Title (en)

CIRCUITS FOR MODULAR ARITHMETIC BASED ON THE COMPLEMENTATION OF CONTINUED FRACTIONS

Title (de)

SCHALTUNGEN FÜR DIE MODULARE ARITHMETIK BASIEREND AUF DER ERGÄNZUNG VON KETTENBRÜCHEN

Title (fr)

CIRCUITS D'ARITHMÉTIQUE MODULAIRE BASÉS SUR LA FERMETURE DE RUPTURES DE CHAÎNE

Publication

EP 2062131 A1 20090527 (DE)

Application

EP 07764859 A 20070626

Priority

- EP 2007005635 W 20070626
- DE 102006042513 A 20060907

Abstract (en)

[origin: WO2008028529A1] Method for carrying out modular multiplication RN[ab] of integer numbers for a modulus N and modular multiplication RN(X)[a(x)b(x)] of polynomials for a modulus polynomial N = N(x), where the integer numbers a < N, b < N, and N are presented for a radix p, whereas the polynomials a = a(x) with degrees(a(x)) < degrees(N(x)), b = b(x) with degrees(b(x)) < degrees(N(x)) and N(x) are presented for powers of the free variable x and with coefficients of an integer remainder class ring ZM, comprising the following steps: - calculating a complemented product continued fraction c = (ab+jN)/t by means of complementation of individual numerators for a product fraction (ab)/t represented as a continued fraction, where, in the first case of the calculation with integer numbers, c and j are likewise integer numbers and t = p?, whereas, in the second case of the calculation with polynominals, c = c(x) and j = j(x) are likewise polynomials with coefficients of ZM and t = t(x) =x?, and where in both cases K is an integer number greater than or equal to the length ?p(a) of the operand a broken down in the continued fraction - calculating a second complemented product continued fraction r = (cd+kN)/t from the previously calculated modular remainder d = RN[t2] and the result c from the calculation performed in the aforementioned step, where in the first case r, k and d are integer numbers and in the second case r = r(x) = RN(x) [a(x)b(x)], k = k(x) and d = d(x) are polynomials with coefficients of ZM.

IPC 8 full level

G06F 7/72 (2006.01)

CPC (source: EP US)

G06F 7/724 (2013.01 - EP US); **G06F 7/728** (2013.01 - EP US)

Citation (search report)

See references of WO 2008028529A1

Cited by

CN109669670A

Designated contracting state (EPC)

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC MT NL PL PT RO SE SI SK TR

Designated extension state (EPC)

AL BA HR MK RS

DOCDB simple family (publication)

WO 2008028529 A1 20080313; EP 2062131 A1 20090527; US 2012057695 A1 20120308

DOCDB simple family (application)

EP 2007005635 W 20070626; EP 07764859 A 20070626; US 44034007 A 20070626