WON Series in Discrete Mathematics and Modern Algebra Volume 5

# THE PRIMITIVE ROOT THEOREM

Amin Witno

**Abstract**

A primitive root $g$ modulo $n$ is when the congruence $g^x \equiv 1 \pmod{n}$ holds if $x = \phi(n)$ but not if $0 < x < \phi(n)$, where $\phi(n)$ is the Euler's function. The primitive root theorem identifies all the positive integers $n$ modulo which primitive roots exist. We give detailed proof of this theorem using elementary number theory and shortly discuss some connection with results in abstract algebra.

These notes[1] are written for a supplementary lecture in the Number Theory course (Math 313) at Philadelphia University, Jordan. Outline notes are more like a revision. No student is expected to fully benefit from these notes unless they have regularly attended the lectures.

## Appetizer

Throughout these notes, the integer $n$ is understood no less than 2. We use the notation $a\,\%\,n$ to mean the residue upon dividing the integer $a$ by $n$. In particular, when $a\,\%\,n = b\,\%\,n$ then we write $a \equiv b \pmod{n}$ and refer to $n$ as the modulus of the congruence. An earlier theorem which will be mentioned a few times in these notes is the so-called Chinese remainder theorem, abbreviated CRT.

**Theorem 1** (Chinese Remainder Theorem)**.** Let $\gcd(m, n) = 1$. Then $a \equiv b \pmod{mn}$ if and only if $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$.

We will also assume the familiar Euler's theorem, which we shall state after briefly reintroducing the Euler's phi function.

**Definition.** For a fixed $n$, let $R = \{x \in \{1, 2, \ldots, n-1\} \mid \gcd(x, n) = 1\}$. We define $\phi(n) = |R|$. Moreover, we define a *reduced residue system* modulo $n$, abbreviated RRS, to be any set $S$ with $|S| = \phi(n)$ such that $\{x\,\%\,n \mid x \in S\} = R$.

For example, for $n = 12$ we have $R = \{1, 5, 7, 11\}$. Hence $\phi(12) = 4$. In this case, an RRS modulo 12 can be any set of four integers as long as their residues form the set $R$, e.g., $\{5, 7, 11, 13\}, \{13, 17, 19, 23\}$, or simply $\{1, 5, 7, 11\}$.

To evaluate $\phi(n)$ in general, we go by factoring $n$ into primes and computing for each prime power according to the following rules.

[1] Copyrighted under a Creative Commons License

Last Revision: 21–04–2012

awitno@gmail.com

1. For any prime number $p$, we have $\phi(p) = p - 1$.
2. For any prime power $p^k$, we have $\phi(p^k) = p^k - p^{k-1}$.
3. If $\gcd(m, n) = 1$ then $\phi(mn) = \phi(m)\phi(n)$.

For example, since $1200 = 2^4 \times 3 \times 5^2$, we evaluate

$$\begin{aligned}
\phi(1200) &= \phi(2^4 \times 3 \times 5^2) \\
&= \phi(2^4) \times \phi(3) \times \phi(5^2) \\
&= (2^4 - 2^3) \times (3 - 1) \times (5^2 - 5) \\
&= 8 \times 2 \times 20 \\
&= 320
\end{aligned}$$

As a light exercise before we enter the main part of the discussion, try to prove the following fact concerning $\phi(n)$ which will prove useful later as we move on.

**Exercise 2.** The function $\phi(n)$ returns an even number for all $n \geq 3$.

**Theorem 3** (Euler's Theorem)**.** Let $\gcd(a, n) = 1$. Then $a^{\phi(n)} \equiv 1 \pmod{n}$.

# Main Course

Euler's theorem, in particular, allows us to proceed with the following definition of orders modulo $n$.

**Definition.** Let $\gcd(a, n) = 1$. By the *order* of $a$ modulo $n$, denoted by $|a|_n$, we mean the least positive integer $k$ for which $a^k \,\%\, n = 1$.

For example, let $a = 2$ and $n = 7$. We have $2^1 \,\%\, 7 = 2$, $2^2 \,\%\, 7 = 4$, and $2^3 \,\%\, 7 = 1$. Therefore, $|2|_7 = 3$. Because of Euler's theorem, we will always have $|a|_n \leq \phi(n)$. Also true, but not too obvious, is the fact that $|a|_n \mid \phi(n)$. We will illustrate this special relation using the example $n = 13$ and different values of $a$ in the range $1 \leq a \leq 12$. The following table displays the residues $a^k \,\%\, 13$, up to $k = \phi(13) = 12$, and the respective order $|a|_{13}$ for each number $a$, all of which are divisors of 12.

| $a$ | $a^2$ | $a^3$ | $a^4$ | $a^5$ | $a^6$ | $a^7$ | $a^8$ | $a^9$ | $a^{10}$ | $a^{11}$ | $a^{12}$ | $\|a\|_{13}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 4 | 8 | 3 | 6 | 12 | 11 | 9 | 5 | 10 | 7 | 1 | 12 |
| 3 | 9 | 1 | 3 | 9 | 1 | 3 | 9 | 1 | 3 | 9 | 1 | 3 |
| 4 | 3 | 12 | 9 | 10 | 1 | 4 | 3 | 12 | 9 | 10 | 1 | 6 |
| 5 | 11 | 8 | 1 | 5 | 11 | 8 | 1 | 5 | 11 | 8 | 1 | 4 |
| 6 | 10 | 8 | 9 | 2 | 12 | 7 | 3 | 5 | 4 | 11 | 1 | 12 |
| 7 | 10 | 5 | 9 | 11 | 12 | 6 | 3 | 8 | 4 | 2 | 1 | 12 |
| 8 | 11 | 5 | 1 | 8 | 11 | 5 | 1 | 8 | 11 | 5 | 1 | 4 |
| 9 | 3 | 1 | 9 | 3 | 1 | 9 | 3 | 1 | 9 | 3 | 1 | 3 |
| 10 | 9 | 12 | 3 | 4 | 1 | 10 | 9 | 12 | 3 | 4 | 1 | 6 |
| 11 | 4 | 5 | 3 | 7 | 12 | 2 | 9 | 8 | 10 | 4 | 1 | 12 |
| 12 | 1 | 12 | 1 | 12 | 1 | 12 | 1 | 12 | 1 | 12 | 1 | 2 |

**Theorem 4** (Order Divides Phi)**.** Let $\gcd(a,n)=1$. Then for any exponent $k\geq 1$, we have $a^k\equiv 1 \pmod{n}$ if and only if $|a|_n \mid k$. In particular, we have $|a|_n \mid \phi(n)$.

*Proof.* Let $|a|_n = m$, so that $a^m \,\%\, n = 1$, and choose a positive integer $k$. Then let $k \,\%\, m = r$ and write $k = mq + r$, where $q = \lfloor k/m \rfloor$. We have

$$a^k = a^{mq+r} = (a^m)^q \times a^r \equiv a^r \pmod{n}$$

In particular, since $r < m$, we must have $a^k \equiv 1 \pmod{n}$ if and only if $r = 0$, i.e., if and only if $m \mid k$. Combined with Euler's theorem, this result immediately gives the second claim, $|a|_n \mid \phi(n)$. ▽

Using the preceding theorem plus CRT, we may obtain another result on modular order which we will need later in proving our main theorem.

**Theorem 5.** Let $|a|_n = k$ and $|b|_n = l$ such that $\gcd(k,l) = 1$. Then $|ab|_n = kl$.

*Proof.* Let $|ab|_n = h$. We first claim that $a^{lh} \equiv 1 \pmod{n}$ by observing that

$$a^{lh} \equiv a^{lh}(b^l)^h = (ab)^{lh} = ((ab)^h)^l \equiv 1 \pmod{n}$$

Hence Theorem 4 implies that $k \mid lh$. However, as $\gcd(k,l) = 1$, we then have $k \mid h$. A completely symmetrical argument swapping the roles of $a$ and $b$ will give us $l \mid h$, which by CRT yields $kl \mid h$. On the other hand we can see that $h \mid kl$ upon observing that $(ab)^{kl} = (a^k)^l (b^l)^k \equiv 1 \pmod{n}$. Thus we conclude that $h = kl$, as desired. ▽

So we have seen that $|a|_n \mid \phi(n)$ and, in particular, the largest possible order of an integer modulo $n$ is $\phi(n)$. The peculiar case where $|a|_n = \phi(n)$ is the center of our attention throughout this lecture.

**Definition.** An integer $g$ such that $\gcd(g,n) = 1$ is called a *primitive root* modulo $n$ when $|g|_n = \phi(n)$.

In the table given earlier, we see that there are four primitive roots modulo 13, i.e., elements of order 12, namely 2, 6, 7, and 11. Note that these four correspond to the table rows in which the entries are all distinct. This is the first observation concerning primitive roots.

**Theorem 6.** Let $\gcd(g,n) = 1$. Then $g$ is a primitive root modulo $n$ if and only if the set $\{g, g^2, g^3, \ldots, g^{\phi(n)}\}$ is an RRS modulo $n$.

*Proof.* Let $G = \{g, g^2, g^3, \ldots, g^{\phi(n)}\}$. Note that every element of $G$ is relatively prime to $n$. Hence $G$ is an RRS modulo $n$ if and only if these powers of $g$ are all distinct modulo $n$, in which case $|g|_n = \phi(n)$ since $g^{\phi(n)} \equiv 1 \pmod{n}$ by Euler's theorem. On the other hand if $G$ is not an RRS, say $g^k \equiv g^h \pmod{n}$ with $1 \leq k < h \leq \phi(n)$, then $g^{h-k} \equiv 1 \pmod{n}$ with $h - k < \phi(n)$ and so $|g| < \phi(n)$. Thus the claim. ▽

The next observation is not too obvious: Consider the row of $2, 2^2, 2^3, \ldots$ in the previous table. With 2 being a primitive root, we know that this row forms an RRS modulo 13. Now observe that the four primitive roots modulo 13 come in the form $2^1 \equiv 2$, $2^5 \equiv 6$, $2^7 \equiv 11$, and $2^{11} \equiv 7$. What do we know about the exponents 1, 5, 7, 11? They form an RRS modulo 12! This fact generalizes to a result which enables us to count ahead of time the number of primitive roots modulo a given $n$.

**Theorem 7.** Let $g$ be a primitive root modulo $n$. Then $g^m$ is also a primitive root modulo $n$ if and only if $m$ is relatively prime to $\phi(n)$.

*Proof.* Let $|g^m| = k$ and $\phi = \phi(n)$. Since $|g| = \phi$ and $g^{mk} \equiv 1 \pmod{n}$, we have that $\phi \mid mk$. Meanwhile, we also have $(g^m)^\phi \equiv 1 \pmod{n}$, so that $k \mid \phi$. Now if $\gcd(m, \phi) = 1$ then the relation $\phi \mid mk$ implies $\phi \mid k$, in which case $k = \phi$ and $g^m$ is a primitive root. But if $\gcd(m, \phi) = d > 1$ then

$$(g^m)^{\phi/d} = (g^\phi)^{m/d} \equiv 1 \pmod{n}$$

In this case $k \leq \phi/d < \phi$, showing that $g^m$ is not a primitive root modulo $n$. ▽

**Corollary 8.** If any exists, there are exactly $\phi(\phi(n))$ primitive roots modulo $n$.

*Proof.* Let $g$ be a primitive root modulo $n$. To see how many primitive roots we have, according to Theorem 6 it suffices to count from the RRS $\{g, g^2, g^3, \ldots, g^{\phi(n)}\}$. Theorem 7 then tells us exactly when the exponent $m$ in the range $1 \leq m \leq \phi(n)$ yields a primitive root $g^m$. The number of such $m$ is given by $\phi(\phi(n))$. ▽

Note that the corollary applies only when at least one primitive root modulo $n$ exists. In fact, for some $n$ there will be no primitive roots at all. For example, let $n = 8$, for which an RRS is $\{1, 3, 5, 7\}$. Observe that $a^2 \,\%\, 8 = 1$ for each $a$ in this RRS. This shows that the order of $a$ is at most 2 and will never equal $\phi(8) = 4$. We conclude that no primitive root exists modulo 8.

Therefore, we wish to know when we have and when we do not have primitive roots, for a given modulus $n$. The complete answer is stated in the so-called primitive root theorem, whose proof is the main reason for this lecture.

**Theorem 9** (The Primitive Root Theorem)**.** Let $n$ equal 2 or an odd prime power. Then there exist primitive roots modulo $n$ and also modulo $2n$. There are no primitive roots with any other moduli.

To prove the primitive root theorem, hencefoth abbreviated PRT, we break it down into a number of smaller claims. The case $n = 2$ is, of course, quite trivial to verify. The next first observation sheds light on the "$2n$" part in the statement of the theorem.

**Lemma 10.** Let $n$ be an odd modulus. There are primitive roots modulo $n$ if and only if there are modulo $2n$.

*Proof.* Note that $\phi(2n) = \phi(n)$ since $n$ is odd. Let us consider an odd number $g$. The relation $g^k \equiv 1 \pmod{2}$ holds for an arbitrary exponent $k$, hence by CRT, $g^k \equiv 1 \pmod{n}$ if and only if $g^k \equiv 1 \pmod{2n}$. In particular, $g$ is a primitive root modulo $n$ if and only if $g$ is modulo $2n$. Now observe that by definition a primitive root modulo $2n$ is necessarily odd, whereas an even number $h$ can be a primitive root modulo $n$. In the latter case, the number $h + n$, being of the same residue class, will be an odd primitive root modulo $n$. In other words, a primitive root modulo $2n$ is also a primitive root modulo $n$, and conversely, a primitive root modulo $n$ leads to a (possibly different) primitive root modulo $2n$. ▽

The next lemma reveals why primitive roots cannot exist when the modulus $n$ has more than one odd prime factor.

**Lemma 11.** Suppose that $p \mid n$ for some odd prime $p$. If there is a primitive root modulo $n$, then either $n = p^k$ or $n = 2p^k$ for some integer $k \geq 1$.

*Proof.* Write $n = mp^k$ for some integer $m$ with $p \nmid m$. Let us assume that $m \geq 3$ and we will show that primitive roots modulo $n$ do not exist. To start, note that $\phi(n) = \phi(m)\phi(p^k)$, where both $\phi(m)$ and $\phi(p^k)$ are even numbers. (Your Exercise 2!) For any integer $a$ relatively prime to $n$, we have

$$a^{\phi(n)/2} = (a^{\phi(m)})^{\phi(p^k)/2} \equiv 1 \pmod{m}$$

and similarly

$$a^{\phi(n)/2} = (a^{\phi(p^k)})^{\phi(m)/2} \equiv 1 \pmod{p^k}$$

both by Euler's theorem. It follows that $a^{\phi(n)/2} \equiv 1 \pmod{n}$ by CRT, showing that $|a|_n \leq \phi(n)/2$, and that is why there can be no primitive roots. ▽

The preceding two lemmas leave us with two items left in order to claim PRT: (1) that primitive roots exist modulo any odd prime power and (2) that primitive roots do not exist modulo a power of two higher than the second. We deal with (2) first.

**Lemma 12.** Let $n = 2^k$ with $k \geq 3$. Then there are no primitive roots modulo $n$.

*Proof.* For $k = 3$, we have seen why there are no primitive roots modulo 8, i.e., because $a^2 \equiv 1 \pmod{8}$ for all odd numbers $a$, whereas to have a primitive root we need an odd number of order $\phi(8) = 4$. We proceed by induction on $k$ to show that

$$a^{2^{k-2}} \equiv 1 \pmod{2^k} \tag{1}$$

for all odd numbers $a$, the order of which will never reach $\phi(2^k) = 2^{k-1}$. In fact, if we assume (1) then there is a number $m$ such that $a^{2^{k-2}} = 1 + m2^k$. Square both sides of this equality and we get

$$a^{2^{k-1}} = 1 + m2^{k+1} + m^2 2^{2k} \equiv 1 \pmod{2^{k+1}}$$

Thus the induction step is justified. ▽

We are now down to one last claim: that we have primitive roots modulo $p^k$, where $p$ is any odd prime. We choose to first assume that primitive roots exist modulo $p$—whose proof we save for last—and then see that we do not need to look far to find a primitive root modulo $p^k$ for all $k \geq 2$. This step will take two lemmas.

**Lemma 13.** Let $g$ be a primitive root modulo an odd prime $p$ such that $g^{p-1} \not\equiv 1 \pmod{p^2}$. Then $g^{\phi(p^k)} \not\equiv 1 \pmod{p^{k+1}}$ for all $k \geq 1$.

*Proof.* The stated condition is merely the base case $k = 1$ for an inductive proof. The induction step goes as follows. Euler's theorem allows us to write $g^{\phi(p^k)} = 1 + mp^k$. The induction hypothesis implies that $p \nmid m$. Since $\phi(p^{k+1}) = p^{k+1} - p^k = \phi(p^k) \times p$, the binomial theorem (explained in the appendix) applies to give us

$$g^{\phi(p^{k+1})} = (1 + mp^k)^p \equiv 1 + mp^{k+1} \not\equiv 1 \pmod{p^{k+2}}$$

as desired. ▽

**Lemma 14.** Let $g$ be a primitive root modulo an odd prime $p$. Then either $g$ or $g+p$ is a primitive root modulo $p^k$ for all $k \geq 1$.

*Proof.* Consider first the case where $g^{p-1} \not\equiv 1 \pmod{p^2}$, in which we will prove our claim by showing that for all $k \geq 1$,

$$|g|_{p^k} = \phi(p^k) = p^{k-1}(p-1) \tag{2}$$

Well, (2) already holds for $k=1$, so let us proceed by induction. Let $|g|_{p^{k+1}} = m$. Then the congruence $g^m \equiv 1 \pmod{p^k}$ implies, assuming (2), that $p^{k-1}(p-1) \mid m$. At the same time, we have $m \mid \phi(p^{k+1}) = p^k(p-1)$. That leaves only two possibilities: either $m = \phi(p^{k+1})$ as we wish, or else $m = p^{k-1}(p-1) = \phi(p^k)$. Thanks to the preceding lemma, it is not possible to have $|g|_{p^{k+1}} = \phi(p^k)$, so we are done.

Now in case $g^{p-1} \equiv 1 \pmod{p^2}$, we will instead consider $g+p$, which is still a primitive root modulo $p$ and which, by the binomial theorem, satisfies the condition

$$(g+p)^{p-1} \equiv g^{p-1} + (p-1)g^{p-2}p \equiv 1 - g^{p-2}p \not\equiv 1 \pmod{p^2}$$

as $p \nmid g$. The same argument as before now implies that $g+p$ is a primitive root modulo all powers of $p$. ▽

Thus, let us deal with the final task: primitive roots modulo an odd prime. Just for convenience, however, we will include the prime 2 in the coming propositions since the results, though trivial, also hold modulo 2. This last section is actually not as easy as it may seem, but not too hard either. We break the proof in three parts.

**Lemma 15.** Consider a polynomial with integer coefficients of the form

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_kx^k$$

and let $p$ denote a prime such that $p \nmid a_k$. (This is to say that the *degree* of $f(x)$ is $k$ modulo $p$.) Then $f(x)$ can have at most $k$ zeros modulo $p$. In other words, no more than $k$ elements in the RRS $\{1, 2, \ldots, p-1\}$ can be a solution to the congruence $f(x) \equiv 0 \pmod{p}$.

*Proof.* We use induction. For $k=0$, it is clear that $f(x) = a_0$ has no zero (i.e., zero zero!) modulo $p$ as $p \nmid a_0$. Now assume that the claim is already true for all polynomials of degree up to $k-1$ modulo $p$. If $f(x)$ has less than $k$ zeros, we have nothing to prove; otherwise let $z_1, z_2, \ldots, z_k$ denote $k$ distinct zeros of $f(x)$ modulo $p$. Then we let

$$g(x) = f(x) - a_k(x-z_1)(x-z_2)\cdots(x-z_k)$$

Note that the degree of $g(x)$, if any, is strictly less than $k$ and yet $g(z_i) \equiv 0 \pmod{p}$ for the $k$ values of $z_i$. The induction hypothesis forces that $g(x)$ be the zero polynomial modulo $p$. It follows that

$$f(x) \equiv a_k(x-z_1)(x-z_2)\cdots(x-z_k) \pmod{p}$$

Therefore, as $p$ is a prime number, $f(x) \equiv 0 \pmod{p}$ if and only if $p$ divides one of the $k$ brackets on the right hand side, i.e., if and only if $x \equiv z_i \pmod{p}$. Thus we have proved that any zero of $f(x)$ must come from among these $k$ already here, and the induction is complete. ▽

**Lemma 16.** Suppose that $d \mid p-1$ for some prime number $p$. Then the polynomial $x^d - 1$ has exactly $d$ zeros modulo $p$.

*Proof.* Write $p-1 = dk$ and let $f(x) = 1 + x^d + (x^d)^2 + \cdots + (x^d)^{k-1}$. Then we have the relation

$$x^{p-1} - 1 = (x^d - 1)f(x)$$

Now Euler's theorem says that $a^{p-1} \equiv 1 \pmod{p}$ for all $a \in \{1, 2, \ldots, p-1\}$, hence the polynomial $x^{p-1} - 1$ has $dk$ zeros modulo $p$. Since $p$ is prime, every zero of $x^{p-1} - 1$ must be a zero of either $x^d - 1$ or of $f(x)$. But the preceding lemma says that both $x^d - 1$ and $f(x)$ have at most $d$ and $dk - d$ zeros, respectively. This is possible only when $x^d - 1$ has *exactly* $d$ zeros and $f(x)$ exactly $dk - d$ zeros. $\bigtriangledown$

At last, we establish PRT with the following proposition, itself quite an important result.

**Theorem 17.** There are exactly $\phi(p-1)$ primitive roots modulo every prime $p$.

*Proof.* The quantity $\phi(p-1)$ is, of course, given by Corollary 8 once we show that we have at least one primitive root.

Let $q$ be a prime such that $q^k \mid p-1$ for any fixed exponent $k \geq 1$. We will show that there exists an integer $a$ such that $|a|_p = q^k$. Well, the preceding lemma allows us to consider the $q^k$ zeros of the polynomial $x^{q^k} - 1$ modulo $p$. If $a$ is one of these zeros, then the congruence $a^{q^k} \equiv 1 \pmod{p}$ implies that $|a|_p \mid q^k$ by Theorem 4. Hence, $|a|_p = q^j$ where $0 \leq j \leq k$. Now if $j < k$ then $a$ would be a zero of the polynomial $x^{q^{k-1}} - 1$, for which again Theorem 4 says that there are only $q^{k-1}$ such zeros. It follows that we actually have $q^k - q^{k-1}$ choices for an integer $a$ with $|a|_p = q^k$.

To complete the proof, we factor $p-1$ into prime powers of the form $p - 1 = \prod q^k$. For each prime power $q^k$, we find as above an element $a_q$ such that $|a_q|_p = q^k$. Then Theorem 5 applies to enable us to construct the integer $g = \prod a_q$, whose order modulo $p$ is $\prod q^k = p - 1$; thus a primitive root modulo $p$. $\bigtriangledown$

Please note the interesting quantity $q^k - q^{k-1} = \phi(q^k)$ appearing in the above proof.

# Side Dish

As a passing remark, students who have studied Abstract Algebra may realize that primitive roots are really generators for the group $U_n$, i.e., the multiplicative group of units of integers modulo $n$. Hence, the group $U_n$ is cyclic if and only if there is a primitive root modulo $n$: exactly for the values of $n$ stated in PRT.

Just for fun, we will now demonstrate an alternate proof for the existence of a primitive root modulo a prime using the language of abstract algebra. We shall assume some common notation and results, with or without proofs, but bear in mind that this section is strictly for advanced students.

Let $G$ be a group and $a \in G$. Recall that a cyclic subgroup generated by $a$ is given in the form $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$. The order of $a$ in $G$ is then defined by $|a|_G = |\langle a \rangle|$. It is known that the order of any group element must divide the order of the group. In fact, the order of any subgroup must divide the order of the group.

If it happens that $\langle a \rangle = G$ then we call the group $G$ cyclic. The following fact concerning cyclic groups is quite well known, and we will rely on it to prove another result involving the Euler's phi function.

**Theorem 18.** Let $G$ be a cyclic group of order $n$. Then $G$ has a unique subgroup of order $d$ if $d \mid n$, and no subgroup of order $d$ if $d \nmid n$.

**Theorem 19.** We have $n = \sum \phi(d)$, where the sum ranges over all divisors $d \mid n$.

*Proof.* Consider a cyclic group $G$ of order $n$ and let $a$ have order $d$ in $G$. Write $\langle a \rangle = \{a, a^2, a^3, \ldots, a^d\}$, where $a^d = e$, the identity element of $G$. We can think of $\langle a \rangle$ like the RRS of Theorems 6 and 7. In this case, we see that $a^m$ have order $d$ if and only if $\gcd(m, d) = 1$, and so there are $\phi(d)$ elements of order $d$ in the subgroup $\langle a \rangle$. And if $b \in G$ is any other element of order $d$, then $\langle b \rangle = \langle a \rangle$ by the preceding theorem. We conclude that $G$ contains *exactly* $\phi(d)$ elements of order $d$. Moreover, Theorem 18 allows us to partition the elements of $G$ according to their order $d$, all of which form the complete divisors of $n$. Thus the claim $\sum \phi(d) = n$. $\triangledown$

It will take two more lemmas in order to reach our goal of proving that the group $U_p$ is cyclic, provided that $p$ is a prime number.

**Lemma 20.** Let $G$ be a finite group with identity element $e$. Suppose that $x^k - e$ has at most $k$ zeros in $G$ for every $k \geq 1$. Then $G$ is cyclic.

*Proof.* Let $|G| = n$ and choose an element $a \in G$. Suppose that the cyclic subgroup $\langle a \rangle$ has order $d$. Then every $x \in \langle a \rangle$ satisfies the relation $x^d = e$, hence by assumption, *all* the zeros of $x^d - e$ belong to $\langle a \rangle$. In particular, if an element $b \in G$ has order $d$, then $b \in \langle a \rangle$ and therefore, $\langle b \rangle = \langle a \rangle$. We conclude that *if* there is an element of order $d$ in $G$, then there are exactly $\phi(d)$ such elements. With the fact that such $d$ must divide $n$, in order to meet the equality $\sum \phi(d) = n$ from Theorem 19, we see it necessary that $G$ have an element of order $d$ for *every* divisor $d \mid n$. In particular, there is an element of order $n$, i.e., one that generates $G$ as a cyclic group. $\triangledown$

**Lemma 21.** Let $F$ be a field. Every polynomial of degree $k$ over $F$ has at most $k$ zeros.

*Proof.* We use the fact that if $z$ is a zero of $f(x)$ over a field, then $f(x) = (x-z)g(x)$ for some polynomial $g(x)$ of degree one less than that of $f(x)$. Moreover, another property of a field, any other zero of $f(x)$ would then be a zero of $g(x)$. This situation calls for a proof by induction, where the base case $k = 0$ is trivial since a constant polynomial has no zero. $\triangledown$

**Theorem 22.** Let $F$ be a finite field. The multiplicative group $F^* = \{x \in F \mid x \neq 0\}$ is cyclic. In particular, if $p$ is a prime number, then the group $U_p$ is cyclic.

*Proof.* The result is an obvious consequence of the two lemmas applied to the finite group $F^*$. The group $U_p$, where $p$ is prime, is none other but the set of nonzero elements of the field $\mathbb{Z}_p$ as a special case. $\triangledown$

# Dessert

The binomial theorem employed in Lemmas 13 and 14 refers to the following formula for expanding powers of a binomial over the real numbers.

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$$

The notation $\binom{n}{k}$ stands for the binomial coefficient and is given by

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!}$$

In particular, $\binom{n}{0} = 1$ and $\binom{n}{1} = n$. Hence for example, with $x = 1$ and $n = 7$, the formula writes as follows.

$$(1+y)^7 = 1 + 7y + 21y^2 + 35y^3 + 35y^4 + 21y^5 + 7y^6 + y^7$$

To prove the binomial theorem, you just need to write out the $n$ brackets

$$(x+y)(x+y)\cdots(x+y)$$

and observe that each like term comes by collecting $x$-terms from $n-k$ brackets and $y$-terms from the remaining $k$ brackets. How many terms of this kind will determine the coefficient $\binom{n}{k}$, and that is the number of ways we can choose $k$ elements out of $n$. If ordering were important, there would be

$$n\,(n-1)\,(n-2)\,\cdots\,(n-k+1)$$

choices. Without ordering, we just need to divide this quantity by $k!$, i.e., the number of ways we can permute the $k$ selections. Thus,

$$\binom{n}{k} = \frac{n\,(n-1)\,(n-2)\,\cdots\,(n-k+1)}{k!}$$

Now multiply denominator and numerator by $(n-k)!$ and we are set.

## Take Away

Students who are interested to learn more about primitive roots, or elementary number theory in general, may wish to look up my text *Theory of Numbers,* BookSurge Publishing 2008. In particular, the fifth chapter, which deals with the topic of primitive roots, is available on the Internet as a pdf file at the following address.

`http://www.witno.com/numbers/chap5.pdf`