THE MULTIPLICATIVE GROUP OF A FINITE FIELD
IS CYCLIC
UNDERGRADUATE SEMINAR

These notes present a self-contained proof of Lemma 7.1.5 in the
photocopied page (from the book "Abstract Algebra", by N. Herstein)
handed out in class:

**Lemma 7.1.5** Let $G$ be a finite abelian group so that for any $n$, the
number of $x \in G$ with $x^n = 1$ is at most $n$. Then $G$ is cyclic.

Let $G$ be a group. Recall the *order* of an element $x \in G$ is the least
integer $k \geq 1$ such that $x^k = 1$ (notation : $\text{ord}(x)$). A basic property
is that
$$x^k = 1 \text{ if and only if } \text{ord}(x) \mid k.$$ 
and that
$$\text{ord}(x) \mid \#G.$$

In your number theory course you should have seen the following
fact:

**Lemma 1.** $\text{ord}(x^j) = \text{ord}(x)/\gcd(j, \text{ord}(x))$

In particular, we see that in the cyclic group generated by $x$,
$$\#\{y \in \langle x \rangle : \text{ord}(y) = \text{ord}(x)\} = \#\{1 \leq j \leq \text{ord}(x) : \gcd(j, \text{ord}(x)) = 1\} = \phi(\text{ord}(x))$$

Denote by
$$f(d) := \#\{x \in G : \text{ord}(x) = d\}$$
Then $f(d) = 0$ unless $d \mid \#G$. We want to show that $f(\#G) \neq 0$. We
will in fact show that

**Proposition 2.** Let $G$ be a finite abelian group so that for any $n$, the
number of $x \in G$ with $x^n = 1$ is at most $n$. Then for all $d \mid \#G$,
$f(d) = \phi(d)$.

As a first step, we claim

**Lemma 3.** If $f(d) \neq 0$ then $f(d) = \phi(d)$. 
2 THE MULTIPLICATIVE GROUP OF A FINITE FIELD IS CYCLIC

Proof. Assume that \( f(d) \neq 0 \), that is there is some \( x_0 \in G \) with \( \text{ord}(x_0) = d \). We claim that under our assumptions,

\[ \{ y \in G : y^d = 1 \} = \{ x_0^j : 1 \leq j \leq d \} \]

Indeed, all elements on the RHS satisfy \( y^d = 1 \) and there are exactly \( d \) of them (why?), and by our assumptions there are no more solutions in \( G \) of this equation.

This implies that

\[ \{ y \in G : \text{ord}(y) = d \} = \{ x_0^j : \gcd(j, d) = 1 \} \]

Indeed, if \( \text{ord}(y) = d \) then certainly \( y^d = 1 \), and so \( y = x_0^j \) for some \( 1 \leq j \leq d \), and we know that \( \text{ord}(x^j) = d = \text{ord}(x_0) \) if and only if \( \gcd(j, \text{ord}(x_0)) = 1 \).

Thus if \( f(d) \neq 0 \) then

\[ f(d) = \# \{ 1 \leq j \leq d : \gcd(j, d) = 1 \} = \phi(d) \, . \]
as claimed. \( \square \)

We clearly have

(1) \[ \sum_{d | \#G} f(d) = \#G \]

-tthis says that every element has an order which divides \( \#G \). By Lemma 3, we have

(2) \[ \sum_{d | \#G} f(d) \leq \sum_{d | \#G} \phi(d) \]

We will thus prove Proposition 2 (why?), hence Lemma 7.1.5 , if we show:

Lemma 4. For every \( N \geq 1 \),

\[ \sum_{d | N} \phi(d) = N \]

Proof. In the cyclic group \( \mathbb{Z}/N\mathbb{Z} \) (with addition as the group law), we have \( f(d) = \phi(d) \) for all \( d \mid N \) because \( f(d) \neq 0 \), e.g. the element \( x = N/d \) has order exactly \( d \) in \( \mathbb{Z}/N\mathbb{Z} \). Applying (1) gives the claim. \( \square \)

Lemma 7.1.5 is used to show that any finite subgroup of the multiplicative group of a field is cyclic, because in a field the equation \( x^n = 1 \) has at most \( n \) solutions.