Bounds on the Size of S
by Kevin Hughes

I will show

Theorem

$$|S| \leq \frac{\varphi(n)}{2^{k-1}\prod p_i^{\alpha_i - 1}}$$

Proof

Let n be an odd number with $n-1 = 2^r b$ with b odd. Define $w(n)$ be the number of prime factors of n (let $k = w(n)$) and $v(n)$ to be the largest power of 2 that divides $p_i - 1$ for all i. So $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ where the p_i are primes. Similarly $p_i - 1 = 2^{r_i} b_i$ for all i. (a,b) means the gcd(a,b).

Consider the sets $S = \{a \in \mathbb{Z}/n | a^b = 1 \text{ or } a^{2^j b} = -1 \text{ for some } 0 \leq j < r\}$ and $\bar{S} = \{a \in \mathbb{Z}/n | a^{2^{v(n)-1} b} = \pm 1\}$. We know that $\bar{S}$ is generated by S, so that $S \subseteq \bar{S}$ which implies that $|S| \leq |\bar{S}|$.

So the strategy to prove the theorem for S is to show it for $\bar{S}$ then the thoerem follows.

It is known that

$$|\bar{S}| = 2 \cdot 2^{w(n)(v(n)-1)} \prod (b, p-1)$$

And since b is odd,

$$(b, p-1) \leq \frac{p-1}{2^{v(n)}}$$

Then

$$\frac{|\bar{S}|}{\varphi(n)} = \frac{2 \cdot 2^{w(n)(v(n)-1)} \prod (b, p-1)}{\prod p^{\alpha-1}(p-1)}$$

$$\leq \frac{2 \cdot 2^{k(v(n)-1)} \prod 2^{-v(n)}(p-1)}{\prod p^{\alpha-1}(p-1)}$$

$$= \frac{2 \cdot 2^{k(v(n)-1)} \cdot 2^{-kv(n)}}{\prod p^{\alpha-1}} = \frac{1}{2^{k-1}\prod p^{\alpha-1}}$$

Furthermore, if S is a group then for $|S| = |\bar{S}| \geq 2^{-k}, n$ must be square-free and $2^{v(n)} || p-1$ for all $p|n$ (otherwise you could pull out another power of 2 into the denominator). Also, if there exist a prime $p|n$ but $p-1 \nmid n-1$ then $(b, p-1) < (p-1)$ which implies that $\frac{p-1}{(b,p-1)} = x > 2$

$$|\bar{S}| \leq \frac{1}{x\dot{2}^{k-1}\prod p^{\alpha}} < \frac{1}{2^k}$$

Therefore n must be carmichael.

This is only done precisely for $|\bar{S}|$ but I will repeat the same ideas for S making the bounds as precise as possible and have that soon. So far though this confirms the computational work of Jamie Sloat.