Finite Subgroups of F^* are Cyclic

S. Kumaresan
School of Math. and Stat.
University of Hyderabad
Hyderabad 500046
kumaresa@gmail.com

We denote by F a finite field and by F^*, the multiplicative group of nonzero elements of F.

Theorem 1. *$G := F^*$ is cyclic.*

Proof. We give two proofs of this result.

Proof (1): Let $N := |F^*|$. If $x \in G$, then x is of finite order, say k. That is, the cyclic subgroup generated by x contains k elements. In particular, k is a divisor of N, by Lagrange. If k is a divisor of N, let $\psi(k)$ denote the number of elements $x \in G$ whose order is k. Then $\psi(k) \geq 0$. We observe that $\sum_{k|N} \psi(k) = N$, as any element $x \in G$ will contribute to at most one $\psi(k)$.

Let φ denotes the Euler's phi-function. Recall that for any positive integer k, $\varphi(k)$ stands for those r such that $1 \leq r \leq k$ and r is relatively prime to k. We claim that $\psi(k) \leq \varphi(k)$ for any divisor k of N.

If $\psi(k) = 0$, the claim is obviously true. If $\psi(k) \geq 1$, we then claim $\psi(k) = \varphi(k)$. Let $x \in G$ be of order k. Let r, $1 \leq r \leq k$, be relatively prime to k. Then x^r is of order k. Hence $\psi(k) \geq \varphi(k)$. We claim that if $y \in G$ is of order k, then $y = x^r$ for an r relatively prime to k. For, otherwise, the equation $X^k = 1$ has at least $k+1$ solutions, x^j, $1 \leq j \leq k$ and y in the field F. Hence the claim that $\psi(k) \leq \varphi(k)$ for any dividor k of N is proved.

It is well-known that $\sum_{k|N} \varphi(k) = N$. (See below for a proof of this fact.) We thus arrive at

$$N = \sum_{k|N} \psi(k) \leq \sum_{k|N} \varphi(k) = N.$$

Thus equality holds everywhere. Since $\psi(k) \leq \varphi(k)$, we are led to conclude that $\psi(k) = \varphi(k)$ for all divisors k of N. In particular, when $k = N$, we get $\psi(N) = \varphi(N)$. Since 1 is relatively prime to N, we see that $\varphi(N) \geq 1$, and hence $\psi(N) \geq 1$. That is, there exists an element $a \in G$ which is of order N.

We now give a group-theoretic proof of $\sum_{k|N} \varphi(k) = N$. Let $C \equiv C_N$ denote the cyclic group of order N. If k is a divisor of N, then one knows that there is exactly one cyclic subgroup of order k and the number of generators of this cyclic group is $\varphi(k)$. Now as seen earlier, any $g \in C$ will have to lie in exactly one such cyclic subgroup, namely, the cyclic subgroup generated by g itself. Thus we have $N = \sum_{k|N} \varphi(k)$.

Proof (2): Let $a \in G$ be of maximal order, that is, the order of a is greater than or equal to the order of any $x \in G$. Since G is finite such an a exists. Let m be the order of a. Note that m is a divisor of N and hence $m \leq N$. If $x \in G$ has order $k > 1$, we claim that k divides m. (See Exercise below.) Thus $x^m = 1$ holds true for all $x \in G$. Thus the equation $X^m = 1$ has N solutions in the field F. But on the other hand, it can have at most m solutions. We therefore conclude that $N \leq m \leq N$. That is, $m = N$ or $a \in G$ is a generator of G. □

Ex. 2. Let G be an abelian group. Let x and y have orders m and n respectively.
(i) If m and n are relatively prime, then the order of xy is mn.
(ii) There exists an element $z \in G$ of order $\mathrm{l.c.m.}(m, n)$. *Hint:* Let $d = \gcd(m, n)$. Then $r := n/d$ and m are realtively prime.
(iii) Let m be the maximum of orders of elements of G. If a has order k, then k divides m.

Remark 3. Note that both the proofs yield the following stronger result. If G is a finite subgroup of the multiplicative group F^* of a field F, then G is cyclic.

Remark 4. The first proof yields the following result in group theory. If G is a group of order N and if for any divisor d of N, there exists at most one subgroup of order d in G, then G is cyclic.