A.13 The BBS Sequence

Let n be a positive integer. Let x be invertible $\bmod n$, and let $s := \mathrm{ord}(x)$ be its order in the multiplicative group $\bmod n$.

Lemma 26 *For each integer r we have*

$$r \equiv 1 \pmod{s} \Longleftrightarrow x^r \equiv x \pmod{n}.$$

Proof. "$\Longrightarrow$": Let $r = 1 + c \cdot s$. Then

$$x^r = x^{1+c\cdot s} \equiv x \cdot 1 = x \bmod n.$$

"$\Longleftarrow$": Dividing $\bmod n$ by the invertible element x gives

$$x^{r-1} \equiv 1 \pmod{n},$$

hence $s \mid r - 1$. $\diamond$

Now let $x_0 := x$, and define the **BBS sequence** of integers x_i by the recursive formula $x_i = x_{i-1}^2$ for $i \geq 1$, or

$$x_i = x^{2^i} \bmod n \quad \text{for } i = 0, 1, 2, 3, \ldots \tag{1}$$

Lemma 27 *The BBS sequence (x_i) is purely periodic if and only if $s = \mathrm{ord}(x)$ is odd. Then the period ν equals the multiplicative order of $2 \bmod s$.*

Proof. Assume the sequence is purely periodic with period ν. Then ν is minimal with $x_\nu \equiv x_0 \pmod{n}$. Hence

$$x_0^{2^\nu} \equiv x_0 \pmod{n}.$$

Thus $s \mid (2^\nu - 1)$ by Lemma 26, and ν is minimal with this property too, or with $2^\nu \equiv 1 \bmod s$. In particular s is odd, and ν is the order of $2 \bmod s$.

Conversely assume that s is odd. Then 2 is invertible $\bmod s$. Let μ be the multiplicative order of $2 \bmod s$. Then $2^\mu \equiv 1 \bmod s$, hence $x_\mu = x^{2^\mu} \equiv x_0 \bmod n$ by Lemma 26, thus the sequence is purely periodic. $\diamond$

Proposition 26 *Let n be a* Blum *integer and x be a quadratic residue $\neq 1 \bmod n$. Then the BBS sequence x_i as defined in (1) is purely periodic of period $\nu = \mathrm{ord}_s(2)$.*

Proof. Assume $n = pq$ where p and q are two different odd primes $\equiv 3 \bmod 4$. Let $p = 4k+3$ and $q = 4l+3$ with integers k and l. Then the multiplicative group $\mathbb{M}_n$ has order $(p-1)(q-1) = (4k+2)(4l+2)$. The group $\mathbb{M}_n^2$ of quadratic residues has index 4 in $\mathbb{M}_n$, hence order $(2k+1)(2l+1)$, an odd integer. Thus every quadratic residue has odd order, and Lemma 27 applies for x. $\diamond$

Corollary 4 *Let n be a* Blum *integer and ν, the period of a BBS sequence. Then $\nu \mid \lambda(\lambda(n))$ where λ is the* Carmichael *function.*

Proof. By Proposition 26 we have $\nu = \operatorname{ord}_s(2) \mid \lambda(s)$. Moreover $s = \operatorname{ord}_n(x) \mid \lambda(n)$, hence $\lambda(s) \mid \lambda(\lambda(n))$. We conclude that $\nu \mid \lambda(\lambda(n))$. $\diamond$