PROOF OF ALGORITHM 386 [A1]
GREATEST COMMON DIVISOR
OF n INTEGERS AND MULTIPLIERS *

by

Larry C. Ragland and Donald I. Good

November 1972 TR - 5

*[Gordon H. Bradley, Comm. ACM 13 (July 1970), 447]

ABSTRACT

Algorithm 386 is proved using the inductive assertion method. In the course of the proof, some errors were found and corrected. Some additional program changes are necessary for certain implementations of DØ statements.

KEY WORDS AND PHRASES: proof of algorithms, greatest common divisor, Euclidean algorithm, inductive assertion method.

CR CATEGORIES: 3.15, 4.42, 5.10, 5.24

INTRODUCTION

Subroutine GCDN, Algorithm 386 as described in [1,2], computes the greatest common divisor, IGCD, of n integers A(1),...,A(n) by using the Euclidean algorithm to compute first gcd(A(1),A(2)), then gcd(gcd(A(1),A(2)),A(3)), etc. It also computes integer multipliers Z(1),...,Z(n) such that IGCD = $\sum_{i=1}^{n}$ A(i)Z(i). A proof that a modified version of GCDN performs these two tasks is given ~~below~~ using the inductive assertion method.

PROOF PROCEDURE

The correctness of GCDN is proved by the inductive assertion method using a slight variation of one of the techniques described in [3]. Assertions concerning the progress of the computation are associated with various points in the program. The proof consists of showing that each assertion at a point is true each time control reaches that point in the program.

The inductive assertions are inserted as comments in the program below, assertion j.k being the k^{th} assertion associated with statement j. A variable name with a zero subscript denotes the initial value of that variable (its value upon initiating the execution of GCDN) and a variable name without a subscript denotes the "current" value of that variable. The current value is the value of the variable just before execution of the program statement with which the inductive assertion is associated. For example, $N = N_o \wedge A = A_o$ is the fourth of four assertions associated with statement 2. This assertion states that the current value of N equals its initial value, and similarly, the current value of A equals its initial value.

The notation $A = A_o$, where A is an array name as in 2.4, is an abbreviation for $A(i) = A_o(i)$ for all i within the dimension limits of A. Also in writing the assertions, S(I,M,A,Z,ISIGN) is an abbreviation for the assertion

$$\gcd(A_o(1),\ldots,A_o(I)) = \sum_{k=M+1}^{I} \left(\prod_{j=k+1}^{I} A(j)\right) Z(k)A_o(k) + \left(\prod_{j=M+1}^{I} A(j)\right)(-2*ISIGN+1)A_o(M)$$

and R(K,I,M,A,Z,ISIGN) is an abbreviation for

$$IGCD = \sum_{j=M+1}^{I} Z(j)A_o(j) - \sum_{j=M+1}^{K-1} Z(j)A_o(j) + \sum_{k=M+1}^{K-1}\left(\prod_{j=k+1}^{K} A(j)\right) Z(k)A_o(k)$$

$$+\left(\prod_{j=M+2}^{K} A(j)\right)(-2*ISIGN+1)A(M+1)A_o(M).$$

Inductive assertions 1.1, 61.1 and 61.2 provide the formal statement of correctness for GCDN. GCDN will be considered to be correct provided it has the following property: For every execution of GCDN initiated with 1.1 ($1 \leq N_o \leq \dim(A) = \dim(Z)$) true, and such that the execution terminates, then both 61.1 ($IGCD = \gcd[A_o(1),\ldots,A_o(N_o)]$) and 61.2 ($IGCD = \sum_{i=1}^{N_o} A_o(i)Z(i)$) are true when the execution terminates. This is proved by the inductive assertion method, and hence, GCDN is correct. This property often is called "partial correctness". The term "correctness" then, is reserved for a program that not only is partially correct but also terminates for all executions satisfying the initial assertion. No formal proof is given here that GCDN always terminates under initial assertion 1.1. However, this can be deduced from the bounds Bradley describes for the algorithm in [2]. In view of this, correctness does in fact simply amount to GCDN possessing the preceding property.

In a proof by inductive assertions, a verification condition is constructed for each control path. These verification conditions are mathematical conjectures that may be constructed in one of several forms [3,5]. The form used here is a variation of the path-forward form described in [3]. The first change is in the method of assigning alteration counters[1] to the program variable names. Let n be the name of a program variable. Instead of using n_1 to denote the value of variable n at the beginning of a path, we simply use n, and then n_1 denotes the value of n after the first time it appears on the left of an assignment, n_2 its value after the second time,.... This change in notation simply makes the verification condition more readable. The other change in the form of the verification condition is in the treatment of statements involving subscripted variables or division. In [3], it is suggested that an implicit test statement on the legality of subscripts be inserted before every statement containing a subscripted variable. Instead of this approach, we use a slightly different term in the verification condition. Consider, for example, the term due to statement 10, Z(M) = A(M) / IGCD, along the path

[1] An alteration counter is a subscript attached to each variable name that indicates how many times that variable has appeared on the left of an assignment statement along a particular control path.

(2,8,9,10,11,61). According to [3], the terms to be used in the verification condition for this statement are (under the new alteration counter convention)

$$Z_1(M) = A(M) \ / \ IGCD_1$$

$$r \neq M \supset Z_1(r) = Z(r).$$

Instead of these terms, we shall use

$$(1 \leq M \leq \dim(Z)) \wedge (1 \leq M \leq \dim(A)) \wedge (IGCD_1 \neq 0) \supset Z_1(M) = A(M) \ / \ IGCD_1$$

$$r \neq M \supset Z_1(r) = Z(r).$$

By including the precondition in the first term, one is forced to prove that M is a legal subscript for both A and Z and that the division operation is defined before the term resulting from the assignment, $Z_1(M) = A(M) / IGCD_1$, can be used in further steps in the proof.

MODIFICATIONS OF ORIGINAL ALGORITHM

Some modifications to the original version of GCDN have been made solely to facilitate the proof of correctness. First, the original comments are removed and the inductive assertions are inserted. The original statement numbers have also been removed and each line of the program has been numbered.

To make explicit the interpretation of DØ statements, all DØ loops have been rewritten as IF loops. The statements which correspond with the original DØ loops have a single leading zero in the line number. DØ statements have been assumed to consist of the following four steps. (1) Assign the control variable the value of the initial parameter. (2) Execute the body of the DØ statement. (3) If control reaches the terminal statement, execute the terminal statement and increment the control variable by the incrementation parameter. (4) If the value of the control variable is less than or equal to the value of the terminal parameter, go back to 2, otherwise the DØ is satisfied and execution continues out of the statement.

Also the **RETURN** statements have been replaced by GØ TØ statements that go to a single RETURN at statement 61.

CORRECTIONS TO THE ORIGINAL ALGORITHM

Three modifications of the program were necessitated by errors in the original algorithm. The statements in the code below which represent changes or corrections have their statement number field filled with leading zeros. Statements 9 and 10 are necessary in order to yield a positive greatest common divisor in the event that all elements of array A are zero except the last and it is negative. Statement 45 replaces the statement K = I-J+2 which is valid only if the first element of array A is non-zero. Statement 55 is necessary in the event that the greatest common divisor becomes one on the last element of array A. If $N_o < \dim(Z)$, then statement 55 may be omitted, however, this leads to the possibility of the value of the initial parameter of a DØ statement being greater than the value of the terminal parameter.

For implementations in which DØ statements are not handled as described above, some additional program modifications may be necessary. For example, according to the USA FØRTRAN standard [4], at step 1 the value of the initial parameter must be less than or equal to the value of the terminal parameter and in step 4, if the DØ is satisfied, the control variable becomes undefined. In subroutine GCDN, the only DØ loop in which the value of the initial parameter may be greater than the value of the terminal parameter is the loop in statements 44 to 50. The program will give the correct results if this loop is executed once (as in the proof) or is bypassed, however if a fatal error will result, then the statement IF(MP2.GT.I)GØ TØ 51 should be inserted between statements 43 and 44. In many implementations, the control variable remains defined at the last value used in execution of the body of the DØ when the DØ is satisfied, in which case statement 42 may be omitted (as in the original version of the algorithm). Statement 42 is necessary if the control variable becomes undefined, or if the control variable remains defined at its last value used in execution, incremented by the incrementation parameter (as in this proof).

PRESENTATION OF THE PROOF

The verification conditions for each control path are given in the tabular form described in [3]. First the path with which the verification condition is associated is given. The inductive assertion associated with the program statement at the beginning of the path is not rewritten with the verification condition since under the new alteration counter convention, the terms in the verification condition due to the assertion at the beginning of the path are identical with the assertion itself. The terms above the line in the verification condition are the terms constructed from the program statements along the control path. These terms are numbered with their respective program statement numbers. The terms below the line are the ones constructed from the inductive assertions associated with the program statement at the end of the path.

According to the inductive assertion method, if for every verification condition it can be shown that each term below the line follows from the terms above the line, including the inductive assertion at the beginning of the path and assertion 1.1, then the program is correct. For the sake of brevity, we have exhibited only those proofs which require more than a few straightforward steps. It is assumed throughout these proofs that all arithmetic operations are integer operations of arbitrarily high precision. Also we use the following properties of gcd:

P1. $\gcd(0,0) = 0$

P2. $\gcd(1,n) = 1$

P3. $\gcd(0,n) = |n|$

P4. $\gcd(a_1,\ldots,a_n) = \gcd(\gcd(a_1,\ldots,a_{n-1}),a_n)$

P5. If $am + bn = c$, then $\gcd(a,b) = \gcd(a,c)$

P6. $\gcd(m,n) = \gcd(|m|,n)$

P7. If $\gcd(m,n) = 0$, then $m = n = 0$.

P8. $\gcd(m,n) = \gcd(n,m)$

P9. $\gcd(n) = |n|$

REFERENCES

[1] Bradley, G.H. Algorithm 386, Greatest common divisor of n integers and multipliers. Comm. ACM 13, 7 (July, 1970), 447-448.

[2] Bradley, G. H. Algorithm and bound for the greatest common divisor of n integers. Comm. ACM 13, 7 (July, 1970), 433-436.

[3] Good, D. I. Toward a man-machine system for proving program correctness. Ph.D. Thesis, University of Wisconsin, June 1970.

[4] USA Standard X3.9-1966 FØRTRAN. United States of America Standards Institute, New York, 1966.

[5] King, J. C. A program verifier. Ph.D. Thesis, Carnegie-Mellon University, 1969.

```
            SUBRØUTINE  GCDN(N,A,Z,IGCD)
            DIMENSIØN   A(dim(A)),Z(dim(Z))
            INTEGER  A,Z,C1,C2,Y1,Y2,Q
C  1.1      1 ≤ N_o ≤ dim(A) = dim(Z)
        01  M = 1
C  2.1      1 ≤ M ≤ N_o
C  2.2      1 ≤ i ≤ M - 1 ⊃ A(i) = 0
C  2.3      1 ≤ i ≤ M - 1 ⊃ Z(i) = 0
C  2.4      N = N_o  ∧  A = A_o
         2  IF(A(M).NE.0) GØ TØ 8
         3  Z(M) = 0
        04  M = M + 1
        05  IF(M.LE.N) GØ TØ 2
         6  IGCD = 0
         7  GØ TØ 61
         8  IF(M.NE.N) GØ TØ 12
     00009  IGCD = IABS(A(M))
     00010  Z(M) = A(M) / IGCD
        11  GØ TØ 61
        12  MP1 = M + 1
        13  MP2 = M + 2
        14  ISIGN = 0
        15  IF(A(M).GE.0) GØ TØ 18
        16  ISIGN = 1
        17  A(M) = -A(M)
        18  C1 = A(M)
       019  I = MP1
C 20.1      1 ≤ i ≤ M - 1 ⊃ Z(i) = 0
C 20.2      N = N_o  ∧  MP1 = M + 1  ∧  MP2 = M + 2  ∧  0 ≤ ISIGN ≤ 1
C 20.3      2 ≤ M + 1 ≤ I ≤ N_o
C 20.4      C1 = A(M) = gcd(A_o(1),...,A_o(I-1)) ≠ 0
C 20.5      k ≥ I ⊃ A(k) = A_o(k)
C 20.6      S(I-1,M,A,Z,ISIGN)
```

```
        20  IF(A(I).NE.0) GØ TØ 23
        21  A(I) = 1
        22  Z(I) = 0
            GØ TØ 39
        23  Y1 = 1
        24  Y2 = 0
        25  C2 = IABS(A(I))
        26  Q = C2 / C1
        27  C2 = C2 - Q * C1
C 28.1      1 ≤ i ≤ M - 1 ⊃ Z(i) = 0
C 28.2      N = N_o ∧ MP1 = M + 1 ∧ MP2 = M + 2 ∧ 0 ≤ ISIGN ≤ 1
C 28.3      2 ≤ M + 1 ≤ I ≤ N_o
C 28.4      A(M) = gcd(A_o(1),...,A_o(I-1)) ≠ 0
C 28.5      k ≥ I ⊃ A(k) = A_o(k)
C 28.6      gcd(C1,C2) = gcd(A_o(1),...,A_o(I))
C 28.7      A_o(I) ≠ 0
C 28.8      S(I-1,M,A,Z,ISIGN)
C 28.9      A(I) divides C1 - Y1 * A(M)
C 28.10     A(I) divides C2 - (Y2 - Q * Y1) * A(M)
        28  IF(C2.EQ.0) GØ TØ 36
        29  Y2 = Y2 - Q * Y1
        30  Q = C1 / C2
        31  C1 = C1 - Q * C2
        32  IF(C1.EQ.0) GØ TØ 34
        33  Y1 = Y1 - Q * Y2
            GØ TØ 26
        34  C1 = C2
        35  Y1 = Y2
        36  Z(I) = (C1 - Y1 * A(M)) / A(I)
        37  A(I) = Y1
        38  A(M) = C1
```

```
C 39.1        1 ≤ i ≤ M - 1 ⊃ Z(i) = 0
C 39.2        N = N_o ∧ MP1 = M + 1 ∧ MP2 = M + 2 ∧ 0 ≤ ISIGN ≤ 1
C 39.3        2 ≤ M + 1 ≤ I ≤ N_o
C 39.4        C1 = A(M) = gcd(A_o(1),...,A_o(I)) ≠ 0
C 39.5        k > I ⊃ A(k) = A_o(k)
C 39.6        S(I,M,A,Z,ISIGN)
           39 IF(C1.EQ.1) GØ TØ 55
          040 I = I + 1
          041 IF(I.LE.N) GØ TØ 20
        00042 I = N
           43 IGCD = A(M)
          044 J = MP2
        00045 K = I - J + MP1
           46 KK = K + 1
           47 Z(K) = Z(K) * A(KK)
           48 A(K) = A(K) * A(KK)
C 49.1        1 ≤ i ≤ M - 1 ⊃ Z(i) = 0
C 49.2        I + 1 ≤ i ≤ N_o ⊃ Z(i) = 0
C 49.3        MP1 = M + 1 ∧ MP2 = M + 2 ∧ 0 ≤ ISIGN ≤ 1
C 49.4        2 ≤ M + 1 ≤ I ≤ N_o ∧ MP2 ≤ J
C 49.5        K = I - J + MP1
C 49.6        R(K,I,M,A,Z,ISIGN)
C 49.7        IGCD = gcd(A_o(1),...,A_o(N_o))
          049 J = J + 1
          050 IF(J.LE.I) GØ TØ 45
           51 Z(M) = A(MP1)
           52 IF(ISIGN.EQ.0) GØ TØ 54
           53 Z(M) = -Z(M)
           54 GØ TØ 61
        00055 IF(I.EQ.N) GØ TØ 43
           56 IP1 = I + 1
          057 J = IP1
           58 Z(J) = 0
```

```
C 59.1        1 ≤ i ≤ M - 1 ⊃ Z(i) = 0
C 59.2        I + 1 ≤ i ≤ J ⊃ Z(i) = 0
C 59.3        N = N_o ∧ MP1 = M + 1 ∧ MP2 = M + 2 ∧ 0 ≤ ISIGN ≤ 1
C 59.4        2 ≤ M + 1 ≤ I < J ≤ N_o
C 59.5        A(M) = gcd(A_o(1),...,A_o(I)) = gcd(A_o(1),...,A_o(N_o))
C 59.6        S(I,M,A,Z,ISIGN)
          059 J = J + 1
          060 IF(J.LE.N) GØ TØ 58
              GØ TØ 43
C 61.1        IGCD = gcd(A_o(1),...,A_o(N_o))
C 61.2        IGCD = Σ_{i=1}^{N_o} A_o(i)Z(i)
           61 RETURN
              END
```

Path (1,2).

1	$M_1 = 1$
2.1	$1 \leq M_1 \leq N_o$
2.2	$1 \leq i \leq M_1 - 1 \supset A_o(i) = 0$
2.3	$1 \leq i \leq M_1 - 1 \supset Z_o(i) = 0$
2.4	$N_o = N_o \wedge A_o = A_o$

Path (2,3,4,5,2).

2	$1 \leq M \leq \dim(A) \supset A(M) = 0$
3a	$1 \leq M \leq \dim(Z) \supset Z_1(M) = 0$
b	$r \neq M \supset Z_1(r) = Z(r)$
4	$M_1 = M + 1$
5	$M_1 \leq N$
2.1'	$1 \leq M_1 \leq N_o$
2.2'	$1 \leq i \leq M_1 - 1 \supset A(i) = 0$
2.3'	$1 \leq i \leq M_1 - 1 \supset Z_1(i) = 0$
2.4'	$N = N_o \wedge A = A_o$

Path (2,3,4,5,6,61).

2	$1 \leq M \leq \dim(A) \supset A(M) = 0$
3a	$1 \leq M \leq \dim(Z) \supset Z_1(M) = 0$
b	$r \neq M \supset Z_1(r) = Z(r)$
4	$M_1 = M + 1$
5	$M_1 > N$
6	$IGCD_1 = 0$

61.1 $IGCD_1 = \gcd(A_o(1),\ldots,A_o(N_o))$

Proof. Note that all elements of A are zero.

61.2 $IGCD_1 = \sum_{i=1}^{N_o} A_o(i)Z_1(i)$

Path (2,8,9,10,61).

2	$1 \leq M \leq \dim(A) \supset A(M) \neq 0$
8	$M = N$
9	$1 \leq M \leq \dim(A) \supset IGCD_1 = IABS(A(M))$
10a	$(1 \leq M \leq \dim(Z)) \wedge (1 \leq M \leq \dim(A)) \wedge (IGCD_1 \neq 0) \supset Z_1(M) = A(M)/IGCD_1$
b	$r \neq M \supset Z_1(r) = Z(r)$

61.1 $IGCD_1 = \gcd(A_o(1),\ldots,A_o(N_o))$

Proof. $A_o(N_o)$ is the only non-zero element.

61.2 $IGCD_1 = \sum_{i=1}^{N_o} A_o(i)Z_1(i)$

Path (2,8,12,13,14,15,16,17,18,19,20).

2 $1 \le M \le \dim(A) \supset A(M) \ne 0$

8 $M \ne N$

12 $MP1_1 = M + 1$

13 $MP2_1 = M + 2$

14 $ISIGN_1 = 0$

15 $1 \le M \le \dim(A) \supset A(M) < 0$

16 $ISIGN_2 = 1$

17a $1 \le M \le \dim(A) \supset A_1(M) = -A(M)$

b $r \ne M \supset A_1(r) = A(r)$

18 $1 \le M \le \dim(A) \supset C1_1 = A_1(M)$

19 $I_1 = MP1_1$

20.1 $1 \le i \le M-1 \supset Z(i) = 0$

20.2 $N = N_o \wedge MP1_1 = M + 1 \wedge MP2_1 = M + 2 \wedge 0 \le ISIGN_2 \le 1$

20.3 $2 \le M + 1 \le I_1 \le N_o$

20.4 $C1_1 = A_1(M) = \gcd(A_o(1),\dots,A_o(I_1-1)) \ne 0$

Proof. $C1_1 = A_1(M) \ne 0$ from 2,18.

$\gcd(A_o(1),\dots,A_o(I_1-2)) = 0$ from 2.2,12,19.

$\gcd(A_o(1),\dots,A_o(I_1-1)) = |A_o(I_1-1)| = |A_o(M)|$.

$\gcd(A_o(1),\dots,A_o(I_1-1)) = A_1(M)$ from 15,17.

20.5 $k \ge I_1 \supset A_1(k) = A_o(k)$

20.6 $S(I_1-1, M, A_1, Z, ISIGN_2)$

Proof. $\gcd(A_o(1),\dots,A_o(I_1-1)) = -A_o(M)$ from 20.4

$I_1-1 < M + 1$

$$\gcd(A_o(1),\dots,A_o(I_1-1)) = \sum_{k=M+1}^{I_1-1} \left(\prod_{j=k+1}^{I_1-1} A_1(j) \right) Z(k)A_o(k)$$

$$+ \left(\prod_{j=M+1}^{I_1-1} A_1(j) \right) (-2*ISIGN_2 + 1)A_o(M)$$

Path (2,8,12,13,14,15,18,19,20).

2 $1 \leq M \leq \dim(A) \supset A(M) \neq 0$

8 $M \neq N$

12 $MP1_1 = M + 1$

13 $MP2_1 = M + 2$

14 $ISIGN_1 = 0$

15 $1 \leq M \leq \dim(A) \supset A(M) \geq 0$

18 $1 \leq M \leq \dim(A) \supset C1_1 = A(M)$

19 $I_1 = MP1_1$

20.1 $1 \leq i \leq M - 1 \supset Z(i) = 0$

20.2 $N = N_o \wedge MP1_1 = M + 1 \wedge MP2_1 = M + 2 \wedge 0 \leq ISIGN_1 \leq 1$

20.3 $2 \leq M + 1 \leq I_1 \leq N_o$

20.4 $C1_1 = A(M) = \gcd(A_o(1),\ldots,A_o(I_1-1)) \neq 0$

Proof. See 20.4 on previous path.

20.5 $k \geq I_1 \supset A(k) = A_o(k)$

20.6 $S(I_1-1,M,A,Z,ISIGN_1)$

Proof. See 20.6 on previous path.

Path (20,21,22,39).

20 $1 \leq I \leq \dim(A) \supset A(I) = 0$

21a $1 \leq I \leq \dim(A) \supset A_1(I) = 1$

b $r \neq I \supset A_1(r) = A(r)$

22a $1 \leq I \leq \dim(Z) \supset Z_1(I) = 0$

b $r \neq I \supset Z_1(r) = Z(r)$

39.1 $1 \leq i \leq M-1 \supset Z_1(i) = 0$

39.2 $N = N_o \wedge MP1 = M + 1 \wedge MP2 = M + 2 \wedge 0 \leq ISIGN \leq 1$

39.3 $2 \leq M + 1 \leq I \leq N_o$

39.4 $C1 = A_1(M) = \gcd(A_o(1),\ldots,A_o(I)) \neq 0$

Proof. $C1 = \gcd(A_o(1),\ldots,A_o(I)) \neq 0$ from 20.4, 20.

$C1 = A_1(M) = \gcd(A_o(1),\ldots,A_o(I)) \neq 0$ from 20.4 since $A_1(M) = A(M)$ from 21b.

39.5 $k > I \supset A_1(k) = A_o(k)$

Proof. See 20.5, 21b.

39.6 $S(I,M,A_1,Z_1,ISIGN)$

Proof. $S(I-1,M,A_1,Z_1,ISIGN)$ from 20.6, 21b, 22b.

$A_o(I) = 0$ from 20.5, 20.

$$\prod_{j=k+1}^{I-1} A_1(j) = \prod_{j=k+1}^{I} A_1(j) \text{ from 21a}$$

$$\gcd(A_o(1),\ldots,A_o(I)) = \sum_{k=M+1}^{I-1}\left(\prod_{j=k+1}^{I} A_1(j)\right) Z_1(k)A_o(k) + \left(\prod_{j=M+1}^{I} A_1(j)\right)(-2*ISIGN + 1)A_o(M) \text{ from above statements}$$

$S(I,M,A_1,Z_1,ISIGN)$ since $Z_1(I) = 0$ from 22a.

Path (20,23,24,25,26,27,28).

20 $1 \leq I \leq \dim(A) \supset A(I) \neq 0$

23 $Y1_1 = 1$

24 $Y2_1 = 0$

25 $1 \leq I \leq \dim(A) \supset C2_1 = IABS(A(I))$

26 $C1 \neq 0 \supset Q_1 = C2_1 / C1$

27 $C2_2 = C2_1 - Q_1 * C1$

28.1 $1 \leq i \leq M-1 \supset Z(i) = 0$

28.2 $N = N_o \wedge MP1 = M + 1 \wedge MP2 = M + 2 \wedge 0 \leq ISIGN \leq 1$

28.3 $2 \leq M + 1 \leq I \leq N_o$

28.4 $A(M) = \gcd(A_o(1),\ldots,A_o(I-1)) \neq 0$

28.5 $k \geq I \supset A(k) = A_o(k)$

28.6 $\gcd(C1,C2_2) = \gcd(A_o(1),\ldots,A_o(I))$

Proof. $\gcd(C1,C2_2) = \gcd(C1,C2_1)$ from 27 and P5

$= \gcd(C1,A_o(I))$ from 25

$= \gcd(A_o(1),\ldots,A_o(I))$ from 20.4, P4

28.7 $A_o(I) \neq 0$

Proof. See 20.5, 20.

28.8 S(I-1,M,A,Z,ISIGN)

28.9 A(I) divides $C1 - Y1_1 * A(M)$

Proof. $C1 = A(M)$ from 20.4

$Y1_1 = 1$ from 23

A(I) divides $0 = C1 - Y1_1 * A(M)$

28.10 A(I) divides $C2_2 - (Y2_1 - Q_1 * Y1_1) * A(M)$

Proof. $C2_2 - (Y2_1 - Q_1 * Y1_1) * A(M) = C2_1 - Q_1 * C1 + Q_1 * A(M)$

from 23,24,27.

$= C2_1 = |A(I)|$ since $C1 = A(M)$

from 20.4,25.

A(I) divides $|A(I)| = C2_2 - (Y2_1 - Q_1 * Y1_1) * A(M)$

Path (28,36,37,38,39).

28 $C2 = 0$

36a $1 \le I \le \dim(Z) \wedge 1 \le M \le \dim(A) \wedge 1 \le I \le \dim(A) \wedge A(I) \ne 0 \supset Z_1(I) = (C1 - Y1 * A(M)) / A(I)$

b $r \ne I \supset Z_1(r) = Z(r)$

37a $1 \le I \le \dim(A) \supset A_1(I) = Y1$

b $r \ne I \supset A_1(r) = A(r)$

38a $1 \le M \le \dim(A) \supset A_2(M) = C1$

b $r \ne M \supset A_2(r) = A_1(r)$

39.1 $1 \le i \le M-1 \supset Z_1(i) = 0$

39.2 $N = N_o \wedge MP1 = M + 1 \wedge MP2 = M + 2 \wedge 0 \le ISIGN \le 1$

39.3 $2 \le M + 1 \le I \le N_o$

39.4 $C1 = A_2(M) = \gcd(A_o(1),\ldots,A_o(I)) \ne 0$

Proof. $\gcd(A_o(1),\ldots,A_o(I-1)) \ne 0$ from 28.4

$\gcd(A_o(1),\ldots,A_o(I)) \ne 0$ from P7

$C1 = A_2(M) = \gcd(A_o(1),\ldots,A_o(I)) \ne 0$ from 28.6, 28, 38a, P3

39.5 $k > I \supset A_2(k) = A_o(k)$

Proof. See 28.5, 37b, 38b.

39.6 $S(I,M,A_2,Z_1,ISIGN)$

Proof. (a) $S(I-1,M,A,Z,ISIGN)$ from 28.8

(b) $$A(M) = \sum_{k=M+1}^{I-1} \left(\prod_{j=k+1}^{I-1} A_2(j) \right) Z_1(k) A_o(k) + \left(\prod_{j=M+1}^{I-1} A_2(j) \right) (-2*ISIGN + 1) A_o(M)$$ from 28.4, 36b, 37b, 38b.

(c) $C1 = Z_1(I) * A(I) + Y1 * A(M)$ from 28.9, 36

(d) $C1 = Z_1(I) * A_o(I) + A_2(I) * A(M)$ from 28.5, 37a, 38b

(e) $\gcd(A_o(1),\ldots,A_o(I)) = Z_1(I) * A_o(I) + A_2(I) * A(M)$ from 28.6, 28, P3.

(f) $S(I,M,A_2,Z_1,ISIGN)$ substitute (b) into (e).

Path (28,29,30,31,32,33,26,27,28).

28 $C2 \neq 0$

29 $Y2_1 = Y2 - Q * Y1$

30 $C2 \neq 0 \supset Q_1 = C1 \; / \; C2$

31 $C1_1 = C1 - Q_1 * C2$

32 $C1_1 \neq 0$

33 $Y1_1 = Y1 - Q_1 * Y2_1$

26 $C1_1 \neq 0 \supset Q_2 = C2 \; / \; C1_1$

27 $C2_1 = C2 - Q_2 * C1_1$

28.1' $1 \leq i \leq M-1 \supset Z(i) = 0$

28.2' $N = N_o \wedge MP1 = M + 1 \wedge MP2 = M + 2 \wedge 0 \leq ISIGN \leq 1$

28.3' $2 \leq M + 1 \leq I \leq N_o$

28.4' $A(M) = gcd(A_o(1),\ldots,A_o(I-1)) \neq 0$

28.5' $k \geq I \supset A(k) = A_o(k)$

28.6' $gcd(C1_1, C2_1) = gcd(A_o(1),\ldots,A_o(I))$

Proof. See 28.6, 27,31.

28.7' $A_o(I) \neq 0$

28.8' $S(I-1,M,A,Z,ISIGN)$

28.9' $A(I)$ divides $C1_1 - Y1_1 * A(M)$

Proof. $C1_1 - Y1_1 * A(M) = (C1-Q_1*C2)-(Y1-Q_1*Y2_1)*A(M)$ from 31,33

$= (C1-Y1*A(M))-Q_1(C2-(Y2-Q*Y1)*A(M))$ from 29

$A(I)$ divides $(C1-Y1*A(M))-Q_1(C2-(Y2-Q*Y1)*A(M))$ from 28.9,28.10.

28.10' $A(I)$ divides $C2_1-(Y2_1-Q_2*Y1_1)*A(M)$

Proof. $C2_1-(Y2_1-Q_2*Y1_1)*A(M)=(C2-Q_2*C1_1)-((Y2-Q*Y1)-Q_2*Y1_1)*A(M)$

from 27,29.

$=(C2-(Y2-Q*Y1)*A(M))-Q_2(C1_1-Y1_1*A(M))$

$A(I)$ divides $(C2-(Y2-Q*Y1)*A(M))-Q_2(C1_1-Y1_1*A(M))$

from 28.10, 28.9'.

Path (28,29,30,31,32,34,35,36,37,38,39).

28	$C2 \neq 0$
29	$Y2_1 = Y2-Q * Y1$
30	$C2 \neq 0 \supset Q_1 = C1 / C2$
31	$C1_1 = C1-Q_1 * C2$
32	$C1_1 = 0$
34	$C1_2 = C2$
35	$Y1_1 = Y2_1$
36a	$1 \leq I \leq \dim(Z) \wedge 1 \leq M \leq \dim(A) \wedge 1 \leq I \leq \dim(A) \wedge A(I) \neq 0 \supset Z_1(I) = (C1_2-Y1_1 * A(M)) / A(I)$
b	$r \neq I \supset Z_1(r) = Z(r)$
37a	$1 \leq I \leq \dim(A) \supset A_1(I) = Y1_1$
b	$r \neq I \supset A_1(r) = A(r)$
38a	$1 \leq M \leq \dim(A) \supset A_2(M) = C1_2$
b	$r \neq M \supset A_2(r) = A_1(r)$

39.1 $1 \leq i \leq M-1 \supset Z_1(i) = 0$

Proof. See 36b.

39.2 $N = N_o \wedge MP1 = M + 1 \wedge MP2 = M + 2 \wedge 0 \leq ISIGN \leq 1$

39.3 $2 \leq M + 1 \leq I \leq N_o$

39.4 $C1_2 = A_2(M) = \gcd(A_o(1),\ldots,A_o(I)) \neq 0$

Proof. $\gcd(C1,C2) = \gcd(A_o(1),\ldots,A_o(I))$ from 28.6

$\gcd(C1_1,C2) = \gcd(A_o(1),\ldots,A_o(I))$ from 31, P5

$C2 = \gcd(A_o(1),\ldots,A_o(I)) \neq 0$ from 28,32

$C1_2 = A_2(M) = \gcd(A_o(1),\ldots,A_o(I)) \neq 0$ from 34,38a

39.5 $k > I \supset A_2(k) = A_o(k)$

Proof. See 28.5, 37b, 38b.

39.6 $S(I,M,A_2,Z_1,ISIGN)$

Proof. (a) S(I-1,M,A,Z,ISIGN) from 28.8

(b) $$A(M) = \sum_{k=M+1}^{I-1} \left(\prod_{j=k+1}^{I-1} A_2(j) \right) Z_1(k)A_o(k) + \left(\prod_{j=M+1}^{I-1} A_2(j) \right) (-2*ISIGN + 1)A_o(M)$$ from 28.4, 36b,37b,38b.

(c) A(I) divides C2-(Y2-Q * Y1) * A(M) from 28.10

(d) A(I) divides $C1_2$-$Y1_1$ * A(M) from 29,34,35

(e) $C1_2 = Z_1(I) * A(I) + Y1_1 * A(M)$ from 36a

(f) $C2 = Z_1(I) * A(I) + A_2(I) * A(M)$ from 34,37a,38b

(g) $gcd(C1,C2) = Z_1(I) * A(I) + A_2(I) * A(M)$ from 31,32,P3,P5

(h) $gcd(A_o(1),\ldots,A_o(I)) = Z_1(I) * A(I) + A_2(I) * A(M)$ from 28.6

(i) $S(I,M,A_2,Z_1,ISIGN)$ substitute (b) into (h).

Path (39,40,41,20).

39	$C1 \neq 1$
40	$I_1 = I + 1$
41	$I_1 \leq N$

20.1	$1 \leq i \leq M-1 \supset Z(i) = 0$
20.2	$N = N_o \wedge MP1 = M + 1 \wedge MP2 = M + 2 \wedge 0 \leq ISIGN \leq 1$
20.3	$2 \leq M + 1 \leq I_1 \leq N_o$
20.4	$C1 = A(M) = \gcd(A_o(1),\ldots,A_o(I_1-1)) \neq 0$
20.5	$k \geq I_1 \supset A(k) = A_o(k)$
20.6	$S(I_1-1,M,A,Z,ISIGN)$

Path (39,55,56,57,58,59).

39	$C1 = 1$
55	$I \neq N$
56	$IP1_1 = I + 1$
57	$J_1 = IP1_1$
58a	$1 \leq J_1 \leq \dim(Z) \supset Z_1(J_1) = 0$
b	$r \neq J_1 \supset Z_1(r) = Z(r)$

59.1	$1 \leq i \leq M-1 \supset Z_1(i) = 0$
59.2	$I + 1 \leq i \leq J_1 \supset Z_1(i) = 0$
	Proof. See 56,57,58.
59.3	$N = N_o \wedge MP1 = M + 1 \wedge MP2 = M + 2 \wedge 0 \leq ISIGN \leq 1$
59.4	$2 \leq M + 1 \leq I < J_1 \leq N_o$
59.5	$A(M) = \gcd(A_o(1),\ldots,A_o(I)) = \gcd(A_o(1),\ldots,A_o(N_o))$
	Proof. See 39.4,39,P2
59.6	$S(I,M,A,Z_1,ISIGN)$
	Proof. See 58b.

Path (39,55,43,44,45,46,47,48,49).

39 $C1 = 1$

55 $I = N$

43 $1 \leq M \leq \dim(A) \supset IGCD_1 = A(M)$

44 $J_1 = MP2$

45 $K_1 = I - J_1 + MP1$

46 $KK_1 = K_1 + 1$

47a $1 \leq K_1 \leq \dim(Z) \wedge 1 \leq KK_1 \leq \dim(A) \supset Z_1(K_1) = Z(K_1) * A(KK_1)$

b $r \neq K_1 \supset Z_1(r) = Z(r)$

48a $1 \leq K_1 \leq \dim(A) \wedge 1 \leq KK_1 \leq \dim(A) \supset A_1(K_1) = A(K_1) * A(KK_1)$

b $r \neq K_1 \supset A_1(r) = A(r)$

49.1 $1 \leq i \leq M-1 \supset Z_1(i) = 0$

Proof. See 47b.

49.2 $I + 1 \leq i \leq N_o \supset Z_1(i) = 0$

Proof. See 55.

49.3 $MP1 = M + 1 \wedge MP2 = M + 2 \wedge 0 \leq ISIGN \leq 1$

49.4 $2 \leq M + 1 \leq I \leq N_o \wedge MP2 \leq J_1$

49.5 $K_1 = I - J_1 + MP1$

49.6 $R(K_1, I, M, A_1, Z_1, ISIGN)$

Proof. (a) $K_1 = I-1$ from 44,45

(b) $KK_1 = K_1 + 1 = I$ from 46

(c) $S(I,M,A,Z,ISIGN)$ from 39.6

(d) $M + 1 \leq I$ and $M \leq K_1$ from 39.3

CASE 1: $I = M + 1$, $K_1 = M$

(e) $\gcd(A_o(1),\ldots,A_o(I)) = Z_1(M + 1)A_o(M + 1)$
$+ A_1(M + 1)(-2*ISIGN + 1)A_o(M)$ from (c), 47b,48b

(f) $R(K_1, I, M, A_1, Z_1, ISIGN)$

CASE 2: $I > M + 1$, $K_1 > M$

(g) $$A(M) = Z(I)A_o(I) + A(I)Z(I-1)A_o(I-1) + \sum_{k=M+1}^{I-2}\left(\prod_{j=k+1}^{I} A(j)\right)Z(k)A_o(k) + \left(\prod_{j=M+1}^{I} A(j)\right)(-2*ISIGN + 1)A_o(M)$$ from (c), 39.4

(h) $$IGCD_1 = Z(I)A_o(I) + A(KK_1)Z(K_1)A_o(I-1) + \sum_{k=M+1}^{K_1-1}\left(\prod_{j=k+1}^{K_1+1} A(j)\right)Z(k)A_o(k) + \left(\prod_{j=M+1}^{K_1+1} A(j)\right)(-2*ISIGN +1)A_o(M)$$ from (a), (b), 43

(i) $$IGCD_1 = Z_1(I)A_o(I) + Z_1(K_1)A_o(I-1) + \sum_{k=M+1}^{K_1-1}\left(\prod_{j=k+1}^{K_1} A_1(j)\right) Z_1(k)A_o(k) + \left(\prod_{j=M+1}^{K_1} A_1(j)\right) (-2*ISIGN + 1)A_o(M)$$ from 47, 48

(j) $$IGCD_1 = \sum_{j=M+1}^{I} Z_1(j)A_o(j) - \sum_{j=M+1}^{K_1-1} Z_1(j)A_o(j) + \sum_{k=M+1}^{K_1-1}\left(\prod_{j=k+1}^{K_1} A_1(j)\right) Z_1(k)A_o(k) + \left(\prod_{j=M+1}^{K_1} A_1(j)\right) (-2*ISIGN + 1)A_o(M)$$

(k) $R(K_1, I, M, A_1, Z_1, ISIGN)$

49.7 $IGCD_1 = \gcd(A_o(1),\ldots,A_o(N_o))$

Proof. See 39.4, 39, 43, P2.

Path (39,40,41,42,43,44,45,46,47,48,49).

39 $C1 \neq 1$

40 $I_1 = I + 1$

41 $I_1 > N$

42 $I_2 = N$

43 $1 \leq M \leq \dim(A) \supset IGCD_1 = A(M)$

44 $J_1 = MP2$

45 $K_1 = I_2 - J_1 + MP1$

46 $KK_1 = K_1 + 1$

47a $1 \leq K_1 \leq \dim(Z) \wedge 1 \leq KK_1 \leq \dim(A) \supset Z_1(K_1) = Z(K_1) * A(KK_1)$

b $r \neq K_1 \supset Z_1(r) = Z(r)$

48a $1 \leq K_1 \leq \dim(A) \wedge 1 \leq KK_1 \leq \dim(A) \supset A_1(K_1) = A(K_1) * A(KK_1)$

b $r \neq K_1 \supset A_1(r) = A(r)$

49.1 $1 \leq i \leq M-1 \supset Z_1(i) = 0$

Proof. See 47b.

49.2 $I_2 + 1 \leq i \leq N_o \supset Z_1(i) = 0$

Proof. See 42.

49.3 $MP1 = M + 1 \wedge MP2 = M + 2 \wedge 0 \leq ISIGN \leq 1$

49.4 $2 \leq M + 1 \leq I_2 \leq N_o \wedge MP2 \leq J_1$

49.5 $K_1 = I_2 - J_1 + MP1$

49.6 $R(K_1, I_2, M, A_1, Z_1, ISIGN)$

Proof. See proof of 49.6 on previous path.

49.7 $IGCD_1 = \gcd(A_o(1), \ldots, A_o(N_o))$

Proof. See 39.4, 39, 43,P2.

Path (49,50,45,46,47,48,49).

49 $J_1 = J + 1$

50 $J_1 \leq I$

45 $K_1 = I - J_1 + MP1$

46 $KK_1 = K_1 + 1$

47a $1 \leq K_1 \leq \dim(Z) \wedge 1 \leq KK_1 \leq \dim(A) \supset Z_1(K_1) = Z(K_1) * A(KK_1)$

b $r \neq K_1 \supset Z_1(r) = Z(r)$

48a $1 \leq K_1 \leq \dim(A) \wedge 1 \leq KK_1 \leq \dim(A) \supset A_1(K_1) = A(K_1) * A(KK_1)$

b $r \neq K_1 \supset A_1(r) = A(r)$

49.1' $1 \leq i \leq M-1 \supset Z_1(i) = 0$

Proof. See 47b.

49.2' $I + 1 \leq i \leq N_o \supset Z_1(i) = 0$

Proof. See 47b.

49.3' $MP1 = M + 1 \wedge MP2 = M + 2 \wedge 0 \leq ISIGN \leq 1$

49.4' $2 \leq M + 1 \leq I \leq N_o \wedge MP2 \leq J_1$

49.5' $K_1 = I - J_1 + MP1$

49.6' $R(K_1, I, M, A_1, Z_1, ISIGN)$

Proof. (a) $R(K,I,M,A,Z,ISIGN)$ from 49.6

(b) $M + 1 \leq K-1 \leq I$

(c) $$IGCD = \sum_{j=k}^{I} Z(j)A_o(j) + \sum_{j=M+1}^{K-1} \left(\prod_{k=j+1}^{K} A(k)\right) Z(j)A_o(j) + \left(\prod_{k=M+2}^{K} A(k)\right) (-2*ISIGN + 1)A_o(M)A(M + 1)$$ from (a),(b).

(d) $K_1 = K-1$ from 49.5,45,49

(e) $$IGCD = \sum_{j=K}^{I} Z_1(j)A_o(j) + A(K)Z(K-1)A_o(K-1) + \sum_{j=M+1}^{K-2} \left(\prod_{k=j+1}^{K} A(k)\right) Z(j)A_o(j) + \left(\prod_{k=M+2}^{K} A(k)\right)(-2*ISIGN + 1)A_o(M)A(M + 1)$$

from (c),(d)

(f) $$IGCD = \sum_{j=K_1+1}^{I} Z_1(j)A_o(j) + Z_1(K_1)A_o(K_1) + \sum_{j=M+1}^{K_1-1} \left(\prod_{k=j+1}^{K_1} A_1(k)\right) Z_1(j)A_o(j) + \left(\prod_{k=M+2}^{K_1} A_1(k)\right)(-2*ISIGN + 1)A_o(M)A(M + 1)$$

from (d),47,48

(g) $$IGCD = \sum_{j=M+1}^{I} Z_1(j)A_o(j) - \sum_{j=M+1}^{K_1-1} Z_1(j)A_o(j) + \sum_{j=M+1}^{K_1-1} \left(\prod_{k=j+1}^{K_1} A_1(k)\right) Z_1(j)A_o(j) + \left(\prod_{k=M+2}^{K_1} A_1(k)\right)(-2*ISIGN + 1)A_o(M)A(M + 1)$$

(h) $R(K_1,I,M,A_1,Z_1,ISIGN)$

49.7' $IGCD = gcd(A_o(1),\ldots,A_o(N_o))$

Path (49,50,51,52,53,61).

49 $J_1 = J + 1$

50 $J_1 > I$

51a $1 \leq M \leq \dim(Z) \wedge 1 \leq MP1 \leq \dim(A) \supset Z_1(M) = A(MP1)$

b $r \neq M \supset Z_1(r) = Z(r)$

52 $ISIGN \neq 0$

53a $1 \leq M \leq \dim(Z) \supset Z_2(M) = -Z_1(M)$

b $r \neq M \supset Z_2(r) = Z_1(r)$

61.1 $IGCD = \gcd(A_o(1),\ldots,A_o(N_o))$

Proof. See 49.7.

61.2 $IGCD = \sum_{i=1}^{N_o} A_o(i)Z_2(i)$

Proof. (a) R(K,I,M,A,Z,ISIGN) from 49.6

(b) $K \leq M + 1$ from 49.3,49.5,49,50

(c) $IGCD = \sum_{j=M+1}^{I} Z_2(j)A_o(j) - A_o(M)A(M+1)$ from (a),49.3, 51b,52,53b.

(d) $IGCD = \sum_{j=1}^{M-1} Z_2(j)A_o(j) - A(MP1)A_o(M) + \sum_{j=M+1}^{I} Z_2(j)A_o(j)$

$+ \sum_{j=I+1}^{N_o} Z_2(j)A_o(j)$ since first and last terms are zero, 49.1,49.2

(e) $IGCD = \sum_{j=1}^{N_o} A_o(j)Z_2(j)$ from 51a,53a.

Path (49,50,51,52,61)

49	$J_1 = J + 1$
50	$J_1 > I$
51a	$1 \leq M \leq \dim(Z) \wedge 1 \leq MP1 \leq \dim(A) \supset Z_1(M) = A(MP1)$
b	$r \neq M \supset Z_1(r) = Z(r)$
52	ISIGN = 0

61.1 $IGCD = \gcd(A_o(1),\ldots,A_o(N_o))$

Proof. See 49.7.

61.2 $IGCD = \sum_{i=1}^{N_o} A_o(i)Z_1(i)$

Proof. (a) R(K,I,M,A,Z,ISIGN) from 49.6

(b) $K \leq M + 1$ from 49.3, 49.5, 49,50

(c) $IGCD = \sum_{j=M+1}^{I} Z_1(j)A_o(j) + A(MP1)A_o(M)$

from (a),49.3,51b,52.

(d) $IGCD = \sum_{j=1}^{M-1} Z_1(j)A_o(j) + Z_1(M)A_o(M) + \sum_{j=M+1}^{I} Z_1(j)A_o(j)$

$+ \sum_{j=I+1}^{N_o} Z_1(j)A_o(j)$ since first and last

terms are zero, 49.1,49.2,51a.

(e) IGCD $\sum_{j=1}^{N_o} Z_1(j)A_o(j)$

Path (59,60,58,59).

59 $J_1 = J + 1$

60 $J_1 \leq N$

58a $1 \leq J_1 \leq \dim(Z) \supset Z_1(J_1) = 0$

b $r \neq J_1 \supset Z_1(r) = Z(r)$

59.1' $1 \leq i \leq M-1 \supset Z_1(i) = 0$

Proof. See 59.1,58b

59.2' $I + 1 \leq i \leq J_1 \supset Z_1(i) = 0$

Proof. See 59.2,58b.

59.3' $N = N_o \wedge MP1 = M + 1 \wedge MP2 = M + 2 \wedge 0 \leq ISIGN \leq 1$

59.4' $2 \leq M + 1 \leq I < J_1 \leq N_o$

Proof. See 59.4,59,60

59.5' $A(M) = \gcd(A_o(1),\ldots,A_o(I)) = \gcd(A_o(1),\ldots,A_o(N_o))$

59.6' $S(I,M,A,Z_1,ISIGN)$

Proof. See 59.6, 58b.

Path (59,60,43,44,45,46,47,48,49).

59 $J_1 = J + 1$

60 $J_1 > N$

43 $1 \leq M \leq \dim(A) \supset IGCD_1 = A(M)$

44 $J_2 = MP2$

45 $K_1 = I - J_2 + MP1$

46 $KK_1 = K_1 + 1$

47a $1 \leq K_1 \leq \dim(Z) \wedge 1 \leq KK_1 \leq \dim(A) \supset Z_1(K_1) = Z(K_1) * A(KK_1)$

b $r \neq K_1 \supset Z_1(r) = Z(r)$

48a $1 \leq K_1 \leq \dim(A) \wedge 1 \leq KK_1 \leq \dim(A) \supset A_1(K_1) = A(K_1) * A(KK_1)$

b $r \neq K_1 \supset A_1(r) = A(r)$

49.1 $1 \leq i \leq M-1 \supset Z_1(i) = 0$

Proof. See 59.1,47b.

49.2 $I + 1 \leq i \leq N_o \supset Z_1(i) = 0$

Proof. See 59.2,47b

49.3 $MP1 = M + 1 \wedge MP2 = M + 2 \wedge 0 \leq ISIGN \leq 1$

49.4 $2 \leq M + 1 \leq I \leq N_o \wedge MP2 \leq J_2$

49.5 $K_1 = I - J_2 + MP1$

49.6 $R(K_1, I, M, A_1, Z_1, ISIGN)$

Proof. See 49.6 on Path (39,55,43,44,45,46,47,48,49).

49.7 $IGCD_1 = \gcd(A_o(1), \ldots, A_o(N_o))$

Proof. See 59.5,43