When is $U(n)$ Cyclic? An Algebraic Approach

David R. Guichard
Whitman College
Walla Walla, WA 99362

Early in a typical abstract algebra course we learn that the set $U(n) = \{0 < x \leq n \mid \gcd(x, n) = 1\}$ is a group under multiplication mod n for every $n \geq 1$. This first appears as example 11 in Chapter 2 of Gallian's excellent text [2], for instance. These groups are particularly nice: it is not hard to see, but not immediately obvious, that they *are* groups; they are important in some modern cryptographic applications; and they figure prominently in elementary number theory.

Some of the groups $U(n)$ are cyclic and some are not, and the two categories can be completely characterized by the form of the prime factorization of n. If $U(n)$ is cyclic then we can write $U(n) = \langle g \rangle$ for some $g \in \mathbb{Z}_n$, relatively prime to n. In number theory g is known as a *primitive root* modulo n; we will call the characterization of those n with primitive roots the *Primitive Root Theorem*, or *PRT*.

I recently taught an abstract algebra course using Gallian's text, and I wanted to prove the PRT for the class. Though this result is standard in elementary number theory books (See, e.g., in [3]), the number-theoretic notation and proofs would have led me farther afield than I cared to go. I failed to find an algebraic proof of the result, but put one together by mining the proof in [3] for hints. The proof uses many results and exercises from [2]; this made it a satisfying conclusion to my course. Most of the proof requires only group theory, though some field theory and experience with polynomial rings is required at the very end.

This proof should be accessible to students who have been through any standard undergraduate course. I will refer explicitly to theorems and exercises in [2].

Here is what we are shooting for:

THEOREM. (*Primitive Root Theorem*) *$U(n)$ is cyclic if and only if n is 1, 2, 4, p^k, or $2p^k$, where p is an odd prime and $k \geq 1$.*

Preliminaries First, we need some facts from number theory. The number of elements in $U(n)$ is commonly denoted by $\phi(n)$, the *Euler phi-function* or *totient function*. When p is prime, $\phi(p) = p - 1$, because every number in $\{1, 2, \ldots, p-1\}$ is relatively prime to p. Also, $\phi(p^k) = p^k - p^{k-1}$ for

prime p, because precisely p^{k-1} of the p^k integers in $\{1, 2, \ldots, p^k\}$ are multiples of p, and all other integers in that range that are relatively prime to p^k. Note for future reference that if p is an odd prime, or if $p = 2$ and $k \geq 2$, then $p^k - p^{k-1}$ is even. (This is all we will need about ϕ, but it is also true that if m and n are relatively prime then $\phi(mn) = \phi(m)\phi(n)$. Thus $\phi(n) = \prod_{i=1}^{k}(p_i^{a_i} - p_i^{a_i-1})$ if $n = \prod_{i=1}^{k} p_i^{a_i}$ is the prime factorization of n.)

It is easy to check the primitive root theorem for $n = 1$, 2, 4 directly. (Don't take my word for it—do it!)

Recall that every cyclic group has exactly one subgroup of order d for each d that divides the order of the group. Thus we may show that $U(2^k)$ is not cyclic for $k > 2$ by showing that $U(2^k)$ contains two distinct elements of order 2, each of which generates a subgroup of order 2. We leave this as an exercise; it is number 54 in chapter 4 of Gallian.

In Chapter 8, *External Direct Products*, Gallian characterizes the direct products that are cyclic groups:

> *If $G \cong G_1 \oplus \cdots \oplus G_m$, then G is cyclic if and only if the G_i are cyclic and their orders are pairwise relatively prime.*

Gallian also proves (modulo some exercises left to the reader) that if $m = n_1 n_2 \cdots n_k$, and the n_i are pairwise relatively prime, then $U(m) \cong U(n_1) \oplus \cdots \oplus U(n_k)$. It is now not hard to see that $U(n)$ is not cyclic if n is divisible by two distinct odd primes or by 4 and an odd prime, using the fact (mentioned earlier) that $p^k - p^{k-1}$ is even when p is an odd prime or $p = 2$ and $k \geq 2$, together with $U(\prod_{i=1}^{k} p_i^{a_i}) \cong U(p_1^{a_1}) \oplus \cdots \oplus U(p_k^{a_k})$. (Exercise 46 of Chapter 8 is essentially this result.)

Now we know that the only groups that might be cyclic are $U(p^k)$ and $U(2p^k)$. (A different algebraic proof of this much appeared in [1].)

In what follows, p always denotes an odd prime. Since $U(2p^k) \cong U(2) \oplus U(p^k) \cong U(p^k)$, we need only show that $U(p^k)$ is cyclic. We will show that, if $U(p)$ is cyclic, then $U(p^2)$ is cyclic; that this implies that $U(p^k)$ is cyclic for $k > 2$; and, finally, that $U(p)$ is cyclic.

If G is a finite group, every $g \in G$ has an *order*, denoted $|g|$, which is the smallest positive integer m such that $g^m = e$ (e is the identity of the group). Recall that $g^k = e$ if and only if $|g|$ divides k, and that Lagrange's Theorem tells us that $|g|$ divides $|G|$.

For the first step, we suppose that $U(p)$ is cyclic and show that $U(p^2)$ is cyclic. Let $U(p) = \langle g \rangle$, $g \in \{1, 2, \ldots, p-1\}$. We will show that either g or $g + p$ generates $U(p^2)$. Let h_t be the order of $g + tp$, $t = 0$ or 1, so that $(g + tp)^{h_t} \equiv 1 \pmod{p^2}$; then $(g + tp)^{h_t} \equiv 1 \pmod{p}$ as well. Now

$$1 \equiv (g + tp)^{h_t} = g^{h_t} + \binom{h_t}{1} g^{h_t - 1} tp + \binom{h_t}{2} g^{h_t - 2} (tp)^2 + \cdots + (tp)^{h_t} \equiv g^{h_t} \pmod{p},$$

so the order of g in $U(p)$ divides h_t, that is, $(p-1)$ divides h_t. Since h_t is the order of an element of $U(p^2)$, we also know that h_t divides $|U(p^2)| = p(p-1)$. Thus, $h_t = p-1$ or $h_t = p(p-1)$; we want to show that the latter is true for at least one of $t = 0$ or $t = 1$. Suppose not, so that

$$g^{p-1} \equiv (g+p)^{p-1} \equiv 1 \pmod{p^2}.$$

Then

$$(g+p)^{p-1} = g^{p-1} + \binom{p-1}{1} g^{p-2}p + \binom{p-1}{2} g^{p-3}p^2 + \cdots + p^{p-1},$$

or, modulo p^2,

$$1 \equiv 1 + (p-1)g^{p-2}p, \quad \text{so} \quad 0 \equiv (p-1)g^{p-2}p.$$

But p^2 does not divide $(p-1)g^{p-2}p$. This contradiction implies that either g or $g+p$ has order $p(p-1)$, and generates $U(p^2)$.

Now we suppose that g generates $U(p^2)$ and show that g generates $U(p^k)$, $k \geq 2$. We proceed by induction. Suppose that g generates $U(p^2)$ and $U(p^i)$, for all i such that $2 \leq i \leq k$, where $k \geq 2$. In particular, in $U(p^k)$, the order of g is $p^{k-1}(p-1)$ and, if $k > 2$, in $U(p^{k-1})$ the order of g is $p^{k-2}(p-1)$. Let h denote the order of g in $U(p^{k+1})$; we want to show that $h = p^k(p-1)$. Since $g^h \equiv 1 \pmod{p^{k+1}}$, it is also true that $g^h \equiv 1 \pmod{p^k}$. This means that the order of g in $U(p^k)$ divides h, that is, $p^{k-1}(p-1)$ divides h. Also, h divides $|U(p^{k+1})|$, that is, h divides $p^k(p-1)$, because h is the order of an element of $U(p^{k+1})$. Thus $h = p^k(p-1)$ or $h = p^{k-1}(p-1)$; we need to show that the latter is not possible. It suffices to show that $g^{p^{k-1}(p-1)} \not\equiv 1 \pmod{p^{k+1}}$. We know that $g^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$ and $g^{p^{k-2}(p-1)} \equiv 1 \pmod{p^{k-1}}$, by the induction hypothesis (or by direct verification if $k = 2$). Thus $g^{p^{k-2}(p-1)} = 1 + bp^{k-1}$ for some b not divisible by p. Then

$$\begin{aligned} g^{p^{k-1}(p-1)} &= (1+bp^{k-1})^p \\ &= 1 + \binom{p}{1} bp^{k-1} + \binom{p}{2} b^2 p^{2k-2} + \cdots + \binom{p}{p-1} b^{p-1} p^{(p-1)(k-1)} + b^p p^{pk-p}. \end{aligned}$$

Since $pk - p \geq k+1$, p^{k+1} divides the last term in this sum. The binomial coefficient $\binom{p}{i}$ is divisible by p when $1 \leq i \leq p-1$, because p is prime and

$$\binom{p}{i} = \frac{p!}{i!(p-i)!},$$

with every factor in the denominator $i!(p-i)!$ less than p. Together with the fact that $2k-2 \geq k$, this means that p^{k+1} divides every term in the preceding sum except the first two, so

$$g^{p^{k-1}(p-1)} \equiv 1 + bp^k \pmod{p^{k+1}}.$$

Since p does not divide b,

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

which is what we were after—now we know that g generates $U(p^{k+1})$.

Completing the Cycle Finally, it all comes down to $U(p)$. We need to know that some $g \in U(p)$ has order $m = p - 1$. Pick g to have order m in $U(p)$, with m as large as possible. If h is any element of $U(p)$, then $|h|$ divides $|g|$, for suppose not. Then we may write $|h| = q^r a$ and $|g| = q^s b$, where q is prime, $r > s$, and q does not divide either a or b. That is, if $|h|$ does not divide $|g|$, it must be because some prime q appears more often in the factorization of $|h|$ than the factorization of $|g|$. Now in $U(p)$,

$$(h^a g)^{q^r b} = (h^{q^r a})^b (g^{q^s b})^{q^{r-s}} = 1,$$

so $|h^a g|$ divides $q^r b$. Thus the order of $h^a g$ must be $q^t c$, where $t \leq r$ and $c|b$. If $t < r$, then

$$1 = (h^a g)^{q^{r-1} b} = (h^{q^{r-1} a})^b (g^{q^{r-1} b}) = (h^{q^{r-1} a})^b,$$

so $|h|$ divides $q^{r-1}ab$, a contradiction. On the other hand, if $c < b$, then

$$1 = (h^a g)^{q^r c} = (h^{q^r a})^c g^{q^r c} = g^{q^r c},$$

so $|g|$ divides $q^r c$, another contradiction. Thus $t = r$ and $c = b$, and the order of $h^a g$ is $q^r b > q^s b = |g|$, yet another contradiction, since g was chosen to have largest possible order. Hence, $|h|$ divides $|g| = m$.

Now we need a bit of field theory and we're done. For every $h \in U(p)$, $h^m = 1$, that is, h is a root of the polynomial $x^m - 1$, so $x^m - 1$ has $p - 1$ roots in $U(p)$ and in $\mathbb{Z}_p$. But since $\mathbb{Z}_p$ is a field, $x^m - 1$ can have at most m roots. Thus $p - 1 \leq m$, so in fact the order of g is $p - 1$ and $U(p)$ is cyclic.

Acknowledgment. Many thanks to the referee for suggesting the proof used here that $U(p)$ is cyclic.

References

[1] David J. DeVries, The group of units in $\mathbb{Z}_m$, this MAGAZINE 62 (1989), 340.

[2] Joseph A. Gallian, *Contemporary Abstract Algebra*, Fourth Edition, Houghton Mifflin, Boston, MA, 1998.

[3] Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery, *An Introduction to the Theory of Numbers*, Fifth Edition, John Wiley & Sons, Inc., New York, NY, 1991.