A.8 Quadratic Non-Residues

How to find a quadratic *non-residue* modulo a prime p? That is, an integer a with $p \nmid a$ that is not a quadratic residue $\bmod a$. The preferred solution is the smallest possible positive one. Nevertheless we start with -1:

Proposition 21 *Let $p \geq 3$ be prime.*

(i) -1 *is a quadratic non-residue* $\bmod p \Longleftrightarrow p \equiv 3 \pmod 4$.

(ii) 2 *is a quadratic non-residue* $\bmod p \Longleftrightarrow p \equiv 3$ *or* $5 \pmod 8$.

(iii) (*For* $p \geq 5$) 3 *is a quadratic non-residue* $\bmod p \Longleftrightarrow p \equiv 5$ *or* $7 \pmod{12}$.

(iv) (*For* $p \geq 7$) 5 *is a quadratic non-residue* $\bmod p \Longleftrightarrow p \equiv 2$ *or* $3 \pmod 5$.

Proof. (i) This follows from Proposition 20. However there is an even simpler proof:

$$\begin{aligned} -1 \in \mathbb{M}_p^2 &\iff \bigvee_{i \in \mathbb{Z}} i^2 \equiv -1 \pmod p \iff \bigvee_{i \in \mathbb{Z}} \operatorname{ord}_p i = 4 \\ &\iff 4 \mid \#\mathbb{F}_p^\times = p-1 \iff p \equiv 1 \pmod 4. \end{aligned}$$

(ii) This also follows from Proposition 20: By the adjacent remark $2 \in \mathbb{M}_p^2 \Longleftrightarrow p \equiv 1$ or $7 \pmod 8$.

(iii) We use the law of quadratic reciprocity:

$$\begin{aligned} (\frac{3}{p}) = (-1)^{\frac{p-1}{2}}(\frac{p}{3}) &= \begin{cases} (-1)^{6k}(\frac{1}{3}) = 1 & \text{if } p = 12k+1, \\ (-1)^{6k+2}(\frac{2}{3}) = -1 & \text{if } p = 12k+5, \\ (-1)^{6k+3}(\frac{1}{3}) = -1 & \text{if } p = 12k+7, \\ (-1)^{6k+5}(\frac{2}{3}) = 1 & \text{if } p = 12k+11, \end{cases} \\ &= \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 11 \pmod{12}, \\ -1 & \text{if } p \equiv 5 \text{ or } 7 \pmod{12}. \end{cases} \end{aligned}$$

(iv) By quadratic reciprocity

$$(\frac{5}{p}) = (\frac{p}{5}) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 4 \pmod 5, \\ -1 & \text{if } p \equiv 2 \text{ or } 3 \pmod 5, \end{cases}$$

as claimed. $\diamond$

Corollary 1 241 *is the unique odd prime* < 400 *for which none of* -1, 2, 3, 5 *are quadratic non-residues.*

Corollary 2 *For each odd prime p at least one of -1, 2, 3, or 5 is a quadratic non-residue except for $p \equiv 1, 49 \pmod{120}$.*

For arbitrary, not necessarily prime, modules we have some analogous results:

Lemma 19 *Let $n \in \mathbb{N}$, $n \geq 2$. Assume that $(\frac{a}{n}) = -1$ for some $a \in \mathbb{Z}$. Then a is a quadratic non-residue in $\mathbb{Z}/n\mathbb{Z}$.*

Proof. Let $n = p_1^{e_1} \cdots p_r^{e_r}$ be the prime decomposition. Then

$$(\frac{a}{n}) = (\frac{a}{p_1})^{e_1} \cdots (\frac{a}{p_r})^{e_r}.$$

Hence for some k the exponent e_k is odd, and $(\frac{a}{p_k}) = -1$. Then a is a quadratic non-residue mod p_k. Since $\mathbb{F}_{p_k}$ is a homomorphic image of $\mathbb{Z}/n\mathbb{Z}$, a is a forteriori a quadratic non-residue mod n. $\diamond$

Corollary 3 *Let $n \in \mathbb{N}$, $n \geq 2$, and not a square in $\mathbb{Z}$.*

(i) *If $n \equiv 3 \pmod 4$, then -1 is a quadratic non-residue in $\mathbb{Z}/n\mathbb{Z}$.*

(ii) *If $n \equiv 5 \pmod 8$, then 2 is a quadratic non-residue in $\mathbb{Z}/n\mathbb{Z}$.*

And so on. Unfortunately this approach doesn't completely cover all cases, see the remark below. Nevertheless we note that an algorithm for finding a quadratic non-residue needs to address the cases $n \equiv 1 \pmod 8$ only. Again there are two variants:

- A deterministic algorithm that tests $a = 2, 3, 5, \ldots$ in order. Assuming ERH—for the character $\chi = (\frac{\bullet}{n})$—it is polynomial in the number $\log(n)$ of places.

- A probabilistic algorithm that randomly chooses a and succeeds with probability $\frac{1}{2}$ each time, yielding $(\frac{a}{n}) = -1$. Computing the Jacobi symbol takes $O(\log(n)^2)$ steps. In the average we need two trials to hit a quadratic non-residue.

Exercise For which prime modules is 7, 11, or 13 a quadratic non-residue? What is the smallest prime module for which this approach (together with Proposition 21) doesn't provide a quadratic non-residue?

Remark A result by Chowla/Fridlender/Salié says that (with a constant $c > 0$) there are infinitely many primes such that all integers a with $1 \leq a \leq c \cdot \log(p)$ are quadratic residues mod p. Ringrose/Graham and—assuming ERH—Montgomery have somewhat stronger versions of this result.

Remark There is no global polynomial (in $\log(n)$) upper bound for the smallest quadratic non-residue that is valid for all modules n. A very weak but simple result is in the following proposition.

Proposition 22 *Let $p \geq 3$ be a prime. Then there is a quadratic non-residue $a < 1 + \sqrt{p}$.*

Proof. There are quadratic non-residues > 1 (and $< p$). Let a be the smallest of these. Let $m = \lceil \frac{p}{a} \rceil$. Thus $(m-1) \cdot a < p < m \cdot a$, or

$$0 < m \cdot a - p < a.$$

Hence $m \cdot a \equiv m \cdot a - p$ is a quadratic residue. This is possible only if m is a quadratic non-residue. Since a is minimal we have $a \leq m$. We conclude

$$(a-1)^2 < (m-1) \cdot a < p,$$

hence $a - 1 < \sqrt{p}$. $\diamond$

Relevant references

- V. R. Fridlender: On the least n-th power non-residue. Dokl. Akad. Nauk. SSSR 66 (1949), 351–352.
- H. Salié: Über den kleinsten positiven quadratischen Nichtrest nach einer Primzahl. Math. Nachr. 3 (1949), 7–8.
- N. C. Ankeney: The least quadratic nonresidue. Ann. of Math. 55 (1952), 65–72.
- H. L. Montgomery: *Topics in Multiplicative Number Theory.* Springer LNM 227 (1971).
- J. Buchmann/V. Shoup: Constructing nonresidues in finite fields and the extended Riemann hypothesis. Preprint 1990.
- S. W. Graham/C. Ringrose: Lower bounds for least quadratic non-residues. In: B. C. Berndt et al. (Eds): *Analytic Number Theory,* Birkhäuser, Boston 1990, 270–309.
- D. J. Bernstein: Faster algorithms to find non-squares modulo worst-case integers. Preprint 2002.