On differences of quadratic residues

Guillermo Morales-Luna
Computer Science
Cinvestav-IPN, Mexico City
gmorales@cs.cinvestav.mx

October 8, 2008

Abstract

Factoring an integer is equivalent to express the integer as the difference of two squares. We test that for any odd modulus, in the corresponding ring of remainders, any element can be realized as the difference of two quadratic residues, and also that, for a fixed remainder value, the map assigning to each modulus the number of ways to express the remainder as difference of quadratic residues is non-decreasing with respect to the divisibility ordering in the odd numbers. The reduction to remainders rings of the problem to express a remainder as the difference of two quadratic residues does not diminish the complexity of the factorization problem.

1 Introduction

Whenever an integer is written as the difference of two squares $n = x_1^2 - x_0^2$ in $\mathbb{Z}$, then $n = (x_1 - x_0)(x_1 + x_0)$ and the greatest common divisors $(n, x_1 - x_0)$, $(n, x_1 + x_0)$ will provide non-trivial divisors of n, whenever $\{x_1 - x_0, x_1 + x_0\} \neq \{1, n\}$. This is the basis of Shor's Factoring Quantum Algorithm [3] and a main component of Scolnik's talk at this year Spanish Meeting on Cryptology [2].

If $n = x_1^2 - x_0^2$ then for any integer $m > 1$, $\pi_m(n) = [\pi_m(x_1)]^2 - [\pi_m(x_0)]^2$ in $\mathbb{Z}_m$, where $\pi_m : x \mapsto x \bmod m$ is the canonical projection $\mathbb{Z} \to \mathbb{Z}_m$. In other words, $\pi_m(n)$ is the difference of two quadratic residues in $\mathbb{Z}_m$.

In this paper we state some basic remarks related to quartets (z, x_0^2, x_1^2, m) with $\pi_m(z) = x_1^2 - x_0^2$ in $\mathbb{Z}_m$.

2 Difference of squares in the integers

Certainly, if $n = x_1^2 - x_0^2$ in $\mathbb{Z}$, then $z_0 = (x_1 - x_0)$ and $z_1 = (x_1 + x_0)$ give two factors of n, although they can be trivial. Let us say that the triplet (z, x_0^2, x_1^2) determines a *splitting difference*. Conversely, if n factors as $n = z_0 z_1$ then the equation system $x_1 - x_0 = z_0$, $x_1 + x_0 = z_1$ can be stated as

$$A\mathbf{x} = \mathbf{z} \text{ with } A = \begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix},\ \mathbf{x} = \begin{bmatrix} x_0 \\ x_1 \end{bmatrix},\ \mathbf{z} = \begin{bmatrix} z_0 \\ z_1 \end{bmatrix}. \tag{1}$$

Clearly, $A^2 = 2I_2$, where I_2 is the (2×2)-identity matrix. Thus the rational values $x_0 = \frac{1}{2}(z_1 - z_0)$, $x_1 = \frac{1}{2}(z_1 + z_0)$ are such that $n = x_1^2 - x_0^2$. These values are indeed integer whenever both z_0, z_1 have the same parity, either they are odd or they are even.

The map $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, $(x_0, x_1) \mapsto x_1^2 - x_0^2$, has as contour lines equilateral hyperbolas (see figure 1), and for each integer $n \in \mathbb{Z}$, $f^{-1}(n) \cap \mathbb{Z}$ is a finite set because n has finitely many divisors.

As an elementary remark [1], we have that if (n, x_0^2, x_1^2) determines a splitting difference then for any integer $m > 1$, $((m^2 - 1)n, (x_1 + mx_0)^2, (mx_1 + x_0)^2)$ also determines a splitting difference. Namely,

$$\begin{aligned}
(m^2 - 1)n &= (m^2 - 1)(x_1^2 - x_0^2) \\
&= m^2 x_1^2 - x_1^2 - m^2 x_0^2 + x_0^2 \\
&= (m^2 x_1^2 + x_0^2 + 2m x_1 x_0) - (x_1^2 + m^2 x_0^2 + 2m x_1 x_0) \\
&= (m x_1 + x_0)^2 - (x_1 + m x_0)^2.
\end{aligned} \tag{2}$$

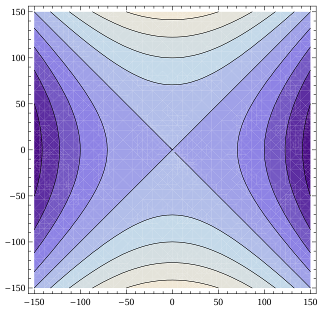

Figure 1: Contour lines of map $(x_0, x_1) \mapsto x_1^2 - x_0^2$. The lighter zones correspond to greater values.

This difference determines the factors $(m-1)(x_0 - x_1)$ and $(m+1)(x_0 + x_1)$ of $(m^2 - 1)n$.

3 Differences of quadratic residues

In what follows, the statements quoted as "remarks" are rather obvious and no proofs are provided.

Let $m \in \mathbb{N}$ be an integer greater than 1 and let $\mathbb{Z}_m^*$ be the multiplicative group of the ring of remainders $\mathbb{Z}_m$. The order of the group is $o(\mathbb{Z}_m^*) = \phi(m)$ where ϕ is Euler's totient function. Let Q_m denote the set of quadratic residues in $\mathbb{Z}_m$ and let $Q_m^* = Q_m \cap \mathbb{Z}_m^*$ be the subgroup in $\mathbb{Z}_m^*$ consisting of unit quadratic residues. The *squaring map* $x \mapsto \sigma(x) = x^2$ is an epimorphism $\mathbb{Z}_m^* \to Q_m^*$ and its kernel $U_m = \{x \in \mathbb{Z}_m | \ x^2 = 1\}$ consists of the elements of order 2 in $\mathbb{Z}_m^*$.

Let $Q_m - 1 = \{z \in \mathbb{Z}_m | \ \exists y \in Q_m : \ z = y - 1\}$ be the collection of remainders that can be expressed as the difference of a quadratic residue and 1. Obviously, $y \mapsto y - 1$ is a bijection $Q_m \to Q_m - 1$ and we may realize $Q_m - 1$ as a "shifted copy" of Q_m.

Let $D_m = \{z \in \mathbb{Z}_m | \ \exists y_0, y_1 \in Q_m : \ z = y_1 - y_0\}$ be the collection of remainders that can be expressed as the difference of two quadratic residues:

$$\forall z \in \mathbb{Z}_m : \ z \in D_m \iff \exists x_1, x_0 \in \mathbb{Z} : \ z = (x_1^2 - x_0^2) \bmod m.$$

If $z = (x_1^2 - x_0^2) \bmod m$ we will say that the quartet (z, x_0^2, x_1^2, m) determines a *splitting difference*.

Remark 3.1 *If (z, y_0, y_1) determines a splitting difference in the ring $\mathbb{Z}$ of integers, then for any $m > 1$, $(\pi_m(z), \pi_m(y_0), \pi_m(y_1), m)$ determines a splitting difference in $\mathbb{Z}_m$.*

Remark 3.2 (Scolnik) *Suppose that (z, y_0, y_1, m) determines a splitting difference in $\mathbb{Z}_m$, and that for some integers $z_1, w_0, w_1, m_1 \in \mathbb{Z}$, $z = y_1 - y_0 + z_1 \bmod m$ and (z_1, w_0, w_1, m_1) determines a splitting difference. If there exist $c_0, c_1 \in \mathbb{Z}$ such that $y_0 + mw_0 + c_0 mm_1, y_1 + mw_1 + c_1 mm_1 \in Q_{mm_1}$ and $m_1 | (c_1 - c_0)$, then $(z, y_0 + mw_0 + c_0 mm_1, y_1 + mw_1 + c_1 mm_1, mm_1)$ determines a splitting difference.*

Remark 3.3 *Clearly,*

$$y \in Q_m \ \& \ z \in D_m \implies yz \in D_m. \tag{3}$$

For any $z \in D_m$, let $E_{zm} = \{(y_0, y_1) \in Q_m^2 | \ z = y_1 - y_0\}$ be the collection of pairs of quadratic residues whose difference produces z. Evidently,

- $[z \in Q_m \implies (0, z) \in E_{zm}]$
- $[z \in Q_m - 1 \implies (1, z + 1) \in E_{zm}]$
- $[(y_0, y_1) \in E_{zm} \implies (y_1, y_0) \in E_{-z \bmod m, m}]$

Besides, if $y_0 \in Q_m^*$, then for any $y_1 \in Q_m$: $y_1 - y_0 = y_0(y_0^{-1} y_1 - 1)$; thus the map $\eta : Q_m^* \times Q_m \to Q_m$, $(y_0, y_1) \mapsto y_0^{-1} y_1$ (where multiplicative inverse is on the group $\mathbb{Z}_m^*$) is such that

$$\forall z \in \mathbb{Z}_m \, , \, (y_0, y_1) \in Q_m^* \times Q_m : \ (y_0, y_1) \in E_{zm} \iff z = y_0(\eta(y_0, y_1) - 1). \tag{4}$$

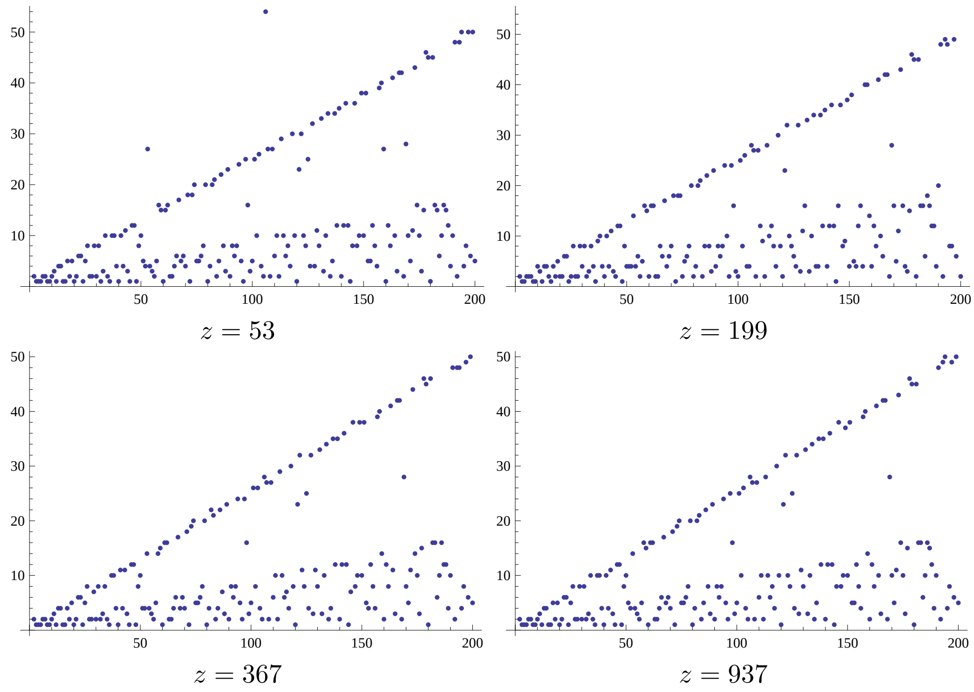

Figure 2: Sequences $(e_{zm})_{2\leq m\leq 200}$ for different odd values of z.

Remark 3.4 *The image of the product $\cdot$ restricted to $Q_m^* \times (Q_m - 1)$ lies within the set D_m.*

Remark 3.5 *Let $z \in \mathbb{Z}_m$ be an arbitrary element and let $d = (m, z)$ be the greatest common divisor of z and the modulus m. Indeed, for some $z_0 \in \mathbb{Z}_m^*$, $z = dz_0$.*

If $z \in D_m$, $z_0 \in Q_m^*$ and $(y_0, y_1) \in E_{zm}$, then $d = z_0^{-1}z = z_0^{-1}(y_1 - y_0) \in D_m$ and $(z_0^{-1}y_0, z_0^{-1}y_1) \in E_{dm}$. Conversely, if $(w_0, w_1) \in E_{dm}$ and $z_0 \in Q_m^*$, then $(z_0w_0, z_0w_1) \in E_{zm}$.

Thus, whenever $z_0 \in Q_m^*$ the map $E_{dm} \to E_{zm}$, $(w_0, w_1) \mapsto (z_0w_0, z_0w_1)$, is a bijection.

Remark 3.6 *Let m be an odd modulus. Then $D_m = \mathbb{Z}_m$. In other words, the map $\delta_m : Q_m \times Q_m \to \mathbb{Z}_m$, $(y_0, y_1) \mapsto y_1 - y_0$, is onto.*

Indeed, if for some $z \in \mathbb{Z}_m$ and $x_0, x_1 \in \mathbb{Z}_m$, we would have $z = x_1^2 - x_0^2 = (x_1 - x_0)(x_1 + x_0)$, then for any factorization $z_0z_1 = z$ the equation system (1) can be posed, and it possesses an unique solution $\mathbf{x} = 2^{-1}A\mathbf{z} \in \mathbb{Z}_m^2$ whenever $2 \in \mathbb{Z}_m^*$, i.e. the modulus m is odd. □

We remark here that the more non-trivial factorizations $z_0z_1 = z$ do occur, more systems (1) can be posed and there will be more elements in the sets E_{zm}.

For any integer $z \in \mathbb{Z}$, let us define $E_{zm} = E_{\pi_m(z),m}$. The number of elements in the set E_{zm}, $e_{zm} = \mathrm{card}(E_{zm})$, gives the number of ways to realize z as the difference of two quadratic residues in $\mathbb{Z}_m$. Exhaustive accounts show that for a fixed value of z and for most values of m, $\varepsilon_m \leq e_{zm} \leq \frac{1}{4}m$, where $\varepsilon_m = m \bmod 2$. In figure 2 we plot the values of e_{zm}, for $2 \leq m \leq 200$ and $z = 53, 199, 367, 937$.

The displayed sequences hint that the smallest value $e_{zm} = 1$ is attained in most cases when m is even, which correspond to the cases in which system (1) has no an unique solution.

Remark 3.7 *The following assertions are inmediate:*

1. *If m is odd, then $\forall z \in \mathbb{Z}_m$: $E_{zm} \neq \emptyset$.*
2. *If $m_1|m$ then $\pi_{m_1}(E_{zm}) \subset E_{zm_1}$, and consequently $\mathrm{card}(\pi_{m_1}(E_{zm})) \leq \mathrm{card}(E_{zm_1})$. (Here, notation has the following meaning: $\pi_{m_1}(E_{zm}) = \{(\pi_{m_1}(y_0), \pi_{m_1}(y_1)) | \ (y_0, y_1) \in E_{zm}\}$.)*

3. If p is a prime factor of both z and m, then: $\left[(y_0,y_1)\in E_{zm} \implies \pi_p(y_0,y_1)\in E_{\frac{z}{p}\frac{m}{p}}.\right]$

As an example of second assertion, we have $E_{3,15}=\{(1,4),(6,9)\}$ although $E_{3,5}=\{(1,4)\}$ since $\pi_5(6,9)=(1,4)$. As an example of third assertion, we have $(10,25)\in E_{15,45}$ ($(40^2-35^2)=8\cdot 45+15$, $40^2=25 \bmod 45$ and $35^2=10 \bmod 45$,) thus $(2,3)=\pi_5(10,25)\in E_{5,9}$.

Remark 3.8 *Whenever (z,x_0^2,x_1^2,m) determines a splitting difference in $\mathbb{Z}_m$ then there exists $t\in\mathbb{Z}$ such that $z=(x_1^2-x_0^2)+tm$, thus if $m_1|tm$ we have also that (z,x_0^2,x_1^2,m_1) determines a splitting difference. Hence,*

$$\left.\begin{array}{r}(y_0,y_1)\in E_{zm}\ \&\\ y_0=x_0^2 \bmod m\ \&\\ y_1=x_1^2 \bmod m\ \&\\ z=(x_1^2-x_0^2)+tm\ \&\\ m_1|tm\end{array}\right\}\implies \pi_{m_1}(y_0,y_1)\in E_{zm_1}. \tag{5}$$

Let $(2\mathbb{Z}^+-1)$ denote the set of odd positive integers. It is a poset with the "divisibility" relation, its minimum element is 1 and its *atoms*, i.e. the minimal elements greater than the minimimum, are the prime numbers. The reciprocal form of second assertion at remark 3.7 above can be generalized as follows:

Proposition 3.1 *For any $z\in\mathbb{N}$, the map $(2\mathbb{Z}^+-1)\to\mathbb{N}$, $m\mapsto e_{zm}=\mathrm{card}(E_{zm})$, is non-decreasing with respect to the divisibility ordering in $(2\mathbb{Z}^+-1)$ and the usual ordering in $\mathbb{N}$.*

And the above proposition can be re-stated as follows:

Proposition 3.2 *For any $z\in\mathbb{N}$, and for any ℓ odd primes $p_1,\dots,p_\ell$ there exist $e_1,\dots,e_\ell\in\mathbb{N}$ such that*

$$[\forall j\leq\ell: d_j\geq e_j]\ \&\ \left[m=\prod_{j=1}^{\ell}p_j^{d_j}\right] \implies \mathrm{card}(E_{zm})>1.$$

Whenever the modulus m is odd, given $z\in\mathbb{Z}_m$, if one has a factorization $z=z_0z_1$ in $\mathbb{Z}_m$, then by solving the corresponding equation system (1), one can realize z as the difference of two quadratic residues. Conversely, any expression of z as the difference of two quadratic residues will provide a factorization $z=z_0z_1$ in $\mathbb{Z}_m$.

If $n=w_0w_1$ is factored as the product of two integers in $\mathbb{Z}$, then for all odd prime modulus $p\in\mathbb{Z}^+$ we have $\pi_p(n)=z_0z_1 \bmod p$, where $z_0=\pi_p(w_0)$ and $z_1=\pi_p(w_1)$. Thus whenever $p_1,\dots,p_k\in\mathbb{Z}^+$ is a collection of k odd prime numbers, the pair (w_0,w_1) is a solution of the equation system

$$\pi_{p_i}(x_0)=z_{0i} \bmod p_i\ ,\ \pi_{p_i}(x_1)=z_{1i} \bmod p_i\ ,\ \pi_{p_i}(n)=z_{0i}z_{1i}\ \text{ in }\ \mathbb{Z}_{p_i}\ ,\ i=1,\dots,k. \tag{6}$$

Nevertheless the converse is not a direct matter. By the Chinese Remainder Theorem, for any k the system has a solution but it does not provide neither a factorization of n nor even a congruence classes modulus $\prod_{i=1}^n p_i$ in which the factors of n may appear.

4 Conclusions

Although the factorization problem is equivalent to represent the argument integer as the difference of two squares, the reduction of the problem to express a remainder as the difference of two quadratic residues is of no help.

References

[1] Edward J. Barbeau. *Pell's Equation.* Springer, Berlin, Heidelberg, 2003.

[2] Luis Hernández-Encinas and Angel Martín-del Rey, editors. *Actas de la Décima Reunión Española sobre Criptología y Seguridad de la Información.* Signe, S. A., 2008.

[3] Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *IEEE Symposium on Foundations of Computer Science*, pages 124–134, 1994.