Cycles of Residues Generated by Divisibility Tests

James T. Bruening and Deanna Kindhart

Introduction

Divisibility tests have long fascinated mathematicians and mathematics students. Tests for divisibility by 2, 3, 5, 9, and 11, for example, are very familiar and are based on modular arithmetic. The tests for 2 and 5 work because $10 \equiv 0 \pmod{2}$ and $10 \equiv 0 \pmod{5}$; tests for 3 and 9 work because $10 \equiv 1 \pmod{3}$ and $10 \equiv 1 \pmod{9}$ and the test for 11 works because $10 \equiv -1 \pmod{11}$. The history of mathematics has recorded many efforts to devise tests for divisibility by other positive integers, especially primes [1], [2], [3], [5], [7]. This paper will study cycles of residues generated by repeating tests for divisibility by a prime, and we will show relationships between the cycles and aspects of group theory from abstract algebra.

Divisibility Tests

To check for divisibility of the positive integer N by the prime 7, we write N as $10t + u$, where t and u are integers with $0 \leq u < 10$. We have $N = 10t + u \equiv 3t - 6u \equiv 3(t - 2u) \pmod{7}$. Since 3 is relatively prime to 7, we have $N \equiv 0 \pmod{7}$ if and only if $t - 2u \equiv t + 5u \equiv 0 \pmod{7}$. We will say that $t + 5u$ is a divisibility test for 7.

In general, for a prime p, we will say that $t + ku$, $1 \leq k \leq p - 1$, is a *divisibility test* for p if, for each positive integer N,

$$N = 10t + u \equiv 0 \pmod{p} \quad \text{if and only if} \quad t + ku \equiv 0 \pmod{p} .$$

See [1], [5]. We first prove the following.

Lemma 1 Let p be a prime that does not divide 10 and let k_p denote the smallest positive solution of $10x \equiv 1 \pmod{p}$). Then k_p is the only integer for which $t + k_p u$ is a divisibility test for p.

Proof: Since $\gcd(10, p) = 1$, the congruence $10x \equiv 1 \pmod{p}$ has exactly one incongruent solution. Hence, $10k_p \equiv 1 \pmod{p}$. Thus, for each positive integer $N = 10t + u$, one has

$$\begin{aligned} p \mid N &\iff 10t + u \equiv 0 \pmod{p} \\ &\iff 10t + 10k_p u \equiv 0 \pmod{p} \\ &\iff t + k_p u \equiv 0 \pmod{p} . \end{aligned}$$

■

Examples of Cycles

Example 1: Let $p = 7$. As noted earlier, $t + 5u$ is a divisibility test for 7. If $N = 104$, then $t = 10$ and $u = 4$, and we have $t + 5u = 30$. Note that $30 \equiv 2 \pmod 7$. Since $t + 5u = 30$ in the first step, we next let $N = 30$. For this value of N, we have $t = 3$ and $u = 0$, and $t + 5u = 3$. Continuing in this fashion, one can check that the cycle of residues that one generates is

N	104	30	3	15	26	32	13
$t + 5u$	30	3	15	26	32	13	16
Res	2	3	1	5	4	6	2

This is the cyclic group $\langle 5 \rangle \pmod 7$. (We chose 5 as the generator, since $k_7 = 5$.) Later we prove that this is true in general. Note that the remainder when 104 is divided by 7 is 6, the last number in the cycle before it repeats. We will also prove this in general. See Theorem 1.

Example 2: A divisibility test for the prime 13 is of the form $t + 4u$ (from Lemma 1), since $10 \cdot 4 \equiv 1 \pmod{13}$. For $N = 107$, we generate the following residues:

N	107	38	35	23	14	17	29
$t + 4u$	38	35	23	14	17	29	38
Res	12	9	10	1	4	3	12

Again, the residues form a cycle, also of length 6. But this time the cycle is the cyclic group $\langle 4 \rangle \pmod{13}$, since $k_{13} = 4$ and $4^6 \equiv 1 \pmod{13}$. The remainder when 107 is divided by 13 is 3, as seen by the residue that appears just before the cycle repeats.

Example 3: Consider the cycle of residues when 93 is divided by 13.

N	93	21	6	24	18	33	15
$t + 4u$	21	6	24	18	33	15	21
Res	8	6	11	5	7	2	8

This cycle of residues also contains six elements, but there are no elements in common with the cycle generated when 107 is divided by 13, because the last cycle is the left coset $8 \cdot \langle 4 \rangle \pmod{13}$. Thus, when the two cycles are combined, they give exactly the multiplicative group $\mathbb{Z}_{13}^*$, or the set of positive integers less than the divisor 13. We will say that the prime 13 has two cycles of length 6.

Cycles Generated by Repeating the Divisibility Test

We want to investigate the cycle of residues formed by repeating the $t + k_p u$ divisibility test for a given number N and a given prime $p > 5$. Let $N = N_1 = 10t_1 + u_1$, $0 \leq u_1 \leq 9$, and assume that $N \equiv \gamma \pmod p$, $1 \leq \gamma \leq p - 1$. Thus, γ is the remainder when N is divided by p. Find γ_1 such that $t_1 + k_p u_1 \equiv \gamma_1 \pmod p$, $1 \leq \gamma_1 \leq p - 1$. To generate the cycle, let $N_2 = t_1 + k_p u_1 = 10t_2 + u_2$, $0 \leq u_2 \leq 9$, and then calculate

$\gamma_2 \equiv t_2 + k_p u_2 \pmod{p}$, $1 \leq \gamma_2 \leq p-1$. Continuing this process, we can form the sequence $\{\gamma_1, \gamma_2, \gamma_3, \ldots\}$, where $1 \leq \gamma_i \leq p-1$ for all i. We have implied that the cycles of residues are either the cyclic subgroup $\langle k_p \rangle \pmod{p}$ or a coset of this subgroup. We will show that this is true in general.

Lemma 2 Let p be a prime that does not divide 10. Then the sequence of residues $\{\gamma_1, \gamma_2, \gamma_3, \ldots\}$ satisfies $\gamma_{i+1} \equiv k_p \gamma_i \pmod{p}$, for $i = 1, 2, \ldots$.

Proof: We know that $t_1 + k_p u_1 \equiv \gamma_1 \pmod{p}$. Hence, $10k_p \equiv 1 \pmod{p}$ implies that

$$N_1 = 10t_1 + u_1 \equiv \gamma \equiv 10t_1 + 10k_p u_1 \equiv 10k_p \gamma \pmod{p} .$$

Since 10 and p are relatively prime, we have $t_1 + k_p u_1 \equiv k_p \gamma \pmod{p}$. Therefore, $\gamma_1 \equiv k_p \gamma \pmod{p}$. Repeating the test for $N_2 = t_1 + k_p u_1$ gives $\gamma_2 \equiv k_p \gamma_1 \pmod{p}$. It follows by induction that for all i, one has $\gamma_{i+1} \equiv k_p \gamma_i \pmod{p}$. ∎

It follows at once that if a cycle of residues contains an element $\gamma_j = 1$, then this cycle forms the cyclic subgroup $\langle k_p \rangle = \{k_p, k_p^2, k_p^3, \ldots, k_p^{L_p} = 1\}$ of the multiplicative group $\mathbb{Z}_p^*$, where L_p is the number of elements in a cycle. That is, $\gamma_i \neq \gamma_j$, $1 \leq i < j \leq L_p$ and $\gamma_{L_p+1} = \gamma_1$. From this we can establish the following result.

Theorem 1 Let p be a prime that does not divide 10. Then γ_{L_p}, the last element of the cycle formed by applying the divisibility test $t + k_p u$ to N, is the remainder when N is divided by p.

Proof: As usual, let $N = 10t + u$, $0 \leq u \leq 9$. Then $k_p^{L_p} \equiv 1 \pmod{p}$, $10k_p \equiv 1 \pmod{p}$, $t + k_p u \equiv \gamma_1 \pmod{p}$, and $\gamma_{i+1} \equiv k_p \gamma_i \pmod{p}$. Thus,

$$\begin{aligned} 10t + u &\equiv 10k_p^{L_p} t + k_p^{L_p} u \equiv 10k_p k_p^{L_p - 1} t + k_p^{L_p} u \\ &\equiv k_p^{L_p - 1} t + k_p^{L_p} u \equiv k_p^{L_p - 1}(t + k_p u) \\ &\equiv k_p^{L_p - 1} \gamma_1 \equiv \gamma_{L_p} \pmod{p} . \end{aligned}$$

Since $1 \leq \gamma_{L_p} < p$, we see that γ_{L_p} is the remainder when N is divided by p. ∎

The last computation in the proof of Theorem 1 shows that we do not need to calculate the whole cycle $\{\gamma_1, \gamma_2, \ldots, \gamma_{L_p}\}$ to find the remainder. The fact that $10k_p \equiv 1 \pmod{p}$ implies that 10 is the inverse of k_p in the multiplicative group $\mathbb{Z}_p^*$. Hence, from $\gamma_1 \equiv \gamma_{L_p+1} \equiv k_p \gamma_{L_p} \pmod{p}$, we conclude that $\gamma_{L_p} \equiv k_p^{-1} \gamma_1 \equiv 10\gamma_1 \pmod{p}$. For example, if $N = 125$ and $p = 17$, then $k_{17} = 12$. Performing the $t + k_{17} u$ divisibility test on $N = 125$ gives $12 + 12(5) = 72$. Then $72 \equiv 4 \pmod{17}$. Thus, $\gamma_1 = 4$, and $\gamma_{L_p} \equiv 10 \cdot 4 \equiv 6 \pmod{17}$. The remainder when 125 is divided by 17 is 6.

We now relate this study of cycles of residues to established theorems and results from group theory. Using Theorem 1 and the fact that

$\langle 10\rangle = \langle k_p^{-1}\rangle = \langle k_p\rangle$, we have $\{\gamma_1, \gamma_2, \ldots, \gamma_{L_p}\} = r \cdot \langle 10\rangle$, where r denotes the remainder on division of N by p. Hence, the cycle is a group if and only if $r \in \langle 10\rangle$. That is, if and only if $10^j \equiv r \pmod p$ for some non-negative integer j. The examples given above illustrate these facts.

Note that the length L_p of the cycle is also the order of k_p in $\mathbb{Z}_p^*$, since $k_p^{L_p} \equiv 1 \pmod p$ and $k_p^j \not\equiv 1 \pmod p$ for $1 \le j < L_p$. Thus, either k_p or 10 generates the cyclic subgroup $\mathbb{Z}_p^*$ if and only if $L_p = p - 1$, see [4, pp. 74-75].

Furthermore, from Lagrange's Theorem [4, p. 137], we know that the order of $\langle k_p\rangle$ is a divisor of $p - 1$, the order of the group $\mathbb{Z}_p^*$. Hence, there are exactly $m_p = (p-1)/L_p$ different cycles, and all of these cycles can be obtained by applying the $t + k_p u$ divisibility test to appropriate elements of any reduced system of positive residues $\bmod p$.

Consider also the period of the decimal expansion of $1/p$ which has been shown to be the order of $10 \pmod p$ [6]. We have discussed earlier that 10 has order L_p modulo p; whence, the period of the decimal expansion of $1/p$ will be L_p also. For example, $1/7 = .\overline{142857}$, and the period of the decimal expansion of $p = 7$ is 6, the same as the length of the cycle illustrated in Example 1. For $p = 13$, one has $1/13 = .\overline{076923}$. Thus, the period of the decimal expansion and the length of the cycles illustrated in the second and third examples are all 6.

Cycles of Residues for Different Forms of N

Generalizing the definition of a divisibility test for p given for the case that N is written as $N = 10t + u$, $0 \le u < 10$, we say that $t + k_p^s b$ is the divisibility test for p when N is written as $N = 10^s t + b$, $0 \le b < 10^s$, where $10k_p \equiv 1 \pmod p$ (which implies that $10^s k_p^s \equiv 1 \pmod p$.) As before,

$$\begin{aligned} p \mid N &\iff N = 10^s t + b \equiv 0 \pmod p \\ &\iff 10^s t + 10^s k_p^s b \equiv 0 \pmod p \\ &\iff t + k_p^s u \equiv 0 \pmod p\ . \end{aligned}$$

Therefore, $t + k_p^s u$ is a divisibility test for the prime p when N is written in the form $N = 10^s t + b$.

Let us again look at the example with $N = 107$ and $p = 13$. If N is written in the form $N = 100t + b$, then $4^2 = 16 \equiv 3 \pmod{13}$ implies that $t + 3b$ is now the divisibility test for the prime 13. We then get

N	107	22	66	198
$t + 3u$	22	66	198	295
Res	9	1	3	9

The length of this cycle is now only three, and this cycle is a proper subset of the earlier cycle $\{12, 9, 10, 1, 4, 3\}$. This is not surprising, since $k_{13} = 4$, and $4^6 \equiv 1 \pmod{13}$ implies that $4^6 = (4^2)^3 \equiv 3^3 \equiv 1 \pmod{13}$. Therefore, k_{13}^2 has order 3.

If $L_{p,s}$ is the length of the cycle of residues generated by repeating the divisibility test $t+k_p^s u$ for some number $N = 10^s t+b$, $0 \leq b < 10^s$, divided by the prime p, then each cycle of residues is a coset of $\langle k_p^s \rangle \pmod p$, and the number of distinct cycles is $m_{p,s} = (p-1)/L_{p,s}$. It is well known that k_p^s has order $L_p/\gcd(L_p, s)$; whence, $L_{p,s} = L_p/\gcd(L_p, s)$, and $m_{p,s} = (p-1) \cdot \gcd L_{p,s}/L_p = m_p \cdot \gcd(L_p, s)$.

To illustrate the formulas for $L_{p,s}$ and $m_{p,s}$, consider the prime $p = 17$ and the divisibility test $t+12u$. Now 12 is a primitive root modulo 17. Thus, $L_{17} = 16$ and $m_{17} = 1$. For $s = 2$, one has $L_{17,2} = L_{17}/\gcd(L_{17}, 2) = 8$, and $m_{17,2} = m_{17} \cdot \gcd(L_{17}, 2) = 2$. On the other hand, for $s = 3$, we have $L_{17,2} = L_{17}/\gcd(L_{17}, 3) = 16$, and $m_{17,3} = m_{17} \cdot \gcd(L_{17}, 3) = 1$. These values can be verified by direct calculation.

We have worked in bases of the form $b = 10^s$, with $s \geq 1$ and p a prime that does not divide 10. One can readily verify that all of the results in this paper are also true in an arbitrary base b that is not a multiple of p.

Acknowledgement: The authors wish to thank the referee for his constructive remarks which have helped to improve the quality of this paper.

References

[1] Mangho Ahuja and James Bruening, A survey of divisibility tests with a historical perspective, *Bulletin of the Malaysian Math. Soc.* **22** (1999), 35–43.

[2] S.J. Bezuszka, A Test for Divisibility by Primes, *Arithmetic Teacher* **33** (1985), 36–38.

[3] B. Bold, A General Test for Divisibility by any Prime (except 2 and 5), *The Mathematics Teacher* **58** (1965), 311–312.

[4] Joseph A. Gallian, *Contemporary Abstract Algebra*, 5th ed., Houghton Mifflin, 2002.

[5] R.L. Morton, Divisibility by 7, 11, 13, and greater primes, *The Mathematics Teacher* **16** (1968), 370–373.

[6] The Prime Glossary, http://primes.utm.edu/glossary

[7] F. Smith, Divisibility Rules for the First Fifteen Primes, *Arithmetic Teacher* **18** (1971), 85–87.

James T. Bruening
Department of Mathematics
Southeast Missouri State University
One University Plaza
Cape Girardeau, MO 63701
USA
jbruening@semo.edu

Deanna Kindhart
Department of Mathematics
Illinois Central College
One College Drive
East Peoria, IL 61635
USA
dkindhart@icc.edu