A.14 The BBS Sequence for Superspecial BLUM Integers

Again we get the most satisfying results in the superspecial case:

Definition A **superspecial** BLUM **integer** is a product of two different superspecial primes.

Examples The two smallest superspecial primes are $p = 23$ (with $p' = 11$, $p'' = 5$) and $q = 47$ (with $q' = 23$, $q'' = 11$). Thus the smallest superspecial BLUM integer is $n = 23 \cdot 47 = 1081$. By Section 2.1 we are confident (however don't know for sure) that there are very many superspecial BLUM integers.

Now let $n = pq$ be a superspecial BLUM integer with $p = 2p'+1 = 4p''+3$ and $q = 2q' + 1 = 4q'' + 3$. Form the BBS sequence (1) for an initial value $x \in \mathbb{M}_n^2 - \{1\}$. Then $s = \mathrm{ord}_n(x)$ takes one of the values p', q', or $p'q'$, the last on with extremely high probability, and the first two may be excluded by an easy check. The period of the BBS sequence is $\nu = \mathrm{ord}_s(2)$ by Proposition 26, and we may assume that $s = p'q'$. By the chinese remainder theorem and Lemma 21

$$\nu = \mathrm{lcm}(\mathrm{ord}_{p'}(2), \mathrm{ord}_{q'}(2))$$

By the Corollary of Proposition 23 in Section A.9

$$\mathrm{ord}_{p'}(2) = \begin{cases} 2p'' & \text{if } p'' \equiv 1 \pmod 4), \\ p'' & \text{if } p'' \equiv 3 \pmod 4), \end{cases}$$

$$\mathrm{ord}_{q'}(2) = \begin{cases} 2q'' & \text{if } q'' \equiv 1 \pmod 4), \\ q'' & \text{if } q'' \equiv 3 \pmod 4), \end{cases}$$

Thus finally we have shown:

Proposition 27 *Let n be a superspecial* BLUM *integer. Let x be a quadratic residue* mod n *with $x \not\equiv 1 \pmod p$ and $x \not\equiv 1 \pmod q$. Then the BBS sequence* mod n *for x has period*

$$\nu = \begin{cases} p''q'' & \text{if } p'' \equiv q'' \equiv 3 \pmod 4, \\ 2p''q'' & \text{otherwise.} \end{cases}$$

If p'' and q'' are $(l-2)$-bit primes (hence $> 2^{l-3}$, and n is an l-bit integer), then the period is $> 2^{l-2}$ or about $n/4$.