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).

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 $j = \bar{j}$. 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 $P \in E_R(a,b)$
          until $qP = I_\infty$;
          return( $(P, q, a, b)$ appended to GK($q$) )
end;
```

Figure 1: The Goldwasser-Kilian Algorithm

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

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

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

               $(x\ y)^T$ := 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

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 $p = N_D(\nu_{x,y}) = p^2x^2 + bpxy + y^2(\frac{b^2+D}{4p})$ 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 $[p, b, \frac{b^2+D}{4}]$ 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

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

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 $\overline{H}_{-D}(x) = x^h H_{-D}\left(\frac{(x-16)^3}{x}\right)$. 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 $\overline{H}_{-D}(x) = x^h \prod_{i=1}^{h}\left(\frac{(x-16)^3}{x} - \beta_i\right) = \prod_{i=1}^{h}((x - 16)^3 - x\beta_i)$. 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.

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 Certificate Of Primality

We present a certificate of primality for the number 886389468759746441206823904403022554463 . 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 **WROOT** of the Watson equation to the desired root **HROOT** of the Hilbert equation. The results of these transformations are also depicted in such cases.

```
CERTIFICATE-OF-PRIMALITY

(N= 886389468759746441206823904403022554463
 K= 16 Q= 5539934179748415258240124404139694023
 A= 48168915976079488938009020288137257956
 B= 13669570947859443562533340317694801156
 P= (746388339 23307399113241088723083031121380080682))
  (Using DISC= -31
     WATSEQN= (1 -1 0 -1)
     WROOT= 21217821680133787540148229752828498612
     TRANSFORMED TO  HROOT= 86370742134816758992866005547696514022
   )

(N= 5539934179748415258240124404139694023
 K= 92004 Q= 60214057864314760810393273735183
 A= 346001064090897808894540616836935197
 B= 2431357638974085637535314671764106570
 P= (178776266 2680609137898471413937430924866500820))
  (Using DISC= -123
     HILBEQN= (1 1354146840576000 148809594175488000000)
     HROOT= 2156060498211044567316001115257605707
   )

(N= 60214057864314760810393273735183
 K= 17 Q= 3542003403783220999181515765037
 A= 60065706047834347567625868590152
 B= 60115156653327818648548336971829
 P= (1747970121 18887586229752557844146371888460))
  (Using DISC= -123
     HILBEQN= (1 1354146840576000 148809594175488000000)
     HROOT= 37466348834964750581819581164695
   )

(N= 3542003403783220999181515765037
 K= 16 Q= 221375212736451183251805682583
 A= 816276962733305719504229153689
 B= 2905520244344351145790496612484
 P= (192588469 2788415046748075176001935567704))
  (Using DISC= -1747
     HILBEQN=
      (1 10641787589974170558561247134527907023876313316947271680000
      -1073980648086639795645379984231813344252858982220169216000000
      -5035877279568158128379680839999923826224948571172503552000000000
        4905320267498993584283801805836981106400576099319808000000000000000
     109722760088830642850800118707182494014465387926902538240000000000000000)
     HROOT= 1965797676947426290278122699171
   )

(N= 2213752127364511832518056825883 K= 48
 Q= 46119835986760789125464010071 A= 197596315361653412420696230275
 B= 131730876907768941613797486850
 P= (1739899125 21420646574268654462027969110))
  (Using DISC= -119
     WATSEQN= (1 -4 5 -8 9 -7 5 -4 2 -1 1)
     WROOT= 81412001108955131347193666157
     TRANSFORMED TO HROOT= 176730192107069678137767922324
   )

(N= 46119835986760789125464010071  K= 3708
 Q= 12437927720270260849448887 A= 275296490510577514842101223
 B= 1717411804777736185936404469 P= (393406008 2868481708688893990557602277))
  (Using DISC= -443
     HILBEQN= (1 52095503201744864610381824000
               -1945661384100482010970186328309760000000
                7266644577605164712252927855487520604160000000000
               -6456776195727100079078962908487022018560000000000000
                158038389963230406919280467763961371033600000000000000000)
     HROOT= 1655516228668989738303118037
    )

(N= 12437927720270260849448887  K= 9 Q= 138199196891685976750213
 A= 970811219516661021460984 B= 232609889002098652659027
 P= (824597783 534317101019577950214061))
  (Using DISC= -443
     HILBEQN= (1 52095503201744864610381824000
               -1945661384100482010970186328309760000000
                7266644577605164712252927855487520604160000000000
               -6456776195727100079078962908487022018560000000000000
                158038389963230406919280467763961371033600000000000000000)
     HROOT= 996008531292492922365807
    )

(N= 138199196891685976750213  K= 4 Q= 34549799222933253471379
 A= 104701578296406078177774 B= 62007325637914667547473
 P= (13240145 86984553015130498903472))
  (Using DISC= -967
     WATSEQN= (1 -43 68 -122 99 -81 18 -6 -13 1 -2 -1)
     WROOT= 91791838250150617570608
     TRANSFORMED TO HROOT= 75453534190109869337056
   )
```

Eleven more reductions are made, finally yielding 383, which is easily prime by trial division.