q,\chi)$は、$D_i(\chi)$のうちの最高次数の$D_{dmax}(\chi)$を、ϕ_qとχを変数とする多項式$h(\phi_q,\chi)$に置き換え可能であることを示しており、最高次数よりも小さい次数までの演算に抑えることができ、特に、$\chi=a$とした場合には、t-1進展開したスカラーnをさらに$D_{dmax}(a)$進展開して、$D_{dmax}(a)$に換えて$h(\phi_q,a)$を用いることによって演算回数を大きく削減でき、スカラー倍算を高速化することができる。

[0045] また、$D_i(\chi)$のうちでもっとも次数の高いものが複数存在する場合には、最高次数をdmaxで表すものとし、最高次数dmaxの項であるχ^{dmax}の係数を$T_{dmax}(\phi_q)$として、$r(\chi)$｜$m(\chi)$を満たす最小次数の多項式$m(\chi)$を用いて

$$V(\phi_q)\mid m(\phi_q),\gcd(T_{dmax}(\phi_q),V(\phi_q))=1$$

を満たす$V(\phi_q)$を特定する。ここで、多項式$m(\chi)$には円周等分多項式などを用いることができる。

[0046] そして、拡張ユークリッドの互除法を用いて、

$$g(\phi_q)V(\phi_q)\equiv v(\mathrm{mod}\ m(\phi_q))$$

を満たす整数のスカラーv及び$g(\phi_q)$を特定し、

$$[T_{dmax}(\phi_q)\chi^{dmax}]Q=\Sigma\ \phi_q^i([D_i(\chi)]Q)-[T_{dmax}(\phi_q)\chi^{dmax}]Q$$
$$=[f(\phi_q,\chi)]Q$$

としてϕ_qとχを変数とする2変数の多項式$f(\phi_q,\chi)$を導入する。

[0047] さらに、$g(\phi_q)$を用い、$\phi_q^k Q=Q$に基づいて、

$[v\chi^{dmax}]Q=[g(\phi_q)f(\phi_q,\chi)]Q=[h(\phi_q,\chi)]Q$

としてϕ_qとχを変数とする2変数の多項式$h(\phi_q,\chi)$を導入する。

[0048] そして、この$h(\phi_q,\chi)$のϕ_qに関する定数項$h(0,\chi)$が、

$[v\chi^{dmax}-h(0,\chi)]Q=[h(\phi_q,\chi)-h(0,\chi)]Q$

を満たすことを用いて、$\chi=a$として、$s'=va^{dmax}-h(0,a)$及び$h'(\phi_q)=h(\phi_q,a)-h(0,a)$とし、t-1進展開したスカラーnを$D_{dmax}$(a)進展開する換わりに$\{va^{dmax}-h(0,a)\}$進展開して、$va^{dmax}-h(0,a)$の換わりに$h(\phi_q,a)-h(0,a)$を用いることにより演算回数を減できるので、スカラー倍算を高速化することができる。ここで、$h'(\phi_q)$は、ϕ_qとχの2変数の多項式$h(\phi_q,\chi)$において、$\chi=a$としたことによりϕ_qの1変数となっていることを示している。

[0049] ここまでスカラー倍算について説明したが、べき乗算の場合には、

F_q^k:位数qの有限体F_qのk次拡大体

H:F_q^kの素数位数rの部分乗法群

ϕ_q:有限体F_qに関する元のフロベニウス自己準同型写像

と定義して、非負整数nに対するHの元Aのn乗算を行うものであり、qとrの差分をs=q-rとし、このsをスカラー倍算におけるt-1に置き換えて上述の説明をべき乗算として読み換えるだけであり、詳細な説明は省略する。べき乗算の場合でも、最高次数部分の演算がより低い次数の演算に置き換えられることにより、演算回数を減してべき乗算を高速化することができる。

[0050] 以下において、既知のペアリングフレンドリ曲線を用いながら具体例を説明する。

[0051] 埋め込み次数8のペアリングフレンドリ曲線として、$\#E(F_q)$を割り切る素数$r(\chi)$、フロベニウス自己準同型写像ϕ_qのトレース$t(\chi)$が、

$r(\chi)=\chi^4-8\chi^2+25$

$t(\chi)=(2\chi^3-11\chi+15)/15$

と与えられるものが知られている。

[0052] この場合、$r(\chi)$を$t(\chi)-1$進展開して、フロベニウス準同型写像ϕ_qを用いることにより、

$2r(\chi)=(15\chi)\phi_q+(-5\chi^2+50)$

$$0\equiv(15\chi)\phi_q+(-5\chi^2+50)\pmod{r(\chi)}$$

となる。

[0053] したがって、$D_i(\chi)$は、

$$D_0(\chi)=-5\chi^2+50$$

$$D_1(\chi)=15\chi$$

となる。

[0054] このうち、$D_0(\chi)$が最も次数が高いので、$D_0(\chi)$以外を右辺に移すことにより、

$$-5\chi^2+50=15\chi\,\phi_q$$

となり、式を整理することにより、

$$\chi^2-10=3\chi\,\phi_q$$

が得られる。

[0055] したがって、非負整数nに対するGの有理点Qのスカラーn倍算、または非負整数nに対するHの元Aのn乗算を行わせるべき乗算を行う場合には、非負整数nに対してnをt－1進展開し、さらにχ^2-10進展開して、χ^2-10に換えて$15\chi\,\phi_q$を用いることにより、Gの有理点のスカラーn倍算またはHの元Aのn乗算を、有理点に対するフロベニウス自己準同型写像ϕ_qを用いて演算を行うことができ、演算回数を減してべき乗算を高速化することができる。

[0056] 他の埋め込み次数8のペアリングフレンドリ曲線として、$\#E(F_q)$を割り切る素数$r(\chi)$、フロベニウス自己準同型写像ϕ_qのトレース$t(\chi)$が

$$r(\chi)=\chi^8-\chi^4+1$$

$$t(\chi)=\chi^5-\chi+1$$

と与えられた場合には、$r(\chi)$を$t(\chi)-1$進展開し、フロベニウス準同型写像ϕ_qを用いることにより、

$$r(\chi)=\chi^3\phi_q+1$$

$$0\equiv3\phi_q+1\pmod{r(\chi)}$$

となる。

[0057] したがって、$D_i(\chi)$は、

$$D_0(\chi)=-1$$

$$D_1(\chi)=\chi^3$$

となる。

[0058] このうち、$D_1(\chi)$が最も次数が高いので、$D_1(\chi)\phi_q$以外を右辺に移すことにより、

$$\chi^3\phi_q=-1$$

となり、両辺にϕ_q^{-1}を掛けることで

$$\chi^3=-\phi_q^{-1}$$

が得られる。

[0059] したがって、非負整数nに対するGの有理点Qのスカラーn倍算、または非負整数nに対するHの元Aのn乗算を行わせるべき乗算を行う場合には、非負整数nに対してnをt－1進展開し、さらにχ^3進展開して、χ^3に換えて$-\phi_q^{-1}$を用いることにより、Gの有理点のスカラーn倍算またはHの元Aのn乗算を、有理点に対するフロベニウス自己準同型写像ϕ_qを用いて演算を行うことができ、演算回数を減してべき乗算を高速化することができる。

[0060] また、埋め込み次数10のペアリングフレンドリ曲線の場合には、$\#E(F_q)$を割り切る素数$r(\chi)$、フロベニウス自己準同型写像ϕ_qのトレース$t(\chi)$が、

$$r(\chi)=25\chi^4+25\chi^3+15\chi^2+5\chi+1$$

$$t(\chi)=10\chi^2+5\chi+3$$

と与えられるものが知られている。

[0061] この場合、$r(\chi)$を$t(\chi)-1$進展開して、フロベニウス準同型写像ϕ_qを用いることにより、

$$8r(\chi)=2\phi_q^2-\phi_q+(5\chi+2)$$

$$0\equiv 2\phi_q^2-\phi_q+(5\chi+2)\pmod{r(\chi)}$$

となる。

[0062] したがって、$D_i(\chi)$は、

$$D_0(\chi)=5\chi+2$$

$$D_1(\chi)=-1$$

$$D_2(\chi)=2$$

となる。

[0063] このうち、$D_0(\chi)$が最も次数が高いので、$D_0(\chi)$以外を右辺に移すことにより

$$5\chi+2=-2\phi_q^2+\phi_q$$

が得られる。

[0064] したがって、非負整数nに対するGの有理点Qのスカラーn倍算、または非負整数nに対するHの元Aのn乗算を行わせるべき乗算を行う場合には、非負整数nに対してnをt－1進展開し、さらに$5\chi+2$進展開して、$5\chi+2$に換えて$-2\phi_q^2+\phi_q$を用いることにより、Gの有理点のスカラーn倍算またはHの元Aのn乗算を、有理点に対するフロベニウス自己準同型写像ϕ_qを用いて演算を行うことができ、演算回数を減してべき乗算を高速化することができる。

[0065] また、埋め込み次数12のペアリングフレンドリ曲線の場合には、$\#E(F_q)$を割り切る素数$r(\chi)$、フロベニウス自己準同型写像ϕ_qのトレース$t(\chi)$が、

$$r(\chi)=36\chi^4-36\chi^3+18\chi^2-6\chi+1$$

$$t(\chi)=6\chi^2+1$$

と与えられるものが知られている。

[0066] この場合、$r(\chi)$を$t(\chi)-1$進展開して、フロベニウス準同型写像ϕ_qを用いることにより、

$$r(\chi)=\phi_q^2+(-6\chi+3)\phi_q+(-6\chi+1)$$

$$0\equiv\phi_q^2+(-6\chi+3)\phi_q+(-6\chi+1)\ (\mathrm{mod}\ r(\chi))$$

となる。

[0067] したがって、$D_i(\chi)$は、

$$D_0(\chi)=-6\chi+1$$

$$D_1(\chi)=-6\chi+3$$

$$D_2(\chi)=1$$

となる。

[0068] ここで、$D_0(\chi)$と$D_1(\chi)$が共に最も次数が高いので、$D_0(\chi)$と$D_1(\chi)\phi_q$の最高次数を与えるχの項以外を右辺に移すことにより、

$$6\chi(\phi_q+1)=\phi_q^2+3\phi_q+1$$

となる。

[0069] ここで、$g(\phi_q)=\phi_q^4-\phi_q^2+1$とすると、$\gcd(\phi_q+1, g(\phi_q))=1$を満たし、拡張ユークリッドの互除法より

$$(\phi_q+1)^{-1}\equiv\phi_q^2(1-\phi_q) \pmod{g(\phi_q)}$$

が得られる。

[0070] したがって、両辺に$\phi_q^2(1-\phi_q)$を乗じることにより、

$$6\chi=\phi_q^2(1-\phi_q)(\phi_q^2+3\phi_q+1)$$

が得られる。

[0071] したがって、非負整数nに対するGの有理点Qのスカラーn倍算、または非負整数nに対するHの元Aのn乗算を行わせるべき乗算を行う場合には、非負整数nに対してnをt－1進展開し、さらに6χ進展開して、6χに換えて$\phi_q^2(1-\phi_q)(\phi_q^2+3\phi_q+1)$を用いることにより、Gの有理点のスカラーn倍算またはHの元Aのn乗算を、有理点に対するフロベニウス自己準同型写像ϕ_qを用いて演算を行うことができ、演算回数を減してべき乗算を高速化することができる。

[0072] より具体的な例として、$\chi=825$(10ビット)とする。このとき、

$r=16656811746301$(44ビット)

$t=4083751$(22ビット)

である。

[0073] この場合、

$$6\chi=4950\text{(13ビット)}=\phi_q^2(1-\phi_q)(\phi_q^2+3\phi_q+1)$$

となるので、Gの有理点のスカラーn倍算またはHの元Aのn乗算を行う場合には、有理点に対するフロベニウス自己準同型写像ϕ_qを用いて13ビット程度のスカラー倍算またはべき乗算に変換してから演算を行うこととなり、演算回数の大幅な削減が可能となっている。

[0074] また、埋め込み次数18のペアリングフレンドリ曲線の場合には、$\#E(F_q)$を割り切る素数$r(\chi)$、フロベニウス自己準同型写像ϕ_qのトレース$t(\chi)$が、

$$r(\chi)=\chi^6+37\chi^3+343$$

$$t(\chi)=(\chi^4+16\chi+7)/7$$

と与えられるものが知られている。

[0075] この場合、r(χ)をt(χ)－1進展開して、フロベニウス準同型写像ϕ_qを用いることにより、

$$r(\chi)=(7\chi^2)\phi_q+(21\chi^3+343)$$

$$0\equiv(7\chi^2)\phi_q+(21\chi^3+343)\ (\mathrm{mod}\ r(\chi))$$

となる。

[0076] したがって、$D_i(\chi)$は、

$$D_0(\chi)=21\chi^3-343$$

$$D_1(\chi)=7\chi^2$$

となる。

[0077] このうち、$D_0(\chi)$が最も次数が高いので、$D_0(\chi)$以外を右辺に移すことにより、

$$21\chi^3-343=7\chi^2\phi_q$$

となり、式を整理することによって、

$$\chi^3-49=\chi^2\phi_q$$

が得られる。

[0078] したがって、非負整数nに対するGの有理点Qのスカラーn倍算、または非負整数nに対するHの元Aのn乗算を行わせるべき乗算を行う場合には、非負整数nに対してnをt－1進展開し、さらにχ^3-49進展開して、χ^3-49に換えて$\chi^2\phi_q$を用いることにより、Gの有理点のスカラーn倍算またはHの元Aのn乗算を、有理点に対するフロベニウス自己準同型写像ϕ_qを用いて演算を行うことができ、演算回数を減してべき乗算を高速化することができる。

[0079] 最後に、スカラー倍算の演算プログラム及びべき乗算の演算プログラムについて詳説する。なお、スカラー倍算の演算プログラム及びべき乗算の演算プログラムは、本実施形態では、IDベース暗号やグループ署名などを電子計算機で実行している際に、サブルーチンの一つとしてそれぞれ実行されるものである。

[0080] 図1に示すように、スカラー倍算の演算プログラム及びべき乗算の演算プログラムを実行する電子計算機10は、演算処理を実行するCPU11と、所要のプログラムやデータを記憶したハードディスクなどの記憶装置12と、所要のプログラムを展開して実行可能とするとともに、演算にともなって生成されたデータを一時的に記憶するRAM

などで構成されたメモリ装置13を備えている。図1中、14はバスである。本実施形態では、記憶装置12には、メインルーチンのプログラムやスカラー倍算の演算プログラム及びべき乗算の演算プログラムなどの各種プログラム、及びこれらのプログラムが使用するデータを記憶させている。

[0081] 電子計算機10が、例えばグループ署名における認証装置として機能する場合には、インターネットなどの電気通信回線20に接続して、この電気通信回線20に接続されたクライアント装置30から送信されたグループ署名の署名データを受信し、メモリ装置13に一次的に記憶して、グループ署名用のプログラムに基づいて署名データの正当性を判定して認証処理を行っている。図1中、15は電子計算機10の入出力制御部である。

[0082] スカラー倍算の演算プログラム及びべき乗算の演算プログラムは、それぞれ署名データの正当性を判定する処理を行う際に数多く実行されるものであり、以下においては、スカラー倍算の演算プログラム、及びべき乗算の演算プログラムについてのみ説明する。なお、本発明に係るスカラー倍算の演算プログラム及びべき乗算の演算プログラムは、グループ署名の処理において用いられるものではなく、多種多様な用途で用いられるものである。しかも、本発明に係るスカラー倍算の演算プログラム及びべき乗算の演算プログラムは、記憶装置12や電子計算機で読み取り可能な記録媒体に、或いはサーバからダウンロードして記憶装置に記憶可能な形態である場合だけでなく、半導体回路として構成することによりいわゆるハードウェア実装される形態であってもよい。

[0083] まず、t－1進展開によるスカラー倍算nQについて説明する。

[0084] 図2は、スカラー倍算nQ(＝Z)を求めるフローチャート図である。スカラー倍算の演算プログラムを実行させて電子計算機をスカラー倍算機として機能させる。図2に示すように、はじめに、CPU11は、クライアント装置30から電気通信回線20、入出力制御部15を介して、スカラーnと、$E(F_q)$のフロベニウス自己準同型写像のトレースtと、有理点$Q \in G \subset E(F_{q^k})$の値を入力し、メモリ装置13に記憶する(ステップS101)。この場合、電子計算機は、入力手段として機能する。

[0085] 次いで、CPU11は、演算結果を格納するZをメモリ装置13に確保して、このZを初

期化(Z←O)する(ステップS102)。従って、電子計算機は、入力手段として機能する。CPU11は、入力したQに対して、$2^{j}Q$により表される演算を実行する(ステップS103)。

[0086] ステップS103では、T[j]＝$2^{j}Q$として、CPU11は、メモリ装置13からQ、tの値を読み出し、以下のアルゴリズムを実行している。

(1)for(j=0;j<「$\log_2 s$」;j++)

(2) T[j]←Q

(3) Q←Q+Q

(4)End for

ここで、(1)の「$\log_2 s$」は、厳密には、

[数14]

$$\lceil \log_2 s \rceil$$

であるが、表記上の制限のため、「」を用いている。ここで、CPU11は、s=t-1とし、jを自然数として、T[j]←Q及びQ←Q+Qにより表される代入演算をj=0からj<「$\log_2 s$」まで繰り返して実行し、メモリ装置13に演算結果の値を記憶する。なお、以下において、アルゴリズム中の「」は同じ意味に用いる。

[0087] 次いで、t－1＝sとして、CPU11は、メモリ装置11からc[i]、s、スカラーnの値を読み出し、転換手段として機能して、スカラーnを、

[数15]

$$n = \sum_{i=0}^{\lceil \log_s n \rceil} c[i] s^{i}, 0 \le c[i] \le s.$$

とs進展開する(ステップS104)。ここで、iは自然数であり、iの大きさは、nの大きさによって決定されるものである。

[0088] ステップS104では、s進展開の演算として、CPU11は、以下のアルゴリズムを実行している。

(1)for(i=0;i<「$\log_s n$」;i++)

(2) c[i]←n%s

(3) n←(n-c[i])/s

(4)End for

ここで、「%」は、剰余をとっていることを表している。即ち、CPU11は、メモリ装置13からc[i]、s、nの値を読み出して、c[i]←n%s及びn←(n-c[i])/sにより表される代入演算をi=0からi<「$\log_s n$」まで繰り返して実行して、各係数c[i]、及びスカラーnの値をメモリ装置13に記憶する。

[0089] 次いで、本実施形態では、電子計算機は、第2の演算手段として、Q[i]=c[i]Qの演算を行う(ステップS105)。

[0090] ステップS105では、バイナリ法を用いており、CPU11は、以下のアルゴリズムを実行している。

(1)for(i=0;i<「$\log_s n$」;i++)

(2) Q[i]←O

(3) for(j=0;c[i]!=0;i++)

(4) if(c[i]&1)

(5) Q[i]←Q[i]+T[j]

(6) End if

(7) c[i]←c[i]/2

(8) End for

(9)End for

[0091] 即ち、CPU11は、i=0からi<「$\log_s n$」まで、Q[i]←0の代入演算によりメモリ装置11に記憶されたQ[i]を初期化し、更に、以下の演算を繰り返して実行する。CPU11はメモリ装置13から係数Q[i]、T[j]の値を読み出し、c[i]&1の場合にQ[i]←Q[i]+T[j]により表される代入演算を、その他の場合にc[i]←c[i]/2により表される代入演算を、j=0からc[i]!=0まで繰り返して実行し、各Q[i]及び係数c[i]の値をメモリ装置13に記憶する。

[0092] 次いで、電子計算機は、合成手段として機能し、ステップS105で演算したQ[i]を用いて、スカラー倍算nQを、

[数16]

$$nQ = \sum_{i=0}^{\lceil \log_s n \rceil} \phi_q^i(Q[i]).$$

によって合成する(ステップS106)。

[0093] ステップS106では、CPU11は、以下のアルゴリズムを実行している。

(1)for(i=0;i<「$\log_s n$」;i++)

(2) $Z \leftarrow Z+\phi_q^i(Q[i])$

(3)End for

即ち、CPU11は、メモリ装置13からQ[i]、Zの値を読み出して、$Z \leftarrow Z+\phi_q^i(Q[i])$により表される代入演算をi=0からi<「$\log_s n$」まで繰り返して実行し、メモリ装置13にZの値を記憶する。

[0094] そして、電子計算機は、出力手段として機能し、スカラー倍算の演算プログラムの実行結果として、入出力制御部15からZの値を出力し(ステップS107)、スカラー倍算の演算プログラムを終了している。これによって、スカラーnを$\log_s n$分割したので、ϕ_qを用いることで楕円2倍算の演算回数をおよそ$1/(\log_s n)$に削減することができる。

[0095] また、楕円曲線の有限体F_qの位数q、$\#E(F_q)$を割り切る素数位数r、フロベニウス自己準同型写像ϕ_qのトレースtが、整数変数χを用いてそれぞれ$q(\chi)$、$r(\chi)$、$t(\chi)$とあらかじめ特定されている場合には、$r(\chi)$を$t(\chi)-1$進展開することにより

$$[r(\chi)]Q=\Sigma[D_i(\chi)(t(\chi)-1)^i]Q=\Sigma\phi_q^i([D_i(\chi)]Q)$$

として表される$D_i(\chi)$のうちでもっとも次数の高いものを$D_{dmax}(\chi)$とし、

$$\phi_q^{dmax}([D_{dmax}(\chi)]Q)=\Sigma\phi_q^i([D_i(\chi)]Q)-\phi_q^{dmax}([D_{dmax}(\chi)]Q)$$
$$=[f(\phi_q,\chi)]Q$$

となる多項式$f(\phi_q,\chi)$を用い、$\phi_q^k Q=Q$に基づいて

$$[D_{dmax}(\chi)]Q=[f(\phi_q,\chi)\phi_q^{-dmax}]Q=[h(\phi_q,\chi)]Q$$

となる多項式$h(\phi_q,\chi)$と、$D_{dmax}(\chi)$を用いることにより、スカラー倍算nQをより高速化することができる。

[0096] すなわち、$D_{dmax}(\chi)$及び多項式$h(\phi_q,\chi)$が特定されている場合には、$\chi=a$としてスカラーnを$D_{dmax}(a)$進展開して、$D_{dmax}(a)$に換えて$h(\phi_q,a)$を用いることにより、演算回数を削減している。

[0097] $D_{dmax}(\chi)$及び多項式$h(\phi_q,\chi)$が特定されている場合のスカラー倍算nQでは、スカラー倍算の演算プログラムを実行させて電子計算機をスカラー倍算機として機能させ

る。この際に、図3に示すように、はじめに、CPU11は、スカラーnと、χ＝aとしてs＝D_{dmax}(a)及びh'(ϕ_q)＝h(ϕ_q,a)と、有理点Q∈G⊂E(F_q^k)の各値を入力してメモリ装置13に記憶する(ステップS201)。この場合、電子計算機は、入力手段として機能する。

[0098] 次いで、電子計算機は、初期化手段として機能する。即ち、CPU11は、演算結果を格納するZをメモリ装置13に確保して初期化(Z←O)する(ステップS202)。そして、電子計算機は第1の演算手段として機能する。即ち、CPU11は、入力されたQに対して、2^iQをあらかじめ演算しておく(ステップS203)。ステップS203の演算はステップS103の演算とアルゴリズムは同じであるので、説明は省略する。

[0099] 次いで、電子計算機は、第1の展開手段として機能し、スカラーnを、

[0100] [数17]

$$n=\sum_{i=0}^{\lceil \log_s n \rceil} c[i]s^i, 0 \le c[i] \le s.$$

とs進展開する(ステップS204)。ステップS204でのs進展開は、ステップS104でのs進展開とアルゴリズムは同じであるので、説明は省略する。

[0101] 次いで、電子計算機は、第2の展開手段として機能し、スカラーnを、h'(ϕ_q)及びc[i]を用いながら、

[数18]

$$n=\sum_{i=0}^{k-1} d[i]\phi_q^i, 0 \le d[i] \le s.$$

とϕ_q進展開する(ステップS205)。

[0102] ステップS205では、ϕ_q進展開の演算として、CPU11は、以下のアルゴリズムを実行している。

(1) T(ϕ_q)←1

(2) for(i=0;i<「$\log_s$ n」;i++)

(3) d[i]←c[i]

(4) if(d[i]≧s)

(5) for(j=0;j<「$\log_s$ d[i]」;j++)

(6) e[j]←d[i]%s

(7) d[i]←(d[i]-e[j])%s

(8) End for

(9) $U(\phi_q)\leftarrow 1$

(10) for(j=0;j<「$\log_s$ d[i]」;j++)

(11) $U(\phi_q)\leftarrow\{U(\phi_q)*e[j]*h'(\phi_q)^j\}\%(\phi_q^k-1)$

(12) End for

(13) $T(\phi_q)\leftarrow\{T(\phi_q)+U(\phi_q)*h'(\phi_q)^i\}\%(\phi_q^k-1)$

(14) End if

(15) else

(16) $T(\phi_q)\leftarrow\{T(\phi_q)+d[i]*h'(\phi_q)^i\}\%(\phi_q^k-1)$

(17) End else

(18) End for

[0103] 即ち、CPU11は、メモリ装置13に記憶された$T(\phi_q)$を1に初期化する。CPU11は、メモリ装置13からc[i]の値を読み出し、d[i]←c[i]の代入演算を行ってd[i]の値をメモリ装置13に記憶する。次に、CPU11は、メモリ装置13からd[i]、sの値を読み出して、d[i]≧sを満たす場合にはe[j]←d[i]%s及びd[i]←(d[i]-e[j])%sにより表される代入演算をj=0からj<「$\log_s$ d[i]」まで繰り返し実行し、$U(\phi_q)\leftarrow 1$に初期化した後に$U(\phi_q)\leftarrow\{U(\phi_q)*e[j]*h'(\phi_q)^j\}\%(\phi_q^k-1)$により表される演算をj=0からj<「$\log_s$ d[i]」まで繰り返し実行し、次に$T(\phi_q)\leftarrow\{T(\phi_q)+d[i]*h'(\phi_q)^i\}\%(\phi_q^k-1)$により表される演算を実行して、$T(\phi_q)$の値をメモリ装置13に記憶する。CPU11は、d[i]≧sを満たさない場合は$T(\phi_q)\leftarrow\{T(\phi_q)+d[i]*h'(\phi_q)^i\}\%(\phi_q^k-1)$により表される演算を実行して$T(\phi_q)$の値をメモリ装置13に記憶する。CPU11は、以上の演算を、i=0からi<「$\log_s$ n」まで繰り返して実行し、各iにおけるd[i]、$T(\phi_q)$の値をメモリ装置11に記憶する。

[0104] なお、スカラーnをϕ_q進展開した場合に、ϕ_q進展開の係数d[i]がsよりも大きくなることがある。CPU11は、ϕ_q進展開の係数d[i]とsとを比較して、ϕ_q進展開の係数d[i]がsよりも大きいと判定した場合(ステップS206:NO)には、ϕ_q進展開の係数d[i]に対してsの剰余をとることにより、ϕ_q進展開の係数d[i]がsよりも小さくなるように調整してい

る(ステップS207)。この場合、電子計算機は、ステップS206において比較手段として機能し、ステップS207において調整手段として機能する。

[0105] ステップS207では、電子計算機は、以下のアルゴリズムを実行している。

(1) until(∀d[i]＜s)
(2) for(i=0;i<k-1;i++)
(3) d[i]←the i-th coefficient of $T(\phi_q)$
(4) if(d[i]≧s)
(5) the i-th coefficient of $T(\phi_q)$←0
(6) for(j=0;j<「$\log_s d[i]$」;j++)
(7) e[j]←d[i]%s
(8) d[i]←(d[i]-e[j])%s
(9) End for
(10) $U(\phi_q)$←1
(11) for(j=0;j<「$\log_s d[i]$」;j++)
(12) $U(\phi_q)$←{$U(\phi_q)$*e[j]*h'$(\phi_q)^j$}%(ϕ_q^k-1)
(13) End for
(14) $T(\phi_q)$←{$T(\phi_q)$+$U(\phi_q)$*ϕ_q^i}%(ϕ_q^k-1)
(15) End if
(16) End for
(17) End until

[0106] 即ち、CPU11は、メモリ装置13から$T(\phi_q)$のi番目の係数の値を読み出してd[i]にその値を記憶し、d[i]とsの値を比較する。CPU11は、d[i]≧sを満たす場合に、$T(\phi_q)$のi番目の係数に0を記憶し、e[j]←d[i]%s及びd[i]←(d[i]-e[j])%sにより表される演算をj=0からj<「$\log_s d[i]$」まで繰り返し実行し、次に$U(\phi_q)$←1に初期化した後に、$U(\phi_q)$←{$U(\phi_q)$*e[j]*h'$(\phi_q)^j$}%(ϕ_q^k-1)により表される演算を、j=0からj<「$\log_s d[i]$」まで繰り返し実行し、次に$T(\phi_q)$←{$T(\phi_q)$+$U(\phi_q)$*ϕ_q^i}%(ϕ_q^k-1)により表される演算を実行してメモリ装置13に$T(\phi_q)$の値を記憶する。CPU11は、d[i]≧sを満たさない場合には上記一連の演算を行わない。CPU11は、以上の演算をi=0からi<k-1まで繰り返し実行

し、これを$^{\forall}$d[i]＜sを満たすまで行う。

[0107] 次いで、電子計算機は、第2の演算手段として機能し、Q[i]＝d[i]Qの演算を行う（ステップS208）。

[0108] ステップS208でも、バイナリ法を用いており、CPU11は、以下のアルゴリズムを実行している。

(1) for(i=0;i<k;i++)

(2) Q[i]←O

(3) for(j=0;d[i]!=0;i++)

(4) if(d[i]＆1)

(5) Q[i]←Q[i]+T[j]

(6) End if

(7) d[i]←d[i]/2

(8) End for

(9) End for

[0109] 即ち、CPU11はメモリ装置13からd[i]及びT[j]の値を読み出して、Q[i]←OとしてQ[i]を初期化した後に、d[i]＆1を満たす場合は、Q[i]←Q[i]+T[j]により表される代入演算を、d[i]＆1を満たさないときはd[i]←d[i]/2の代入演算を実行して、Q[i]及びd[i]の値をメモリ装置13に記憶する。

[0110] 次いで、電子計算機は、合成手段として機能し、ステップS208で演算したQ[i]を用いて、スカラー倍算nQを、

[数19]

$$nQ = \sum_{i=0}^{k-1} \phi_q^i(Q[i]).$$

によって合成する（ステップS209）。

[0111] ステップS209では、CPU11は、以下のアルゴリズムを実行している。

(1) for(i=0;i<k;i++)

(2) Z←Z+ ϕ_q^i(Q[i])

(3) End for

[0112] 即ち、CPU11はメモリ装置13からZ及びQ[i]の値を読み出して、Z←Z+ϕ_q^i(Q[i])により表される代入演算を、i=0からi<kまで繰り返して実行して、メモリ装置13にZの値を記憶する。CPU11は、入出力制御部15からZの値を出力する。つまり、電子計算機は、出力手段として機能し、スカラー倍算の演算プログラムの実行結果として、Zを出力し(ステップS210)、スカラー倍算の演算プログラムを終了している。これによって、スカラーnを$\log_s n$分割したので、ϕ_qを用いることで楕円2倍算の演算回数をおよそ$\deg D_{dmax}(\chi)/\deg r(\chi)$に削減することができる。

[0113] $D_{dmax}(\chi)$及び多項式$h(\phi_q,\chi)$は、楕円曲線の有限体F_qの位数$q(\chi)$、$\#E(F_q)$を割り切る素数位数$r(\chi)$、フロベニウス自己準同型写像ϕ_qのトレース$t(\chi)$があらかじめ与えられていることから、あらかじめ特定でき、$q(\chi)$、$r(\chi)$及び$t(\chi)$とともに、$D_{dmax}(\chi)$と多項式$h(\phi_q,\chi)$をスカラー倍算の演算プログラムに組み込んでもよいし、$r(\chi)$及び$t(\chi)$を用いて以下の補助プログラムによって、$D_{dmax}(\chi)$と多項式$h(\phi_q,\chi)$を求めてもよい。

[0114] 電子計算機は、補助プログラムを起動させると、図4に示すように、はじめに、入力手段として機能する。即ち、CPU11は、$r(\chi)$と$t(\chi)$の値を入力してメモリ装置13に記憶する(ステップS221)。

[0115] 次いで、電子計算機は、展開手段として機能し、入力された$t(\chi)$を用いて、$t(\chi)-1=s(\chi)$として、$r(\chi)$を、

[数20]

$$r(\chi)=\sum_{i=0}^{\lceil \deg r(\chi)/\deg s(\chi)\rceil} D_i(\chi)s(\chi)^i,\ 0\le \deg(D_i(\chi))<\deg(s(\chi)).$$

と$s(\chi)$進展開する(ステップS222)。ここで、iの大きさは、$r(\chi)$及び$s(\chi)$から自動的に決定される。ステップS222では、$s(\chi)$進展開の演算として、CPU11は、以下のアルゴリズムを実行している。

(1) for(i=0;i<「$\deg r(\chi)/\deg s(\chi)$」;i++)

(2) $D_i(\chi)\leftarrow r(\chi)\%s(\chi)$

(3) $r(\chi)\leftarrow(r(\chi)-D_i(\chi))/s(\chi)$

(4) End for

[0116] 即ち、CPU11は、メモリ装置13からr(χ)及びs(χ)の値を読み出して、$D_i(\chi)\leftarrow r(\chi)\%s(\chi)$及び$r(\chi)\leftarrow(r(\chi)-D_i(\chi))/s(\chi)$により表される代入演算を、i=0からi<degr(χ)/degs(χ)まで繰り返し実行し、メモリ装置13に$D_i(\chi)$及びr(χ)の値を記憶する。

[0117] 次いで、電子計算機は、抽出手段として機能し、$\deg(D_i(\chi))$が最大のものを抽出して、$D_{dmax}(\chi)$として出力する(ステップS223)。即ち、CPU11は、メモリ装置13から$D_i(\chi)$の値を読み出して比較し、最大の$D_i(\chi)$を$D_{dmax}(\chi)$としてその値をメモリ装置13に記憶する。

[0118] 次いで、電子計算機は、演算手段として機能する。即ち、CPU11は、

[数21]

$$h(\phi_q,\chi)=\sum_{i=0}^{\lceil \deg r(\chi)/\deg s(\chi)\rceil} D_i(\chi)(\phi_q^{i-d\max})-D_{d\max}(\chi).$$

の演算を行って多項式$h(\phi_q,\chi)$を特定し、メモリ装置13にその値を記憶し、出力している(ステップS224)。このようにして、電子計算機では、補助プログラムを用いて$D_{dmax}(\chi)$及び多項式$h(\phi_q,\chi)$を求めることができる。この$D_{dmax}(\chi)$及び多項式$h(\phi_q,\chi)$を図3のステップ201に用いることで図3に示すスカラー倍算により楕円2倍算の演算回数をおよそ$\deg D_{dmax}(\chi)/\deg r(\chi)$に削減することができる。

[0119] また、楕円曲線の有限体F_qの位数q、$\#E(F_q)$を割り切る素数位数r、フロベニウス自己準同型写像ϕ_qのトレースtが、整数変数χを用いてそれぞれq(χ)、r(χ)、t(χ)とあらかじめ特定されているとともに、r(χ)をt(χ)−1進展開することにより

$$[r(\chi)]Q=\Sigma[D_i(\chi)(t(\chi)-1)^i]Q=\Sigma\,\phi_q^{\,i}([D_i(\chi)]Q)$$

として表される$D_i(\chi)$において最高次数dmaxとなる$D_i(\chi)$が複数存在する場合には、最高次数dmaxの項であるχ^{dmax}の係数を$T_{dmax}(\phi_q)$として、$r(\chi)\mid m(\chi)$を満たす最小次数の多項式m(χ)を用いて

$$V(\phi_q)\mid m(\phi_q),\gcd(T_{dmax}(\phi_q),V(\phi_q))=1$$

を満たす$V(\phi_q)$を特定し、

$$g(\phi_q)V(\phi_q)\equiv v(\mathrm{mod}\ m(\phi_q))$$

を満たす整数のスカラーv及び$g(\phi_q)$を拡張ユークリッドの互除法により特定し、

$$[T_{dmax}(\phi_q)\chi^{dmax}]Q=\Sigma\,\phi_q^{\,i}([D_i(\chi)]Q)-[T_{dmax}(\phi_q)\chi^{dmax}]Q$$

$$=[f(\phi_q,\chi)]Q$$

となる多項式$f(\phi_q,\chi)$と、$g(\phi_q)$を用い、$\phi_q^k Q=Q$に基づいて、

$$[v\chi^{dmax}]Q=[g(\phi_q)f(\phi_q,\chi)]Q=[h(\phi_q,\chi)]Q$$

となる多項式$h(\phi_q,\chi)$を特定し、この$h(\phi_q,\chi)$のϕ_qに関する定数項$h(0,\chi)$が、

$$[v\chi^{dmax}-h(0,\chi)]Q=[h(\phi_q,\chi)-h(0,\chi)]Q$$

を満たすことを用いることにより、スカラー倍算nQをより高速化することができる。

[0120] すなわち、$\chi=a$として、$s'=va^{dmax}-h(0,a)$及び$h'(\phi_q)=h(\phi_q,a)-h(0,a)$とし、スカラーnを$D_{dmax}(a)$進展開する換わりに$va^{dmax}-h(0,a)$進展開して、$va^{dmax}-h(0,a)$の換わりに$h(\phi_q,a)-h(0,a)$を用いることにより、演算回数を削減している。

[0121] $s'=va^{dmax}-h(0,a)$及び$h'(\phi_q)=h(\phi_q,a)-h(0,a)$が特定されている場合のスカラー倍算nQでは、スカラー倍算の演算プログラムを実行させて電子計算機をスカラー倍算機として機能させる。その際に、図5に示すように、はじめに、CPU11は、スカラーnと、$\chi=a$としてスカラー$s'=va^{dmax}-h(0,a)$及び$h'(\phi_q)=h(\phi_q,a)-h(0,a)$と、有理点$Q\in G\subset E(F_q^k)$の値を入力してメモリ装置13に記憶する(ステップS301)。この場合、電子計算機は、入力手段として機能する。

[0122] 次いで、電子計算機は初期化手段として機能し、CPU11は、メモリ装置13に演算結果を格納するZを確保して、初期化(Z←O)する(ステップS302)。そして、電子計算機は第1の演算手段として機能し、CPU11はメモリ装置13に記憶されたQの値を読み出して、2^jQをあらかじめ演算し、メモリ装置13に記憶しておく(ステップS303)。ステップS303の演算はステップS103の演算とアルゴリズムは同じであり、CPU11が行う処理も同じなので、説明は省略する。

[0123] 次いで、電子計算機は、第1の展開手段として機能し、スカラーnを、

[数22]

$$n=\sum_{i=0}^{\lceil \log_{s'} n\rceil} c[i]s'^{i},0\le c[i]\le s'.$$

とs'進展開する(ステップS304)。ステップS304でのs'進展開は、ステップS204でのs進展開とアルゴリズムは同じであり、CPU11が行う処理も同じなので、説明は省略する。

[0124] 次いで、電子計算機は、第2の展開手段として機能し、スカラーnを、h'(ϕ_q)及びc[i]を用いながら、

[数23]

$$n=\sum_{i=0}^{k-1} d[i]\phi_q^i, 0\le d[i]\le s'.$$

とϕ_q進展開する(ステップS305)。ステップS305でのϕ_q進展開は、スカラーs'(=va^{dmax}−h(0,a))が、ステップS205でのスカラーs(=D_{dmax}(a))とは異なる点以外では、ステップS205でのs進展開とアルゴリズムは同じであり、CPU11が行う処理も同じであるため、詳細な説明は省略する。

[0125] ステップS305でのϕ_q進展開でも、ϕ_q進展開の係数がs'よりも大きくなることがある。このように、ϕ_q進展開の係数がs'よりも大きい場合(ステップS306:NO)には、ϕ_q進展開の係数に対してs'の剰余をとることにより、ϕ_q進展開の係数がs'よりも小さくなるように調整している(ステップS307)。このステップS307での演算も、スカラーs'(=va^{dmax}−h(0,a))が、ステップS207でのスカラーs(=D_{dmax}(a))とは異なる点以外では、ステップS207での演算とアルゴリズムは同じであり、CPU11が行う処理も同じであるため、詳細な説明は省略する。この場合、電子計算機は、ステップS306において比較手段として機能し、ステップS307において調整手段として機能する。

[0126] 次いで、電子計算機は、第2の演算手段として機能し、Q[i]=d[i]Qの演算を行う(ステップS308)。ステップS308でも、バイナリ法を用いており、ステップS308の演算もステップS208の演算とアルゴリズムは同じであり、CPU11が行う処理も同じであるので、説明は省略する。

[0127] 次いで、電子計算機は、合成手段として機能し、ステップS308で演算したQ[i]を用いて、スカラー倍算nQを、

[数24]

$$nQ=\sum_{i=0}^{k-1}\phi_q^i(Q[i]).$$

によって合成する(ステップS309)。ステップS309の演算もステップS209の演算とアルゴリズムは同じであり、CPU11が行う処理も同じであるので、説明は省略する。

[0128] そして、電子計算機は、出力手段として機能し、スカラー倍算の演算プログラムの実行結果として、Zを出力し(ステップS310)、スカラー倍算の演算プログラムを終了している。これによって、スカラーnを$\log_s n$分割したので、ϕ_qを用いることで楕円2倍算の演算回数をおよそdmax/degr(a)に削減することができる。

[0129] 多項式$h(\phi_q, \chi)$及び$v\chi^{dmax} - h(0, \chi)$は、楕円曲線の有限体$F_q$の位数$q(\chi)$、$\#E(F_q)$を割り切る素数位数$r(\chi)$、フロベニウス自己準同型写像$\phi_q$のトレース$t(\chi)$があらかじめ与えられていることから、あらかじめ特定できるので、$q(\chi)$、$r(\chi)$及び$t(\chi)$とともに、多項式$h(\phi_q, \chi)$及び$v\chi^{dmax} - h(0, \chi)$をスカラー倍算の演算プログラムに組み込んでもよいし、$r(\chi)$及び$t(\chi)$を用いて以下の補助プログラムによって、多項式$h(\phi_q, \chi)$及び$v\chi^{dmax} - h(0, \chi)$を求めてもよい。

[0130] 電子計算機は、補助プログラムを起動させると、図6に示すように、はじめに、入力手段として機能する。CPU11は、入力した$r(\chi)$、$t(\chi)$及び$m(\chi)$の値をメモリ装置13に記憶する(ステップS321)。ここで、$m(\chi)$は$r(\chi) \mid m(\chi)$を満たす最小次数の多項式であり、一般的には円周等分多項式が用いられる。

[0131] 次いで、電子計算機は、展開手段として機能し、入力された$t(\chi)$を用いて、$t(\chi) - 1 = s(\chi)$として、$r(\chi)$を、

[数25]

$$r(\chi) = \sum_{i=0}^{\lceil \deg r(\chi)/\deg s(\chi) \rceil} D_i(\chi) s(\chi)^i, 0 \le \deg(D_i(\chi)) < \deg(s(\chi)).$$

と$s(\chi)$進展開する(ステップS322)。ここで、iの大きさは、$r(\chi)$及び$s(\chi)$から自動的に決定される。ステップS322では、$s(\chi)$進展開の演算として、CPU11は、以下のアルゴリズムを実行している。

(1) for(i=0;i<「degr(χ)/degs(χ)」;i++)

(2) $D_i(\chi) \leftarrow r(\chi) \% s(\chi)$

(3) $r(\chi) \leftarrow (r(\chi) - D_i(\chi))/s(\chi)$

(4) End for

[0132] 即ち、CPU11は、メモリ装置13から$r(\chi)$及びχの値を読出し、$D_i(\chi) \leftarrow r(\chi) \% s(\chi)$及び$r(\chi) \leftarrow (r(\chi) - D_i(\chi))/s(\chi)$により表される演算をi=0からi<「degr($\chi$)/degs($\chi$)」

まで繰り返し実行し、メモリ装置13に$D_i(\chi)$及び$r(\chi)$の値を記憶する。

[0133] 次いで、電子計算機は、第1の特定手段として機能し、$\deg(D_i(\chi))$の最大の次数dmaxの項であるχ^{dmax}の係数を抽出して、抽出された係数の和を$T(\phi_q,\chi)$とし、それ以外の和を$U(\phi_q,\chi)$とする(ステップS323)。ステップS323では、CPU11は、具体的に以下のアルゴリズムを実行している。

(1) for(i=0;i<「degr(χ)/degs(χ)」;i++)

(2) $T(\phi_q,\chi)\leftarrow 0, U(\phi_q,\chi)\leftarrow 0$

(3) if($\deg(D_i(\chi))$=dmax)

(4) $T(\phi_q,\chi)\leftarrow T(\phi_q,\chi)+D_i(\chi)\phi_q^i$

(5) End if

(6) else

(7) $U(\phi_q,\chi)\leftarrow U(\phi_q,\chi)+D_i(\chi)\phi_q^i$

(8) End else

(9) End for

[0134] 即ち、CPU11は、メモリ装置13から$r(\chi)$、$s(\chi)$及び$D_i(\chi)$の値を読出し、$T(\phi_q,\chi)\leftarrow 0, U(\phi_q,\chi)\leftarrow 0$の初期化処理を行った後に、$\deg(D_i(\chi))$=dmaxを満たす場合は$T(\phi_q,\chi)\leftarrow T(\phi_q,\chi)+D_i(\chi)\phi_q^i$により表される代入演算を、$\deg(D_i(\chi))$=dmaxを満たさない場合は$U(\phi_q,\chi)\leftarrow U(\phi_q,\chi)+D_i(\chi)\phi_q^i$により表される代入演算を、i=0からi<「degr(χ)/degs(χ)」まで繰り返して実行し、メモリ装置13に$T(\phi_q,\chi)$及び$U(\phi_q,\chi)$を記憶する。

[0135] 次いで、電子計算機は、第2の特定手段として機能する。CPU11は、ステップS323で特定した$T(\phi_q,\chi)$の最高次数係数$T_{dmax}(\phi_q)$を特定し、メモリ装置13に記憶する(ステップS324)。

[0136] 次いで、電子計算機は、第3の特定手段として機能し、ステップS324で特定した最高次数係数$T_{dmax}(\phi_q)$を用い、

$$V(\phi_q)\mid m(\phi_q),\gcd(T_{dmax}(\phi_q),V(\phi_q))=1$$

を満たす$V(\phi_q)$を特定する(ステップS325)。ステップS325では、CPU11は、具体的に以下のアルゴリズムを実行している。

(1)$W(\phi_q)\leftarrow gcd(T_{dmax}(\phi_q),m(\phi_q))$

(2)$V(\phi_q)\leftarrow W(\phi_q)$

即ち、CPU11は、メモリ装置13から$T_{dmax}(\phi_q)$及び$m(\phi_q)$の値を読出し、$W(\phi_q)\leftarrow gcd(T_{dmax}(\phi_q),m(\phi_q))$及び$V(\phi_q)\leftarrow W(\phi_q)$により表される演算を実行して、メモリ装置13に、$W(\phi_q)$及び$V(\phi_q)$の値を記憶する。

[0137] 次いで、電子計算機は、第4の特定手段として機能する。即ち、CPU11はメモリ装置13から、ステップS325で特定した$V(\phi_q)$を読み出して、

$$g(\phi_q)V(\phi_q)\equiv v(\mathrm{mod}\ m(\phi_q))$$

を満たすスカラーv及び$g(\phi_q)$を、拡張ユークリッドの互除法によって特定し、メモリ装置13に記憶する(ステップS326)。この拡張ユークリッドの互除法は、一般的なライブラリにおいて準備されている既知のプログラムに基づいて実行されるものであり、特に、$g(\phi_q)$の係数及びスカラーvが小さくなるようにしておくことが望ましい。

[0138] 次いで、CPU11は、ステップS326で特定した$g(\phi_q)$をメモリ装置13から読み出し、

[数26]

$$h(\phi_q,\chi)=g(\phi_q)(T(\phi_q,\chi)-T_{d\max}(\phi_q)\chi^{d\max}+U(\phi_q,\chi))\bmod\phi_q^k-1.$$

の演算を行って多項式$h(\phi_q,\chi)$を特定し(ステップS327)、多項式$h(\phi_q,\chi)$及び$v\chi^{dmax}-h(0,\chi)$の値をメモリ装置13に記憶し出力している(ステップS328)。このようにして、電子計算機では、補助プログラムを用いて多項式$h(\phi_q,\chi)$及び$v\chi^{dmax}-h(0,\chi)$を求めることができる。この場合、電子計算機は、ステップS327において演算手段として機能し、ステップS328において出力手段として機能する。この$v\chi^{dmax}-h(0,\chi)$及び多項式$h(\phi_q,\chi)$を図5のステップ301に用いることで図5に示すスカラー倍算により楕円2倍算の演算回数をおよそdmax/degr(χ)に削減することができる。

[0139] 以下において、べき乗算の演算プログラムについて説明する。まず、t−1進展開によるべき乗算A^nについて説明する。

[0140] べき乗算の演算プログラムを実行させて電子計算機をべき乗算として機能させる際に、図7に示すように、はじめに、べき数nと、位数qとF_q^kの素数位数rとの差分sと、元$A\in H\subset F_q^k$が入力される(ステップS401)。この場合、電子計算機は、入力手段として機能する。

[0141] 次いで、電子計算機は、初期化手段として機能する。即ち、CPU11は、演算結果を格納するZをメモリ装置13に確保して、このZを初期化(Z←1)する(ステップS402)。そして、電子計算機は第1の演算手段として機能する。CPU11は、元Aの値を入力してメモリ装置13に記憶し、X^{Y}はX^{Y}を表すものとして、入力された元Aに対して、A^{2^{j}}をあらかじめ演算しておく(ステップS403)。

[0142] ステップS403では、T[j]=A^{2^{j}}として、CPU11は、以下のアルゴリズムを実行している。

(1) for(;j++)

(2) T[j]←A

(3) A←A*A

(4) End for

即ち、CPU11は、メモリ装置13から元A、sの値を読み出して、T[j]←A及びA←A*Aにより表される代入演算を、j=0からj<「$\log_2 s$」まで繰り返して実行し、メモリ装置13にT[j]及びAの値を記憶する。

[0143] 次いで、電子計算機は、展開手段として機能し、べき数nを、差分sにより

[数27]

$$n = \sum_{i=0}^{\lceil \log_s n \rceil} c[i] s^i, 0 \le c[i] \le s.$$

とs進展開する(ステップS404)。ここで、iの大きさは、nの大きさによって決定するものである。

[0144] ステップS404では、s進展開の演算として、CPU11は、以下のアルゴリズムを実行している。

(1) for(i=0;i<「$\log_s n$」;i++)

(2) c[i]←n%s

(3) n←(n-c[i])/s

(4) End for

ここで、「%」は、剰余をとっていることを表している。即ち、CPU11は、メモリ装置13からn、sの値を読み出して、c[i]←n%s及びn←(n-c[i])/sにより表される演算を、i=0か

らiく「$\log_s n$」まで繰り返して実行し、メモリ装置13に各係数c[i]及びnの値を記憶する。

[0145] 次いで、本実施形態では、電子計算機は、第2の演算手段として機能し、$A[i]=A^{c[i]}$の演算を行う(ステップS405)。

[0146] ステップS405では、バイナリ法を用いており、CPU11は、以下のアルゴリズムを実行している。

(1) for(i=0;iく「$\log_s n$」;i++)

(2) A[i]←1

(3) for(j=0;c[i]!=0;i++)

(4) if(c[i]&1)

(5) A[i]←A[i]*T[j]

(6) End if

(7) c[i]←c[i]/2

(8) End for

(9) End for

[0147] 即ち、CPU11は、i=0からiく「$\log_s n$」まで、A[i]←1の代入演算によりメモリ装置11に記憶されたA[i]を初期化し、更に、以下の演算を繰り返して実行する。CPU11はメモリ装置13から係数c[i]、T[j]の値を読み出し、c[i]&1の場合にQ[i]←Q[i]*T[j]により表される代入演算を、その他の場合にc[i]←c[i]/2により表される代入演算を、j=0からc[i]!=0まで繰り返して実行し、各Q[i]及び係数c[i]の値をメモリ装置13に記憶する。

[0148] 次いで、電子計算機は、合成手段として機能し、ステップS405で演算したA[i]を用いて、べき乗算A^nを、

[数28]

$$A^n = \prod_{i=0}^{\lceil \log_s n \rceil} \phi_q^i(A[i]).$$

によって合成する(ステップS406)。

[0149] ステップS406では、CPU11は、以下のアルゴリズムを実行している。

(1) for(i=0;iく「$\log_s n$」;i++)

(2) $Z \leftarrow Z * \phi_q^i(A[i])$

(3) End for

即ち、CPU11は、メモリ装置13からA[i]、Zの値を読み出して、$Z \leftarrow Z * \phi_q^i(A[i])$により表される代入演算をi＝0からi<「$\log_s n$」まで繰り返して実行し、メモリ装置13にZの値を記憶する。

[0150] そして、電子計算機は、出力手段として機能し、べき乗算の演算プログラムの実行結果として、入出力制御部15からZの値を出力し(ステップS407)、べき乗算の演算プログラムを終了している。これによって、べき数nを$\log_s n$分割したので、ϕ_qを用いることで2乗算の演算回数をおよそ$1/(\log_s n)$に削減することができる。

[0151] また、位数q、素数位数r、差分sが、整数変数χを用いてそれぞれ$q(\chi)$、$r(\chi)$、$s(\chi)$で与えられている場合には、$r(\chi)$を$s(\chi)$進展開することにより

$$A\hat{}\{r(\chi)\} = \prod A\hat{}\{D_i(\chi)s(\chi)^i\} = A\hat{}\{\Sigma D_i(\chi)q^i\}$$

として表される$D_i(\chi)$のうちでもっとも次数の高いものを$D_{dmax}(\chi)$とし、

$$(A\hat{}\{D_{dmax}(\chi)\})\hat{}\{q^{dmax}\} = A\hat{}\{\Sigma_{i\neq dmax} - D_i(\chi)q^i\} = A\hat{}\{f(q,\chi)\}$$

となる多項式$f(\phi_q,\chi)$を用い、$\phi_q^k(A)=A$に基づいて、

$$A\hat{}\{D_{dmax}(\chi)\} = A\hat{}\{\Sigma_{i\neq dmax} - D_i(\chi)q^i - q^{dmax}\} = A\hat{}\{h(q,\chi)\}$$

となる多項式$h(\phi_q,\chi)$と、$D_{dmax}(\chi)$を用いることにより、スカラー倍算nQをより高速化することができる。

[0152] すなわち、$D_{dmax}(\chi)$及び多項式$h(\phi_q,\chi)$が特定されている場合には、χ＝aとしてべき数nを$D_{dmax}(a)$進展開して、$D_{dmax}(a)$に換えて$h(\phi_q,a)$を用いることにより、演算回数を削減している。

[0153] $D_{dmax}(\chi)$及び多項式$h(\phi_q,\chi)$が特定されている場合のべき乗算nQでは、べき乗算の演算プログラムを実行させて電子計算機をべき乗算機として機能させる。この際に、図8に示すように、はじめに、CPU11は、べき数nと、χ＝aとして$s=D_{dmax}(a)$及び$h'(q)=h(q,a)$と、元$A\in H\subset F_q^k$の各値を入力してメモリ装置13に記憶する(ステップS501)。この場合、電子計算機は、入力手段として機能する。

[0154] 次いで、電子計算機は、初期化手段として機能する。即ち、CPU11は、演算結果を格納するZをメモリ装置13に確保し、Zを初期化(Z←1)する(ステップS502)。そし

て、第1の演算機能として、入力されたAに対して、A^{2^j}をあらかじめ演算しておく(ステップS503)。ステップS503の演算はステップS403の演算とアルゴリズムは同じであるので、説明は省略する。

[0155] 次いで、電子計算機は、第1の展開手段として機能し、べき数nを、

[数29]

$$n=\sum_{i=0}^{\lceil \log_s n \rceil} c[i]s^i, 0 \le c[i] \le s.$$

とs進展開する(ステップS504)。ステップS504でのs進展開は、ステップS404でのs進展開とアルゴリズムは同じであるので、説明は省略する。

[0156] 次いで、電子計算機は、第2の展開手段として機能し、べき数nを、h'(q)及びc[i]を用いながら、

[数30]

$$n=\sum_{i=0}^{k-1} d[i]q^i, 0 \le d[i] \le s.$$

とq進展開する(ステップS505)。

[0157] ステップS505では、q進展開の演算として、CPU11は、以下のアルゴリズムを実行している。

(1) T(q)←1

(2) for(i=0;i<「$\log_s$ n」;i++)

(3) d[i]←c[i]

(4) if(d[i]≧s)

(5) for(j=0;j<「$\log_s$ d[i]」;j++)

(6) e[j]←d[i]%s

(7) d[i]←(d[i]-e[j])%s

(8) End for

(9) U(q)←1

(10) for(j=0;j<「$\log_s$ d[i]」;j++)

(11) U(q)←{U(q)*e[j]*h'(q)^{j}}%(q^k-1)

(12) End for

(13) $T(q) \leftarrow \{T(q)+U(q)*h'(q)^{j}\}\%(q^{k}-1)$

(14) End if

(15) else

(16) $T(q) \leftarrow \{T(q)+d[i]*h'(q)^{j}\}\%(q^{k}-1)$

(17) End else

(18) End for

[0158] 即ち、CPU11は、メモリ装置13に記憶されたT(q)を1に初期化する。CPU11は、メモリ装置13からc[i]の値を読み出し、d[i]←c[i]の代入演算を行ってd[i]の値をメモリ装置13に記憶する。次に、CPU11は、メモリ装置13からd[i]、sの値を読み出して、d[i]≧sを満たす場合にはe[j]←d[i]%s及びd[i]←(d[i]-e[j])%sにより表される代入演算をj=0からj<「$\log_s d[i]$」まで繰り返し実行し、$U(\phi_q)$←1に初期化した後にU(q)←{U(q)*e[j]*h'(q)^{j}}%(q^{k}-1)により表される演算をj=0からj<「$\log_s d[i]$」まで繰り返し実行し、次にT(q)←{T(q)+U(q)*h'(q)^{j}}%(q^{k}-1)により表される演算を実行して、T(q)の値をメモリ装置13に記憶する。CPU11は、d[i]≧sを満たさない場合はT(q)←{T(q)+d[i]*h'(q)^{j}}%(q^{k}-1)により表される演算を実行してT(q)の値をメモリ装置13に記憶する。CPU11は、以上の演算を、i=0からi<「$\log_s n$」まで繰り返して実行し、各iにおけるd[i]、T(q)の値をメモリ装置11に記憶する。

[0159] なお、べき数nをq進展開した場合に、q進展開の係数がsよりも大きくなることがある。CPU11は、q進展開の係数d[i]とsとを比較して、q進展開の係数d[i]がsよりも大きいと判定した場合(ステップS506:NO)には、q進展開の係数d[i]に対してsの剰余をとることにより、q進展開の係数d[i]がsよりも小さくなるように調整している(ステップS507)。この場合、電子計算機は、ステップS506において比較手段として機能し、ステップS507において調整手段として機能する。

[0160] ステップS507では、電子計算機は、以下のアルゴリズムを実行している。

(1) until(∀d[i]<s)

(2) for(i=0;i<k-1;i++)

(3) d[i]←the i-th coefficient of T(q)

(4) if(d[i]≧s)

(5) the i-th coefficient of T(q)←0

(6) for(j=0;j<「$\log_s$ d[i]」;j++)

(7) e[j]←d[i]%s

(8) d[i]←(d[i]-e[j])%s

(9) End for

(10) U(q)←1

(11) for(j=0;j<「$\log_s$ d[i]」;j++)

(12) U(q)←{U(q)*e[j]*h'(q)^j}%(q^k-1)

(13) End for

(14) T(q)←{T(q)+U(q)*q^i}%(q^k-1)

(15) End if

(16) End for

(17) End until

[0161] 即ち、CPU11は、メモリ装置13からT(q)のi番目の係数の値を読み出してd[i]にその値を記憶する。CPU11は、d[i]とsの値を比較し、d[i]≧sを満たす場合に、T(q)のi番目の係数に0を記憶し、e[j]←d[i]%s及びd[i]←(d[i]-e[j])%sにより表される演算をj=0からj<「$\log_s$ d[i]」まで繰り返し実行し、次にU(q)←1に初期化した後に、U(q)←{U(q)*e[j]*h'(q)^j}%(q^k-1)により表される演算を、j=0からj<「$\log_s$ d[i]」まで繰り返し実行し、次にT(q)←{T(q)+U(q)*q^i}%(q^k-1)により表される演算を実行してメモリ装置13にT(q)の値を記憶する。CPU11は、d[i]≧sを満たさない場合には上記一連の演算を行わない。CPU11は、以上の演算をi=0からi<k-1まで繰り返し実行し、これを$^\forall$d[i]＜sを満たすまで行う。

[0162] 次いで、電子計算機は、第2の演算手段として機能し、A[i]＝$A^{d[i]}$の演算を行う(ステップS508)。

[0163] ステップS508でも、バイナリ法を用いており、CPU11は、以下のアルゴリズムを実行している。

(1) for(i=0;i<k;i++)

(2) A[i]←O

(3) for(j=0;d[i]!=0;i++)

(4) if(d[i]＆1)

(5) A[i]←A[i]*T[j]

(6) End if

(7) d[i]←d[i]/2

(8) End for

(9)End for

[0164] 即ち、CPU11はメモリ装置13からd[i]及びT[j]の値を読み出して、A[i]←OとしてA[i]を初期化した後に、d[i]＆1を満たす場合は、A[i]←A[i]*T[j]により表される代入演算を、d[i]＆1を満たさないときはd[i]←d[i]/2の代入演算を実行して、A[i]及びd[i]の値をメモリ装置13に記憶する。

[0165] 次いで、電子計算機は、合成手段として機能し、ステップS508で演算したA[i]を用いて、べき乗算A^nを、

[数31]

$$A^n = \prod_{i=0}^{k-1} \phi_q^i(A[i]).$$

によって合成する(ステップS509)。

[0166] ステップS509では、CPU11は、以下のアルゴリズムを実行している。

(1)for(i=0;i<k;i++)

(2) Z←Z*ϕ_q^i(A[i])

(3)End for

[0167] 即ち、CPU11はメモリ装置13からZ及びA[i]の値を読み出して、i=0からi<kまで繰り返して演算を実行して、メモリ装置13にZの値を記憶する。CPU11は、入出力制御部15からZの値を出力する。つまり、電子計算機は、出力手段として機能し、べき乗算の演算プログラムの実行結果として、Zを出力し(ステップS510)、べき乗算の演算プログラムを終了している。これによって、べき数nを$\log_s n$分割したので、ϕ_qを用いることで2乗算の演算回数をおよそ$degD_{dmax}(a)/degr(a)$に削減することができる。

[0168] $D_{dmax}(\chi)$及び多項式h(q,χ)は、q(χ)、r(χ)及びs(χ)があらかじめ与えられていることから、あらかじめ特定でき、q(χ)、r(χ)及びs(χ)とともに、$D_{dmax}(\chi)$と多項式h(q,χ)をべき乗算の演算プログラムに組み込んでもよいし、r(χ)及びs(χ)を用いて以下の補助プログラムによって、$D_{dmax}(\chi)$と多項式h(q,χ)を求めてもよい。

[0169] 電子計算機は、補助プログラムを起動させると、図9に示すように、はじめに、入力手段として機能する。即ち、CPU11は、r(χ)とs(χ)の値を入力してメモリ装置13に記憶する(ステップS521)。

[0170] 次いで、電子計算機は、展開手段として機能し、入力されたs(χ)を用いて、r(χ)を、

[数32]

$$r(\chi)=\sum_{i=0}^{\lceil \deg r(\chi)/\deg s(\chi)\rceil} D_i(\chi)s(\chi)^i, 0\le \deg(D_i(\chi))<\deg(s(\chi)).$$

とs(χ)進展開する(ステップS522)。ここで、iの大きさは、r(χ)及びs(χ)から自動的に決定される。ステップS522では、s(χ)進展開の演算として、CPU11は、以下のアルゴリズムを実行している。

(1)for(i=0;i<「degr(χ)/degs(χ)」;i++)

(2) $D_i(\chi)\leftarrow r(\chi)\%s(\chi)$

(3) $r(\chi)\leftarrow(r(\chi)-D_i(\chi))/s(\chi)$

(4)End for

[0171] 即ち、CPU11は、メモリ装置13からr(χ)及びs(χ)の値を読み出して、$D_i(\chi)\leftarrow r(\chi)\%s(\chi)$及び$r(\chi)\leftarrow(r(\chi)-D_i(\chi))/s(\chi)$により表される代入演算を、i=0からi<degr(χ)/degs(χ)まで繰り返し実行し、メモリ装置13に$D_i(\chi)$及びr(χ)の値を記憶する。

[0172] 次いで、電子計算機は、抽出手段として機能し、deg($D_i(\chi)$)が最大のものを抽出して、$D_{dmax}(\chi)$として出力する(ステップS523)。即ち、CPU11は、メモリ装置13から$D_i(\chi)$の値を読み出して比較し、最大の$D_i(\chi)$を$D_{dmax}(\chi)$としてその値をメモリ装置13に記憶する。

[0173] 次いで、電子計算機は、演算手段として機能する。即ち、CPU11は、

[数33]

$$h(q,\chi)=\sum_{i=0}^{\lceil \deg r(\chi)/\deg s(\chi)\rceil} D_i(\chi)(q^{i-d\max})-D_{d\max}(\chi).$$

の演算を行って多項式h(q,χ)を特定し、メモリ装置13にその値を記憶し、出力している(ステップS524)。このようにして、電子計算機では、補助プログラムを用いて$D_{dmax}(\chi)$及び多項式h(q,χ)を求めることができる。この$D_{dmax}(\chi)$及び多項式h(q,χ)を図8のステップ501に用いることで図8に示すべき乗算により2乗算の演算回数をおよそ$\deg D_{dmax}(\chi)/\deg r(\chi)$に削減することができる。

[0174] また、位数q、素数位数r及び差分sが、整数変数χを用いてそれぞれq(χ)、r(χ)及びs(χ)とあらかじめ特定されているとともに、r(χ)をs(χ)進展開することにより

$$A\hat{}\{r(\chi)\}=\Pi A\hat{}\{D_i(\chi)s(\chi)^i\}=A\hat{}\{\Sigma D_i(\chi)q^i\}$$

として表される$D_i(\chi)$において最高次数dmaxとなる$D_i(\chi)$が複数存在する場合には、最高次数dmaxの項であるχ^{dmax}の係数を$T_{dmax}(q)$として、r(χ)|m(χ)を満たす最小次数の多項式m(χ)を用いて

$$V(q)\mid m(q),\gcd(T_{dmax}(q),V(q))=1$$

を満たすV(q)を特定し、

$$g(q)V(q)\equiv v(\mathrm{mod}\ m(q))$$

を満たす整数のスカラーv及びg(q)を拡張ユークリッドの互除法により特定し、

$$A\hat{}\{T_{dmax}(q)\chi^{dmax}\}=A\hat{}\{\Sigma D_i(\chi)q^i-T_{dmax}(q)\chi^{dmax}\}$$
$$=A\hat{}\{f(q,\chi)\}$$

となる多項式f(q,χ)と、g(q)を用い、$\phi_q^k(A)=A$に基づいて、

$$A\hat{}\{v\chi^{dmax}\}=A\hat{}\{g(q)f(q,\chi)\}=A\hat{}\{h(q,\chi)\}$$

となる多項式h(q,χ)を特定し、このh(q,χ)のqに関する定数項h(0,χ)が、

$$A\hat{}\{v\chi^{dmax}-h(0,\chi)\}=A\hat{}\{h(q,\chi)-h(0,\chi)\}$$

を満たすことを用いることにより、べき乗算A^nをより高速化することができる。

[0175] すなわち、χ=aとして、s'=va^{dmax}−h(0,a)及びh'(q)=h(q,a)−h(0,a)とし、べき数nを$D_{dmax}(a)$進展開する換わりにva^{dmax}−h(0,a)進展開して、va^{dmax}−h(0,a)の換わりにh(q,a)−h(0,a)を用いることにより、演算回数を削減している。

[0176] s'=va^{dmax}−h(0,a)及びh'(q)=h(q,a)−h(0,a)が特定されている場合のべき乗算A

^{n}では、べき乗算の演算プログラムを実行させて電子計算機をべき乗算機として機能させる。その際に、図10に示すように、はじめに、CPU11は、べき数nと、χ＝aとしてスカラーs'＝va^{dmax}－h(0,a)及びh'(q)＝h(q,a)－h(0,a)と、元A∈H⊂F$_{q}^{k}$の値を入力してメモリ装置13に記憶する(ステップS601)。この場合、電子計算機は、入力手段として機能する。

[0177] 次いで、電子計算機は、初期化手段として機能し、CPU11は、メモリ装置13に演算結果を格納するZを確保して、初期化(Z←1)する(ステップS602)。そして、電子計算機は第1の演算手段として機能し、CPU11はメモリ装置13に記憶された元Aの値を読み出して、A^{2^{j}}をあらかじめ演算し、メモリ装置13に記憶しておく(ステップS603)。ステップS603の演算はステップS403の演算とアルゴリズムは同じであり、CPU11が行う処理も同じであるので、説明は省略する。

[0178] 次いで、電子計算機は、第1の展開手段として機能し、スカラーnを、

[数34]

$$n=\sum_{i=0}^{\lceil \log_{s'} n \rceil} c[i]s'^{i},0\le c[i]\le s'.$$

とs'進展開する(ステップS604)。ステップS604でのs'進展開は、ステップS404でのs進展開とアルゴリズムは同じであり、CPU11が行う処理も同じなるので、説明は省略する。

[0179] 次いで、電子計算機は、第2の展開手段として機能し、べき数nを、h'(q)及びc[i]を用いながら、

[数35]

$$n=\sum_{i=0}^{k-1} d[i]q^{i},0\le d[i]\le s'.$$

とq進展開する(ステップS605)。ステップS605でのq進展開は、スカラーs'(＝va^{dmax}－h(0,a))が、ステップS505でのスカラーs(＝D$_{dmax}$(a))とは異なる点以外では、ステップS505でのs進展開とアルゴリズムは同じであり、CPU11が行う処理も同じであるため、詳細な説明は省略する。

[0180] ステップS605でのq進展開でも、q進展開の係数がs'よりも大きくなることがある。こ

のように、q進展開の係数がs'よりも大きい場合（ステップS606：NO）には、q進展開の係数に対してs'の剰余をとることにより、q進展開の係数がs'よりも小さくなるように調整している（ステップS607）。このステップS607での演算も、スカラーs'（$=va^{dmax}-h(0,a)$）が、ステップS507でのスカラーs（$=D_{dmax}(a)$）とは異なる点以外では、ステップS507での演算とアルゴリズムは同じであり、CPU11が行う処理も同じであるため、詳細な説明は省略する。ここで、電子計算機は、ステップS606において比較手段として機能し、ステップS607において調整手段として機能する。

[0181] 次いで、電子計算機は、第2の演算手段として機能し、$A[i]=A^{d[i]}$の演算を行う（ステップS608）。ステップS608でも、バイナリ法を用いており、ステップS608の演算もステップS508の演算とアルゴリズムは同じであり、CPU11が行う処理も同じであるので、説明は省略する。

[0182] 次いで、電子計算機は、合成手段として機能し、ステップS608で演算したA[i]を用いて、べき乗算A^nを、

[数36]

$$A^n=\prod_{i=0}^{k-1}\phi_q^i(A[i]).$$

によって合成する（ステップS609）。ステップS609の演算もステップS509の演算とアルゴリズムは同じであり、CPU11が行う処理も同じであるので、説明は省略する。

[0183] そして、電子計算機は、出力手段として機能し、べき乗算の演算プログラムの実行結果として、Zを出力し（ステップS610）、べき乗算の演算プログラムを終了している。これによって、べき数nを$\log_s n$分割したので、ϕ_qを用いることで2乗算の演算回数をおよそdmax/degr(a)に削減することができる。

[0184] 多項式$h(q,\chi)$及び$v\chi^{dmax}-h(0,\chi)$は、位数$q(\chi)$、素数位数$r(\chi)$及び差分$s(\chi)$があらかじめ与えられていることから、あらかじめ特定できるので、$q(\chi)$、$r(\chi)$及び$s(\chi)$とともに、多項式$h(q,\chi)$及び$v\chi^{dmax}-h(0,\chi)$をべき乗算の演算プログラムに組み込んでもよいし、$r(\chi)$及び$s(\chi)$を用いて以下の補助プログラムによって、多項式$h(q,\chi)$及び$v\chi^{dmax}-h(0,\chi)$を求めてもよい。

[0185] 電子計算機は、補助プログラムを起動させると、図11に示すように、はじめに、入力

手段として機能する。CPU11は、入力したr(χ)、s(χ)及びm(χ)の値をメモリ装置13に記憶する(ステップS621)。ここで、m(χ)はr(χ)|m(χ)を満たす最小次数の多項式であり、一般的には円周等分多項式が用いられる。

[0186] 次いで、電子計算機は、展開手段として機能し、入力されたs(χ)を用いて、r(χ)を、

[数37]

$$r(\chi)=\sum_{i=0}^{\lceil \deg r(\chi)/\deg s(\chi)\rceil} D_i(\chi)s(\chi)^i, 0\le \deg(D_i(\chi))<\deg(s(\chi)).$$

とs(χ)進展開する(ステップS622)。ここで、iの大きさは、r(χ)及びs(χ)から自動的に決定される。ステップS622では、s(χ)進展開の演算として、電子計算機は、以下のアルゴリズムを実行している。

(1) for(i=0;i<「degr(χ)/degs(χ)」;i++)

(2) $D_i(\chi)\leftarrow r(\chi)\%s(\chi)$

(3) $r(\chi)\leftarrow(r(\chi)-D_i(\chi))/s(\chi)$

(4) End for

即ち、CPU11は、メモリ装置13からr(χ)及びχの値を読出し、$D_i(\chi)\leftarrow r(\chi)\%s(\chi)$及び$r(\chi)\leftarrow(r(\chi)-D_i(\chi))/s(\chi)$により表される演算をi=0からi<「degr(χ)/degs(χ)」まで繰り返し実行し、メモリ装置13に$D_i(\chi)$及びr(χ)の値を記憶する。

[0187] 次いで、電子計算機は、第1の特定手段として機能し、deg($D_i(\chi)$)の最大の次数dmaxの項であるχ^{dmax}の係数を抽出して、抽出された係数の和をT(q,χ)とし、それ以外の和をU(q,χ)とする(ステップS623)。ステップS623では、電子計算機は、具体的に以下のアルゴリズムを実行している。

(1) for(i=0;i<「degr(χ)/degs(χ)」;i++)

(2) $T(q,\chi)\leftarrow 0, U(q,\chi)\leftarrow 0$

(3) if(deg($D_i(\chi)$)=dmax)

(4) $T(q,\chi)\leftarrow T(q,\chi)+D_i(\chi)q^i$

(5) End if

(6) else

(7) $U(q,\chi)\leftarrow U(q,\chi)+D_i(\chi)q^i$

(8) End else

(9) End for

[0188] 即ち、CPU11は、メモリ装置13からr(χ)、s(χ)及び$D_i(\chi)$の値を読出し、$T(q,\chi)\leftarrow 0, U(q,\chi)\leftarrow 0$の初期化処理を行った後に、$\deg(D_i(\chi))=dmax$を満たす場合は$T(q,\chi)\leftarrow T(q,\chi)+D_i(\chi)q^i$により表される代入演算を、$\deg(D_i(\chi))=dmax$を満たさない場合は$U(q,\chi)\leftarrow U(q,\chi)+D_i(\chi)q^i$により表される代入演算を、i=0からi<「degr(χ)/degs(χ)」まで繰り返して実行し、メモリ装置13にT(q,χ)及びU(q,χ)を記憶する。

[0189] 次いで、電子計算機は、第2の特定手段として機能。CPU11は、ステップS623で特定したT(q,χ)の最高次数係数$T_{dmax}(q)$を特定、メモリ装置13に記憶する(ステップS624)。

[0190] 次いで、電子計算機は、第3の特定手段として機能し、ステップS624で特定した最高次数係数$T_{dmax}(q)$を用い、

$V(q) \mid m(q), \gcd(T_{dmax}(q), V(q))=1$

を満たすV(q)を特定する(ステップS625)。ステップS625では、電子計算機は、具体的に以下のアルゴリズムを実行している。

(1) $W(q)\leftarrow \gcd(T_{dmax}(q), m(q))$

(2) $V(q)\leftarrow W(q)$

即ち、CPU11は、メモリ装置13から$T_{dmax}(q)$及びm(q)の値を読出し、$W(q)\leftarrow \gcd(T_{dmax}(q), m(q))$及び$V(q)\leftarrow W(q)$により表される演算を行って、メモリ装置13に、W(q)及びV(q)の値を記憶する。

[0191] 次いで、電子計算機は、第4の特定手段として機能する。即ち、CPU11はメモリ装置13から、ステップS625で特定したV(q)を読み出して、

$g(q)V(q)\equiv v \pmod{m(q)}$

を満たすスカラーv及びg(q)を、拡張ユークリッドの互除法によって特定し、メモリ装置13に記憶する(ステップS626)。この拡張ユークリッドの互除法は、一般的なライブラリにおいて準備されている既知のプログラムに基づいて実行されるものであり、特に、g(q)の係数及びスカラーvが小さくなるようにしておくことが望ましい。

[0192] 次いで、電子計算機は、ステップS626で特定したg(q)をメモリ装置13から読み出し、

[数38]

$$h(q,\chi) = g(q)(T(q,\chi) - T_{d\max}(q)\chi^{d\max} + U(q,\chi)) \bmod q^k - 1.$$

の演算を行って多項式h(q,χ)を特定し(ステップS627)、多項式h(q,χ)及びvχ^{dmax}−h(0,χ)の値をメモリ装置13に記憶し出力している(ステップS628)。このようにして、電子計算機では、補助プログラムを用いて多項式h(q,χ)及びvχ^{dmax}−h(0,χ)を求めることができる。この場合、電子計算機は、ステップS627において演算手段として機能し、ステップS628において出力手段として機能する。このvχ^{dmax}−h(0,χ)及び多項式h(q,χ)を図10のステップ601に用いることで図10に示すべき乗算により2乗算の演算回数をおよそdmax/degr(χ)に削減することができる。

請求の範囲

[1] 楕円曲線をE／F_q ＝x^3＋ax＋b－y^2＝0, a∈F_q , b∈F_q とし、

$E(F_q)$を有限体F_qで定義される楕円曲線の有理点が成す加法群、

$E(F_q^k)$を有限体F_qの拡大体F_q^kで定義される楕円曲線の有理点が成す加法群、

ϕ_qを有限体F_qに関する有理点のフロベニウス自己準同型写像、

tをフロベニウス自己準同型写像ϕ_qのトレース、

r を$E(F_q)$の位数＃$E(F_q)$＝q＋1－tを割り切る素数位数、

E[r]を位数が素数rである有理点の集合、

[j]を有理点をj倍する写像、

Gを

$$G=E[r]\cap \mathrm{Ker}(\phi_q-[q])$$

を満たす$E(F_q^k)$に含まれる有理点の集合として、

非負整数nに対するGの有理点Qのスカラーn倍算を、CPU及び記憶手段を備えた電子計算機により演算するスカラー倍算の演算方法において、

CPUが、前記非負整数nの値、前記トレースtの値、及び、Q∈G⊂$E(F_q^k)$により表される有理点Qの値を入力して前記記憶手段に記憶する入力ステップと、

CPUが、演算結果Zを記憶する前記記憶手段を初期化する初期化ステップと、

Gの有理点Qに対し、

$$\phi_q(Q)=[q]Q=[t-1]Q$$

が成り立つことにより、

CPUが、s＝t－1として、前記nをs進展開した次式に基づいて、

[数39]

$$n=\sum_i c[i]s^i, 0\le c[i]\le s.$$

c[i]←n％s及びn←(n-c[i])/sにより表される代入演算をi＝0から所定回繰り返し行って各係数c[i]及び非負整数nの値を前記記憶手段に記憶する展開ステップと、

CPUが、前記記憶手段から前記有理点Q及び前記係数c[i]を読み出して、Q[i]＝c[i]Qにより表される演算をi＝0から所定回繰り返し行って各Q[i]の値を前記記

憶手段に記憶する演算ステップと、

CPUが、t-1に換えて有理点に対するフロベニウス自己準同型写像ϕ_qを用いて表される次式のスカラー倍算nQに基づいて、

[数40]

$$nQ = \sum_i \phi_q^i(Q[i]).$$

前記記憶手段からQ[i]及び演算結果Zを読み出し、Z←Z+ϕ_q^i(Q[i])により表される代入演算をi＝0から所定回繰り返し行ってスカラー倍算の演算結果Zを前記記憶手段に記憶する合成ステップと、

を有することを特徴とするスカラー倍算の演算方法。

[2] 前記楕円曲線の有限体F_qの位数q、＃E(F_q)を割り切る素数位数r、フロベニウス自己準同型写像ϕ_qのトレースtが、整数変数χを用いてそれぞれq(χ)、r(χ)、t(χ)で与えられている場合に、

CPUが、前記q(χ)、r(χ)、t(χ)の各値を入力して前記記憶手段に記憶する補助入力ステップと、

CPUが、前記記憶手段からr(χ)及びt(χ)の値を読み出して、前記s(χ)＝t(χ)－1として、r(χ)をs(χ)進展開した次式に基づいて、

[数41]

$$r(\chi) = \sum_{i=0}^{\lceil \deg r(\chi)/\deg s(\chi) \rceil} D_i(\chi)s(\chi)^i, 0 \le \deg(D_i(\chi)) < \deg(s(\chi)).$$

D_i(χ)←r(χ)%s(χ)及びr(χ)←(r(χ)-D_i(χ))/s(χ)により表される代入演算をi＝0からi<「degr(χ)/degs(χ)」まで繰り返し行って、各係数D_i(χ)及びr(χ)の値を前記記憶手段に記憶する補助展開ステップと、

CPUが、前記記憶された係数D_i(χ)のうち、deg(D_i(χ))が最大のものをD_{dmax}(χ)として抽出し、前記記憶手段に記憶する補助抽出ステップと、

CPUが、前記記憶手段からD_{dmax}(χ)、D_i(χ)、Qの値を読み出して、

$$\phi_q^{dmax}([D_{dmax}(\chi)]Q) = \Sigma\, \phi_q^{i}([D_i(\chi)]Q) - \phi_q^{dmax}([D_{dmax}(\chi)]Q)$$
$$= [f(\phi_q, \chi)]Q$$

となる多項式$f(\phi_q,\chi)$を用い、$\phi_q^{k}Q=Q$に基づいて

$[D_{dmax}(\chi)]Q=[f(\phi_q,\chi)\phi_q^{-dmax}]Q=[h(\phi_q,\chi)]Q$

となる多項式$h(\phi_q,\chi)$を特定し、前記多項式$h(\phi_q,\chi)$の値を前記記憶手段に記憶する補助特定ステップと、

CPUが、前記s進展開を$\chi=a$として$s=D_{dmax}(a)$からなる$D_{dmax}(a)$進展開に置換え、前記$D_{dmax}(a)$に換えて前記多項式$h(\phi_q,a)$を用いるステップと、を有することを特徴とする請求項1に記載のスカラー倍算の演算方法。

[3] 前記係数$D_i(\chi)$において最高次数dmaxとなる係数$D_i(\chi)$が複数存在する場合に、

前記補助入力ステップは、CPUが、$r(\chi)\mid m(\chi)$を満たす$m(\chi)$の値を入力して前記記憶手段に記憶するステップを更に含み、

CPUが、$\deg(D_i(\chi))$の最高次数dmaxの項であるχ^{dmax}の係数を$T_{dmax}(\phi_q)$として、前記記憶手段から係数$D_i(\chi)$を読み出し、前記記憶手段に$T(\phi_q,\chi)$及び$U(\phi_q,\chi)$を初期値を0として割り当て、$\deg(D_i(\chi))=dmax$となる場合に$T(\phi_q,\chi)\leftarrow T(\phi_q,\chi)+D_i(\chi)\phi_q^{i}$、その他の場合に$U(\phi_q,\chi)\leftarrow U(\phi_q,\chi)+D_i(\chi)\phi_q^{i}$により表される代入演算をi＝0からi<「$\deg r(\chi)/\deg s(\chi)$」まで繰り返し行って、$T(\phi_q,\chi)$及び$U(\phi_q,\chi)$の値を前記記憶手段に記憶し、最高次数係数$T_{dmax}(\phi_q)$を特定する第2の補助特定ステップと、

CPUが、前記記憶手段から$m(\chi)$及び$R(\chi)$の値を読み出して、$r(\chi)\mid m(\chi)$を満たす最小次数の多項式$m(\chi)$を用いて

$V(\phi_q)\mid m(\phi_q),\gcd(T_{dmax}(\phi_q),V(\phi_q))=1$

を満たす$V(\phi_q)$を、$W(\phi_q)\leftarrow\gcd(T_{dmax}(\phi_q),m(\phi_q))$及び$V(\phi_q)\leftarrow W(\phi_q)$により表される代入演算を行って特定し、前記$V(\phi_q)$の値を前記記憶手段に記憶する第3の補助特定ステップと、

CPUが、前記記憶手段から$V(\phi_q)$及び$m(\phi_q)$の値を読み出して、

$g(\phi_q)V(\phi_q)\equiv v(\mathrm{mod}\ m(\phi_q))$

を満たす整数のスカラーv及び$g(\phi_q)$を拡張ユークリッドの互除法により特定し、前記スカラーv及び$g(\phi_q)$の値を前記記憶手段に記憶する第4の補助特定ステップと、

前記補助特定ステップに換えて、CPUが、前記記憶手段から$T_{dmax}(\phi_q)$、χ^{dmax}、$D_i(\chi)$、Qの各値を読み出して、

$$[T_{dmax}(\phi_q)\chi^{dmax}]Q=\Sigma\phi_q^i([D_i(\chi)]Q)-[T_{dmax}(\phi_q)\chi^{dmax}]Q$$
$$=[f(\phi_q,\chi)]Q$$

となる多項式$f(\phi_q,\chi)$と、前記$g(\phi_q)$を用い、$\phi_q^k Q=Q$に基づいて、

$$[v\chi^{dmax}]Q=[g(\phi_q)f(\phi_q,\chi)]Q=[h(\phi_q,\chi)]Q$$

となる多項式$h(\phi_q,\chi)$を特定し、前記多項式$h(\phi_q,\chi)$の値を前記記憶手段に記憶する第5の補助特定ステップと、

CPUが、前記記憶手段から前記$h(\phi_q,\chi)$の値を読み出して、

この$h(\phi_q,\chi)$のϕ_qに関する定数項$h(0,\chi)$が、

$$[v\chi^{dmax}-h(0,\chi)]Q=[h(\phi_q,\chi)-h(0,\chi)]Q$$

を満たすことを用いて、

$\chi=a$として、$s'=va^{dmax}-h(0,a)$及び$h'(\phi_q)=h(\phi_q,a)-h(0,a)$により表される演算を行ってs'、$h'(\phi_q)$の値を前記記憶手段に記憶し、

t-1進展開した前記nを$D_{dmax}(a)$進展開する換わりに$va^{dmax}-h(0,a)$進展開して、$va^{dmax}-h(0,a)$の換わりに$h(\phi_q,a)-h(0,a)$を用いるステップと、を有することを特徴とする請求項2に記載のスカラー倍算の演算方法。

[4] F_q^kを位数qの有限体F_qのk次拡大体、

HをF_q^kの素数位数rの部分乗法群、

ϕ_qを有限体F_qに関する元のフロベニウス自己準同型写像として、

非負整数nに対するHの元Aのn乗算を行うべき乗算を、CPU及び記憶手段を備えた電子計算機により演算する演算方法において、

CPUが、前記非負整数nの値、前記位数qの値、前記F_q^kの素数位数rの値、$A\in H\subset F_q^k$により表される元Aの値を入力して前記記憶手段に記憶する入力ステップと、

CPUが、演算結果Zを記憶する前記記憶手段を初期化する初期化ステップと、

CPUが、前記位数q、前記元Aの値を前記記憶手段から読み出して、前記qとrの差分をs=q-rとし、T[j]←A及びA←A*Aにより表される代入演算を、j=0からj<「$\log_2$ s」まで繰り返し行って前記T[j]及び前記Aの値を前記記憶手段に記憶する第1の演

算ステップと、

CPUが、前記記憶手段から前記n及び差分sの値を読み出して、差分sにより展開した次式に基づいて、

[数42]

$$n = \sum_i c[i]s^i, 0 \le c[i] \le s.$$

c[i]←n%s及びn←(n-c[i])/sにより表される代入演算をi＝0から所定回繰り返して行い、各係数c[i]及び非負整数nの値を前記記憶手段に記憶する展開ステップと、

CPUが、前記記憶手段からc[i]及び前記nの値を読み出して、A[i]＝$A^{c[i]}$に基づいて、A[i]＝1に初期化し、c[i]&1である場合にA[i]←A[i]*T[j]、c[i]←c[i]/2により表される代入演算を、i＝0から所定回繰り返して行い、前記記憶手段にA[i]及びc[i]の値を記憶する第2の演算ステップと、

CPUが、前記記憶手段から各A[i]を読み出し、次式に基づいて、

[数43]

$$A^n = \prod_i \phi_q^i(A[i]).$$

Z←Z＊ϕ_q^i(A[i])により表されるべき乗演算を、i＝0から所定回繰り返して行い、計算結果Zとして前記記憶手段に記憶する合成ステップと、を有することを特徴とするべき乗算の演算方法。

[5] X^{Y}はX^Yであることを表すこととし、

前記位数q、前記素数位数r、前記sが、整数変数χを用いてそれぞれq(χ)、r(χ)、s(χ)で与えられている場合に、

CPUが、前記q(χ)、r(χ)、s(χ)の各値を入力して前記記憶手段に記憶する補助入力ステップと、

CPUが、前記記憶手段からr(χ)及びs(χ)を読み出して、前記s(χ)を用いて前記r(χ)をs(χ)進展開した次式に基づいて、

[数44]

$$r(\chi) = \sum_{i=0}^{\lceil \deg r(\chi)/\deg s(\chi) \rceil} D_i(\chi)s(\chi)^i, 0 \le \deg(D_i(\chi)) < \deg(s(\chi)).$$

$D_i(\chi)\leftarrow r(\chi)\%s(\chi)$及び$r(\chi)\leftarrow(r(\chi)-D_i(\chi))/s(\chi)$により表される代入演算を、i＝0からi<「$degr(\chi)/degs(\chi)$」まで繰り返して行い、前記係数$D_i(\chi)$及び$r(\chi)$を前記記憶手段に記憶する補助展開ステップと、

CPUが、前記記憶された係数$D_i(\chi)$のうち、$deg(D_i(\chi))$が最大のものを$D_{dmax}(\chi)$として抽出し、前記記憶手段に記憶する補助抽出ステップと、

CPUが、前記記憶手段から前記$D_{dmax}(\chi)$、$D_i(\chi)$、qの値を読み出して、

$$(A\hat{}\{D_{dmax}(\chi)\})\hat{}\{q^{dmax}\}=A\hat{}\{\Sigma_{i\neq dmax}-D_i(\chi)q^i\}=A\hat{}\{f(q,\chi)\}$$

となる多項式$f(q,\chi)$を用い、$\phi_q^k(A)=A$に基づいて

$$A\hat{}\{D_{dmax}(\chi)\}=A\hat{}\{\Sigma_{i\neq dmax}-D_i(\chi)q^i-q^{dmax}\}=A\hat{}\{h(q,\chi)\}$$

となる多項式$h(q,\chi)$を特定し、前記多項式$h(q,\chi)$の値を前記記憶手段に記憶する補助特定ステップと、

CPUが、前記s進展開した前記nを、$\chi=a$として$s=D_{dmax}(a)$からなる$D_{dmax}(a)$進展開に置き換え、前記$D_{dmax}(a)$に換えて前記多項式$h(q,a)$を用いるステップと、を有することを特徴とする請求項4に記載のべき乗算の演算方法。

[6] 前記係数$D_i(\chi)$において最高次数dmaxとなる係数$D_i(\chi)$が複数存在する場合に、

前記補助記憶ステップは、CPUが、$r(\chi)\mid m(\chi)$を満たす$m(\chi)$の値を入力して前記記憶手段に記憶するステップを更に含み、

CPUが、$deg(D_i(\chi))$の最高次数dmaxの項であるχ^{dmax}の係数を$T_{dmax}(q)$として、前記記憶手段から係数$D_i(\chi)$を読み出し、前記記憶手段に$T(q,\chi)$及び$U(q,\chi)$を初期値を0として割り当て、$deg(D_i(\chi))=dmax$となる場合に$T(q,\chi)\leftarrow T(q,\chi)+D_i(\chi)q^i$、その他の場合に$U(q,\chi)\leftarrow U(q,\chi)+D_i(\chi)q^i$により表される代入演算をi＝0からi<「$degr(\chi)/degs(\chi)$」まで繰り返して行って$T(q,\chi)$及び$U(q,\chi)$の値を前記記憶手段に記憶し、最高次数係数$T_{dmax}(q)$を特定する第2の補助特定ステップと、

CPUが、前記記憶手段から$m(\chi)$及び$R(\chi)$の値を読み出して、$r(\chi)\mid m(\chi)$を満たす最小次数の多項式$m(\chi)$を用いて

$$V(q)\mid m(q),gcd(T_{dmax}(q),V(q))=1$$

を満たす$V(q)$を、$W(q)\leftarrow gcd(T_{dmax}(q),m(q))$及び$V(q)\leftarrow W(q)$により表される演算を行

って特定し、前記V(q)の値を前記記憶手段に記憶する第3の補助特定ステップと、

CPUが、前記記憶手段からV(q)及びm(q)の値を読み出して、

$g(q)V(q)\equiv v(\mathrm{mod}\ m(q))$

を満たす整数のスカラーv及びg(q)を拡張ユークリッドの互除法により特定し、前記スカラーv及びg(q)の値を前記記憶手段に記憶する第4の補助特定ステップと、

前記補助特定ステップに換えて、CPUが、前記記憶手段から$T_{dmax}(q)$、χ^{dmax}、$D_i(\chi)$、Qの各値を読み出して、

$$A\hat{}\{T_{dmax}(q)\chi^{dmax}\}=A\hat{}\{\Sigma D_i(\chi)q^i-T_{dmax}(q)\chi^{dmax}\}$$
$$=A\hat{}\{f(q,\chi)\}$$

となる多項式$f(q,\chi)$と、前記g(q)を用い、$\phi_q^k(A)=A$に基づいて、

$$A\hat{}\{v\chi^{dmax}\}=A\hat{}\{g(q)f(q,\chi)\}=A\hat{}\{h(q,\chi)\}$$

となる多項式$h(q,\chi)$を特定し、前記多項式$h(q,\chi)$の値を前記記憶手段に記憶する第5の補助特定ステップと、

CPUが、前記記憶手段から前記$h(q,\chi)$の値を読み出して、

この$h(q,\chi)$のqに関する定数項$h(0,\chi)$が、

$$A\hat{}\{v\chi^{dmax}-h(0,\chi)\}=A\hat{}\{h(q,\chi)-h(0,\chi)\}$$

を満たすことを用いて、

$\chi=a$として、$s'=va^{dmax}-h(0,a)$及び$h'(q)=h(q,a)-h(0,a)$ により表される演算を行ってs'、h'(q)の値を前記記憶手段に記憶し、s進展開した前記nを$D_{dmax}(a)$進展開する換わりに$va^{dmax}-h(0,a)$進展開して、$va^{dmax}-h(0,a)$の換わりに$h(q,a)-h(0,a)$を用いるステップと、を有することを特徴とする請求項5に記載のべき乗算の演算方法。

[7] 楕円曲線を$E/F_q=x^3+ax+b-y^2=0,\ a\in F_q,\ b\in F_q$とし、

$E(F_q)$を有限体F_qで定義される楕円曲線の有理点が成す加法群、

$E(F_q^k)$を有限体F_qの拡大体F_q^kで定義される楕円曲線の有理点が成す加法群、

ϕ_qを有限体F_qに関する有理点のフロベニウス自己準同型写像、

tをフロベニウス自己準同型写像ϕ_qのトレース、

rを$E(F_q)$の位数$\#E(F_q)=q+1-t$を割り切る素数位数、

E[r]を位数が素数rである有理点の集合、

[j]を有理点をj倍する写像、

Gを

$$G=E[r]\cap \mathrm{Ker}(\phi_q-[q])$$

を満たす$E(F_q^k)$に含まれる有理点の集合として、

非負整数nに対するGの有理点Qのスカラーn倍算を、CPU及び記憶手段を備えた電子計算機に実行させるためのスカラー倍算の演算プログラムにおいて、

電子計算機に、

前記非負整数nの値、前記トレースtの値、及び、$Q\in G\subset E(F_q^k)$により表される有理点Qの値を入力して前記記憶手段に記憶する入力手順と、

演算結果Zを記憶する前記記憶手段を初期化する初期化手順と、

Gの有理点Qに対し、

$$\phi_q(Q)=[q]Q=[t-1]Q$$

が成り立つことにより、

s＝t－1として、前記nをs進展開した次式に基づいて、

[数45]

$$n=\sum_i c[i]s^i, 0\le c[i]\le s.$$

c[i]←n％s及びn←(n-c[i])/sにより表される代入演算をi＝0から所定回繰り返し行って各係数c[i]及び非負整数nの値を前記記憶手段に記憶する展開手順と、

前記記憶手段から前記有理点Q、非負整数n、及び前記c[i]の値を読み出して、Q[i]＝c[i]Qにより表される演算をi＝0から所定回繰り返し行って各Q[i]の値を前記記憶手段に記憶する演算手順と、

t-1に換えて有理点に対するフロベニウス自己準同型写像ϕ_qを用いて表される次式のスカラー倍算nQに基づいて、

[数46]

$$nQ=\sum_i \phi_q^i(Q[i]).$$

前記記憶手段からQ[i]及び演算結果Zを読み出し、$Z\leftarrow Z+\phi_q^i(Q[i])$により表される代入演算をi＝0から所定回繰り返し行ってスカラー倍算の演算結果Zを前記記憶手

段に記憶する合成手順と、

を実行させるためのスカラー倍算の演算プログラムを記録した電子計算機読取可能な記録媒体。

[8] 前記楕円曲線の有限体F_qの位数q、$\#E(F_q)$を割り切る素数位数r、フロベニウス自己準同型写像ϕ_qのトレースtが、整数変数χを用いてそれぞれ$q(\chi)$、$r(\chi)$、$t(\chi)$で与えられている場合に、電子計算機に、

前記$q(\chi)$、$r(\chi)$、$t(\chi)$の各値を入力して前記記憶手段に記憶する補助入力手順と、

前記記憶手段から$r(\chi)$及び$t(\chi)$の値を読み出して、前記$s(\chi)=t(\chi)-1$として、$r(\chi)$を$s(\chi)$進展開した次式に基づいて、

[数47]

$$r(\chi)=\sum_{i=0}^{\lceil \deg r(\chi)/\deg s(\chi)\rceil} D_i(\chi)s(\chi)^i, 0\le \deg(D_i(\chi))<\deg(s(\chi)).$$

$D_i(\chi)\leftarrow r(\chi)\%s(\chi)$及び$r(\chi)\leftarrow(r(\chi)-D_i(\chi))/s(\chi)$により表される代入演算をi＝0からi<「$\deg r(\chi)/\deg s(\chi)$」まで繰り返し行って、各係数$D_i(\chi)$及び$r(\chi)$の値を前記記憶手段に記憶する補助展開手順と、

前記記憶された係数$D_i(\chi)$のうち、$\deg(D_i(\chi))$が最大のものを$D_{dmax}(\chi)$として抽出し、前記記憶手段に記憶する補助抽出手順と、

前記記憶手段から$D_{dmax}(\chi)$、$D_i(\chi)$、Qの値を読み出して、

$$\phi_q^{dmax}([D_{dmax}(\chi)]Q)=\Sigma\,\phi_q^{i}([D_i(\chi)]Q)-\phi_q^{dmax}([D_{dmax}(\chi)]Q)$$
$$=[f(\phi_q,\chi)]Q$$

となる多項式$f(\phi_q,\chi)$を用い、$\phi_q^{k}Q=Q$に基づいて

$$[D_{dmax}(\chi)]Q=[f(\phi_q,\chi)\phi_q^{-dmax}]Q=[h(\phi_q,\chi)]Q$$

となる多項式$h(\phi_q,\chi)$を特定し、前記多項式$h(\phi_q,\chi)$の値を前記記憶手段に記憶する補助特定手順と、

前記s進展開を$\chi=a$として$s=D_{dmax}(a)$からなる$D_{dmax}(a)$進展開に置換え、前記$D_{dmax}(a)$に換えて前記多項式$h(\phi_q,a)$を用いる手順と、を実行させるためのスカラー倍算の演算プログラムを記録した請求項7に記載の電子計算機読取可能な記録媒体。

[9] 前記係数$D_i(\chi)$において最高次数dmaxとなる係数$D_i(\chi)$が複数存在する場合に、

前記補助入力手順は、$r(\chi) \mid m(\chi)$を満たす$m(\chi)$の値を入力して前記記憶手段に記憶する手順を更に含み、

電子計算機に、

$\deg(D_i(\chi))$の最高次数dmaxの項であるχ^{dmax}の係数を$T_{dmax}(\phi_q)$として、前記記憶手段から係数$D_i(\chi)$を読み出し、前記記憶手段に$T(\phi_q,\chi)$及び$U(\phi_q,\chi)$を初期値を0として割り当て、$\deg(D_i(\chi))=dmax$となる場合に$T(\phi_q,\chi)\leftarrow T(\phi_q,\chi)+D_i(\chi)\phi_q^i$、その他の場合に$U(\phi_q,\chi)\leftarrow U(\phi_q,\chi)+D_i(\chi)\phi_q^i$により表される代入演算をi＝0からi＜「$degr(\chi)/degs(\chi)$」まで繰り返し行って、$T(\phi_q,\chi)$及び$U(\phi_q,\chi)$の値を前記記憶手段に記憶し、最高次数係数$T_{dmax}(\phi_q)$を特定する第2の補助特定手順と、

前記記憶手段から$m(\chi)$及び$R(\chi)$の値を読み出して、$r(\chi) \mid m(\chi)$を満たす最小次数の多項式$m(\chi)$を用いて

$$V(\phi_q) \mid m(\phi_q), \gcd(T_{dmax}(\phi_q), V(\phi_q)) = 1$$

を満たす$V(\phi_q)$を、$W(\phi_q)\leftarrow\gcd(T_{dmax}(\phi_q), m(\phi_q))$及び$V(\phi_q)\leftarrow W(\phi_q)$により表される代入演算を行って特定し、前記$V(\phi_q)$の値を前記記憶手段に記憶する第3の補助特定手順と、

CPUが、前記記憶手段から$V(\phi_q)$及び$m(\phi_q)$の値を読み出して、

$$g(\phi_q)V(\phi_q) \equiv v \pmod{m(\phi_q)}$$

を満たす整数のスカラーv及び$g(\phi_q)$を拡張ユークリッドの互除法により特定し、前記スカラーv及び$g(\phi_q)$の値を前記記憶手段に記憶する第4の補助特定手順と、

前記補助特定手順に換えて、CPUが、前記記憶手段から$T_{dmax}(\phi_q)$、χ^{dmax}、$D_i(\chi)$、Qの各値を読み出して、

$$[T_{dmax}(\phi_q)\chi^{dmax}]Q = \Sigma\,\phi_q^i([D_i(\chi)]Q) - [T_{dmax}(\phi_q)\chi^{dmax}]Q$$
$$= [f(\phi_q,\chi)]Q$$

となる多項式$f(\phi_q,\chi)$と、前記$g(\phi_q)$を用い、$\phi_q^k Q = Q$に基づいて、

$$[v\chi^{dmax}]Q = [g(\phi_q)f(\phi_q,\chi)]Q = [h(\phi_q,\chi)]Q$$

となる多項式$h(\phi_q,\chi)$を特定し、前記多項式$h(\phi_q,\chi)$の値を前記記憶手段に記憶

する第5の補助特定手順と、

前記記憶手段から前記$h(\phi_q,\chi)$の値を読み出して、

この$h(\phi_q,\chi)$のϕ_qに関する定数項$h(0,\chi)$が、

$[v\chi^{dmax}-h(0,\chi)]Q=[h(\phi_q,\chi)-h(0,\chi)]Q$

を満たすことを用いて、

$\chi=a$として、$s'=va^{dmax}-h(0,a)$及び$h'(\phi_q)=h(\phi_q,a)-h(0,a)$により表される演算を行って$s'$、$h'(\phi_q)$の値を前記記憶手段に記憶し、

t-1進展開した前記nをD_{dmax}(a)進展開する換わりに$va^{dmax}-h(0,a)$進展開して、$va^{dmax}-h(0,a)$の換わりに$h(\phi_q,a)-h(0,a)$を用いる手順と、を実効させるためのスカラー倍算の演算プログラムを記録した請求項8に記載の電子計算機読取可能な記録媒体。

[10] F_q^kを位数qの有限体F_qのk次拡大体、

HをF_q^kの素数位数rの部分乗法群、

ϕ_qを有限体F_qに関する元のフロベニウス自己準同型写像として、

非負整数nに対するHの元Aのn乗算を行うべき乗算を、CPU及び記憶手段を備えた電子計算機により実行させるための演算プログラムにおいて、電子計算機に、

前記非負整数nの値、前記位数qの値、前記F_q^kの素数位数rの値、$A\in H\subset F_q^k$により表される元Aの値を入力して前記記憶手段に記憶する入力手順と、

演算結果Zを記憶する前記記憶手段を初期化する初期化手順と、

前記位数q、前記元Aの値を前記記憶手段から読み出して、前記qとrの差分を$s=q-r$とし、T[j]←A及びA←A*Aにより表される代入演算を、j=0からj<「$\log_2 s$」まで繰り返して行って前記T[j]及び前記Aの値を前記記憶手段に記憶する第1の演算手順と、

前記記憶手段から前記n及び差分sの値を読み出して、差分sにより展開した次式に基づいて、

[数48]

$$n=\sum_i c[i]s^i,\ 0\le c[i]\le s.$$

c[i]←n%s及びn←(n-c[i])/sにより表される代入演算をi=0から所定回繰り返して行

い、各係数c[i]及び非負整数nの値を前記記憶手段に記憶する展開手順と、

前記記憶手段からc[i]及び前記nの値を読み出して、A[i]＝$A^{c[i]}$に基づいて、A[i]＝1に初期化し、c[i]＆1である場合にA[i]←A[i]*T[j]、c[i]←c[i]/2により表される代入演算を、i＝0から所定回繰り返して行い、前記記憶手段にA[i]及びc[i]の値を記憶する第2の演算手順と、

前記記憶手段から各A[i]を読み出し、次式に基づいて、

[数49]

$$A^n = \prod_i \phi_q^i(A[i]).$$

Z←Z＊ϕ_q^i(A[i])により表されるべき乗演算を、i＝0から所定回繰り返して行い、計算結果Zとして前記記憶手段に記憶する合成手順と、を実行させるためのべき乗算の演算プログラムを記録した電子計算機読取可能な記録媒体。

[11] X^{Y}はX^Yであることを表すこととし、

前記位数q、前記素数位数r、前記sが、整数変数χを用いてそれぞれq(χ)、r(χ)、s(χ)で与えられている場合に、電子計算機に、

前記q(χ)、r(χ)、s(χ)の各値を入力して前記記憶手段に記憶する補助入力手順と、

前記記憶手段からr(χ)及びs(χ)を読み出して、前記s(χ)を用いて前記r(χ)をs(χ)進展開した次式に基づいて、

[数50]

$$r(\chi) = \sum_{i=0}^{\lceil \deg r(\chi)/\deg s(\chi) \rceil} D_i(\chi)s(\chi)^i, 0 \le \deg(D_i(\chi)) < \deg(s(\chi)).$$

D_i(χ)←r(χ)%s(χ)及びr(χ)←(r(χ)-D_i(χ))/s(χ)により表される代入演算を、i＝0からi<「degr(χ)/degs(χ)」まで繰り返して行い、前記係数D_i(χ)及びr(χ)を前記記憶手段に記憶する補助展開手順と、

前記記憶された係数D_i(χ)のうち、deg(D_i(χ))が最大のものをD_{dmax}(χ)として抽出し、前記記憶手段に記憶する補助抽出手順と、

前記記憶手段から前記D_{dmax}(χ)、D_i(χ)、qの値を読み出して、

$(A\hat{}\{D_{dmax}(\chi)\})\hat{}\{q^{dmax}\}=A\hat{}\{\Sigma_{i\neq dmax}-D_i(\chi)q^i\}=A\hat{}\{f(q,\chi)\}$

となる多項式$f(q,\chi)$を用い、$\phi_q^k(A)=A$に基づいて

$A\hat{}\{D_{dmax}(\chi)\}=A\hat{}\{\Sigma_{i\neq dmax}-D_i(\chi)q^i-q^{dmax}\}=A\hat{}\{h(q,\chi)\}$

となる多項式$h(q,\chi)$を特定し、前記多項式$h(q,\chi)$の値を前記記憶手段に記憶する補助特定手順と、

前記s進展開した前記nを、$\chi=a$としてs＝$D_{dmax}(a)$からなる$D_{dmax}(a)$進展開に置き換え、前記$D_{dmax}(a)$に換えて前記多項式$h(q,a)$を用いる手順と、を実行させるためのべき乗算の演算プログラムを記録した請求項10に記載の電子計算機読取可能な記録媒体。

[12] 前記係数$D_i(\chi)$において最高次数dmaxとなる係数$D_i(\chi)$が複数存在する場合に、

前記補助記憶手順は、$r(\chi)\mid m(\chi)$を満たす$m(\chi)$の値を入力して前記記憶手段に記憶する手順を更に含み、

電子計算機に、

$deg(D_i(\chi))$の最高次数dmaxの項であるχ^{dmax}の係数を$T_{dmax}(q)$として、前記記憶手段から係数$D_i(\chi)$を読み出し、前記記憶手段に$T(q,\chi)$及び$U(q,\chi)$を初期値を0として割り当て、$deg(D_i(\chi))=dmax$となる場合に$T(q,\chi)\leftarrow T(q,\chi)+D_i(\chi)q^i$、その他の場合に$U(q,\chi)\leftarrow U(q,\chi)+D_i(\chi)q^i$により表される代入演算をi＝0からi<「$degr(\chi)/degs(\chi)$」まで繰り返して行って$T(q,\chi)$及び$U(q,\chi)$の値を前記記憶手段に記憶し、最高次数係数$T_{dmax}(q)$を特定する第2の補助特定手順と、

前記記憶手段から$m(\chi)$及び$R(\chi)$の値を読み出して、$r(\chi)\mid m(\chi)$を満たす最小次数の多項式$m(\chi)$を用いて

$V(q)\mid m(q),gcd(T_{dmax}(q),V(q))=1$

を満たす$V(q)$を、$W(q)\leftarrow gcd(T_{dmax}(q),m(q))$及び$V(q)\leftarrow W(q)$により表される演算を行って特定し、前記$V(q)$の値を前記記憶手段に記憶する第3の補助特定手順と、

前記記憶手段から$V(q)$及び$m(q)$の値を読み出して、

$g(q)V(q)\equiv v(\mathrm{mod}\ m(q))$

を満たす整数のスカラーv及び$g(q)$を拡張ユークリッドの互除法により特定し、前記ス

カラーv及びg(q)の値を前記記憶手段に記憶する第4の補助特定手順と、

前記補助特定手順に換えて、前記記憶手段から$T_{dmax}(q)$、χ^{dmax}、$D_i(\chi)$、Qの各値を読み出して、

$$A\hat{}\{T_{dmax}(q)\chi^{dmax}\}=A\hat{}\{\Sigma D_i(\chi)q^i-T_{dmax}(q)\chi^{dmax}\}$$
$$=A\hat{}\{f(q,\chi)\}$$

となる多項式$f(q,\chi)$と、前記g(q)を用い、$\phi_q^k(A)=A$に基づいて、

$$A\hat{}\{v\chi^{dmax}\}=A\hat{}\{g(q)f(q,\chi)\}=A\hat{}\{h(q,\chi)\}$$

となる多項式$h(q,\chi)$を特定し、前記多項式$h(q,\chi)$の値を前記記憶手段に記憶する第5の補助特定手順と、

CPUが、前記記憶手段から前記$h(q,\chi)$の値を読み出して、

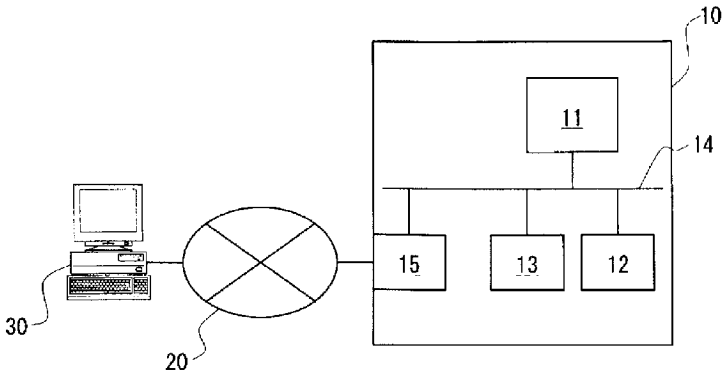
この$h(q,\chi)$のqに関する定数項$h(0,\chi)$が、

$$A\hat{}\{v\chi^{dmax}-h(0,\chi)\}=A\hat{}\{h(q,\chi)-h(0,\chi)\}$$

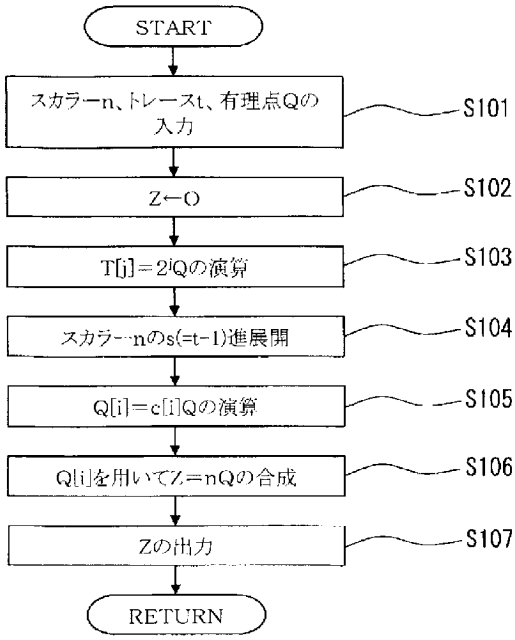
を満たすことを用いて、

$\chi=a$として、$s'=va^{dmax}-h(0,a)$及び$h'(q)=h(q,a)-h(0,a)$ により表される演算を行ってs'、h'(q)の値を前記記憶手段に記憶し、s進展開した前記nを$D_{dmax}(a)$進展開する換わりに$va^{dmax}-h(0,a)$進展開して、$va^{dmax}-h(0,a)$の換わりに$h(q,a)-h(0,a)$を用いる手順と、を実行させるためのべき乗算の演算プログラムを記録した請求項11に記載の電子計算機読取可能な記録媒体。

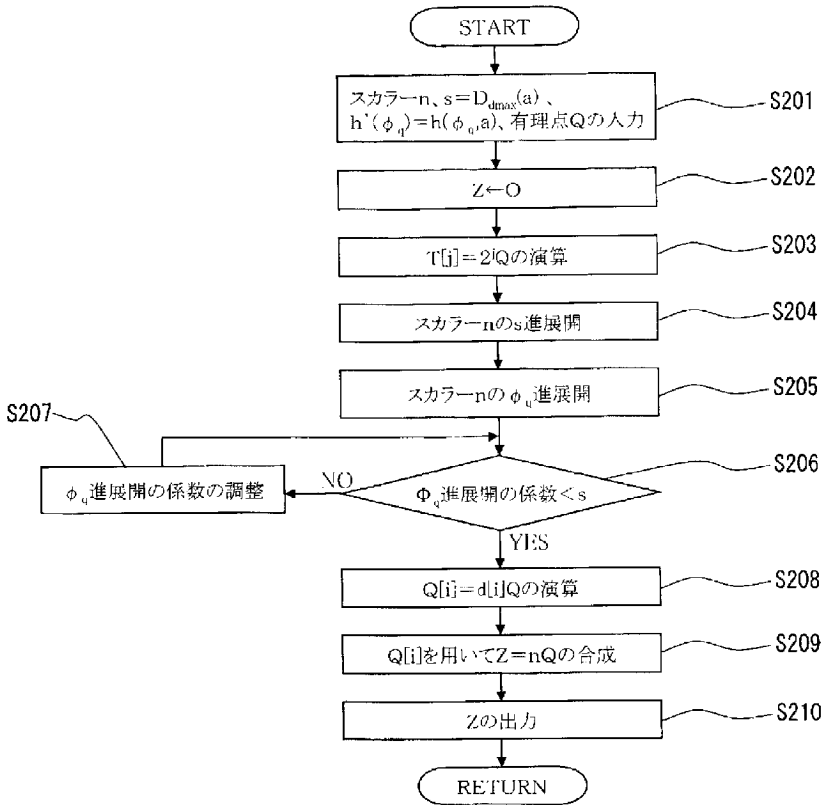
[図1]


10
11
14
15
13
12
30
20

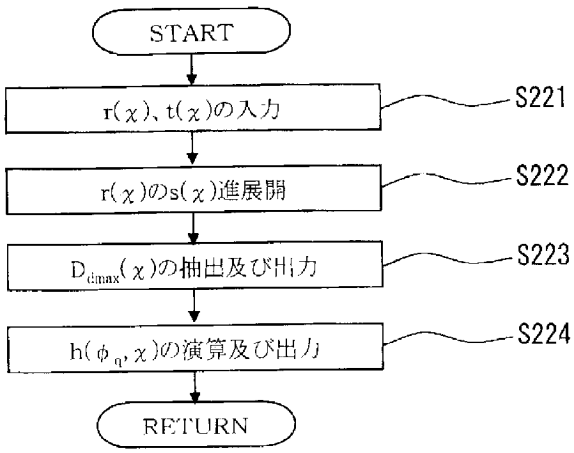
[図2]


START
スカラーn、トレースt、有理点Qの入力
S101
Z←O
S102
T[j]＝2jQの演算
S103
スカラーnのs(=t-1)進展開
S104
Q[i]＝c[i]Qの演算
S105
Q[i]を用いてZ＝nQの合成
S106
Zの出力
S107
RETURN

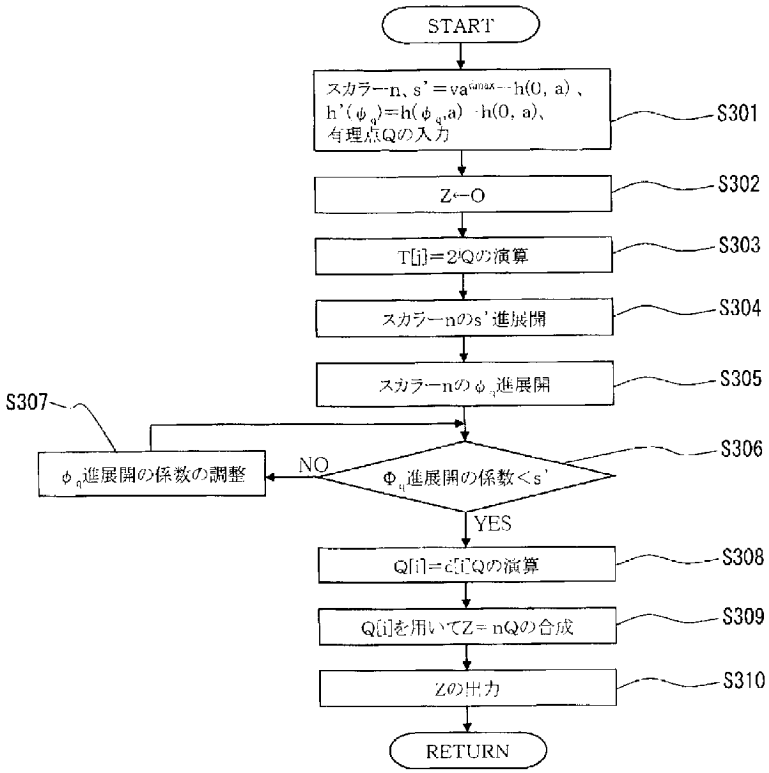
[図3]


START
スカラーn、s=$D_{dmax}(a)$、
$h'(\phi_q)=h(\phi_q,a)$、有理点Qの入力
S201
Z←O
S202
T[j]=2jQの演算
S203
スカラーnのs進展開
S204
スカラーnのϕ_q進展開
S205
S207
ϕ_q進展開の係数の調整
NO
Φ_q進展開の係数<s
S206
YES
Q[i]=d[i]Qの演算
S208
Q[i]を用いてZ=nQの合成
S209
Zの出力
S210
RETURN

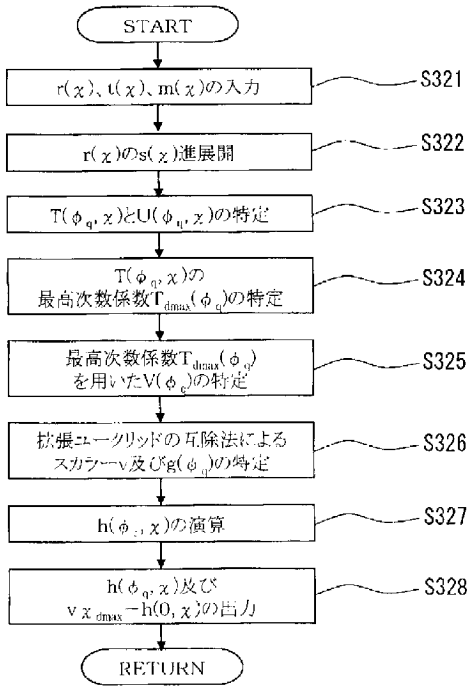
[図4]


START
r(χ)、t(χ)の入力
S221
r(χ)のs(χ)進展開
S222
$D_{dmax}(\chi)$の抽出及び出力
S223
$h(\phi_q,\chi)$の演算及び出力
S224
RETURN

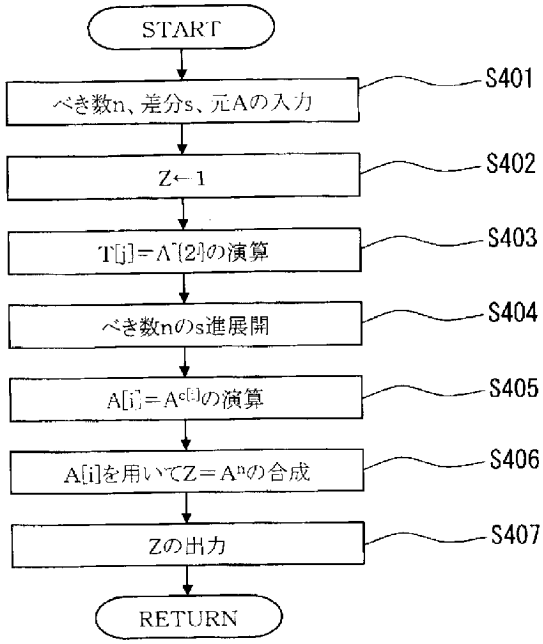
[図5]


START
スカラーn、s'=va^dmax…h(0, a)、
h'(φq)=h(φq,a) …h(0, a)、
有理点Qの入力
S301
Z←O
S302
T[j]=2jQの演算
S303
スカラーnのs'進展開
S304
スカラーnのφq進展開
S305
S307
φq進展開の係数の調整
NO
Φq進展開の係数<s'
S306
YES
Q[i]=ciQの演算
S308
Q[i]を用いてZ=nQの合成
S309
Zの出力
S310
RETURN

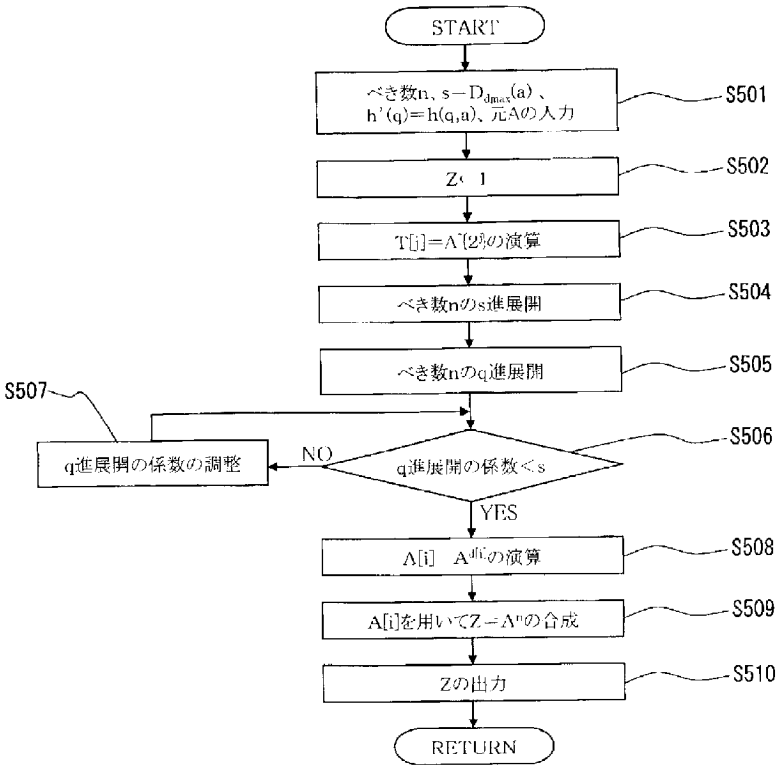
[図6]


START
r(χ)、u(χ)、m(χ)の入力
S321
r(χ)のs(χ)進展開
S322
T(φq, χ)とU(φq, χ)の特定
S323
T(φq, χ)の
最高次数係数Tdmax(φq)の特定
S324
最高次数係数Tdmax(φq)
を用いたV(φq)の特定
S325
拡張ユークリッドの互除法による
スカラーv及びg(φq)の特定
S326
h(φq, χ)の演算
S327
h(φq, χ)及び
v χdmax…h(0, χ)の出力
S328
RETURN

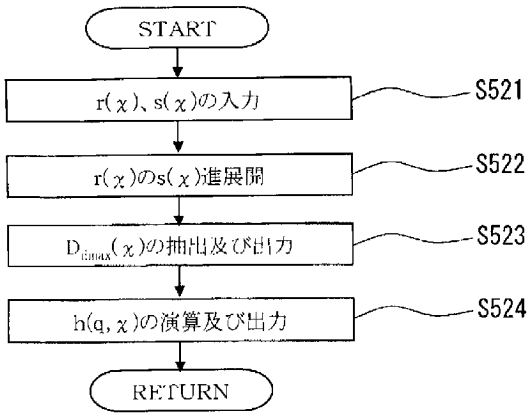
[図7]


START
べき数n、差分s、元Aの入力
S401
Z←1
S402
T[j]=A^{2^j}の演算
S403
べき数nのs進展開
S404
A[i]=A^{c[i]}の演算
S405
A[i]を用いてZ=A^nの合成
S406
Zの出力
S407
RETURN

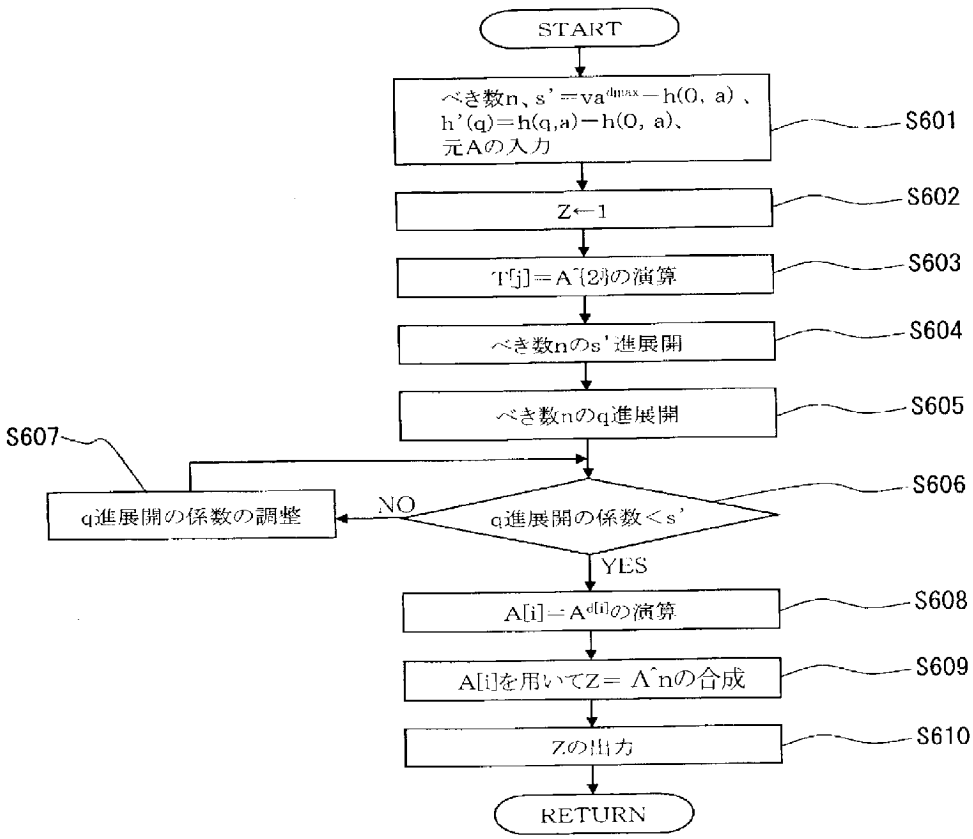
[図8]


START
べき数n、s−D_dmax(a)、h'(q)=h(q,a)、元Aの入力
S501
Z←1
S502
T[j]=A^{2^j}の演算
S503
べき数nのs進展開
S504
べき数nのq進展開
S505
S507
q進展開の係数<s
S506
NO
q進展開の係数の調整
YES
A[i] A^{d[i]}の演算
S508
A[i]を用いてZ=A^nの合成
S509
Zの出力
S510
RETURN

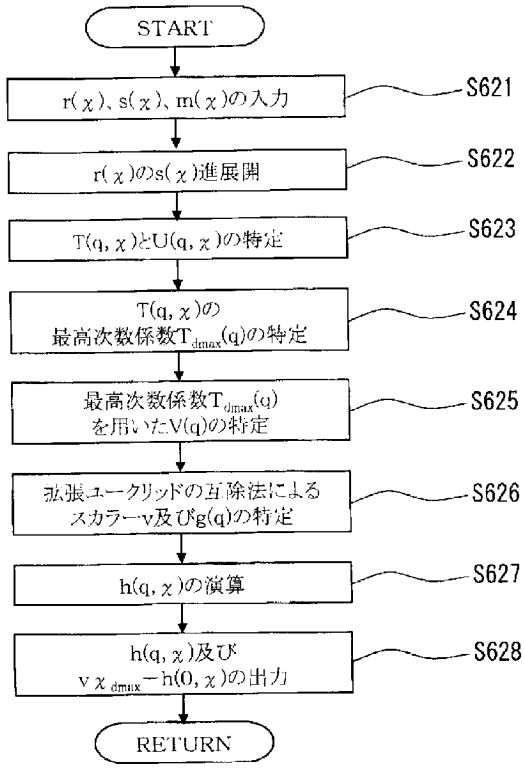
[図9]


START
r(χ)、s(χ)の入力
S521
r(χ)のs(χ)進展開
S522
$D_{i\max}(\chi)$の抽出及び出力
S523
h(q,χ)の演算及び出力
S524
RETURN

[図10]


START
べき数n、s'=va^dmax−h(0, a)、
h'(q)=h(q,a)−h(0, a)、
元Aの入力
S601
Z←1
S602
T[j]=A^{2}の演算
S603
べき数nのs'進展開
S604
べき数nのq進展開
S605
S607
q進展開の係数の調整
NO
q進展開の係数<s'
S606
YES
A[i]=A^d[i]の演算
S608
A[i]を用いてZ= A^nの合成
S609
Zの出力
S610
RETURN

[図11]


START
r(χ)、s(χ)、m(χ)の入力
S621
r(χ)のs(χ)進展開
S622
T(q, χ)とU(q, χ)の特定
S623
T(q, χ)の
最高次数係数T_dmax(q)の特定
S624
最高次数係数T_dmax(q)
を用いたV(q)の特定
S625
拡張ユークリッドの互除法による
スカラーv及びg(q)の特定
S626
h(q, χ)の演算
S627
h(q, χ)及び
vχ_dmax−h(0, χ)の出力
S628
RETURN

PATENT COOPERATION TREATY

PCT

DECLARATION OF NON-ESTABLISHMENT OF INTERNATIONAL SEARCH REPORT

(PCT Article 17(2)(a), Rules 13*ter*.1(c) and 39)

Applicant's or agent's file reference OP00413PCT	**IMPORTANT DECLARATION**	Date of mailing *(day/month/year)* 21 April, 2009 (21.04.09)
International application No. PCT/JP2009/053395	International filing date *(day/month/year)* 25 February, 2009 (25.02.09)	(Earliest) Priority Date *(day/month/year)* 25 February, 2008 (25.02.08)
International Patent Classification (IPC) or both national classification and IPC *G09C1/00* (2006.01)i		
Applicant Okayama University		

This International Searching Authority hereby declares, according to Article 17(2)(a), that **no international search report will be established** on the international application for the reasons indicated below.

1. [x] The subject matter of the international application relates to:
   - a. [x] scientific theories.
   - b. [x] mathematical theories.
   - c. [ ] plant varieties.
   - d. [ ] animal varieties.
   - e. [ ] essentially biological processes for the production of plants and animals, other than microbiological processes and the products of such processes.
   - f. [ ] schemes, rules or methods of doing business.
   - g. [ ] schemes, rules or methods of performing purely mental acts.
   - h. [ ] schemes, rules or methods of playing games.
   - i. [ ] methods for treatment of the human body by surgery or therapy.
   - j. [ ] methods for treatment of the animal body by surgery or therapy.
   - k. [ ] diagnostic methods practised on the human or animal body.
   - l. [x] mere presentations of information.
   - m. [ ] computer programs for which this International Searching Authority is not equipped to search prior art.
2. [x] The failure of the following parts of the international application to comply with prescribed requirements prevents a meaningful search from being carried out:
   [x] the description [x] the claims [ ] the drawings
3. [ ] A meaningful search could not be carried out without the sequence listing; the applicant did not, within the prescribed time limit:
   - [ ] furnish a sequence listing on paper complying with the standard provided for in Annex C of the Administrative Instructions, and such listing was not available to the International Searching Authority in a form and manner acceptable to it.
   - [ ] furnish a sequence listing in electronic form complying with the standard provided for in Annex C of the Administrative Instructions, and such listing was not available to the International Searching Authority in a form and manner acceptable to it.
   - [ ] pay the required late furnishing fee for the furnishing of a sequence listing in response to an invitation under Rule 13ter.1(a) or (b).
4. [ ] A meaningful search could not be carried out without the tables related to the sequence listings; the applicant did not, within the prescribed time limit, furnish such tables in electronic form complying with the technical requirements provided for in Annex C-bis of the Administrative Instructions, and such tables were not available to the International Searching Authority in a form and manner acceptable to it.
5. Further comments:

Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

特 許 協 力 条 約

ＰＣＴ

国際調査報告を作成しない旨の決定

（法第８条第２項、法施行規則第42条、第50条の３第７項）
〔ＰＣＴ17条(2)(a)、ＰＣＴ規則13の3.1(c) 及び(d)、39〕

出願人又は代理人 の書類記号 OP00413PCT	重要決定	発送日 （日.月.年）　２１．０４．２００９
国際出願番号 ＰＣＴ／ＪＰ２００９／０５３３９５	国際出願日 （日.月.年）　２５．０２．２００９	優先日 （日.月.年）　２５．０２．２００８
国際特許分類（ＩＰＣ）Int.Cl. G09C1/00(2006.01)i		
出願人（氏名又は名称） 国立大学法人　岡山大学		

この出願については、法第８条第２項（ＰＣＴ17条(2)(a)）の規定に基づき、次の理由により国際調査報告を作成しない旨の決定をする。

１．☑ この国際出願は、次の事項を内容としている。
- a．☑ 科学の理論
- b．☑ 数学の理論
- c．☐ 植物の品種
- d．☐ 動物の品種
- e．☐ 植物及び動物の生産の本質的に生物学的な方法（微生物学的方法による生産物及び微生物学的方法を除く。）
- f．☐ 事業活動に関する計画、法則又は方法
- g．☐ 純粋に精神的な行為の遂行に関する計画、法則又は方法
- h．☐ 遊戯に関する計画、法則又は方法
- i．☐ 人の身体の手術又は治療による処置方法
- j．☐ 動物の身体の手術又は治療による処置方法
- k．☐ 人又は動物の身体の診断方法
- l．☑ 情報の単なる提示
- m．☐ この国際調査機関が先行技術を調査できないコンピューター・プログラム

２．☑ この国際出願の次の部分が所定の要件を満たしていないので、有効な国際調査をすることができない。
☑ 明細書　☑ 請求の範囲　☐ 図面

３．☐ 入手可能な配列表が存在せず、有意義な調査を行うことができなかった。
出願人は所定の期間内に、
- ☐ 実施細則の附属書Ｃに定める基準を満たす紙形式の配列表を提出しなかったため、国際調査機関は、認められた形式及び方法で配列表を入手することができなかった。
- ☐ 実施細則の附属書Ｃに定める基準を満たす電子形式の配列表を提出しなかったため、国際調査機関は、認められた形式及び方法で配列表を入手することができなかった。
- ☐ ＰＣＴ規則13の3.1(a)又は(b)に基づく命令に応じた、要求された配列表の遅延提出手数料を支払わなかった。

４．☐ 入手可能な配列表に関連するテーブルが存在しないため、有意義な調査ができなかった。すなわち、出願人が、所定の期間内に、実施細則の附属書Ｃの２に定める技術的な要件を満たす電子形式のテーブルを提出しなかったため、国際調査機関は、認められた形式及び方法でテーブルを入手することができなかった。

５．附記

名称及びあて名 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員） 青木　重徳 電話番号　０３－３５８１－１１０１　内線　３５４６	５Ｓ　４２２９

様式ＰＣＴ／ＩＳＡ／２０３（２００５年４月）