19. Miscellanea

We know that the group of units in a finite field is always cyclic. It is interesting to figure out all of the generators in a given example.

Example 19.1. *What are the generators of the units in $\mathbb{Z}_{13}$?*

By general theory, the units U in $\mathbb{Z}_{13}$ are a cyclic group of order 12.

Actually we can prove this by hand. Any abelian group of order $12 = 2^2 \cdot 3$ is isomorphic to one of

(1) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$,
(2) $\mathbb{Z}_4 \times \mathbb{Z}_3$,

by the fundamental theorem of finitely generated abelian groups. The second group is cyclic. In the first group every element has order dividing six. But then for every unit $\alpha \in U$ we have

$$\alpha^6 = 1.$$

Thus α is a root of the polynomial $x^6 - 1 \in \mathbb{Z}_{13}[x]$ and this polynomial has at most 6 roots. As U has twelve elements, this is not possible. Thus U is cyclic of order 12.

Any such is abstractly isomorphic to the group $\mathbb{Z}_{12}$ under addition. The generators of this group are the numbers from 1 to 12 coprime to 12. This is computed by Euler's phi-function

$$\varphi(12) = \varphi(3)\varphi(4) = (3-1)(4-2) = 4.$$

Thus there are four generators of the group of units.

By Lagrange if $a \in U$ is a unit then a has order dividing 12. The divisors of 12 are 1, 2, 3, 4, 6 and 12. So if a does not have order 12, we must either have $a^4 = 1$ or $a^6 = 1$. To find a generator we just need to find a such that $a^4 \neq 1$ and $a^6 \neq 1$. We use trial and error. If $a = 2$ then

$$2^2 = 4 \qquad 2^4 = 16 = 3 \neq 1 \qquad \text{and} \qquad 2^6 = 4 \cdot 3 = 12 = -1 \neq 1.$$

Thus 2 is a generator of U.

We could use trial and error to find the other generators.

Here is another way. As U has order 12, U is isomorphic to $\mathbb{Z}_{12}$. The generators of this are the numbers coprime to 12,

$$1 \qquad 5 \qquad 7 \qquad \text{and} \qquad 11.$$

Thus the generators of U are

$$2^1 = 2 \qquad 2^5 = 6 \qquad 2^7 = 11 \qquad \text{and} \qquad 2^{11} = 7.$$