Quadratic residue

Rikard Hjort
hjortr@student.chalmers.se

July 10, 2018

1 Algorithm for finding non-residue

If $p = 2$, then $Z_p^* = \{1\}$, and since 1 is a a quadratic residue, Z_p^* contains no quadratic residues. We will therefore restrict ourselves to the case when $p \geq 3$.

Lemma 1.1. *Exactly half the elements in Z_p^* are quadratic residues.*

Proof. Since Z_p^* is cyclic, it has at least one generator, g. By proposition 2, g^k is a quadratic residue iff $k \mid 2$. Since $\mathrm{ord}(g) = |Z_p^*| = p - 1$, and p is odd, there are precisely $\frac{p-1}{2}$ values of k for which g^k is a quadratic residue, and as many that are quadratic non-residues. □

This means that random sampling is efficient.
This makes it simple to devise an algorithm.

Algorithm 1.2.

Input *p, a prime number ≥ 3.*

Output *a, a quadratic non-residue.*

1. *Pick a random integer $1 < a < p$. (Skip 1 as it is always both quadratic residues.)*
2. *Calculate $a^{\frac{p-1}{2}} = r$.*
   (a) *If $r = 1$, repeat from step 1.*
   (b) *Else, return a.*

The algorithm will only return correct values (it is a Las Vegas algorithm), by proposition 4. The algorithm will probabilistically terminate, since there is $\frac{p-1}{2}$ quadratic non-residues in Z_p^*.

Runtime analysis Exponentiation can be done in polynomial time in $\log p$ with binary exponentiation, and decrementing p and halving it can be done in linear time or better, since it is simply a matter of flipping the least significant bit and shifting. Testing eqaulity with 1 can be done in constant time.

The algorithm runs an expected number of 2 times, since by lemma 1.1 it has a $\frac{1}{2}$ probability to find a quadratic non-residueat every iteration. The total runtime is donimated by exponentiation, and thus runs in polynomial time in $\log p$.

2 Find quadratic residueof $a \in Z_p^*$ given a quadratic non-residue b

We start with some helpful findings.

Lemma 2.1. *Every quadratic residue of Z_p^* has exactly 2 roots.*

Proof. If $a \in Z_p^*$ is a quadratic residue, and $a = g^{2k}$ for some generator g, then also $a = (p - g^k)^2 = p^2 - 2pg^k + g^{2k} = g^{2k}$. Also, g^k and $p - g^k$ are different, since $g^k = p - g^k \Leftrightarrow p = 2g^k \Rightarrow 2 \mid p$ which is not possible, since p is odd. Furthermore,

$$b^2 = c^2 \Leftrightarrow c^{-1}bc^{-1}b = 1$$

which means $c^{-1}b$ is its own inverse (keep in mind Z_p^* is Abelian). Recall that that $|O_2| = \phi(2) = 1$, and $\text{ord}(-1) = 2$, and thus $O_2 = \{-1\}$. Thus, only one element is its own inverse, namely -1. This means that $c^{-1}b = -1$, which in turn means $b = c^{-1}$. Thus, a can have precicesly 2 roots, which are each other's inverses. □

Lemma 2.2. *For $a \in Z_p^*$, $a^{\frac{p-1}{2}} = \begin{cases} 1 \text{ if } a \text{ is a quadratic residue} \\ -1 \text{ if } a \text{ is a quadratic non-residue} \end{cases}$*

Proof. If a is a quadratic residue, then for a generator g such that $g^{2k} = a$ we can express $a^{\frac{p-1}{2}} = g^{2k\frac{p-1}{2}} = g^{k(p-1)} = 1$. If a is a quadratic non-residue, then for a generator g such that $g^{2k+1} = a$, we can express $a^{\frac{p-1}{2}} = g^{(2k+1)\frac{p-1}{2}} = g^{k(p-1)}g^{\frac{p-1}{2}} = g^{\frac{p-1}{2}} \neq 1$ since $\text{ord}(g) \geq \frac{p-1}{2}$. On the other hand, $g^{\frac{p-1}{2}}$ is a root of 1, because squaring it gives 1. Thus, $g^{\frac{p-1}{2}} = -1$ by lemma 2.1. □

We divide the solution into three cases.

2.1 $p \equiv 3 \mod 4$

For the case $p \equiv 3 \mod 4$ we need not bother with b. It suffices to note that $a^{\frac{p-1}{2}} \equiv 1 \mod p \Rightarrow a^{\frac{p-1}{2}}a = a^{\frac{p+1}{2}} \equiv a \mod p$, and since $p + 1 \equiv 0 \mod 4$, we can safely divide $p + 1$ by 4, and get $a^{\frac{p+1}{4}}$ as a root of a, and $p - a^{\frac{p+1}{4}}$ as the other.

2.2 $p \equiv 5 \mod 5$

If $p \equiv 1 \mod 4$, there are two more cases: $p \equiv 1 \mod 8$ and $p \equiv 5 \mod 8$. The second case is simpler. $a^{\frac{p-1}{2}} = 1$ means $a^{\frac{p-1}{4}}$ is a root of 1 (we can safely divide by 4, as $p - 1 \equiv 4 \mod 8$), and thus ± 1. If $a^{\frac{p-1}{4}} = 1$, we are done by the same trick as before and return $a^{\frac{p+3}{4}}$. However, if $a^{\frac{p-1}{4}} = -1$, we can make use of b. $b^{\frac{p-1}{2}} = -1$ by lemma 2.2, so

$$a^{\frac{p-1}{4}} * b^{\frac{p-1}{2}} = 1 \Rightarrow a^{\frac{p+3}{4}} * b^{\frac{p-1}{2}} = a$$

Dividing by 2 again gives us that $\pm a^{\frac{p+3}{8}} * b^{\frac{p-1}{4}}$ is the roots of a.

2.3 $p \equiv 1 \mod 5$

This is by far the trickiest case. TODO.

3 Computational relation between square roots modulo n and factoring n

Equivalent, TODO