事实3 证明.

已知$a^r, a^{2r}, a^{2^2 r}, a^{2^3 r}, \cdots, a^{2^s r} \equiv 1$。

若不符合事实3的条件，必有

$a^{2^j r} \neq 1$而$a^{2^j r} \equiv 1 (0 \leq j \leq s-1)$,

因此,$\left(a^{2^j r}\right)^2 \equiv 1$，因此,$\left(a^{2^j r} - 1, n\right)$有非平凡因子与$n$是素数矛盾。

算法3 证明.

(1) $p_0 + 2jrs - 1 \equiv (2(s^{r-2} (\mathrm{mod}\, r))s - 1 + 2jrs - 1) \equiv 2(s^{r-2} (\mathrm{mod}\, r))s - 2 \equiv 2(s^{r-2} s - 1)$
$\equiv 0 (\mathrm{mod}\, r)$。

(2) $p_0 + 2jrs + 1 \equiv (2(s^{r-2} (\mathrm{mod}\, r))s + 2jrs) \equiv 0 (\mathrm{mod}\, s)$。

(3) $r - 1 \equiv 2it \equiv 0 (\mathrm{mod}\, t)$。