Orbits of the Multiplicative Group mod m

Klaus Pommerening
Fachbereich Mathematik
der Johannes-Gutenberg-Universität
Saarstraße 21
D-55099 Mainz

February 13, 2018—last change February 13, 2018

Let R be the ring $\mathbb{Z}/m\mathbb{Z}$ of residue classes mod m for an integer $m \geq 2$. Then the multiplicative group $R^\times$ acts by multiplication on R. A trivial fact is that $R^\times$ itself is one orbit. A standard result of elementary number theory, see also [1], says that $R^\times$ consists exactly if the residues of $b \in \mathbb{Z}$ with $\gcd(m, b) = 1$, in other words:

Proposition 1 *For $b \in \mathbb{Z}$ with $\gcd(m, b) = 1$ there is an $a \in \mathbb{Z}$ with*

$$ab \equiv 1 \pmod{m}.$$

More generally:

Proposition 2 *Let $m \in \mathbb{N}$, $m \geq 2$, and $a, b \in \mathbb{Z}$ with $\gcd(b, m) = d$. Then a is divisible by b in $\mathbb{Z}/m\mathbb{Z}$, if and only if $d|a$. In this case there are exactly d solutions z of $zb \equiv a \pmod{m}$ with $0 \leq z < m$, and any two of them differ by a multiple of $\bar{m} = m/d$. If $d = xm + yb$ and $a = td$, then $z = yt$ is a solution.*

Proposition 2 applies in particular for $a = d$ and yields:

Corollary 1 *Let $m \in \mathbb{N}$, $m \geq 2$, and $b \in \mathbb{Z}$ with $\gcd(b, m) = d$. Let $c \in \{1, \ldots, \bar{m} - 1\}$ represent the multiplicative inverse of $\bar{b} = b/d$ in $\mathbb{Z}/\bar{m}\mathbb{Z}$. Then the d solutions x of $xb \equiv d \pmod{m}$ with $0 \leq x < m$ are*

$$c + t\bar{m} \quad \text{for } t = 0, \ldots, d-1. \tag{1}$$

This statement includes the triviality $cb \equiv d \bmod m$. However c is not necessarily relatively prime with m, as the following example demonstrates.

Example Let $m = 30$ and $b = 20$. Then $d = 10$, $\bar{m} = 3$, $\bar{b} = 2$, $c = 2$ since $2 \cdot 2 = 4 \equiv 1 \bmod 3$. Thus the solutions of $xb \equiv d \pmod{m}$ with $0 \leq x < m$ are

$$2,\ 5,\ 8,\ 11,\ 14,\ \ldots,$$

the first three of them having a common divisor with m. However the fourth one, 11, is relatively prime with m.

This is not by fluke:

Theorem 1 *Let $m \in \mathbb{N}$, $m \geq 2$, and $b \in \mathbb{Z}$ with $\gcd(b, m) = d$. Then there is an $a \in \mathbb{Z}$, relatively prime with m, such that $ab \equiv d \pmod{m}$.*

Proof. Let P be the set of prime divisors of m and $r_p \geq 1$ be the multiplicity of $p \in P$ in m. Thus

$$m = \prod_{p \in P} p^{r_p}.$$

For each $p \in P$ let $s_p \geq 0$ be the multiplicity of p in b. Then

$$d = \prod_{p \in P} p^{q_p} \qquad \text{with } q_p = \begin{cases} s_p & \text{if } r_p > s_p, \\ r_p & \text{if } r_p \leq s_p, \end{cases}$$
$$\bar{m} = \prod_{p \in P} p^{r_p - q_p}.$$

Now $b = d \cdot u$ where u is relatively prime with $\bar{m}$, and $c \in \{1, \ldots, \bar{m} - 1\}$ is defined by $cu \equiv 1 \pmod{\bar{m}}$. In particular $p \not| c$ if $p \,|\, \bar{m}$, that is if $r_p > s_p$. The solutions x of $xb \equiv d \pmod{m}$ with $0 \leq x < m$ are given by Formula (1). We want to find at least one among them that has no prime divisor in P. To this end let

$$Q := \{p \in P \mid r_p \leq s_p,\ p \not| c\}, \quad \text{and } t := \prod_{p \in Q} p.$$

Then $p \not| (c + t\bar{m})$ for all $p \in P$:

Case 1, $s_p < r_p$. Then $p \,|\, \bar{m}$ and $p \not| c$, hence $p \not| (c + t\bar{m})$.

Case 2, $s_p \geq r_p$ and $p \in Q$. Then $p \not| c$, $p \not| \bar{m}$, and $p \,|\, t$. Hence $p \not| (c + t\bar{m})$.

Case 3, $s_p \geq r_p$ and $p \notin Q$. Then $p \,|\, c$, $p \not| \bar{m}$, $p \not| t$. Hence $p \not| (c + t\bar{m})$.

The proof of the theorem is complete. $\diamond$

Therefore the divisors of m represent all $(\mathbb{Z}/m\mathbb{Z})^\times$-orbits in $\mathbb{Z}/m\mathbb{Z}$:

Corollary 2 *The orbits of $(\mathbb{Z}/m\mathbb{Z})^\times$ in $\mathbb{Z}/m\mathbb{Z}$ are the orbits of the divisors of m.*

References

[1] K. Pommerening: The Euclidean Algorithm. Online: http://www.staff.uni-mainz.de/pommeren/MathMisc/LinDio.pdf