1. Число Кармайкла $\Rightarrow$ условия

а) не делится на квадрат.

От обратного. Пусть n делится на p^k, $k > 1$. p - простое.

$n = p^k \cdot m$

Тогда по КТО существует b: $b \equiv p+1$ и $b \equiv m$

$(b, m) = 1$ $(b, p^2) = 1 \Rightarrow (b, n) = 1$, а значит $b^{n-1} \equiv 1 \Rightarrow b^{n-1} \equiv 1$, $(1+p)^{n-1} \equiv 1$

$(1+p)^{n-1} \equiv 1 + (n-1)p + p^2 \ldots \equiv 1 + (n-1)p$

$1 + (n-1)p \equiv 1$

$np - p \equiv 0$

$\vdots p^2$

$p \equiv 0$ - невозможно

б) $n : p \Rightarrow n-1 : p-1$

Возьмём первообразный корень по модулю p, а

По тео КТО $\exists b$: $b \equiv a$ и $b \equiv 1$

$(b, p) = 1$, т.к. по прошлому пункту нет квадратов.

$(a, n) = 1$

$a^{n-1} \equiv 1 \pmod{n}$, по карманчиковости

$a^{n-1} \equiv 1 \pmod{p} \Rightarrow a^{n-1} \equiv 1 \pmod{p} \Rightarrow n-1 : p-1$; ЧТД

2. Карманчиковость $\Leftarrow$ условия

n - не делится на квадраты и $\forall p : n : p \Rightarrow$

$\Rightarrow n-1 : p-1$.

$n = p_1 \cdot p_2 \cdots \cdot p_k$

$(b, n) = 1$, то и $(p_1, n) = 1$ ....

$b^{p-1} \equiv 1 \pmod{p}$, но $n-1 : p-1$, то $b^{n-1} \equiv 1 \pmod{p}$

Очевидно, что $b^{n-1} \equiv 1 \pmod{p}$ и т.к. нет квадратов, то делим p

$b^{n-1} \equiv 1 \pmod{p_1 \cdot p_2 \cdots \cdot p_k} \Rightarrow b^{n-1} \equiv 1 \pmod{n}$. ЧТД