Problems on Discrete Mathematics[1]

Chung-Chih Li[2]
Kishan Mehrotra[3]

LaTeX at January 11, 2007

[2]Illinois State University, Normal, Illinois. cli2@ilstu.edu
[3]Syracuse University, Syracuse, New York. kishan@ecs.syr.edu

Part II

Specific Topics

Chapter 6

Integers

— Preliminary Background for Number Theoretics & Cryptography

The integers were created by God;
all else is the work of man.

– Ludwig Kronecker

It is quite true to say that the concept of integers is the very first mathematical concept grasped by everyone. We can count almost right after we can barely speak at the age of three or four. Within a few years, through education, everyone will learn to have a fair skill of doing basic operations on integers such as addition, substraction, multiplication, and division. It may be fair to say that the four basic arithmetic operations we just mentioned are more than enough for our daily life. However, number theory – the study of integers – had been developed far beyond daily applications. In fact, numerous civilizations had independently conceived some mechanical procedures (algorithms) for solving problems related to integers from earliest times. Most of the antiquities were discovered by amateur mathematicians called numerologists either for fun or for spiritual purposes. Recently, with the development of modern computers, number theory turns out to be an indispensable tool in many important applications such as coding theory and cryptography. Since the theory has been well developed into an independent and deep branch in mathematics on its own right, it is worthwhile for us to study the subject once again and carefully analyze the mathematical properties behind this seeming elementary school topic. We will find that integers are not as naive as they look like.

6.1 Floor and Ceiling Functions

Let $\mathbf{R}$ denote the set of all real numbers, $\mathbf{Z}$ the set of all integers, and $\mathbf{N}$ the set of all natural numbers. By convention, $0 \notin \mathbf{N}$. In number theory, we study integers only. We use the following two functions to trim any number into an integer.

Definition 6.1: Floor function $\lfloor\ \rfloor$ and Ceiling function $\lceil\ \rceil$

Let $t \in \mathbf{R}$.

- $\lfloor t \rfloor$ is the largest integer a such that $a \leq t$.
- $\lceil t \rceil$ is the smallest integer a such that $t \leq a$.

Here are some examples:

$$\lfloor 1.1 \rfloor = 1, \quad \lfloor -2.1 \rfloor = \lfloor -2.3 \rfloor = -3, \quad \lfloor \pi \rfloor = 3,$$
$$\lceil 1.1 \rceil = 2, \quad \lceil -2.1 \rceil = \lceil -2.3 \rceil = -2, \quad \lceil \pi \rceil = 4.$$

We can easily check their correctness according to the definitions above. It is also easy to see that neither the floor nor the ceiling function is injective. We observe that, for an arbitrary $x \in \mathbf{R}$. $\lfloor x \rfloor$ may not be the nearest integer to t. How about $\lfloor x + \frac{1}{2} \rfloor$? Consider the following theorem.

Theorem 6.1 For any number x, if $(x+\frac{1}{2}) \notin \mathbf{Z}$, then $\lfloor x+\frac{1}{2} \rfloor$ is the unique nearest integer to x.

Proof: Suppose $x+\frac{1}{2} \notin \mathbf{Z}$. Let $x = k+s$, where $k \in \mathbf{Z}$ and $0 < s < 1$. Since $x+\frac{1}{2} \notin \mathbf{Z}$, it follows that $s \neq \frac{1}{2}$. We observe that 1.) if $0 < s < \frac{1}{2}$ then the integer nearest to x is k;, and 2.) if $\frac{1}{2} < s < 1$ then the integer nearest to x is $k+1$. Thus, it is sufficient to prove that

1. if $0 < s < \frac{1}{2}$, then $\lfloor x+\frac{1}{2} \rfloor = k$, and
2. if $\frac{1}{2} < s < 1$, then $\lfloor x+\frac{1}{2} \rfloor = k+1$.

case 1:

$$\begin{array}{rcl} 0 < s < \frac{1}{2} & \Rightarrow & \frac{1}{2} < s+\frac{1}{2} < 1 \\ & \Rightarrow & k+\frac{1}{2} < k+s+\frac{1}{2} < k+1 \\ & \Rightarrow & k+\frac{1}{2} < x+\frac{1}{2} < k+1 \\ & \Rightarrow & k < x+\frac{1}{2} < k+1 \\ & \Rightarrow & \lfloor x+\frac{1}{2} \rfloor = k. \end{array}$$

case 2:

$$\begin{array}{rcl} \frac{1}{2} < s < 1 & \Rightarrow & 1 < s+\frac{1}{2} < 1+\frac{1}{2} \\ & \Rightarrow & k+1 < k+s+\frac{1}{2} < k+1+\frac{1}{2} \\ & \Rightarrow & k+1 < x+\frac{1}{2} < k+1+\frac{1}{2} \\ & \Rightarrow & \lfloor x+\frac{1}{2} \rfloor = k+1. \end{array}$$

□

The result of the above theorem is not particularly important, but its proof provides another chance to be familiar with mathematical arguments of this kind.

Definition 6.2: For $a \in \mathbf{R}$, the absolute value, denoted by $|a|$, of a is defined as follows.

$$|a| = \begin{cases} a & \text{if } a \geq 0; \\ -a & \text{if } a < 0. \end{cases}$$

6.2 Divisibility

Among the four arithmetic operation, division is the most interesting one. We will have a close look at integer division in this section.

Definition 6.3: For $a, b \in \mathbf{Z}$ we say a divides b iff there exists an integer k such that $ak = b$. We use $a|b$ to denote that a divides b.

Definition 6.4: $p \in \mathbf{N}$ is said to be prime if and only if $p \geq 2$ and p has no positive divisors except 1 and p itself.

Definition 6.5: Let $a, b \in \mathbf{N}$. We say that a and b are relatively prime to each other if and only if there is no integer other than 1 that divides both a and b.

Note that 1 is a natural number without positive divisors except 1 and itself, but we do not consider 1 as a prime number by convention due to the fact that otherwise many interested theorems will become trivial.

Theorem 6.2 Every integer can be presented as a product of primes. Moreover, for every $n \in \mathbf{Z}$ with $n > 1$, z can be uniquely factorized as

$$n = p_1 p_2 \cdots p_k, \quad \text{where } p_1 \leq p_2 \leq \cdots \leq p_k.$$

Proof: We will prove the moreover-part of the theorem by mathematical induction. When $n = 2$, it is self-evident. Suppose when $n \geq 2$ the statement is true. Consider $n + 1$. If $n + 1$ is a prime, then the statement is automatically true for $n+1$. Suppose $n+1$ is not a prime. Then, there are two integers a and b such that, $2 \leq a < n$, $2 \leq b < n$, and $n = ab$. By the inductive hypothesis, we can uniquely factorize a and b as:

$$a = p_1 p_2 \cdots p_i, \text{ and } b = q_1 q_2 \cdots q_j,$$

where $p_1 \leq p_2 \leq \cdots \leq p_i$ and $q_1 \leq q_2 \leq \cdots \leq q_j$. Since $p_1 p_2 \cdots p_i$ and $q_1 q_2 \cdots q_j$ are unique, with some proper arrangement, n can be uniquely presented as

$$n = ab = r_1 r_2 \cdots r_{i+j}.$$

where $r_1 \leq r_2 \leq \cdots \leq r_{i+j}$ are prime numbers. □

Algorithms: Algorithm is a very old concept in many civilizations dating from ancient times. An algorithm is nothing more or less than a recipe for carrying out a sequence of operations to solve a problem. In mathematics, an algorithm that can correctly construct mathematical objects of required or give answers to mathematical problems is perfectly to be considered as a mathematical proof. In fact, some mathematicians known as *constructivists* or *intuitionists* maintain a doctrine that giving an effective algorithm is the only legitimate way to prove mathematical theorems. Their philosophy is straightforward: if you claim that something exists, then you have to provide an effective way to built it or find it, and an algorithm is such an *effective way.*

Let's take a look at the notion of algorithms. Here we borrow the definition from *Encyclopedia of Computer Science and Engineering*: An algorithm is "the precise characterization of a method of solving a problem". The phrase in the

definition that needs emphasis is "precise characterization." The encyclopedia further notes that any algorithm must have the following properties:

1. **Finiteness.** Application of the algorithm to a particular set of data must result in a *finite* sequence of actions.

2. **Unique Initialization.** The action that starts the algorithm must be unique.

3. **Unique Succession.** Each action in the algorithm must be followed by a unique successor action.

4. **Solution.** The algorithm must terminate with a solution to the problem, or it must indicate that for the given data the problem is insoluble by the algorithm.

Except the first property, the readers should not take properties 2, 3, and 4 too serious. Properties 2 and 3 are redundant in a sense that they do not enhance or undermine the power of algorithms. The last property requires the correctness of an algorithm for an interested problem. In fact, any algorithm does solve some problem, only may not be the one we want to solve. If the problem is given and we are asked to write an algorithm to solve it, usually, it is the last property that is most difficult to verify.

In the following we prove a theorem by giving a "correct" algorithm. We will repeatedly use the theorem in this chapter. To most of us, the theorem is so basic that can be understood intuitively. However, a formal proof is demanded. However, to formally prove the correctness of a given algorithm is a big pain on the neck and is way beyond the scope of this book. Here we simply follow the algorithm and comprehend its correctness by out intuition.

Theorem 6.3 Let $a, b \in \mathbf{Z}$ and $b \neq 0$. There exist unique integers q and r such that

$$a = qb + r, \text{ where } 0 \leq r < |b|;$$

Note that we require r to be nonnegative. Such an r is called the remainder of a divided by b.

Proof: As we mentioned earlier, an easy way to prove the theorem is to write an algorithm that takes two integers a and b, and if $b \neq 0$, the algorithm will output correct q and r.

Consider the algorithm in Figure 6.1. The algorithm will be a bit easier if we restrict the input numbers to be positive. □

To get a better idea about how this algorithm works, run the division algo-

```
Input a, b
    r ⟵ a; q ⟵ 0;
    while not 0 ≤ r < |b| do
        if a × b ≥ 0
            then r ⟵ r − b;
            else r ⟵ r + b;
        endif
        q ⟵ q + 1;
    endwhile
    if a × b ≥ 0
        then return(q, r);
        else return(−q, r);
    endif
```

Figure 6.1: The Division Algorithm

rithm on the following inputs as an exercise.

$$a = 10, b = 3;\ a = 10, b = -3;\ a = -10, b = 3;\ a = -10, b = -3.$$

Although an algorithm is considered as a formal mathematical proof, we have to face a few challenges. How can you be sure that the algorithm indeed does what it is supposed to do? Even it does, how can you be sure that all other algorithms for the same problem always give the same answer on the same input so we can claim the uniqueness of q and r? Unfortunately, it is in principle impossible to prove correctness and *uniqueness* by simply giving an algorithm. We do not intend to answer the questions and complete our proof here. Our purpose here is to get a feel for the concept that an algorithm can serve as a mathematical tool to prove theorems. Also, Theorem 6.3 itself lies as the very foundation of the entire number theory.

6.3 Greatest Common Divisor

Definition 6.6: Given two integers m and n, we use $\gcd(m, n)$ to denote the greatest common divisor of m and n, which is the *largest* positive integer that divides both m and n.

Consider the following examples. $\gcd(12, 16) = 4$, $\gcd(-315, 91) = 7$, and $\gcd(10, 0) = 10$. By convention, we take $\gcd(0, 0) = 0$. We can rewrite the definition of "relatively prime" as follows:

Definition 6.7: Integers a and b are said to be relatively prime to each other if $\gcd(a, d) = 1$.

We present some useful properties related to gcd in the following theorems. Most of the theorems are intuitively understandable and can be verified by our intuition. However, intuition was built up from experience, not from rigorous mathematical arguments. As we go deeper into the theory, intuition no longer helps. (Have a quick peek at Theorem 6.10. to see if you can be convinced by intuition.) Here we present proofs in terms of mathematical arguments that meet a certain level of rigorousness.

Theorem 6.4 Suppose $a, b \in \mathbf{N}$ with $a = da'$ and $b = db'$. $\gcd(a, b) = d$ iff a' and b' are relatively prime, i.e., $\gcd(a', b') = 1$.

Proof: Given $a, b \in \mathbf{N}$ with $a = da'$ and $b = db'$. Let $\gcd(a, b) = d$ and $\gcd(a', b') = k$. By contradiction, assume $k \neq 1$. We have $a = dka''$ and $b = dkb''$ and that dk is a common divisor of a and b. Since $a, b \in \mathbf{N}$, it follows that $k \neq 0$ and $dk > d$. This contradicts the assumption that d is the greatest common divisor of a and b.

For the other direction, assume $a = da'$ and $b = db'$ and $\gcd(a', b') = 1$. It is clear that d is a common divisor of a and b. Since $\gcd(a', b') = 1$, there is no common divisor other than 1 that can be extracted from a' and b'. Thus, it is impossible to obtain a common divisor of a and b bigger than d. Therefore, $\gcd(a, b) = d$. □

Theorem 6.5 Let $a, b, m \in \mathbf{N}$. We have

$$\gcd(ma, mb) = m \gcd(a, b).$$

Proof: Let $\gcd(a, b) = d$. By Theorem 6.4, there are a' and b' such that $a = da'$, $b = db'$, and $\gcd(a', b') = 1$. Clearly, $ma = mda'$ and $mb = mdb'$. By the other direction of Theorem 6.4, since $\gcd(a', b') = 1$, it follows that md is the greatest common divisor of ma and mb. Thus, $\gcd(ma, mb) = md = m \gcd(a, b)$. □

Theorem 6.6 For any $a, b, x, y \in \mathbf{Z}$, $xa + yb$ is divisible by $\gcd(a, b)$.

Proof: Let $\gcd(a, b) = d$. There must be two integers a' and b' such that $a = da'$ and $b = db'$. We have

$$xa + yb = xda' + ydb'; = (xa' + yb')d.$$

Since x, y, a', and b' are all integers, $xa' + yb'$ must be an integer too, say k. Therefore, $xa + yb = kd$, which is divisible by d. □

Theorem 6.7 Let $a, b \in \mathbf{N}$ with $a \geq b$. Then,

$$\gcd(a, b) = \gcd(a - b, b).$$

Proof: Let $a, b \in \mathbf{N}$ with $a \geq b$. and $\gcd(a, b) = d$. By Theorem 6.4, there are a' and b' such that $a = da'$, $b = db'$, and $\gcd(a', b') = 1$. Also, $a - b = d(a' - b')$. One can verify that if a' and b' are relatively prime, then so are $a' - b'$ and b'. Thus, $\gcd(a' - b', b')$=1. With Theorem 6.5, we have

$$\gcd(a - b, b) = \gcd(d(a' - b'), db') = d\gcd((a' - b'), b') = d = \gcd(a, b).$$

□

Definition 6.8: Given two nonzero integers a and b, we use $\text{lcm}(a, b)$ to denote the least positive common multiple of a and b, which is the *least* positive integer that can be divided by a and of b.

The following theorem connects the concepts of gcd and lcm.

Theorem 6.8 Let a and b be two natural numbers. We have

$$\text{lcm}(a, b) = \frac{ab}{\gcd(a, b)}.$$

Proof: Let $\gcd(a, b) = d$. By Theorem 6.4, we have that $a = da'$, $b = db'$, and $\gcd(a', b') = 1$. Thus,

$$\frac{ab}{\gcd(a, b)} = da'b'.$$

It is clear that $da'b'$ is a common multiple of a and b. What remains to prove is that $da'b'$ is the least one. Let m be any common positive multiple of a and b, i.e., $a|m$ and $b|m$. Since $a = da'$, by division algorithm, there is some $k \in \mathbf{N}$ such that $m = da'k$. Also, since $b|m$, we have $db'|da'k$. It follows that $b'|a'k$. Since $\gcd(a', b') = 1$, we have $b'|k$. It is clear that, if $b'|k$, then $b' \leq k$, and hence $da'b' \leq da'k = m$. Therefore, any common positive multiple of a and b must be greater than or equal to $da'b'$. □

Theorem 6.9 Let a, b be integers. If m is a multiple of both a and b, then m is also a multiple of $\text{lcm}(a, b)$.

Proof: Suppose $\gcd(a, b) = d$, and let $a = da', b = db'$. Thus, $\gcd(a', b') = 1$ and $\text{lcm}(a, b) = da'b'$. Since m is a common multiple of a and b, there exist integers k_1 and k_2 such that $m = k_1 a = k_2 b$. We have

$$m = k_1 da' = \frac{k_1}{b'} da'b' = \frac{k_1}{b'} \text{lcm}(a, b).$$

We will now prove that $\frac{k_1}{b'}$ is an integer. From the assumption we have

$$k_1 da' = k_2 db' \quad \Rightarrow \quad \frac{k_1}{b'} a' = k_2.$$

Since k_2 is an integer and $\gcd(a', b') = 1$, $\frac{k_1}{b'}$ must be an integer. □

In the following, we present a theorem that is important in a sense that it can help us simplify many proofs. The proof of the theorem itself is not trivial.

Theorem 6.10 For any $a, b \in \mathbf{Z}$, there exist integers x and y such that

$$xa + yb = \gcd(a, b).$$

Proof: It is clear that if one of a and b is a zero, we can easily assign 1 or 0 to x and y to satisfy the theorem. For simplicity, we can assume $a, b \in \mathbf{N}$ without loss of generality. Let

$$s = \min\{xa + yb > 0 \ : \ x, y \in \mathbf{Z}\}. \tag{6.1}$$

That is, s is the smallest natural number of all possible $xa + yb$ with $x, y \in \mathbf{Z}$. We argue that, for any $x, y \in \mathbf{Z}$, $s|(xa + yb)$. Let $s = ua + vb$ for some $u, v \in \mathbf{Z}$. Also, let $a = da', b = db'$ and $\gcd(a, b) = d$. Thus,

$$s = ua + vb = d(ua' + vb').$$

Fix $x, y \in \mathbf{Z}$. By the division algorithm, we have $q, r \in \mathbf{Z}$ such that,

$$xa + yb = sq + r, 0 \leq r < s.$$

It follows that

$$r = xa + yb - sq = xa + yb - uqa - vqb = (x - uq)a + (y - vq)b.$$

Thus, r is also a linear combination of a and b with integral coefficients and $r \neq s$. Together with the assumption in (6.1), we conclude that the only possible value for r is 0. Therefore, $s|(xa + yb)$ for any $x, y \in \mathbf{Z}$. Consequently, $s|a$ (when $x = 1, y = 0$) and $s|b$ (when $x = 0, y = 1$). In other words, s is a common divisor of a and b. Thus, $s \leq \gcd(a, b)$. By Theorem 6.6, $\gcd(a, b)|s$, and hence $\gcd(a, b) \leq s$. Therefore, $s = \gcd(a, b) = ua + vb$ for some $u, v \in \mathbf{Z}$. □

Theorem 6.11 Consider $a, b, q \in \mathbf{Z}$. If both a and b are divisible by q, then $\gcd(a, b)$ is divisible by q.

Proof: Suppose $a = qa'$ and $b = qb'$, where q, a' and b' are all integers. Let $\gcd(a, b) = d$. By Theorem 6.10, there exist integers x, y such that $d = xa + yb$. Thus,

$$\begin{aligned} d &= xqa' + yqb' \\ \frac{d}{q} &= xa' + yb'. \end{aligned}$$

Because x, y, a', and b' are integers, $\frac{d}{q}$ must be an integer. Therefore, $q|d$. □

Theorem 6.12 Let $a, b \in \mathbf{Z}$. There exist $x, y \in \mathbf{Z}$ such that $xa + yb = 1$ iff $\gcd(a, b) = 1$.

Proof: Suppose $xa + yb = 1$ where x and y are integers. Let $a = da', b = db'$ and $\gcd(a, b) = d$. Without loss of generality, we may assume $d \neq 0$. We have

$$xda' + ydb' = 1 \quad \Longrightarrow \quad d = \frac{1}{xa' + yb'}.$$

The only case that both d and $xa'+yb'$ are integers is that when $d = xa'+yb' = 1$. The other direction of this theorem is simply a special case of Theorem 6.10. □

The following theorem is a corollary of Theorem 6.12.

Theorem 6.13 If $a, b_1, b_2, \ldots, b_n \in \mathbf{Z}$ and $\gcd(a, b_1) = \gcd(a, b_2) = \cdots = \gcd(a, b_n) = 1$, then $\gcd(a, b_1 b_2 \ldots b_n) = 1$.

Proof: By Theorem 6.10 we find $x_1, x_2, \ldots, x_n$ and $y_1, y_2, \ldots, y_n$ such that

$$\begin{aligned} 1 &= x_1 a + y_1 b_1; \\ 1 &= x_2 a + y_2 b_2; \\ &\vdots \\ 1 &= x_n a + y_n b_n. \end{aligned}$$

Thus,

$$1^n = (x_1 a + y_1 b_1)(x_2 a + y_2 b_2) \cdots (x_n a + y_n b_n).$$

Therefore, $1 = Aa + B(b_1 b_2 \ldots b_n)$, where A is a polynomial in $a, x_1, \ldots, x_n$, $b_1, \ldots b_n$ and $y_1, \ldots, y_n$, and $B = y_1 y_2 \cdots y_n$. Since both A and B are integers, by Theorem 6.12, $\gcd(a, b_1 b_2 \ldots b_n) = 1$. □

Euclid's Algorithm Our next question is: how do we find the greatest common divisor of any two integers? This is not a particularly difficult problem; we can by brute force check 1, 2, ..., up to the smaller one of the two to see if they are common divisors and pick up the greatest one. This always works, but we also want to solve in an efficient way. The great Greek mathematician, Euclid, about 2300 years ago gave an elegant algorithm now known as Euclid's algorithm to solve this problem. The algorithm is one of the oldest algorithms. Before we introduce the algorithm, we at first make some observations. Let m and n be any two integers.

$$\gcd(m, n) = \gcd(n, m) \tag{6.2}$$

```
function gcd(m, n)
  if n = 0
      then return m;
      else return gcd(n, m − ⌊m/n⌋n);
  endif
endfunction
```

Figure 6.2: Euclid's Algorithm

$$\gcd(-m,-n) = \gcd(-m,n) = \gcd(m,-n) = \gcd(m,n). \tag{6.3}$$

Equation (6.2) implies that we can assume the first argument of our algorithm never less than the second one without loss of generality. Equation (6.3) implies that we can confine our attention to non-negative integers. Our second observation is:

$$\gcd(m,0) = m, \gcd(0,n) = n \text{ and } \gcd(0,0) = 0. \tag{6.4}$$

In other words, if one of the two integers is 0, then the other integer is the gcd. This tells us when to terminate our algorithm. Together with Theorem 6.7, we have an idea about how to proceed in our algorithm to guarantee that the algorithm will reach the terminating condition.

As we recursively call the algorithm with new arguments $m - n$ and n, we can subtract as many n's as possible from m, so long as the difference remains non-negative? To find how many times n can be subtracted from m we simply use the division algorithm.

$$m = q \times n + r,$$

where $0 \leq r \leq n-1$. Let $q = \lfloor \frac{m}{n} \rfloor$. It is clear that we can remove n from m q many times. With this background we are ready to present this easy but not trivial algorithm. Note that we have decided to use non-negative integers m and n only. The algorithm is shown in Figure 6.2.

A nonrecursive version of Euclid's algorithm is shown in Figure 6.3.

Consider the following two examples. Let $q = \lfloor \frac{m}{n} \rfloor$ and $r = m - \lfloor \frac{m}{n} \rfloor n$.

m	=	$n \times q$	+	r,
946	=	726×1	+	220,
726	=	220×3	+	66,
220	=	66×3	+	22,
66	=	22×3	+	0.

m	=	$n \times q$	+	r,
1247	=	98×12	+	71,
98	=	71×1	+	27,
71	=	27×2	+	17,
27	=	17×1	+	10,
17	=	10×1	+	7,
10	=	7×1	+	3,
7	=	3×2	+	1,
3	=	1×3	+	0.

```
function gcd (m, n)
  repeat while  n ≠ 0
    q ⟵ ⌊m/n⌋;
    r ⟵ m − q × n;
    m ⟵ n;
    n ⟵ r;
  endrepeat
  return m;
endfunction
```

Figure 6.3: Nonrecursive Euclid's Algorithm

Therefore, $\gcd(946, 726) = 22$ and $\gcd(1247, 98) = 1$. □

Extended Euclid's Algorithm: Recall Theorem 6.10 stating that for any integers a and b, there are integers x and y, such that $xa+yb = \gcd(a, b)$. As we mentioned earlier, it is an important theorem in a sense that it simplifies many proofs for interested theorems. Moreover, the values of x and y are needed for solving *linear congruence equations*, which will be introduced in the next section. The proof given for Theorem 6.10 is logically perfect, but it says nothing about how to actually find out the values of x and y. (They do exist, alright!) A proof of that kind is called *"nonconstructive"*. Clearly, a correct algorithm to find x and y indeed is a legitimate proof for the existence claim stated in Theorem 6.10. We call this kind of proofs *"constructive"*, where an effective procedure to construct the claimed objects is provided. In the following we give an algorithm to actually find out the values of x and y in Theorem 6.10.

Since the idea to find values for x and y in Theorem 6.10 is in fact involved in the Euclid's algorithm and we only make some modifications, the algorithm is called *Extended Euclid's Algorithm*. Again, we make some observations first, which will help us present our arguments. (i) It is obvious that if $n = 0$, then $x = 1, y = 0$. This gives the terminating condition. (ii) if $n \neq 0$, we set $n_1 = m - \lfloor \frac{m}{n} \rfloor n, m_1 = n$ and apply the method recursively. That is, we compute x_1, y_1 such that

$$x_1 m_1 + y_1 n_1 = \gcd(m_1, n_1) = \gcd(m, n).$$

To make this presentation easier to follow, we rewrite $m = m_0$, $n = n_0$, $x = x_0$, and $y = y_0$. Suppose that we have obtained x_1 and y_1 such that

$$x_1 m_1 + y_1 n_1 = \gcd(m_1, n_1) = \gcd(m_0, n_0).$$

```
function egcd(m, n)
  if n = 0
      then return (1, 0);
      else (x, y) ⟵ egcd(n, m − ⌊m/n⌋n);
  endif
  return (y, x − ⌊m/n⌋y);
endfunction
```

Figure 6.4: Extended Euclid's Algorithm

```
function egcd(m, x0, y0; n, x1, y1)
  if n = 0
      then return (x0, y0);
  endif
  r ⟵ m − ⌊m/n⌋n;
  x2 ⟵ x1 − ⌊m/n⌋x1;
  y2 ⟵ y1 − ⌊m/n⌋y1;
  return egcd(n, x1, y1; r, x2, y2);
endfunction
```

Figure 6.5: Extended Euclid's Algorithm (V.2)

Substituting for m_1 and n_1 in terms of m_0 and n_0, we get

$$\begin{aligned} \gcd(m_0, n_0) &= x_1 n_0 + y_1(m_0 - \lfloor \frac{m_0}{n_0} \rfloor n_0) \\ &= y_1 m_0 + (x_1 - \lfloor \frac{m_0}{n_0} \rfloor y_1) n_0 \end{aligned}$$

Thus, $x_0 = y_1$ and $y_0 = x_1 - \lfloor \frac{m_0}{n_0} \rfloor y_1$. In general, the following result is obtained:

$$\begin{aligned} x_{i-1} &= y_i, \\ y_{i-1} &= x_i - \lfloor \tfrac{m_{i-1}}{n_{i-1}} \rfloor y_i. \end{aligned}$$

In the last step we have $x_n = 1$ and $y_n = 0$. We can find (x_{i-1}, y_{i-1}) from (x_i, y_i). Then, find (x_{i-2}, y_{i-2}) from (x_{i-1}, y_{i-1}), and so on, until we obtain the desired values of x_0 and y_0. We build these step into the algorithm shown in Figure 6.4. We can also build these steps into a forward version as shown in Figure 6.5. Given any nonnegative integers m and n, the function will be called by egcd$(m, 1, 0; n, 0, 1)$. □

The algorithm in Figure 6.5 is easier for us to work with paper and pencil. Consider 246 and 165. To find x and y such that, $\gcd(242, 165) = 242x + 165y$,

we have

m/n	x_0/x_1	y_0/y_1	r
242	1	0	
165	0	1	1
77	1	-1	2
11	-2	3	7
0			

The result shows that $x = -2$ and $y = 3$.

6.4 Congruence

Congruence is a term used in number theory to express statements about divisibility. As we have seen earlier, a division gives two numbers, a quotient and a remainder. In number theory, we are interested in remainders. What left when an integer divided by a concerned divisor turns out to be an important property in many applications. Here is the easiest example: odd numbers and even numbers, where we fix the divisor to 2. Numbers are separated into two categories. In each category, all numbers share the same property that they leave the same remainder when divided by 2. Clearly, if we change the divisor to a bigger number, we then can separate numbers into more categories according to their remainders left by the division. For convenience, we define the following notations.

Definition 6.9: Let a and m be two integers with $m \neq 0$. The remainder of a divided by m is denoted by $(a \mod m)$.

Definition 6.10: Let $a, b, m \in \mathbf{Z}$ with $m \neq 0$. If $(a \mod m) = (b \mod m)$, we say that m is a *modulus* of a and b.

Note that, although the division algorithm is not limited to positive divisors, we generally confine our attention to positive moduli (plural of modulus). Thus, when m serves as a modulus, we simply let $m \in \mathbf{N}$ for the time beings. Recall that $0 \notin \mathbf{N}$ under our conventions. Thus, for any $m \in \mathbf{N}$, $(a \mod m)$ is well-defined.

Definition 6.11: Let $a, b \in \mathbf{Z}$ and $m \in \mathbf{N}$. We say that a is congruent to b modulo m iff $(a \mod m) = (b \mod m)$. We denote this by

$$a \equiv b \pmod{m}.$$

Alternatively, we also use $a \equiv_m b$ as a standard notation for $a \equiv b \pmod{m}$. Since $\equiv_m$ is symmetric (i.e., if $a \equiv_m b$, then $b \equiv_m a$), we can simply say that a

and b are congruent modulo m. It is also easy to verify that $\equiv_m$ is reflexive and transitive. Therefore, $\equiv_m$ is an equivalent relation over integers. Consequently, $\equiv_m$ induces an equivalent class over $\mathbf{Z}$.

Definition 6.12: Let $a \in \mathbf{Z}$ and $m \in \mathbf{N}$. $\underline{\lfloor a \rfloor}_m \subseteq \mathbf{Z}$ is defined by

$$\underline{\lfloor a \rfloor}_m = \{x : x \in \mathbf{Z} \text{ and } x \equiv a \pmod{m}\}.$$

$\underline{\lfloor a \rfloor}_m$ is called the *congruence class* (or *residue class*) of a modulo m.

In other words, $\underline{\lfloor a \rfloor}_m$ is the set of integers that leave the same remainder when divided by m. Clearly, for any $m \in \mathbf{N}$ as a divisor, there are m many possible remainders, which are $0, 1, \ldots,$ and $m-1$. We generalize this fact into the following theorem.

Theorem 6.14 For any $m \in \mathbf{N}$, there are exactly m distinct residue classes.

Proof: The theorem above follows directly from the result of the division algorithm that r, as the remainder, has $0 \leq r < m$. Thus,

$$\underline{\lfloor 0 \rfloor}_m, \underline{\lfloor 1 \rfloor}_m, \ldots, \underline{\lfloor m-1 \rfloor}_m \tag{6.5}$$

are m distinct residue classes. For any $x \in \mathbf{Z}$, by the division algorithm, the remainder is unique, and hence $\underline{\lfloor x \rfloor}_m$ must be one of the residue classes we just listed in (6.5). □

Definition 6.13: Let $m \in \mathbf{N}$. We say that $\{a_0, a_1, \ldots, a_{m-1}\}$ is a complete system of residues modulo m if

$$\underline{\lfloor a_0 \rfloor}_m \cup \underline{\lfloor a_1 \rfloor}_m \cup \cdots \cup \underline{\lfloor a_{m-1} \rfloor}_m = \mathbf{Z}.$$

Recall the definition of *partition* from Chapter 4. If $\{a_0, a_1, \ldots, a_{m-1}\}$ is a complete system of residues mod m, one can verify that

$$\left\{\underline{\lfloor a_0 \rfloor}_m, \underline{\lfloor a_1 \rfloor}_m, \ldots, \underline{\lfloor a_{m-1} \rfloor}_m\right\}$$

forms a partition of $\mathbf{Z}$.

Theorem 6.15 Let $a, b \in \mathbf{Z}$ and $m \in \mathbf{N}$. We have,

$$a \equiv b \pmod{m} \iff m|(a-b).$$

Proof: By definition, if $a \equiv b \pmod{m}$, then $a = xm + r$ and $b = ym + r$ for some integers x, y, and r with $0 \leq r < m$. Since $a - b = (x-y)m$, it follows

that $m|(a-b)$. For the other direction, suppose $(a-b) = km$ for some integer k. By the division algorithm, there are unique integers q and r with $0 \leq r < m$ such that, $b = qm + r$. Therefore, $a = km + b = (k+q)m + r$. By definition, $a \equiv b \pmod{m}$. □

Theorem 6.16 Let $a, b \in \mathbf{Z}$ and $m \in \mathbf{N}$. We have,

$$a \equiv b \pmod{m} \iff \forall k \in \mathbf{Z}[a \equiv b + km \pmod{m}].$$

Proof: It is clear that if $a - b$ is a multiple of m, then for any integer k, $a - (b + km)$ is also a multiple of m. We directly use Theorem 6.15 to obtain this theorem. □

Theorem 6.17 Let $a, b \in \mathbf{Z}$ and $m \in \mathbf{N}$. Suppose $a \equiv b \pmod{m}$ and $d \in \mathbf{N}$ is a common divisor of a, b, and m. We have

$$\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}.$$

Proof: By the division algorithm and the assumption, there are $p, q, r \in \mathbf{Z}$ with $0 \leq r < m$ such that, $a = pm + r$ and $b = qm + r$. Again, by the division algorithm, $r = sd + t$ for some integers s and t with $0 \leq t < d$.

$$\frac{a}{d} = p \times \frac{m}{d} + \frac{r}{d}; \quad \frac{b}{d} = q \times \frac{m}{d} + \frac{r}{d}.$$

Since $d|a$ and $d|m$, $\frac{a}{d}$ and $\frac{m}{d}$ are integers. It follows that $\frac{r}{d}$ must be an integer. Also,

$$0 < d \text{ and } 0 \leq r < m \implies 0 \leq \frac{r}{d} < \frac{m}{d}.$$

Thus, $\frac{r}{d}$ is the remainder of $\frac{a}{d}$ divided by $\frac{m}{d}$. Likewise, $\frac{r}{d}$ is also the remainder of $\frac{b}{d}$ divided by $\frac{m}{d}$. Therefore, $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}$. □

Note that, in general, if $d \in \mathbf{N}$ is a common divisor of a and b, $a \equiv b \pmod{m}$ does not imply $\frac{a}{d} \equiv \frac{b}{d} \pmod{m}$. For example, $8 \equiv 20 \pmod{6}$. Consider $d = 4$, we obtain $2 \not\equiv 5 \pmod{6}$. In other words, giving $ac \equiv bc \pmod{m}$ *does not imply* $a \equiv b \pmod{m}$. Nevertheless, in some special case, the implication does hold (see Theorems 6.20 and 6.21.)

Except division, the other three arithmetic operations ($+$, $-$, and $\times$) in fact preserve the equivalence relation $\equiv_m$ in the following sense.

Theorem 6.18 Suppose $a \equiv b \pmod{m}$ and $x \equiv y \pmod{m}$. We have:

1. $(a + x) \equiv (b + y) \pmod{m}$.
2. $(a - x) \equiv (b - y) \pmod{m}$.
3. $(a \times x) \equiv (b \times y) \pmod{m}$.

Proof: Since the proofs for properties 1. and 2. are straightforward, we skip them. For property 3., consider the the division algorithm and let p_1, p_2, q_1, q_2, r, and r' be the integers obtained by the algorithm such that, $a = p_1 m + r$, $b = p_2 m + r$, $x = q_1 m + r'$, and $y = q_2 m + r'$. Thus,

$$a \times x = p_1 q_1 m^2 + (p_1 r' + q_1 r)m + rr';$$
$$b \times y = p_2 q_2 m^2 + (p_2 r' + q_2 r)m + rr'.$$

Therefore, $a \times x \equiv rr' \pmod{m}$ and $b \times y \equiv rr' \pmod{m}$. By transitivity, we have $(a \times x) \equiv (b \times y) \pmod{m}$. □

Proof: Here we provide another proof. By assumptions, $a - b$ and $x - y$ are both multiples of m. Consequently, so is $(a - b)(x - y)$. Consider

$$\begin{aligned}(a-b)(x-y) &= ax - ay - bx + by \\ &= ax - by - ay - bx + 2by \\ &= ax - by - y(a-b) - b(x-y).\end{aligned}$$

Thus, $ax - by = (a - b)(x - y) + y(a - b) + b(x - y)$ must be a multiple of m, and hence $ax \equiv by \pmod{m}$. □

Theorem 6.19 Suppose $a \equiv b \pmod{m}$. Then, for any integer $n \geq 0$, we have $a^n \equiv b^n \pmod{m}$.

Proof: It is clear when $n = 0$, $a^n = b^n = 1$. For $0 < n$, use the assumption that $a \equiv b \pmod{m}$ and repeatedly use the multiplication rule in Theorem 6.18 to get the result. (A formal proof requires arguments using mathematical inductions. Try it!) □

Theorem 6.20 Let $a, b, c \in \mathbf{Z}$ and $m \in \mathbf{N}$. Suppose $\gcd(c, m) = 1$. Then,

$$ac \equiv bc \pmod{m} \iff a \equiv b \pmod{m}.$$

Proof: Suppose $ac \equiv bc \pmod{m}$ and $c \neq 1$ and $m \neq 1$. By Theorem 6.15, $ac - bc = km$ for some integer k. In other words, $\frac{c(a-b)}{m}$ is an integer (i.e., k). But $\gcd(c, m) = 1$, c is not divisible by m. Thus, it must be the case that $m|(a-b)$, and hence $a \equiv b \pmod{m}$. The other direction is a trivial application of the multiplication rule in Theorem 6.18. (Hint: $c \equiv c \pmod{m}$.) □

The previous theorem can be generalized as follows.

Theorem 6.21 Let $a, b, c \in \mathbf{Z}$ and $m \in \mathbf{N}$. Suppose $\gcd(c, m) = d$. Then,

$$ac \equiv bc \pmod{m} \iff a \equiv b \pmod{\frac{m}{d}}.$$

Proof: We omit the proof which is similar to the proof for Theorem 6.20. (Compare the proofs for the next two theorems.) □

Theorem 6.22 Suppose $\gcd(m, n) = 1$. We have

$$[a \equiv b \pmod{m} \text{ and } a \equiv b \pmod{n}] \iff [a \equiv b \pmod{mn}].$$

Proof: Let $\gcd(m, n) = 1$. For one direction, suppose $a \equiv b \pmod{m}$, and $a \equiv b \pmod{n}$. Then, there are some integers p and q such that, $a - b = pm$ and $a - b = qn$. Thus, $pm = qn$ and $p = \frac{qn}{m}$. Since $\gcd(m, n) = 1$, it follows that $\frac{q}{m}$ must be an integer. Let $q = km$ for some integer k. Therefore, $a - b = qn = kmn$, and hence $a \equiv b \pmod{mn}$. For the other direction, consider $a - b = kmn = (km) \cdot n = (kn) \cdot m$. □

Theorem 6.23

$$[a \equiv b \pmod{m} \text{ and } a \equiv b \pmod{n}] \iff [a \equiv b \pmod{\text{lcm}(m, n)}].$$

Proof: Suppose $\gcd(m, n) = d$. By Theorem 6.4, we have $m = dm'$ and $n = dn'$ where $\gcd(m', n') = 1$. Also, suppose $a \equiv b \pmod{m}$, and $a \equiv b \pmod{n}$. Thus, there are some integers p and q such that, $a - b = pm = pdm'$ and $a - b = qn = qdn'$. Thus, $pm = qn$ and $p = \frac{qn'}{m'}$. Since $\gcd(m', n') = 1$, it follows that $\frac{q}{m'}$ is an integer, i.e., $q = km'$ for some integer k. Therefore, $a - b = qn = km'n = kdm'n'$, and hence $a \equiv b \pmod{dm'n'}$. By Theorem 6.8 $dm'n' = \text{lcm}(m, n)$. Therefore, $a \equiv b \pmod{\text{lcm}(m, n)}$. The other direction is straightforward. Consider $a - b = kdm'n' = kn'm = km'n$. □

Note that the argument in the proof above is unnecessarily involved; our purpose is to let the readers be familiar with the definition of linear congruence equations and some proven theorems. We can argue Theorem 6.23 like self-evident. Here is the argument: If $a - b$ is common multiple of n and m, then, by Theorem 6.9, $a - b$ is also a multiple of $\text{lcm}(m, n)$.

Definition 6.14: Let $a \in \mathbf{Z}$ and $m \in \mathbf{N}$. If $b \in \mathbf{Z}$ and $ab \equiv 1 \pmod{m}$, we say that b is a *multiplicative inverse* of a modulo m.

Theorem 6.24 Let $a \in \mathbf{Z}$ and $m \in \mathbf{N}$. If $\gcd(a, m) = 1$, then, there is a multiplicative inverse of a.

Proof: By Theorem 6.10, there exist integers x and y such that, $xa + ym = \gcd(a, m) = 1$. Thus, $m|(xa - 1)$, and hence such x is a multiplicative inverse of a. □

For convenience, we use a^- to denote the *multiplicative inverse* of a, especially when we restrict the numbers of interest to $\mathbf{Z}_m = \{0, 1, 2, \ldots, m-1\}$. It is clear that if a multiplicative does exists, we can use the extended Euclid's Algorithm to find it, and, moreover, there must be one and only one in $\mathbf{Z}_m$. It is also clear to see that, $aa^- \equiv a^-a \equiv 1 \pmod{m}$.

Theorem 6.25 Let $a, b \in \mathbf{Z}, m \in \mathbf{N}$. Suppose $ab \equiv c \pmod{m}$ and a^- exists, then $b \equiv a^-c \pmod{m}$.

Proof: Since $ab \equiv c \pmod{m}$, we have $a^-ab \equiv a^-c \pmod{m}$. By definition, $aa^- = km + 1$ for some $k \in \mathbf{Z}$. Thus, $a^-ab = kbm + b \equiv a^-c \pmod{m}$. By Theorem 6.16, $b \equiv a^-c \pmod{m}$. □

6.5 Solving Linear Congruence Equations

Consider the following equation with one variable x:

$$3x \equiv 5 \pmod{7}. \tag{6.6}$$

By trial and error, we may find $x = 4$ to be a solution to equation (6.6), for $3 \times 4 \equiv 5 \pmod{7}$. Are there any other solutions? How about equation

$$3x \equiv 5 \pmod{6}? \tag{6.7}$$

The values $0, 1, 2, 3, 4$ and 5 don't seem to work. But how far should we try before we announce that there is no solution to equation (6.7)? Is there a systematic way to solve equations of this kind? With the backgrounds we have learned from previous sections, we are now in a good position to answer these questions by presenting a method for solving equations of this kind.

Definition 6.15: Let $a, b \in \mathbf{Z}$ and $m \in \mathbf{N}$. The following equation:

$$ax \equiv b \pmod{m}, \tag{6.8}$$

is called a *linear congruence equation* with variable x ranged over $\mathbf{Z}$.

Solving a linear congruence equation is to find the values for x such that equation (6.8) holds. In other words, we want to find the integer solution x such that $ax - b$ is a multiple of m. At first, we want to examine under what condition the solutions do exist.

According to Theorem 6.15, we can rewrite (6.8) and ask what is the solution for x in the following equation?

$$\begin{array}{ll} & ax - b = km, \quad \text{for some } k \in \mathbf{Z}; \\ \text{or} & ax + mk = b, \quad \text{for some } k \in \mathbf{Z}. \end{array} \tag{6.9}$$

Consider equation (6.9). By Theorem 6.6, if $\gcd(a, m) = d$, then $ax + mk$ must be a multiple of d. Moreover, by Theorem 6.10, there exists integers x' and k' such that $x'a + k'm = d$. Put these together, if d divides b, then there exists an integer x for the equality in (6.9). On the other hand, if $\gcd(a, m)$ does not divide b, the above arguments become invalid. Consider the following congruence equation:

$$2x \equiv 3 \pmod 4. \tag{6.10}$$

We claim that there is no solution for this equation. Why? An easy explanation is that since, for any integer x, $2x - 3$ is an odd number, and it is impossible for an odd number to be a multiple of even number, 4. Thus there is no solution for (6.10). How about the equation in (6.7)? We shall generalize our discussion in the following theorem.

Theorem 6.26 For any $a, b \in \mathbf{N}$ and $m \in \mathbf{N}$. The linear congruence equation $ax \equiv b \pmod m$ has a solution iff $\gcd(a, m)|b$.

Proof: Suppose $x_0 \in \mathbf{Z}$ is a solution of the equation. Then, there is an integer k such that

$$x_0 a + km = b.$$

By Theorem 6.6, $\gcd(a, m)$ divides b.

Conversely, suppose $\gcd(a, m) = d$ and $d|b$. Let $a = da', m = dm'$ and $b = db'$. We argue that,

$$a'x \equiv b' \pmod{m'} \tag{6.11}$$

has a solution. By Theorem 6.4, $\gcd(a', m') = 1$. By Theorem 6.10, there are integers x' and y' such that

$$x'a' + y'm' = \gcd(a', m') = 1.$$

Multiply b' on both sides to get

$$b'x'a' + b'y'm' = b'. \tag{6.12}$$

Clearly, since $b'y'$ is an integer, $b'x'a' - b'$ is a multiple of m'. Thus, $b'x'a' \equiv b' \pmod{m'}$, and hence $b'x'$ is a solution to equation (6.11). Multiply d on both sides of (6.12), we have

$$b'x'da' + b'y'dm' = db'.$$

Thus, $b'x'a + b'y'm = b.$, which means $b'x'a \equiv b \pmod m$ and $b'x'$ is too a solution to $ax \equiv b \pmod m$. □

Note that, by contrapositive, we have a usefully statement: if $\gcd(a, m) \not| b$, then $ax \equiv b \pmod m$ has no solution. Also, from the proof above, it is already clear about how to actually find a solution, if any, to a given linear congruence equations. We summarize the procedure in Figure 6.6.

Given $ax \equiv b \pmod{m}$.

Step 1: Use the extended Euclid's algorithm to find integers x' and y' such that $x'a + y'm = d = \gcd(a, m)$.

Step 2: If d does not divide b, then stop (no solution exists).

Step 3: $x = \frac{x'b}{d}$.

Output x as a solution.

Figure 6.6: Solving Linear Congruence Equation

Note that, if your extended Euclid's algorithm requires a to be positive and if the given $a < 0$, then you have to change the sign of a when you call the extended Euclid's algorithm and take $x = -\frac{x'b}{d}$ in step 3.

It seems that the solution, if any, given by the algorithm above is not the only solution. Our next question: what are others?

Theorem 6.27 Given a linear congruence equation $ax \equiv b \pmod{m}$, if x_0 is a solution to the equation, then $\lfloor x_0 \rfloor_{m'}$ is the set of all solution, where $m' = m/\gcd(a, m)$.

Proof: Let x_0 be a solution and i be some integer such that $x_0 + i$ is another solutions. Thus, $m|(ax_0 - b)$ and $m|(a(x_0 + i) - b)$. Consider

$$\frac{a(x_0 + i) - b}{m} = \frac{ax_0 - b}{m} + \frac{ai}{m}.$$

Clearly, i must be some integer that makes $\frac{ai}{m}$ to be an integer. Let $\gcd(a, m) = d$, we have

$$\frac{ai}{m} = \frac{da'i}{dm'} = \frac{a'i}{m'}.$$

Since $\gcd(a', m') = 1$, i must be a multiple of m'. Therefore, every element in the following set is a solution.

$$S = \left\{ x_0 + km' \ : \ k \in \mathbf{Z} \text{ and } m' = \frac{m}{\gcd(a, m)} \right\}.$$

Clearly, $S = \lfloor x_0 \rfloor_{m'}$ where $m' = m/\gcd(a, m)$.

What remains to prove is to argue that S does contain *all* solutions? Let $a = da'$ and $m = dm'$. Since x_0 is a solution, $ax_0 - b = k_0 m$ for some integer

k_0. Fix any solution x to the equation. Since x is a solution, we also have $ax - b = km$ for some integer k. Consider

$$x - x_0 = \frac{b + km}{a} - \frac{b + k_0 m}{a} = \frac{(k - k_0)m}{a} = \frac{(k - k_0)m'}{a'} = \frac{k - k_0}{a'} \times m'.$$

Since $(x - x_0) \in \mathbf{Z}$ and $\gcd(a', m') = 1$, it follows that $\frac{k-k_0}{a'} \in \mathbf{Z}$. Therefore, $x - x_0$ is a multiple of m', and hence $x \in \lfloor x_0 \rfloor_{m'}$. □

Theorem 6.28 Let $m, n \in \mathbf{N}$ with $\gcd(m, n) = 1$. Then, x_0 is a solution to $ax \equiv b \pmod{mn}$ iff x_0 is a solution to the following system:

$$\begin{aligned} ax &\equiv b \pmod{m}, \\ ax &\equiv b \pmod{n}. \end{aligned}$$

Proof: This theorem directly follows Theorem 6.23. □

Recall the definition of *multiplicative inverse* from Definition 6.14, and Theorem 6.25. If $ax \equiv b \pmod{m}$, then we have

$$a^- ax \equiv x \equiv a^- b \pmod{m}.$$

Note that the condition for the existence of a^- is sufficient to the existence of the solutions to the linear congruence equitation.

6.6 Solving Linear Congruence Equations with multiple variables

The form of the linear congruence equation with one variable shown in equation (6.8) is the easiest one. Nevertheless, we have spent a great deal of time to learn how to solve it, because it is the most basic one to which a more complicate congruence equation can be reduced. More precisely, solving some complicate congruence equation may be reduced to solving a series of equations in the form of (6.8). In many cases we also need the techniques introduced in the next section to solve congruence equations. Solving more general linear congruence equations is by all means a difficult subject and is way out of the scope of this book. Here we just briefly examine another form of *linear* congruence equations, in which we have more than one variables.

Definition 6.16: Let $a_1, a_2, \ldots, a_n \in \mathbf{Z}, n, m \in \mathbf{N}$, and $x_1, x_2, \ldots, x_n$ are variables range over $\mathbf{Z}$. The equation,

$$a_1 x_1 + a_2 x_2 + \cdots + a_n x_n \equiv b \pmod{m}, \tag{6.13}$$

is called a *linear* congruence equation with n variables.

Given a congruence in (6.13), let $\gcd(a_1, a_2, \ldots, a_n, m) = d$. It is easy to see that, if $d \not| b$, then there is no solution to (6.13). Moreover, since we can cancel d from both sides and the modulus, we can assume $d = 1$ without loss of generality. Let this be the case and assume that

$$\gcd(a_1, a_2, \ldots, a_{n-1}, m) = d'.$$

We know that, $\gcd(a_n, d') = 1$, because otherwise $d \neq 1$ (here we assume $d' \neq 1$). Therefore, there is a solution to

$$a_n x_n \equiv b \pmod{d'}.$$

Using the method introduced in the previous section, we obtain the solution set $\lfloor u \rfloor_{d'}$. For convenience, we restrict our solutions to $\mathbf{Z}_m$ and find a u such that $0 \leq u < d'$. Let $\frac{m}{d'} = m'$. Thus, every values in

$$\{u, u + d', u + 2d', \ \ldots \ , u + (m' - 1)d'\}, \tag{6.14}$$

is a possible value of x_n in the solutions to (6.13). Then, we substitute each value in (6.14) for x_n to remove the variable x_n and repeat the process above until no more variables left. Consider the following congruence as an example, where we want to find $(x, y) \in \mathbf{Z}_{12} \times \mathbf{Z}_{12}$ for the equation.

$$9x + 4y \equiv 5 \pmod{12}. \tag{6.15}$$

Since $\gcd(9, 4, 12) = 1$ which divides 5, we can proceed. To remove the variable y, consider $\gcd(9, 12) = 3$ and solve

$$4y \equiv 5 \pmod{3},$$

where the modulus 3 is the value of $\gcd(9, 12)$. Equivalently, we solve

$$y \equiv 2 \pmod{3}$$

to get $y = 2, 5, 8$, or 11. Then, we substitute every value for y in (6.15) and solve the result congruence. Here we just consider one case: $y = 2$. The other cases are similar. If $y = 2$, the equation (6.15) yields

$$9x + 8 \equiv 5 \pmod{12}.$$

We can further simplify as follows:

$$\begin{aligned} 9x + 8 + 4 &\equiv 5 + 4 && \pmod{12} \\ 9x + 12 &\equiv 9 && \pmod{12} \\ 9x &\equiv 9 && \pmod{12} \\ 3x &\equiv 3 && \pmod{4}. \end{aligned}$$

Thus, $x = 1, 5$, or 9. Therefore, the solutions in this case are $(1, 2), (5, 2)$, and $(9, 2)$.

6.7 Applications

6.7.1 Chinese Remainder Theorem

Let's consider the following game. A person thinks of an integer less than 60 and divides the number by 3, 4, and 5, respectively. Then, the person will tell you the remainders, respectively. Based on the three remainders told, you are asked to figure out what the number is. Does the number always exist? Are the three remainders you have sufficient to locate the number? About 400 A.D., a Chinese mathematician named Sun Tsu gave a beautiful theorem now known as *Chinese Remainder Theorem* to answer these question.

The game we just mentioned is a simplified form of the theorem. Here we translate the game into the notations we have learned. Suppose that x is the chosen integer. Given the following simultaneous congruence equations,

$$\begin{aligned} x &\equiv a \pmod 3, \\ x &\equiv b \pmod 4, \\ x &\equiv c \pmod 5, \end{aligned}$$

where a, b, and c are the remainders of x divided by 3, 4, and 5, respectively. Our goal is to find a solution for x that lies between 0 and 60.

The idea for solving the above simultaneous congruences is straightforward. We start with the first congruence equation and solve it by using the technique introduced in Section 6.5. In this simple form, the solution always exists, which is $3k + 2$, for any $k \in \mathbf{Z}$. The, put the solution into the second congruence equation to obtain a new equation with variable k, and solve it. Repeat the process until all equations are solved or an unsolvable equation is encountered. Consider the following example:

$$x \equiv 2 \pmod 3, \tag{6.16}$$
$$x \equiv 2 \pmod 4, \tag{6.17}$$
$$x \equiv 3 \pmod 5. \tag{6.18}$$

At first, we solve (6.16) to obtain the solution set, $\{3k + 2 : k \in \mathbf{Z}\}$. But not every value in the solution set is a solution to (6.17), i.e., not every k for $3k+2$ gives a solution to (6.17). Thus, we put $3k + 2$ as x into (6.17) to have

$$3k + 2 \equiv\ 2 \pmod 4,$$

or, equivalently,

$$3k \equiv\ 0 \pmod 4. \tag{6.19}$$

The solution of (6.19) is $k = 4u, u \in \mathbf{Z}$. Thus, the solution candidates so far we have is

$$x = 3k + 2 = 3 \times 4u + 2 = 12u + 2, u \in \mathbf{Z}.$$

Putting this x into the last equation(6.18), we have

$$12u + 2 \equiv 3 \pmod 5,$$

or equivalently,

$$12u \equiv 1 \pmod 5. \tag{6.20}$$

The solution to (6.20) is $u = 3+5v, v \in \mathbf{Z}$. Therefore, the solution to the original simultaneous congruences is

$$x = 12 \cdot (3 + 5v) + 2 = 60v + 38, v \in \mathbf{Z}.$$

Thus, $x = 38$ is one of the solutions, where $v = 0$. The set of all solution of the system of congruence equations is $\boxed{38}_{60}$.Clearly, if we restrict $x \in \mathbf{Z}_{60}$, then 38 is the solution.

Let us review the above solution. To be able to solve the congruences (6.16), (6.19), and (6.20), we need

$$\gcd(1, 3)|2, \ \gcd(3, 4)|0, \ \text{ and } \ \gcd(12, 5)|1. \tag{6.21}$$

Clearly, if the divisors, 3, 4, and 5 are relatively prime to each other, then the gcd's in (6.21) are 1's and the divisibility in (6.21) is true, and hence there exists a solution to the simultaneous congruences. If this is not the case, then not all of the equations in (6.16), (6.19), and (6.20) are solvable. Numerous nontrivial variations of the Chinese Remainder Theorem have been discovered by other mathematicians, including Fibonacci (1202) and Euler (1734). The formulation we state in the following is probably the easiest one. Nevertheless, the method can be generalized to solve a more general form of simultaneous congruence system as shown in (6.25).

Theorem 6.29 (Chinese Remainder Theorem) Let the congruence system be given as follows.

$$\begin{array}{rcll} x & \equiv & a_1 & \pmod{m_1}, \\ x & \equiv & a_2 & \pmod{m_2}, \\ \vdots & \vdots & & \vdots \\ x & \equiv & a_n & \pmod{m_n}. \end{array} \tag{6.22}$$

If $m_1, \ldots, m_n$ are relatively prime to each other, then the system has a solution:

$$x = \sum_{1 \le i \le n} a_i x_i \frac{M}{m_i}, \tag{6.23}$$

where $M = m_1 \cdots m_n$, and x_i is a solution of

$$\frac{M}{m_i} x \equiv 1 \pmod{m_i}. \tag{6.24}$$

Proof: Suppose that $m_1, \ldots, m_n$ are relatively prime to each other. It is clear that for each i, $\frac{M}{m_i}$ and m_i are relatively prime, i.e., $\gcd(\frac{M}{m_i}, m_i) = 1$, and hence, for every $i \in \{1, 2, \ldots, n\}$, the congruence in (6.24) has a solution.

Next, we prove that (6.23) is indeed a solution to every congruence equation in (6.22). In other words, we want to prove that, for every $j = 1, \ldots, n$,

$$\left(\sum_{1 \le i \le n} a_i x_i \frac{M}{m_i} \right) - a_j$$

is a multiple of m_j. It is clear that, if $i \neq j$, then $a_i x_i \frac{M}{m_i}$ is a multiple of m_j. Thus, what remains to prove is that

$$a_j x_j \frac{M}{m_j} - a_j = a_j (x_j \frac{M}{m_j} - 1)$$

is a multiple of m_j. Since x_j is a solution of $x \frac{M}{m_j} \equiv 1 \pmod{m_j}$, there exists an integer k such that

$$(x_j \frac{M}{m_j} - 1) = k m_j.$$

Therefore, $a_j (x_j \frac{M}{m_j} - 1) = a_j k m_j$ is also a multiple of m_j. □

Here we consider a bit more general from of simultaneous linear congruence systems, where the coefficients of the variables can be any integers.

$$\begin{array}{rcll} a_1 x & \equiv & b_1 & \pmod{m_1}, \\ a_2 x & \equiv & b_2 & \pmod{m_2}, \\ \vdots & \vdots & & \vdots \\ a_n x & \equiv & b_n & \pmod{m_n}. \end{array} \tag{6.25}$$

It is clearly that if one of the congruence in system (6.25) has no solution, then the system has no solution too. Thus, we at first check, for every $1 \le i \le n$, $\gcd(a_i, m_i) | b_i$. If this is the case, we can solve each congruence in (6.25) independently. Let $\lfloor u_i \rfloor_{m_i'}$ be the set of solutions to $a_i x \equiv b_i \pmod{m_i}$ where $m_i' = \frac{m_i}{\gcd(a_i, m_i)}$. Clearly, the solutions to (6.25) is the intersection:

$$\lfloor u_1 \rfloor_{m_1'} \cap \lfloor u_2 \rfloor_{m_2'} \cap \lfloor u_n \rfloor_{m_n'}$$

which is simply the solution of the following system:

$$\begin{array}{rcll} x & \equiv & u_1 & \pmod{m_1'}, \\ x & \equiv & u_2 & \pmod{m_2'}, \\ \vdots & \vdots & & \vdots \\ x & \equiv & u_n & \pmod{m_n'}. \end{array}$$

Then, we use the method in Theorem 6.29 to solve the system above.

6.7.2 Fermat's Little Theorem and Euler's Theorem

This is one of Fermat's best known theorems and was proved by Fermat himself in 1640. It is known as his "little theorem" to distinguish it from his "great" theorem.[1] The theorem was once thought to be one of the least applicable theorems in mathematics. Just for fun, Fermat wanted to derive a condition to construct "big" perfect numbers.[2] But due to the use of computer science in areas such as coding theory and cryptography, Fermat's little theorem has become one of the most useful tools from number theory.

Theorem 6.30 **(Fermat's Little Theorem)** If p is a prime number and $p \not| n$, then

$$n^{p-1} \equiv 1 \pmod{p}.$$

Proof: Let $i, j \in \mathbf{Z}$ with $1 \leq i, j \leq (p-1)$ and

$$in \equiv jn \pmod{p}$$

That is, $(i-j)n = kp$ for some integer k. Since p is a prime number and $p \not| n$, it follows that $\gcd(p, n) = 1$. Therefore, if $p|(i-j)n$, then it must be the case that $p|(i-j)$. But $1 \leq i, j \leq (p-1)$, the only possible case is $(i-j) = 0$, and hence $i = j$. Therefore,

$$[in \equiv jn \pmod{p}] \implies [i = j]. \tag{6.26}$$

The contrapositive of (6.26) is:

$$[i \neq j] \implies [in \not\equiv jn \pmod{p}]. \tag{6.27}$$

In other words, there are exactly $(p-1)$ residue classes modulo p in the following list:

$$\lfloor 1n \rfloor_p, \lfloor 2n \rfloor_p, \ldots, \lfloor (p-1)n \rfloor_p. \tag{6.28}$$

It is clear that $1n, 2n, \ldots,$ and $(p-1)n$ are not multiples of p. Thus, none of the residue classes in (6.29) is equivalent to $\lfloor 0 \rfloor_p$. By Theorem 14, there are exactly p distinct residue classes mod p. After removing $\lfloor 0 \rfloor_p$, they are

$$\lfloor 1 \rfloor_p, \lfloor 2 \rfloor_p, \ldots, \lfloor p-1 \rfloor_p \quad . \tag{6.29}$$

Therefore, the residue classes in (6.29) and (6.28) are exactly the same, except perhaps in a different order. By the multiplicative property in Theorem 6.18,

[1] The "great" theorem best known as Fermat's "last theorem" stated by Fermat himself but failed to provide a proof. The theorem after more than 300 years since first stated was finally proved in 1992.

[2] A perfect number is a natural number that equals the sum of its proper factors. For example, 6 and 28 are perfect numbers since 6=1+2+3 and 28 = 1+2+4+7+14, while 8 is not since $8 \neq 1+2+4$. Perfect numbers turns out to be very rare. There are only 4 perfect numbers less than 10000!!

we have

$$\begin{aligned} 1 \cdot 2 \cdots (p-1) &\equiv (n \cdot 2n \cdots (p-1)n) \pmod{p} \\ &\equiv (1 \cdot 2 \cdots (p-1))n^{p-1} \pmod{p}. \end{aligned}$$

Since p is a prime, it follows that $\gcd(1 \cdot 2 \cdots (p-1), p) = 1$. By Theorems 6.20, we can cancel $1 \cdot 2 \cdots (p-1)$ from both sides and obtain the result:

$$1 \equiv n^{p-1} \pmod{p}.$$

□

Euler's Phi Function and Theorem: Fermat's little theorem was generalized by Euler. Euler's theorem gives us an easy way to find the residue class of a composed number. In other words, if m is a huge composed number, we can use Euler's theorem to find the remainder of m, when divided by d quickly, without actually performing the division algorithm.

Definition 6.17: Define $\varphi : \mathbf{N} \to \mathbf{N}$ where, $\varphi(m)$ is the total number of residue classes mod m that are relatively prime to m. This function is called Euler's Phi function.

For example, let the modulus $m = 3$. There are three residue classes, $\boxed{0}_3, \boxed{1}_3$, and $\boxed{2}_3$. Numbers in $\boxed{0}_3$ are not relatively prime to 3. Therefore, $\varphi(3) = 2$. If $m = 4$, there are 4 residue classes. But numbers in $\boxed{0}_4$ and $\boxed{2}_4$ are not relatively prime to 4. Therefore, $\varphi(4) = 2$. In view of these observations, we can redefine Euler's Phi function as follows.

Definition 6.18: Euler's Phi function, $\varphi(m)$, is the total number of elements in $\{0, 1, 2, \ldots, m-1\}$ that are relatively prime to m.

Clearly, if p is a prime number, then $\varphi(p) = p - 1$. Note that 0 is not relatively prime to any numbers.

Theorem 6.31 Let p be a prime number. Then, for any $e \in \mathbf{N}$, we have

$$\varphi(p^e) = p^e - p^{e-1}.$$

Proof: Since p is a prime number, only those numbers that are multiples of p are not relatively prime to p. They are

$$0, p, 2p, 3p, \ \ldots, \ p^e - p.$$

Since $p^e - p = (p^{e-1} - 1)p$, it follows that there are p^{e-1} numbers among $0, 1, 2, \ldots, p^e - 1$ not relatively prime to p. Therefore, $\varphi(p^e) = p^e - p^{e-1}$. □

Theorem 6.32 If $a, b \in \mathbf{N}$ are two integers such that $\gcd(a, b) = 1$, then

$$\varphi(ab) = \varphi(a)\varphi(b).$$

Proof: Let $A \subseteq \mathbf{Z}_a$, $B \subseteq \mathbf{Z}_b$, and $C \subseteq \mathbf{Z}_{ab}$ be three residue systems relatively prime to a, b, and ab, respectively, given as follows.

$$\begin{aligned} A &= \{a_1, a_2, \ldots, a_{\varphi(a)}\}, \\ B &= \{b_1, b_2, \ldots, b_{\varphi(b)}\}, \\ C &= \{c_1, c_2, \ldots, c_{\varphi(ab)}\}. \end{aligned}$$

Moreover, we assume all elements in each system are distinct. In other words, $|A| = \varphi(a)$, and same to B and C. Our task is to define a bijection $f : C \to A \times B$. If such a function exists, then $|C| = |A \times B| = |A| \times |B|$, and hence $\varphi(ab) = \varphi(a)\varphi(b)$.

For each $x \in C$, define $f(x) = (r_a, r_b)$, where $x \in \boxed{r_a}_a$ and $x \in \boxed{r_b}_b$. Since $x \in C$, by assumption, $\gcd(x, ab) = 1$. Also,

$$[\gcd(x, ab) = 1] \Longrightarrow [\gcd(x, a) = 1 \text{ and } \gcd(x, b) = 1].$$

It follows that there must exist some $r_a \in A$ and $r_b \in B$ that satisfy the definition of f. Moreover, by the division algorithm, such r_a and r_b are uniquely determined to ensure that f is single valued. Therefore, for every $x \in C$, $f(c)$ is well defined in $A \times B$.

What remains is to argue that f is bijection. Fix an $r_a \in A$ and an $r_b \in B$. Consider the following system:

$$\begin{aligned} x &\equiv r_a \pmod{a}, \\ x &\equiv r_b \pmod{b}. \end{aligned} \tag{6.30}$$

Clearly, if x can satisfy both congruences in (6.30), then $f(x) = (r_a, r_b)$. Since $\gcd(a, b) = 1$, by the Chinese Remainder Theorem, the congruence system (6.30) has a solution, say, x'. Moreover,

$$(\gcd(x', a) = 1 \text{ and } \gcd(x', b) = 1) \quad \Longrightarrow \quad \gcd(x', ab) = 1.$$

In other words, $x' \in \boxed{c_i}_{ab}$ for some $c_i \in C$. Thus, f is surjective. By the division algorithm, such a c_i is unique, and hence f is injective. □

With Theorems 6.31 and 6.32, we can easily find the value of $\varphi(n)$. For example, to compute $\varphi(210)$, we factorize $210 = 2 \cdot 3 \cdot 5 \cdot 7$ first. Then,

$$\begin{aligned} \varphi(210) &= \varphi(2 \cdot 3 \cdot 5 \cdot 7) \\ &= \varphi(2) \cdot \varphi(3) \cdot \varphi(5) \cdot \varphi(7) \\ &= 1 \cdot 2 \cdot 4 \cdot 6 \\ &= 48. \end{aligned}$$

For another example, consider 2016. Since $2016 = 2^5 \cdot 3^2 \cdot 7$, we have

$$\begin{aligned}\varphi(2016) &= \varphi(2^5 \cdot 3^2 \cdot 7) \\ &= \varphi(2^5) \cdot \varphi(3^2) \cdot \varphi(7) \\ &= (2^5 - 2^4) \cdot (3^2 - 3) \cdot 6 \\ &= 576.\end{aligned}$$

That is, there are 576 natural numbers in $\mathbf{Z}_{2016}$ relatively prime to 2016.

Theorem 6.33 **(Euler's Theorem)** Let $a, m \in \mathbf{N}$ with $\gcd(a, m) = 1$. Then,

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Proof: The idea is similar to the proof of Fermat's little theorem. Let $\varphi(m) = n$ and $p_1, p_2, \ldots p_n$ are natural numbers less than m and relatively prime to m. Thus, the following classes are residue classes relatively prime to m.

$$\lfloor p_1 \rfloor_m, \lfloor p_2 \rfloor_m, \ldots, \lfloor p_n \rfloor_m \tag{6.31}$$

Let $i \in \mathbf{N}$ with $1 \leq i \leq n$. Since $\gcd(a, m) = 1$ and $\gcd(p_i, m) = 1$, it follows that $\gcd(ap_i, m) = 1$ and therefore $\lfloor ap_i \rfloor_m$ is a residue class relatively prime to m. Therefore,

$$\lfloor ap_1 \rfloor_m, \lfloor ap_2 \rfloor_m, \ldots, \lfloor ap_n \rfloor_m \tag{6.32}$$

are also residue classes relatively prime to m. With the same argument used in the proof of Fermat's Little Theorem, we conclude that the residue classes in (6.31) and (6.32) are indeed the same. Similarly,

$$p_1 p_2 \cdots p_n \equiv a p_1 a p_2 \cdots a p_n \equiv p_1 p_2 \cdots p_n a^n \pmod{m}.$$

Since $\gcd(p_1 p_2 \cdots p_n, m) = 1$, By Theorems 6.20, we can cancel $p_1 p_2 \cdots p_n$ from both sides to have $1 \equiv a^n \pmod{p}$ we we want. □

6.7.3 RSA Cryptosystem

RSA Cryptosystem probably is the most important application of number theory of all time, which is a *public-key* cryptosystem named for its inventors, Rivest, Shamir, and Adleman who put forward the idea in their celebrated paper in 1977. The RSA algorithm lies down the foundation of cryptography for an entire generation of modern cryptographers and remains the most widely used encryption method for today's communication technology. The three inventors were awarded Truing Award in 2002 that was considered the Nobel Prize of computer science.

Consider the following situation. Bob wants Alice to send him secret information over an insecure channel. For some unavoidable difficulties, Bob and Alice can't meet in person or communicate through a secure channel, and thus, it is impossible for them to share a secret key without the fear of being intercepted. How can Alice transfer the secret information to Bob under this situation? Public-key cryptosystem is a solution. Here is the idea:

1. Bob chooses public-keys and secret-keys. He then keeps the secret-keys to himself and announces the public-keys to Alice.
2. Alice gets the public-keys and uses them to encrypt the information she intends to send to Bob. Then, she sends off the encrypted text.
3. Bob receives the encrypted text and uses the secret-keys to decrypt it.

Note that, a third person may also have the public-keys but only Bob has the secret-keys. Thus, only Bob can retrieve the information from the encrypted text. If necessary, Bob can openly teach Alice how to encrypt the information with the public-keys. Without the knowledge of the secret-keys, a third person can't[3] feasibly reverse the encryption procedure to obtain the original information, even if the encryption algorithm is given. Now, we present the RSA cryptosystem.

RSA Cryptosystem:

1. Bob does the followings:
   (a) Choose two different big prime numbers p and q.
   (b) Calculate m and n such that, $m = pq$ and $n = \varphi(pq)$.
   (c) Find a and b such that, $ab \equiv 1 \pmod{n}$.
   (d) Tell Alice a and m. (Keep b, p, q, n in a safe.)
2. Alice does the followings:
   (a) Calculate $t = (s^a \mod m)$, where s is the secret information she wants to send.
   (b) Send t to Bob.
3. Bob receives t and reads the result of $(t^b \mod m)$

Clearly, if $s = (t^b \mod m)$, then Bob does get the secret information from Alice. To see this is the case, fix an s with $0 < s < \min(p, q)$.[4] Thus, $\gcd(s, m) = 1$ since p and q are primes and $m = pq$.

[3] Well, we believe he/she can't, unless P = NP.

[4] In fact, $0 < s < \min(p, q)$ is more restrictive than necessary. Any $s \in \mathbf{Z}_{(pq-1)}$ can be correctly encrypted and decrypted. See the discussion below.

$$\begin{aligned} t^b &\equiv (s^a)^b && \pmod m \\ &\equiv s^{ab} && \pmod m, \quad \text{recall that } ab \equiv 1 \pmod n \\ &\equiv s^{1+kn} && \pmod m, \quad \text{where } n = \varphi(m), k \in \mathbf{Z} \\ &\equiv s \cdot s^{k\varphi(m)} && \pmod m \\ &\equiv s \cdot 1 && \pmod m, \quad \text{by Euler's Theorem} \\ &\equiv s && \pmod m \end{aligned}$$

Note that, we have had restricted the message s to be smaller than $\min(p, q)$ in order to ensure that $\gcd(s, m) = 1$ so we can apply the Euler's Theorem. In fact, this restriction can be removed. Let $s \in \mathbf{Z}_{(pq-1)}$. It is obvious that s cannot be greater than $(pq - 1)$ due to the modulus, $m = pq$. Suppose $p = \min(p, q)$ and $\gcd(s, m) > 1$. Then, it must be the case that $s = s'p$ for some integer s' with $1 \leq s' \leq q - 1$. It follows that $\gcd(s', q) = 1$ and $\gcd(s, q) = 1$. As above, we can verify that,

$$s^{\varphi(m)} \equiv s^{\varphi(p)\varphi(q)} \equiv s^{\varphi(p)(q-1)} \equiv 1 \pmod q.$$

Therefore, there is some $k \in \mathbf{Z}$ such that

$$1 = s^{\varphi(m)} + kq.$$

Multiply each side by s,

$$s = s \cdot s^{\varphi(m)} + s \cdot kq = s^{1+\varphi(m)} + s'kpq. = s^{1+\varphi(m)} + s'km.$$

Thus,

$$s \equiv s^{1+\varphi(m)} \pmod m.$$

Based on the discussion above, the only two restrictions for the RSA algorithm to work is $p \neq q$ and $s \in \mathbf{Z}_{pq-1}$. If $s = 0$ or $s = 1$, obviously, the plaintext and ciphertext will be the same and there will be no secret at all.

Clearly, if a third person knows p or q, then the third person can derive b from a as Bob does and break the system. In practices, we choose two prime numbers with about 100 digits in decimal. This should be sufficient for many sensitive information such as, credit card numbers, bank accounts, licence numbers, and so on. For textual information such as classified documents, we can divide the information into small blocks. To find two prime numbers with 100 digits is not trivial but can be easily done with today's computers. However, to factorize a 200 digits number that is the product of two prime numbers is impossible with today's number theory and technology. Thus, the security of an RSA cryptosystem depends on the intractability of factorizing m.

6.8 Problems

Problem 1: For what integers a does the following equation hold?

$$|2^a| \;=\; |2^{-a}|.$$

Problem 2: Consider functions g and h defined as follows.

$$g(x) = x - \lfloor x \rfloor;$$
$$h(x) = x - \lceil x \rceil.$$

For which $x \in \mathbf{R}$ is $|g(x)| = |h(x)|$? Prove your answer.

Problem 3: Prove that for all odd integers n, 8 divides $n^2 - 1$.

Problem 4: According to the values of a and b given in the following, find, by *the division algorithm*, the values of q and r such that,

$$a = qb + r, \text{ where } 0 \le r < |b|.$$

(i) $a = 387, b = 28$; (ii) $a = 191, b = -14$; (iii) $a = -78, b = 15$; (iv) $a = -105, b = -7$.

Problem 5: Let $n \ge 0$ be an integer. Without using mathematical induction, prove that 5 divides $n(n^4 - 1)$.

Problem 6: Let $m \in \mathbf{N}, x \in \mathbf{Z}$. Prove that

$$\left\lceil \frac{x}{m} \right\rceil \;=\; \left\lfloor \frac{x + m - 1}{m} \right\rfloor.$$

Problem 7: Let $m, n \in \mathbf{Z}$ where $m > n > 0$ and

$$r = m - \lfloor \frac{m}{n} \rfloor n.$$

Show that $r < \frac{m}{2}$.

Problem 8: Let $t \in \mathbf{Z}$. Prove that

$$\left\lceil \frac{1}{2} \left\lfloor \frac{t}{2} \right\rfloor \right\rceil = \left\lfloor \frac{t+2}{4} \right\rfloor.$$

Problem 9: Prove that the results of the above problem hold for any $t \in \mathbf{R}$.

Problem 10: Egyptian mathematicians in 1800 B.C. represented rational numbers between 0 and 1 as sums of unit fractions $1/a + 1/b + \cdots + 1/k$ where $a, b, \ldots, k$ were distinct positive integers. E.g., they wrote $2/5$ as $1/3 + 1/15$. Prove that it is always possible to do this in a systematic way as described below: If $0 < m/n < 1$, then for $q = \lceil \frac{n}{m} \rceil$

$$\frac{m}{n} = \frac{1}{q} + \left\{ \text{ representation of } \frac{m}{n} - \frac{1}{q} \right\}.$$

Show that the above procedure terminates after a finite number of steps.

Problem 11: Find the base-8 representation of 100 and base-9 representation of 1000. Show details of your work.

Problem 12: Let $b \geq 2$ be an integer. Write a recursive algorithm to find, for any $n \in \mathbf{N}$, the base-b expression of n.

Problem 13: Let $a,\ b,\ x$, and y be integers such that $\gcd(a, b) = ax + by$. Prove that x and y are relatively prime.

Problem 14: Let a, b be relatively prime integers. Suppose m is any integer such that $a|m$ and $b|m$. Prove that $ab|m$.

Problem 15: Find integers a, b, x, y such that $ax+by = 2$, but $\gcd(a, b) \neq 2$. Explain how that can be possible.

Problem 16: Find $\gcd(242, 165)$ and $\gcd(17296, 18416)$.

Problem 17: Define $F_0 = 0, F_1 = 1$, and for $n \geq 2$,

$$F_n = F_{n-1} + F_{n-2}.$$

This sequence is called the Fibonacchi sequence. Let $m, n \in \mathbf{N}$ and $m > n \geq 0$. Prove by mathematical induction that if Euclid's algorithm performs k recursive calls to find gcd of m and n, then

$$m \geq F_{k+2} \quad \text{and} \quad n \geq F_{k+1}.$$

Problem 18: Find $x, y \in \mathbf{Z}$ such that

$$\gcd(375, 275) = 375x + 275y.$$

Problem 19: Prove that if x and y are odd numbers, then it is impossible to find an integer a such that $x^2 + y^2 = a^2$.

Problem 20: Prove that if x and y are not divisible by 3, then it is impossible to find an integer a such that $x^2 + y^2 = a^2$.

Problem 21: Prove that if $2^n - 1$ is prime, then n is a prime. Is the converse true?

Problem 22: Find all $m \geq 1$ such that $27 \equiv 9 \pmod{m}$.

Problem 23: Which of the elements of A are congruent to which other elements mod 3? mod 7? Explain.

$$A := \{687, 589, 931, 847, 527\}.$$

Problem 24: For each pair (x, m) in B, find the least positive integer r such that $x \equiv r \pmod{m}$. Explain.

$$B := \{(19, 2),\ (131, 5),\ (84, 14),\ (141, 17)\}.$$

Problem 25: Find the solutions, if any, to the following congruences:

1. $5x \equiv 9 \pmod{17}$.
2. $18y \equiv 8 \pmod{15}$.
3. $12z \equiv 15 \pmod{42}$.

Problem 26: Let $m, n \geq 1$ and $a \in \mathbf{Z}$. Prove that if $a^n \equiv 1 \pmod{m}$ then $\gcd(a, m) = 1$.

Problem 27: Do the numbers 19, 8, -3, -5, 10, 5 form a complete residue system modulo 6?

Problem 28: Let $m \in \mathbf{N}$ and $s \in \mathbf{Z}$, and let C be any complete system of residues mod m. Prove that

$$C + s := \{c + s;\ c \in C\}$$

is also a complete system of residues mod m.

Problem 29: Find the least positive residue of $(15)^{35}$ mod 19. Show your steps and explain your procedure.

Problem 30: Find the least positive residue of $(29)^{36}$ mod 17.

Problem 31: Let $\gcd(t, m) = 1$, and let $\{a_0, \ldots, a_{m-1}\}$ be any complete system of residues mod m. Prove that $\{ta_0, \ldots, ta_{m-1}\}$ is also a complete system of residues mod m.

Problem 32: Without referring to calendars, show that the calendar for December 1976 is the same as that for July 1987.

Problem 33: Let $f(x) = 13x^3 - 5x^2 + 14x - 10$. Compute the least positive residue of $f(12)$ mod 7.

Problem 34: Let $m \geq 1$. Prove that for all $a,\ x \in \mathbf{Z}$, if $x \in \underline{[a]}_m$, then $\gcd(x, m) = \gcd(a, m)$.

Problem 35: In the following calculate the least positive residues.

1. $2^{14} \pmod{17}$
2. $3^{100} \pmod{5}$

Problem 36: Solve the following three congruence systems, respectively.

$x \equiv 3 \pmod{5}$	$y \equiv 2 \pmod{5}$	$z \equiv 7 \pmod{16}$
$x \equiv 2 \pmod{6}$	$y \equiv 7 \pmod{13}$	$z \equiv 1 \pmod{9}$
$x \equiv 3 \pmod{7}$	$y \equiv 11 \pmod{8}$	$z \equiv 2 \pmod{25}$

Problem 37: Prove that for all integers $m \geq 0$,

$$(2^m - 1)(2^m - 2)(2^m - 4) \equiv 0 \pmod{7}.$$

Problem 38: Find all $n \geq 0$ for which

$$3^n + 4^n \equiv 0 \pmod{7}.$$

Problem 39: Let m and n be positive integers. Prove that the partition of $\mathbf{Z}$ given by congruence mod m is a refinement of that for congruence mod n iff m is a multiple of n.

Problem 40: Define a sequence $a_0, a_1, a_2, \ldots$ of integers by the recursion $a_{n+2} = a_{n+1} + a_n$ (for all $n \geq 0$) and the initial conditions $a_0 = 0$ and $a_1 = 1$. Prove (by induction?) that $a_{5k} \equiv 0 \pmod{5}$ for all $k \geq 0$.

Problem 41: Find $\varphi(18)$, $\varphi(40)$, and $\varphi(72)$.

Problem 42: Prove that $2^{20} \equiv 1 \pmod{75}$ by using Euler's theorem and Theorem 6.23.

Problem 43: Prove that for any $m \geq 1$,

$$\varphi(m) = m \prod_{p|m} (1 - \frac{1}{p}).$$

Here $p|m$ means that p is a *prime* dividing m. The product is taken over all such primes.

Problem 44: (*i*) Prove that if n is odd, then $\varphi(2n) = \varphi(n)$.

(*ii*) Is there an $n \geq 1$ for which $\varphi(3n) = \varphi(n)$?

(*iii*) Prove that if n is even, then $\varphi(2n) = 2\varphi(n)$.

Problem 45: Find all integers $n \geq 1$ such that $\varphi(n) = 8$.

6.9 Solutions

Solution 1: Since for all integer a, $2^a > 0$ and $2^{-a} > 0$, we can get rid of the absolute value sign. Therefore,

$$\begin{array}{rcl} |2^a| = |2^{-a}| & \Rightarrow & 2^a = 2^{-a} \\ & \Rightarrow & 2^a 2^a = 1 \\ & \Rightarrow & 2^a = 1 \\ & \Rightarrow & a = 0. \end{array}$$

□

Solution 2: For all $x \in \mathbf{R}$ we know that $x \geq \lfloor x \rfloor$, and $x \leq \lceil x \rceil$. Therefore, for all $x \in \mathbf{R}, g(x) \geq 0$, and $h(x) \leq 0$. Let $x = k + s$, where $k \in \mathbf{Z}, s \in \mathbf{R}$ and $0 \leq s < 1$.

$$\begin{array}{rl} & |g(x)| = |h(x)| \\ \Rightarrow & g(x) = -h(x) \\ \Rightarrow & x - \lfloor x \rfloor = \lceil x \rceil - x \\ \Rightarrow & 2x = \lceil x \rceil + \lfloor x \rfloor \end{array}$$

Thus, $2k + 2s = \lceil k + s \rceil + \lfloor k + s \rfloor$.

case 1: If $s = 0$, i.e., if x is an integer, then for all $k \in \mathbf{Z}$ the above equality holds.

case 2: If $0 < s < 1$, then $\lceil k + s \rceil = k + 1$, and $\lfloor k + s \rfloor = k$. If the above equality holds, then $2k + 2s = 2k + 1$. Therefore, $s = 1/2$.

From the two cases above, the true set of $|g(x)| = |h(x)|$ is

$$\{0, \pm\frac{1}{2}, \pm 1, \pm(1 + \frac{1}{2}), \pm 2, \pm(2 + \frac{1}{2}), \pm 3, \ldots\}.$$

□

Solution 3: Let $n = 2k + 1$, $k \in \mathbf{Z}$. $n^2 - 1 = (2k + 1)^2 - 1 = 4k(k + 1)$.

Let k' range over $\mathbf{Z}$.

case 1: If $k = 2k'$, then $n^2 - 1 = 8k'(2k' + 1)$.

case 2: If $k = 2k' + 1$, then

$$n^2 - 1 = 4(2k' + 1)(2k' + 2) = 8(2k' + 1)(k' + 1).$$

In either case, $n^2 - 1$ is divisible by 8. □

Solution 4:

(i) $387 = 28 \times 13 + 23,\ q = 13, r = 23.$

(ii) $191 = -14 \times -13 + 9,\ q = -13, r = 9.$

(iii) $-78 = 15 \times -6 + 12,\ q = -6, r = 12.$

(iv) $-105 = -7 \times 15 + 0,\ q = 15, r = 0.$

□

Solution 5: The solution is easy to follow if we write $n(n^4 - 1)$ as

$$(n - 1)n(n + 1)(n^2 + 1).$$

Any $n \in \mathbf{Z}$ can be written as $n = 5q + r$, where $q \in \mathbf{Z}$ and $0 \leq r < 5$. We have 5 cases. In each case one of the factors of $n(n^4 - 1)$ is 0, as seen below.

case 1: $n = 5q$; n itself is divisible by 5.

case 2: $n = 5q + 1$; $n - 1$ is divisible by 5.

case 3: $n = 5q + 2$;

$$n^2 + 1 = (5q + 2)^2 + 1 = 25q^2 + 20q + 4 + 1 = 5(5q^2 + 4q + 1).$$

Therefore $n^2 + 1$ is divisible by 5.

case 4: $n = 5q + 3$;

$$n^2 + 1 = (5q + 3)^2 + 1 = 25q^2 + 30q + 9 + 1 = 5(5q^2 + 6q + 2).$$

Therefore $n^2 + 1$ is divisible by 5.

case 5: $n = 5q + 4$; $n + 1$ is divisible by 5.

□

Solution 6: By the division algorithm we get $x = qm + r$ where $q, r \in \mathbf{Z}$ and $0 \le r < m$.

Therefore,

$$\left\lceil \frac{x}{m} \right\rceil = \left\lceil q + \frac{r}{m} \right\rceil = \begin{cases} q & \text{if } r = 0, \\ q+1 & \text{if } r > 0, \end{cases}$$

and

$$\left\lfloor \frac{x+m-1}{m} \right\rfloor = \left\lfloor q + \frac{r}{m} + 1 - \frac{1}{m} \right\rfloor = \begin{cases} q & \text{if } r = 0, \\ q+1 & \text{if } 0 < r < m. \end{cases}$$

Therefore,

$$\left\lceil \frac{x}{m} \right\rceil = \left\lfloor \frac{x+m-1}{m} \right\rfloor.$$

□

Solution 7: By the division algorithm $0 \le r < n$. Consider the following two cases:

case 1: $0 < n \le \frac{m}{2}$. In this case, $r < \frac{m}{2}$ immediately follows.

case 2: $\frac{m}{2} < n < m$. In this case it is obvious that $1 < \frac{m}{n} < 2$, or $\lfloor \frac{m}{n} \rfloor = 1$. Consequently, $r = m - \lfloor \frac{m}{n} \rfloor n = m - n < m - \frac{m}{2}$. Therefore, $r < \frac{m}{2}$.

□

Solution 8: Problem 9 is a special case of problem 10, hence its solution is obtained from the following solution. □

Solution 9: Let $t \in \mathbf{R}$. By the division algorithm, $t = 2k + r$, where $0 \le r < 2, r \in \mathbf{R}$, and $k \in Z$. By substituting $t = 2k + r$ in the left side we get

$$\begin{aligned} \left\lceil \frac{1}{2} \left\lfloor \frac{t}{2} \right\rfloor \right\rceil &= \left\lceil \frac{1}{2} \left\lfloor \frac{2k+r}{2} \right\rfloor \right\rceil \\ &= \left\lceil \frac{1}{2} \left\lfloor k + \frac{r}{2} \right\rfloor \right\rceil = \left\lceil \frac{1}{2} k \right\rceil, \text{ because } 0 \le \frac{r}{2} < 1. \end{aligned}$$

Similarly, by substituting $t = 2k + r$ in the right side we get

$$\left\lfloor \frac{t+2}{4} \right\rfloor = \left\lfloor \frac{2k+r+2}{4} \right\rfloor = \left\lfloor \frac{k}{2} + \frac{r+2}{4} \right\rfloor = \left\lfloor \frac{k}{2} + s \right\rfloor,$$

where $\frac{1}{2} \leq s = \frac{r+2}{4} < 1$. The integer k is either odd or even.

case 1: If k is even, then $k = 2n$ for some n, $\lceil \frac{k}{2} \rceil = \lceil n \rceil = n$, and

$$\left\lfloor \frac{k}{2} + s \right\rfloor = \lfloor n + s \rfloor = n.$$

Thus, the equality holds.

case 2: If k is odd, then $k = 2n + 1$ for some n, $\lceil \frac{k}{2} \rceil = \lceil n + \frac{1}{2} \rceil = n + 1$, and

$$\begin{aligned} \left\lfloor \frac{k}{2} + s \right\rfloor = \left\lfloor n + \frac{1}{2} + s \right\rfloor &= \left\lfloor n + 1 + (s - \frac{1}{2}) \right\rfloor \\ &= n + 1, \text{ because } 0 \leq s - \frac{1}{2} < \frac{1}{2}. \end{aligned}$$

Therefore, in both cases the equality holds. □

Solution 10: First we consider a variant of the division algorithm. Let $m, n \in \mathbf{Z}$ where $m \neq 0$, then there exist unique integers q, r such that

$$[n = mq - r, \text{ and } 0 \leq r < |m|, \tag{6.33}$$

where $q = \lceil \frac{n}{m} \rceil$ and $r = mq - n$. In addition, let $0 < m < n$ so that $0 \leq r < m$. Dividing both sides of (6.33)by n and simple manipulation gives

$$\frac{m}{n} = \frac{1}{q} + \frac{r}{nq}.$$

Now, we construct a recursive algorithm to express a ratio as Egyptians did.

```
f(m, n)
    if m = 1 then
       { print(1/n); stop; }
    q ← ⌈n/m⌉;
    r ← mq − n;
    if r = 0 then
       { print(1/q); stop; }
    print(1/q+);
    f(r, nq);
end f
```

How do we know this algorithm will stop for any integers n, m with $0 < m < n$? Because we know that r is strictly smaller than m. Therefore, if we

recursively apply f to r as the first argument, eventually the first argument will become 0 or 1 and no more recursive calls will be made. □

Solution 11: In both cases we use the division algorithm and successively write the remainders:

$$\begin{aligned} 100 &= 12\times 8 + 4 \\ 12 &= 1\times 8 + 4 \\ 1 &= 0\times 8 + 1 \end{aligned}$$

Therefore, $100 = (144)_8$.

$$\begin{aligned} 1000 &= 111\times 9 + 1 \\ 111 &= 12\times 9 + 3 \\ 12 &= 1\times 9 + 3 \\ 1 &= 0\times 9 + 1 \end{aligned}$$

Therefore, $1000 = (1331)_9$. □

Solution 12:

```
b(n)
    if n = 0 then    stop;
    k ← ⌊n/b⌋;
    r ← n − bk;
    b(k);    print(r);    stop;
end b
```

□

Solution 13: Let $a = da', b = db'$ and $d = \gcd(a, b) = ax + by$ for some integers x and y. We have

$$\begin{aligned} & d = ax + by = da'x + db'y \\ \Longrightarrow \quad & 1 = a'x + b'y. \end{aligned}$$

Because a' and b' are integers, by Theorem 6.12, $\gcd(x, y) = 1$. □

Solution 14: Suppose $a|m, b|m$, $m \in Z$. Since a and b are relatively prime

integers, we obtain

$$\begin{aligned} \gcd(a,b)=1 &\Rightarrow \quad xa+yb=1 \quad \text{for some } x,y\in\mathbf{Z} \\ &\Rightarrow \quad mxa+myb=m \\ &\Rightarrow \quad \frac{mxa}{ab}+\frac{mby}{ab}=\frac{m}{ab} \\ &\Rightarrow \quad \frac{m}{b}x+\frac{m}{a}y=\frac{m}{ab} \end{aligned}$$

Since all $\frac{m}{b}, x, \frac{m}{a}$, and y are integers, therefore $\frac{m}{ab}$ is an integer too, and hence $ab|m$. □

Solution 15: Let $a=b=x=y=1$. It is easy to see that $ax+by=2$, but $\gcd(a,b)\neq 2$. □

Solution 16: Let $q=\lfloor\frac{m}{n}\rfloor$ and $r=m-\lfloor\frac{m}{n}\rfloor n$.

m	=	$n\times q$	+	r,	
242	=	165×1	+	77,	
165	=	77×2	+	11,	
77	=	11×7	+	0.	Therefore, $\gcd(242,165)=11$.

m	=	$n\times q$	+	r,	
18416	=	17296×1	+	1120	
17296	=	1120×15	+	496	
1120	=	496×2	+	128	
496	=	128×3	+	112	
128	=	112×1	+	16	
112	=	16×7	+	0.	Therefore, $\gcd(18416,17296)=16$.

□

Solution 17: The statement is correct, which will be proven by mathematical induction as follows.

- **Inductive Basis:** $k=1$. Under the condition $m,n\in\mathbf{N}$ and $0\leq n<m$ and because the algorithm makes one recursive call, the smallest values of m,n are 2, 1, respectively. Since $F_{k+2}=F_3=2$, and $F_{k+1}=F_2=1$, the base is proven.
- **Inductive Hypothesis:** Suppose the algorithm makes k recursive calls and $F_{k+2}\leq m, F_{k+1}\leq n$.

- **Inductive Step:** Suppose the algorithm makes $k+1$ recursive calls. After the first recursive call the new arguments are n and $m - \lfloor m/n \rfloor n$. Let

$$m' = n, \tag{6.34}$$
$$n' = m - \lfloor \frac{m}{n} \rfloor n. \tag{6.35}$$

By the assumption we know that $\gcd(m', n')$ will make k recursive calls, and by the inductive hypothesis we also know that

$$F_{k+2} \leq m', \tag{6.36}$$
$$F_{k+1} \leq n'. \tag{6.37}$$

From (6.34) and (6.36) we have $F_{k+2} \leq n$. The given condition, $n < m$, implies that $1 \leq \lfloor \frac{m}{n} \rfloor$. Thus, from (6.35) we have

$$\begin{aligned} n' \leq m - n &\implies n' + n \leq m \\ &\implies F_{k+1} + F_{k+2} \leq n' + n \leq m \implies F_{k+3} \leq m. \end{aligned}$$

□

Solution 18:

$$\gcd(375, 275) = 375x + 275y.$$

m/n	x_0/x_1	y_0/y_1	r
375	1	0	
275	0	1	1
100	1	−1	2
75	−2	3	1
25	3	−4	3
0			

Therefore, $x = 3, y = -4$. □

Solution 19: Let $x = 2p + 1, y = 2q + 1$ where $p, q \in \mathbf{Z}$. Then,

$$\begin{aligned} x^2 + y^2 &= (2p+1)^2 + (2q+1)^2 \\ &= 4p^2 + 4p + 1 + 4q^2 + 4q + 1 \\ &= 4(p^2 + p + q^2 + q) + 2 \\ &= 4K + 2 \end{aligned}$$

where $K = p^2 + p + q^2 + q$, which is an integer.

Suppose it is possible to find an integer a such that $a^2 = x^2 + y^2$. Then there are two possible cases:

case 1: $a = 2k$ for some integer k. Then $a^2 = 4k^2$, and

$$4K + 2 = 4k^2 \implies K + \frac{1}{2} = k^2.$$

This is impossible, because both K and k^2 are integers.

case 2: $a = 2k + 1$ for some integer k. Then $a^2 = 4k^2 + 4k + 1$, and

$$4K + 2 = 4k^2 + 4k + 1 \implies K + \frac{1}{4} = k^2 + k.$$

This is also impossible, because K, k, and k^2 are integers.

Therefore, $x^2 + y^2 = a^2$ is impossible. □

Solution 20: If x is not divisible by 3, then there are two cases: $x = 3p + 1$ and $x = 3p + 2$ for some integer p. Similarly, if y is not divisible by 3, there are two cases: $y = 3q + 1$ and $y = 3q + 2$. Also, integer a itself has 3 cases: $a = 3k, a = 3k + 1$, and $3k + 2$. All together, we have $2 \times 2 \times 3$ cases. The proof for each case is essentially the same. Here we just prove one case: $x = 3p + 2, y = 3q + 2, a = 3k + 2$, where $p, q, r \in \mathbf{Z}$.

$$\begin{aligned} x^2 + y^2 &= (3p + 2)^2 + (3q + 2)^2 \\ &= 9p^2 + 12p + 4 + 9q^2 + 12q + 4 \\ &= 3(3p^2 + 4p + 3q^2 + 4q) + 8 \\ &= 3K + 8 \end{aligned}$$

where $K = 3p^2 + 4p + 3q^2 + 4q$, which is an integer. Similarly,

$$\begin{aligned} a^2 &= (3k + 2)^2 \\ &= 9k^2 + 12k + 4 \\ &= 3(3k^2 + 4k) + 4 \\ &= 3K' + 4 \end{aligned}$$

where $K' = 3p^2 + 4p$, which is an integer. Therefore,

$$3K + 8 = 3K' + 4 \implies K + \frac{4}{3} = K'.$$

Since both K and k' are integers, this is impossible. □

Solution 21: Suppose that $2^n - 1$ is a prime and n is not a prime. If n is not a prime, then there exist $p, q \in \mathbf{Z}$ and $p, q \geq 2$ such that $n = pq$.

$$\begin{aligned} 2^n - 1 &= 2^{pq} - 1 \\ &= (2^p)^q - 1 \\ &= (2^p - 1)((2^p)^{q-1} + (2^p)^{q-2} + \cdots + 1). \end{aligned}$$

Because $p, q \geq 2$, both $2^p - 1$ and $(2^p)^{q-1} + (2^p)^{q-2} + \cdots + 1$ are greater than or equal to 2. Therefore, $2^n - 1$ is not a prime number, which contradicts the assumption.

The converse is wrong. Here is a counterexample: $n = 11$, which is prime. We have, $2^n - 1 = 2047 = 23 \times 89$, which is not prime. □

Solution 22: $27 \equiv 9 \pmod{m}$ means for some integer k, $(27 - 9) = km$. Therefore, we have to find all possible m such that $(27 - 9)/m$ is an integer. Nothing but the factors of 18 can satisfy the requirement. Therefore, $m \in \{1, 2, 3, 6, 9, 18\}$. □

Solution 23: In this question we seek the elements of A that have the same remainder after being divided by 3 and 7, respectively; such elements are congruent to each other.

$$\begin{aligned} 687 &= 229\times3 + 0 = \ \ 98\times7 + 1 \\ 589 &= 196\times3 + 1 = \ \ 84\times7 + 1 \\ 931 &= 310\times3 + 1 = 133\times7 + 0 \\ 847 &= 282\times3 + 1 = 121\times7 + 0 \\ 527 &= 175\times3 + 2 = \ \ 75\times7 + 2 \end{aligned}$$

Therefore,

$$\begin{aligned} &589 \equiv 931 \equiv 847 \equiv 1 \pmod{3} \\ &687 \equiv 589 \equiv 1 \pmod{7} \\ &931 \equiv 847 \equiv 0 \pmod{7} \end{aligned}$$

□

Solution 24:

We find the remainder of x after dividing by m for each pair x and m.

$$\begin{array}{rcl} x & = & k \times m \ + \ r, \\ \hline 19 & = & 9 \times 2 \ + \ 1 \\ 131 & = & 26 \times 5 \ + \ 1 \\ 84 & = & 6 \times 14 \ + \ 0 \\ 141 & = & 8 \times 17 \ + \ 5 \end{array}$$

Therefore,

$$\begin{aligned} 19 &\equiv 1 \pmod 2 \\ 131 &\equiv 1 \pmod 5 \\ 84 &\equiv 0 \pmod{14} \\ 141 &\equiv 5 \pmod{17} \end{aligned}$$

□

Solution 25:

1. To solve $5x \equiv 9 \pmod{17}$, we first note that $\gcd(5, 17) = 1$. Clearly, $\gcd(5, 17)|9$, and hence the given congruence equation has a solution. Using the extended Euclid's algorithm, one may have

   $$\gcd(5, 17) = 1 = 5 \times 7 + 17 \times (-2).$$

   Thus, $x_0 = 7 \times 9 = 63$ is a solution. Moreover, $\text{lcm}(5, 17)/5 = 17$. Thus, $\overline{\lfloor 63 \rfloor}_{17}$, or equivalently, $\overline{\lfloor 12 \rfloor}_{17}$ is the set of all solutions.

2. $18y \equiv 8 \pmod{15}$ has no solution, because $\gcd(18, 15) = 3 \not| \, 8$.

3. $12z \equiv 15 \pmod{42}$ has no solution, because $\gcd(12, 42) = 6 \not| \, 15$.

□

Solution 26: Let $a^n \equiv 1 \pmod m$. Therefore, $a^n - 1 = km$ for some $k \in \mathbf{N}$.

$$\begin{aligned} a^n - km = 1 \Rightarrow \ & (a^{n-1})a + (-k)m = 1 \\ \Rightarrow \ & \gcd(a, m) = 1, \quad \text{by Theorem 6.12} \end{aligned}$$

□

Solution 27: Given a set of integers of size m, the easiest way to see whether the given set is a complete residue system modulo m is to use the division algorithm to find the remainder for each element divided by m. If the remainders cover all of the integers in

$$\{0, 1, 2, \ldots, m-1\},$$

then the given set is a complete residue system modulo m. In other words, if we find that two of them have the same remainder, then the given set is not a complete residue system modulo m, because we need m distinct equivalence classes to cover the entire $\mathbf{Z}$. Therefore, this problem is simply to find the remainders and check them. By using the division algorithm, we know,

$$\begin{array}{lll} 19 \in \underline{\lfloor 1 \rfloor}_6 & 8 \in \underline{\lfloor 2 \rfloor}_6 & -3 \in \underline{\lfloor 3 \rfloor}_6 \\ -5 \in \underline{\lfloor 1 \rfloor}_6 & 10 \in \underline{\lfloor 4 \rfloor}_6 & 5 \in \underline{\lfloor 5 \rfloor}_6 \end{array}$$

Therefore, $\{19, 8, -3, -5, 10, 5\}$ is not a complete residue system modulo 6, because $\underline{\lfloor 19 \rfloor}_6 = \underline{\lfloor -5 \rfloor}_6$. □

Solution 28: We want to prove that if $s \in \mathbf{Z}$, then

$$\mathbf{Z} = \bigcup_{c \in C} \underline{\lfloor c \rfloor}_m \quad \Longrightarrow \quad \mathbf{Z} = \bigcup_{c \in C} \underline{\lfloor c + s \rfloor}_m$$

Let $k \in \mathbf{Z}$. Since C is a complete residue system modulo m, if $s \in \mathbf{Z}$, then

$$\begin{aligned} k - s \in \mathbf{Z} \quad &\Rightarrow \exists c \in C, k - s \in \underline{\lfloor c \rfloor}_m \\ &\Rightarrow k - s \equiv c \pmod{m} \end{aligned}$$

Such a c must exist because C is a complete system of residues mod m. By the properties stated in Theorem 6.18 and the fact that $s \equiv s \pmod{m}$, we have

$$\begin{aligned} (k - s) + s &\equiv c + s \pmod{m} \\ k &\equiv c + s \pmod{m} \\ k &\in \underline{\lfloor c + s \rfloor}_m \end{aligned}$$

That means,

$$\forall k \in \mathbf{Z}, \exists \mu \in (C + s), k \in \underline{\lfloor c + s \rfloor}_m$$

where $\mu = c + s$. Therefore, $C + s$ is a complete residue system modulo m. □

Solution 29: There are many ways to find the least positive residue of $(15)^{35}$ mod 19. We can use Theorem 6.18 directly to solve this problem. In the following reduction we use the facts that $225 \equiv 16 \pmod{19}$, $256 \equiv 9 \pmod{19}$, etc.

$$\begin{aligned} 15^{35} = 15^{2\cdot 17+1} = 225^{17} \cdot 15 &\equiv 16^{17} \cdot 15 = (16^2)^8 \cdot 16 \cdot 15 = 256^8 \cdot 240 \\ &\equiv 9^8 \cdot 12 = 81^4 \cdot 12 \\ &\equiv 5^4 \cdot 12 = 25^2 \cdot 12 \\ &\equiv 6^2 \cdot 12 = 36 \cdot 12 \\ &\equiv 17 \cdot 12 = 204 \\ &\equiv 14 \pmod{19} \end{aligned}$$

Alternatively, we can use Fermat's theorem. We observe that 15 and 19 are relative primes and $35 \geq 19$. If we take $p = 19, a = 15$, we get

$$15^{18} \equiv 1 \pmod{19}.$$

This removes a big exponent of 15, and the rest of the exponent can be simplified as before:

$$\begin{aligned} 15^{35} = 15^{18} \cdot 15^{17} &\equiv 1 \cdot 15^{17} = (15^2)^8 \cdot 15 = 225^8 \cdot 15 \\ &\equiv 16^8 \cdot 15 = 2^{32} \cdot 15 = 2^{18} \cdot 2^{14} \cdot 15 \\ &\equiv 1 \cdot 2^{14} \cdot 15 = 64^2 \cdot 60 \\ &\equiv 7^2 \cdot 3 \\ &\equiv 11 \cdot 3 \\ &\equiv 14 \pmod{19} \end{aligned}$$

□

Solution 30: Observe that 29 and 17 are relative primes and $36 \geq 17$. By Fermat's theorem $(29)^{16} \mod 17 \equiv 1$ and $29^{36} = (29^2)^{16} \cdot 29^4$. Since $29 = 12 \mod 17$, we get

$$\begin{aligned} 29^4 &\equiv 1 \cdot 12^4 = 144^2 \\ &\equiv 8^2 = 64 \\ &\equiv 13 \pmod{17} \end{aligned}$$

□

Solution 31: From the definition of the complete system of residues mod m we obtain the following result.

Result: Let S be a set of integers with size m. S is a complete system of residues mod m if and only if no two elements in S are congruent mod m to each other.

The proof of this result, left as an exercise, can be obtained by an application of the pigeonhole principle.

Let $\{a_0, \ldots, a_{m-1}\}$ be a complete system of residues mod m. Let $0 \le i, j < m, i \ne j$, t relatively prime to m, and $\lfloor ta_i \rfloor_m = \lfloor ta_j \rfloor_m$. Then it follows that

$$\begin{aligned} ta_i \equiv ta_j \pmod{m} &\Rightarrow ta_i - ta_j = km \text{ for some } k \in \mathbf{Z} \\ &\Rightarrow t(a_i - a_j) = km \text{ for some } k \in \mathbf{Z} \\ &\Rightarrow m | t(a_i - a_j) \\ &\Rightarrow m | (a_i - a_j) \text{ because } \gcd(t, m) = 1 \\ &\Rightarrow a_i - a_j = km \text{ for some } k \in \mathbf{Z} \\ &\Rightarrow \lfloor a_i \rfloor_m = \lfloor a_j \rfloor_m \end{aligned}$$

This is a contradiction, because $\{a_0, \ldots, a_{m-1}\}$ is a complete system of residues mod m, and from the corollary we know that $\lfloor a_i \rfloor_m \ne \lfloor a_j \rfloor_m$ if and only if $a_i \ne a_j$. Therefore, the assumption that $\lfloor ta_i \rfloor_m = \lfloor ta_j \rfloor_m$ is wrong. □

Solution 32: The number of days between December 1, 1976, and July 1, 1987, is 3864, which is $552 \cdot 7$. If the number of days is a multiple of 7, then the two months have the same monthly calendar. Therefore, December 1976 and July 1987 share the same monthly calendar. Try `cal 1976` and `cal 1987` on Unix. □

Solution 33: $f(x) = 13x^3 - 5x^2 + 14x - 10$.

We will use the following congruent relations:

$$\begin{aligned} 13 \equiv 6 \equiv -1 &\pmod{7} \\ 12 \equiv 5 \equiv -2 &\pmod{7} \\ 14 \equiv 0 &\pmod{7} \end{aligned}$$

Therefore,

$$\begin{aligned} f(12) &\equiv 13 \cdot 12^3 - 5 \cdot 12^2 + 14 \cdot 12 - 10 \\ &\equiv 6 \cdot (-2)^3 - (-2) \cdot (-2)^2 + 0 - 3 \pmod{7} \\ &= -48 + 8 - 3 = -43 \\ &\equiv 6 \pmod{7} \end{aligned}$$

□

Solution 34: Recall Theorem 6.6 stating that, for any $a, b, x, y \in \mathbf{Z}$, $\gcd(a, b) \mid (xa + yb)$.

Let $m \geq 1, a, x \in \mathbf{Z}$. We want to prove that

$$x \in \underline{\lfloor a \rfloor}_m \Longrightarrow \quad \gcd(x, m) = \gcd(a, m).$$

If $x \in \underline{\lfloor a \rfloor}_m$, we know $x - a = km$ for some $k \in \mathbf{Z}$. Therefore,

$$x + (-k)m = a \tag{6.38}$$

$$a + km = x. \tag{6.39}$$

Let $\gcd(x, m) = d$ and $\gcd(a, m) = d'$, thus $d|m$ and $d'|m$. From (6.38) we know a is a linear combination of x and m. Thus, $d|a$ and

$$d|a, d|m \implies d|\gcd(a, m) \implies d|d'. \tag{6.40}$$

Similarly, from (6.39), we have $d'|x$ and

$$d'|x, d'|m \implies d'|\gcd(x, m) \implies d'|d. \tag{6.41}$$

Therefore, $d = d'$ and $\gcd(x, m) = \gcd(a, m)$. □

Solution 35: (i)

$$\begin{aligned} 2^{14} &\equiv (2^4)^3 \cdot 2^2 = 16^3 \cdot 4 \\ &\equiv (-1)^3 \cdot 4 = -4 \\ &\equiv 13 \qquad\qquad (\text{mod } 17) \end{aligned}$$

(ii) We use Fermat's little theorem for this problem,

$$3^{(100)} \equiv (3^{25})^4 \equiv 1 \pmod 5,$$

because 5 is a prime and $5 \nmid 3^{25}$. □

Solution 36:

- To solve

$$\begin{aligned} x &\equiv 3 \pmod 5 \\ x &\equiv 2 \pmod 6 \\ x &\equiv 3 \pmod 7 \end{aligned}$$

we first note that 5, 6, and 7 are relatively prime to each other. Therefore, we can use the Chinese Remainder Algorithm to find the solutions.

Let $M = 5 \cdot 6 \cdot 7 = 210$. We first solve the following equations separately.

$$\begin{aligned} c_1 \cdot \frac{M}{5} &\equiv 1 \pmod 5 \\ c_2 \cdot \frac{M}{6} &\equiv 1 \pmod 6 \\ c_3 \cdot \frac{M}{7} &\equiv 1 \pmod 7 \end{aligned}$$

That is,

$$\begin{cases} c_1 \cdot 42 \equiv 1 \pmod 5 \\ c_2 \cdot 35 \equiv 1 \pmod 6 \\ c_3 \cdot 30 \equiv 1 \pmod 7 \end{cases} \Rightarrow \begin{cases} c_1 \in \underline{\lfloor 3 \rfloor}_5 \\ c_2 \in \underline{\lfloor 5 \rfloor}_6 \\ c_3 \in \underline{\lfloor 4 \rfloor}_7 \end{cases}$$

After we get one solution for each c_1, c_2, and c_3, we can find our first solution, x_0, for the simultaneous congruence,

$$\begin{aligned} x_0 &= c_1 \cdot 42 \cdot 3 + c_2 \cdot 35 \cdot 2 + c_3 \cdot 30 \cdot 3 \\ &= 3 \cdot 42 \cdot 3 + 5 \cdot 35 \cdot 2 + 4 \cdot 30 \cdot 3 \\ &= 1088 \end{aligned}$$

Therefore, the solution set is $\underline{\lfloor 1088 \rfloor}_{210}$ or equivalently, $x \in \underline{\lfloor 38 \rfloor}_{210}$

- To solve

$$\begin{aligned} y &\equiv 2 \pmod 5 \\ y &\equiv 7 \pmod{13} \\ y &\equiv 11 \pmod 8 \end{aligned}$$

we first check and witness that 5, 13, and 8 are relatively prime to each other. Let $M = 5 \cdot 13 \cdot 18 = 520$. First, we solve the following equations separately.

$$\begin{aligned} c_1 \cdot \frac{M}{5} &\equiv 1 \pmod 5 \\ c_2 \cdot \frac{M}{13} &\equiv 1 \pmod{13} \\ c_3 \cdot \frac{M}{8} &\equiv 1 \pmod 8 \end{aligned}$$

That is,

$$\begin{cases} c_1 \cdot 104 \equiv 1 \pmod 5 \\ c_2 \cdot 40 \equiv 1 \pmod{13} \\ c_3 \cdot 65 \equiv 1 \pmod 8 \end{cases} \Rightarrow \begin{cases} c_1 \in \underline{\lfloor -1 \rfloor}_5 \\ c_2 \in \underline{\lfloor 1 \rfloor}_{13} \\ c_3 \in \underline{\lfloor 1 \rfloor}_8 \end{cases}$$

Then we can find a solution y_0,

$$\begin{aligned} y_0 &= c_1 \cdot 104 \cdot 2 + c_2 \cdot 40 \cdot 7 + c_3 \cdot 65 \cdot 11 \\ &= -1 \cdot 104 \cdot 2 + 1 \cdot 40 \cdot 7 + 1 \cdot 65 \cdot 11 \\ &= 787 \equiv 267 \pmod{520} \end{aligned}$$

Therefore, the solution set is $\boxed{\lfloor 267 \rfloor}_{520}$

- To solve,

$$\begin{aligned} z &\equiv 7 \pmod{16} \\ z &\equiv 1 \pmod{9} \\ z &\equiv 2 \pmod{25} \end{aligned}$$

we first make sure that 16, 9, and 25 are relatively prime to each other. Let $M = 16 \cdot 9 \cdot 25 = 3600$, and solve the following equations separately.

$$\begin{aligned} c_1 \cdot \frac{M}{16} &\equiv 1 \pmod{16} \\ c_2 \cdot \frac{M}{9} &\equiv 1 \pmod{9} \\ c_3 \cdot \frac{M}{25} &\equiv 1 \pmod{25} \end{aligned}$$

That is,

$$\begin{cases} c_1 \cdot 225 \equiv 1 \pmod{16} \\ c_2 \cdot 400 \equiv 1 \pmod{9} \\ c_3 \cdot 144 \equiv 1 \pmod{25} \end{cases} \Rightarrow \begin{cases} c_1 \in \boxed{\lfloor 1 \rfloor}_{16} \\ c_2 \in \boxed{\lfloor -2 \rfloor}_{9} \\ c_3 \in \boxed{\lfloor 4 \rfloor}_{25} \end{cases}$$

$$\begin{aligned} z_0 &= c_1 \cdot 225 \cdot 7 + c_2 \cdot 400 \cdot 1 + c_3 \cdot 144 \cdot 2 \\ &= 1927 \pmod{3600} \end{aligned}$$

Therefore, the solution set is $\boxed{\lfloor 1927 \rfloor}_{3600}$

□

Solution 37: Observe that 7 is a prime number, and 7 cannot divide 2^q for any positive integer q. Thus, we can make use of Fermat's little theorem and

$$(2^q)^6 \equiv 1 \pmod{7} \text{ for any integer } q \geq 1.$$

Moreover, by the division algorithm we know that for any positive integer m, there are unique q and r such that

$$m = 6q + r \quad 0 \leq r < 6.$$

Therefore, for $m \geq 0$ and $\alpha = 1, 2, 4$, we get $2^m - \alpha \equiv 2^{6q+r} - \alpha \equiv 2^{6q}2^r - \alpha \equiv (2^r - \alpha) \pmod 7$. Consequently, $(2^m - 1)(2^m - 2)(2^m - 4) \equiv (2^r - 1)(2^r - 2)(2^r - 4) \pmod 7$. Therefore, we only have to prove that for each possible r the later polynomial is 0. For any integer r, $0 \leq r \leq 6$, one of the factors of the above equation is 0, e.g., if $r = 4$, then $2^r - 2 = 16 - 2 = 14 = 0 \pmod 7$.

Therefore, in all cases $(2^m - 1)(2^m - 2)(2^m - 4) \equiv 0 \pmod 7$.

Alternatively, we can expand the polynomial and apply Fermat's theorem:

$$\begin{aligned} & (2^m - 1)(2^m - 2)(2^m - 4) \\ = \; & (2^{2m} - 3 \cdot 2^m + 2)(2^m - 4) \\ = \; & 2^{3m} - 3 \cdot 2^{2m} + 2 \cdot 2^m - 4 \cdot 2^{2m} + 12 \cdot 2^m - 8 \\ = \; & 8^m - 7 \cdot 2^{2m} + 14 \cdot 2^m - 8 \\ \equiv \; & 1^m - 0 \cdot 2^{2m} + 0 \cdot 2^m - 1 \pmod 7 \\ \equiv \; & 0 \pmod 7 \end{aligned}$$

□

Solution 38: We can use Fermat's little theorem to solve this problem easily. We observe that 7 is a prime number and for any positive integer k, $7 \not| 3^k$ and $7 \not| 4^k$, and by Fermat's little theorem, $3^6 \equiv 4^6 \equiv 1 \pmod 7$. Given any integer n, by using the division algorithm we can find unique p and r such that $n = 6p + r$, where $0 \leq r < 6$.

$$\begin{aligned} 3^n + 4^n = \; & 3^{6p+r} + 4^{6p+r} \\ = \; & (3^p)^6 3^r + (4^p)^6 4^r \\ \equiv \; & 1 \cdot 3^r + 1 \cdot 4^r \pmod 7 \\ \equiv \; & 3^r + 4^r \pmod 7 \end{aligned}$$

Therefore, n is a solution of

$$3^n + 4^n \equiv 0 \pmod 7$$

if and only if r is a solution of

$$3^r + 4^r \equiv 0 \pmod 7.$$

In other words, if r is a solution, so is any element in $\boxed{r}_6$. Let's check all possible r:

$r = 0$: $3^0 + 4^0 = 2 \not\equiv 0 \pmod 7$.

$r = 1$: $3^1 + 4^1 = 7 \equiv 0 \pmod 7$.

$r = 2$: $3^2 + 4^2 = 25 \not\equiv 0 \pmod 7$.

$$r = 3: \quad 3^3 + 4^3 \equiv 2 \cdot 3 + 2 \cdot 4 \equiv 0 \pmod 7.$$

$$r = 4: \quad 3^4 + 4^4 \equiv 2^2 + 2^2 \not\equiv 0 \pmod 7.$$

$$r = 5: \quad 3^5 + 4^5 \equiv 12 + 16 \equiv 0 \pmod 7.$$

Therefore, the solutions are

$$x \in \boxed{1}_6 \bigcup \boxed{3}_6 \bigcup \boxed{5}_6 .$$

□

Solution 39: Given any positive integers m and n, let R_m and R_n be two partitions of $\mathbf{Z}$ given by congruences mod m and n respectively. That is,

$$R_m = \left\{\boxed{0}_m, \boxed{1}_m, \cdots, \boxed{m-1}_m\right\}$$
$$R_n = \left\{\boxed{0}_n, \boxed{1}_n, \cdots, \boxed{n-1}_n\right\}$$

We want to prove that

$$R_m \text{ is a refinement of } R_n \iff m = kn, k \in \mathbf{Z}.$$

1. ($\Longleftarrow$) Suppose $m = kn$ for some integer k. Consider any $\boxed{i}_m \in R_m$. We want to prove that there exists a $\boxed{j}_n \in R_n$ such that $\boxed{i}_m \subseteq \boxed{j}_n$. Let $x, y \in \boxed{i}_m$ and $x \neq y$. Consequently, $x \equiv y \pmod m$, or in other words, $x - y = qm$ for some $q \in \mathbf{Z}$. Substituting for $m = kn$, we get $x - y = qkn$ or $x \equiv y \pmod n$. Thus, $x, y \in \boxed{j}_n$ where $\boxed{j}_n \in R_n$ and R_m is a refinement of R_n. (Think why do we need two elements, x and y, in the above proof?)

2. ($\Longrightarrow$) Suppose R_m is a refinement of R_n. Let $\boxed{i}_m \in R_m, \boxed{j}_n \in R_n$, and $\boxed{i}_m \subseteq \boxed{j}_n$. It is clear that $i \in \boxed{i}_m$ and $j \in \boxed{j}_n$.

$$(i \in \boxed{i}_m, \boxed{i}_m \subseteq \boxed{j}_n) \Longrightarrow i \in \boxed{j}_n$$

Therefore, $i \equiv j \pmod n$, and hence $\boxed{i}_n = \boxed{j}_n$. Moreover,

$$\begin{aligned} i + m \in \boxed{i}_m &\Rightarrow i + m \in \boxed{j}_n \text{ because } \boxed{i}_m \subseteq \boxed{j}_n \\ &\Rightarrow i + m \in \boxed{i}_n \text{ because } \boxed{j}_n = \boxed{i}_n \\ &\Rightarrow i + m \equiv i \pmod n \\ &\Rightarrow i + m - i = kn, \ k \in \mathbf{Z} \\ &\Rightarrow m = kn, \ k \in \mathbf{Z} \end{aligned}$$

Therefore, R_m is a refinement of R_n iff $m = kn$ for some integer k. □

Solution 40: We prove this problem by mathematical induction on k.

- **Inductive Basis:** For $k = 0$, $a_0 = 0 \equiv 0 \pmod 5$.
- **Inductive Hypothesis:** Assume $a_{5k} \equiv 0 \pmod 5$.
- **Inductive Step:** We want to prove that $a_{5(k+1)} \equiv 0 \pmod 5$. Towards this goal we repeatedly use $a_n = a_{n-1} + a_{n-2}$ to expand $a_{5(k+1)}$ in the following equalities:

$$\begin{aligned}
a_{5(k+1)} &= a_{5k+5} \\
&= a_{5k+3} + a_{5k+4} \\
&= a_{5k+1} + a_{5k+2} + a_{5k+2} + a_{5k+3} \\
&= a_{5k+1} + 2a_{5k+2} + a_{5k+3} \\
&= a_{5k+1} + 2a_{5k+2} + a_{5k+1} + a_{5k+2} \\
&= 2a_{5k+1} + 3a_{5k+2} \\
&= 2a_{5k+1} + 3(a_{5k} + a_{5k+1}) \\
&= 3a_{5k} + 5a_{5k+1} \\
&\equiv 0 + 0 \pmod 5 \\
&\equiv 0 \pmod 5
\end{aligned}$$

Therefore, for all $k \geq 0$, $a_{5k} \equiv 0 \pmod 5$. □

Solution 41:

$$\begin{aligned}
\varphi(18) &= \varphi(2 \cdot 3^2) \\
&= \varphi(2)\varphi(3^2) \\
&= 1 \cdot (3^2 - 3^1) \\
&= 6.
\end{aligned}$$

$$\begin{aligned}
\varphi(40) &= \varphi(2^3 \cdot 5) \\
&= \varphi(2^3)\varphi(5) \\
&= (2^3 - 2^2) \cdot 4 \\
&= 16.
\end{aligned}$$

$$\begin{aligned}
\varphi(72) &= \varphi(2^3 \cdot 3^2) \\
&= \varphi(2^3)\varphi(3^2) \\
&= (2^3 - 2^2) \cdot (3^2 - 3) \\
&= 24.
\end{aligned}$$

□

Solution 42:

By Euler's Theorem if $\gcd(a, m) = 1$, then $a^{\varphi(m)} \equiv 1 \pmod{m}$. By Theorem 6.23, if $a \equiv b \pmod{m_1}$ and $a \equiv b \pmod{m_2}$, then $a \equiv b \pmod{\text{lcm}(m_1, m_2)}$.

Using $75 = 3 \cdot 5^2$ we can apply Theorem 6.23. Note that $\varphi(5^2) = (5^2 - 5) = 20$. Since 5 is a prime and $\gcd(2, 5) = 1$, by Euler's theorem we have

$$2^{\varphi(5^2)} \equiv 1 \pmod{5^2} \Rightarrow 2^{20} \equiv 1 \pmod{25}$$

Since 3 is a prime, and 3 cannot divide 2^{10}, then by Fermat's theorem we have

$$(2^{10})^2 \equiv 1 \pmod{3} \Rightarrow \quad 2^{20} \equiv 1 \pmod{3} \tag{6.42}$$

Because $\text{lcm}(3, 25) = 75$, by Theorem (6.23) we have $(2^{10})^2 \equiv 1 \pmod{75}$. Therefore, $2^{20} \equiv 1 \pmod{75}$. □

Solution 43: Given any integer $m \geq 1$, we can factor m into a product of prime numbers:

$$m = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}.$$

Thus,

$$\begin{aligned}
\varphi(m) &= \varphi(p_1^{e_1} p_2^{e_2} \dots p_n^{e_n}) \\
&= \varphi(p_1^{e_1})\varphi(p_2^{e_2}) \dots \varphi(p_n^{e_n}) \\
&= (p_1^{e_1} - p_1^{e_1 - 1})(p_2^{e_2} - p_1^{e_2 - 1}) \dots (p_n^{e_n} - p_n^{e_n - 1}) \\
&= p_1^{e_1}(1 - \frac{1}{p_1}) p_2^{e_2}(1 - \frac{1}{p_2}) \dots p_n^{e_n}(1 - \frac{1}{p_n}) \\
&= m \prod_{p|m} (1 - \frac{1}{p}).
\end{aligned}$$

Comment: In $\prod_{p|m}(1 - \frac{1}{p})$ it is better to let m range over all integers greater but not equal to 1, unless we define $\prod \emptyset = 1$.

□

Solution 44: (i) If n is odd, then $\gcd(2, n) = 1$. Therefore,

$$\varphi(2n) = \varphi(2)\varphi(n) = 1 \cdot \varphi(n) = \varphi(n).$$

□

(ii) Because $n \geq 1$, we know $\varphi(n) \neq 0$. Let's discuss it in cases.

Case 1: $\gcd(3, n) = 1$.

$$\varphi(3n) = \varphi(3)\varphi(n) = 2 \cdot \varphi(n) \neq \varphi(n).$$

Case 2: $\gcd(3, n) \neq 1$.

Because 3 is a prime number, if $\gcd(3, n) \neq 1$, then $3|n$. Let $n = 3^k m$, where $k \geq 1$ and $\gcd(3, m) = 1$.

$$\begin{aligned}\varphi(n) &= \varphi(3^k m) \\ &= \varphi(3^k)\varphi(m) \\ &= (3^k - 3^{k-1})\varphi(m).\end{aligned}$$

$$\begin{aligned}\varphi(3n) &= \varphi(3^{k+1} m) \\ &= \varphi(3^{k+1})\varphi(m) \\ &= (3^{k+1} - 3^k)\varphi(m).\end{aligned}$$

Because $(3^k - 3^{k-1}) \neq (3^{k+1} - 3^k)$, therefore $\varphi(n) \neq \varphi(3n)$.

In both cases, $\varphi(n) \neq \varphi(3n)$. □

(iii) If n is even, then we can present n as $2^k m$, where $k \geq 1$ and $\gcd(2, m) = 1$.

$$\begin{aligned}\varphi(2n) &= \varphi(2 \cdot 2^k m) \\ &= \varphi(2^{k+1})\varphi(m) \\ &= (2^{k+1} - 2^k)\varphi(m).\end{aligned}$$

$$\begin{aligned}2\varphi(n) &= 2\varphi(2^k m) \\ &= 2\varphi(2^k)\varphi(m) \\ &= 2(2^k - 2^{k-1})\varphi(m) \\ &= (2^{k+1} - 2^k)\varphi(m).\end{aligned}$$

Therefore, $\varphi(2n) = 2\varphi(n)$. □

Solution 45: Any integer $n \geq 1$ can be represented as a product of prime numbers, $n = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$, and

$$\varphi(n) = \varphi(p_1^{e_1})\varphi(p_2^{e_2}) \cdots \varphi(p_n^{e_n}).$$

Thus, we find all possible combinations of $p_1^{e_1}, p_2^{e_2}, \ldots, p_n^{e_n}$ that make $\varphi(n) = 8$.

To do this, let's list the values of $\varphi(p_i^{e_1})$ in a systematic manner:

$$\begin{array}{llll} \varphi(2)=1 & \varphi(2^2)=2 & \varphi(2^3)=4 & \varphi(2^4)=8 \\ \varphi(3)=2 & \varphi(3^2)=6 & \varphi(3^3)=18 & \cdots \\ \varphi(5)=4 & \varphi(5^2)=20 & \cdots & \\ \varphi(7)=6 & \varphi(7^2)=42 & \cdots & \\ \varphi(11)=10 & \cdots & & \end{array}$$

Although φ is not a monotone increasing function, integers in each column representing $\lambda p \cdot \varphi(p^e)$ are monotone increasing. Likewise, integers in each row representing $\lambda e \cdot \varphi(p^e)$ are monotone increasing. Here p ranges over prime numbers and e over natural numbers. Therefore, we don't have to consider the p and e where $\varphi(p^e)$ is greater than 8.

It is not difficult to search the table and find that there are only 5 possible numbers that satisfy the desired property:

$$\begin{aligned} \varphi(2)\varphi(3)\varphi(5)=8 \quad & n=30 \\ \varphi(2^2)\varphi(5)=8 \quad & n=20 \\ \varphi(2^3)\varphi(3)=8 \quad & n=24 \\ \varphi(2^4)=8 \quad & n=16 \\ \varphi(3)\varphi(5)=8 \quad & n=15. \end{aligned}$$

Therefore, for $n \in \{30, 20, 24, 16, 15\}$, $\varphi(n) = 8$. □