This problem is extracted from Dummit and Foote, problems 9.5.5 and 9.5.6.

Let $\varphi(n)$ denote the *Euler φ-function*: for any positive integer n, $\varphi(n)$ is the number of positive integers less than or equal to n which are relatively prime to n. By convention, $\varphi(1) = 1$. You may use the following facts about φ:

- If p is prime, then $\varphi(p) = p-1$.
- If p^k is a power of a prime p, then $\varphi(p^k) = p^{k-1}(p-1)$.
- If a and b are relatively prime, then $\varphi(ab) = \varphi(a)\varphi(b)$.
- For any positive integer n, $\varphi(n)$ is the order of the group $(\mathbf{Z}/n\mathbf{Z})^\times$.

Prove the following:

(a) $\sum_{d|n} \varphi(d) = n$. (The notation here means: for every divisor d of n, add up the numbers $\varphi(d)$. For example, if $n = 6$, then the sum is $\varphi(1) + \varphi(2) + \varphi(3) + \varphi(6) = 1+1+2+2$.)

(b) Let F be a field and let G be a finite subgroup of the group of units $F^\times$. For any integer d, let $\psi(d)$ denote the number of elements of G of order d. Prove that $\psi(d) = \varphi(d)$ for every divisor d of $|G| = n$.

(c) Let $d = n$ to conclude that $\psi(n) \geq 1$, so G is cyclic. That is, *any finite subgroup of the group of units of a field is cyclic.*

Hints:

(a) Here are two approaches: (i) First prove the formula when n is a power of a prime. In general, write $n = p^m n'$ for some prime p and some integer n' not divisible by p; show that

$$\sum_{d|n} \varphi(d) = \sum_{d''|p^m} \varphi(d'') \sum_{d'|n'} \varphi(d'),$$

and use induction to finish the proof. (ii) Let C_n be a cyclic group of order n and show that since C_n contains a unique subgroup of order d for each factor d of n, the number of elements of C_n of order d is $\varphi(d)$. Hence $n = |C_n|$ is the sum of $\varphi(d)$ as d ranges over all divisors of n.

(b) For any integer N, $x^N - 1$ has at most N roots in F, and so $\sum_{d|N} \psi(d) \leq N$. Since $\sum_{d|N} \varphi(d) = N$, show by induction that $\psi(d) \leq \varphi(d)$ for every divisor d of n. Since $\sum_{d|n} \psi(d) = n = \sum_{d|n} \varphi(d)$, conclude that $\psi(d) = \varphi(d)$ for every divisor d of n.