Wedderburn's Theorem on Division Rings: A finite division ring is a field.

Necessary facts:

(1) If V is a vector space of dimension n over a finite field F with $|F| = q$ (note $q \geq 2$, because any field contains both a 0 and a 1), then because $V \cong F^n$ as vector spaces, we have $|V| = q^n$. In particular, if R is a finite ring containing a field F with q elements, then it is a vector space over F (ignoring the multiplication on R and just allowing addition of elements of R and multiplication by elements of F), so $|R| = q^n$ where $n = \dim_F(R)$.

(2) If q is an integer > 1, then for positive integers n, d, we have $q^d - 1$ divides $q^n - 1$ if and only if d divides n. [One direction is high school algebra: If $n = dk$, then $(q^n - 1)/(q^d - 1) = (q^d)^{k-1} + (q^d)^{k-2} + \ldots + q^d + 1$, which is an integer. The other direction is group theory: If $q^d - 1$ divides $q^n - 1$, i.e., if $q^n \equiv 1 \bmod (q^d - 1)$, then the order of q in the group $U(\mathbb{Z}_{q^d-1})$ of units in $\mathbb{Z}_{q^d-1}$ divides n; but that order, i.e., the smallest power of q that is congruent to to 1 mod $q^d - 1$, is clearly d.]

(3) Let n be a positive integer, and set $\zeta_n = \cos(2\pi/n) + i\sin(2\pi/n)$. Then for $j = 0, 1, \ldots, n-1$, we get

$$\zeta_n^j = \cos(2\pi j/n) + i\sin(2\pi j/n) \ .$$

The ζ_n^j's are the n complex numbers whose n-th power is 1, so they are called the "n-th roots of unity." In other words, they are all the n roots of the n-th degree polynomial $x^n - 1$. If j is not relatively prime to n, then a smaller power of ζ_n^j is equal to 1; the j's that *are* relatively prime to n give the ζ_n^j's whose order in the group $\mathbb{C} - \{0\}$ is exactly n; we call these ζ_n^j's the "primitive n-th roots of unity." The polynomial whose roots are the primitive n-th roots of unity,

$$\Phi_n(x) = \prod\{(x - \zeta_n^j) : \gcd(n, j) = 1\}$$

is called the "n-th cyclotomic polynomial." We get

$$\Phi_n(x) = \frac{x^n - 1}{\prod\{\Phi_d(x) : d|n, d < n\}} \ .$$

It follows from this quotient that each $\Phi_n(x)$ has integer coefficients. (Think about how to long-divide polynomials: As long as you are dividing by a polynomial in which the coefficient of the highest power of x is 1, which is true of all the $\Phi_n(x)$'s, you never need to introduce fractions. So the result follows by induction on the number of primes in the factorization of n.)

$$\Phi_1(x) = x - 1 \qquad \Phi_2(x) = \frac{x^2 - 1}{x - 1} = x + 1 \qquad \Phi_3(x) = \frac{x^3 - 1}{x - 1} = x^2 + x + 1$$

$$\Phi_4(x) = \frac{x^4 - 1}{(x-1)(x+1)} = x^2 + 1 \qquad \Phi_5(x) = \frac{x^5 - 1}{x - 1} = x^4 + x^3 + x^2 + x + 1$$

$$\Phi_6(x) = \frac{x^6 - 1}{(x-1)(x+1)(x^2 + x + 1)} = x^2 - x + 1$$

Pf of Wedderburn's Thm: Let D be a finite division ring. Then the center F of D, i.e., the set of elements of D that commute with every element of D, is a finite field; say it has q elements. Then, because D is a vector space over F, of dimension n, say, we have $|D| = q^n$ by (1) above. Also, if d is an element of D, then the set $Z(d)$ of elements that commute with d is a division ring containing F, and $|Z(d)| = q^m$ for some $m \leq n$ (again, by (1)) — strictly less than, if $d \notin F$. Thus, the class equation for the multiplicative group $D - \{0\}$ is

$$q^n - 1 = |D - \{0\}| = |F - \{0\}| + \sum_{i=1}^{r} [D - \{0\} : Z(d_i) - \{0\}] = q - 1 + \sum_{i=1}^{r} \frac{q^n - 1}{q^{m_i} - 1} ,$$

where $d_1, d_2, \ldots, d_r$ is a set of representatives of the conjugacy classes in $D - \{0\}$ that have more than one element, and $|Z(d_i)| = q^{m_i}$ for each i. Because each $(q^n - 1)/(q^{m_i} - 1) = [D - \{0\} : Z(d_i) - \{0\}]$ is an integer, we see that each m_i is a factor of n, by (2) above. For each $i = 1, 2, \ldots, r$, consider the quotient of polynomials

$$\frac{x^n - 1}{\Phi_n(x)(x^{m_i} - 1)} \ ;$$

the numerator is the product of all $\Phi_d(x)$ where $d|n$, and the denominator is the product of all $\Phi_d(x)$ where either $d|m_i$ or $d = n$; so the quotient is a product of the $\Phi_d(x)$'s where d is a proper divisor of n that does not divide m_i; hence the quotient is a polynomial with integer coefficients. Substituting the integer q for the variable x, we see that the integer $\Phi_n(q)$ divides the integer $(q^n - 1)/(q^{m_i} - 1)$. It follows from the class equation above that $\Phi_n(q)$ divides $q - 1$, because it divides all the other terms. Thus, $|\Phi_n(q)| \leq q - 1$. On the other hand, because 1 is the closest point, on the unit circle in $\mathbb{C}$, to the positive integer q, we have that for every primitive n-th root of unity ζ_n^j,

$$|q - \zeta_n^j| \geq q - 1 \geq 1 \ ,$$

and the first inequality is strict unless $\zeta_n^j = 1$, i.e., unless 1 is a primitive n-th root of unity, i.e., unless $n = 1$. So the product $|\Phi_n(q)|$ of the $|q - \zeta_n^j|$'s is greater than or equal to $q - 1$, with equality only if $n = 1$. Because $|\Phi_n(q)|$ is both at most $q - 1$ and at least $q - 1$, we have $|\Phi_n(q)| = q - 1$, and hence $n = 1$. But n was the dimension of D as a vector space over its center F, so $D = F$, and D is a field.//