An Improved Las Vegas Primality Test *

Erich Kaltofen and *Thomas Valente*
Department of Computer Science, Rensselaer Polytechnic Institute
Troy, New York 12180

Noriko Yui
Department of Mathematics, Queen's University
Kingston,Ontario,Canada K7L3N6

April 25, 1989

ABSTRACT: We present a modification of the Goldwasser-Kilian-Atkin primality test, which, when given an input n, outputs either *prime* or *composite,* along with a certificate of correctness which may be verified in polynomial time. Atkin's method computes the order of an elliptic curve whose endomorphism ring is isomorphic to the ring of integers of a given imaginary quadratic field $Q(\sqrt{-D})$. Once an appropriate order is found, the parameters of the curve are computed as a function of a root modulo n of the Hilbert class equation for the Hilbert class field of $Q(\sqrt{-D})$. The modification we propose determines instead a root of the Watson class equation for $Q(\sqrt{-D})$ and applies a transformation to get a root of the corresponding Hilbert equation. This is a substantial improvement, in that the Watson equations have much smaller coefficients than do the Hilbert equations.

1 Introduction

The Goldwasser-Kilian (1986) primality test, as modified by Atkin, allows one to efficiently certify a large integer on a computer to be a prime number. Atkin's modification abandons the rigorous polynomial-time running time property of the algorithm in order to make the production of the elliptic curve based certificate practical (see also Morain (1988)). In this paper, we further improve on this modification by using Watson's (1935) defining equations for the Hilbert class fields that Atkin selects.

Elliptic curves gained prominence in computational number theory with the integer factorization paper by Lenstra (1986) and the Goldwasser-Kilian (1986) primality test. The latter used elliptic curves to construct a certificate of correctness for the assertion that the given input was prime. In this test, curves are generated at random and their points counted until a curve with a desired order is found. The point counting (Schoof 1984) is an expensive operation, however. The Atkin test (cf. A.Lenstra and H.Lenstra 1987) avoids this problem by computing first the order of curve, then the curve itself, from the complex multiplication field $Q(\sqrt{-D})$ associated with the curve. The curve's parameters are then obtained from a root of the Hilbert class equation for the Hilbert class field of $Q(\sqrt{-D})$. The Hilbert equation, however, has coefficients which are extremely large, though the constant term and the discriminant are highly divisible numbers.

The modification we propose uses Watson equations instead of Hilbert equations. The Watson class equations have coefficients which are very small compared to those of their Hilbert counterparts. Indeed, the roots of the Watson equations are, in certain cases, units.

We begin in section 2 by presenting some background material on elliptic curves. In section 3 we describe the Goldwasser-Kilian algorithm and present a theorem on which the correctness of this algorithm and the modifications based on it depend. The modification due to Atkin is presented in section 4, along with the necessary background on quadratic forms and quadratic fields. Finally, section 5 introduces the Watson equation and demonstrates how a root of it can be transformed to a root of the Hilbert equation. A sample output of a test run with this new modification is provided as an appendix.

*This material is based on work supported by the National Science Foundation under Grant Nos. CCR-87-05363 and CDA-8805910 (first and second author); and by the National Science and Engineering Research Council (Canada) under Grant No. A8566 (third author); appears in the Proceedings of the International Symposium of Symbolic and Algebraic Computing, ACM Press, July 1989, pp.26-33.

2 Elliptic Curves

We present some material on elliptic curves. Further details may be found in Lenstra (1985).

Let F be a field of characteristic $\neq 2, 3$, and let $a, b \in F$ satisfy $4a^3 + 27b^2 \neq 0_F$.

Definition 2.1: The *elliptic curve* $E_F(a, b)$ is the set of points given by $\{(x, y) \in F \times F | \; y^2 = x^3 + ax + b\} \cup \{I_\infty\}$. The point I_∞ is said to be the *point at infinity* of the curve. The quantities $\Delta = -16(4a^3 + 27b^2)$ and $j = \frac{1728(4a)^3}{\Delta}$ are respectively the *discriminant* and the *j-invariant* of $E_F(a, b)$.

Theorem 2.2: The set $E_F(a, b)$ is an additive abelian group with identity I_∞ and addition defined as follows:
(i): $(x, y) + (x, -y) = I_\infty$
(ii): if $y \neq 0$ then

$$(x, y) + (x, y) = (\lambda^2, \lambda^3 - y + \lambda x),$$

where $\lambda = \frac{3x^2+a}{2y}$
(iii): if $x_1 \neq x_2$ then

$$(x_1, y_1) + (x_2, y_2) = (x_3, -\lambda x_3 - y_1 + \lambda x_1),$$

where $x_3 = \lambda^2 - x_1 - x_2$ and $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$

We note that the addition of Theorem 2.2 may be a partial function if we allow elliptic curves to be defined over arbitrary rings. Indeed, the quotients used to define λ must exist in the ring if the addition function is to be total.

Our interest is in elliptic curves over $GF(p), p$ prime. The following result, due to Hasse, allows us to confine our search for the order of an elliptic curve over $GF(p)$ to a small interval centered at $p + 1$. To simplify notation, we let E denote $E_{GF(p)}(a, b)$ and $|E|$ the order of the group $(E, +)$.

Theorem 2.3: $|E| = p + 1 - t$, where $|t| \leq 2\sqrt{p}$.

Finally, we define the notion of elliptic curve isomorphism. (cf. Silverman (1986) or Husemöller (1987)).

Definition 2.4: Two elliptic curves $E = E_F(a, b)$ and $\bar{E} = E_F(\bar{a}, \bar{b})$ are *isomorphic* if there is a change of variables $x = u^2\bar{x}, y = u^3\bar{y}, \; u \in F - \{0\}$ such that $(x, y) \in E \iff (\bar{x}, \bar{y}) \in \bar{E}$.

Note that the isomorphic curves of Definition 2.4 must have $a = u^4\bar{a}, b = u^6\bar{b}$, and $\jmath = \bar{\jmath}$. Thus the quantity j is invariant under isomorphism . Conversely, two elliptic curves with the same j value are isomorphic over the algebraic closure $\bar{F}$ of F. Thus, once we know a curve's j-invariant, we have determined the $\bar{F}$-isomorphism class of the curve.

3 The Goldwasser-Kilian Algorithm

The probabilistic primality test due to Goldwasser and Kilian (1986) was the first of its kind to use elliptic curves and to produce a certificate of correctness for its assertion of primality. This recursive algorithm, which we sketch in Figure 1, serves as a model for the Atkin test and its modification, which we describe in sections 4 and 5.

We remark that B may be any reasonable bound below which it makes sense to use trial division (e.g. 10^6). Also, qP denotes a repeated addition

$$\underbrace{P + P + \ldots + P}_{q \text{ times}},$$

which may fail (see the remarks following Theorem 2.2). If failure does occur, we terminate with a non-trivial divisor of p as a certificate of p's compositeness. Finally, we note that the above algorithm employs Schoof's (1984) $O(log^8(p))$ algorithm for computing the order of $E_R(a, b)$, given a and b.

The correctness of the Goldwasser-Kilian algorithm hinges on the following result, which is the basis for the recursive call above.

Theorem 3.1: Let $(n, 6) = 1$, $R = Z/nZ$, $a, b \in R$ satisfy $(n, 4a^3 + 27b^2) = 1$. Suppose there exists $P \in E_R(a, b) - I_\infty$ such that $qP = I_\infty$ for some prime $q > (n^{1/4} + 1)^2$. Then n is prime.

Thus GK(p) computes a sequence $p = p_1, p_2, \ldots, p_t$ such that

$$p_t \text{ prime} \Rightarrow \ldots \Rightarrow p_1 \text{ prime}.$$

4 Atkin's Modification

Whereas the Goldwasser-Kilian algorithm generates elliptic curves randomly and counts their points, the Atkin test uses the notion of a "complex multiplication field" to compute an elliptic curve's order, and from this, the curve itself. Thus, Atkin avoids the expense of Schoof's technique.

```
Algorithm GK(p)
Input: p, a highly-probable prime.
Output: Either prime or composite along with a certificate of correctness
for the assertion.
begin
   If p < B then
            perform trial divisions to determine whether p is prime
            and return list of trial-divisors
   else
            repeat
               let a, b be randomly chosen elements of R = Z/pZ;
               let q = |E_R(a, b)|/2
            until probable-prime(q);
            repeat
               randomly generate P ∈ E_R(a, b)
            until qP = I_∞;
            return( (P, q, a, b) appended to GK(q) )
end;
```

Figure 1: The Goldwasser-Kilian Algorithm

We now outline the theory underlying Atkin's method. Further details may be found in Lenstra and Lenstra (1987). Throughout this section, F denotes $GF(p)$, p prime, and $E = E_F(a, b)$.

Theorem 4.1: The ring $End_F(E)$, consisting of endomorphisms of E which fix F elementwise, is isomorphic to the ring of integers O_{-D} of a quadratic field $Q(\sqrt{-D})$. This quadratic field is said to be the *complex multiplication field* of E. Specifically, the complex multiplication field of an elliptic curve E over $GF(p)$ with order $p + 1 - t$ is $Q(\sqrt{t^2 - 4p})$.

For more general results regarding endomorphism rings of elliptic curves over arbitrary fields, the reader is referred to Silverman (1984), chapter III, section 9.

Theorem 4.2: Under the isomorphism of Theorem 4.1, the endomorphism $x \mapsto x^p$ is identified with $\pi \in O_{-D}$ satisfying $N_D(\pi) = \pi\bar{\pi} = p$. (Here, N_D is the norm function on $Q(\sqrt{-D})$ and $\bar{\pi}$ is the conjugate of π). From this, it follows that $|E| = p + 1 - (\pi + \bar{\pi}) = p + 1 - t$, where $t \in Z$ and, by Theorem 2.3, $|t| \leq 2\sqrt{p}$.

We call $-D$ a *fundamental discriminant* if $D \equiv 3 \pmod 4$ or $D \equiv 4 \pmod{16}$ or $D \equiv 8 \pmod{16}$, and D is squarefree in its odd prime divisors. We note that if $D \geq 4$, there are two factorizations of p of the type described in Theorem 4.2, corresponding to $\pm\pi$. In general, the number of such factorizations is equal to the number of units of O_{-D}.

The Atkin test finds a fundamental discriminant satisfying $(\frac{-D}{p}) = 1$,a necessary condition for a split of p to occur. If p can be split, the order of E is computed using Theorem 4.2. But, how does the Atkin test attempt to split the integer p? The answer is found in the theory of quadratic forms, which we now summarize.

Definition 4.2: A *binary quadratic form* $Q = [a, b, c]$ is a polynomial $Q(x, y) = ax^2 + bxy + cy^2 \in Z[x, y]$. Its *discriminant* is $b^2 - 4ac$. The form is *primitive* if $(a, b, c) = 1$ and *reduced* if $|b| \leq a \leq c$ and $b \geq 0$ whenever $c = a$ or $|b| = a$. The *matrix corresponding to* Q is

$$M_Q = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}.$$

Definition 4.3: Two forms Q and Q' are *equivalent* if there exists a matrix A with determinant 1 such that $M_{Q'} = A^T M_Q A$.

Theorem 4.4: Equivalent forms have the same discriminant and represent the same set of integers. Every equivalence class of primitive quadratic forms contains exactly one reduced form.

Theorem 4.5: The equivalence classes of primitive reduced quadratic forms of discriminant $-D$ are in one-to-one correspondence with the equivalence classes of ideals of O_{-D}, where the latter equivalence is defined by

$$I \sim J \iff \exists \alpha, \beta \in O_{-D} \; s.t. \; (\alpha)I = (\beta)J.$$

It follows from Theorem 4.5 and the definition of "class number" that there are $h(-D)$ reduced forms of discriminant $-D$, where $h(-D)$ is the class number of $Q(\sqrt{-D})$.

Atkin applies the preceding theory in the following way: In the case $-D \equiv 1 \pmod 4), D \geq 7$, we have $O_{-D} = \{a + b\omega | a, b \in Z\}$, with $\omega = \frac{1+\sqrt{-D}}{2}$. We search for π by attempting to find a short vector in the lattice $L = pZ + Z(\frac{b+\sqrt{-D}}{2})$, where $b^2 \equiv -D(mod\ p)$. Note that $\nu_{x,y} = px + (\frac{b+\sqrt{-D}}{2})y \in L$ satisfies $p = N_D(\nu_{x,y}) = p^2x^2 + bpxy + y^2(\frac{b^2+D}{4})$ if and only if $[p, b, \frac{b^2+D}{4p}] \sim [1, 1, \frac{1-D}{4}]$ since the form $x^2 + xy + \frac{1-D}{4}y^2$ represents 1 when $x = 1$ and $y = 0$. Thus, if $[p, b, \frac{b^2+D}{4p}]$ reduces to $[1, 1, \frac{1-D}{4}]$, we set π to $\nu_{x,y}$, where $(x, y)^T = S(1, 0)^T$, S is the matrix of transformation from $[p, b, \frac{b^2+D}{4p}]$ to $[1, 1, \frac{1-D}{4}]$.

At this point, we have $p = \nu\overline{\nu}$, where $\nu = \pm\pi$, and one must check $m_+ = p + 1 + (\pi + \overline{\pi})$ and $m_- = p + 1 - (\pi + \overline{\pi})$ to determine if either factors as kq with $k > 1$ and q a large prime. Once such a ν is found, the j-invariant of the elliptic curve E and the parameters a and b of E are determined as a function of a root modulo p of the Hilbert class equation

$$H_{-D}(x) = \prod_{i=1}^{h(-D)} (x - j(\tau_i))$$

where $\tau_i = \frac{b_i+\sqrt{-D}}{2a_i}$ and the $[a_i, b_i, c_i](i = 1, \ldots, h(-D))$ are the reduced forms of discriminant $-D$. The modular function $j(z)$ is given by

$$j(z) = \frac{(1 + 240 \sum_{k=1}^{\infty} \frac{k^3q^k}{1-q^k})^3}{q \prod_{k=1}^{\infty} (1 - q^k)^{24}}, \; q = e^{2\pi iz}$$

Approximations to the values of $j(z)$ can be computed via a power series approximation (cf. Kaltofen and Yui (1984)). If $r \in GF(p)$ is a root of H_{-D}, the curve we are interested in is either $E_{GF(p)}(3l, 2l)$ or $E_{GF(p)}(3lc^2, 2lc^3)$, where $l \equiv r(1728 - r)^{-1} \pmod p$ and c is a randomly chosen quadratic non-residue modulo p. The correct curve for our purposes is the one which has order kq. We remark also that k is well-defined and non-zero since we are assuming $D \geq 7$. Computation of $H_{-D}(x)$ is costly and its coefficients are very large. In the next section, we provide an alternative to the use of $H_{-D}(x)$ in our construction of elliptic curves. The Atkin test is summarized in Figure 2.

5 A New Approach

Let $H_{-D}(x), h(-D)$, and $j(z)$ be as in section 4, and put $h = h(-D)$. Recall that the Atkin modification computed the elliptic curve j-invariant as a root of $H_{-D}(x)$. In this section, we propose a technique by which we instead factor a "reduced" class equation $w_{-D}(x)$, known as the *Watson class equation* for the Hilbert class field of $Q(\sqrt{-D})$. Again, the Watson equations have dramatically smaller coefficients than their Hilbert counterparts. The idea is to somehow transform a root of w_{-D} to a root of H_{-D}, which is what we require. We illustrate how to do this in the case $-D \equiv 1 \pmod 8$ with a theorem due to Watson (1935).

Theorem 5.1: Let $\overline{H}_{-D}(x) = x^h H_{-D}\Big(\frac{(x-16)^3}{x}\Big)$. Then $\overline{H}_{-D}(x)$ has an irreducible (over Q) monic factor $\overline{h}_{-D}(x) = \prod_{k=1}^{h}(x - \alpha_k) \in C[x]$. Moreover, for a suitable choice of 24th root of α_k $(k = 1, \ldots, h)$,

$$w_{-D}(x) = x^h \prod_{k=1}^{h} (\frac{1}{x} - \sqrt[24]{\alpha_k}).$$

We note that w_{-D} may be computed from an approximation of a single real root via a technique which involves lattice reduction (cf. Kaltofen and Yui 1989).

We make use of Theorem 5.1 as follows:

Let $\gamma \neq 0$ be a root of w_{-D}. Then $(\frac{1}{\gamma})^{24} = \alpha_k$ for some k. From Theorem 5.1, $x - \alpha_k$ divides $\overline{H}_{-D}(x)$, i.e. α_k is a root of $\overline{H}_{-D}(x)$. Now, letting $\beta_1, \ldots, \beta_h$ denote the roots of the Hilbert equation $H_{-D}(x)$, we have $\overline{H}_{-D}(x) = x^h \prod_{i=1}^{h}\Big(\frac{(x-16)^3}{x} - \beta_i\Big) = \prod_{i=1}^{h}((x - 16)^3 - x\beta_i)$. Thus, for some i, α_k satisfies

$$(\alpha_k - 16)^3 - \alpha_k\beta_i = 0.$$

This yields a Hilbert root as a function of the Watson root:

$$\beta_i = \frac{(\alpha_k - 16)^3}{\alpha_k}.$$

Naturally, in our modified Atkin test, these transformations are performed modulo the number to be proven prime. A sample output, using this new technique, appears as an appendix.

Procedure Atkin(p)
Input: p, a highly-probable prime.
Output: Either *prime* or *composite* along with a certificate of correctness for this assertion.

begin

  If $p < B$ **then**

    perform trial divisions to determine whether p is prime
    and return a list of trial-divisors

  else

    repeat

      repeat

        find a fundamental discriminant $-D \leq -7$ satisfying$(\frac{-D}{p}) = 1$;
        set b to $\sqrt{-D} \pmod{p}$;
        adjust b so that its parity is equal to that of $-D$
        reducedform := Reduce$[p, b, \frac{b^2+D}{4p}]$

      until reducedform $= [1, 1, \frac{1-D}{4}]$;

      $(x\ y)^T := \mathrm{S}(1\ 0)^T$, where S is the transformation matrix
        from $[p, b, \frac{b^2+D}{4p}]$ to $[1, 1, \frac{1-D}{4}]$;
      {remark: now $\pi = x + y(\frac{1+\sqrt{-D}}{2})$}
      $t := 2px + by$; $m_+ := p + 1 + t$; $m_- := p + 1 - t$

    until m_+ or $m_- = kq$, $q > (p^{\frac{1}{4}} + 1)^2$, and probable-prime($q$);

    $r :=$ root mod p of $H_{-D}(x)$; $l := r(1728 - r)^{-1} \pmod{p}$;
    $(a, b) := (3l, 2l) \pmod{p}$; $E := E_F(a, b)$;

    If $(kq)P \neq I_\infty$ **then**
      $c :=$ randomly chosen quadratic non-residue mod p;
      $(a, b) := (ac^2, bc^3)$; $E := E_F(a, b)$
    EndIf ;

    Randomly generate $P \in E$ until $kP \neq I_\infty$ and $(kq)P = I_\infty$;
    Append (P, k, q, a, b) to Atkin(q)

end;

Figure 2: The Atkin Test

6 References

S.Goldwasser and J.Kilian, "Almost all primes can be quickly certified", Proc. 18th STOC, Berkeley, 1986, pp.316-329

D.Husemöller, *Elliptic Curves* , Springer GTM 111, 1987

E.Kaltofen and N.Yui, "Explicit construction of the Hilbert class fields of imaginary quadratic fields with class numbers 7 and 11", EUROSAM'84, *Lecture Notes in Computer Science* 174 (1984), pp.310-320, Springer-Verlag

E.Kaltofen and N.Yui, "Explicit construction of the Hilbert class fields of imaginary quadratic fields by integer lattice reduction", New York Number Theory, *Lec. Notes Math.,*Springer Verlag, to appear, 1989

A.K.Lenstra and H.W.Lenstra Jr., "Algorithms in Number Theory", in *Handbook of Theoretical Science,* North Holland, Amsterdam 1987

H.W.Lenstra Jr., "Factoring integers with elliptic curves", Annals of Math, 126, 1987, pp.649-673

F.Morain, "Implementation of the Goldwasser-Kilian-Atkin Primality Testing Algorithm", (Draft), University of Limoges, 1988

J.H.Silverman, *The Arithmetic of Elliptic Curves,* Springer GTM 106, 1986

G.N.Watson, "Singular Moduli (4)", Acta Arithmetica 1 (1935), pp.284-323

APPENDIX: A Primality Certificate for a 209 Digit Number

We present a portion of a certificate for a 209 digit number. The certificate was obtained from our Lisp implementation of the modified Goldwasser-Kilian-Atkin test on a Symbolics 3670 computer.

At each level, we exhibit the number N to be proven prime, the parameters A and B of an elliptic curve $E = E_{GF(N)}(A, B)$, a decomposition $|E| = KQ$, with $Q > (N^{\frac{1}{4}} + 1)^2$ a probable prime, and $P \in E$ a point satisfying $(KQ)P = I$ and $KP \neq I$. Theorem 3.1 assures us that N is prime provided Q is prime. At the next level, we therefore proceed with N replaced by the Q of this level.

In addition to this, we include at each level information regarding how the curve was constructed. We show the discriminant `DISC` and either the Watson (`WATSEQN`) or Hilbert (`HILBEQN`) class equation for the field $Q(\sqrt{\texttt{DISC}})$. Note that whenever $\texttt{DISC} \equiv 1 \pmod 8$, we can employ the theory of section 5 to transform the root `W-ROOT` of the Watson equation to the desired root `H-ROOT` of the Hilbert equation. The results of these transformations are also depicted in such cases.

```
(N= 44849522402294576388062847465075375801818813514437743394932401135594/
 70701107169469859688779135585699141886647146117855269161083338750352040/
 5324743895419257626810889993197886070602123649861148338395777376394079
 DISC= -1528)
(HILBEQN= (1 -215268892142320585480835263642311079363564257459264000
 998784775249544021655512244994326693088930344827693660386718303730239915/
52000000
 130243728283299475446073413827510639336517994515982186679121131367955079/
20896000000000
 440965705781341613340051370543735443449794646350475924862081008378403105/
30048000000000000
-162745667020938810121011563088932982210195336187506214454855144644001744/
99758080000000000000
 253491423236741884924851766355082859460724386592025708388888189188727434/
955980800000000000000000
-133043485505562670948914734781089766016360603667515974615534226800332653/
1469312000000000000000000000
 354575195374461844246948169302330676593475440368426716439789752420588738/
052096000000000000000000000000)
 H-ROOT= 1648927564002510749416996730441210023410096821471374972292984198/
7684549031584329726567146823205814262854207907962600981493647864092228299/
952213429001442574873342903254185397925273860595281816475454849938270698)
)
(K= 39406
 Q= 113813943060180115688125786593603450748157167726837901321962140627302/
2052760282563533393082052374181378959803714042961109683212049866919389546/
614575571814780868244492594269034742888765005120202166186174183
 A= 250517222971774900024837533408005967813407643241520204508332671174429/
9165884092152529804958039776925779633512951864928493885549669718367174735/
090827742381530450928154155082067869354808083423747771380868798396
 B= 175130739735346787230155307217527258695423837795543250224471103309709/
2102203382783999737123146560508057934595858706672395366720002287941029792/
357553142790994069224363301251762261657503935775539048994787067571
 P= (686472019
     40227378384215312715461923173265645300929851500319910701416206175782/
9922285492345919788530551065606024388738920103733709359795282960836279550/
03497587296772200413778435838221459529760927084567010704035277367945))
```

```
(N= 1138139430601801156881257865936034507481571677268379013219621406273/
02205276028256353339308205237418137895980371404296110968321204986691938/
9546614575571814780868244492594269034742888765005120202166186174183
 DISC= -571)
(HILBEQN= (1 400497845154831586723701480652800
              818520809154613065770038265334290448384
              4398250752422094811238689419574422303726895104
             -16319730975176203906274913715913862844512542392320
              15283054453672803818066421650036653646232315192410112)
                         ...
                    .
                    .
                    .
(N= 167914564828063403047877737704654289373393305605166432906761217057
 DISC= -47)
(WATSEQN= (1 0 -1 -2 -2 -1)
 H-ROOT= 157802772974708238730713964995978423824267305127219319095974461077)
(TRANSFORMED_FROM_W-ROOT=
         98943962984957353716765947459669649176084326493611331376732901259)
(K= 1845504 Q= 90985749599059879061696825205827135337925381756228286851577
 A= 148908828340387242415672401248818027503230076346660057525192560720
 B= 80559905361800237505510331044231416602289767192410946878075514778
 P= (1581278695
     53341474148687862270570699866495456892135289611515267460682123534)
)

(N= 90985749599059879061696825205827135337925381756228286851577 DISC= -463)
(WATSEQN= (1 -11 -9 -8 -7 -7 -3 -1)
 H-ROOT= 89269063821083628669686104610140304331597503052637374453663)
(TRANSFORMED_FROM_W-ROOT=
         52500329291704501488386480971208755282874239293568282807051)
(K= 4 Q= 22746437399764969765424206301347842659703211196334784520281
 A= 83408272427817509053027933398633442929109311269726523824918
 B= 85934098151564965722584230667698007065381334765227111500471
 P= (556388845 33280120002543536945823748149405006167558800785473982376373)
)
                    .
                    .
                    .

(N= 299181570129062362581619776823 DISC= -7)
(HILBEQN= (1 3375) H-ROOT= 299181570129062362581619773448)
(K= 202372016 Q= 1478374214195025720161
 A= 80731534794564966901210191982 B= 72890765758395612443350295079
 P= (1114665619 109659926675783084815657590861)
)

(N= 1478374214195025720161 DISC= -7)
(HILBEQN= (1 3375) H-ROOT= 1478374214195025716786)
(K= 107120384 Q= 13801054094879
 A= 1259710778715252563263 B= 900930232093972691732
 P= (638640083 1084169087079598897830)
)
```