A.9 Primitive Elements for Special Primes

For many prime modules finding quadratic non-residues has turned out to be extremely easy. The same is true for finding primitive roots.

Proposition 23 *Let $p = 2p' + 1$ be a special prime. Then:*

(i) $a \in [2 \dots p-2]$ *is a primitive root* mod p *if and only if it is a quadratic non-residue.*

(ii) $(-1)^{\frac{p'-1}{2}} \cdot 2$ *is a primitive root* $\bmod p$.

Proof. We have $p \equiv 3 \pmod 4$, thus -1 is a quadratic non-residue by Proposition 21.

(i) Since the order $\#\mathbb{F}_p^\times = p - 1$ is even, moreover each primitive root is also a quadratic non-residue. There are $\varphi(p-1) = p' - 1$ of them, thus we have found p' quadratic non-residues. Since $p' = \frac{p-1}{2}$, these must be all of them.

(ii) In the case $p' \equiv 1 \pmod 4$ we have $p \equiv 3 \pmod 8$, hence $2 = (-1)^{\frac{p'-1}{2}} \cdot 2$ is a quadratic non-residue by Proposition 21, hence also primitive.

In the case $p' \equiv 3 \pmod 4$ we have $p \equiv 7 \pmod 8$, hence 2 is a quadratic residue, and -1 is a quadratic non-residue again by Proposition 21. Therefore $-2 = (-1)^{\frac{p'-1}{2}} \cdot 2$ is a quadratic non-residue, hence also primitive. $\diamond$

The effortlessness of finding a primitive root is one of several reasons why cryptologists like special primes.

Corollary 1 *Let $p = 2p' + 1$ be a special prime. Then the order of 2 in $\mathbb{F}_p^\times$ is*

(i) $p - 1 = 2p'$ *if* $p' \equiv 1 \pmod 4$,

(ii) $(p-1)/2 = p'$ *if* $p' \equiv 3 \pmod 4$.

Proof. (i) 2 is a primitive root.

(ii) The divisors of $\#\mathbb{F}_p^\times$ are $\{1, 2, p', 2p'\}$. Since 2 is a quadratic residue, it is not primitive, hence the order is not $2p'$. The order cannot be 1 since $2 \neq 1$ in $\mathbb{F}_p$. And the order 3 would imply that $4 = 1$, hence $3 = 0$ in $\mathbb{F}_p$, hence $p = 3$ which ic not a special prime. $\diamond$