A.12 The Multiplicative Group Modulo Special Blum Integers

Let $p = 2p' + 1$ be a special prime. Then the multiplicative group $\mathbb{M}_p = \mathbb{F}_p^\times$ is cyclic of order $p - 1 = 2p'$. Its subgroup $\mathbb{M}_p^2 \le \mathbb{M}_p$ of quadratic residues has index 2 and is itself cyclic, its order being the prime p'. Thus

$$\begin{aligned} \mathbb{M}_p &\cong \mathcal{Z}_{2p'}, & \#\mathbb{M}_p &= \varphi(p) = \lambda(p) = 2p', \\ \mathbb{M}_p^2 &\cong \mathcal{Z}_{p'}, & \#\mathbb{M}_p^2 &= p'. \end{aligned}$$

Let $n = pq$ be a special Blum integer, $p = 2p' + 1$ and $q = 2q' + 1$ being special primes. Then we know that

$$\begin{aligned} \mathbb{M}_n &\cong \mathbb{M}_p \times \mathbb{M}_q, & \#\mathbb{M}_n &= \varphi(n) = 4p'q', \\ \mathbb{M}_n^2 &\cong \mathbb{M}_p^2 \times \mathbb{M}_q^2, & \#\mathbb{M}_n^2 &= p'q'. \end{aligned}$$

Moreover $\lambda(n) = \operatorname{lcm}(2p', 2q') = 2p'q'$. Since $\mathbb{M}_n^2$ as a direct product of two cyclic groups of coprime orders is itself cyclic of order $p'q'$ we conclude:

Proposition 25 *Let n be a special* Blum *integer as above. Then the group $\mathbb{M}_n^2$ of quadratic residues* $\bmod n$ *is cyclic of order $p'q'$ and consists of*

(i) 1 *element of order* 1,

(ii) $p' - 1$ *elements x of order p', characterized by* $x \bmod q = 1$,

(iii) $q' - 1$ *elements x of order q', characterized by* $x \bmod p = 1$,

(iv) $(p' - 1)(q' - 1)$ *elements of order $p'q'$.*

Note that these numbers sum up to $p'q'$, the order of $\mathbb{M}_n^2$.

Corollary 1 *Let n be a special* Blum *integer with prime factors $p = 2p'+1$ and $q = 2q' + 1$. Then the probability $\eta = P\{x \in \mathbb{M}_n^2 \mid \operatorname{ord}(x) = p'q'\}$ that a randomly chosen quadratic residue* $\bmod n$ *has the maximum possible order $p'q'$ is*

$$\eta = 1 - \frac{p' + q' - 1}{p'q'}.$$

If we follow the common usage of choosing (RSA or) BBS modules n as products of two l-bit primes, or p' and q' as $(l - 1)$-bit primes, then

$$2^{l-1} < p' < 2^l, \quad 2^{l-1} < q' < 2^l,$$

$$2^l < p' + q' - 1 < 2^{l+1}, \quad 2^{2l-1} < p' \cdot q' < 2^{2l},$$

$$\frac{1}{2^l} = \frac{2^l}{2^{2l}} < \frac{p' + q' - 1}{p'q'} < \frac{2^{l+1}}{2^{2l-1}} = \frac{1}{2^{2l-3}} = \frac{8}{2^l}.$$

We resume

Corollary 2 *Let n be a special* BLUM *integer with prime factors $p = 2p' + 1$ and $q = 2q' + 1$ of bitlengths l. Then the probability η is bounded by*

$$1 - \frac{8}{2^l} \; < \; \eta \; < \; 1 - \frac{1}{2^l}.$$

The deviation of this probability from 1 is asymptotically negligible: If we choose a random quadratic residue x (say as the square of a random element of $\mathbb{M}_n$), then with overwhelming probability its order has the maximum possible value. However there is an easy test: Check that neither $x \bmod p$ nor $x \bmod q$ is 1.

Since $\mathbb{M}_n$ is the direct product of $\mathbb{M}_n^2$ with a KLEIN four-group we also know the orders of the elements of $\mathbb{M}_n$ and their numbers, in particular

Corollary 3 *Let n be a special* BLUM *integer with prime factors $p = 2p' + 1$ and $q = 2q' + 1$. Then $\mathbb{M}_n$ has exactly $(p' - 1)(q' - 1)$ elements of order $p'q'$, and exactly $3(p' - 1)(q' - 1)$ elements of order $2p'q'$.*