On generators for the group of units of the ring of integers modulo n

S.P. Glasby

Let n be an integer > 1, and let $\mathbb{Z}_n$ denote the quotient ring $\mathbb{Z}/n\mathbb{Z}$. The group U_n of units of $\mathbb{Z}_n$ occurs commonly in group theory as the automorphism group $\mathrm{Aut}(C_n)$ of the cyclic group C_n of order n, and number theory as the Galois group of the extension $\mathbb{Q}(e^{2\pi i/n}) : \mathbb{Q}$. The purpose of this note is to prove concisely some elementary facts concerning generators for U_n and to mention a very curious result which is true for all odd primes less than 10^7, except for 40 487. Some facts like Theorem 2 are known (see [**2**, Theorem 2.40]) but are not widely known, or are proved awkwardly, while others like Theorem 4(b), (c) appear not to be known. If p is an odd prime, then U_{p^i} is cyclic, so $U_{p^i} = \langle a_i + p^i\mathbb{Z}\rangle$ for some $a_i \in \mathbb{Z}$. It is less well-known that show that a_i may be chosen to be independent of i. This result is generalized in Theorem 4 to U_n. In addition, a rather surprising connection between the least positive primitive roots modulo an odd prime p, and primitive roots modulo p^i for $i \geq 2$, is mentioned in Theorem 3.

It is straightforward to prove that U_n is an abelian group and that $k + n\mathbb{Z} \in U_n$ if and only if $\gcd(k, n) = 1$. If $\phi(n)$ denotes the order of U_n, and p is prime, then $\phi(p^k) = p^{k-1}(p-1)$. Suppose that $n = n_1 \cdots n_r$ where the n_i are powers of distinct primes. The Chinese Remainder Theorem gives an explicit (ring) isomorphism $\mathbb{Z}_n \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$, which restricts to a (group) isomorphism $U_n \cong U_{n_1} \times \cdots \times U_{n_r}$. Therefore $\phi(n) = \phi(n_1) \cdots \phi(n_r)$. If $a + n\mathbb{Z} \in U_n$ has order k, we write $\mathrm{ord}_n(a) = k$.

Lemma 1. *Let p be a prime divisor of a positive integer r. If $p = 2$ assume 4 divides r. If $ord_r(a) = k$ and $ord_{rp}(a) = kp$, then $ord_{rp^2}(a) = kp^2$ (and hence $ord_{rp^i}(a) = kp^i$ for $i > 2$).*

Proof. First note that $\gcd(a, r) = 1$ implies $\gcd(a, rp^i) = 1$ for $i \geq 0$. It suffices to prove the result for $i = 2$, for we may then 'bootstrap' by replacing r by rp. The above formula for ϕ gives $\phi(rp) = p\phi(r)$. Hence the kernel of the group epimorphism $U_{rp} \to U_r$ given by $x + rp\mathbb{Z} \mapsto x + r\mathbb{Z}$, comprises the p elements $\{1 + rx + rp\mathbb{Z} \mid 0 \leq x < p\}$. Since $\mathrm{ord}_r(a) = k$ and $\mathrm{ord}_{rp}(a) = kp$, so $(a + rp\mathbb{Z})^k = 1 + rx + rp\mathbb{Z}$ where p does not divide x. Suppose $a^k = 1 + rx + rpy$ where $y \in \mathbb{Z}$. Applying the binomial theorem twice and noting that p divides $\binom{p}{i}$ if $0 < i < p$, shows

$$a^{kp} = (1 + rx + rpy)^p \equiv (1 + rx)^p \equiv 1 + rpx \pmod{rp^2}.$$

(When $p = 2$, the last step assumes p^2 divides r.) Thus $\mathrm{ord}_{rp^2}(a)$ is a multiple of kp, is not equal to kp, and divides kp^2. Hence $\mathrm{ord}_{rp^2}(a) = kp^2$ as desired. $\square$

THEOREM 2. *(a) Let p be an odd prime and suppose that $U_p = \langle a + p\mathbb{Z}\rangle$. Then either $U_{p^i} = \langle a + p^i\mathbb{Z}\rangle$ for $i \geq 1$, or for any x not divisible by p, $U_{p^i} = \langle a(1 + px) + p^i\mathbb{Z}\rangle$ for $i \geq 1$.*
(b) If $a \equiv 5 \pmod 8$, then $U_{2^i} = \langle a + 2^i\mathbb{Z}\rangle \dot{\times} \langle -1 + 2^i\mathbb{Z}\rangle$ is an internal direct product for $i \geq 1$.

Proof. (a) If $\mathrm{ord}_{p^2}(a) = p(p-1)$, then it follows from Lemma 1 and $\mathrm{ord}_p(a) = p-1$ that $\mathrm{ord}_{p^i}(a) = p^{i-1}(p-1)$ for $i \geq 1$. Otherwise $\mathrm{ord}_{p^2}(a) = p - 1$, and for any x not divisible by p, $a(1 + px) + p^2\mathbb{Z}$ has order $p(p - 1)$. Similarly, by Lemma 1 $\mathrm{ord}_{p^i}(a(1 + xp)) = p^{i-1}(p - 1)$ for $i \geq 1$.
(b) Since $\mathrm{ord}_4(a) = 1$ and $\mathrm{ord}_8(a) = 2$ by Lemma 1, $\mathrm{ord}_{2^i}(a) = 2^{i-2}$ for $i \geq 3$. Therefore, $(a + 2^i\mathbb{Z})^{2^{i-3}} = 1 + 2^{i-1} + 2^i\mathbb{Z}$ for $i \geq 3$, and so $\langle a + 2^i\mathbb{Z}\rangle \cap \langle -1 + 2^i\mathbb{Z}\rangle$ is trivial. As U_{2^i} has order 2^{i-1}, it follows that $U_{2^i} = \langle a + 2^i\mathbb{Z}\rangle \dot{\times} \langle -1 + 2^i\mathbb{Z}\rangle$. (Note that $\langle a + 2^i\mathbb{Z}\rangle$ is trivial if $i = 1, 2$.) □

Let p be a prime > 2, and let a_p denote the least positive primitive root modulo p. Now $a_p + p^2\mathbb{Z}$ has order $p - 1$ or $p(p - 1)$, and I guessed initially that both cases would occur frequently. I wrote a short program using MAGMA [**1**] to investigate the frequency of each case. After a few minutes, MAGMA showed that $\mathrm{ord}_{p^2}(a_p) = p(p-1)$ for *all* odd primes $p < 10^4$. Before attempting to prove the conjecture that $\mathrm{ord}_{p^i}(a_p) = p^{i-1}(p-1)$ for all odd primes p, I thought it prudent to investigate some probabilities. We know that $(a_p + p^2\mathbb{Z})^{p-1} = 1 + px + p^2\mathbb{Z}$ and that $\mathrm{ord}_{p^2}(a_p) = p(p-1)$ if and only if p does not divide x. Although x is determined once we know a_p, for convenience assume that x is equally likely to lie in any of the p congruence classes modulo p, and hence that $\mathrm{ord}_{p^2}(a_p) = p(p - 1)$ with probability $1 - 1/p$. If p_i denotes the ith prime, and the order of $a_{p_i} + p_i^2\mathbb{Z}$ is assumed to be independent of the previous primes, then this heuristic reasoning gives the probability that all odd primes $< n$ have order $p(p - 1)$ is $P(n) = \prod(1 - 1/p)$ where the product ranges over odd primes $< n$. Since $P(10^4) \approx 0.12$, we should perhaps think twice before conjecturing that $\mathrm{ord}_{p^i}(a_p) = \phi(p^i)$ for all odd primes p, and $i \geq 1$. It is easy to prove that $(1 - 1/2)P(n) < (\log n)^{-1}$ (see [**2**, p.29]). Hence $P(\infty)$ diverges (very slowly) to zero. Thus the above (admittedly tenuous heuristic) argument, suggests that counterexamples should exist, and furthermore that they should be large. I used MAGMA to search for counterexamples in the range $10^4 \leq p \leq 10^7$. After approximately 12 CPU days (!) I was very surprised to see that precisely one counterexample was found, namely $p = 40\,487$ and $a_p = 5$.

The following theorem summarizes some computational findings.

THEOREM 3. *For each prime p let a_p be the least positive integer, and b_p the greatest negative integer satisfying $U_p = \langle a_p + p\mathbb{Z}\rangle = \langle b_p + p\mathbb{Z}\rangle$. If $2 < p < 10^7$, then $U_{p^i} = \langle a_p + p^i\mathbb{Z}\rangle$ for all $i \geq 1$ except when $p = 40\,487$; and $U_{p^i} = \langle b_p + p^i\mathbb{Z}\rangle$ for all $i \geq 1$ except when $p = 3, 11$ or $3\,511$.*

While the assumption $p < 10^7$ in Theorem 3 may be superfluous, the following remark may cast some doubt on this. If the requirement that a_p be least positive were dropped, then examples abound with $\mathrm{ord}_{p^2}(a_p) = \mathrm{ord}_p(a_p) = p - 1$. For example, $p = 29, a_p = 14$; $p = 37, a_p = 18$; $p = 43, a_p = 19$ etc. The prime $3\,511$ arises in connection with the 'first case' of Fermat's last theorem. In 1909

A. Wieferich proved that if p is an odd prime and $x^p + y^p = z^p$ has a solution in the integers with xyz not divisible by p, then $2^{p-1} \equiv 1 \pmod{p^2}$. There are only two primes less than 10^7 satisfying this condition, namely 1 093 and 3 511.

Note that if $m > 1$ is a power of 3 and $n > 1$ is a power of 7, then $U_m = \langle 2+m\mathbb{Z}\rangle$ and $U_n = \langle 3 + n\mathbb{Z}\rangle$. Although U_{mn} is generated by 2 elements, it does not equal $\langle 2 + mn\mathbb{Z}, 3 + mn\mathbb{Z}\rangle$, as $3 + mn\mathbb{Z}$ is not even a unit! Note that if a and b satisfy $a \equiv 2 \pmod{m}$, $a \equiv 1 \pmod{n}$ and $b \equiv 1 \pmod{m}$, $b \equiv 3 \pmod{n}$, then $U_{mn} = \langle a + mn\mathbb{Z}, b + mn\mathbb{Z}\rangle$. However, it is not clear that a and b can be chosen to be *independent* of m and n. In fact, $U_{mn} = \langle 29 + mn\mathbb{Z}, 52 + mn\mathbb{Z}\rangle$.

Let $d(G)$ denote the minimal number of generators of a finite abelian group G.

THEOREM 4. *(a) If $n = n_1 \cdots n_r$ where $n_1, \ldots, n_r$ are pairwise coprime, then $d(U_n) = d(U_{n_1}) + \cdots + d(U_{n_r})$. Furthermore, if n is a prime-power, then $d(U_n) = 2$ if 8 divides n, and 1 otherwise.*
(b) Let $p_1, \ldots, p_r$ be distinct odd primes. Let $k_1, \ldots, k_r$ be arbitrary positive integers and set $n = p_1^{k_1} \cdots p_r^{k_r}$. If $a_i \in \mathbb{Z}$ satisfies $\mathrm{ord}_{p_i^2}(a_i) = p_i(p_i - 1)$ and $\mathrm{ord}_{p_j}(a_i) = 1$ for $j \neq i$, then $d(U_n) = r$ and $U_n = \langle a_1 + n\mathbb{Z}, \ldots, a_r + n\mathbb{Z}\rangle$.
(c) Let $p_1 = 2, p_2, \ldots, p_r$ be distinct primes. Let $k_1, \ldots, k_r$ be arbitrary positive integers and set $n = p_1^{k_1} \cdots p_r^{k_r}$. Let $a_i \in \mathbb{Z}$ satisfy $a_0 \equiv 5 \pmod{8}, a_1 \equiv -1 \pmod{8}$, $\mathrm{ord}_{p_i^2}(a_i) = p_i(p_i - 1)$ for $i \geq 2$ and $\mathrm{ord}_{p_j}(a_i) = 1$ if $p_j \neq p_i$ (set $p_0 = 2$). Then $U_n = \langle a_0 + n\mathbb{Z}, a_1 + n\mathbb{Z}, \ldots, a_r + n\mathbb{Z}\rangle$. If 8 divides n, then $d(U_n) = r + 1$, otherwise $d(U_n) = r$ and the generator $a_0 + n\mathbb{Z}$ is superfluous.

Proof. (a) It suffices to prove the theorem when the n_i are prime-powers. By the Chinese Remainder Theorem $U_n \cong U_{n_1} \times \cdots \times U_{n_r}$, and so $d(U_n) \leq d(U_{n_1}) + \cdots + d(U_{n_r})$. The reverse inequality follows from the observation that if the direct product of k copies of C_2 is a subgroup of an abelian group G, then $d(G) \geq k$. Note that if $\Omega(G)$ denotes the subgroup $\{g \in G \mid g^2 = 1\}$ of G, then $d(U_{n_i}) = d(\Omega(U_{n_i}))$. It follows by considering dimensions of vector spaces that

$$d(\Omega(U_{n_1}) \times \cdots \times \Omega(U_{n_r})) = d(\Omega(U_{n_1})) + \cdots + d(\Omega(U_{n_r})),$$

and hence that $d(U_n) \geq d(U_{n_1}) + \cdots + d(U_{n_r})$.

(b) Let $n_i = p_i^{k_i}$. Then $\mathrm{ord}_{n_i}(a_i) = \phi(n_i)$ for each i. However, it does not follow from this that $U_n = \langle a_1 + n\mathbb{Z}, \ldots, a_r + n\mathbb{Z}\rangle$. Without loss of generality assume that $p_1 < p_2 < \cdots < p_r$. If $j \neq i$, then $\mathrm{ord}_{p_j}(a_i) = 1$, so $\mathrm{ord}_{n_j}(a_i)$ divides n_j (indeed, it divides n_j/p_j). Let $e_i = n_{i+1} \cdots n_r$. If $j > i$, then $\mathrm{ord}_{n_j}(a_i^{e_i}) = 1$, and since e_i is coprime to $\phi(n_i)$, so $\mathrm{ord}_{n_i}(a_i^{e_i}) = \mathrm{ord}_{n_i}(a_i) = \phi(n_i)$. It follows now that $U_n = \langle a_1^{e_1} + n\mathbb{Z}, \ldots, a_r^{e_r} + n\mathbb{Z}\rangle$ and hence $U_n = \langle a_1 + n\mathbb{Z}, \ldots, a_r + n\mathbb{Z}\rangle$.

(c) This follows from Theorems 2(b) and 4(a) by arguing as in (b) above. □

Suppose that $p_1, \ldots, p_r$ are distinct (odd) primes and that p_i does not divide $p_j - 1$ for all $i \neq j$. Then a stronger conclusion than that in Theorem 4(b) holds. Given $n = p_1^{k_1} \cdots p_r^{k_r}$, set $n_i = p_i^{k_i}$ and $f_i = n/n_i$. Then arguing as in the proof of Theorem 4(b), $\mathrm{ord}_{n_i}(a_i^{f_i}) = \mathrm{ord}_{n_i}(a_i) = \phi(n_i)$, and $\mathrm{ord}_{n_j}(a_i^{f_i}) = 1$ if $i \neq j$. Hence, U_n is the internal direct product

$$U_n = \langle a_1^{f_1} + n\mathbb{Z}\rangle \dot{\times} \cdots \dot{\times} \langle a_r^{f_r} + n\mathbb{Z}\rangle$$

where $U_{n_i} = \langle a_i^{f_i} + n_i\mathbb{Z}\rangle \cong \langle a_i^{f_i} + n\mathbb{Z}\rangle$.

Acknowledgement

I would like to thank Weib Bosma for his helpful comments.

References

1. W. Bosma and J. Cannon, *Handbook of Magma Functions*, Sydney University, 1994.
2. I. Niven, H.S. Zuckerman and H.L. Montgomery, *An Introduction to the Theory of Numbers, Fifth Edition*, Wiley and Sons, 1991.

School of Mathematics and Statistics
University of Sydney, N.S.W. 2006, Australia