VOL. 88, NO. 1, FEBRUARY 2015

Factoring subgroups and factor groups of groups of units modulo n*

Joseph A. Gallian
University of Minnesota Duluth
jgallian@d.umn.edu

Shahriyar Roshan Zamir
University of Nebraska Lincoln
sroshanzamir2@huskers.unl.edu

Abstract

The group $U(n)$ is the set of all positive integers less than or equal to n and relatively prime to n under multiplication modulo n. For $n \geq 1$ and k an integer the set $U_k(n) = \{x \in U(n) | \, x = kt + 1 \pmod{n} \text{ for } t \in \mathbb{Z}\}$ is a subgroup of $U(n)$. In this article we show how to express the subgroups $U_k(n)$ and factor groups $U(n)/U_k(n)$ of $U(n)$ as a direct product of groups of the form Z_m, the group of integers modulo m under addition. Similar results are given for generalizations of $U_k(n)$ and for subgroups of the form $U(n)^{(k)} = \{x^k | \, x \in U(n)\}$. Lastly, we give a construction that proves every finite Abelian group is a subgroup of $U(n)$ for infinitely many values of n.

*The results of this paper are part of Shahriyar Roshan Zamir's 2019 Master's thesis, with the same title, done at the University of Minnesota Duluth under the supervision of Joseph A. Gallian.

Introduction

Early in a course on abstract algebra one encounters the multiplicative group $U(n)$ of integers modulo n that consist of the set of integers less than or equal to n and relatively prime to n. By definition, the order of $U(n)$, $|U(n)| = \phi(n)$ where ϕ is the Euler phi function. This group was introduced by Euler in 1761 and investigated in detail by Gauss in 1801 in his famous book on number theory *Disquisitiones Arithmeticae*, where he elucidated its structure as a direct product of groups of the form Z_m, the group of integers modulo m under addition.

In his classic book on algebra *Lehrbuch der Algebra* Heinrich Weber gave an extensive treatment of the groups $U(n)$ and described them as the most important examples of finite Abelian groups. One of their striking properties proved later in this paper is that every finite Abelian group is isomorphic to a subgroup of $U(n)$ for infinitely many n. The textbook [**4**] uses the groups $U(n)$ and their subgroups to illustrate in a concrete way the concepts of cyclic and noncyclic groups, isomorphisms, homomorphisms, internal and external direct products, cosets, Lagrange's Theorem, factor groups, and the Fundamental Theorem of Finite Abelian groups. This will be evident in this paper as well.

The groups $U(n)$ arise naturally in algebra, number theory, cryptography, and computer science. They have been studied in four papers in this Magazine ([**5**], [**2**], [**3**], [**6**]). Moreover, [**1**] provides the classification of the group of units of the ring of Gaussian integers modulo n.

In [**5**] and [**4**] it is shown how to express $U(n)$ and certain subgroups of $U(n)$ as a direct product of subgroups of $U(n)$ and as a direct product of groups of the form Z_m. We provide similar results about the structures of some subgroups and factor (quotient) groups of the groups $U(n)$.

Central to our discussion is the following theorem of Gauss:

$$U(p^n) \approx Z_{p^n - p^{n-1}} \text{ for an odd prime } p,$$

$$U(2^n) \approx Z_2 \oplus Z_{2^{n-2}} \text{ for } n \geq 3,$$

$$U(4) \approx Z_2 \text{ and } U(2) \approx U(1) \approx Z_1 \approx \{0\}.$$

Combining this with the result in [**4**] (page 161) that for $n = n_1 n_2 \cdots n_r$, where $gcd(n_i, n_j) = 1$ for $i \neq j$, we have

$$U(n) \approx U(n_1) \oplus U(n_2) \oplus \cdots \oplus U(n_r)$$

and we can easily write every U-group as a direct product of groups of the form Z_m. For example,

$$U(1400) = U(2^3 \cdot 5^2 \cdot 7) \approx U(2^3) \oplus U(5^2) \oplus U(7) \approx Z_2 \oplus Z_2 \oplus Z_{20} \oplus Z_6.$$

This example raises the question of how can we do similar things for certain subgroups and factor groups of $U(n)$. In the next section we show how for $n \geq 1$ and an integer k the subgroup of $U(n)$ defined by

$$U_k(n) = \{x \in U(n) |\ x \equiv kt + 1\ (\ n)\ \text{ for }\ t \in \mathbb{Z}\}$$

and the factor group $U(n)/U_k(n)$ of $U(n)$ can be expressed as a direct product of groups of the form Z_m. In later sections we do the same for two generalizations of $U_k(n)$ and for subgroups of $U(n)$ of the form

$$U(n)^{(k)} = \{x^k |\ x \in U(n)\}.$$

Results related to $U_k(n)$

In [**4**] and [**5**] $U_k(n)$ is defined only for positive divisors k of n. Although our definition does not make that requirement, our first theorem shows that for questions about the structure of groups of the form $U_k(n)$ we may assume that k is a positive divisor of n.

Theorem 1.1. *Let n and k be positive integers. Then $U_k(n) = U_{gcd(n,k)}(n)$.*

Proof. Let $gcd(n, k) = d$, $k = dh$, and $x \in U_k(n)$. Then $x \equiv kt + 1$ (mod n) implies $x \equiv d(ht) + 1$ (mod n), which is in $U_d(n)$. For $x \in U_d(n)$ we have $x \equiv dt' + 1$ (mod n). We know there exists integers s and t such that $sk + tn = d$. Hence $x = (sk + tn)t' + 1 \equiv k(st') + 1$ (mod n) and therefore $x \in U_k(n)$. □

Corollary 1.2. *For any positive integer n and an odd integer h we have $U_{2h}(n) = U_h(n)$.*

Proof. If n is odd then $gcd(2h, n) = gcd(h, n)$ and by Theorem 1.1 we get $U_{2h}(n) = U_{gcd(2h,n)}(n) = U_{gcd(h,n)}(n) = U_h(n)$. Now suppose n is even. If $2h$ does not divide n, by Theorem 1.1 we get $U_{2h}(n) = U_{gcd(2h,n)}(n)$. Since n is even the greatest common divisor of $2h$ and n must equal $2h'$ for some odd h'. Hence we may assume $2h$ divides n. It follows by definition that $U_{2h}(n) \subseteq U_h(n)$. Let $x \in U_h(n)$. Since h divides n we have that $x = hk + 1$ where x is smaller than n. If k is odd, then x is even and hence not relatively prime to n, so k has to be even. Let $k = 2t$. Then $x = 2ht + 1$ and therefore $x \in U_{2h}(n)$. □

Theorem 1.1 shows any factor of k in $U_k(n)$ that is relatively prime to n can be "canceled." Corollary 1.2 shows if k has exactly one factor of 2 then it can be "canceled" as well.

$$U_{24}(30) = \{1, 19, 13, 7\} = \{1, 7, 13, 19\} = U_6(30) = U_3(30)$$
$$U_{15}(70) = \{1, 31, 61, 51, 11, 41\} = \{1, 11, 31, 41, 51, 61\} = U_5(70) = U_{10}(70)$$

The above examples illustrate the utility of using cancellation. For $U_{15}(70)$ we generate the set by starting with 1 and successively add 15 to the previous element. This results in terms that exceed the modulus and elements that are not in increasing order. In contrast, for $U_5(70)$ or $U_{10}(70)$ we generate the elements without using mod arithmetic and the elements are in increasing order.

Noting that $U_5(70) = U_{10}(70)$ demonstrates the interesting fact that Corollary 1.2 is useful in opposite ways depending on the parity of n. When n is odd cancelling the 2 offers the same advantages as Theorem 1.1. When n is even it is more efficient to not cancel the 2 because in examining the elements of the form $ht + 1$ every other element is even and therefore is not in $U_h(n) = U_{2h}(n)$. So, one needs only to examine half as many integers for $U_{2h}(n)$. This observation is often overlooked by students.

We next classify the structure of subgroups of the form $U_k(n)$ and their respective factor groups when n is a power of a prime. After that we shift our attention to the general case of any positive integers n and k. For the proof of Lemma 1.3 and Proposition 1.4, we only need to find the order of $U_k(n)$ and use the fact that every subgroup and every factor group of a cyclic group is cyclic.

Lemma 1.3. *For an odd prime p and $1 \leq k \leq m$ we have $U_{p^k}(p^m) \approx Z_{p^{m-k}}$.*

Proof. Note that $U_{p^k}(p^m) = \{1, p^k + 1, 2p^k + 1, 3p^k + 1 \ldots, (p^{m-k} - 1)p^k + 1\}$ and since $U(p^m)$ is cyclic, the result follows. □

For $p^m = 11^5$ and $p^k = 11^3$, Lemma 1.3 gives $U_{11^3}(11^5) \approx Z_{11^{5-3}} \approx Z_{121}$. Note that for $k = m$ we get the subgroup consisting of the identity only. That is, $U_{11^5}(11^5) \approx \{1\} \approx Z_1$.

It is worth mentioning that for an odd prime p, Lemma 1.3 and the formula $|U(p^m)| = (p-1)p^{m-1}$ give us the attractive result that the Sylow p-subgroup of $U(p^m)$ is $U_p(p^m)$.

Proposition 1.4. *For an odd prime p and $1 \leq k \leq m$, we have $U(p^m)/U_{p^k}(p^m) \approx Z_{p^{k-1}(p-1)}$.*

Proof. Since $U(p^m)$ is cyclic, we only need to find the order of $U(p^m)/U_{p^k}(p^m)$, which is $|U(p^m)/U_{p^k}(p^m)| = \dfrac{p^{m-1}(p-1)}{p^{m-k}} = p^{k-1}(p-1)$. □

Suppose in the previous example we wanted to find the structure of $U(11^5)/U_{11^3}(11^5)$. By Proposition 1.4 we have $U(11^5)/U_{11^3}(11^5) \approx Z_{11^{3-1}(11-1)} \approx Z_{1210}$. Notice how much faster this was compared to having to do the calculations by hand. Also note the structure of the factor group depends only on k.

Lemma 1.5. *Let $n \geq 1$ and $2 \leq i \leq n$. Then $U_2(2^n) = U(2^n)$ and $U_{2^i}(2^n) \approx Z_{2^{n-i}}$.*

Proof. The first assertion follows by the definition. For the second part observe that $|U_{2^i}(2^n)| = 2^{n-i}$ because $U_{2^i}(2^n) = \{1, 2^i + 1, \ldots, (2^{n-i} - 1)2^i + 1\}$. Since $U_{2^i}(2^n)$ is a subgroup of $U(2^n) \approx Z_2 \oplus Z_{2^{n-2}}$, we know that $U_{2^i}(2^n)$ is isomorphic to either $Z_{2^{n-i}}$ or $Z_2 \oplus Z_{2^{n-i-1}}$ where $2 \leq i$. This implies the subgroup $U_{2^i}(2^n)$ has either one or three elements of order 2, respectively. We will show it has one. Note the group $U(2^n)$ has exactly three elements of order 2, namely $2^n - 1$ and $2^{n-1} \pm 1$. If $2^n - 1 \in U_{2^i}(2^n)$ then $2^n - 1 = k \cdot 2^i + 1$ for some integer k. This is a contradiction since the left hand side is -1 mod 2^i and right hand side is 1 mod 2^i. So $U_{2^i}(2^n)$ has only one element of order 2, and therefore is isomorphic to $Z_{2^{n-i}}$. □

The following result about factor groups of finite Abelian groups will be helpful for our results about factor groups of U-groups.

Proposition 1.6. *Let $G \approx Z_{p_1^{n_1}} \oplus \cdots \oplus Z_{p_k^{n_k}}$ and H be a subgroup of G such that $|H| = p_1^{n_1-m_1} \cdots p_k^{n_k-m_k}$ where p_i is prime and $0 \leq m_i \leq n_i$ for all i. Then $G/H \approx Z_{p_1^{m_1}} \oplus \cdots \oplus Z_{p_k^{m_k}}$.*

Proposition 1.6 follows from the fact that if G is k-generated then G/H is generated by the canonical image of the generators of G. Thus the number of components in a cyclic group decomposition of a factor group of any group is less than or equal to the number of components in the cyclic group decomposition of that group.

Proposition 1.7. *For $n = i$ we have $U(2^n)/U_{2^i}(2^n) \approx Z_1$. For $n = 2$ and $i = 1$ we have $U(4)/U_2(4) \approx Z_1$. For $2 \leq i < n$ we have $U(2^n)/U_{2^i}(2^n) \approx Z_2 \oplus Z_{2^{i-2}}$.*

Proof. The first two assertions are obvious. So we assume that $2 \leq i < n$. Observe that $|U(2^n)/U_{2^i}(2^n)| = 2^{i-1}$. By Proposition 1.6, $U(2^n)/U_{2^i}(2^n)$ is isomorphic to either $Z_{2^{i-1}}$ or $Z_2 \oplus Z_{2^{i-2}}$ and therefore it has either one or three elements of order 2. We will show the latter is the case by exhibiting two elements of order 2. Let $H = U_{2^i}(2^n)$. Because $((2^n-1)H)^2 = (-1H)^2 = H$ we know that $|(2^n-1)H| = 1$ or 2. If $|(2^n-1)H| = 1$, then $2^n - 1 \in H$ and therefore $2^n - 1 = 2^i \cdot k + 1$. But that's impossible since the left side is $-1 \pmod{2^i}$ and the right side is $1 \pmod{2^i}$. Similarly, we can show that $|(2^{n-1}-1)H| = 2$. □

Theorem 1.8. *Let $p_1, \ldots, p_k$ be distinct primes. For $1 \leq m_i$, $0 \leq j_i \leq m_i$, $1 \leq i \leq k$, we have $U_{p_1^{j_1} \cdots p_k^{j_k}}(p_1^{m_1} \cdots p_k^{m_k}) \approx U_{p_1^{j_1}}(p_1^{m_1}) \oplus \cdots \oplus U_{p_k^{j_k}}(p_k^{m_k})$.*

Proof. We know from [**4**] (p.160) that $U(p_1^{m_1} \cdots p_k^{m_k})$ is isomorphic to $U(p_1^{m_1}) \oplus \cdots \oplus U(p_k^{m_k})$ under the mapping $\gamma(x) = (x \pmod{p_1^{m_1}}, \ldots, x \pmod{p_k^{m_k}})$. We will show the same mapping is the required isomorphism. For convenience, let $a = p_1^{m_1} \cdots p_k^{m_k}$ and $b = p_1^{j_1} \cdots p_k^{j_k}$. If b is divisible by 2 but not 4, then by Corollary 1.2 we can ignore that factor of 2 in b. So, we may assume that if b is even, then b is divisible by 4. The restriction of the domain of γ from $U(a)$ to $U_b(a)$ is a well-defined, one-to-one and operation preserving mapping from $U_b(a)$ to $U_{p_1^{j_1}}(p_1^{m_1}) \oplus \cdots \oplus U_{p_k^{j_k}}(p_k^{m_k})$ because γ is an isomorphism. We need only to show this mapping is onto. Since γ is a one-to-one mapping, it suffices to show that $\gamma(U_b(a))$ is into $U_{p_1^{j_1}}(p_1^{m_1}) \oplus \cdots \oplus U_{p_k^{j_k}}(p_k^{m_k})$ and they have the same order. It follows, from the definition and Corollary 1.2, that the order of $U_b(a)$ is

$\frac{a}{b} = p_1^{m_1-j_1} \cdots p_k^{m_k-j_k}$. (In the case of b even, the previous assumption of b being divisible by 4 was necessary for this and the next claim.)

By definition we have:

$$|U_{p_1^{j_1}}(p_1^{m_1})| = p_1^{m_1-j_1}$$
$$\vdots$$
$$|U_{p_k^{j_k}}(p_k^{m_k})| = p_k^{m_k-j_k}.$$

Therefore the order of $U_{p_1^{j_1}}(p_1^{m_1}) \oplus \cdots \oplus U_{p_k^{j_k}}(p_k^{m_k}) = p_1^{m_1-j_1} \cdots p_k^{m_k-j_k}$. To show the into part, let $x \in U_b(a)$. Note $\gcd(p_i, x) = 1$ for all i since $\gcd(a, x) = 1$. Moreover $\gamma(x) = (x \pmod{p_1^{m_1}}, \cdots, x \pmod{p_k^{m_k}})$. To show $\gamma(x)$ is in $U_{p_1^{j_1}}(p_1^{m_1}) \oplus \cdots \oplus U_{p_k^{j_k}}(p_k^{m_k})$, we mod the i-th component by $p_i^{j_i}$. This yields:

$$(x \pmod{p_1^{m_1}} \pmod{p_1^{j_1}}, \cdots, (x \pmod{p_k^{m_k}} \pmod{p_k^{j_k}}) =$$
$$(x \pmod{p_1^{j_1}}, \cdots, x \pmod{p_k^{j_k}}) = (1, \cdots, 1)$$

since $x \equiv 1 \pmod{b}$. □

The following corollaries are direct consequences of Theorem 1.8, Lemma 1.3, and Lemma 1.5.

Corollary 1.9. *Let k, k' be positive integers such that $U_{gcd(k,n)}(n) = U_{gcd(k',n)}(n)$. Then $gcd(k, n) = gcd(k', n)$.*

Corollary 1.10. *If $|U_k(n)| = p^m$ for an odd prime p and $1 \leq m$ then $U_k(n) \approx Z_{p^m}$.*

Corollary 1.11. *Let $p_1, \ldots, p_k$ be distinct odd primes. For $1 \leq j_i \leq m_i$ and $1 \leq i \leq k$, we have $U_{p_1^{j_1} \cdots p_k^{j_k}}(p_1^{m_1} \cdots p_k^{m_k}) \approx Z_{p_1^{m_1-j_1} \cdots p_k^{m_k-j_k}}$ and $U_{p_1^{j_1} \cdots p_k^{j_k}}(p_1^{m_1} \cdots p_k^{m_k}) = \langle p_1^{j_1} \cdots p_k^{j_k} + 1 \rangle$.*

Proof. The first part follows directly from Theorem 1.8 and Lemma 1.3. To see that $p_1^{j_1} \cdots p_k^{j_k} + 1$ is a generator for $U_{p_1^{j_1} \cdots p_k^{j_k}}(p_1^{m_1} \cdots p_k^{m_k})$ observe that the isomorphism from $U_{p_1^{j_1} \cdots p_k^{j_k}}(p_1^{m_1} \cdots p_k^{m_k})$ to $Z_{p_1^{m_1-j_1} \cdots p_k^{m_k-j_k}}$ given by $\gamma(x) = x \bmod p_1^{j_1} \cdots p_k^{j_k}$ maps $p_1^{j_1} \cdots p_k^{j_k} + 1$ to a generator of $Z_{p_1^{m_1-j_1} \cdots p_k^{m_k-j_k}}$. □

Corollary 1.12. *For $1 \leq k \leq n$, we have $U_k(n) = U(n)$ if and only if $gcd(n, k) = 1$ or 2.*

Proof. If $gcd(k,n) = 1$ by Theorem 1.1 we get $U_k(n) = U_{gcd(k,n)}(n) = U_1(n) = U(n)$. If $gcd(k,n) = 2$, it follows from Theorem 1.1 and Corollary 1.2 that $U_k(n) = U_{gcd(k,n)}(n) = U_2(n) = U(n)$.

Now suppose $U_k(n) = U(n)$. From Theorem 1.1 and Corollary 1.2 we get:

$$U_k(n) = U_{gcd(k,n)}(n) = U(n) = U_2(n) = U_{gcd(2,n)}(n).$$

It follows from Corollary 1.9 that $gcd(k,n) = gcd(2,n)$. This implies $gcd(k,n) = 1$ or 2. □

Example 1.13. To demonstrate how we can use Theorem 1.8, suppose we want to express $U_{140}(1800)$ as a direct product of groups of the form Z_m. We know $U_{140}(1800) = U_{20}(1800) = U_{20}(8 \cdot 9 \cdot 25)$ and by Theorem 1.8, Lemma 1.3 and Lemma 1.5 we get $U_{20}(1800) \approx U_4(8) \oplus U(9) \oplus U_5(25) \approx Z_2 \oplus Z_6 \oplus Z_5$.

Theorem 1.14. *Let $n > 1$ be odd and k a divisor of n. Then $U(n)/U_k(n) \approx U(k)$.*

Proof. Let $n = p_1^{n_1} \cdots p_j^{n_j}$ and $k = p_1^{m_1} \cdots p_j^{m_j}$. Consider the homomorphism $\gamma : U(n) \to U(k)$ given by $\gamma(x) = x \pmod k$. By definition, $Ker(\gamma) = U_k(n)$, so the First Group Isomorphism Theorem gives us $U(n)/U_k(n) \approx \gamma(U(n))$. Moreover, $\gamma(U(n))$ is a subgroup of $U(k)$. We will show $|\gamma(U(n))| = |U(k)|$. We know that $|U(k)| = \phi(k) = p_1^{m_1-1}(p_1-1) \cdots p_j^{m_j-1}(p_j-1)$. By Theorem 1.8 and Lemma 1.3 we get $|\gamma(U(n))| = |U(n)/U_k(n)| = \dfrac{|U(n)|}{|U_k(n)|} =$

$$\frac{p_1^{n_1-1}(p_1-1) \cdots p_j^{n_j-1}(p_j-1)}{p^{n_1-m_1} \cdots p^{n_j-m_j}} = p_1^{m_1-1}(p_1-1) \cdots p_j^{m_j-1}(p_j-1). \qquad \square$$

Theorem 1.15. *If n is even and k is divisible by 4, then $U(n)/U_k(n) \approx U(k)$.*

Proof. The argument is identical to the proof Theorem 1.14. To find the order of $U(n)/U_k(n)$ we use Theorem 1.8, Lemma 1.3, and Lemma 1.5. □

Theorem 1.16. *If n is even and $k = 2h$ where h is odd, then $U(n)/U_k(n) \approx U(h)$.*

Proof. We know from Corollary 1.2 that $U_k(n) = U_h(n)$. We change the mapping in Theorem 1.14 to $\gamma : U(n) \to U(h)$ where $\gamma(x) = x \pmod h$. The rest of the proof is an order argument identical to the one in the proof of Theorem 1.14. □

Generalizations to $U_{\pm k}(n)$ and $U_{k,H}(n)$

Does every subgroup of $U(n)$ have the form $U_k(n)$ where k is a divisor of n? The answer is no. For example $U(36)$, which is isomorphic to $Z_2 \oplus Z_6$, has a subgroup isomorphic to $Z_2 \oplus Z_2$. But looking at cases reveals that for no divisor k of 36 do we get $U_k(36) \approx Z_2 \oplus Z_2$. This motivates our next theorem. It will allow us to give a description of the elements of $U(36)$ that form the subgroup isomorphic to $Z_2 \oplus Z_2$.

Theorem 1.17. *For $n \geq 1$ and a positive integer k, the set*

$$U_{\pm k}(n) = \{x \in U(n) |\ x \equiv kt \pm 1 \ (\textit{mod}\ n) \textit{ for } t \in \mathbb{Z}\}$$

is a subgroup of $U(n)$.

Proof. It suffices to show that $U_{\pm k}(n)$ is closed (see Theorem 3.3 in [**4**]). If $a, b \in U_{\pm k}(n)$ then $ab \bmod n \equiv (a \bmod n)(b \bmod n) \equiv (\pm 1)(\pm 1) \equiv \pm 1$. □

A few examples of $U_{\pm k}(n)$ are:

$$U_{\pm 9}(36) = \{1, 17, 19, 35\}$$
$$U_{\pm 11}(33) = \{1, 10, 23, 32\}$$
$$U_{\pm 5}(45) = \{1, 4, 11, 14, 16, 19, 26, 29, 31, 34, 41, 44\}.$$

The first example answers our question about a non-cyclic subgroup of order four in $U(36)$, since $U_{\pm 9}(36) \approx Z_2 \oplus Z_2$. As was the case with $U_k(n)$, we don't need to know all of the elements of $U(n)$ to find the elements of $U_{\pm k}(n)$. The algorithm is similar. Add ± 1 to all non-negative integer multiples of k and then mod by n and check to see if the result is relatively prime to n. Continue in this fashion until you reach 1. For example, $1 \cdot 9 \pm 1 \pmod{36}$ are not relatively prime to 36 so we discard them and $4 \cdot 9 \pm 1 \equiv 1, 35 \pmod{36}$ so we are done.

Theorem 1.18. *Let $n = st$ with $n \geq 3$ and $gcd(s, t) = 1$. Then $U_{\pm s}(n) \approx U_s(n) \times \{1, n-1\} \approx U(t) \oplus Z_2$.*

Proof. From [**4**] we know if $G = H \times K$, the internal direct product of H and K, then $G = H \oplus K$. By observation $U_{\pm s}(n) = U_s(n) \times \{1, -1\}$, where $-1 \equiv n -$

$1 \pmod{n}$. (A detailed and more general proof of why the two subgroups $U_{\pm s}(n)$ and $U_s(n) \times \{1, -1\}$ are equal is given in Theorem 1.19.) Since $gcd(s, t) = 1$, it follows that $U_s(n) = U_s(st) \approx U(t)$, where the last isomorphism is a result from [**5**]. (See also [**4**] p.160.) Moreover, $\{1, -1\} \approx Z_2$. Therefore $U_{\pm s}(n) \approx U(t) \oplus Z_2$. □

One might wonder if $U_{\pm k}(n) = U_k(n) \times \{1, -1\}$ for all $1 \leq k \leq n$. The answer is "yes" in all non-trivial cases. In Corollary 1.12 we proved that $U_k(n) = U(n)$ if and only if $\gcd(k, n) = 1$ or 2. So, we ignore this case.

Theorem 1.19. *For $1 \leq k \leq n$, and $U_k(n) \neq U(n)$, we have $U_{\pm k}(n) = U_k(n) \times \{1, -1\} \approx U_{gcd(n,k)}(n) \oplus Z_2$.*

Proof. Suppose $U_k(n) \neq U(n)$. It suffices to show $U_{\pm k}(n) = U_k(n) \times \{1, -1\}$. (The rest follows from Theorem 1.1.) Let $A = U_{\pm k}(n)$ and $B = U_k(n) \times \{1, -1\}$. The assumption that $U_k(n) \neq U(n)$ allows for set B to exist. Otherwise, the notion of internal direct product would not make sense. Because both A and B are subgroups of $U(n)$, it suffices to show A and B are subsets of each other. For $x \in A$, if $x = kt + 1$, we are done. If $x = kt - 1$ then $x = -(k(-t) + 1)$, which is an element of B. Now let $x \in B$. If $x = (kt + 1)(1)$ then we are done. If $x = (kt + 1)(-1)$ then $x = k(-t) - 1$, which is an element of A. Finally we have $U_{\pm k}(n) = U_k(n) \times \{1, -1\} \approx U_{gcd(n,k)}(n) \oplus Z_2$. □

The following example demonstrates how the above results taken together easily dispatch problems that appear to be intimidating. As stated in [**4**] "theorems are labor saving devices."

Example 1.20. Let's look at the case of $n = 2^3 \cdot 3^3 \cdot 5^2 \cdot 11 = 59400$ and $k = 2^2 \cdot 3 \cdot 5 \cdot 13 = 780$ and find the structure of $U_{\pm 780}(59400)$. Note that $\gcd(59400, 780) = 60$, implies $U_{\pm 780}(59400) \approx U_{780}(59400) \oplus Z_2 \approx U_{60}(59400) \oplus Z_2 \approx U_{4\cdot 3\cdot 5}(8 \cdot 27 \cdot 25 \cdot 11) \oplus Z_2 \approx U_4(8) \oplus U_3(27) \oplus U_5(25) \oplus U(11) \oplus Z_2 \approx Z_2 \oplus Z_9 \oplus Z_5 \oplus Z_{10} \oplus Z_2 \approx Z_{45} \oplus Z_{10} \oplus Z_2 \oplus Z_2$.

We finish this section with a generalization of $U_{\pm k}(n)$. The following are alternate definitions for the subgroups $U_k(n)$ and $U_{\pm k}(n)$:

$$U_k(n) = \{x \in U(n) |\ x \bmod k \in \{1\}\}$$
$$U_{\pm k}(n) = \{x \in U(n) |\ x \bmod k \in \{1, -1\}\}.$$

We generalize these by replacing $\{1\}$ or $\{1, -1\}$ with any other subgroup H of $U(n)$.

Theorem 1.21. *For $n > 1$, let k be a positive divisor of n and H be a subgroup of $U(n)$. The set $U_{k,H}(n) = \{x \in U(n) |\ x \bmod k \in H\}$ is a subgroup of $U(n)$.*

Proof. The proof follows from the closure of H. □

The advantage of using these subgroups is that by picking certain positive divisors k of n and a subgroup H of $U(n)$ we are able to construct a new subgroup of $U(n)$ by changing the divisor k or the subgroup H (or both) we can create more subgroups of $U(n)$.

Example 1.22. Let $n = 80$, $k = 10$ and $H = \{1, 9\}$. Then we have $U_{10,\{1,9\}}(80) = \{x \in U(80) |\ x = 10t + 1 \text{ or } x = 10t + 9,\ t \in \mathbb{Z}\}$. For $t = 0$, we get H. For $t = 1$ we get 11 and 19. For $t = 2$ we get 21 and 29 and so on. Notice that we need only to check up to $t = 8$. Finally, we have $U_{10,\{1,9\}}(80) = \{1, 9, 11, 19, 21, 29, 31, 39, 41, 49, 51, 59, 61, 69, 71, 79\}$, which is indeed a subgroup of $U(80)$.

Our results about when $U_{\pm k}(n) = U_k(n) \times \{1, -1\}$ raises the question of when $U_{k,H}(n) = U_k(n) \times H$.

Theorem 1.23. *Let $n > 1$, k a positive divisor of n, and H a subgroup of $U(n)$. Then $U_{k,H}(n) = U_k(n) \times H$ if and only if $U_k(n) \cap H = \{1\}$.*

Proof. Suppose $U_k(n) \cap H = \{1\}$. It suffices to show $U_{k,H}(n) = U_k(n)H$ since the rest follows from the definition of internal direct product. For $x \in U_k(n)H$, we have that for some $h \in H$, $x \equiv (kt + 1)h \pmod{n} \equiv k(th) + h \pmod{n}$, which is an element of $U_{k,H}(n)$. For $x \in U_{k,H}(n)$ we have $x = kt + h$ for some $h \in H$. The following chain of equalities shows $x \in U_k(n)H$:

$$x = (kt + h)1 = (kt + h)h^{-1}h = (k(th^{-1}) + 1)h.$$

Thus x has the desired form.

If $U_{k,H}(n) = U_k(n) \times H$, then by definition of internal direct product we get $U_k(n) \cap H = \{1\}$. □

Results about $U(n)^{(k)}$ and a general result about $U(n)$ groups

We now ask the following question: Is every subgroup of a $U(n)$ expressible in the form $U_{\pm k}(n)$ or $U_k(n)$? The answer is again "no." For instance, for $U(252) \approx Z_2 \oplus Z_6 \oplus Z_6$ there is no divisor k of 252 such that $U_k(252)$ or $U_{\pm k}(252)$ yields the subgroup of $U(252)$ isomorphic to $Z_2 \oplus Z_2 \oplus Z_2$. This question motivates another way of producing subgroups in a $U(n)$ group.

Definition 1.24. *Let $n > 1$ and k be any integer. We define*

$$U(n)^{(k)} = \left\{x^k |\ x \in U(n)\right\}.$$

That $U(n)^{(k)}$ is a subgroup of $U(n)$ follows from closure of $U(n)^{(k)}$. If k doesn't divide $|U(n)| = \phi(n)$, this subgroup can be viewed as the image of the automorphism given by $\gamma(x) = x^k$. If k is a divisor of $\phi(n)$, γ defines a homomorphism from $U(n)$ to itself with kernel:

$$Ker(\gamma) = \left\{x \in U(n) |\ x^k = e\right\}.$$

Consequently, by the First Isomorphism Theorem for groups we have $U(n)/Ker(\gamma) \approx U(n)^{(k)}$.

Example 1.25. Consider $U(13) = \{1, 5, 7, 12\}$ and $k = 2$. Then squaring each element we get $\{1, 12, 12, 1\}$ so $U(13)^{(2)} = \{1, 12\}$.

Our next result is the counterpart of $U_k(n) = U_{gcd(n,k)}(n)$.

Proposition 1.26. *For $n > 1$ and any integer k, $U(n)^{(k)} = U(n)^{(gcd(\phi(n),k)}$.*

Proof. Let $\gcd(\phi(n), k) = d$ and $k = dh$. Since $U(n)^{(d)}$ and $U(n)^{(k)}$ are both subgroups of $U(n)$, we only need to show they are subsets of each other. Clearly $U(n)^{(k)} \subseteq U(n)^{(d)}$ since $x^{hd} = (x^h)^d$. Now let $x^d \in U(n)^{(d)}$. We know $d = t_1 k + t_2\phi(n)$, which implies $x^d = x^{t_1 k + t_2\phi(n)} = x^{t_1 k} \cdot x^{t_2\phi(n)} = (x^{t_1})^k \in U(n)^{(k)}$. □

Proposition 1.26 allows us to assume the superscript k is always a divisor of $\phi(n)$.

Example 1.27. Consider $U(252) = U(4 \cdot 9 \cdot 7) \approx U(4) \oplus U(9) \oplus U(7) \approx Z_2 \oplus Z_6 \oplus Z_6$. Direct calculations show that $U(252)^{(3)} = \{1, 55, 71, 125, 127, 181, 197, 251\}$ and every non-identity element has order two. Thus, we have $U(252)^{(3)} \approx Z_2 \oplus Z_2 \oplus Z_2$.

Notice that in the previous example raising the elements of $U(252)$ to the third power is equivalent to multiplying the elements of $Z_2 \oplus Z_6 \oplus Z_6$ by 3 so, in order to find the structure of the latter, all we have to do is trace the generator of each component, namely 1, after being multiplied by 3. In the first component, Z_2, 3 mod 2 is 1 therefore we get Z_2. In the next two Z_6 components, 1 goes to 3 which yields a Z_2. To summarize, finding the structure of $U(n)^{(k)}$ is equivalent to tracing 1 in each term in the cyclic group decomposition of $U(n)$. This is the main idea of Theorem 1.28.

Theorem 1.28. *Let $n = p_1^{m_1} \cdots p_j^{m_j}$ for distinct odd primes p_i and positive integers m_i. Then $U(p_1^{m_1} \cdots p_j^{m_j})^{(k)} \approx Z_{d_1} \oplus \cdots \oplus Z_{d_j}$ where $d_i = \dfrac{\phi(p_i^{m_i})}{gcd(\phi(p_i^{m_i}), k)}$ for all $1 \leq i \leq j$.*

Proof. We know that $U(n) \approx Z_{\phi(p_1^{m_1})} \oplus \cdots \oplus Z_{\phi(p_j^{m_j})}$. Raising every elements in $U(n)$ to the k-th power is equivalent to multiplying all the elements of $Z_{\phi(p_1^{m_1})} \oplus \cdots \oplus Z_{\phi(p_j^{m_j})}$ by k. This is a mapping of cyclic groups to themselves. So, one needs only to trace where the generator, 1, of each cyclic component is mapped. Observe that 1 goes to k for each term. Hence $Z_{\phi(p_i^{m_i})}$ is mapped to Z_{d_i} where $d_i = \dfrac{\phi(p_i^{m_i})}{gcd(\phi(p_i^{m_i}), k)}$. □

Corollary 1.29. *Let $n = 2^b p_1^{m_1} \cdots p_j^{m_j}$ for distinct odd primes p_i and positive integers b and m_i for all i. Define $d_i = \dfrac{\phi(p_i^{m_i})}{gcd(\phi(p_i^{m_i}), k)}$ for all $1 \leq i \leq j$. Then*

1. $U(2 \cdot p_1^{m_1} \cdots p_j^{m_j})^{(k)} \approx U(p_1^{m_1} \cdots p_j^{m_j})^{(k)} \approx Z_{d_1} \oplus \cdots \oplus Z_{d_j}$.
2. $U(2^b p_1^{m_1} \cdots p_j^{m_j})^{(k)} \approx Z_2 \oplus Z_{d_1} \oplus \cdots \oplus Z_{d_j}$ *if $b = 2$ and k is odd.*
3. $U(2^b p_1^{m_1} \cdots p_j^{m_j})^{(k)} \approx Z_{d_1} \oplus \cdots \oplus Z_{d_j}$ *if $b = 2$ and k is even.*
4. $U(2^b p_1^{m_1} \cdots p_j^{m_j})^{(k)} \approx Z_2 \oplus Z_{2^{b-2}} \oplus Z_{d_1} \oplus \cdots \oplus Z_{d_j}$ *if $b \geq 3$ and k is odd.*

5. $U(2^b p_1^{m_1} \cdots p_j^{m_j})^{(k)} \approx Z_{\frac{2^{b-2}}{gcd(2^{b-2},k)}} \oplus Z_{d_1} \oplus \cdots \oplus Z_{d_j}$ *if* $b \geq 3$ *and* k *is even.*

Proof. For $b = 1$ observe that $U(2 \cdot p_1^{m_1} \cdots p_j^{m_j}) \approx U(p_1^{m_1} \cdots p_j^{m_j})$. If $b = 2$, we have $U(n) \approx Z_2 \oplus Z_{\phi(p_1^{m_1})} \oplus \cdots \oplus Z_{\phi(p_j^{m_j})}$. If k is odd, the additional Z_2 term doesn't change and the rest is identical to Theorem 1.28. If k is even, the first Z_2 is gone because we are mapping 1 to k mod 2 which yields zero. For $b \geq 3$ we get $U(n) \approx Z_2 \oplus Z_{2^{b-2}} \oplus Z_{\phi(p_1^{m_1})} \oplus \cdots \oplus Z_{\phi(p_j^{m_j})}$. For odd k, the term $Z_2 \oplus Z_{2^{b-2}}$ stays the same. For even k, the first Z_2 is gone. We need to find the order of $1 \cdot k = k$ in the $Z_{2^{b-2}}$ term to find the structure of the first component of the direct product. But that order is exactly $\frac{2^{b-2}}{gcd(2^{b-2},k)}$. Since every subgroup of a cyclic group is cyclic, the result follows. □

The previous theorem and its corollary help us find the explicit group elements of various subgroups with desired structures, including p-Sylow subgroups.

Example 1.30. Let $n = 3^3 \cdot 7 \cdot 19$. The cyclic group decomposition of $U(n)$ is $Z_6 \oplus Z_{18} \oplus Z_{18}$. By Theorem 1.28 we have $U(n)^{(9)} \approx Z_{\frac{6}{gcd(6,9)}} \oplus Z_{\frac{18}{gcd(18,9)}} \oplus Z_{\frac{18}{gcd(18,9)}} \approx Z_2 \oplus Z_2 \oplus Z_2$. Therefore, after raising every element of $U(n)$ to the 9th power the elements that are left form the Sylow 2-subgroup of $U(n)$. Define $\gamma : U(n) \to U(n)$ by $\gamma(x) = x^9$. We claim $Ker(\gamma)$ is the Sylow 3-subgroup of $U(n)$. By the First Isomorphism Theorem observe that $U(n)/Ker(\gamma) \approx (U(n))^{(9)} \approx Z_2 \oplus Z_2 \oplus Z_2$, which implies $Ker(\gamma)$ is the set of all elements of $U(n)$ whose orders divide 9 and is isomorphic to $Z_3 \oplus Z_9 \oplus Z_9$, which is the structure of the 3-Sylow subgroup of $U(n)$. Hence $Ker(\gamma) \approx Z_3 \oplus Z_9 \oplus Z_9$.

The group $U(n)^{(2)}$ is another way to obtain the Sylow 3-subgroup of $U(n)$. Observe, by Theorem 1.28, that $U(n)^{(2)} \approx Z_{\frac{6}{gcd(6,2)}} \oplus Z_{\frac{18}{gcd(18,2)}} \oplus Z_{\frac{18}{gcd(18,2)}} \approx Z_3 \oplus Z_9 \oplus Z_9$.

Example 1.31. Suppose in the previous example we wanted to produce the elements of $U(n)$ that form a subgroup isomorphic to $Z_6 \oplus Z_2$. To this end let $H = U_{7 \cdot 19}(3^3 \cdot 7 \cdot 19)^{(9)}$ and $K = U_{3^3 \cdot 19}(3^3 \cdot 7 \cdot 19)$. Using Theorem 1.8 it's clear that $U_{7 \cdot 19}(3^3 \cdot 7 \cdot 19) \approx Z_{18}$ and by Theorem 1.28 we have $H = U_{7 \cdot 19}(3^3 \cdot 7 \cdot 19)^{(9)} \approx Z_2$. Noting that $K \approx Z_6$, we let $L = H \times K$. Since $H \cap K = \{1\}$ we have $L \approx H \oplus K \approx Z_2 \oplus Z_6$.

For completeness, we conclude this paper by proving that every finite Abelian group is a subgroup of a U-group thereby offering support for Weber's assertion in the introduction that the U-groups are the most important examples of finite Abelian groups. We know of no proof of the fact that does not use number theory in an essential way. Indeed, we will use the Dirichlet's theorem [**7**], also called Dirichlet's prime number theorem, which states for any two relatively prime integer a and b, there are infinitely many primes of the form $q = an + b$ where n is a non-negative integer.

Theorem 1.32. *Every finite Abelian group is isomorphic to a subgroup of a U-group.*

Proof. Let G be a finite Abelian group. By the Fundamental Theorem of Finite Abelian Groups we have $G \approx Z_{p_1^{a_1}} \oplus \cdots \oplus Z_{p_1^{a_i}} \oplus \cdots \oplus Z_{p_s^{r_1}} \oplus \cdots \oplus Z_{p_s^{r_h}}$ where p_i's are distinct primes and we have arranged the subscripts such that a_1 is the largest exponent of p_1 and r_1 is the largest exponent of p_s. Let $a = p_1^{a_1}$ and $b = 1$ in the statement of Dirichlet's theorem. Then there are infinitely many primes of the form $q = p_1^{a_1}n + 1$ which implies $p_1^{a_1}$ divides $\phi(q)$ and therefore $U(q)$ has a subgroup of order $p_1^{a_1}$. We can find i distinct primes, $q_1, \ldots, q_i$, of the form $p_1^{a_1}n + 1$, each of which will have a subgroup of order $p_1^{a_1}$ and since that was the largest power of p_1, we can get every subgroup of a smaller power of p_1. Repeating this process for each prime up to p_s and multiply all these primes and we obtain the desired n. □

Acknowledgments: We would like to thank the referees and the editor of the Mathematics Magazine for their constructive comments and suggestions.

References

1. Adam A. Allan, Micheal J. Dunne, John R. Jack, Justin C. Lynd and Harold W. Ellingsen Jr, Classification of the group of units in Gaussian integers modulo n, *Pi Mu Epsilon Journal* 12 (9) (Fall 2008), 513-519.

2. Y. Cheng, Decompostions of U-groups, *Mathematics Magazine* 62 (1989), 271-273.

3. David J. Devries, The group of units in Z_m, *Mathematics Magazine* 62 (1989), 340-342.

4. Joseph A. Gallian, "Contemporary Abstract Algebra," Ninth Edition, Cengage Learning Boston, 2017.

5. Joseph A. Gallian and D. Rusin, Factoring groups of integers modulo n, *Mathematics Magazine* 53 (1980), 33-36.

6. David R. Guichard, When is $U(n)$ cyclic? An algebraic approach, *Mathematics Magazine* 72 (1999), 139-142.

7. D. Shanks, "Solved and Unsolved Problems in Number Theory," 2nd ed., New York: Chelsea, 1978.

Summary: We introduce several ways of producing subgroups of $U(n)$, the group of units of Z_n. Our results find the structure of these various subgroups in terms of external direct product of cyclic groups. We then use our classifications to give a description of elements of $U(n)$ that form a subgroup of $U(n)$ with a desired cyclic group decomposition. This includes giving a description of which elements form a Sylow-p subgroup.

Joe Gallian received a PhD from Notre Dame in 1971. He has had the good fortune of being at the University of Minnesota Duluth since 1972. He is proud to be a joint author with his student and friend Shah. He enjoys spending time nearly everyday with his ten year old grandson Joey.

Shariyar Roshan Zamir obtained his B.A. in Pure Mathematics from Georgia Gwinnett College and his M.S. in Mathematics from University of Minnesota Duluth, where he had the honor of having Joe Gallian as his Master's thesis adviser. He considers it a great privilege to call Joe his friend. He is currently a Ph.D student at the University of Nebraska Lincoln.