A Note on Quadratic Residuosity and UP

Jin-Yi Cai [a,*] Robert A. Threlfall [b]

[a] *Computer Sciences Department, University of Wisconsin, 1210 West Dayton St, Madison, WI 53706, USA*

[b] *B & C Group International, 955 Broadway Drive, Sun Prairie, WI 53590, USA*

Abstract

UP is the class of languages accepted by polynomial-time nondeterministic Turing machines that have at most one accepting path. We show that the quadratic residue problem belongs to UP ∩ coUP. This affirmatively answers an open problem, discussed in *Theory of Computational Complexity* (Du and Ko, 2000), of whether the quadratic nonresidue problem is in NP. We generalize to higher powers and show the higher power residue problem belongs to UP ∩ coUP.

Key words: Computational complexity, UP, One-way functions, Quadratic residuosity, Higher power residuosity

1 Introduction

The complexity class UP was defined by Valiant[19], see also [18,3,4].

* Corresponding author. (Research supported in part by NSF CCR-0208013.)
Email addresses: jyc@cs.wisc.edu (Jin-Yi Cai), rt@secure-systems.org (Robert A. Threlfall).

Definition 1

(1) A nondeterministic Turing machine (NTM) is unambiguous if, for every input, the machine has at most one accepting computation path.

(2) UP is the class of languages accepted by polynomial-time unambiguous nondeterministic Turing machines.

From the definition it is immediately apparent that P $\subseteq$ UP $\subseteq$ NP. It is not known if either inclusion is strict, although it is widely believed that both inclusions are strict. In particular, Hartmanis and Hemachandra [9] conjectured that UP does not have complete languages, which has a consequence that P $\neq$ UP $\neq$ NP.

The notion of UP has proved useful in the context of structural complexity theory. It characterizes the complexity of certain weak one-way functions.

Berman [3], Ko [12] and Grollmann and Selman [8] independently showed that P $\neq$ UP if and only if there exist one-to-one one-way functions according to the definition in [6, page 120]. Roughly, this definition states that a function f is polynomial time computable, but is not polynomial time invertible [1]. (While there are more stringent and widely used definitions of cryptographic one-way functions [13], they are probably not equivalent to this definition and no clean cut condition for their existence in terms of complexity classes has yet been found.)

[1] See Selman's 1992 [17] survey paper for the history of this theorem and other interesting results on one-way functions and complexity theory [17].

Rabin [15] showed finding square roots modulo n is random polytime computationally equivalent to factoring n, but it is not known if the factoring problem polytime reduces to the quadratic residue problem. Whereas, Manders and Adleman [14] showed that given positive integers a, c and n, determining if there is a positive integer $x < c$ such that $x^2 \equiv a \pmod{n}$ is NP-complete, even if the factorization of n is given.

Watnatabe pointed out that the work of Fellows and Koblitz [7] implies that Primality is in UP $\cap$ coUP. This has been superceeded by the recent AKS proof that Primality is in P [1].

In section 2 we show the quadratic nonresidue problem (QNR) is in UP $\cap$ coUP. In section 3 we generalize to higher power residuosity [2] (HPR) and show HPR also is in UP $\cap$ coUP. In both problems the only place nondeterminism is used is in the prime factorization of the modulus n.

[2] Aka "residuacity", a spelling which has a longer history, see [5].

2 Quadratic Residuosity in UP ∩ coUP

Definition 2

(1) For integer $n > 1$, $\mathbb{Z}_n^* = \{x \in \mathbb{Z} : 0 < x < n, \gcd(x, n) = 1\}$. *In other words,* $\mathbb{Z}_n^*$ *is the multiplicative group of integers relatively to* n.

(2) An integer $a \in \mathbb{Z}$, *with* $a \pmod n \in \mathbb{Z}_n^*$, *is a quadratic residue (QR) mod* n *if* $a \equiv x^2 \pmod n$, *for some* $x \in \mathbb{Z}_n^*$; *and* a *is a quadratic nonresidue (QNR) mod* n *otherwise.*

Definition 3

(1) Quadratic Residue Problem (QR) – given integers (a, n), *all written in binary, where* $n > 1$ *and* a *is relatively prime to* n, *determine if* a *is a quadratic residue mod* n, *i.e., if there exists* $x \in \mathbb{Z}_n^*$, *such that* $x^2 \equiv a \pmod n$.

(2) Quadratic Nonresidue Problem (QNR) – the complementary problem of determining if a *is a quadratic nonresidue mod* n.

Note that, as is traditionally done, we restrict to those integers a relatively prime to n. These two problems (QR and QNR) can be regarded as complementary, for one efficiently can check whether a is relatively prime to n in $O(\lg a \cdot \lg n)$ bit operations, where $\lg u$ equals the number of bits in the binary representation of the integer u, excepting the sign bit [2, pages 41 and 67-70].

While it is clear that QR is in NP (or equivalently QNR is in coNP), the membership of QNR in NP has escaped notice and remained an open problem.

In their recent book Du and Ko specifically comment that it is unknown whether QNR $\in$ NP (see [6] page 356). We give a simple proof that QNR $\in$ NP by showing that both QR and QNR are in UP $\cap$ coUP.

2.1 Preliminaries

We start by recalling some basic number theory.

Criterion 4 *(Euler) [11]–For any odd prime p and $a \in \mathbb{Z}_p^*$ we have $a^{(p-1)/2} \,(mod\, p) = 1$ when a is a QR mod p, and $= -1$ when a is a QNR mod p – for $a \in \mathbb{Z}_p^*$ there are no other possibilities.*

This follows easily from the fact that $\mathbb{Z}_p^*$ is a cyclic group of order $p-1$.

The next few Lemmas are all known. For the convenience of the readers we include short proofs.

Lemma 5 *If a is a* QR *mod p and p is an odd prime, then a is a* QR *mod p^i, for all $i \geq 1$.*

Proof of Lemma 5. Proof by induction on i. Given $x^2 \equiv a \bmod p^i$, for some $i \geq 1$, then $x^2 \equiv a + bp^i \bmod p^{i+1}$ for some b. We let $y = x + \alpha p^i$, where $\alpha \equiv -(2x)^{-1}b \pmod p$, then $y^2 \equiv a \bmod p^{i+1}$. □

Lemma 6 *If a is a QR mod 8, then a is QR mod 2^k, for all $k \geq 1$.*

Proof of Lemma 6. If a is a QR mod 8, then a is a QR mod 2 and 4. Inductively, let $x^2 \equiv a \bmod 2^k$ for some $k \geq 3$. Then $x^2 = a + b2^k \bmod 2^{k+1}$.

Let $y = x - b2^{k-1}$, then

$$\begin{aligned} y^2 &= x^2 - 2xb2^{k-1} + b^2 2^{2k-2} \\ &\equiv a + b2^k - b2^k \bmod 2^{k+1} \qquad (1) \\ &\equiv a \bmod 2^{k+1} \end{aligned}$$

where equation (1) follows from the fact that x is odd and $2k - 2 \geq k + 1$. □

For $a \in \mathbb{Z}^*_{2^k}$, where $k = 1, 2$ or 3, the test for quadratic residuosity is trivial: a is a quadratic residue mod 2^k if and only if $a \equiv 1 \bmod 2^k$.

Lemma 7 *Let $n = q_1 q_2 \cdots q_m$ be the unique prime factorization of n, where $q_i = p_i^{\alpha_i}$, $\alpha_i > 0$, each p_i is a prime number, and $p_1 < p_2 < \cdots < p_{m-1} < p_m$. Then, a is a* QR *mod n if and only if a is a* QR *for each prime power q_i of n. Furthermore, a is a* QR *mod n if and only if the following conditions are met.*

(1) For each odd prime factor, p_i, a is a QR*.*

(2) When n is even, a is a QR mod $2^{\min\{3,\alpha_1\}}$, where $p_1 = 2$ and $\alpha_1 > 0$.

Proof of Lemma 7. By the Chinese Remainder Theorem, the square root of $a \pmod n$ exists if and only if it exists for each modulus q_i, since the q_i are pair-wise relatively prime. The rest follows from Lemmas 5 and 6. □

Euler's totient function is defined as $\phi(n) = |\mathbb{Z}^*_n|$. For p^s, p a prime number, $\phi(p^s) = p^{s-1}(p-1)$. A primitive root of a number n is an integer g such that g has order $\phi(n)$ modulo n. In other words, g is a multiplicative generator of $\mathbb{Z}^*_n$.

2.2 Membership of QR and QNR in UP

Theorem 8 QNR *and* QR *are in* $\mathrm{UP} \cap \mathrm{coUP}$.

PROOF. We show membership of QNR and QR in UP. Define a polynomial-time NTM M as follows. Given input (a, n), M first verifies that $n > 1$ and $\gcd(a, n) = 1$. Then M on each computation path guesses the prime factors p_i in ascending order, with multiplicities $\alpha_i > 0$, where $1 \leq i \leq r$, and $1 \leq r \leq \lfloor \log_2 n \rfloor$. Verify that p_i are primes, and $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$. Primality can be verified in deterministic polynomial time using the recent AKS result that Primality is in P [1]). By unique factorization exactly one path finds the correct factorization, and all paths except this one are terminated.

Next, deterministically for every odd prime p_i, we have M compute $x_i = a^{(p_i-1)/2} (\mathrm{mod}\, p_i)$. If n is even, say $p_1 = 2$, we check if a is a QR mod 2^i, by inspection; namely we set $x_1 = 1$ if and only if $a \equiv 1 \bmod 2^{\min\{3,i\}}$ (and set $x_1 = -1$ otherwise). Then clearly a is a QNR mod n if and only if some $x_i = -1$, and M accepts. And a is a QR if and only if all $x_i = 1$. □

Remark 9 *Verifying the primality of the factorization of n can also be done unambiguously by the result of Watanabe [7] that Primality is in* $\mathrm{UP} \cap \mathrm{coUP}$.

Corollary 10 QNR *is in* $\mathrm{NP} \cap \mathrm{coNP}$.

This answers the question of Du and Ko [6].

3 Higher Power Residuosity

In this section we consider the natural generalization of quadratic residuosity to higher power residuosity. We show that this problem is also in UP $\cap$ coUP.

Definition 11 *Higher power residue problem (HPR) – given integers (a, k, n), all written in binary, where $n > 1$, $k \geq 1$, and a is relatively prime to n, determine if a is a kth power residue mod n, i.e., if there exists $x \in \mathbb{Z}_n^*$, such that $x^k \equiv a \pmod{n}$.*

This problem has relevance with the RSA cryptosystem [16]. Note that we write the modulus and the exponent as binary numbers.

Our approach is the same as for QNR. We first reduce the problem to the k-th power residues mod prime powers of n. For odd prime powers p^s, we can use a generalized Euler's criterion which follows from the cyclic structure of the group $\mathbb{Z}_{p^s}^*$. We have to work just a little harder for prime powers 2^s if n is even.

3.1 Preliminaries

Theorem 12 *(Gauss)* [10]*. The only numbers that have primitive roots are $2, 4, p^s$ and $2p^s$, where p is an odd prime and $s \geq 1$.*

Theorem 13 [10] *Given $s \geq 3$, then for any odd a, there exists a unique $0 \leq t < 2^{s-2}$ such that*

$$a \equiv (-1)^{\frac{a-1}{2}} 5^t \pmod{2^s}.$$

In other words, the multiplicative group $\mathbb{Z}_{2^s}^*$ of order 2^{s-1} is isomorphic to the

direct product $\mathbb{Z}_2 \times \mathbb{Z}_{2^{s-2}}$*, with generators* -1 *and* 5 *respectively.*

The following lemma follows from the Chinese Remainder Theorem.

Lemma 14 *Let* $n = q_1 q_2 \cdots q_m$ *be the unique prime factorization of* n*, where* $q_i = p_i^{\alpha_i}$*,* $\alpha_i > 0$*, each* p_i *is a prime number, and* $p_1 < p_2 < \cdots < p_{m-1} < p_m$*. Then,* a *is a* k*-th power residue mod* n *if and only if* a *is a* k*-th power residue mod each prime power* q_i *of* n*.*

Criterion 15 *(Euler) Let* p *be an odd prime,* $\gcd(a, p) = 1$ *and* $d = \gcd(k, \phi(p^s))$*, then* a *is a* k*th power residue* $(mod\ p^s)$ *if and only if* $a^{\phi(p^s)/d} \equiv 1 \pmod{p^s}$*.*

To prove this criterion we need the following lemma.

Lemma 16 *Let* p *be an odd prime, and* a, k *and* s *be integers,* $k, s \geq 1$*,* $(a, p) = 1$*, and let* $d = \gcd(k, \phi(p^s))$*. Then* $x^k \equiv a\ (mod\ p^s)$ *is solvable if and only if* $y^d \equiv a\ (mod\ p^s)$ *is solvable.*

Proof of Lemma 16. (ONLY IF PART) Given $d|k$, if we let $y = x^{k/d}$, it immediately follows that $y^d = x^k \equiv a \bmod p^s$.

(IF PART) By Theorem 12, $\mathbb{Z}_{p^s}^*$ is a cyclic group of order $\phi(p^s)$. Let g be a primitive root that generates this group. We are given some $y \equiv g^r \bmod p^s$ for some power r, such that $y^d \equiv a \bmod p^s$. Since $d = (k, \phi(p^s))$, we have $(k/d, \phi(p^s)/d) = 1$, there exists an integer u, such that $u \cdot (k/d) \equiv 1 \bmod \phi(p^s)/d$. It follows that $uk \equiv d \bmod \phi(p^s)$. Let $x = g^t$, where $t = ru$. Then $x^k = g^{ruk} \equiv g^{rd} \bmod p^s \equiv a \bmod p^s$. □

Now Euler's Generalized Criterion 15 follows from the cyclic group structure of $\mathbb{Z}_{p^s}^*$ of order $\phi(p^s)$: As $d|\phi(p^s)$, clearly $a \in \mathbb{Z}_{p^s}^*$ is a d-th power if and only if $a^{\phi(p^s)/d} \equiv 1 \bmod p^s$.

We now consider the case of powers of 2. For modulus 2 or 4 the same criterion as above works, since $\mathbb{Z}_n^*$ is cyclic, for $n = 2$ and 4. More concretely, for modulus 2, $x^k \equiv a \pmod 2$ is always solvable for every odd a, and for modulus 4, $x^k \equiv a \pmod 4$ is unsolvable precisely when $a \equiv -1 \pmod 4$ and k is even (solvable precisely when $a \equiv 1 \pmod 4$ or k is odd).

For the next three Lemmas, we suppose $s \geq 3$ and consider the modulus 2^s. The group $\mathbb{Z}_{2^s}^*$ is a direct product of a cyclic group of order 2 with another cyclic group of order 2^{s-2}, $\mathbb{Z}_2 \times \mathbb{Z}_{2^{s-2}}$, with -1 and 5 as generators respectively (cf. Theorem 13).

Lemma 17 *If $x^k \equiv a \bmod 2^s$ is solvable then*

$$a^{2^{s-2}/d} \equiv 1 \bmod 2^s,$$

where $d = \gcd(k, 2^{s-2})$.

PROOF. Let x be a solution to $x^k \equiv a \bmod 2^s$ in $\mathbb{Z}_{2^s}^*$. Then $a^{2^{s-2}/d} \equiv x^{2^{s-2} \cdot (k/d)} \equiv 1 \bmod 2^s$, as $d|k$. □

Lemma 18 *If $a \equiv 1 \pmod 4$ and $a^{2^{s-2}/d} \equiv 1 \bmod 2^s$, then a solution to $x^k \equiv a \bmod 2^s$ exists, where, again, $d = \gcd(k, 2^{s-2})$.*

PROOF. As $a \equiv (-1)^{\frac{a-1}{2}} 5^r \bmod 2^s$, for some $0 \leq r < 2^{s-2}$, we have $a \equiv 5^r \bmod 2^s$, since $a \equiv 1 \pmod 4$. Since $a^{2^{s-2}/d} \equiv 1 \bmod 2^s$, and 5 has order 2^{s-2} in $\mathbb{Z}_{2^s}^*$, we get $d|r$. Denote by $q = r/d$.

Since $(k/d, 2^{s-2}/d) = 1$, there exists an integer u, $u \cdot k/d \equiv 1 \bmod 2^{s-2}/d$, hence $uk \equiv d \bmod 2^{s-2}$.

Now let $x = 5^{qu}$. Then we can verify

$$x^k \equiv 5^{quk} \equiv 5^{qd} \equiv 5^r \equiv a \bmod 2^s.$$

□

Lemma 19 *If $a \equiv -1 \pmod 4$ then $x^k \equiv a \bmod 2^s$ has a solution if and only if k is odd.*

PROOF. Suppose $a \equiv -1 \pmod 4$. Clearly, if k is even, then for all $x \equiv \pm 5^t \bmod 2^s$, $x^k \equiv 5^{kt} \bmod 2^s$, and taking it further mod 4, we get $x^k \equiv 1 \pmod 4 \not\equiv -1 \pmod 4$. Hence $x^k \equiv a \bmod 2^s$ has no solution in this case.

Now suppose k is odd. Note that $a \equiv -5^r \bmod 2^s$, for some $0 \leq r < 2^{s-2}$. As $\gcd(k, 2^{s-2}) = 1$, there exists an integer u, such that $uk \equiv 1 \bmod 2^{s-2}$.

Now let $x = -5^{ru}$. Then

$$x^k \equiv -5^{ruk} \equiv -5^r \equiv a \bmod 2^s.$$

□

Note that in the case of odd k in the above lemma, $d = \gcd(k, 2^{s-2}) = 1$ and $a^{2^{s-2}/d} \equiv 1 \bmod 2^s$ always holds.

Summarizing, we have the following theorem.

Theorem 20 *For $s \geq 3$, $x^k \equiv a \bmod 2^s$ has a solution if and only if the following conditions are satisfied:*

(1) $a^{2^{s-2}/d} \equiv 1 \bmod 2^s$, *for* $d = \gcd(k, 2^{s-2})$

(2) $a \equiv 1 \pmod 4$ *or* [$a \equiv -1 \pmod 4$ *and* k *is odd*].

3.2 Membership of HPR in UP ∩ coUP

Theorem 21 *The Higher Power Residuosity problem (HPR) is in UP ∩ coUP.*

PROOF. Based on these facts, a UP machine, M, for HPR can easily be designed as in the quadratic (non)residue case. M simply guesses, with ascending order of prime powers, the unique prime factorization of n, and verifies it. On the unique computation path with the correct prime factorization of n, M can check in deterministic polynomial time, for each of the prime powers of n, whether a is a k-th power residue, using Criterion 15 and Theorem 20. Then by Lemma 14 the UP machine, M, accepts the input for HPR mod n if and only if it is a HPR mod each of the prime powers of n. □

Acknowledgements

We thank Eric Bach for his very insightful comments and the anonymous referees for their many helpful suggestions which improved the readability of this note.

The second author thanks Venkatesan Chakaravarthy for taking the time to explain some theorems in structural complexity theory which though not mentioned here were none the less "required reading" for writing this note.

References

[1] M. Agrawal, N. Kayal, N. Saxena, PRIMES is in P, Preprint, to appear in Annals of Mathematics.

[2] E. Bach, J. Shallit, Algorithmic Number Theory, Vol. 1: Efficient Algorithms, MIT Press, Cambridge, Massachusetts, 1996.

[3] L. Berman, Polynomial reducibilities and complete sets, Ph.D. thesis, Cornell University, Ithaca, New York (1977).

[4] A. Borodin, A. Demers, Some Comments on Functional Self Reducibility and the NP-Hierarchy, Tech. Rep. TR 76-284, Cornell University, Ithaca, New York (1976).

[5] A. Cunningham, On 2 as a 16-ic residue, Proceedings of the London Mathematical Society 27 (1896) 85–122.

[6] D.Z. Du, K.I. Ko, Theory of Computational Complexity, John Wiley & Sons, New York, 2000.

[7] M.R. Fellows, N. Koblitz, Self-Witnessing Polynomial-Time Complexity and Prime Factorization, in: Proceedings of the Seventh Annual Structure in Complexity Theory Conference, IEEE Computer Society Press, Boston, Massachusetts, 1992, pp. 107–110.

[8] J. Grollmann, A.L. Selman, Complexity measures for public-key cryptosystems, SIAM J. Comput. 17(2) (1988) 309–335.

[9] J. Hartmanis, L. Hemachandra, Complexity classes without machines: On complete languages for UP, Theoret. Comput. Sci. 58 (1988) 129–142.

[10] L.K. Hua, P. Shiu (translator), Introduction to Number Theory, Springer-Verlag, New York, 1982.

[11] K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory, Springer-Verlag, New York, 1990.

[12] K. Ko, On some natural complete operators, Theoret. Comput. Sci. 37 (1985) 1–30.

[13] M. Luby, Pseudorandomness and Cryptographic Applications, Princeton University Press, Princeton, New Jersey, 1996.

[14] K. Manders, L. Adleman, NP-complete decision problems for binary quadratics, J. Comput. System Sci. 16 (1978) 168–184.

[15] M.O. Rabin, Digitalized signatures and public-key functions functions as intractable as factorization, Tech. Rep. MIT/LCS/TR-212, MIT Laboratory for Computer Science, Cambridge, Massachusetts (1979).

[16] R.L. Rivest, A. Shamir, L.M. Adleman, A method for obtaining digital signatures and public-key crytosystems, Comm. ACM 21 (1978) 120–126.

[17] A. Selman, A survey of one-way functions in complexity theory, Mathematical Systems Theory 25(3) (1992) 203–221, (note, journal renamed to Theory Comput. Syst. in 1997).

[18] L. Valiant, On the Relative Complexity of Checking and Evaluating, Tech. Rep. LS29JT, University of Leeds, Leeds, United Kingdom (October, 1974).

[19] L. Valiant, Relative complexity of checking and evaluating, Inform. Process. Lett. 5 (1976) 20–23.