Odd Quadratic Residues modulo powers of 2
Write up 2017

Jared Marx-Kuo

June 21st, 2017

1 Introduction

Finding solutions to

$$x^2 \equiv q \mod p$$

is a well known problem, with a solution given by the Tonelli-Shanks algorithm. Furthermore, for a prime $p > 2$, the solutions to

$$x^2 \equiv q \mod p^k \qquad k \geq 1$$

are uniquely determined by an application of Hensel's lemma to the function $f(x) = x^2 - q$, for which $f'(x) = 2x \not\equiv 0$ assuming $p^k \nmid x$. However, in the case that $p = 2$, hensel lifting from $k = 1$ to higher values fails as $f'(x) = 2x \equiv 0 \mod 2$. Thus another method is needed to determine the solutions to $x^2 \equiv q \mod 2^k$. We provide such a method for odd values of q, as well as a simple classification of these residues for each value of 2^k.

2 Main Claims

Let Q_k denote the collection of odd residues modulo 2^k. The following theorems determine the structure of all residues modulo 2^k in relation to residues modulo 2^{k-1} for $k > 3$.

Theorem 2.1 (Main Theorem 1). *For $k \geq 3$, odd quadratic residues are of the form $q = 8c + 1$, and iterating through all values of $c = \{0, \ldots, 2^{k-3} - 1\}$ yields all such odd quadratic residues.*

Note that this implies that for 2^k, there are 2^{k-3} odd quadratic residues, or $1/8$ of all values in $\mathbb{Z}/2^k\mathbb{Z}$.

Theorem 2.2 (Main Theorem 2). *For each quadratic residue q and power k, there are 4 distinct solutions to $x^2 = q \mod 2^k$, $\{a_i(q,k)\}$, such that*

$$x \in \{a_1(q,k), a_2(q,k), a_3(q,k), a_4(q,k)\} = \{a_1(q,k), a_2(q,k), 2^k - a_2(q,k), 2^k - a_1(q,k)\}$$

with

$$a_2(q,k) = 2^{k-1} - a_1(q,k)$$

Here I assume that the roots are ordered from least to greatest (which amounts to the convention that $a_1(q,k) < a_2(q,k)$).

Theorem 2.3 (Main Theorem 3). *Given a quadratic residue q mod 2^k, then q is a residue mod 2^{k+1} with*

$$a_1(q,k) = a_1(q,k+1) \quad \text{or} \quad a_1(q,k) = a_1(q+2^k, k+1)$$

With these 3 theorem, all of the quadratic residues modulo powers of 2 and the solutions to $x^2 \equiv \mod 2^k$ can be determined inductively starting with $k = 3$.

3 Preliminary Lemmas

Lemma 3.1 (Residue Hierarchy). *If q_k is an odd quadratic residue of 2^k, then it is of the form*

$$q_k = q_{k-1} + c \cdot 2^{k-1}$$

for q_{k-1} a quadratic residue of 2^{k-1} and $c = 0, 1$.

Proof: Note that

$$r^2 = q_k \mod 2^k \implies r^2 = q_k + n \cdot 2^k, \quad n \in \mathbb{N}$$

$$\implies r^2 \mod 2^{k-1} = q_k \mod 2^{k-1}$$

yet in that $r \in \mathbb{Z}$ is odd, we set $q_{k-1} = q_k \mod 2^{k-1}$ which will be non-zero by oddness, so that

$$r^2 = q_{k-1} \mod 2^{k-1}$$

$$\implies q_k = q_{k-1} + c \cdot 2^{k-1} \text{ s.t. } c = 0 \text{ or } 1$$

because we always restrict $0 \leq q_k < 2^k$ by convention. □

Taking the base case of $k = 3$, we have 1 quadratic residue of $q = 1$, so from the above lemma, we see that the number of quadratic residues can at most double, i.e., the number of quadratic residues modulo 2^k is at most, $n = 2^{k-3}$, which provides the correct upper bound for our first lemma.

Lemma 3.2 (Residue symmetry). *For $k \geq 4$, q_k is an odd residue modulo 2^k, then so is $q_k + 2^{k-1}$.*

Proof: Given that

$$\exists r \text{ s.t. } r^2 \equiv q_k \mod 2^k$$

$$(2^{k-2} - r)^2 = 2^{2k-4} - 2^{k-1}r + r^2 = 2^{2k-4} - 2^{k-1}(r+1) + r^2 + 2^{k-1}$$

Noting that $r + 1$ is even, and that for $k \geq 4$, $2^k \mid 2^{2k-4}$, so that

$$(2^{k-2} - r)^2 \equiv 2^{2k-4} - 2^k \left(\frac{r+1}{2}\right) + r^2 + 2^{k-1} \equiv q_k + 2^{k-1} \mod 2^k$$

□

Lemma 3.3 (Residue solution sets)**.** *For $k \geq 3$ and q_k odd, if r is a solution to $x^2 \equiv q_k \mod 2^k$, then so are $\{2^k - r, 2^{k-1} - r, 2^k - 2^{k-1} + r\}$.*

Proof: Note that

$$(2^k - r)^2 \equiv r^2 \mod 2^k \equiv q_k \mod 2^k$$

$$(2^{k-1} - r)^2 \equiv 2^{2k-2} - 2^k r + r^2 \equiv q_k \mod 2^k$$

$$(2^k - 2^{k-1} + r)^2 \equiv (2^{k-1} - r)^2 \equiv q_k \mod 2^k$$

Using the fact that q_k (and thus r) is odd, it is clear that these four solutions are distinct. □

4 Proof of Theorem 1

We prove theorem 3.1 by induction. The base case of $k = 3$ is true (see Appendix for a table of the odd residues for the first few powers of 2^k). Assume that the odd quadratic residues modulo 2^k are given by the set $Q_k = \{8c + 1\}$ for $0 \leq c < 2^{k-3}$. Applying Lemma 4.1, we note that $8 \mid 2^k$ for $k > 3$, so that

$$Q_{k+1} \subseteq \{8c + 1\}_{c=0}^{c=2^{k-2}-1}$$

$$\forall q \in Q_k, \quad q \in Q_{k+1} \text{ or } q + 2^k \in Q_{k+1}$$

but applying Lemma 4.2, we see that both $q, q + 2^k \in Q_{k+1}$, for all $q \in Q_k$. This implies that $Q_{k+1} \supseteq \{8c+1\}_{c=0}^{c=2^{k-2}-1}$, implying set equality. This verifies the inductive hypothesis.

5 Proof of Theorem 2

Given that for each k, there are 2^{k-3} residues of the form $\{8c + 1\}$. We now partition the odd integers in $\mathbb{Z}/2^k\mathbb{Z}$, or rather $(\mathbb{Z}/2^k\mathbb{Z})^\times$ by which residue their square corresponds to. For each $q \in Q_k$, there are at least four distinct solutions to $x^2 \equiv q \mod 2^k$, which account for at least

$$|Q_k| * 4 = 2^{k-3} * 4 = 2^{k-1}$$

elements of $(\mathbb{Z}/2^k\mathbb{Z})^\times$. Yet $|(\mathbb{Z}/2^k\mathbb{Z})^\times| = 2^{k-1}$ so that we've accounted for all elements of this group, meaning that to each odd residue, there are exactly 4 solutions to $x^2 \equiv q \mod 2^k$. Moreover, they have the form as stated in Theorem 3.2 by applying Lemma 4.3 □

6 Proof of Theorem 3

We have that

$$a_1(q,k)^2 \equiv q \mod 2^k \implies a_1(q,k)^2 = q + n \cdot 2^k, \quad n \in \mathbb{N}$$

If n is even, then

$$\begin{aligned} a_1(q,k)^2 &= q + c \cdot 2^{k+1}, \quad c \in \mathbb{N} \\ \implies a_1(q,k)^2 &\equiv q \mod 2^{k+1} \end{aligned}$$

If n is odd, then

$$a_1(q,k)^2 = q + 2^k + (n-1) \cdot 2^k = q + 2^k + c \cdot 2^{k+1}, \quad c \in \mathbb{N}$$

$$\implies a_1(q,k)^2 \equiv q + 2^k \mod 2^{k+1}$$

Note that both such cases do occur (see Appendix). □

7 Appendix

Below is a table of residues for $1 \leq k \leq 6$.

Table 1: Powers of 2 greater than or equal to 8 and Their Respective Residues and Solutions

P = 8	P = 16		P = 32			
$q \equiv 1$	$q \equiv 1$	$q \equiv 9$	$q \equiv 1$	$q \equiv 9$	$q \equiv 17$	$q \equiv 25$
x = 1	x = 1	x = 3	x = 1	x = 3	x = 7	x = 5
x = 3	x = 7	x = 5	x = 15	x = 13	x = 9	x = 11
x = 5	x = 9	x = 11	x = 17	x = 19	x = 23	x = 21
x = 7	x = 15	x = 13	x = 31	x = 29	x = 25	x = 27

P = 64							
$q \equiv 1$	$q \equiv 9$	$q \equiv 17$	$q \equiv 25$	$q \equiv 33$	$q \equiv 41$	$q \equiv 49$	$q \equiv 57$
x = 1	x = 3	x = 9	x = 5	x = 15	x = 13	x = 7	x = 11
x = 31	x = 29	x = 23	x = 27	x = 17	x = 19	x = 25	x = 21
x = 33	x = 35	x = 41	x = 37	x = 47	x = 45	x = 39	x = 43
x = 63	x = 61	x = 55	x = 59	x = 49	x = 51	x = 57	x = 53

With regards to theorem 3, we see that for $q = 1$, and $P = 32, 64$ (or rather $k = 5, 6$), that $a_1(1,5) = a_1(1,6)$. However, for $q = 17$, we have $a_1(17,5) = a_1(17+32,6) = a_1(49,6)$, so both cases do occur.