$(\mathbb{Z}/2^n\mathbb{Z})^\times$

R. C. Daileda

October 17, 2020

If p is an odd prime, we have seen that $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is cyclic for all $n \geq 1$. However, we have also shown that the group $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is only cyclic for $n = 1, 2$. This is because $\varphi(2^n) = 2^{n-1}$ but we have congruence

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

for all odd a and $n \geq 3$. This means that when $n \geq 3$, there are no elements of order exceeding 2^{n-2} in $(\mathbb{Z}/2^n\mathbb{Z})^\times$. Notice that $2^{n-2} = \varphi(2^n)/2$ is then the largest possible order allowed for an element of $(\mathbb{Z}/2^n\mathbb{Z})^\times$, and it is natural to ask whether an element of this order actually exists. As we will shortly see, such an "almost primitive root" always exists, and can be given explicitly. We begin with two lemmas.

Lemma 1. *Let $k \in \mathbb{N}$. Then $5^k + 1 = 2\ell$ where ℓ is odd.*

Proof. We have

$$5^k + 1 \equiv 1^k + 1 \equiv 1 + 1 \equiv 2 \pmod 4.$$

The conclusion follows at once. □

Lemma 2. *Let $k \in \mathbb{N}$. Then*

$$5^{2^k} - 1 = 4\prod_{j=0}^{k-1}\left(5^{2^j} + 1\right).$$

Proof. We induct on k. When $k = 1$ we have

$$5^2 - 1 = (5-1)(5+1) = 4(5^{2^0} + 1),$$

so that the result holds. Now assume the result for some $k \geq 1$. Then

$$\begin{aligned} 5^{2^{k+1}} - 1 &= \left(5^{2^k}\right)^2 - 1 = \left(5^{2^k} - 1\right)\left(5^{2^k} + 1\right) \\ &= 4\prod_{j=0}^{k-1}\left(5^{2^j} + 1\right)\left(5^{2^k} + 1\right) = 4\prod_{j=0}^{k}\left(5^{2^j} + 1\right), \end{aligned}$$

which completes the induction.

□

Remarks.

1. The conclusion of Lemma 2 holds for $k = 0$, too, provided we interpret the empty product as equal to 1.

2. If we replace 5 by the variable X, the proof of Lemma 2 yields the polynomial factorization

   $$X^{2^k} - 1 = (X-1)\prod_{j=0}^{k-1}(X^{2^j}+1),$$

   which expresses $X^{2^k} - 1$ as the product of irreducible *cyclotomic polynomials.*

3. All of our results remain valid if 5 is replaced by any integer a satisfying $a \equiv 5 \pmod{8}$.

Corollary 1. *Let $k \in \mathbb{N}_0$. Then 2^{k+2} exactly divides $5^{2^k} - 1$. That is, $2^{k+2} | 5^{2^k} - 1$, but $2^{k+3} \nmid 5^{2^k} - 1$.*

Proof. If $k = 0$, the result is immediate, so we assume that $k \geq 1$. By Lemmas 1 and 2 we then have

$$5^{2^k} - 1 = 4\prod_{j=0}^{k-1}\left(5^{2^j}+1\right) = 5^{2^k} - 1 = 4\prod_{j=0}^{k-1}(2\ell_j) = 2^{k+2}\prod_{j=0}^{k-1}\ell_j,$$

for some odd integers ℓ_j. The result now follows. □

We can now prove our first main result.

Theorem 1. *Let $n \geq 2$. Then 5 has order 2^{n-2} modulo 2^n.*

Proof. When $n = 2$ there is nothing to prove, since $5 \equiv 1 \pmod{4}$. So we suppose that $n \geq 3$. Then we may apply Corollary 1 with $k = n-3$ to conclude that $5^{2^{n-3}} \equiv 1 \pmod{2^{n-1}}$ and $5^{2^{n-3}} \not\equiv 1 \pmod{2^n}$. Since the order of 5 modulo 2^n must divide 2^{n-2} by (1), this yields the conclusion. □

Because 5 is "almost" a primitive root modulo 2^n, we can "almost" express every odd integer (modulo 2^n) as a power of 5. Specifically we have:

Theorem 2. *Let $n \geq 2$. Then for every odd $a \in \mathbb{Z}$ there exist unique $\epsilon \in \{\pm 1\}$ and $0 \leq k \leq 2^{n-2} - 1$ so that*

$$a \equiv \epsilon 5^k \pmod{2^n}.$$

Proof. Because 5 has order 2^{n-2}, the 2^{n-2} congruence classes

$$5^k + 2^n\mathbb{Z}, \;\; 0 \leq k \leq 2^{n-2} - 1$$

are all distinct, as are the 2^{n-2} classes

$$-5^k + 2^n\mathbb{Z}, \;\; 0 \leq k \leq 2^{n-2} - 1.$$

If we can show that these two lists have no classes in common we will be finished, since then we will have $2^{n-2} + 2^{n-2} = 2 \cdot 2^{n-2} = 2^{n-1} = \varphi(2^n)$ distinct congruence classes.

So assume to the contrary that $5^k + 2^n\mathbb{Z} = -5^\ell + 2^n\mathbb{Z}$ for some k, ℓ. Then, by cancellation, we find that $5^j \equiv -1 \pmod{2^n}$ for some $j \in \mathbb{N}_0$. That is, $2^n | 5^j + 1$. This contradicts Lemma 1, and completes the proof.

□

In the language of group theory, Theorem 2 shows that for $n \geq 3$ there is an isomorphism

$$(\mathbb{Z}/2^n\mathbb{Z})^\times \cong \{\pm 1\} \times \langle 5 + 2^n\mathbb{Z}\rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}.$$