Summary: Applications of Congruences

The main goals of this chapter are to become more comfortable working with modular arithmetic, and to study some concrete applications of congruences.

Theorem 4.1 (RQ1) *The check digit in an ISBN will always change if (a) one digit of the number is changed, or (b) two digits (if they are different) of the number are interchanged.*

Proof. Recall that if $a_1, \ldots, a_9$ are the digits of an ISBN, then the check digit is determined by computing

$$\sum_{i=1}^{9} ia_i \pmod{11}.$$

We begin with part (a). Suppose that for some j satisfying $1 \leq j \leq 9$, we change a_j to b, where $a_j \neq b$. In order for the check digit to remained unchanged, the old and new check sums must be equal mod 11. Since the only difference between the two check sums occurs at the jth term, this means that

$$ja_j \equiv jb \pmod{11}.$$

Therefore it follows that $11 \mid j(a_j - b)$, and since 11 is prime, this means that either $11 \mid j$ or $11 \mid (a_j - b)$. Because $1 \leq j \leq 9$, it's clear that $11 \nmid j$. Thus it must be that $11 \mid (a_j - b)$, that is, that $a_j \equiv b \pmod{11}$. However, since $0 \leq a_j \leq 9$ and $0 \leq b \leq 9$, both a_j and b are possible remainders when dividing by 11. Since two remainders are congruent if and only if they are equal, we have that $a_j = b$ which contradicts our assumption that $a_j \neq b$.

The proof of assertion (b) is similar in spirit to that of assertion (a). Suppose that the digits a_j and a_k are interchanged, where $j \neq k$ and $a_j \neq a_k$. (Of course, if $a_j = a_k$, then the ISBN won't change.) In order for the check sum to remain the same, we must have

$$ja_j + ka_k \equiv ja_k + ka_j \pmod{11}.$$

Equivalently, 11 divides

$$(ja_j + ka_k) - (ja_k + ka_j) = (j - k)(a_j - a_k).$$

So, we see that either $11 \mid (j - k)$ or $11 \mid (a_j - a_k)$ because 11 is prime. As before, the only way that this can happen is if $j = k$ or $a_j = a_k$, both of which are contradictions to earlier assumptions. □

We now turn our attention to the "rock game", introduced in the lab. Recall that two players (we are counting the computer as a player) take turns removing rocks from a pile. Each player may remove 1, 2, or 3 rocks during a turn. The player who removes the last rock wins the game. In the lab, the computer always goes first.

Theorem 4.2 (RQ2(a)) *Suppose that n is the number of rocks in the pile when the game begins. If $n \not\equiv 0 \pmod 4$, then the computer always wins. If $n \equiv 0 \pmod 4$, then it is possible to beat the computer.*

Proof. First, we describe a winning strategy:

Pick enough rocks so that the number left is a multiple of 4.

If you leave a multiple of 4 rocks, then your opponent will take 1, 2, or 3 rocks making the number in the pile congruent to 3, 2, or 1 modulo 4 respectively. In particular, the number of rocks your opponent will leave you cannot be a multiple of 4. When it is your turn again, it will be possible to leave a multiple of 4 again so you can repeat the strategy. The number of rocks goes down and you never lose (since your opponent cannot leave 0 rocks, that would be a multiple of 4), so ultimately you win!

Now it is clear that when $n \not\equiv 0 \pmod 4$ the computer will win (since the computer goes first and follows this strategy), and when $n \equiv 0 \pmod 4$ you can always win. □

Theorem 4.3 (RQ2(b)) *Suppose that we adopt the modified rules for the game, and that n is the number of rocks in the pile when the game begins. If $n \not\equiv 0 \pmod 7$, then the computer always wins. If $n \equiv 0 \pmod 7$, then it is possible to beat the computer.*

Proof. The proof of this theorem is similar to the proof given above. The details are left to the reader. □

Theorem 4.4 (RQ3) *An integer n is divisible by 9 if and only if the sum of the digits of n is divisible by 9.*

Proof. The key observation that we shall use is the following: since $10 \equiv 1 \pmod 9$, it follows that

$$10^j \equiv 1^j \equiv 1 \pmod 9$$

for all $j \geq 0$. Now suppose that $n = d_k d_{k-1} \ldots d_1 d_0$, where $d_0, d_1, \ldots, d_k$ are the digits of n. Then we have

$$\begin{aligned} n &= d_k 10^k + d_{k-1} 10^{k-1} + \cdots + d_1 10 + d_0 \\ &\equiv d_k + d_{k-1} + \cdots + d_1 + d_0 \pmod 9. \end{aligned}$$

Therefore we see that n is congruent to the sum of its digits modulo 9, and so n is divisible by 9 if and only if the sum of the digits of n is divisible by 9. □

Theorem 4.5 (RQ4) *Suppose that $n = d_k d_{k-1} \ldots d_1 d_0$, where $d_0, d_1, \ldots, d_k$ are the digits of n. Then n is divisible by 37 if and only if the sum*

$$d_0 + 10d_1 + 26d_2 + d_3 + 10d_4 + 26d_5 + \cdots \tag{4.1}$$

is also divisible by 37.

Proof. The nature of this proof is similar to that of the preceding proof, although the details are a bit more complicated. First, we note that

$$\begin{aligned} 1 &\equiv 1 && \pmod{37} \\ 10 &\equiv 10 && \pmod{37} \\ 10^2 &\equiv 26 && \pmod{37} \\ 10^3 &\equiv 1 && \pmod{37} \\ 10^4 &\equiv 10 && \pmod{37} \\ 10^5 &\equiv 26 && \pmod{37} \\ &\vdots \end{aligned}$$

Therefore we see that

$$\begin{aligned} n &= d_0 + d_1 10 + d_2 10^2 + d_3 10^3 + d_4 10^4 + d_5 10^5 + \cdots \\ &\equiv d_0 + 10d_1 + 26d_2 + d_3 + 10d_4 + 26d_5 + \cdots \pmod{37}, \end{aligned}$$

and so it follows that n is divisible by 37 if and only if the sum given in (4.1) is divisible by 37. □

Theorem 4.6 (RQ5) *Suppose that $n = d_k d_{k-1} \ldots d_1 d_0$, where $d_0, d_1, \ldots, d_k$ are the digits of n. Then n is divisible by 7 if and only if the sum*

$$d_0 + 3d_1 + 2d_2 + 6d_3 + 4d_4 + 5d_5 + d_6 + 3d_7 + \cdots \tag{4.2}$$

is also divisible by 7.

Proof. We begin by noting that

$$\begin{aligned} 1 &\equiv 1 \pmod{7} \\ 10 &\equiv 3 \pmod{7} \\ 10^2 &\equiv 2 \pmod{7} \\ 10^3 &\equiv 6 \pmod{7} \\ 10^4 &\equiv 4 \pmod{7} \\ 10^5 &\equiv 5 \pmod{7} \\ 10^6 &\equiv 1 \pmod{7} \\ 10^7 &\equiv 3 \pmod{7} \\ &\vdots \end{aligned}$$

Therefore we have

$$\begin{aligned} n &= d_0 + d_1 10 + d_2 10^2 + d_3 10^3 + d_4 10^4 + d_5 10^5 + d_6 10^6 + d_7 10^7 + \cdots \\ &\equiv d_0 + 3d_1 + 2d_2 + 6d_3 + 4d_4 + 5d_5 + d_6 + 3d_7 + \cdots \pmod 7, \end{aligned}$$

and thus it follows that n is divisible by 7 if and only if the sum given in (4.2) is divisible by 7. □

Solutions to Selected Exercises

Exercise 4.2 Prove that the sequence $10^j \,\%\, p$ $(j = 0, 1, 2, \ldots)$ is purely periodic for any prime $p \neq 2$ or 5.

Rather than provide a proof here, the reader is referred to Proposition 4.8 below which gives a more general result.

In producing a divisibility test for an integer m, the key observation is that when we test an integer n with decimal digits $d_0, \ldots, d_k$ (as above), we write n in expanded form

$$n = d_0 10^0 + d_1 10^1 + d_2 10^2 + \cdots + d_k 10^k$$

and then replace the powers of 10 with integers to which they are congruent modulo m. We could take any integers $a_j \equiv 10^j \pmod m$ and have that

$$n \equiv d_0 a_0 + d_1 a_1 + d_2 a_2 + \cdots + d_k a_k \pmod m.$$

The result is then always congruent to n modulo m.

In the tests described earlier, we replaced the powers 10^j with their remainders modulo m. This is the output of the function `divtestmultipliers` in the lab, and so we will refer to the choice $a_j = 10^j \,\%\, m$ as the *standard multipliers* for the divisibility test for m.

We now apply this idea in exercise 3.

Exercise 4.3 The standard divisibility test for 11 uses multipliers 1 and -1 instead of 1 and 10. In other words, the test applied to 64368 would say that

$$\begin{aligned} 64368 &\equiv 8 \cdot 1 + 6 \cdot (-1) + 3 \cdot 1 + 4 \cdot (-1) + 6 \cdot 1 \pmod{11} \\ &\equiv 7 \pmod{11}, \end{aligned}$$

which gets to the answer much more quickly. Explain why the two versions of the divisibility test for 11 are both valid.

Solution. On the basis of the remarks above, we see that any choice of multipliers $a_i \equiv 10^i \pmod{11}$ would be valid. The two tests for divisibility by 11 given here differ only when i is odd. In that case, $10^i \equiv 10 \equiv -1 \pmod{11}$, so both tests work. □

Note, the same approach could be applied to other tests, such as the test for 7.

Alternative divisibility test for 7: *Suppose that* $n = d_k d_{k-1} \ldots d_1 d_0$*, where* $d_0, d_1, \ldots, d_k$ *are the digits of* n*. Then* n *is divisible by* 7 *if and only if the sum*

$$d_0 + 3d_1 + 2d_2 - d_3 - 3d_4 - 2d_5 + d_6 + 3d_7 + \cdots$$

is also divisible by 7*.*

Exercise 4.4 Justify the standard tests for divisibility by $n = 2,\ 5$, and 10. In each of these three cases, the standard test states that a number is congruent to its units digit modulo n.

Solution. First, we could note that if d_0 is the units digit of an integer a, then $a = d_0 + 10k$ for some integer k. For $n = 2$, 5, or 10, this implies that $a \equiv d_0 \pmod{n}$, and so the tests work.

Alternatively, we could apply our standard procedure for manufacturing divisibility tests and compute $10^j \,\%\, n$ for these three values of n. In each case, $10 \equiv 0 \pmod{n}$, and so $10^j \equiv 0^j \equiv 0 \pmod{n}$ for $j \geq 1$. The only multiplier which is nonzero is $a_0 \equiv 10^0 \equiv 1 \pmod{n}$. Thus, the test with the standard multipliers in these cases yields the desired result: the integer a is congruent to its units digit, d_0, modulo n. □

Exercise 4.6 How many different shift ciphers are possible with a 95-letter alphabet? How many different shift ciphers are possible with an n-letter alphabet?

Solution. A shift cipher with a n-letter alphabet is computed by the transformation

$$C \equiv P + k \pmod{n}$$

where P is a letter in the original message, and C is the corresponding encoded letter. There is one shift cipher for each candidate for k. If we are working mod n, there are n possible values for k, and each value of k gives a different shift cipher. So, there are n shift ciphers for a n-letter alphabet (and 95 shift ciphers for a 95-letter alphabet).

One could argue that the shift cipher with $k = 0$ does not count since it leaves the original message unchanged. In that case, one would conclude that there are $n - 1$ shift ciphers for an n-letter alphabet.

Both answers, that there are n different shift ciphers or that there are $n - 1$ shift ciphers, are acceptable if properly explained. □

Exercise 4.7 Text which was encoded with a shift cipher with key 9 was given. You were asked to do the following.

(a) Decode the message.

(b) The author of this message was trying to predict what important mathematical breakthroughs may occur in the near future. Explain why the statement is nonsensical.

Solution. The decoded message says: "The obvious mathematical breakthrough would be development of an easy way to factor large prime numbers. Bill Gates." The reason it does not make sense is that, by definition, prime numbers only have trivial factorizations; the only positive divisors of a prime number p are 1 and p, no matter how large p is. What Mr. Gates meant to refer to was the problem of factoring large numbers as a product of primes, and that this problem is especially hard when the prime factors are all large. This question is particularly important for cracking modern cryptographic schemes, such as the public key encryption schemes RSA and PGP.[1] We will study RSA in a later chapter. □

Going Farther: More Analysis of Divisibility Tests

Having looked at the process of deducing divisibility tests for different integers m, we are now in a position to analyze the process more thoroughly. First, we will prove some general properties of the multipliers for the standard divisibility test for an integer m. Then, we will be able to apply this information to determine all integers m which have simple divisibility tests.

We begin by establishing that the standard mulitpliers in a divisibility test always repeat for *any* value of m. Let's first look at the standard multipliers for $m = 6$:

$$10^0 \equiv 1,\ 10^1 \equiv 4,\ 10^2 \equiv 4,\ 10^3 \equiv 4,\ \ldots \pmod 6$$

Here, the multiplier 4 is repeated but the repetition does not begin with 10^0. Thus in this case, the standard multipliers are not purely periodic, but instead are only ultimately periodic. So, the most general result we can prove is the following:

Proposition 4.7 *For a positive integer m, the standard multipliers for testing divisibility by m form an ultimately periodic sequence.*

[1] PGP uses RSA.

Proof. The standard multipliers are remainders modulo m. Therefore, there are only m possible values for these multipliers to take. We are looking at infinitely many powers of 10, so at some point we must have[2] 10^i and 10^j having the same remainder modulo m, with $i < j$. Once we have a single repetition, part of the sequence of multipliers must be repeated from there on. For instance if $10^i \equiv 10^j$, then

$$10^{j+a} \equiv 10^j \cdot 10^a \equiv 10^i \cdot 10^a \equiv 10^{i+a} \pmod{m}.$$

In other words, letting $b = i + a$ and $P = j - i$, $10^b \equiv 10^{b+P} \pmod{m}$ for $b \geq i$. Thus, the sequence of standard multipliers is ultimately periodic. □

In most of the divisibility tests we have considered, the standard multipliers have been purely periodic. The next proposition gives the exact condition which must be satisfied to guarantee that the standard multipliers will be purely periodic.

Proposition 4.8 *The standard multipliers for the divisibility test for m are purely periodic if and only if* $\gcd(m, 10) = 1$.

Proof. We first will prove that $\gcd(m, 10) = 1$ implies that the sequence of standard multipliers are purely periodic. We already know that the standard multipliers are ultimately periodic. In particular, there will exist positive integers i and j with $i < j$ such that $10^i \equiv 10^j \pmod{m}$. Therefore m divides $10^j - 10^i = 10^i(10^{j-i} - 1)$. Since $\gcd(m, 10) = 1$, it is clear that $\gcd(m, 10^i) = 1$, and therefore $m \mid (10^{j-i} - 1)$ by exercise 6 of Chapter 1. So, $10^{j-i} \equiv 1 \pmod{m}$.

Now, we have produced an integer $P = j - i > 0$ so that $10^P \equiv 10^0 \pmod{m}$. As above, we now multiply both sides of the congruence by 10^k to get $10^{k+P} \equiv 10^k \pmod{m}$. Since these powers have the same remainders modulo m, we have that $a_{i+P} = a_i$ for all $i \geq 0$.

The other direction of the proof is left as a homework exercise. □

Note that our proof provides a little extra information about how the multipliers repeat. Namely, any repetition $10^i \equiv 10^j$ $(i < j)$ implies that $j - i$ is a period.

We now restrict the discussion to integers m which are relatively prime to 10. By Proposition 4.8, the multipliers for the test of divisibility by m are purely periodic, which will simplify a few of the details.

We have seen that some divisibility tests are easy to use, and some are not so easy to use. For example, the tests for divisibility by 3 and by 9 are especially easy since one just has to add up the digits of the number. In the test for divisibility by 11, one alternates multiplying the digits by +1 and by −1 before adding them up. The divisibility test for 37 is a little more complicated because there are three different multipliers (1, 10, and 26). On the other hand, the test for 7 is pretty horrendous

[2] This is an application of the Pigeonhole Principle: "If you put r pigeons in s holes with $r > s$, then some pigeonhole must hold more than one pigeon".

with 6 different multipliers.[3] In fact, the test for 7 is so unwieldy that many people believe that there is no such thing as a divisibility test for 7.

The number of multipliers for a divisibility test is an indication of how easy it will be to use. Before continuing, we pause to make the following definition.

Definition Let $\gcd(m, 10) = 1$. The *length* of the test for divisibility by m is the number of distinct multipliers in the divisibility test.

As we remarked above, any repetition in the sequence of standard multipliers is a period for the sequence. So, the length of a divisibility test is the same as the minimal period of its sequence of standard multipliers. Thus, for example, the length of the test for divisibility by 37 is 3, and the length of the test for divisibility by 7 is 6.

Proposition 4.9 *Let m be a positive integer relatively prime to 10. Then, the length of the test for divisibility by m is at most $m - 1$.*

Proof. The multipliers for the divisibility test for m are the remainders of 10^i when divided by m. In general, there are m possible remainders when dividing by m. However, since m and 10 are relatively prime, we cannot have $10^i \equiv 0 \pmod{m}$. Hence, there are at most $m - 1$ possible values for the remainder of 10^i when divided by m. □

We now restrict to prime numbers $p \neq 2, 5$, and analyze the length of the test for divisibilty by p. Below is a table of lengths of the divisibility test for the first few primes $p \neq 2, 5$:

p	3	7	11	13	17	19	23	29	31	37	41	43	47	53	59
Length	1	6	2	6	16	18	22	28	15	3	5	21	46	13	58

Length of the divisibility test for small primes p

Notice that the divisibility test for approximately half of the primes shown require the maximum number of multipliers (the maximum is $p - 1$ according to Proposition 4.9). If we continued the table, would we find more primes with very short divisibility tests? The next proposition allows us to analyze the problem from another direction.

Proposition 4.10 *Let p be a prime number different from 2 and 5. Then the length of test for divisibility by p is the smallest positive integer j such that $10^j \equiv 1 \pmod{p}$.*

The proof only requires us to bring together various statements made above.

[3] While this may be difficult for a human to remember and use, it would make the basis for a computer algorithm which was testing large numbers for divisibility by 7, if we store the numbers as an array of their digits in base 10. In practice, almost all computers store integers using a power of 2 as the base. In that case, we would need a corresponding test in that base. Divisibility tests for bases other than base 10 are discussed in the homework exercises.

Proof. Since p is a prime distinct from 2 and 5, it is relatively prime to 10. Thus, the sequence of standard multipliers for a divisibility test for p is purely periodic, and the minimal period for this sequence is the length of the divisibility test for p. Moreover, since any repetition in the sequence of standard multipliers gives a period, the length of the divisibility test will be given by the first repetition, that is, the smallest integer j such that $10^j \equiv 10^0 \pmod{p}$.

□

Suppose we wanted to look for other primes with a short divisibility tests. If p has a divisibility test of length j, then $10^j \equiv 1 \pmod{p}$, which implies $p \mid (10^j - 1)$. We list the factorizations of $10^j - 1$ for small values of j:

$$\begin{aligned} 10^1 - 1 &= 3^3 \\ 10^2 - 1 &= 3^2 \cdot 11 \\ 10^3 - 1 &= 3^3 \cdot 37 \end{aligned}$$

The first line containing a prime p gives the length of its divisibility test. So, 3 is the only prime with a test of length 1, 11 is the only prime with a test of length 2, and 37 is the only prime with a test of length 3. In particular, this chapter already contained all of the divisibility tests of length ≤ 3 (for primes p).