An Elementary Proof for Problem 3

Kevin Hughes
Zach Jones

$n = \prod p_i^{\alpha_i}$ with $n - 1 = 2^r b$, b odd.

$$S = \{a \in \mathbb{Z}/n | a^b = 1 \text{ or } a^{2^j b} = -1 \text{ for some } 0 \leq j < r\}$$

and

$$G = \{a \in \mathbb{Z}/n | a^{(n-1/2)} = (\frac{a}{n})\}$$

Theorem S is a subgroup of G if and only if $k = 1$ or there exists $p_i \equiv 3 \bmod 4$.

Proof

($\Leftarrow$) *case 1* Suppose that $n = p^\alpha$, p an odd prime.

Lemma The only square roots of 1 are ± 1 in $\mathbb{Z}/(p^\alpha)$.

Proof Suppose $x^2 \equiv 1$, then $p^\alpha | x^2 - 1 = (x-1)(x+1)$. Since p is an odd prime, $p|x+1$ or $p|x-1$ which implies that $p^\alpha | x+1$ or $p^\alpha | x-1$.

Let $a_1, a_2 \in S$, $(a_1)^b = 1$ and $(a_2)^{2^j b} = -1$ for some j. That implies that $(a_1 a_2)^{2^j b} = -1$. So, assume that $(a_1)^{2^{j_1} b} = (a_2)^{2^{j_2} b} = -1$ and $a_1 a_2 \in S$. Let $j = \max\{j_i\}$ then $(a_1)^{2^j b}(a_2)^{2^j b} = (a_1 a_2)^{2^j b} = \pm 1$. If it is -1, then the theorem holds. But if it is 1, since the only squareroots of 1 are $\pm 1, a_1 a_2 \in S$.

case 2 Assume that there exists a prime $p \equiv 3 \bmod 4$. Without loss of generality call this p_1. Then $p_1 = 1 + 2b_1$ with b_1 odd. And let $a_1, a_2 \in S$ with $c_i = (a_i)^b$. Again, if $c_1 = 1$ then $a_1 a_2 \in S$. Otherwise, there exists j_1, j_2 such that $(c_1)^{2^{j_1}} \equiv (c_2)^{2^{j_2}} \equiv -1 \pmod{n} \Rightarrow (c_1)^{2^{j_1}} \equiv (c_2)^{2^{j_2}} \equiv -1 \pmod{p_1}$ $\Rightarrow (c_1)^{2^{j_1+1}} \equiv (c_2)^{2^{j_2+1}} \equiv 1 \pmod{p_1}$ which implies that $2^{j_1+1}, 2^{j_2+1} | p-1$ but that implies that $j_1 = j_2 = 0$ because 2 is the highest power of 2 that divides $p_1 - 1$. So $(a_1)^b = c_1 \equiv (a_2)^b = c_2 \equiv -1$. And thus, $(a_1)^b (a_2)^b = (a_1 a_2)^b \equiv 1$ which implies that $a_1 a_2 \in S$.

($\Rightarrow$) Proof (contrapositive).

Assume that all the $p_i \equiv 1 \bmod 4$. That implies that $\left(\frac{-1}{p_i^{\alpha_i}}\right) = 1$ for all i. That is there exists x_i such that $x_i^2 \equiv -1 \bmod p_i^{\alpha_i}$.

Let

$$x \equiv \begin{cases} x_1 \bmod p_1^{\alpha_1} \\ -x_i \bmod p_i^{\alpha_i} \quad i > 1 \end{cases}$$

$$y \equiv -x_i \bmod p_i^{\alpha_i}$$

Note that x and y exist by the chinese remainder theorem and that $y^2 = x^2 = -1(n)$. So $y^{2b} = x^{2b} = -1(n)$ since b is odd which implies that $x, y \in S$. But $(xy)^{2b} = 1(n)$ and

$$xy = \begin{cases} -x_1^2 \bmod p_1^{\alpha_1} \\ -x_i^2 \bmod p_i^{\alpha_i} \quad i > 1 \end{cases}$$

$$= \begin{cases} 1 \bmod p_1^{\alpha_1} \\ -1 \bmod p_i^{\alpha_i} \quad i > 1 \end{cases}$$

$\Rightarrow (xy)^b \not\equiv \pm 1 \bmod n \Rightarrow xy \notin S$.