Il risultato principale di questa nota è l'esistenza di una *radice primitiva* nel gruppo moltiplicativo modulo un primo p. Si tratta del seguente teorema.

Teorema. *Sia p un numero primo. Allora esiste $\overline{x} \in \mathbf{Z}_p^*$ di ordine $p-1$.*

Il piccolo Teorema di Fermat dice che $\overline{x}^{p-1} = \overline{1}$, per ogni $\overline{x}$ in $\mathbf{Z}_p^*$. Questo implica che l'ordine di un elemento $\overline{x}$ di $\mathbf{Z}_p^*$ non può essere maggiore di $p-1$. Il valore $p-1$ è il più grande possibile. Siccome $\#\mathbf{Z}_p^* = p-1$, una conseguenza del teorema è che l'insieme $\mathbf{Z}_p^*$ consiste delle potenze $\overline{x}, \overline{x}^2, \ldots, \overline{x}^{p-1} = \overline{1}$ di $\overline{x}$. Ogni elemento di $\mathbf{Z}_p^*$ è quindi potenza di $\overline{x}$.

Un altro modo per esprimere il contenuto del Teorema è di dire che $\mathbf{Z}_p^*$ *è un gruppo ciclico.*

Lemma 1. *Sia n un numero naturale, allora*

$$\sum_{d|n} \varphi(d) \;=\; n,$$

dove d varia sui divisori positivi di n.

Dimostrazione. Esercizio.

Lemma 2. *Sia n un numero naturale e sia $x \in \mathbf{Z}$ con $\mathrm{mcd}(x,n) = 1$. Sia $a = \mathrm{ord}_n(x)$. Allora*

(a) Per ogni $k \in \mathbf{Z}$ il numero $\mathrm{ord}_n(x^k)$ divide $a = \mathrm{ord}_n(x)$.

(b) Si ha che $\mathrm{ord}_n(x^k)$ è uguale ad $a = \mathrm{ord}_n(x)$ se e solo se $\mathrm{mcd}(k,a) = 1$.

Dimostrazione. La dimostrazione della parte (a) è facile. Dimostriamo (b). Se d divide $\mathrm{mcd}(k,a)$, allora $(x^k)^{a/d} \equiv (x^a)^{k/d} \equiv 1 \pmod{n}$. Se quindi $\mathrm{mcd}(k,a) \neq 1$, allora l'ordine di $\overline{x}^k$ non è uguale a a. Viceversa, supponiamo che $\mathrm{mcd}(k,a) = 1$. Per la parte (a) sappiamo già che $b = \mathrm{ord}_n(x^k)$ divide $a = \mathrm{ord}_n(x)$. Per stabilire che a divide b, basta dimostrare che $x^b \equiv 1 \pmod{n}$.

Per il Teorema di Bézout esistono $\lambda, \mu \in \mathbf{Z}$ tali che $\lambda k + \mu a = 1$. Adesso abbiamo che

$$x^b = x^{b(\lambda k + \mu a)} = (x^k)^{b\lambda} \cdot (x^a)^{b\mu}.$$

Siccome l'ordine di x^k è b e siccome $x^a \equiv 1 \pmod{n}$, vediamo che l'espressione a destra è congrua a 1 (mod n). Quindi $x^b \equiv 1 \pmod{n}$ e concludiamo che a divide b come richiesto.

Lemma 3. *Sia p un numero primo e sia $f \in \mathbf{Z}_p[X]$ un polinomio monico di grado d. Allora f ammette al più di d zeri in $\mathbf{Z}_p$.*

Dimostrazione. Non c'è niente da dimostrare se f non ammette nessuno zero in $\mathbf{Z}_p$. Supponiamo che $f(\overline{a}) = \overline{0}$ per un certo $\overline{a} \in \mathbf{Z}_p$. Dividendo il polinomio $f(X)$ per $X - \overline{a}$, otteniamo un quoziente $g(X)$ e un resto $\overline{r} \in \mathbf{Z}_p$:

$$f(X) = g(X)(X - \overline{a}) + \overline{r}.$$

Quando sostituiamo $X = \overline{a}$ in questa relazione, troviamo che $\overline{r} = \overline{0}$. Sia $\overline{b}$ adesso un qualsiasi zero di $f(X)$; allora abbiamo che

$$\overline{0} = f(\overline{b}) = g(\overline{b})(\overline{b} - \overline{a}), \quad \text{in } \mathbf{Z}_p.$$

Siccome p *è primo* abbiamo che p divide $b-a$ oppure p divide $g(b)$. Nel primo caso abbiamo che $\overline{b} = \overline{a}$ e nel secondo caso $g(\overline{b}) = \overline{0}$. Adesso concludiamo per induzione: il polinomio $g(X)$ ha grado $d-1$ e non ammette più di $d-1$ zeri. Ci sono quindi al più $(d-1)+1 = d$ possibilità per $\overline{b}$.

Questo dimostra il Lemma.

Dimostrazione del Teorema. Per ogni numero naturale d definiamo

$$g(d) = \#\{\overline{y} \in \mathbf{Z}_p^* : \mathrm{ord}_p(y) = d\}.$$

Affermiamo che si ha $g(d) = 0$ oppure si ha $g(d) = \varphi(d)$. Infatti, se $g(d) \neq 0$, allora esiste $\overline{x} \in \mathbf{Z}_p^*$ di ordine d. Abbiamo che $\overline{x}^d = \overline{1}$ e quindi

$$\{\overline{x}, \overline{x}^2, \ldots, \overline{x}^d\} \quad \subset \quad \{\overline{y} \in \mathbf{Z}_p^* : \overline{y}^d = \overline{1}\}.$$

L'insieme a destra consiste, per definzione, degli zeri del polinomio $X^d - 1$. Per il Lemma 3, quest'insieme ha quindi al più d elementi. Siccome l'insieme a sinistra ha esattamente d elementi, abbiamo l'*uguaglianza*. Adesso consideriamo il sottoinsieme W degli elementi $\overline{y} \in \mathbf{Z}_p^*$ che hanno ordine *uguale* a d. Per definizione della funzione g, la cardinalità di W è uguale a $g(d)$. Abbiamo appena visto che W consiste in potenze di $\overline{x}$. Per il Lemma 2, il sottoinsieme W consiste esattamente nelle potenze $\overline{x}^i$ con $\mathrm{mcd}(i, d) = 1$. Ci sono quindi esattamente $\varphi(d)$ elementi in W. Concludiamo che $g(d) = \varphi(d)$ come affermato.

Adesso scriviamo $\mathbf{Z}_p^*$ come unione disgiunta dei sottoinsiemi di elementi che hanno lo stesso ordine d. Per il piccolo Teorema di Fermat abbiamo che

$$\sum_{d|p-1} g(d) = p - 1.$$

Per il Lemma 1 sappiamo che vale anche $\sum_{d|p-1} \varphi(d) = p - 1$. Siccome $0 \leq g(d) \leq \varphi(d)$ per ogni d, abbiamo quindi uguaglianza per ogni d. In particolare, troviamo che

$$\#\{\overline{x} \in \mathbf{Z}_p^* : \mathrm{ord}_p(x) = p - 1\} = \varphi(p - 1).$$

Siccome questo numero è almeno 1, abbiamo dimostrato il teorema.