On the Factorization of Odd Semiprimes

Janis Kuzmanis

Riga, Latvia
Email: yanisku@gmail.com

Abstract

A mathematically simple odd semiprime factorization method is presented.

Mathematics Subject Classification: 94A60, 94A62, 11A51, 11D09

Keywords: semiprime factorization, RSA cryptosystem attacking

1 Introduction

The well-known "factoring problem" in mathematics means the difficulty of factoring the product of two large prime numbers – large odd semiprime. This task is so time-consuming even on advanced computing systems, that it became the cornerstone to many modern cryptography methods, for example, the RSA algorithm and it's variations [10]. As for cracking, quadratic sieve [12] and general number-field sieve [13] are today's best-known non-quantum algorithms for large semiprime factoring, both have many modifications, which are fine-tuned for semiprime size, possible structure and other features. Even more, the competition between information security and attacking to this security is one of the driving forces in progress of quantum computing, mainly because of Shor's algorithm existence [7].

The main result of the given article is the proven possibility to extract two odd semiprime $N = N_1 \cdot N_2$ forming multipliers N_1 and N_2 separately from the roots of generalized Pell's equations $x^2 - D \cdot y^2 = N_1 \cdot N_2$ and $x^2 - D \cdot y^2 = N_1^2 \cdot N_2^2$. Two versions of such extraction are presented.

The proposed article is the direct consequence of [3], where some of underlying conceptions were introduced. Due to this reason we preserve also previous notations: π for palindromic components in continuants and continued fractions; manipulation with symbols $K(\rho, \omega)/K(\omega)$ for fundamental roots of generalized Pell's equations; see more in [4] and [5].

2 Already known material

Here we present without proofs some items from [3], relevant to further method exposition.

2.1 Conjugation relations

If we have an ordinary negative Pell's equation $x^2 - D \cdot y^2 = -1$ with fundamental roots $K(a_0, \pi)/K(\pi)$ and two generalized Pell's equations

- $x^2 - D \cdot y^2 = -N$ with fundamental roots $\pm K(\rho, \omega)/K(\omega)$, and
- $x^2 - D \cdot y^2 = +N$ with fundamental roots $\pm K(\rho', \omega')/K(\omega')$,

then for all natural $N > 2$ the following conjugation relations exist:

$$\begin{cases} K(\rho', \omega') &= -K(\rho, \omega) \cdot K(a_0, \pi) + D \cdot K(\omega) \cdot K(\pi) \\ K(\omega') &= -K(\rho, \omega) \cdot K(\pi) + K(\omega) \cdot K(a_0, \pi), \end{cases} \tag{1}$$

$$\begin{cases} K(\rho, \omega) &= K(\rho', \omega') \cdot K(a_0, \pi) - D \cdot K(\omega') \cdot K(\pi) \\ K(\omega) &= K(\rho', \omega') \cdot K(\pi) - K(\omega') \cdot K(a_0, \pi). \end{cases} \tag{2}$$

Henceforth we will call such system of mentioned three Pell's equations as corresponding to Property A.

2.2 Ambiguity

Fundamental solutions $K(\rho, \omega) + K(\omega) \cdot \sqrt{D}$ and $K(\rho', \omega') + K(\omega') \cdot \sqrt{D}$ traditionally are defined as the least non-negative values of the given associativity class, satisfying the corresponding generalized Pell's equations [8]. For ambiguous classes zero fundamental solutions can occur. Therefore:

- for all positive $N = k^2$ we have ambiguous fundamental solutions in the form $(k, 0)$ or $K(\rho', \omega') = k$, $K(\omega') = 0$, where $k = 2, 3, 4, ...$ As $K(\omega') = 0$, conjugation relations (2) give ambiguous fundamental solutions

$$\begin{cases} K(\rho, \omega) &= K(\rho', \omega') \cdot K(a_0, \pi) \\ K(\omega) &= K(\rho', \omega') \cdot K(\pi). \end{cases} \tag{3}$$

- for all negative $N = k^2 \cdot D$ we have ambiguous fundamental solutions in the form $(0, k)$ or $K(\rho, \omega) = 0$, $K(\omega) = k$, where $k = 1, 2, 3, ...$ As $K(\rho, \omega) = 0$, conjugation relations (1) give ambiguous fundamental solutions

$$\begin{cases} K(\rho', \omega') &= D \cdot K(\pi) \cdot K(\omega) \\ K(\omega') &= K(a_0, \pi) \cdot K(\omega). \end{cases} \tag{4}$$

2.3 Criterion for squaring

We have $\pm K(\rho,\omega)/K(\omega)$ and $\pm K(\rho',\omega')/K(\omega')$ as fundamental solutions for generalized Pell's equations $x^2 - D \cdot y^2 = -N$ and $x^2 - D \cdot y^2 = +N$, corresponding to Property A system. Then fundamental solutions $\pm K(\sigma',\tau')/K(\tau')$ of generalized Pell's equation $x^2 - D \cdot y^2 = +N^2$ can be obtained in the following way:

- If $D \cdot K(\omega') \cdot K(\omega) > K(\rho',\omega') \cdot K(\rho,\omega)$, then

$$\begin{cases} K(\sigma',\tau') &= K^2(\rho,\omega) + D \cdot K^2(\omega) \\ K(\tau') &= 2K(\rho,\omega) \cdot K(\omega). \end{cases} \tag{5}$$

- If $D \cdot K(\omega') \cdot K(\omega) < K(\rho',\omega') \cdot K(\rho,\omega)$, then

$$\begin{cases} K(\sigma',\tau') &= K^2(\rho',\omega') + D \cdot K^2(\omega') \\ K(\tau') &= 2K(\rho',\omega') \cdot K(\omega'). \end{cases} \tag{6}$$

Expressions $D \cdot K(\omega') \cdot K(\omega) > K(\rho',\omega') \cdot K(\rho,\omega)$ and $D \cdot K(\omega') \cdot K(\omega) < K(\rho',\omega') \cdot K(\rho,\omega)$ are called as criterions for squaring, so (5) executes when criterion for squaring is $>$, but (6) – when criterion for squaring is $<$. For $N =$ prime expressions (5) or (6) give all non-ambiguous fundamental solutions of generalized Pell's equation $x^2 - D \cdot y^2 = +N^2$. For composite N values the situation is much more complex, odd semiprimes $N = N_1 \cdot N_2$ will be our special interest.

Thus fundamental non-ambiguous solutions $\pm K(\sigma',\tau')/K(\tau')$ of generalized Pell's equations $x^2 - D \cdot y^2 = +N^2$ can be obtained. Fundamental non-ambiguous solutions $\pm K(\sigma,\tau)/K(\tau)$ of generalized Pell's equations $x^2 - D \cdot y^2 = -N^2$ then comes from conjugation relations. Corresponding ambiguous fundamental solutions $K(\sigma',\tau') = k$, $K(\tau') = 0$ of these equations were already mentioned.

Remark. *With composite N values more than one pair of $\pm K(\rho,\omega)/K(\omega)$ and $\pm K(\rho',\omega')/K(\omega')$ fundamental roots can occur. Calculations, based on criterion, must be done with conjugation pairs, connected by relations (1) and (2).*

3 Multiplication

Here begins new material.

Suppose that we extend our Property A system to the following characteristics:

- $\pm K(\rho_1,\omega_1)/K(\omega_1)$ and $\pm K(\rho_1',\omega_1')/K(\omega_1')$ are fundamental roots for generalized Pell's equations $x^2 - D \cdot y^2 = -N_1$ and $x^2 - D \cdot y^2 = +N_1$ correspondingly;
- $\pm K(\rho_2,\omega_2)/K(\omega_2)$ and $\pm K(\rho_2',\omega_2')/K(\omega_2')$ are fundamental roots for generalized Pell's equations $x^2 - D \cdot y^2 = -N_2$ and $x^2 - D \cdot y^2 = +N_2$ correspondingly;
- $\pm K(a_0,\pi)/K(\pi)$ are fundamental roots for negative Pell's equation $x^2 - D \cdot y^2 = -1$;

- N_1 and N_2 are different odd primes, coprime to D.

So all mentioned equations are united under the same discriminant D value. According to [8], for generalized Pell's equation $x^2 - D \cdot y^2 = N$ with $N =$ prime not more than one pair of fundamental roots is possible. Thus we have only one pair of conjugated fundamental roots for each pair of equations $x^2 - D \cdot y^2 = \pm N_1$ and $x^2 - D \cdot y^2 = \pm N_2$. Experiments demonstrated that pair of equations $x^2 - D \cdot y^2 = \pm N_1 \cdot N_2$ then have two pairs of conjugated fundamental solutions $K(\sigma, \tau)/K(\tau)$ and $K(\sigma', \tau')/K(\tau')$, whose values can be calculated from initial $K(\rho, \omega)/K(\omega)$ and $K(\rho', \omega')/K(\omega')$.

We proceed analogously to [3], representing initial fundamental solutions in the form $K(\rho, \omega) + K(\omega) \cdot \sqrt{D}$ and $K(\rho', \omega') + K(\omega') \cdot \sqrt{D}$ and multiplicating them. One of such versions is

$$\begin{aligned} &[+K(\rho_1, \omega_1) + \sqrt{D} \cdot K(\omega_1)] \cdot [+K(\rho_2, \omega_2) + \sqrt{D} \cdot K(\omega_2)] = \\ &= K(\rho_1, \omega_1) \cdot K(\rho_2, \omega_2) + D \cdot K(\omega_1) \cdot K(\omega_2) \\ &\quad + \sqrt{D}[K(\rho_1, \omega_1) \cdot K(\omega_2) + K(\rho_2, \omega_2) \cdot K(\omega_1)], \end{aligned} \tag{7}$$

therefore

$$\begin{cases} K(\sigma', \tau') &= K(\rho_1, \omega_1) \cdot K(\rho_2, \omega_2) + D \cdot K(\omega_1) \cdot K(\omega_2) \\ K(\tau') &= K(\rho_1, \omega_1) \cdot K(\omega_2) + K(\rho_2, \omega_2) \cdot K(\omega_1). \end{cases} \tag{8}$$

Suppose that these new roots $K(\sigma', \tau')/K(\tau')$ are positive. As initial multipliers were associated with $-N_1$ and $-N_2$, their multiple is associated with $+N_1 \cdot N_2$.

Now from conjugation relations (1) and (2) we get:

$$\begin{aligned} &K(\tau) = K(\sigma', \tau') \cdot K(\pi) - K(\tau') \cdot K(a_0, \pi) = \\ &= K(\rho_1, \omega_1) \cdot K(\rho_2, \omega_2) \cdot K(\pi) + D \cdot K(\omega_1) \cdot K(\omega_2) \cdot K(\pi) \\ &\quad - K(\rho_1, \omega_1) \cdot K(\omega_2) \cdot K(a_0, \pi) - K(\rho_2, \omega_2) \cdot K(\omega_1) \cdot K(a_0, \pi) = \\ &= K(\rho_1, \omega_1) \cdot \underbrace{[K(\rho_2, \omega_2) \cdot K(\pi) - K(\omega_2) \cdot K(a_0, \pi)]}_{-K(\omega_2')} \\ &\quad + K(\omega_1) \cdot \underbrace{[-K(\rho_2, \omega_2) \cdot K(a_0, \pi) + D \cdot K(\omega_2) \cdot K(\pi)]}_{K(\rho_2', \omega_2')} = \\ &= -K(\rho_1, \omega_1) \cdot K(\omega_2') + K(\omega_1) \cdot K(\rho_2', \omega_2'), \end{aligned} \tag{9}$$

or, analogously

$$= -K(\rho_2, \omega_2) \cdot K(\omega_1') + K(\omega_2) \cdot K(\rho_1', \omega_1').$$

Again from (1) and (2):

$$\begin{aligned} &K(\sigma, \tau) = K(\sigma', \tau') \cdot K(a_0, \pi) - D \cdot K(\tau') \cdot K(\pi) = \\ &= K(\rho_1, \omega_1) \cdot K(\rho_2, \omega_2) \cdot K(a_0, \pi) + D \cdot K(\omega_1) \cdot K(\omega_2) \cdot K(a_0, \pi) \\ &\quad - D \cdot K(\rho_1, \omega_1) \cdot K(\omega_2) \cdot K(\pi) - D \cdot K(\rho_2, \omega_2) \cdot K(\omega_1) \cdot K(\pi) = \\ &= K(\rho_1, \omega_1) \cdot \underbrace{[K(\rho_2, \omega_2) \cdot K(a_0, \pi) - D \cdot K(\omega_2) \cdot K(\pi)]}_{-K(\rho_2', \omega_2')} \\ &\quad + D \cdot K(\omega_1) \cdot \underbrace{[K(\omega_2) \cdot K(a_0, \pi) - K(\rho_2, \omega_2) \cdot K(\pi)]}_{K(\omega_2')} = \\ &= -K(\rho_1, \omega_1) \cdot K(\rho_2', \omega_2') + D \cdot K(\omega_1) \cdot K(\omega_2'), \end{aligned} \tag{10}$$

or, analogously

$$= -K(\rho_2, \omega_2) \cdot K(\rho_1', \omega_1') + D \cdot K(\omega_2) \cdot K(\omega_1').$$

Obtained roots $K(\sigma, \tau)/K(\tau)$ are associated with $-N_1 \cdot N_2$. If we want roots $K(\sigma, \tau)/K(\tau)$ positive, then from (10) follows the first part of the

3.1 Criterion for multiplication

.

Under extended Property A conditions the following relations exist:

- If $D \cdot K(\omega_1) \cdot K(\omega_2') > K(\rho_1, \omega_1) \cdot K(\rho_2', \omega_2')$ or $D \cdot K(\omega_2) \cdot K(\omega_1') > K(\rho_2, \omega_2) \cdot K(\rho_1', \omega_1')$, then

$$\left\{ \begin{array}{rcl} K(\sigma', \tau') & = & K(\rho_1, \omega_1) \cdot K(\rho_2, \omega_2) + D \cdot K(\omega_1) \cdot K(\omega_2) \\ K(\tau') & = & K(\rho_1, \omega_1) \cdot K(\omega_2) + K(\rho_2, \omega_2) \cdot K(\omega_1). \end{array} \right. \tag{11}$$

- If $D \cdot K(\omega_1) \cdot K(\omega_2') < K(\rho_1, \omega_1) \cdot K(\rho_2', \omega_2')$ or $D \cdot K(\omega_2) \cdot K(\omega_1') < K(\rho_2, \omega_2) \cdot K(\rho_1', \omega_1')$, then

$$\left\{ \begin{array}{rcl} K(\sigma', \tau') & = & K(\rho_1', \omega_1') \cdot K(\rho_2', \omega_2') + D \cdot K(\omega_1') \cdot K(\omega_2') \\ K(\tau') & = & K(\rho_1', \omega_1') \cdot K(\omega_2') + K(\rho_2', \omega_2') \cdot K(\omega_1'). \end{array} \right. \tag{12}$$

Missing proof of (12) comes analogously from

$$\begin{array}{l} [+K(\rho_1', \omega_1') + \sqrt{D} \cdot K(\omega_1')] \cdot [+K(\rho_2', \omega_2') + \sqrt{D} \cdot K(\omega_2')] = \\ = K(\rho_1', \omega_1') \cdot K(\rho_2', \omega_2') + D \cdot K(\omega_1') \cdot K(\omega_2') \\ \quad + \sqrt{D}[K(\rho_1', \omega_1') \cdot K(\omega_2') + K(\rho_2', \omega_2') \cdot K(\omega_1')], \end{array} \tag{13}$$

whose initial multipliers are associated with $+N_1$ and $+N_2$, so their multiple is associated with $+N_1 \cdot N_2$. Transformations, analogous (9) and (10), lead to

$$K(\sigma, \tau) = K(\rho_2', \omega_2') \cdot K(\rho_1, \omega_1) - D \cdot K(\omega_2') \cdot K(\omega_1),$$

or, analogously

$$K(\sigma, \tau) = K(\rho_1', \omega_1') \cdot K(\rho_2, \omega_2) - D \cdot K(\omega_1') \cdot K(\omega_2).$$

If $K(\sigma, \tau)$ is positive, we get (12).

But relations (11) or (12) give only one pair or roots $\pm K(\sigma', \tau')/K(\tau')$ (with their conjugated counterparts $\pm K(\sigma, \tau)/K(\tau)$). In generalized Pell's equations both unknowns are of second degree, so non-ambiguous roots come in pairs $\pm K(\rho, \omega)$ and $\pm K(\rho', \omega')$. This gives second pair of roots $\pm K(\sigma', \tau')/K(\tau')$, where differences of terms are used instead of sums:

Under extended Property A conditions also the following relations exist:

- If $D \cdot K(\omega_1) \cdot K(\omega_2') > K(\rho_1, \omega_1) \cdot K(\rho_2', \omega_2')$ or $D \cdot K(\omega_2) \cdot K(\omega_1') > K(\rho_2, \omega_2) \cdot K(\rho_1', \omega_1')$, then

$$\left\{ \begin{array}{rcl} K(\sigma', \tau') & = & |-K(\rho_1, \omega_1) \cdot K(\rho_2, \omega_2) + D \cdot K(\omega_1) \cdot K(\omega_2)| \\ K(\tau') & = & |K(\rho_1, \omega_1) \cdot K(\omega_2) - K(\rho_2, \omega_2) \cdot K(\omega_1)|. \end{array} \right. \tag{14}$$

- If $D \cdot K(\omega_1) \cdot K(\omega_2') < K(\rho_1, \omega_1) \cdot K(\rho_2', \omega_2')$ or $D \cdot K(\omega_2) \cdot K(\omega_1') < K(\rho_2, \omega_2) \cdot K(\rho_1', \omega_1')$, then

$$\begin{cases} K(\sigma', \tau') &= | - K(\rho_1', \omega_1') \cdot K(\rho_2', \omega_2') + D \cdot K(\omega_1') \cdot K(\omega_2')| \\ K(\tau') &= |K(\rho_1', \omega_1') \cdot K(\omega_2') - K(\rho_2', \omega_2') \cdot K(\omega_1')|. \end{cases} \quad (15)$$

Expressions (14) and (15) constitute the second part of criterion for multiplication.

Experimental Table 1 illustrates described formation of two pairs of conjugated fundamental roots for semiprimes. Here $D = 29$ and from tables for negative Pell's equation roots we find $K(a_0, \pi) = 70$, $K(\pi) = 13$. Conjugated roots are written in one row.

Table 1. Extended Property A system with $D = 29$.

N_1 or N_2	$\pm K(\rho, \omega), K(\omega)$	$\pm K(\rho', \omega'), K(\omega')$
5	16,3	11,2
7	43,8	6,1
13	4,1	97,18
$N_1 \cdot N_2$	$\pm K(\sigma, \tau), K(\tau)$	$\pm K(\sigma', \tau'), K(\tau')$
$5 \cdot 7 = 35$	183,34	8,1
	9,2	124,23
$5 \cdot 13 = 65$	102,19	23,4
	14,3	151,28
$7 \cdot 13 = 91$	53,10	60,11
	5,2	404,75

For semiprime $5 \cdot 7 = 35$ we calculate criterion for multiplication as $29 \cdot 3 \cdot 1 < 16 \cdot 6$ or $29 \cdot 2 \cdot 8 < 43 \cdot 11$, therefore roots $K(\sigma', \tau'), K(\tau')$ will be formed from $K(\rho', \omega'), K(\omega')$ values by equations (12) and (15). Sum gives 124,23 and difference 8,1. Conjugated roots $K(\sigma, \tau), K(\tau)$ come from relations (2). Testing of semiprimes 65 and 91 is left to concerned reader.

4 Extraction

Under extended Property A conditions we thus confirmed for odd semiprimes $N = N_1 \cdot N_2$ existence of two pairs of conjugated fundamental roots for equations $x^2 - D \cdot y^2 = \pm N_1 \cdot N_2$. Experiments demonstrated that pair of equations $x^2 - D \cdot y^2 = \pm N_1^2 \cdot N_2^2$ has 5 pairs of conjugated fundamental roots (see Table 2), whose structure is the following (for positive $N_1^2 \cdot N_2^2$). One of these pairs is clearly an ambiguous solution of type (3) with $K(\sigma', \tau') = N$, $K(\tau') = 0$. Two other pairs can be traced down to two pairs of fundamental roots for equation $x^2 - D \cdot y^2 = N_1 \cdot N_2$; they are formed by squaring of these roots according to the criterion for squaring (relations (5) or (6)). These pairs therefore have coprimality $K(\sigma', \tau') \perp K(\tau')$, which can be used for their identification, but their values also can be calculated from (5) or (6).

Remaining two non-coprime pairs are roots from multiplication $N^2 = (N_1^2) \cdot (N_2^2)$. Here each multiplier is a perfect square, it has one pair of coprime fundamental roots and one pair of ambiguous ones, whose greatest common divisor GCD equals N_1 or N_2 – this from (3), because $K(a_0, \pi) \perp K(\pi)$ in negative Pell's equation $x^2 - D \cdot y^2 = -1$. Cross-versions of multiplication,

where coprime roots come from one multiplier and non-coprime ambiguous ones from other, then give these remaining two non-coprime pairs. Their GCD-s will be the necessary N_1 and N_2 values we are hunting for.

Experimental Table 2 is the continuation of Table 1 and shows roots for semiprime squares; $D = 29$; conjugated roots are written in one row.

Table 2. Extended Property A system with $D = 29$.

$N_1^2 \cdot N_2^2$	$\pm K(\sigma,\tau), K(\tau)$	$\pm K(\sigma',\tau'), K(\tau')$	Comments
$5^2 \cdot 7^2 = 1225$	478,89	93,16	GCD = 1
	218,41	197,36	GCD = 1
	130,25	325,60	GCD = 5
	14,7	1659,308	GCD = 7
	2450,455	35,0	Ambiguous
$5^2 \cdot 13^2 = 4225$	142,29	993,184	
	322,61	457,84	
	670,125	225,40	
	26,13	3081,572	
	4550,845	65,0	
$7^2 \cdot 13^2 = 8281$	10,17	5709,1060	
	2330,433	141,20	
	938,175	315,56	
	338,65	845,156	
	6370,1183	91,0	

For semiprime's $5 \cdot 7 = 35$ first pair (from Table 1) we calculate criterion for squaring as $29 \cdot 34 \cdot 1 < 183 \cdot 8$, therefore roots $K(\sigma',\tau'), K(\tau')$ will be formed from root pair 8,1. It gives $K(\sigma',\tau') = 8^2 + 29 \cdot 1^2 = 93$ and $K(\tau') = 2 \cdot 8 \cdot 1 = 16$. Corresponding $K(\sigma,\tau), K(\tau)$ values come from (2). For the second pair criterion for squaring is $29 \cdot 2 \cdot 23 > 9 \cdot 124$, therefore roots $K(\sigma',\tau'), K(\tau')$ will be formed from root pair 9,2; we get $K(\sigma',\tau') = 9^2 + 29 \cdot 2^2 = 197$ and $K(\tau') = 2 \cdot 9 \cdot 2 = 36$. Root pair 35,0 is clearly ambiguous, remaining two pairs are not coprime and their GCD-s are our necessary semiprime factors 5 and 7. Calculations for semiprime squares 4225 and 8281 are left for concerned reader.

Now the result. We have large odd semiprime $N = N_1 \cdot N_2$ and we urgently need it's factors N_1 and N_2. At first we must take discriminant sequence for negative Pell's equation $D =$ 2, 5, 10, 13, 17, ... (A031396 in OEIS [9], re-check before use) and find D value, corresponding to extended Property A system for this N. It can be indicated by two pairs of conjugated fundamental roots with coprimality ($K(\rho',\omega') \perp K(\omega')$). Then find fundamental roots for generalized Pell's equation $x^2 - D \cdot y^2 = N^2$, using this D value. There must be five pairs of conjugated fundamental roots. Ignore ambiguous pair, ignore two pairs with $K(\sigma',\tau') \perp K(\tau')$ coprimality, but the GCD-s from the remaining two ones will be the necessary N_1 and N_2 values.

4.1 Extraction – second version

There exists even more effective extraction method. We can treat semiprime squaring as multiplication $N^2 = (N_1 \cdot N_2) \cdot (N_1 \cdot N_2)$ and use relations (11) and (14) or relations (12) and (15) – depending on calculated criterion for multiplication.

For semiprime $5 \cdot 7 = 35$ we calculate criterion for multiplication (see Table 1) as $29 \cdot 34 \cdot 23 < 183 \cdot 124$ or $29 \cdot 2 \cdot 1 < 9 \cdot 8$, therefore non-coprime roots $K(\sigma', \tau')/K(\tau')$ will be formed from values 8,1 and 124,23 as initials by equations (12) and (15). Sum gives 1659,308 and difference 325,60 (see Table 2). Conjugated roots $K(\sigma, \tau)/K(\tau)$ come from relations (2). The reader is welcomed to make similar calculations for semiprime squares 4225 and 8281.

Now the result. We have large odd semiprime $N = N_1 \cdot N_2$ and we need it's factors N_1 and N_2. At first we must take discriminant sequence for negative Pell's equation $D =$ 2, 5, 10, 13, 17, ... (A031396 in OEIS [9]) and find D value, corresponding to extended Property A system for this N. It can be indicated by two pairs of conjugated fundamental roots with coprimality $(K(\rho', \omega') \perp K(\omega'))$. Calculate their conjugation, write each pair of these conjugated roots in separate row – as in Table 1. Calculate criterion for multiplication, then calculate both non-coprime pairs, whose GCD-s will be the necessary N_1 and N_2 values.

There are other versions of mentioned extraction, but presented ones seems the simplest.

5 Final conclusions

1. Extended Property A systems. All presented material shows significance of extended Property A systems for effective odd semiprime factorization. As discriminant sequence for negative Pell's equation is infinite, there exists infinitely many triples $D/K(\rho, \omega)/K(\omega)$, satisfying Property A conditions for $\pm N_1 = prime$ values and infinitely many of them will satisfy Property A conditions also for $\pm N_2 = prime$ values. So sequence of extended Property A systems for given particular semiprime is infinite. Only – are they frequent or extremely rare?

We tested semiprimes from primes 29983, 29989, 30011 and 30013 against discriminant D sequence 2...1033 and discovered 11...22 extended Property A systems for each semiprime in mentioned D range. Evaluation for large semiprimes is not for author's laptop.

2. Pell's equations. Presented method requires separate finding of fundamental roots for generalized Pell's equations $x^2 - D \cdot y^2 = \pm N$ with large N values, but relatively small discriminants D. Author is not a programmer, but for the beginning there are few online tools with available code [1, 6], see also [11].

3. Generalization. Given method can be effectively generalized for composites from more than two primes, but it is not the subject of presented article.

References

[1] D. Alpern, *Generic two integer variable equation solver* (2026). https://www.alpertron.com.ar/QUAD.HTM.

[2] S. Hallgren, Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem, *Journal of the ACM,* **54**, no.1 (2007), pp.1-19. doi: 10.1145/1206035.1206039.

[3] J. Kuzmanis, Some *abc*-Properties of the Generalized Pell's Equations $x^2 - D \cdot y^2 = \pm N$ and $x^2 - D \cdot y^2 = \pm N^2$, *International Journal of Algebra,* **19**, no. 4 (2025), pp. 251-274. https://doi.org/10.12988/ija.2025.91998.

[4] J. Kuzmanis, On the Origin of *abc*-Triples, *International Journal of Algebra,* **19**, no. 1 (2025), pp. 13-46. https://doi.org/10.12988/ija.2025.91920.

[5] J. Kuzmanis, A subset of generalized Pell's equations $x^2 - Dy^2 = \pm 4$ and it's *abc*-properties, (2024). https://vixra.org/abs/2411.0071.

[6] K. Matthews, *Solving the diophantine equation* $x^2 - Dy^2 = N$*,* $D > 0$ *and not a perfect square* (2026). http://www.numbertheory. org/php/nagell_fundamental.html

[7] N. D. Mermin, Lecture notes on quantum computation. III Breaking RSA Encryption with a Quantum Computer: Shor's Factoring Algorithm, 3/28/2006, 30 pp. https://web.archive.org/web/20121115112940/http://people.ccmr.cornell.edu/∼mermin/qcomp/chap3.pdf.

[8] T. Nagell, *Introduction to Number Theory*, 2nd ed., reprint, AMS Chelsea Publishing, 2010.

[9] Online Encyclopedia of Integer Sequences (2026). A031396 https://oeis.org/A031396.

[10] R. L. Rivest, A. Shamir, L. M. Adleman, Cryptographic communications system and method, US patent 4405829A, 1977, dec. 14.

[11] J. P. Robertson, Solving the Generalized Pell Equation $x^2 - Dy^2 = N$, July 31, 2004, 26 pp. https://web.archive.org/web/20131001001330/http://www.jpr2718.org/pell.pdf.

[12] Wikipedia (2026). https://en.wikipedia.org/wiki/Quadratic_sieve.

[13] Wikipedia (2026). https://en.wikipedia.org/wiki/General_number_field_sieve.