Notes on Fermat Pseudoprimes

Proposition. Suppose that n is a composite number, and a is an integer such that $a^{n-1} \equiv 1 \pmod{n}$. Then

$$\frac{n-1}{\operatorname{ord}_n(a)} \geq 5,$$

except in the cases

$$n = 4, \quad a \equiv 1 \pmod{4}; \quad n = 9, \quad a \equiv -1 \pmod{9}$$

Here $\operatorname{ord}_n(a)$ is the multiplicative order of a module n.

Note that we have the equality if

$$n = 6601, \quad a \not\equiv \pm 1 \pmod{7} \quad a \not\equiv \pm 1 \pmod{23}, \quad a \text{ is a primitive root modulo } 41$$

(for example $a = 11$).

Proof. Let φ be the Euler totient function. We will consider the following cases respectively:
Case 1. n is an even number. Write $n = 2^\alpha q_1 \cdots q_r$, where q_i are coprime prime powers. Since $n-1$ is odd, the multiplicative order of a modulo 2^α and modulo each q_i should also be odd, so

$$a \equiv 1 \pmod{2^\alpha}, \quad a^{\varphi(q_i)/2} \equiv 1 \pmod{q_i},$$

hence

$$\operatorname{ord}_n(a) \leq 1 \cdot \frac{\varphi(q_1)}{2} \cdot \cdots \cdot \frac{\varphi(q_r)}{2} = \frac{\varphi(q_1) \cdots \varphi(q_r)}{2^r}.$$

We deduce that

$$\frac{n-1}{\operatorname{ord}_n(a)} \geq \frac{2^\alpha q_1 \cdots q_r - 1}{\frac{\varphi(q_1) \cdots \varphi(q_r)}{2^r}} \geq 2^{\alpha+r} - 1.$$

The inequality $\frac{n-1}{\operatorname{ord}_n(a)} \geq 5$ can only be violated when $\alpha = 2$ and $r = 0$, corresponding to the first exceptional case given.
Case 2. n is not squarefree. Write $n = p^\alpha m$, where $\alpha \geq 2$. Since $n-1$ is coprime to p, we must have $a^{p-1} \equiv 1 \pmod{p^\alpha}$, which is to say that p is a base-a Wieferich prime, so

$$\operatorname{ord}_n(a) \leq \operatorname{ord}_{p^\alpha}(a) \operatorname{ord}_m(a) \leq (p-1)\varphi(m),$$

and

$$\frac{n-1}{\operatorname{ord}_n(a)} \geq \frac{p^\alpha m - 1}{(p-1)\varphi(m)} \geq \frac{p^\alpha - 1}{p-1}.$$

The inequality $\frac{n-1}{\operatorname{ord}_n(a)} \geq 5$ can only be violated when $p = 2$ or 3, $\alpha = 2$ and $m = 1$, corresponding to the two exceptional cases given.

Case 3. n is odd and has at least three distinct prime factors. Write $m = q_1 \cdots q_r$, where q_i are coprime odd prime powers, then

$$\begin{aligned}\operatorname{ord}_n(a) &\le \operatorname{lcm}(\varphi(q_1), \cdots, \varphi(q_r)) = 2 \operatorname{lcm}\left(\frac{\varphi(q_1)}{2}, \cdots, \frac{\varphi(q_r)}{2}\right) \\ &\le 2 \cdot \frac{\varphi(q_1)}{2} \cdot \cdots \cdot \frac{\varphi(q_r)}{2} = \frac{\varphi(q_1) \cdots \varphi(q_r)}{2^{r-1}},\end{aligned}$$

so

$$\frac{n-1}{\operatorname{ord}_n(a)} \ge \frac{q_1 \cdots q_r - 1}{\frac{\varphi(q_1) \cdots \varphi(q_r)}{2^{r-1}}}.$$

Since $r \ge 3$, we have $q_1 \cdots q_r - 1 > \varphi(q_1) \cdots \varphi(q_r)$, so

$$\frac{n-1}{\operatorname{ord}_n(a)} \ge 2^{r-1} + 1 \ge 5.$$

Case 4. $n = pq$ is the product of two distinct primes. Note that we have

$$a^{\gcd(pq-1, p-1)} \equiv 1 \pmod{p}, \quad a^{\gcd(pq-1, q-1)} \equiv 1 \pmod{q}.$$

Since

$$\gcd(pq-1, p-1) = \gcd(pq - 1 - q(p-1), p-1) = \gcd(q-1, p-1)$$

and similarly $\gcd(pq-1, q-1) = \gcd(p-1, q-1)$, we have

$$a^{\gcd(p-1, q-1)} \equiv 1 \pmod{pq},$$

so

$$\frac{n-1}{\operatorname{ord}_n(a)} \ge \frac{pq-1}{\gcd(p-1, q-1)} > \frac{(p-1)(q-1)}{\gcd(p-1, q-1)} = \operatorname{lcm}(p-1, q-1).$$

This shows that $\frac{n-1}{\operatorname{ord}_n(a)} \ge 6$ if $\max\{p, q\} \ge 7$, and direct verification shows that $\frac{n-1}{\operatorname{ord}_n(a)} \ge 5$ for $p, q \in \{2, 3, 5\}$. $\square$