Int. J. Communications, Network and System Sciences, 2011, 4, 287-296
doi:10.4236/ijcns.2011.45033 Published Online May 2011 (http://www.SciRP.org/journal/ijcns)

Protection of Sensitive Messages Based on Quadratic Roots of Gaussians: Groups with Complex Modulus*

Boris Verkhovsky
Computer Science Department, New Jersey Institute of Technology, University Heights, Newark, USA
E-mail: *verb73@gmail.com*
Received April 5, 2011; *revised May* 3, 2011; *accepted May* 20, 2011

Abstract

This paper considers three algorithms for the extraction of square roots of complex integers {called Gaussians} using arithmetic based on complex modulus $p + iq$. These algorithms are almost twice as fast as the analogous algorithms extracting square roots of either real or complex integers in arithmetic based on modulus p, where p is a real prime. A cryptographic system based on these algorithms is provided in this paper. A procedure reducing the computational complexity is described as well. Main results are explained in several numeric illustrations.

Keywords: Complex Modulus; Computational Efficiency; Cryptographic Algorithm; Digital Isotopes; Multiplicative Control Parameter; Octadic Roots, Quartic Roots, Rabin Algorithm, Reduction of Complexity, Resolventa, Secure Communication, Square Roots

1. Introduction and Problem Statement

The concept of complex modulus was introduced by C. F. Gauss [1]. The set of complex integers is an infinite system of equidistant points located on parallel straight lines, such that the infinite plane is decomposable into infinitely many squares. Analogously, every integer that is divisible by a complex integer $m = a + bi$ forms infinitely many squares, with sides equal to $\sqrt{a^2+b^2}$.

1.1. Complex Moduli

Let's denote $(a,b) := a+bi$. Associates of $G := (p,q)$ are $-G$, iG and $-iG$; they are the vertices of a square where $-G = (-p,-q)$; $iG = (0,1)(p,q) = (-q,p)$; $-iG = (0,-1)(p,q) = (q,-p)$.

To understand the congruencies, let's consider a system of integer Cartesian coordinates. The squares on this system of coordinates are inclined to the former squares if neither of integers a, b is equal to zero [1]. Then the associates of the modulus (p,q) are rotations of "vector" (p,q) on 90 degrees. Let's consider the plane of complex numbers and as an example, the complex prime number $(1,4) := 1+4i$ [2]. Let the left-most bottom point of the mesh be the origin of the coordinate system for Gaussians, and let $G := 1+4i = (1,4)$ be the Gaussian modulus. Inside each square there is a number of Gaussian integers; plus every vertex of each square is also a Gaussian integer. In order to avoid multiple counting of the same vertex, we consider that only the left-most bottom vertex of each square belongs to that square [1]. For more insights and graphics see [2].

This paper is a logical continuation of a recently published paper [3], which considered a cryptographic scheme based on complex integers modulo real semi-prime pq. The above mentioned paper describes an extractor of quadratic roots from complex integers called Gaussians. A slightly different approach is considered in [4]. Several general ideas for computation of a square root in modular arithmetic are provided in [5-7].

This paper considers arithmetic based on complex integers with *Gaussian modulus*. As demonstrated below, the extraction of square roots in such arithmetic requires a smaller number of basic operations. As a result, the described cryptographic system is almost twice faster than the analogous systems in [3,4].

Consider quadratic equation

$$(x,y)^2 = (c,d) \bmod (p,q), \tag{1}$$

where modulus $G := (p,q)$ is a Gaussian prime; and let

$$N := \|(p,q)\| = p^2 + q^2. \tag{2}$$

*Dedicated to the memory of Samuel A. Verkhovsky.

1.2. General Properties

***Proposition* 1**: Gaussian (p,q) is a prime if and only if its norm *N* is a real prime [1].

Remark 1: Since $\|(\pm p,\pm q)\| = \|(\pm q,\pm p)\|$, without loss of generality we assume that, if (p,q) is prime, then *p* is *odd* and *q* is *even* {unless it is stated otherwise}.

***Proposition* 2**: If norm of (p,q) is a prime (2), then for every (p,q), $(N-1)/4$ is an integer.

Proof: Let $p := 2k+1$ and $q := 2r$. Then (2) implies that

$$N-1 = 4\left[k(k+1)+r^2\right]. \text{ Q.E.D.} \quad (3)$$

***Proposition* 3** {cyclic identity}: If $\gcd\left[(a,b),(p,q)\right] = (1,0)$ and $\|G\|$ is a prime, then the following identity holds:

$$(a,b)^{N-1} \bmod (p,q) = (1,0). \quad (4)$$

Remark 2: More details about identity (4) are provided in the Appendix in Proposition 3.A.

***Proposition* 4** {Modular multiplicative inverse}: if $\gcd\left[(a,\ b),(p,q)\right] = (1,0)$, then

$$(a,b)^{-1} \equiv (a,b)^{N-2} \bmod G. \quad (5)$$

Remark 3: Yet, more computationally-efficient is to solve an appropriate Diophantine equation. However, this is beyond the scope of this paper.

***Definition* 1**: Gaussian (x,y) is called a quadratic root of (c,d) modulo *G* if (x,y) and (c,d) satisfy Equation (1); we denote it as

$$(x,y) := \sqrt{(c,d)} \bmod G. \quad (6)$$

2. Quadratic Root Extraction Where $N \equiv 5 \pmod 8$

***Proposition* 5**: If (p,q) is prime and $N \equiv 5 \pmod 8$, then $m := (N-1)/4$ is *odd*.

Proof: Notice that $q \bmod 4 = 2$, otherwise (3) implies that $N \equiv 1 \pmod 8$. Q.E.D.

2.1. Quadratic and Quartic Roots of $(1, 0)$ Modulo (p,q)

Consider a quadratic root (u,w) of $(1, 0) \bmod (p,q)$: $(u,w) := \sqrt{(1,0)} \bmod (p,q)$.

Then $(u,w)^2 = (u^2 - w^2, 2uw) = (1,0) \bmod (p,q)$. This equation holds if either *w* = 0 and $u^2 = 1 \bmod G$; or if *u* = 0 and

$$w^2 = -1 \bmod G. \quad (7)$$

Since the last equation does not have a real integer solution for *w*, it implies that

$$(u,w) = (\pm 1,0) \equiv \left[(\pm 1,0) + (p,\ q)\right] \bmod G. \quad (8)$$

Hence, if a root (x,y) is known, then another root of (c,d) is $(u,w)(x,y) \bmod G$.

Quartic roots: There are four quartic roots of $(1, 0)$, each satisfying $q_k^4 \equiv (1,0)$:

$$q_1 = (1,0);\ q_2 = (-1,0);\ q_3 = (0,1);\ q_4 = (0,-1); \quad (9)$$

where

$$q_{3,4}^2 \equiv q_2 \pmod G;\ q_2^2 \equiv q_1 \equiv (1,0) \pmod G.$$

2.2. Quadratic Root Extractor (*QRE*-1)

Step 1.1: Compute

$$N := p^2 + q^2;\ m := (N-1)/4;\ z = (N+3)/8 \quad (10)$$

Step 2.1: if *N* is not a prime, **then** *QRE*-1 algorithm is not applicable, $\{n/a\}$;

Remark 4:

$$(p-1,q) \equiv (-1,0) \bmod G; \quad (11)$$

Step 3.1: Compute

$$E := (c,d)^m \bmod G; \quad (12)$$

Step 4.1: if $E = (0,\pm 1)$, **then** (c,d) is Gaussian quadratic non-residue (GQNR}, *i.e.* its square root does not exist;

Step 5.1: if $E = (1,\ 0)$, **then**

$$(x,y) := (c,d)^{(N+3)/8} \bmod G; \quad (13)$$

Step 6.1: if $E = (-1,0)$, **then**

$$R := (0,\pm 1) \bmod G;\ \left\{R \equiv \sqrt{E^{-1}} \bmod G\right\}; \quad (14)$$

$$(x,y) := R \times (c,d)^z \bmod G; \quad (15)$$

Step 7.1 {2nd square root}:

$$(t,v) := (p-1,q)(x,y) \bmod G \quad (11). \quad (16)$$

2.3. Validation of Algorithm

***Proposition* 6**: Suppose

a) (p,q) is a prime and $q \equiv 2 \pmod 4$; (17)

b) $z = (N+3)/8;\ E := (c,d)^{(N-1)/4} \bmod G$; (18)

c) $R \equiv \sqrt{E^{-1}} \bmod G$ if $E = (1,0)$ or $(-1,0)$; (19)

then

$$(c,d)^z R \equiv \sqrt{(c,d)} \pmod G. \quad (20)$$

Proof: First of all, (19) implies that

$$ER^2 \bmod G = (1,0). \tag{21}$$

Yet,

$$\begin{aligned}(c,d)^{(N+3)/4} R^2 &\equiv (c,d)(c,d)^{(N-1)/4} R^2 \equiv (c,d)(ER^2) \\ &\equiv (c,d)(\bmod G)\end{aligned} \tag{22}$$

Therefore, (21) and (22) imply equation

$$(c,d)^{2z} R^2 \equiv (c,d)(\bmod G), \tag{23}$$

which itself implies that (20) is correct. Q.E.D.

3. Criterion of Gaussian Quadratic Residuosity Where $N \equiv 5(\bmod 8)$

***Proposition* 7:** Gaussian (c,d) has a quadratic root modulo Gaussian prime (p,q) only if

$$(c,d)^{(N-1)/4} \bmod G = (\pm 1, 0). \tag{24}$$

***Example* 1**: Consider $p = 91, q = -6; N = \|(p,q)\| = 8317$, which is a prime; hence $(\pm 91, \pm 6)$ are Gaussian primes. Compute $m := (N-1)/4/ = 2079$; $z := (N+3)/8 = 1040$;

Let $(c,d) = (81,71)$. Since $(81,71)^m \equiv (96,85) \equiv (-1,0)(\bmod(91,-6))$ (11), therefore,

$$\begin{aligned}(x,y) &= \sqrt{(81,71)} = (81,71)^{1040} \times (0,1) \\ &= (57,75)(\bmod(91,-6)).\end{aligned} \tag{25}$$

Verification: Indeed,

$$(57,75)^2 \bmod(91,-6) = (81,71). \tag{26}$$

4. Numeric Illustration

Consider $p = 10$, $q = -3$. Then $N = 109$; $m = 27$; $z = 14$.

In **Table 1** $(c,d)^m$ are the quartic roots q_k of unity (9), *i.e.*,

$$\begin{aligned}R := \{&q_1 = (1,0); q_2 = (12,7) \equiv (-1,0); q_3 = (3,9) \equiv (0,-1); \\ &q_4 = (10,-2) \equiv (0,1)(\bmod(p,q))\}\end{aligned}.$$

Step-by-step process of extraction of the square roots and criteria of quadratic residuosity are illustrated for several values of (c,d).

5. Quadratic Root Extraction (*QRE*-2) Where $N \equiv 9(\bmod 16)$

5.1. Basic Properties

***Proposition* 8**: if $p \equiv 3(\bmod 8)$ and $q \equiv 0(\bmod 4)$, then

Table 1. Quadratic root extraction and verification; $N \bmod 8 = 5$.

(c,d)	(3, 8)	(4, 8)	(6, 7)	(8, −2)	(9, 2)	(10, 5)
$(c,d)^m$	(1, 0)	(10, −2)	(−1, 0)	(−1, 0)	(3, 9)	(1, 0)
$(c,d)^z$	(9, −2)	*QNR*	(5, 3)	(11, 4)	*QNR*	(2, 2)
$(c,d)^z R$	(9, −2)	*n/a*	(7, 2)	(7, −1)	*n/a*	(2, 2)
$(x,y)^2$	(3, 8)	***	(6, 7)	(8, −2)	***	(10, 5)

$m := (N-1)/8$ is *odd* and $(N+7)/16$ is an integer.

Proof: Since $p = 8w + 3$ and $q = 4r$, therefore $N = 16(4w^2 + 3w + r^2) + 9$ (2). Hence $16 \mid (N+7)$.

If we assume that m is *even*; then

$$(N+7)/16 = (m+1)/2. \tag{27}$$

Thus, if $m/2$ is integer, then $(N+7)/16$ is not (27). This contradiction proves Proposition 8.

***Proposition* 9** {criterion of Gaussian quadratic residuosity}:

Let

$$E := (c,d)^{(N-1)/8} \bmod G; \tag{28}$$

and $\|\gcd((c,d),G)\| = 1$.

Then (c,d) has a quadratic root modulo Gaussian prime G if

$$E := \{(\pm 1,0); (0,\pm 1)\} \equiv \{\pm 1; \pm i\}; \text{ {see the algorithm below}}. \tag{29}$$

***Proposition* 10**: Suppose

a) p is *odd* and $q \equiv 0(\bmod 4)$; (30)

b) $z = (N+7)/16$; (31)

c) Resolventa R satisfies the following conditions:

$$R = \begin{cases} (\pm 1, 0) \bmod G & \text{if } E = (1,0); \quad (32) \\ (0, \pm 1) \bmod G & \text{if } E = (-1,0); \quad (33) \\ \pm\sqrt{E^3} \bmod G & \text{if } E = (0, \pm 1); \quad (34) \end{cases}$$

Then

$$(c,d)^z R \equiv \sqrt{(c,d)}(\bmod G). \tag{35}$$

Proof: Notice that in (32)-(34) $R \equiv \sqrt{E^{-1}} \bmod G$.

If (35) is correct, then it implies that

$$(c,d)^{2z} R^2 \equiv (c,d)(\bmod G). \tag{36}$$

On the other hand,

$$(c,d)^{2z} R^2 \equiv (c,d)\left[(c,d)^{(N-1)/8} R^2\right](\bmod G); \tag{37}$$

therefore (28), (32)-(34) imply that

$$ER^2 \bmod (p,q) = 1. \quad (38)$$

Hence (36) is correct. In other words, it confirms assumption (35). Q.E.D.

5.2. Octadic Roots of $(1, 0)$ Modulo (p,q)

Consider roots of 8th power (called the *octadic* roots) of unity; there are eight such roots: for $k = 1, \cdots, 8$

$$e_k := \sqrt[8]{(1,0)} = \{e_{1,2} := (\pm 1,0); e_{3,4} := (0,\pm 1); e_{5,6} := \pm\sqrt{(0,1)}; e_{7,8} := \pm\sqrt{(0,-1)}\} \quad (39)$$

Then

$$e_2^2 = (1,0) = e_1;\ e_{3,4}^2 = (-1,0) = e_2;\ e_{5,6}^2 = (0,1) = e_3;\ e_{7,8}^2 = (0,-1) = e_4. \quad (40)$$

Therefore, the resolventa R must satisfy the following equations for $k = 1, 2, \cdots, 8$:

$$Re_k \bmod G = (1,0) \text{ or } R = e_k^{-1} \pmod G. \quad (41)$$

Thus, $R := e_k^{-1} = e_k$ if $k = 1,2$;

$$R := e_k^{-1} = e_k^3 = e_k^2 e_k = -e_k \text{ if } k = 3,4; \quad (42)$$

and

$$R := e_k^{-1} = e_k^7 = e_k^4 e_k^2 e_k = -e_k^2 e_k = \begin{cases} (0,-1)e_k & \text{if } k = 5,6 \\ (0,1)e_k & \text{if } k = 7,8 \end{cases}. \quad (43)$$

5.3. Computation of $\sqrt{i} \equiv \sqrt{(0,1)}$ Modulo (p,q)

If (p,q) is fixed and $N \bmod 16 = 9$, then this root must be pre-computed in advance.

Direct computation: Since

$$\sqrt{i} = \sqrt{\cos \pi/2 + i \sin \pi/2} = \cos \pi/4 + i \sin \pi/4 = (1,1)\sqrt{2}/2,$$

it is necessary to compute square root of *two* and multiplicative inverse of *two* modulo G.

5.4. Multiplicative Inverse of 2 Modulo (p,q)

If p is *odd* and q is *even*, then

$$2^{-1} \equiv ((p+1)/2, q/2) \pmod{(p,q)};$$

if q is *odd* and p is *even*, then

$$2^{-1} \equiv ((1-q)/2, p/2) \pmod{(p,q)}.$$

Otherwise the modular inverse of 2 does not exist.

***Example* 2**: Let $G = (8, -3)$; then

$2^{-1} \equiv (2,4) \pmod{(8,-3)}$ and $\sqrt{2} \equiv (5,1) \pmod{(8,-3)}$.

Hence $\sqrt{i} \equiv (1,1)(5,1)(2,4) \equiv (2,3) \pmod{(8,-3)}$ [8]. Indeed, $(2,3)^8 \equiv (1,0) \pmod{(8,-3)}$.

Indirect computation: In general, observe that if square root of 2 does not exist and for a Gaussian (a,b) holds inequality

$$F := (a,b)^{(N-1)/8} \pmod G \neq \{(\pm 1,0); (0,\pm 1)\}, \quad (44)$$

then

$$(a,b)^{(N-1)/8} \bmod G = \{\sqrt{i} \text{ or } \sqrt{-i}\}. \quad (45)$$

Although in this case we do not directly compute $\sqrt{(0,1)} \bmod G$, it is obvious that if $F^2 \bmod G = (0,1)$ (44), then

$$\sqrt{i} \equiv \sqrt{(0,1)} \equiv F \pmod G; \quad (46)$$

otherwise

$$\sqrt{i} \equiv (0,-1)\sqrt{(0,-1)} \equiv (0,-1)F \pmod G. \quad (47)$$

5.5. Algorithm for Quadratic Root Extraction

Step 1.2:

$$N := p^2 + q^2;\ m := (N-1)/8;\ z = (N+7)/16 \quad (48)$$

Step 2.2: if N is not a prime, **then** the *QRE*-2 algorithm is not applicable;

Step 3.2: Find a Gaussian (a,b), for which

$$F := (a,b)^m \bmod G \neq \{(\pm 1,0); (0,\pm 1)\}; \quad (49)$$

Step 4.2: if $F^2 = (0,1)$, **then** $R := F \equiv \sqrt{i} \pmod G$; **if** $F^2 = (0,-1)$, **then** $R := (0,-1)F \equiv \sqrt{i} \pmod G$;

Step 5.2: Compute

$$E := (c,d)^m \bmod G; \quad (50)$$

Step 6.2: if $E \neq \{(\pm 1,0); (0,\pm 1)\}$ (22), **then** square root of (c,d) does not exist;

Step 7.2: if $E = (1,0)$, **then** $(x,y) := (c,d)^z \bmod G$; **goto** Step 10.2;

Step 8.2: if $E = (-1,0)$, **then** $(x,y) := (c,d)^z (0,1) \bmod G$; **goto** Step 10.2;

Step 9.2: if $E = (0,1)$, **then**

$$(x,y) := (c,d)^z \left[(0,1)R\right] \bmod G; \text{ goto Step 10.2;} \quad (51)$$

else

$$(x,y) := (c,d)^z R \bmod G; \quad (52)$$

Step 10.2 {2nd square root}:

$$(t,v) := (p-1,q)(x,y) \bmod G. \quad (53)$$

6. Second Numeric Illustration

Consider $(p,q)=(8,-3)$, then $N=73$, *i.e.*,

$$73\equiv 9 \pmod{16};\ m=9;\ z=5; \tag{54}$$

Octadic roots of $(1, 0)$**:**

$$e_1=(10,5)^2\equiv(1,0);$$

$$e_2=(10,5)\equiv(-1,0)\pmod{(8,-3)};$$

$$(8,-2)^2\equiv(10,5);\ e_3=(8,-2)\equiv(0,1);$$

$$(3,7)^2\equiv(10,5);\ e_4=(3,7)\equiv(0,-1);$$

$$(2,3)^2\equiv(8,-2);\ e_5=(2,3)\equiv\sqrt{(0,1)};$$

$$(9,2)^2\equiv(8,-2);\ e_6=(9,2)\equiv-\sqrt{(0,1)};$$

$$(5,-1)^2\equiv(3,7);\ e_7=(5,-1)\equiv\sqrt{(0,-1)};$$

$$(6,6)^2\equiv(3,7);\ e_8=(6,6)\equiv-\sqrt{(0,-1)}.$$

The following nine values of (c,d) in **Table 2** illustrate various cases of *QRE*-2 algorithm.

7. Quadratic Root Extraction (*QRE*-3) Where $N\equiv 17 \pmod{32}$

7.1. Basic Property and Roots of $(1, 0)$

***Proposition* 11**: Analogously it can be proved that if $p\equiv\pm 7 \pmod{16}$ and $q\equiv 0 \pmod 8$, then $(N+15)/32$ is integer and $m:=(N-1)/16$ is *odd*.

Proof: Let $p=16k\pm 7$ and $q=8r$; then $N=32\left[k(8k\pm 7)+2\right]+49$, *i.e.*, $32\left|(N+15)\right.$.

Notice that $(N+15)/32=(m+1)/2$. On the other hand, if m is *even*, then $(m+1)/2$ is not an integer, which implies that $(N+15)/32$ is not an integer. Q.E.D.

***Definition* 2:** u_i is a *square* root of $(1, 0)$ if

$$u_i^2\equiv(1,0)\pmod{G},\ i=1,2. \tag{55}$$

***Definition* 3:** q_j is a *quartic* root of $(1, 0)$ if

$$q_j^4\equiv(1,0)\pmod{G},\ j=1,2,3,4. \tag{56}$$

***Definition* 4:** e_k is a *octadic* root of $(1, 0)$ if

$$e_k^8\equiv(1,0)\pmod{G},\ k=1,2,\cdots,8. \tag{57}$$

***Definition* 5**: s_l is a *sedonic* root of $(1, 0)$ if

$$s_l^{16}\equiv(1,0)\pmod{G},\ l=1,2,\cdots,16. \tag{58}$$

7.2. Resolventa of Quadratic Root Extractor

***Proposition* 12**: Suppose

a) $p\equiv\pm 7 \pmod{16}$ and $q\equiv 0 \pmod 8$, (59)

b) $L:=c^2+d^2;\ z=(N+15)/32;\ m:=(N-1)/16$ (60)

c) Let $E:=(c,d)^m \bmod(p,q)$; and resolventa R satisfies the following conditions:

$$R:=\pm\sqrt{u_i^{-1}}\equiv\pm\sqrt{u_i}\pmod{G}\ \text{if}\ E=u_i; \tag{61}$$

$$R:=\pm\sqrt{q_j^{-1}}\equiv\pm\sqrt{q_j^3}\pmod{G}\ \text{if}\ E=q_j; \tag{62}$$

$$R:=\pm\sqrt{e_k^{-1}}\equiv\pm\sqrt{e_k^7}\pmod{G}\ \text{if}\ E=e_k; \tag{63}$$

$$R:=\pm\sqrt{s_l^{-1}}\equiv\pm\sqrt{s_l^{15}}\pmod{G}\ \text{if}\ E=s_l; \tag{64}$$

then

$$(c,d)^z R=\sqrt{(c,d)}\pmod{G}. \tag{65}$$

Proof: Let

$$(x,y):=(c,d)^z R=\sqrt{(c,d)}\pmod{G}. \tag{66}$$

Therefore

$$(c,d)^{(N+15)/16}R^2=(c,d)ER^2\pmod{G}. \tag{67}$$

If $E=u_i$, then

$$ER^2=E^2=u_i^2=(1,0)\pmod{G}; \tag{68}$$

if $E=q_j$, then

$$ER^2=E^4=q_j^4=(1,0)\pmod{G}; \tag{69}$$

if $E=e_k$, then

Table 2. Quadratic root extractor where $N\equiv 9 \pmod{16}$.

(c,d)	(1, 1)	(3, −1)	(3, 4)	(4, 3)	(5, 1)	(5, 5)	(7, −1)	(8, 5)	(10, 3)
$(c,d)^m$	(2, 3)	(0, 1)	(0, −1)	(0, −1)	(1, 0)	(0, 1)	(9, 2)	(8, −2)	(−1, 0)
$(c,d)^z$	*n/a*	(8, 5)	(3, 6)	(5, 7)	(1, 2)	(8, 1)	*n/a*	(3, −1)	(9, 19)
$(c,d)^z R$	*n/a*	(4, 5)	(9, 4)	(4, 1)	(1, 2)	(5, 4)	*n/a*	(2, 2)	(7, 6)
$(x,y)^2$	*n/a*	(3, −1)	(3, 4)	(4, 3)	(5, 1)	(5, 5)	*n/a*	(8, 5)	(10, 3)

***NB*1**: If $E=\{e_5,\cdots,e_8\}$, then *QRE*-2 algorithm is not applicable, since the square roots of $e_5,\cdots,e_8$ do not exist.

$$ER^2 = E^8 = e_k^8 = (1,0)(\bmod G); \quad (70)$$

if $E = s_l$, then

$$ER^2 = E^{16} = s_l^{16} = (1,0)(\bmod G). \quad (71)$$

7.3. Sedonic Roots of $(1, 0)$ Modulo *G*

Unity $(1, 0)$ has two square roots $\{(1, 0)$ and $(-1, 0)\}$; four quartic roots $\{(1, 0); (-1, 0); (0, 1); (0, -1)\}$; eight octadic roots $\{(1, 0); (-1,0); (0, 1); (0,-1); e_5, e_6, e_7, e_8\}$ and sixteen sedonic roots $\{\{(1, 0); (-1, 0); (0, 1); (0, -1), e_5, e_6, e_7, e_8, s_9, s_{10}, \cdots, s_{15}, s_{16}\}$, where

$$e_{5,6} = \pm\sqrt{(0,1)},\ e_{7,8} = \pm\sqrt{(0,-1)} \text{ and}$$
$$s_{9,10,11,12} = \pm\sqrt{\pm\sqrt{(0,1)}},\ s_{13,14,15,16} = \pm\sqrt{\pm\sqrt{(0,-1)}}. \quad (72)$$

7.4. Third Numeric Illustration

Consider $N = 113$; $(p,q) = (8,-7)$. Then
$m := (N-1)/16 = 7$; $z := (N+15)/32 = 4$.

In **Table 3** below $(-1,0) \equiv (14,1)$; $(0,1) \equiv (8,-6)$;
$(0,-1) \equiv (7,7)(\bmod(8,-7))$; $\sqrt{(0,-1)} \equiv (6,5)$;
$-\sqrt{(0,-1)} \equiv (9,-4)$; $\sqrt{(0,1)} \equiv (3,-1)$;
$-\sqrt{(0,1)} \equiv (12,2)(\bmod(8,-7))$;

$$-\sqrt{\pm\sqrt{(0,\pm1)}} \equiv \{(10,5);(12,-2);(10,-2);(5,-2)\}(\bmod(8,-7)); \quad (73)$$

$$\sqrt{\pm\sqrt{(0,\pm1)}} \equiv \{(5,-4);(3,3);(5,3);(10,3)\}(\bmod(8,-7)). \quad (74)$$

In (74) there are four sedonic roots of (1,0) that must be pre-computed on the design stage of the *QRE*-3 algorithm. Although this is a non-deterministic process, each of these roots must be computed only once prior to using the extractor. These roots correspond to

$$E := (g,h)^m \equiv \sqrt[16]{(1,0)}(\bmod G),$$

where $m = 7$; $G = (p,q) = (8,-7)$ and Gaussians $(g,h) := \{(6,3);(10,1);(11,3);(5,4)\}$.

The remaining four sedonic roots listed in (73) are equivalent to negative values of roots in (74):

$$(10,5) \equiv -(5,-4);(12,-2) \equiv -(3,3);(10,-2) \equiv -(5,3);(5,-2) \equiv -(10,3).$$

8. Cryptographic Algorithm

Step 1.3 {***System design***}: Every user (Alice, Bob,⋯) selects a pair of Gaussian primes (p,q) and (r,s) as her/his private keys, and computes $n := (p,q)(r,s)$ as her/his public key; she/he pre-computes $N = p^2 + q^2$, *m*, *z* and *R*;

Step 2.3 {Generalized Chinese remainder Theorem modulo composite Gaussian *n*}: Each user pre-computes his/her parameters of CRT:

$$M := (p,q)^{-1} \bmod(r,s);\ W := (r,s)^{-1} \bmod(p,q). \quad (75)$$

Step 3.3 {***Encryption*** by sender (Alice)}: Alice represents the plaintext as an array of Gaussians and inserts digital isotopes into every Gaussian (a,b) [3];

Step 4.3: Using Bob's public key *n*, she computes ciphertext

$$C := (a,b)^2 \bmod n; \quad (76)$$

and transmits *C* to receiver (Bob) via open channels of a communication network;

Step 5.3 {***Decryption*** by receiver (Bob)}: He computes square roots of *C* mod (p,q) and mod (r,s), where (p,q) and (r,s) are Bob's private keys;

Step 6.3: Using the CRT and his pre-computed *M* and *W* (75), Bob computes all quadratic roots of ciphertext *C*;

Step 7.3: Bob recovers the initial plaintext {by select-

Table 3. Binary tree of sedonic roots of $(1, 0)$ where modulus $G = (8, -7)$.

(g,h)	(6, 3)	*	(10, 1)	*	*	(11, 3)	*	(5, 4)	*
$E = \sqrt[16]{(1,0)}$	**(5, −4)**	**(10, 5)**	**(3, 3)**	**(12, −2)**	*	**(5, 3)**	**(10, −2)**	**(10, 3)**	**(5, −2)**
$E^2 = \sqrt[8]{(1,0)}$	*	**(6, 5)**	**(9, −4)**	*	*	*	**(3, −1)**	**(12, 2)**	*
$E^4 = \sqrt[4]{(1,0)}$	*	*	**(7, 7)**	*	*	*	**(8, −6)**	*	*
$E^8 = \sqrt{(1,0)}$	*	*	*	*	**(−1, 0)**	*	*	*	*
E^{16}	*	*	*	*	**(1, 0)**	*	*	*	*

***NB*2:** For the sake of brevity, only 1/2 of all roots are listed in every row of **Table 3**; all remaining roots are listed in the rows below. For instance, $\sqrt[8]{(1,0)} = \{(6,5);(9,-4);(3,-1);(12,2);$ and $(7,7);(8,-6);$ and $(-1,0);$ and $(1,0)\}$.

Table 4. Residues, applicable square root extractors and examples of corresponding *N*.

***N* mod 32**	**5**	**9**	**13**	**17**	**21**	**25**	**29**
QRE	*QRE*-1	*QRE*-2	*QRE*-1	*QRE*-3	*QRE*-1	*QRE*-2	*QRE*-1
N_1	260773	692969	432589	386641	612373	525913	906557
(p,q)	(113, 498)	(212, 805)	(258, 605)	(375, 496)	(522, 583)	(157, 708)	(421, 854)
N_2	812101	249257	360781	676337	159157	405529	750077
(p,q)	(351, 830)	(16, 499)	(275, 534)	(464, 679)	(174, 359)	(48, 635)	(11, 866)

ing the quadratic root of *C* that has digital isotopes [9]}.

This algorithm is a generalization of the Rabin cryptographic algorithm [10], which employs the square root algorithm for encryption and decryption of real integers modulo semi-prime $n = pq$, where *p* and *q* are primes.

9. Reduction of Computational Complexity

In Step 3.1 (12) and Step 4.1 (13), two exponentiations are performed to compute (c,d) to the powers *m* and *z* respectively; these operations are the most time-consuming.

However, observe that there is a simple linear relationship between *m* and *z*:

$$2(z-1) = m-1 \quad \{=(N-5)/4\}. \tag{77}$$

This implies that it is sufficient to execute only one exponentiation. Indeed, we initially compute

$$A_1 := (c,d)^{z-1} \bmod G \text{ ; \{one exponentiation\};} \tag{78}$$

then

$$A_2 := A_1^2 \bmod G = \left\{(c,d)^{2(z-1)}\right\} \text{ ; \{one squaring\};} \tag{79}$$

after that

$$A_3 := A_2 \times (c,d) = \left\{(c,d)^{m}\right\} \text{ ; \{one multiplication\};} \tag{80}$$

and finally $A_4 := A_1 \times (c,d) = \left\{(c,d)^{z}\right\}$; {one multiplication}. (81)

10. Applicability of *QRE* Algorithms

Consider $A := N \bmod 32$, where *N* are primes, which can be represented as a sum of two integer squares. For such *N* the residues are equal $A := \{1, 5, 9, 13, 17, 21, 25 \text{ and } 29\}$. **Table 4** above indicates which algorithm is applicable for each value of residue *A*.

Therefore, the three algorithms provided in this paper cover all cases of prime moduli with the exception of $N \equiv 1 \pmod{32}$. Yet, most of the moduli in the latter case can still be covered if we consider *QRE* algorithms, where the primes $N \equiv 33 \pmod{64}$; $N \equiv 65 \pmod{128}$; and in general, for integer $t \geq 5$ the algorithms described above can be generalized for the cases where

$$N \equiv \left(2^t + 1\right) \left(\bmod 2^{t+1}\right), \tag{82}$$

and the *even* component in the corresponding modulus (p,q) is divisible by 2^{t-1}.

11. Conclusion and Acknowledgements

Three algorithms which extract square roots of Gaussians in arithmetic, based on *Gaussian* modulo reduction, are considered and analyzed in this paper. Several numeric illustrations provide further explanation of these algorithms. A public key encryption/decryption protocol based on this arithmetic is described in the paper. This cryptographic protocol is almost twice as fast as the analogous protocols published by the author of this paper in [3,4].

I appreciate S. Medicherla, S. Sadik and B. Saraswat for assistance in numeric illustrations and my gratitude to J. Jones, A. Koval, M. Linderman, R. Rubino and anonymous reviewers and the typesetter for their suggestions that improved this paper.

12. References

[1] C. F. Gauss, "Theoria Residuorum Biquadraticorum," 2nd Edition, Chelsea, New York, 1965, pp. 534-586.

[2] M. Kirsch, "Tutorial on Gaussian Arithmetic Based on Complex Modulus," 2008. http://wlym.com/~animations/ceres/index.html

[3] B. Verkhovsky, "Information Protection Based on Extraction of Square Roots of Gaussian Integers," *International Journal of Communications*, *Network and System Sciences*, Vol. 4, No. 3, 2011, pp. 133-138. doi:10.4236/ijcns.2011.43016

[4] B. Verkhovsky and A. Koval, "Cryptosystem Based on Extraction of Square Roots of Complex Integers," In: S. Latifi, Ed., *Proceedings of 5th International Conference on Information Technology*: *New Generations*, Las Vegas,

7-9 April 2008, pp. 1190-1191.

[5] E. Bach and J. Shallit, "Efficient Algorithm," *Algorithmic Number Theory*, Vol. 1, MIT Press, Cambridge, MA, 1996.

[6] R. Crandall and C. Pomerance, "Prime Numbers: A computational Perspective," Springer, New York, 2001.

[7] R. Schoof, "Elliptic Curves over Finite Fields and the Computation of Square Roots Mod *p*," *Mathematics of Computation*, Vol. 44, No. 170, 1985, pp. 483-494.

[8] R. V. Churchill, J. W. Brown and R. F. Verhey, "Complex Variables and Applications," 3rd Edition, McGraw Hill, New York, 1976.

[9] B. Verkhovsky, "Cubic Root Extractors of Gaussian Integers and Their Application in Fast Encryption for Time-Constrained Secure Communication," *International Journal of Communications*, *Network and System Sciences*, Vol. 4, No. 4, 2011, pp. 197-204. doi:10.4236/ijcns.2011.44024

[10] M. Rabin, "Digitized Signatures and Public-Key Functions as Intractable as Factorization," MIT/LCS Technical Report, TR-212, 1979.

Appendix

A1. Classification of Roots of $(1, 0)$ Modulo (p,q)

There are various types of unary roots:

Definitions and notations:

$$S_1 := \pm\sqrt{(1,0)} \bmod((p,q)) = \{s_{11}, s_{12}\}; \quad \text{(A.1)}$$

where

$$P_1 := -\sqrt{(1,0)} \bmod((p,q)) = \{p_{11}\} \quad \text{(A.2)}$$

is the set of principal square roots of (1,0) of the first level. Then

$$S_2 := \left\{\pm\sqrt{s_{1k}} \bmod((p,q))\right\},\ k = 1,2; \quad \text{(A.3)}$$

where

$$P_2 := \pm\sqrt{p_{11}} \equiv \{p_{2k}\} \bmod((p,q));\ k = 1,2; \quad \text{(A.4)}$$

is the set of principal square roots of (1,0) of the second level.

In general,

$$S_i := \left\{\pm\sqrt{s_{i-1,k}}\right\} \bmod((p,q)); \quad \text{(A.5)}$$

where

$$P_i := \left\{\pm\sqrt{p_{i-1,k}} \bmod((p,q))\right\} \quad \text{(A.6)}$$

is the set of principal square roots of (1,0) of the *i*-th level.

A2. Criterion of Quadratic Residuosity and General Algorithm

Proposition 1.A: Let $N \bmod 2^k = 2^{k-1} + 1$.

If and only if

$$E := (c,d)^{(N-1)/2^{k-1}} \bmod G \in S_{k-1}, \quad \text{(A.7)}$$

then (c,d) has a square root. In this case

$$R := \pm\sqrt{E^{-1}} \bmod G; \quad \text{(A.8)}$$

and

$$(x,y) = R(c,d)^{\left(N+2^{k-1}-1\right)/2^k} \left(\bmod G\right). \quad \text{(A.9)}$$

A3. Quadratic Extractor Modulo $(n, -1)$

Proposition 2.A: Let $N = \|(n,-1)\|$ be a prime;

$$N \bmod 4 = 1, \text{ but } N \bmod 8 \neq 1. \quad \text{(A.10)}$$

If the norm of (c,d) is co-prime with *N*, then square root (x,y) of (c,d) is equal

$$(x,y) = R \times (c,d)^{\left(n^2+4\right)/8} \bmod(n,-1); \quad \text{(A.11)}$$

where

$$R = \left[\sqrt{(c,d)^{n^2/4}}\right]^{-1} \bmod(n,-1). \quad \text{(A.12)}$$

Proof: First of all, if $N = n^2 + 1$ is a prime integer, then *n* is *even*. Therefore (A.10) implies that $n^2/4$ and $\left(n^2+4\right)/8$ are integers. Then (A.11) and (A.12) imply that

$$(x,y)^2 \equiv R^2 \times (c,d)^{n^2/4} (c,d) \equiv (c,d) \bmod(n,-1). \quad \text{(A.13)}$$

Since the cyclic identity (4) implies that $(c,d)^{n^2} \equiv (1,0)\left(\bmod(n,-1)\right)$, then potentially

$$\sqrt{(c,d)^{n^2/4}} \bmod(n,-1) = \left\{(\pm 1,0);(0,\pm 1);\pm\sqrt{(0,\pm 1)}\right\}. \quad \text{(A.14)}$$

Therefore,

$$R = \begin{cases} (\pm 1,0) \text{ if } (c,d)^{n^2/4} = (1,0); \\ \pm(0,1) \text{ if } (c,d)^{n^2/4} = (-1,0); \\ \pm\sqrt{(0,1)} \text{ if } (c,d)^{n^2/4} = (0,-1); \\ \pm(0,1)\sqrt{(0,1)} \text{ if } (c,d)^{n^2/4} = (0,1). \end{cases} \quad \text{(A.15)}$$

Since $\sqrt{(0,1)} \equiv (1,1)\sqrt{2}/2\left(\bmod(n,-1)\right)$ {see Subsections 5.3}, then *R* does not exist if $\sqrt{2}$ does not exist [1,6]. Therefore (c,d) is the Gaussian *QNR* [3]. For more details see (32)-(34), (A.11), (A.12), Subsection 5.4 and eight examples in **Table A1**.

Remark A1: Here $\pm(1,9)$ and $\pm(10,0)$ are quartic roots of $(1,0)$ modulo $(10,-1)$. Indeed,

$$\begin{aligned} &q_3 = (10,0) \equiv (0,1)\left(\bmod(10,-1)\right); \\ &q_4 = (1,9) \equiv (0,-1)\left(\bmod(10,-1)\right); \quad (9) \\ &q_3^2 = (10,0)^2 \equiv (-1,0)\left(\bmod(10,-1)\right) = q_2; \\ &q_4^2 = (1,9)^2 \equiv (-1,0) \equiv (10,9) = q_2. \end{aligned}$$

A4. Special Cyclic Identity

Proposition 3.A: If $N := \|(p,q)\|$ is prime, then

$$(q,p)^{N-1} \equiv (1,0)\left(\bmod(p,q)\right). \quad \text{(A.16)}$$

Remark A2: Although $\|(p,q)\| = \|(q,p)\|$, identity (A.16) holds because (p,q) and (q,p) are co-prime. Indeed, assumption that $(p,q)(u,w) \equiv (q,p)\left(\bmod(p,q)\right)$, where both *u* and *w* are integers, implies that

$$u \equiv (p+q)/N \text{ and } w \equiv (q-p)/N \left(\bmod(p,q)\right). \quad \text{(A.17)}$$

However, (A.17) is impossible since the inverse of *N* modulo (p,q) does not exist.

Table A1. {Quadratic root extraction where $N \bmod 4 = 1$ and $N \bmod 8 \neq 1$ }: $(n,-1)=(10,-1)$; $m := (n/2)^2 = 25$; $z := (m+1)/2 = 13$.

(c,d)	**(2,0)**	**(3,2)**	**(4,8)**	**(6,7)**	**(7,4)**	**(9,2)**	**(9,9)**	**(10,1)**
$(c,d)^{(n/2)^2}$	(0, −1)	(−1, 0)	(1, 0)	(−1, 0)	(−1, 0)	(0, 1)	(0, 1)	(−1, 0)
$(c,d)^z$	*GQNR*	(9, 4)	(6, 3)	(6, 9)	(5, 8)	*GQNR*	*GQNR*	(9, 0)
R	n/a	±(10, 0)	(1, 0)	±(1, 9)	±(10, 0)	n/a	n/a	±(1, 9)
$(x,y)=(c,d)^z R$	n/a	**±(6, 8)**	**±(6, 3)**	**±(1, 5)**	**±(2, 4)**	n/a	n/a	**±(10, 8)**
$(x,y)^2$	***	(3, 2)	(4, 8)	(6, 7)	(7, 4)	***	***	(10, 1)

***Example* 1.A**: $(-4,10)^{28} \bmod (5,-2) = (1,0)$, although $\gcd\left[\|(-4,10)\|, \|(5,-2)\|\right] = 29 \neq 1$.

***Corollary* 1A:** If $\gcd\left[(s,t),(p,q)\right] = (1,0)$, then

$$\left[(s,t)(q,p)\right]^{N-1} \equiv (1,0)\left(\bmod(p,q)\right) \qquad \text{(A.18)}$$

***Proposition* 4.A:** If n and r in modulus $(n,-r)$ have different parities, then multiplicative inverse of $(-r,n)$ modulo $(n,-r)$ exists and equals

$$(-r,n)^{-1} \equiv (n-r)^{-1}\left[(n-r+1,-n-r-1)/2\right]\left(\bmod(n,-r)\right). \qquad \text{(A.19)}$$

Proof: First of all,

$$(-r,n) \equiv (n-r)(1,1)\left(\bmod(n,-r)\right). \qquad \text{(A.20)}$$

Now let's find integers x and y such that

$$(1,1)(x,y) \equiv (1,0) \equiv (n+1,-r)\left(\bmod(n,-r)\right) \qquad \text{(A.21)}$$

i.e., $x - y = n + 1$; $x + y = -r$.

Hence

$$x = (n-r+1)/2;\ y = (-n-r-1)/2. \qquad \text{(A.22)}$$

Therefore, (A.20) and (A.22) imply

$$(-r,n)(-r,n)^{-1} \equiv \left[(n-r)(1,1)\right](n-r)^{-1}(1,1)^{-1} \equiv$$
$$\equiv (-r,n)\left\{(n-r)^{-1}\left[(n-r+1,-n-r-1)/2\right]\right\} \equiv$$
$$\equiv (1,0)\left(\bmod(n,-r)\right). \quad \text{Q.E.D.} \qquad \text{(A.23)}$$

***Example* 2.A**: Let $n = 10$, $r = 3$. Then $(-3,10)^{-1} \equiv 7^{-1}(4,-7) \equiv (2,1)(4,-7) \equiv (8,3)$.

Indeed, $(-3,10)(8,3) \equiv (1,0)\left(\bmod(10,-3)\right)$.

***Corollary* 2A:** If n and r in modulus (n,r) have different parities and there exists multiplicative inverse of (a,b), then multiplicative inverse of $(r,n)(a,b) \bmod (n,r)$ also exists.

