

(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  
2011 年 3 月 31 日(31.03.2011)

PCT

(10) 国際公開番号  
WO 2011/036746 A1

- (51) 国際特許分類:  
G06F 7/72 (2006.01)
- (21) 国際出願番号: PCT/JP2009/066537
- (22) 国際出願日: 2009 年 9 月 24 日(24.09.2009)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (71) 出願人 (米国を除く全ての指定国について): 株式会社東芝 (Kabushiki Kaisha Toshiba) [JP/JP]; 〒1058001 東京都港区芝浦一丁目 1 番 1 号 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 清水 秀夫 (SHIMIZU, Hideo) [JP/JP]; 〒1058001 東京都港区芝浦一丁目 1 番 1 号 株式会社東芝 知的財産部内 Tokyo (JP). 駒野 雄一 (KOMANO, Yuichi) [JP/JP]; 〒1058001 東京都港区芝浦一丁目 1 番 1 号 株式会社東芝 知的財産部内 Tokyo (JP). 藤崎 浩一 (FUJISAKI, Koichi) [JP/JP]; 〒1058001 東京都港区芝浦一丁目 1 番 1 号 株式会社東芝 知的財産部内 Tokyo (JP). 川村 信一 (KAWAMU-

RA, Shinichi) [JP/JP]; 〒1058001 東京都港区芝浦一丁目 1 番 1 号 株式会社東芝 知的財産部内 Tokyo (JP).

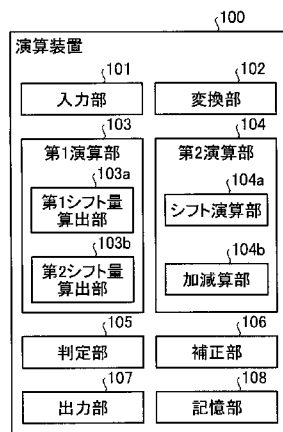
- (74) 代理人: 酒井 宏明, 外 (SAKAI, Hiroaki et al.); 〒1006020 東京都千代田区霞が関三丁目 2 番 5 号 霞が関ビルディング 酒井国際特許事務所 Tokyo (JP).
- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, 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, PE, 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

[続葉有]

(54) Title: CALCULATION DEVICE

(54) 発明の名称: 演算装置

[図1]



100 CALCULATION DEVICE  
101 INPUT UNIT  
102 CONVERSION UNIT  
103 FIRST CALCULATION UNIT  
103a FIRST SHIFT AMOUNT CALCULATION UNIT  
103b SECOND SHIFT AMOUNT CALCULATION UNIT  
104 SECOND CALCULATION UNIT  
104a SHIFT CALCULATION UNIT  
104b ADDITION/SUBTRACTION UNIT  
105 DETERMINATION UNIT  
106 CORRECTION UNIT  
107 OUTPUT UNIT  
108 STORAGE UNIT

(57) Abstract: Provided is a calculation device which executes the Montgomery multiplication on the input of an arbitrary number of bits by using a number of steps substantially identical to the number of steps used in the ZDN method. The calculation device includes: a conversion unit (102) which converts an integer x into a redundant binary expression; a first shift amount calculation unit (103a) which calculates the first shift amount as the number of continuous zeros from the least significant bit toward the most significant bit of the intermediate result of the calculation; a second shift amount calculation unit (103b) which counts the number of continuous zeros from the least significant bit toward the most significant bit of the integer x of the redundant binary expression and calculates a second shift amount in accordance with the counted number; an addition/subtraction unit (104b) which calculates an intermediate result obtained by bit-shifting by the first shift amount and an intermediate result obtained by performing addition/subtraction on integer y and integer p which have been bit-shifted by the second shift amount and transmits the calculated intermediate results to the first shift amount calculation unit (103a); and an output unit (107) which outputs as the Montgomery multiplication result z, the intermediate result when the total of the first shift amounts coincides with the number of bits of the integer p.

(57) 要約:

[続葉有]

WO 2011/036746 A1



(AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, 添付公開書類:

GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL,  
NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ,  
CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN,  
TD, TG).

— 国際調査報告 (条約第 21 条(3))

ZDN法と同程度のステップ数で任意のビット数の入力に対してモンゴメリ乗算を実行する。整数  $x$  を冗長2進表現に変換する変換部102と、演算の中間結果の下位ビットから上位ビットに向けて連続する0の個数である第1シフト量を算出する第1シフト量算出部103aと、冗長2進表現の整数  $x$  の下位ビットから上位ビットに向けて連続する0の個数をカウントし、カウントした個数に基づいて第2シフト量を算出する第2シフト量算出部103bと、第1シフト量だけビットシフトした中間結果と、第2シフト量だけビットシフトした整数  $y$  と、整数  $p$  と、を加減算した中間結果を算出し、算出した中間結果を第1シフト量算出部103aに送出する加減算部104bと、第1シフト量の合計が整数  $p$  のビット数と一致したときの中間結果をモンゴメリ乗算結果  $z$  として出力する出力部107とを備える。

## 明 細 書

**発明の名称 : 演算装置**

**技術分野**

[0001] 本発明は、演算装置に関する。

**背景技術**

[0002] 整数同士の演算結果の剰余を取った結果を利用する有限体上の演算は、誤り訂正符号や暗号といった様々な分野に応用可能な基本技術として利用されている。応用分野が広いこともあって、乗算や剰余算を行う回路の高速化、小型化および省電力化などを実現するための多数の研究が行われている。剰余乗算とは、整数同士を掛けた結果を別の整数で割った余りを計算する演算である。剰余乗算を高速に実行するアルゴリズムとしては、例えばモンゴメリ乗算が知られている。

[0003] モンゴメリ乗算を使用する場合、予め演算の対象となる有限体上の数をモンゴメリ空間上の数に写像しておいてから、モンゴメリ乗算を行い、その結果を有限体上の数に逆写像することで本来求めたかった結果を求めることができる。変換と逆変換の手間が必要なので、モンゴメリ乗算を1回の剰余乗算に対して使用するのはコストが大きくなるが、べき乗剰余演算のように連続して複数回の剰余乗算を行うために使用するのに向いている。

[0004] モンゴメリ乗算の実現方法は大まかに2種類の実現方法がある。1つ目はワード乗算器を使用する実現方法である。1ワードを例えば32ビットとすると、32ビット×32ビットの乗算結果64ビットを求めることのできる32ビット乗算器を用いる方法である。この場合、法のワード数をMとすると $2 \times M^2 + M$ 回の乗算が必要になることが知られている。乗算器が1つだとすると、1回のモンゴメリ乗算に $2 \times M^2 + M$ クロックが必要になる。

[0005] もう1つの実現方法は、長い桁数の加算器を使う方法である。法が1024ビットだとすると1024ビット+1024ビットの結果を求めることの

できる加算器を用いる。法のビット数を $m$ すると $2 \times m$ 回の加算が必要になる。加算器が1つだとするとモンゴメリ乗算1回あたり $2 \times m$ クロックが必要になる。

[0006] 例えば、ワードベースのモンゴメリ乗算で32ビット $\times$ 32ビット乗算器を使うと、法が1024ビットの場合 $M=32$ ワードとなり、2080クロックが必要となる。一方、加算器を使ったモンゴメリ乗算では、法が1024ビットの場合、2048クロックが必要となる。法が2048ビットの場合、 $M=64$ ワードとなり、ワードベースのモンゴメリ乗算では8256クロックが必要となり、加算器を使ったモンゴメリ乗算では4096クロックが必要となる。

[0007] また、乗算を高速する方法として、NAF (Non-Adjacent Form、非特許文献1参照) などの冗長2進表現を使う方法が知られている。この方法では、乗数を冗長2進表現すると平均的に含まれる0の個数が増加することを利用して乗算が高速化される。

[0008] また、乗算だけでなく、剰余乗算も冗長2進表現を使って高速化する方法としてZDN法が知られている（例えば、非特許文献2）。ZDN法では、法のビット数を $m$ とした場合、理想的には $m/3$ クロック（ステップ）で剰余乗算を計算することができる。例えば、法のビット数が1024ビットであるとする、理想的には342ステップで剰余乗算を計算できることになる。

## 先行技術文献

### 非特許文献

[0009] 非特許文献1: D. Hankerson, A. Menezes, S. Vanstone, "Guide to Elliptic Curve Cryptography", Springer, 2004, p. 98.

非特許文献2: H. Sedlak, "The RSA cryptography processor", Proceedings of EUROCRYPT '87 (Amsterdam) (D. Chaum and W. L. Price, eds.), LNCS, vol. 304, Springer-Verlag, Berlin, 1988, pp. 95-105.

## 発明の概要

## 発明が解決しようとする課題

[0010] しかしながら、ZDN法は、演算処理を上位ビットから逐次的に行う方法である。すなわち、ZDN法は、いわゆるleft to rightの処理（L→R処理）である。一般的にL→R処理の場合、処理ビット数の変更が容易にできない点が問題となる。例えば1024ビットを処理する場合と、512ビットを処理する場合とでは、最上位ビットの位置が変わる。このため、処理をいずれのビットから開始するのに対応して複数の回路が必要となる問題がある。したがって、現状ではZDN法を実現するには、処理ビット数を固定長にするのが現実的な解である。このように、ZDN法は、最上位ビットから処理するアルゴリズムなので、処理ビット数を自由に変更できないという問題があった。

[0011] 一方、上述のように、従来のモンゴメリ乗算では、 $2 \times M^2 + M$ クロックまたは $2 \times m$ クロックが必要となり、ZDN法と比較して実行速度が遅いという問題があった。

[0012] 本発明は、上記に鑑みてなされたものであって、ZDN法と同程度のステップ数で、任意のビット数の入力に対してモンゴメリ乗算を実行できる演算装置を提供することを目的とする。

## 課題を解決するための手段

[0013] 本発明は、整数 $x$ と整数 $y$ との積の整数 $p$ を法とするモンゴメリ乗算結果 $z$ を演算する演算装置であって、前記整数 $x$ を冗長2進表現に変換する変換部と、前記モンゴメリ乗算結果 $z$ の演算の中間結果の下位ビットから上位ビットに向けて連続する0の個数をカウントし、カウントした個数に基づいて第1シフト量を算出する第1シフト量算出部と、冗長2進表現の前記整数 $x$ の下位ビットから上位ビットに向けて連続する0の個数をカウントし、カウントした個数に基づいて第2シフト量を算出する第2シフト量算出部と、前記第1シフト量だけビットシフトした前記中間結果と、前記第2シフト量だけビットシフトした前記整数 $y$ と、前記整数 $p$ と、を加減算した前記中間結果を算出し、算出した前記中間結果を前記第1シフト量算出部に送出手加

減算部と、前記第 1 シフト量の合計が前記整数  $p$  のビット数と一致したときの  
前記中間結果を前記モンゴメリ乗算結果  $z$  として出力する出力部と、を備  
えることを特徴とする。

### 発明の効果

[0014] 本発明によれば、ZDN法と同程度のステップ数で、任意のビット数の入  
力に対してモンゴメリ乗算を実行できるという効果を奏する。

### 図面の簡単な説明

- [0015] [図1]演算装置のブロック図。  
[図2]演算装置の回路構成例を示す図。  
[図3]演算処理のフローチャート。  
[図4]シフト量演算処理のフローチャート。  
[図5]関数 `zero count` のフローチャート。  
[図6]冗長 2 進表現を使用する手順を示す図。  
[図7]計算途中の各変数の値を示す図。  
[図8]演算装置のハードウェア構成図。

### 発明を実施するための形態

- [0016] 以下に添付図面を参照して、この発明にかかる演算装置の好適な実施の形  
態を詳細に説明する。
- [0017] 本実施の形態にかかる演算装置は、入力された整数  $x$ 、整数  $y$ 、および整  
数  $p$  を用いて整数  $x$  と整数  $y$  の整数  $p$  を法とするモンゴメリ乗算結果  $z$ （以  
下、乗算結果  $z$  という）を求める。このとき、整数  $x$  の下位ビットから逐次  
冗長 2 進表現に変換しながら、演算を繰り返し実行し、所定の終了条件を満  
たしたときの演算結果を乗算結果  $z$  として出力する。なお、以下では、繰り  
返し実行される演算の結果を中間結果といい、最終的に出力される結果を乗  
算結果という。中間結果および乗算結果のいずれも、乗算結果  $z$  を格納する  
ための所定のレジスタに記憶される。このため、以下では、中間結果および  
乗算結果のいずれも  $z$  と表記する場合がある。

[0018] 図 1 は、本実施の形態にかかる演算装置 100 の構成の一例を示すブロッ

ク図である。図 1 に示すように、演算装置 100 は、入力部 101 と、変換部 102 と、第 1 演算部 103 と、第 2 演算部 104 と、判定部 105 と、補正部 106 と、出力部 107 と、記憶部 108 とを備えている。

[0019] 入力部 101 は、演算に用いる各種データ（入力値）の入力を受付ける。例えば、入力部 101 は、モンゴメリ乗算に用いる整数  $x$ 、整数  $y$ 、および整数  $p$  の入力を受付ける。

[0020] 変換部 102 は、整数を冗長 2 進表現に変換する。例えば、変換部 102 は、入力された整数  $x$  を冗長 2 進表現に変換する。

[0021] 第 1 演算部 103 は、中間結果  $z$  のシフト量  $z\ s\ f\ t$ （第 1 シフト量）、整数  $y$  のシフト量  $y\ s\ f\ t$ （第 2 シフト量）、および、ビットシフトした整数  $y$  および整数  $p$  を加算するか減算するかなどを決定するための情報（ $y\ s\ g\ n$ 、 $p\ s\ g\ n$ ）を算出する。第 1 演算部 103 は、第 1 シフト量算出部 103a と、第 2 シフト量算出部 103b とを備えている。

[0022] 第 1 シフト量算出部 103a は、中間結果  $z$  の下位ビットから上位ビットに向けて連続する 0 の個数をカウントし、この個数を  $z\ s\ f\ t$  として算出する。具体的には、第 1 シフト量算出部 103a は、中間結果  $z$  の最下位ビットから上位ビットに向けて、中間結果  $z$  が算出されるごとに変更されるビット数のビットまでの間で、値が連続して 0 となっているビットの個数である  $z\ s\ f\ t$  を算出する。中間結果  $z$  が算出されるごとに変更されるビット数とは、その時点での  $x$  の処理済みビット数と、 $z$  の処理済みビット数との差分に相当する。すなわち、第 1 シフト量算出部 103a は、中間結果  $z$  の下位ビットから上位ビットに向けて連続する 0 の個数であって、中間結果  $z$  の処理済みビット数との和が  $x$  の処理済みビット数を超えないような値を  $z\ s\ f\ t$  として算出する。

[0023] 第 2 シフト量算出部 103b は、冗長 2 進表現で表された整数  $x$  の下位ビットから上位ビットに向けて連続する 0 の個数をカウントし、当該個数から  $y\ s\ f\ t$  を算出する。具体的には、第 2 シフト量算出部 103b は、冗長 2 進表現で表された整数  $x$  に含まれるビットのうち、連続する 0 の個数のカウ

ントの対象となったビットを表す処理済みビットと、処理済みビットの1つ上位のビット（値は0以外）とを除くビットを対象として、下位ビットから上位ビットに向けて連続する0の個数をカウントする。そして、第2シフト量算出部103bは、カウントした個数、整数xの処理済みビット数、中間結果zの処理済みビット数、およびz s f tを用いて、y s f tを算出する。

[0024] なお、第1演算部103によるz s f t、y s f t、y s g n、およびp s g nの算出方法の詳細は後述する。

[0025] 第2演算部104は、第1演算部103により演算されたz s f t、y s f t、y s g n、およびp s g nをもとに、中間結果zおよび整数yのシフト演算、および、シフト演算結果等の加減算を実行する。第2演算部104は、シフト演算部104aと、加減算部104bとを備えている。

[0026] シフト演算部104aは、z s f tの分だけ中間結果zを右シフトする。また、シフト演算部104aは、y s f tの分だけ整数yを左シフトする。

[0027] 加減算部104bは、シフト演算された中間結果zと、シフト演算された整数yと、整数pとを入力し、中間結果zに対して、y s g nおよびp s g nに応じて整数yおよび整数pの加算または減算を実行する。

[0028] 判定部105は、繰り返し実行される演算の終了を判定する。具体的には、判定部105は、中間結果zの処理済みビット数が、整数pのビット数を超えた場合に、演算を終了すると判定する。

[0029] 補正部106は、終了すると判定されたときの中間結果である乗算結果zを補正する。具体的には、補正部106は、乗算結果zが0より小さい場合に、乗算結果zに整数pを加算して乗算結果zを補正する。また、補正部106は、乗算結果zが整数p以上の場合に、乗算結果zから整数pを減算して乗算結果zを補正する。

[0030] 出力部107は、演算を終了すると判定されたときの中間結果である乗算結果zを出力する。補正部106により補正された場合は、出力部107は、補正後の乗算結果zを出力する。



- [0031] 記憶部 108 は、演算に用いる各種データ（入力値、中間結果等）を記憶する。なお、記憶部 108 は、HDD（Hard Disk Drive）、光ディスク、メモリカード、RAM（Random Access Memory）などの一般的に利用されているあらゆる記憶媒体により構成することができる。
- [0032] 次に、演算装置 100 の回路構成について図 2 を用いて説明する。図 2 は、演算装置 100 の回路構成例を示す図である。なお、図 2 は、主に図 1 の第 1 演算部 103、第 2 演算部 104 および記憶部 108 に対応する回路の構成例を示している。
- [0033] 図 2 に示すように、演算装置 100 は、エンコーダ 201 と、右シフト演算器 202 と、左シフト演算器 203 と、3 入力加減算器 204 と、レジスタ 211、212、213、214 とを備えている。
- [0034] レジスタ 211、212、213、および 214 は、それぞれ中間結果  $z$ （乗算結果  $z$ ）、整数  $y$ 、整数  $p$ 、および整数  $x$  を格納する。レジスタ 211 ~ 214 は、例えば多倍長整数で表された各整数を格納する。レジスタ 211 の出力は、右シフト演算器 202 の入力である。レジスタ 212 の出力は、左シフト演算器 203 の入力である。
- [0035] 右シフト演算器 202 は、入力された中間結果  $z$  を右へ  $z_{\text{shift}}$  ビット右シフトして出力する。左シフト演算器 203 は、入力された整数  $y$  を左へ  $y_{\text{shift}}$  ビット左シフトして出力する。
- [0036] 3 入力加減算器 204 は、右シフト演算器 202 の出力（中間結果  $z$ ）に対して、 $y_{\text{sgn}}$  と左シフト演算器 203 の出力（整数  $y$ ）との積を加算し、さらに、 $p_{\text{sgn}}$  とレジスタ 213 の出力（整数  $p$ ）との積を加算する。すなわち、3 入力加減算器 204 は、中間結果  $z$  に対して、 $y_{\text{sgn}}$  が 1 のときは整数  $y$  を加算し、 $y_{\text{sgn}}$  が -1 のときは整数  $y$  を減算し、 $y_{\text{sgn}}$  が 0 のときは整数  $y$  の加算も減算も行わない。また、3 入力加減算器 204 は、中間結果  $z$  と整数  $y$  との加減算結果に対して、 $p_{\text{sgn}}$  が 1 のときは整数  $p$  を加算し、 $p_{\text{sgn}}$  が -1 のときは整数  $p$  を減算し、 $p_{\text{sgn}}$  が 0 のときは整数  $p$  の加算も減算も行わない。

[0037] エンコーダ 201 は、中間結果  $z$ 、整数  $x$ 、整数  $p$ 、および演算で用いるその他の変数の状態から、 $z\text{ s f t}$ 、 $y\text{ s f t}$ 、 $y\text{ s g n}$ 、および  $p\text{ s g n}$  を決定して出力する。エンコーダ 201 によるこれらの値の決定方法の詳細は後述する。

[0038] なお、図 2 のレジスタ 211、212、213、214 が、図 1 の記憶部 108 に対応する。また、図 2 のエンコーダ 201 が、図 1 の第 1 演算部 103 に対応する。また、図 2 の右シフト演算器 202 および左シフト演算器 203 が、図 1 のシフト演算部 104 a に対応する。また、図 2 の 3 入力加減算器 204 が、図 1 の加減算部 104 b に対応する。

[0039] 次に、このように構成された本実施の形態にかかる演算装置 100 による演算処理について図 3 を用いて説明する。図 3 は、本実施の形態における演算処理の全体の流れを示すフローチャートである。

[0040] まず、入力部 101 が、演算に用いる入力値である整数  $x$ 、整数  $y$ 、および整数  $p$  の入力を受付ける（ステップ S301）。

[0041] 次に、変換部 102 が、整数  $x$  を冗長 2 進表現に変換する（ステップ S302）。なお、図 3 では、入力された整数  $x$  を繰り返し演算（ステップ S303～ステップ S305）の前に冗長 2 進表現に変換しているが、繰り返し演算の中で逐次整数  $x$  を冗長 2 進表現に変換するように構成してもよい。

[0042] 次に、第 1 演算部 103 が、 $y\text{ s f t}$  および  $z\text{ s f t}$  を算出するシフト量演算処理を実行する（ステップ S303）。シフト量演算処理の詳細は後述する。次に、第 2 演算部 104 が、算出されたシフト量に応じて中間結果  $z$  および整数  $y$  をシフトし、シフトした結果を用いて新たな中間結果  $z$  を演算する（ステップ S304）。具体的には、第 2 演算部 104 は、以下の（1）式によって中間結果  $z$  を算出する。なお、「 $>>$ 」および「 $<<$ 」はそれぞれ右シフト演算および左シフト演算を表す。

$$z = (z >> z\text{ s f t}) + y\text{ s g n} \times (y << y\text{ s f t}) + p\text{ s g n} \times p \\ \dots (1)$$

[0043] 次に、判定部 105 が、 $z$  の処理済みビット数が整数  $p$  のビット数より大

きいか否かを判定する（ステップS305）。zの処理済みビット数が整数pのビット数以下の場合（ステップS305：No）、ステップS303に戻り処理が繰り返される。すなわち、ステップS304で算出された中間結果zを用いて、シフト量演算処理（ステップS303）および新たな中間結果zの算出処理（ステップS304）が繰り返し実行される。

[0044] zの処理済みビット数が整数pのビット数より大きい場合（ステップS305：Yes）、補正部106が、必要に応じて乗算結果z（この時点でのレジスタ211の値）を補正する（ステップS306）。そして、出力部107が、乗算結果zをモンゴメリ乗算の結果として出力し（ステップS307）、演算処理を終了する。

[0045] 次に、ステップS303のシフト量演算処理の詳細について図4を用いて説明する。図4は、シフト量演算処理の一例を示すフローチャートである。

[0046] まず、第1演算部103は、連続する0を探索する範囲を表すzextを、以下の（2）式により算出する（ステップS401）。

$$zext = \min(xcnt, size) - zcnt \quad \dots (2)$$

[0047] なお、xcntは、整数xのうち、前のステップ（前の繰り返し演算）までに処理された処理済みビット数の合計を表す。また、zcntは、前のステップまでのzsftの合計を表す。また、sizeは、入力された整数pのサイズを表す。また、min(a, b)は、aおよびbの最小値を返す関数を表す。

[0048] 次に、第1シフト量算出部103aが、以下の（3）式によりzsftを算出する（ステップS402）。なお、関数zerocount(a, b, c)は、aの下位からbビット以上かつcビット未満の部分ビット列で、下位ビットから上位ビットに向けて値が連続して0となっているビットの個数を返す関数を表す。この関数の詳細については後述する。

$$zsft = zerocount(z, 0, zext) \quad \dots (3)$$

[0049] 次に、第1演算部103は、zsftがzextと一致するか否かを判定する（ステップS403）。zsftとzextとが一致する場合（ステッ

プS403: Yes)、第1演算部103は、psgnを0に設定する(ステップS404)。zsftとzex tとが一致しない場合(ステップS403: No)、第1演算部103は、中間結果zの下位からzsft+1ビット目の値と、整数pの下位1ビット目の値とが一致するか否かを判定する(ステップS405)。なお、図4のa[b]は、aの下位からbビット目の値を表す。

[0050] 中間結果zの下位からzsft+1ビット目の値と、整数pの下位1ビット目の値とが一致する場合(ステップS405: Yes)、第1演算部103は、psgnを-1に設定する(ステップS406)。中間結果zの下位からzsft+1ビット目の値と、整数pの下位1ビット目の値とが一致しない場合(ステップS405: No)、第1演算部103は、psgnを+1に設定する(ステップS407)。

[0051] 次に、第1演算部103は、冗長2進表現で表された整数xの下位ビットから上位ビットに向けて連続する0の個数を表すxsftを以下の(4)式により算出する(ステップS408)。

$$xsft = zerocount(x, xcnt, size + 1) \quad \dots \quad (4)$$

[0052] 次に、第1演算部103は、xcntとxsftとの和が、sizeより大きいかな否かを判定する(ステップS409)。xcntとxsftとの和がsizeより大きい場合(ステップS409: Yes)、第1演算部103は、ysgnを0に設定する(ステップS410)。xcntとxsftとの和がsize以下の場合(ステップS409: No)、第1演算部103は、ysgnを以下の(5)式により算出する(ステップS411)。

$$ysgn = x[xcnt + xsft] \quad \dots \quad (5)$$

[0053] 次に、第2シフト量算出部103bが、以下の(6)式によりysftを算出する(ステップS412)。

$$ysft = xcnt + xsft - zcnt - zsft \quad \dots \quad (6)$$

[0054] 次に、第1演算部103が、以下の(7)式によりxcntを算出する(

ステップS 4 1 3)。また、第1演算部103が、以下の(8)式により  $zcnt$  を算出する(ステップS 4 1 4)。

$$xcnt = xcnt + xsft + 1 \quad \dots (7)$$

$$zcnt = zcnt + zsft \quad \dots (8)$$

[0055] 次に、ステップS 4 0 2およびステップS 4 0 8で用いられる関数  $zerocount$  の処理の詳細について図5を用いて説明する。図5は、関数  $zerocount$  の処理の一例を示すフローチャートである。図5は、 $x$ 、 $a$ 、 $b$ が引数として入力された場合( $zerocount(x, a, b)$ )を例に説明する。

[0056] まず、カウンタ  $cnt$  が0に初期化される(ステップS 5 0 1)。次に、変数  $i$  が、入力値  $a$  に設定される(ステップS 5 0 2)。次に、変数  $i$  が入力値  $b$  より小さいか否かが判定される(ステップS 5 0 3)。変数  $i$  が入力値  $b$  より小さい場合(ステップS 5 0 3: Yes)、入力値  $x$  の下位から  $i$  ビット目の値が0であるか否かが判定される(ステップS 5 0 4)。

[0057] 入力値  $x$  の下位から  $i$  ビット目の値が0である場合(ステップS 5 0 4: Yes)、 $i$  および  $cnt$  にそれぞれ1が加算される(ステップS 5 0 5、ステップS 5 0 6)。そして、ステップS 5 0 3に戻り処理が繰り返される。

[0058] ステップS 5 0 3で変数  $i$  が入力値  $b$  以上と判定された場合(ステップS 5 0 3: No)、または、ステップS 5 0 4で入力値  $x$  の下位から  $i$  ビット目の値が0でないと判定された場合(ステップS 5 0 4: No)、その時点での  $cnt$  が関数の出力値として出力される(ステップS 5 0 7)。

[0059] 次に、このように構成された演算装置100により演算処理の具体例について説明する。以下では、「 $f2 \times d5 \bmod fb$ 」を計算する例を示す。すなわち、整数  $x = f2$ 、整数  $y = d5$ 、および整数  $p = fb$  が入力された場合の演算例を示す。なお、整数  $x$ 、 $y$ 、および  $p$  は、いずれも16進数で表されている。

[0060] 図6は、整数  $x (= f2)$  の冗長2進表現を使用する手順の例を示す図で

ある。なお、図6では、下線が付された1が「-1」を意味する。冗長2進表現は色々な種類が存在する。ここでは、冗長2進表現としてNAFを用いた例を説明する。なお、NAF以外の冗長2進表現を使っても同様の手順で本実施の形態の演算処理を実現できる。

[0061]  $f_2$ をNAF形式に変換すると、「1, 0, 0, 0, -1, 0, 0, 1, 0」と表される。なお、16進数の $f_2$ は10進数で表すと242である。NAF形式の「1, 0, 0, 0, -1, 0, 0, 1, 0」は、 $256 - 16 + 2 = 242$ を表すため、「1, 0, 0, 0, -1, 0, 0, 1, 0」が $f_2$ の別の表現であることがわかる。

[0062] 「1, 0, 0, 0, -1, 0, 0, 1, 0」を下位から順に見ていくと、1個の0の後に1が存在し、続いて2個の0の後に-1が存在し、続いて3個の0の後に1が存在する。なお、その後は0が続き1は存在しないと考える。

[0063] モンゴメリ乗算の各ステップ（繰り返し演算）では、0の連続した個数と、その次に存在する0でない値がペアにして使用される。すなわち、図6の例では、ステップ1（最初の繰り返し演算）では、1個の0と、その後の1とが使用される。また、次のステップ2では、2個の0と、その後の-1とが使用される。さらに次のステップ3では、3個の0と、その後の1とが使用される。なお、ステップ4以降では、1が存在せず、0が無限個続いていると考える。

[0064] エンコーダ201は、各ステップで、連続した0の個数を $x_{sf t}$ とし、その後に続く1または-1を $y_{sg n}$ とする。また、エンコーダ201は、整数 $x$ の冗長2進表現のビットのうち、それまでのステップで使用したビット数（処理済みビット数）を記録しておく。なお、エンコーダ201は、各ステップで、連続した0の個数+1個の桁（ビット）を消費（使用）する。

[0065] 図6の例では、まず、ステップ1で1個の0とその後の1とが使用される。すなわちステップ1では2個のビットが消費される。そして、これまでの処理済みビット数の合計は2個となる。ステップ2では、2個の0とその後の-1とが使用される。すなわちステップ2では3個のビットが消費される

。そして、処理済みビット数の合計は5個となる。また、ステップ3では、3個の0とその後の1とが使用される。すなわちステップ3では4個のビットが消費される。そして、処理済みビット数の合計は9個となる。

[0066] エンコーダ201は、0の連続した個数を  $x\ s\ f\ t$  とし、その後の非0（0以外の値）の値を  $y\ s\ g\ n$  とし、前のステップまでに使用したビット数の合計を  $x\ c\ n\ t$  とする。なお、ステップ1での  $x\ c\ n\ t$  は0とする。

[0067] ステップがある程度以上進むと、必ず上位に0が無限個続く状態に陥る。その場合、エンコーダ201は、 $x\ s\ f\ t$  を、 $s\ i\ z\ e$ （=整数  $p$  のビット数） $+1-x\ c\ n\ t$  とする。

[0068] 以上の処理をまとめると次のようになる。すなわち、各ステップでは、以下のような  $x\ c\ n\ t$ 、 $x\ s\ f\ t$ 、 $y\ s\ g\ n$  がそれぞれ算出される。

ステップ1 :  $x\ c\ n\ t=0$ 、 $x\ s\ f\ t=1$ 、 $y\ s\ g\ n=1$

ステップ2 :  $x\ c\ n\ t=2$ 、 $x\ s\ f\ t=2$ 、 $y\ s\ g\ n=-1$

ステップ3 :  $x\ c\ n\ t=5$ 、 $x\ s\ f\ t=3$ 、 $y\ s\ g\ n=1$

ステップ4以降 :  $x\ c\ n\ t=9$ 、 $x\ s\ f\ t=0$ 、 $y\ s\ g\ n=0$

[0069] 次に別の入力値が入力された場合の例について説明する。以下では、整数  $x=72$  が入力され、整数  $p$  のビット数が8である場合の演算例を示す。72をNAF形式に変換すると、「0, 1, 0, 0, -1, 0, 0, 1, 0」と表される。

[0070] 上記の例と同様の手順により、結果として各ステップでは、以下のような  $x\ c\ n\ t$ 、 $x\ s\ f\ t$ 、 $y\ s\ g\ n$  がそれぞれ算出される。

ステップ1 :  $x\ c\ n\ t=0$ 、 $x\ s\ f\ t=1$ 、 $y\ s\ g\ n=1$

ステップ2 :  $x\ c\ n\ t=2$ 、 $x\ s\ f\ t=2$ 、 $y\ s\ g\ n=-1$

ステップ3 :  $x\ c\ n\ t=5$ 、 $x\ s\ f\ t=2$ 、 $y\ s\ g\ n=1$

ステップ4 :  $x\ c\ n\ t=8$ 、 $x\ s\ f\ t=1$ 、 $y\ s\ g\ n=0$

ステップ5以降 :  $x\ c\ n\ t=9$ 、 $x\ s\ f\ t=0$ 、 $y\ s\ g\ n=0$

[0071] この例では、ステップ4で消費するビット数が1ビットである（ $x\ s\ f\ t$  が1ビットで、上位に1が存在しないので  $y\ s\ g\ n$  の分が0ビット）。ステ

ツプ4の $x s f t$ は、整数 $p$ のビット数 $+1 - x c n t = 8 + 1 - 8 = 1$ により求めている。

[0072] 以下、さらに演算装置100により演算処理の具体例について説明する。引き続き「 $f 2 \times d 5 \bmod f b$ 」を計算する場合を例に説明する。図7は、「 $f 2 \times d 5 \bmod f b$ 」を計算する途中の各変数の値を示す図である。

[0073] 上述のように、 $z c n t$ は前のステップまでの $z s f t$ の合計である。初期設定として、 $z = 0$ 、 $x c n t = 0$ 、 $z c n t = 0$ とする。また、 $z$ は16ビットとする。入力された法（整数 $p$ ）のサイズは8ビットなので $s i z e = 8$ である。

[0074] まず、最初のステップ1でのエンコーダ201の出力を求める。上述のようにステップ1では、 $x c n t = 0$ 、 $x s f t = 1$ 、 $y s g n = 1$ 、 $z = 0000$ 、および $z c n t = 0$ が求められる。以下、上述の図4のフローチャートに従って説明する。

[0075]  $z e x t$ は、(2)式により求められる（ステップS401）。この例では、 $x c n t = 0$ 、 $s i z e = 8$ 、 $z c n t = 0$ であるため、 $z e x t = 0$ である。

[0076] 次に、 $z s f t$ が決定される（ステップS402）。 $z s f t$ は、 $z$ の下位の連続した0の個数であるが、 $z e x t$ 以下の値を取る。ここでは、 $z = 0$ であるため、下位には16ビットの0が並んでいることになる。しかし、 $z e x t (=0)$ 以下の値でなければならないため、 $z s f t = 0$ となる。

[0077] 次に、 $p s g n$ が算出される（ステップS403～ステップS407）。ここでは、 $z s f t$ と $z e x t$ とが一致するため、 $p s g n = 0$ となる（ステップS404）。

[0078] 次に、 $x s f t$ および $y s g n$ が算出される（ステップS408～ステップS411）。上述のように、 $x s f t = 1$ および $y s g n = 1$ となる。

[0079] 次に、 $y s f t$ が上記(6)式により算出される（ステップS412）。ここでは、 $y s f t = 0 + 1 - 0 - 0 = 1$ となる。



- [0080] 次に、 $x_{cnt}$  および  $z_{cnt}$  が、それぞれ上記（７）式および（８）式により算出される（ステップ S 4 1 3、ステップ S 4 1 4）。ここでは、 $x_{cnt} = x_{cnt} + x_{sft} + 1 = 0 + 1 + 1 = 2$  に更新される。また、 $z_{cnt} = z_{cnt} + z_{sft} = 0 + 0 = 0$  に更新される。
- [0081] 以上により、エンコーダ 2 0 1 の出力である  $z_{sft}$ （＝０）、 $y_{sft}$ （＝１）、 $y_{sgn}$ （＝＋１）、および  $p_{sgn}$ （＝０）が計算される。これらの出力値を上記（１）式に入力することにより、 $z$  の新しい値が算出される（図 3 のステップ S 3 0 4）。ここでは、 $z$  の新しい値として「0 1 a a」が求められる。
- [0082] 次のステップ 2 では、同様にして  $z_{sft} = 1$ 、 $y_{sft} = 3$ 、 $y_{sgn} = -1$ 、 $p_{sgn} = +1$  が求まり、 $z$  の新しい値は「f b 2 8」となる。
- [0083] ステップ 3 では、同様にして  $z_{sft} = 3$ 、 $y_{sft} = 4$ 、 $y_{sgn} = +1$ 、 $p_{sgn} = +1$  が求まり、 $z$  の新しい値は「0 d b 0」となる。
- [0084] ステップ 4 では、同様にして  $z_{sft} = 4$ 、 $y_{sft} = 1$ 、 $y_{sgn} = 0$ 、 $p_{sgn} = 0$  が求まり、 $z$  の新しい値は「0 0 d b」となる。
- [0085] なお、この例では、求められた結果である  $z = \text{「0 0 d b」}$  は、 $0 \leq z < p$  を満たす。このため、補正部 1 0 6 は  $z$  を補正しない。
- [0086] 以上のように、上記例では、８ビットのモンゴメリ乗算を４ステップで求めることができる。なお、漸近的には法である整数  $p$  のビット数の  $1/3$  ステップでモンゴメリ乗算を求めることができる。以下、本実施の形態の演算処理の漸近的なふるまいを説明する。
- [0087]  $z$  を下位からスキャン（処理）していったときに、あるビットが 0 のとき、次のビットが 0 になる確率は  $1/2$  であり、1 になる確率も  $1/2$  である。逆に、あるビットが 1 のとき、エンコーダ 2 0 1 のアルゴリズムより、次のビットは必ず 0 になる。この確率を状態遷移行列  $A$  で表すと次の（９）式のようになる。

[数 1]

$$A = \begin{pmatrix} 1/2 & 1 \\ 1/2 & 0 \end{pmatrix} \quad \cdots (9)$$

[0088]  $A^n$  ( $A$ の $n$ 乗)の $n$ の極限を調べることで、0である確率と1である確率を知ることができる。 $A^n$ の $n$ を無限大としたときの極限は、以下の(10)式で表される。

[数2]

$$A^\infty = \begin{pmatrix} 2/3 & 2/3 \\ 1/3 & 1/3 \end{pmatrix} \quad \cdots (10)$$

[0089] 上記(10)式に示すように、処理するビットが0である確率は2/3であり、処理するビットが1である確率は1/3である。エンコーダ201のアルゴリズムは、 $z$ のあるビットが1である場合にのみ処理を行う(0はスキップする)ため、平均して、 $p$ のビット数の1/3ステップで処理が完了することになる。

[0090] このように、本実施の形態にかかる演算装置100では、ZDN法と同程度のステップ数でモンゴメリ乗算を演算できる。また、ZDN法と異なり、変数の下位ビットから逐次的に演算を実行するため、任意のビット数の入力に対してモンゴメリ乗算を実行できる。

[0091] 次に、本実施の形態にかかる演算装置100のハードウェア構成について図8を用いて説明する。図8は、本実施の形態にかかる演算装置100のハードウェア構成図である。

[0092] 本実施の形態にかかる演算装置100は、CPU (Central Processing Unit) 51などの制御装置と、ROM (Read Only Memory) 52やRAM 53などの記憶装置と、ネットワークに接続して通信を行う通信I/F 54と、各部を接続するバス61を備えている。

[0093] 本実施の形態にかかる演算装置100で実行される演算プログラムは、ROM 52等に予め組み込まれて提供される。

[0094] 本実施の形態にかかる演算装置100で実行される演算プログラムは、インストール可能な形式又は実行可能な形式のファイルでCD-ROM (Compact Disk Read Only Memory)、フレキシブルディスク (FD)、CD-R (Compact Disk Recordable)、DVD (Digital Versatile Disk) 等

のコンピュータで読み取り可能な記録媒体に記録してコンピュータプログラムプロダクトとして提供されるように構成してもよい。

[0095] さらに、本実施の形態にかかる演算装置 100 で実行される演算プログラムを、インターネット等のネットワークに接続されたコンピュータ上に格納し、ネットワーク経由でダウンロードさせることにより提供するように構成してもよい。また、本実施の形態にかかる演算装置 100 で実行される演算プログラムをインターネット等のネットワーク経由で提供または配布するように構成してもよい。

[0096] 本実施の形態にかかる演算装置 100 で実行される演算プログラムは、コンピュータを上述した演算装置 100 の各部（入力部、変換部、第 1 演算部、第 2 演算部、判定部、補正部、出力部）として機能させうる。このコンピュータは、CPU 51 がコンピュータ読取可能な記憶媒体から演算プログラムを主記憶装置上に読み出して実行することができる。

[0097] なお、本発明は、上記実施の形態そのままに限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で構成要素を変形して具体化することができる。また、上記実施の形態に開示されている複数の構成要素の適宜な組み合わせにより、種々の発明を形成することができる。例えば、実施の形態に示される全構成要素からいくつかの構成要素を削除してもよい。さらに、異なる実施の形態にわたる構成要素を適宜組み合わせても良い。

## 符号の説明

[0098]    51    CPU  
          52    ROM  
          53    RAM  
          54    通信 I/F  
          61    バス  
          100   演算装置  
          101   入力部  
          102   変換部

- 1 0 3 第 1 演算部
- 1 0 3 a 第 1 シフト量算出部
- 1 0 3 b 第 2 シフト量算出部
- 1 0 4 第 2 演算部
- 1 0 4 a シフト演算部
- 1 0 4 b 加減算部
- 1 0 5 判定部
- 1 0 6 補正部
- 1 0 7 出力部
- 1 0 8 記憶部
- 2 0 1 エンコーダ
- 2 0 2 右シフト演算器
- 2 0 3 左シフト演算器
- 2 0 4 3 入力加減算器
- 2 1 1、2 1 2、2 1 3、2 1 4 レジスタ

## 請求の範囲

- [請求項1]        整数  $x$  と整数  $y$  との積の整数  $p$  を法とするモンゴメリ乗算結果  $z$  を演算する演算装置であって、
- 前記整数  $x$  を冗長 2 進表現に変換する変換部と、
- 前記モンゴメリ乗算結果  $z$  の演算の中間結果の下位ビットから上位ビットに向けて連続する 0 の個数をカウントし、カウントした個数に基づいて第 1 シフト量を算出する第 1 シフト量算出部と、
- 冗長 2 進表現の前記整数  $x$  の下位ビットから上位ビットに向けて連続する 0 の個数をカウントし、カウントした個数に基づいて第 2 シフト量を算出する第 2 シフト量算出部と、
- 前記第 1 シフト量だけビットシフトした前記中間結果と、前記第 2 シフト量だけビットシフトした前記整数  $y$  と、前記整数  $p$  と、を加減算した前記中間結果を算出し、算出した前記中間結果を前記第 1 シフト量算出部に送出する加減算部と、
- 前記第 1 シフト量の合計が前記整数  $p$  のビット数と一致したときの前記中間結果を前記モンゴメリ乗算結果  $z$  として出力する出力部と、
- を備えることを特徴とする演算装置。
- [請求項2]        前記第 1 シフト量算出部は、前記中間結果の最下位ビットから上位ビットに向けて、前記中間結果が算出されるごとに変更されるビット数のビットまでの間で連続する 0 の個数をカウントし、カウントした前記個数である前記第 1 シフト量を算出すること、
- を特徴とする請求項 1 に記載の演算装置。
- [請求項3]        前記第 2 シフト量算出部は、冗長 2 進表現の前記整数  $x$  に含まれるビットのうち、連続する 0 の個数のカウントの対象となったビットを表す処理済みビットと、前記処理済みビットの 1 つ上位の 0 でないビットとを除くビットを対象として、下位ビットから上位ビットに向けて連続する 0 の個数をカウントし、カウントした個数に基づいて前記第 2 シフト量を算出すること、

を特徴とする請求項 1 に記載の演算装置。

[請求項4]

前記加減算部は、前記第 1 シフト量だけビットシフトした前記中間結果と、前記第 2 シフト量だけビットシフトした前記整数  $y$  および冗長 2 進表現の前記整数  $x$  に含まれるビットのうち連続する 0 の個数のカウントの対象となったビットを表す処理済みビットの 1 つ上位のビットの値の積と、前記整数  $p$  と、を加減算した前記中間結果を算出し、算出した前記中間結果を前記第 1 シフト量算出部に送出すること、

を特徴とする請求項 1 に記載の演算装置。

[請求項5]

前記加減算部は、前記第 1 シフト量だけビットシフトした前記中間結果と、前記第 2 シフト量だけビットシフトした前記整数  $y$  とを加算した値に対して、前記中間結果に含まれるビットのうち、最下位ビットから前記第 1 シフト量 + 1 ビット目のビットの値が前記整数  $p$  の最下位ビットの値と一致するときは前記整数  $p$  を減算して前記中間結果を算出し、前記中間結果に含まれるビットのうち、最下位ビットから前記第 1 シフト量 + 1 ビット目のビットの値が前記整数  $p$  の最下位ビットの値と一致しないときは前記整数  $p$  を加算した前記中間結果を算出し、算出した前記中間結果を前記第 1 シフト量算出部に送出すること、

を特徴とする請求項 1 に記載の演算装置。

[請求項6]

前記冗長 2 進表現は N A F ( N o n - A d j a c e n t F o r m ) であること、

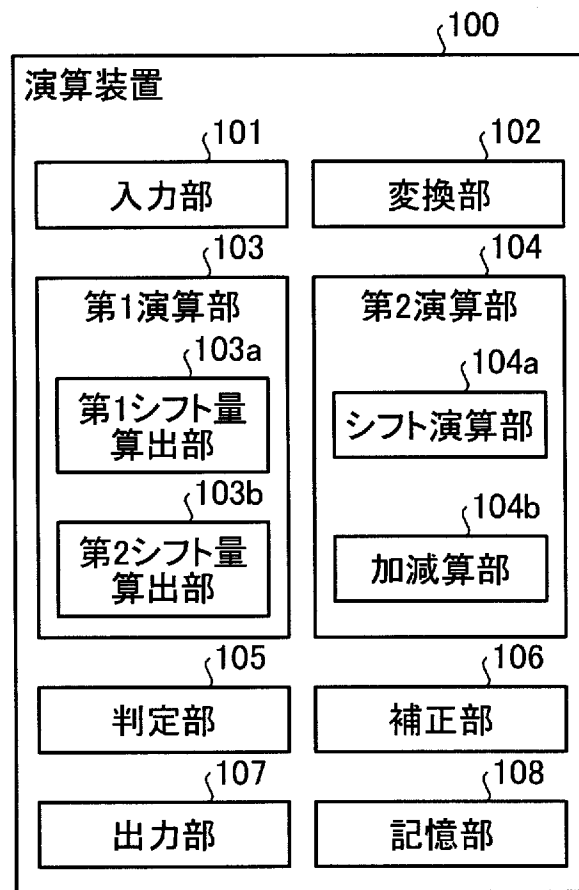
を特徴とする請求項 1 に記載の演算装置。

[請求項7]

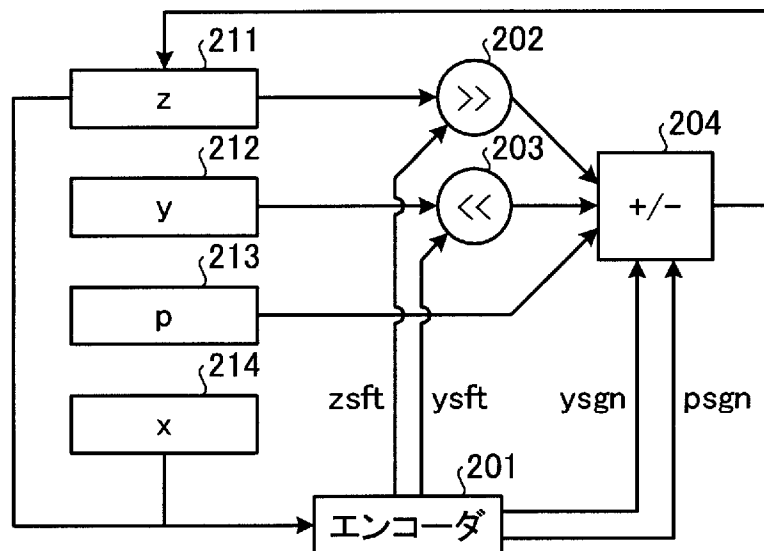
前記出力部は、前記合計が前記整数  $p$  のビット数と一致したときの前記中間結果が 0 より小さいときは、前記中間結果に前記整数  $p$  を加算した値を前記モンゴメリ乗算結果  $z$  として出力し、前記合計が前記整数  $p$  のビット数と一致したときの前記中間結果が  $p$  以上のときは、前記中間結果から前記整数  $p$  を減算した値を前記モンゴメリ乗算結果  $z$  として出力すること、

を特徴とする請求項 1 に記載の演算装置。

[図1]

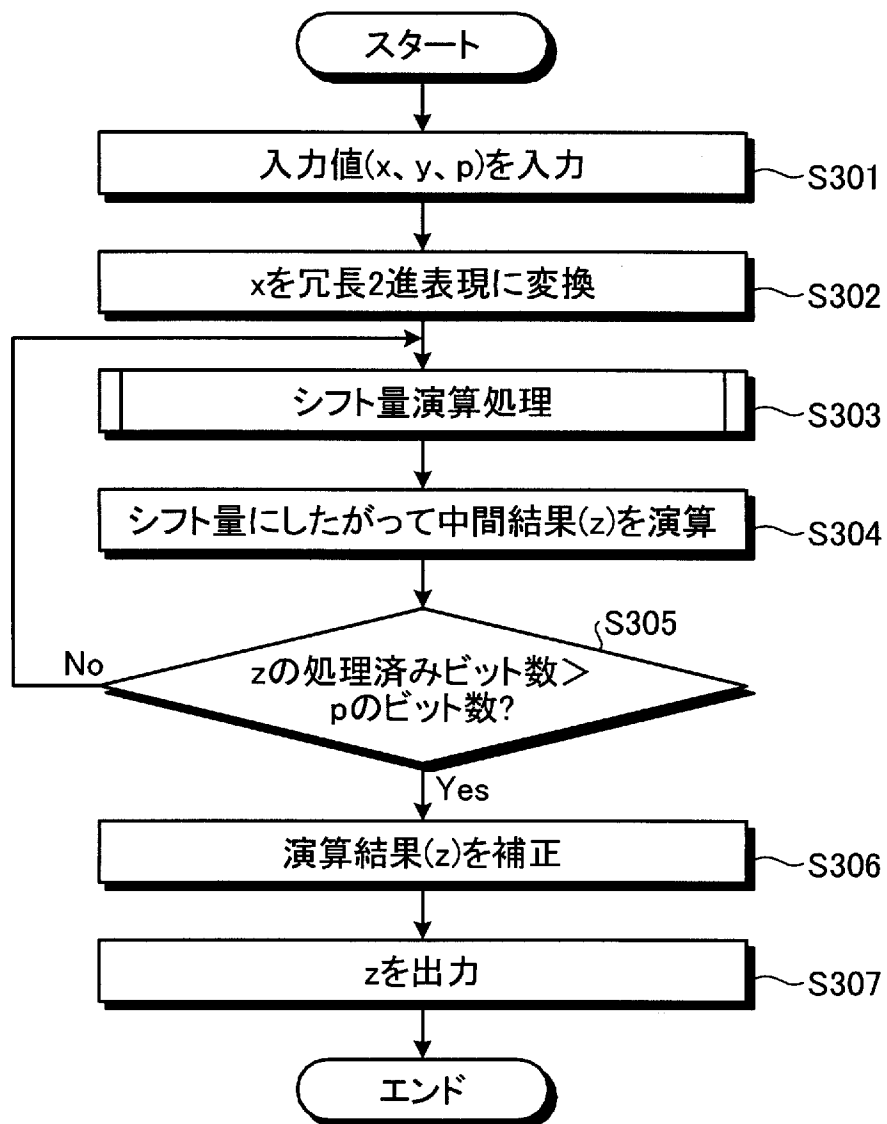


[図2]

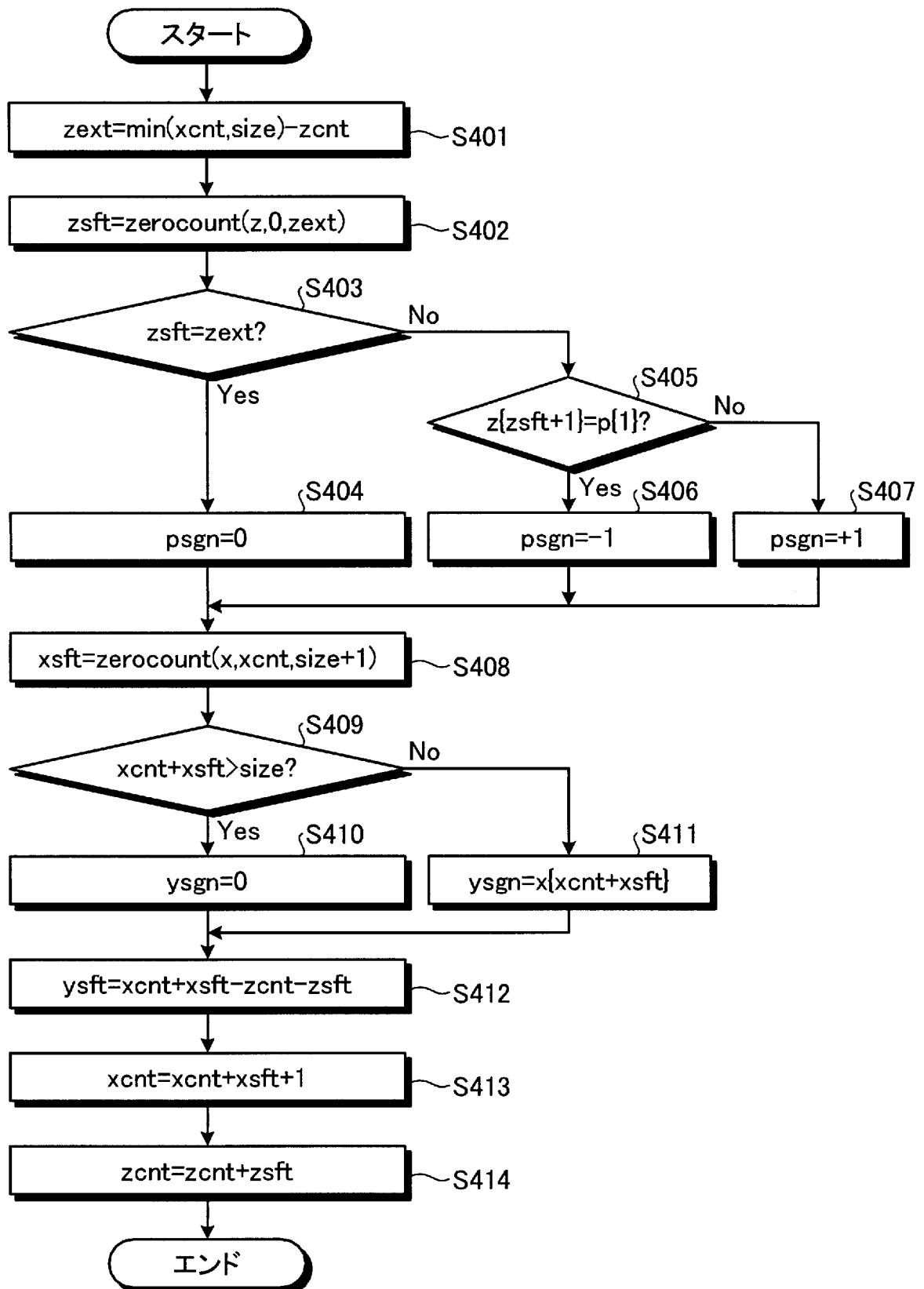




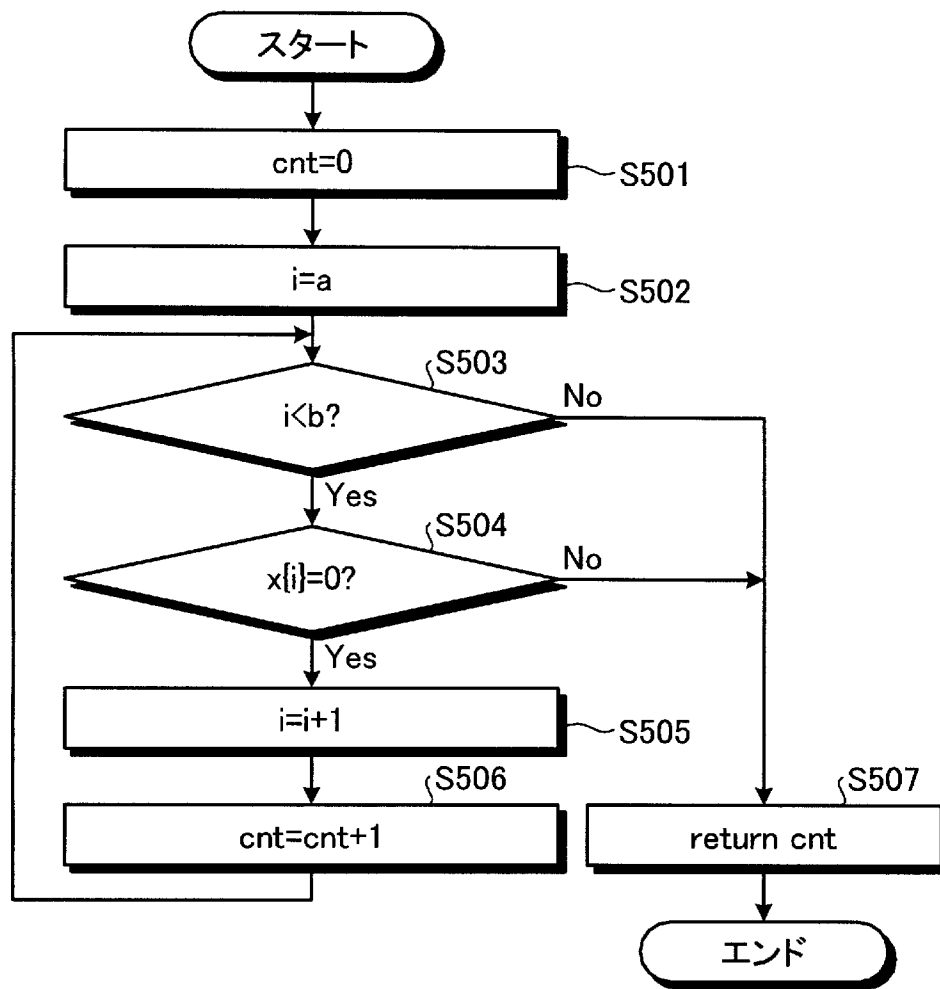
[図3]



[図4]



[図5]



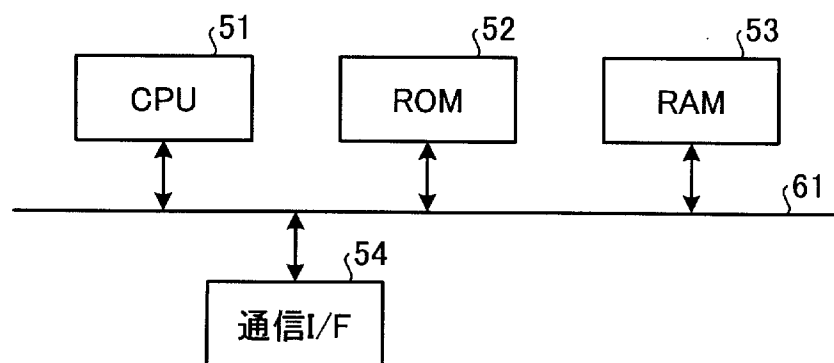
[図6]

|      |         |       |     |                            |
|------|---------|-------|-----|----------------------------|
| f2 = | 1 0 0 0 | 1 0 0 | 1 0 |                            |
|      |         |       |     | ステップ1 1個の0と1 →2ビット消費 計2ビット |
|      |         |       |     | ステップ2 2個の0と1 →3ビット消費 計5ビット |
|      |         |       |     | ステップ3 3個の0と1 →4ビット消費 計9ビット |

[図7]

| step | xcnt | xsft | ysft | ysgn | z    | zcnt | zext | zsft | psgn |
|------|------|------|------|------|------|------|------|------|------|
| 1    | 0    | 1    | 1    | +1   | 0000 | 0    | 0    | 0    | 0    |
| 2    | 2    | 2    | 3    | -1   | 01aa | 0    | 2    | 1    | +1   |
| 3    | 5    | 3    | 4    | +1   | fb28 | 1    | 4    | 3    | +1   |
| 4    | 9    | 0    | 1    | 0    | 0db0 | 4    | 4    | 4    | 0    |
| -    | 10   | -    | -    | -    | 00db | 8    |      | -    | -    |

[図8]



# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2009/066537

## A. CLASSIFICATION OF SUBJECT MATTER

G06F7/72 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F7/72, G06F7/38-7/537

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

|                           |           |                            |           |
|---------------------------|-----------|----------------------------|-----------|
| Jitsuyo Shinan Koho       | 1922-1996 | Jitsuyo Shinan Toroku Koho | 1996-2009 |
| Kokai Jitsuyo Shinan Koho | 1971-2009 | Toroku Jitsuyo Shinan Koho | 1994-2009 |

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages                                                                       | Relevant to claim No. |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| A         | JP 2005-221830 A (Sanyo Electric Co., Ltd.),<br>18 August 2005 (18.08.2005),<br>entire text; all drawings<br>(Family: none)                              | 1-7                   |
| A         | JP 8-147266 A (Nippon Telegraph And Telephone Corp.),<br>07 June 1996 (07.06.1996),<br>entire text; all drawings<br>(Family: none)                       | 1-7                   |
| A         | JP 10-307710 A (Nippon Telegraph And Telephone Corp.),<br>17 November 1998 (17.11.1998),<br>entire text; all drawings<br>& US 6175850 B1 & CA 2228493 A1 | 1-7                   |



Further documents are listed in the continuation of Box C.



See patent family annex.

\* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search  
17 November, 2009 (17.11.09)

Date of mailing of the international search report  
01 December, 2009 (01.12.09)

Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

**INTERNATIONAL SEARCH REPORT**

International application No.

PCT/JP2009/066537

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages                                | Relevant to claim No. |
|-----------|-------------------------------------------------------------------------------------------------------------------|-----------------------|
| A         | US 2001/0054052 A1 (Arazi),<br>20 December 2001 (20.12.2001),<br>entire text; all drawings<br>& WO 2001/071486 A2 | 1-7                   |

|                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                             |                                                                     |                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|---------------------------------------------------------------------|----------------|
| A. 発明の属する分野の分類（国際特許分類（I P C））<br>Int.Cl. G06F7/72(2006.01)i                                                                                                                                                                                                                                                                                                                                                                                |                                                                             |                                                                     |                |
| B. 調査を行った分野<br>調査を行った最小限資料（国際特許分類（I P C））<br>Int.Cl. G06F7/72, G06F7/38-7/537                                                                                                                                                                                                                                                                                                                                                              |                                                                             |                                                                     |                |
| 最小限資料以外の資料で調査を行った分野に含まれるもの<br>日本国実用新案公報 1 9 2 2 - 1 9 9 6 年<br>日本国公開実用新案公報 1 9 7 1 - 2 0 0 9 年<br>日本国実用新案登録公報 1 9 9 6 - 2 0 0 9 年<br>日本国登録実用新案公報 1 9 9 4 - 2 0 0 9 年                                                                                                                                                                                                                                                                       |                                                                             |                                                                     |                |
| 国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                             |                                                                     |                |
| C. 関連すると認められる文献                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                             |                                                                     |                |
| 引用文献の<br>カテゴリー*                                                                                                                                                                                                                                                                                                                                                                                                                            | 引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示                                           | 関連する<br>請求項の番号                                                      |                |
| A                                                                                                                                                                                                                                                                                                                                                                                                                                          | JP 2005-221830 A（三洋電機株式会社）2005.08.18, 全文、全図（ファミリーなし）                        | 1-7                                                                 |                |
| A                                                                                                                                                                                                                                                                                                                                                                                                                                          | JP 8-147266 A（日本電信電話株式会社）1996.06.07, 全文、全図（ファミリーなし）                         | 1-7                                                                 |                |
| A                                                                                                                                                                                                                                                                                                                                                                                                                                          | JP 10-307710 A（日本電信電話株式会社）1998.11.17, 全文、全図 & US 6175850 B1 & CA 2228493 A1 | 1-7                                                                 |                |
| A                                                                                                                                                                                                                                                                                                                                                                                                                                          | US 2001/0054052 A1（A r a z i）2001.12.20, 全文、全図 & WO 2001/071486 A2          | 1-7                                                                 |                |
| <input type="checkbox"/> C欄の続きにも文献が列挙されている。 <input type="checkbox"/> パテントファミリーに関する別紙を参照。                                                                                                                                                                                                                                                                                                                                                   |                                                                             |                                                                     |                |
| * 引用文献のカテゴリー<br>「A」特に関連のある文献ではなく、一般的技術水準を示すもの<br>「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの<br>「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）<br>「O」口頭による開示、使用、展示等に言及する文献<br>「P」国際出願日前で、かつ優先権の主張の基礎となる出願日の後に公表された文献<br>「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの<br>「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの<br>「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの<br>「&」同一パテントファミリー文献 |                                                                             |                                                                     |                |
| 国際調査を完了した日<br>1 7 . 1 1 . 2 0 0 9                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                             | 国際調査報告の発送日<br>0 1 . 1 2 . 2 0 0 9                                   |                |
| 国際調査機関の名称及びあて先<br>日本国特許庁（I S A / J P）<br>郵便番号 1 0 0 - 8 9 1 5<br>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）<br>田中 友章<br>電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 2 1 | 5 E<br>9 3 7 6 |