Mutual Multiples in $\mathbb{Z}_n$

ZUN SHAN
Nanjing Normal University
Nanjing, Jiangsu
People's Republic of China

EDWARD T.H. WANG
Wilfrid Laurier University
Waterloo, Ontario N2L 3C5
Canada

The following problem appeared in [**1**]:

PROBLEM: *Let R be a commutative ring with unit element* 1. *Prove or disprove*: *If $a, b \in R$ are multiples of one another, then they are* unit *multiples of one another*; *that is, there is an invertible element $u \in R$ such that $a = ub$.*

The given statement is false for a general commutative ring R (see [**3**]). We show here, however, that it is true for $\mathbb{Z}_n$.

In what follows we will use ϕ to denote the Euler phi-function; $\tau(n)$ will denote the number of positive divisors of n. The following definition will be convenient:

DEFINITION. Let $\mathbb{Z}_n$ be the commutative ring of integers modulo n, where $n > 1$ is a given natural number. Two elements a and b of $\mathbb{Z}_n$, not necessarily distinct, are said to form an MM pair (mutual multiple pair) if there exist $i, j \in \mathbb{Z}_n$ such that $a = ib$ and $b = ja$ in $\mathbb{Z}_n$; that is, $a \equiv ib \pmod{n}$ and $b \equiv ja \pmod{n}$. In this case, i and j are called *multipliers*.

Note that 0 cannot form an MM pair with any element of $\mathbb{Z}_n$ but itself. Also, if $n = p$ is a prime, then clearly any two non-zero elements of Z_p form an MM pair, and the multipliers i and j are both unique.

Following is a more meaty example.

Example: In $\mathbb{Z}_6$, the numbers 2 and 4 form an MM pair since $4 = 2 \times 2$ and $2 = 5 \times 4$. Similarly, 1 and 5 form an MM pair since $5 = 5 \times 1$ and $1 = 5 \times 5$. On the other hand, 3 and 4 do not form an MM pair since $3j \equiv 0$ or $3 \pmod 6$ depending on whether j is even or odd.

Observe that when a and b form an MM pair, the multipliers i and j need not be unique in general even if $a \neq 0$ and $b \neq 0$; e.g., in $\mathbb{Z}_6$ we could also write $4 = 5 \times 2$ and/or $2 = 2 \times 4$.

LEMMA 1. *Let $a, b \in \mathbb{Z}_n$. Then a and b form an MM pair if and only if* $\gcd(a, n) = \gcd(b, n)$.

Proof. Suppose a and b form an MM pair. Then there exist $i, j \in \mathbb{Z}_n$ such that $a = ib$ and $b = ja$. Since $\gcd(a, n) | a$ implies $\gcd(a, n) | ja$, we have $\gcd(a, n) | b$ and so $\gcd(a, n) | \gcd(b, n)$. Similarly, $\gcd(b, n) | \gcd(a, n)$ and thus $\gcd(a, n) = \gcd(b, n)$.

Conversely, suppose $\gcd(a, n) = \gcd(b, n) = d$. Let $a = da'$ and $b = db'$. Then either $a = b = 0$ or $\gcd(a', n) = \gcd(b', n) = 1$. Since $\gcd(a', n/d) = \gcd(b', n/d) = 1$ there exist $i, j \in \mathbb{Z}_n$ such that $a' \equiv b'i$ and $b' \equiv a'j \pmod{n/d}$. Hence $a \equiv ib$ and $b \equiv ja \pmod{n}$. This completes the proof.

THEOREM 1. *Suppose $a, b \in \mathbb{Z}_n$ form an MM pair. Then there exists an invertible element $u \in \mathbb{Z}_n$ such that $a = ub$.*

Proof. As in the proof of the lemma, let $\gcd(a, n) = \gcd(b, n) = d$, $a = da'$, and $b = db'$.

Then there exists $i \in \mathbb{Z}_n$ such that $a' \equiv b'i \pmod{n/d}$. Clearly $\gcd(i, n/d) = 1$ as $\gcd(a', n/d) = 1$. By the celebrated theorem of Dirichlet, there are infinitely many primes in the sequence $\{i + k(n/d)\}_{k=0}^{\infty}$, and hence, *a fortiori*, there are primes in this sequence that exceed n. Thus there exists $k_0 \in \mathbb{N}$ for which $i + k_0(n/d)$ is such a prime, and so $\gcd(i + k_0(n/d), n) = 1$. If we let u denote the least positive residue of $i + k_0(n/d)$ modulo n, then $u \in \mathbb{Z}_n$ is such that

$$\gcd(u, n) = 1 \quad \text{and} \quad ub' \equiv ib' \equiv a' \pmod{n/d};$$

it follows that $a \equiv ub \pmod{n}$, which completes the proof.

Remark 1. The key to the preceding proof is the existence of an integer in the sequence $\{i + k(n/d)\}_{k=0}^{\infty}$ that is coprime with n. This result, which is a consequence of Dirichlet's theorem, appeared in [**4**, p. 12, Ex. 3] with an elementary proof.

As we explored MM pairs in $\mathbb{Z}_n$, we were led to wonder how many there are. We found the following answer:

THEOREM 2. *Let $f(n)$ denote the number of unordered MM pairs in $\mathbb{Z}_n$. Then $f(n) = \frac{1}{2}[n + \sum_{d|n} \phi(d)^2]$; the summation is over all positive divisors d of n.*

Proof. For each divisor d of n and for any $a \in \mathbb{Z}_n$, note that $\gcd(a, n) = d$ if and only if $a = da'$ for some $a' \in Z_{n/d}$ such that $\gcd(a', n/d) = 1$. Hence if we let $Z_{n/d}^* = \{m \in \mathbb{Z}_{n/d} | \gcd(m, n/d) = 1\}$, then, by Lemma 1, any two elements of $\mathbb{Z}_{n/d}^*$ would form an MM pair and no elements of $\mathbb{Z}_{n/d}^*$ can form an MM pair with elements not in the set. Since $|\mathbb{Z}_{n/d}^*| = \phi(n/d)$, we have

$$f(n) = \sum_{d|n} \left[\phi(n/d) + \binom{\phi(n/d)}{2} \right] = \sum_{d|n} \left[\phi(d) + \binom{\phi(d)}{2} \right]$$

$$= \frac{1}{2} \sum_{d|n} \left[\phi(d) + \phi(d)^2 \right] = \frac{1}{2} \left[n + \sum_{d|n} \phi(d)^2 \right],$$

where the last equality holds because $\sum_{d|n} \phi(d) = n$ (see, e.g., [**2**, Thm. 6.7, p. 212]).

Remark 2. Since there is no known closed form expression for $\sum_{d|n} \phi(d)^2$, the only way to find the exact value of $f(n)$ is to compute $\phi(d)$ for all divisors d of n. A corollary, however, gives a lower bound for $f(n)$.

COROLLARY: $f(n) \geq \frac{n}{2}\left(\frac{n}{\tau(n)} + 1\right)$.

Proof. By the Cauchy–Schwarz inequality,

$$\sum_{d|n} \phi(d)^2 \sum_{d|n} 1^2 \geq \left(\sum_{d|n} \phi(d) \right)^2 = n^2,$$

so $\sum_{d|n} \phi(d)^2 \geq n^2/\tau(n)$. Substituting this into the formula from Theorem 2 completes the proof.

Acknowledgment This paper was written when the first author was visiting the Department of Mathematics at Wilfrid Laurier University, December 1996–August 1997. The hospitality of WLU is greatly appreciated. The authors would like to thank the referee for many constructive suggestions, which substantially improved this paper.

REFERENCES

1. Benkart, G. M., et. al., Problem #600, *College Math. Journal* 28:2 (1997), 146.
2. Rosen, Kenneth H., *Elementary Number Theory and Its Applications*, 3rd ed., Addison Wesley, Reading, MA, 1993.
3. Shan, Zun and Wang, Edward T. H., Solution to Problem #600 (Unit Multiples), *College Math. Journal*, 29:2 (1998), 156–157.
4. Sierpinski, W., *Elementary Theory of Numbers*, North-Holland, Amsterdam, The Netherlands, 1988.

Unevening the Odds of "Even Up"

ARTHUR T. BENJAMIN
Harvey Mudd College
Claremont, CA 91711

JENNIFER J. QUINN
Occidental College
Los Angeles, CA 90041

The Disclaimer The authors take no responsibility for any gambling hustles or scams based on applications of the principles contained in this note.

The Game "Even Up" is a game of solitaire played with 40 cards from a standard deck that has its jacks, queens, and kings removed. The cards are shuffled and dealt in a row. If a consecutive pair of cards adds to an even number, then that pair can be removed. The object of the game is to remove all of the cards.

More generally, we can play Even Up with $2n$ cards, x of them being odd and $2n-x$ being even. We require the number of cards to be even since the game cannot be won with an odd number of cards. In fact, the game cannot be won when x is odd since odd valued cards are removed in pairs. Harkleroad [**1**] showed that the game involves no skill, in that the outcome is predetermined by the original order of the $2n$ cards, and that the probability of winning is $p(2n,x)=\binom{n}{x/2}^2/\binom{2n}{x}$. Thus the probability of winning the original game is $p(40,20)=0.248$.

A few remarks about $p(2n,x)$ are called for. Clearly $p(2n,0)=1=p(2n,2n)$. By comparing $p(2n,x)$ with $p(2n,x-2)$, one sees that for fixed n the probability of winning is minimized when $x=n$. When n is large, we can use Stirling's formula $(n!\approx(n/e)^n\cdot\sqrt{2\pi n}\,)$ to obtain $p(2n,n)\approx 2/\sqrt{\pi n}$.

For our purposes, any arrangement of $2n$ cards can be represented as the product of a's and b's with a's denoting odd cards and b's denoting even cards. The rules of Even Up reduce to the two multiplications $a^2=1$ and $b^2=1$. Every game simplifies to exactly one string of the form $(ab)^z$, where $-n\le z\le n$ and $(ab)^{-z}=(ba)^z$. Winning games occur when $z=0$. Letting $f(2n,x,z)$ denote the number of arrange-