Congruences

We study the basic facts concerning congruences in this chapter. After introducing the notion of congruence, we investigate residue classes, residue systems, and Euler's function φ. We prove the theorems of Euler–Fermat and Wilson, using linear congruences for the latter one. Related to linear congruences, we treat also simultaneous systems of congruences. We shall learn more about congruences in Chapters 3 and 4.

2.1. Elementary Properties

We often see in divisibility problems that only the remainder matters, i.e. two integers behave identically if their remainders are the same. This (too) underlines the introduction of the notion below:

Definition 2.1.1. Let a and b be integers and m a positive integer. We say that a is *congruent* to b modulo m if $m \mid a - b$. ♣

Notation: $a \equiv b \pmod{m}$ or just $a \equiv b\ (m)$. The number m is called the *modulus* and is kept fixed, in general. As $m \mid a - b$ if and only if $m \mid b - a$, therefore

$$a \equiv b \pmod{m} \iff b \equiv a \pmod{m},$$

and so we may say also that "a and b are congruent modulo m". (Instead of "modulo m", we can use the expressions "mod m," or "with respect to the modulus m," or "related to the modulus m," as well.)

Clearly, a and b are congruent modulo m if and only if a and b give the same (least non-negative) remainder when they are divided by m. (The same holds for the remainder of least absolute value.)

If a and b are not congruent modulo m, we write $a \not\equiv b \pmod{m}$, and we say that a and b are *incongruent* modulo m (or a is incongruent to b modulo m).

Example. $11 \equiv 5 \pmod{3}$, $32 \equiv -1 \pmod{11}$, $21 \not\equiv 6 \pmod{10}$.

Clearly, any two integers are congruent with respect to the modulus $m = 1$.

The definition of congruence can trivially be extended for $m < 0$, but we can ignore it since $m \mid a - b$ if and only if $-m \mid a - b$.

Theorem 2.1.2. (i) $a \equiv a \pmod{m}$ *for every* a.

(ii) $a \equiv b \pmod{m} \Longrightarrow b \equiv a \pmod{m}$.

(iii) $a \equiv b \pmod{m}$ *and* $b \equiv c \pmod{m} \Longrightarrow a \equiv c \pmod{m}$.

(iv) $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m} \Longrightarrow a + c \equiv b + d \pmod{m}$ *and* $a - c \equiv b - d \pmod{m}$.

(v) $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m} \Longrightarrow ac \equiv bd \pmod{m}$. ♣

Proof. All the assertions follow easily from the definition of congruence and the elementary properties of divisibility, hence we verify only property (v) as an illustration.

We rewrite the assumptions as $m \mid a - b$ and $m \mid c - d$ which imply

$$m \mid c(a - b) + b(c - d) = ac - bd, \quad \text{so} \quad ac \equiv bd \pmod{m}. \qquad \square$$

Properties (i), (ii), and (iii) express that congruence is *reflexive*, *symmmetric*, and *transitive*, hence it is an *equivalence relation*. We can thus divide the integers into (pairwise) disjoint sets of numbers congruent to each other, i.e. those that give the same remainder when divided by m. (Properties (i)–(iii) guarantee that the expression "congruent to each other" makes sense.) These sets are called *residue classes* modulo m. We shall study them in Section 2.2.

By (iv) and (v), congruences (with the same modulus) can be added, subtracted, and multiplied. This implies immediately that we can add the same number to both sides of a congruence, and this holds also for subtraction and multiplication. Further, a congruence can be multiplied by itself arbitrarily many times, so we may raise a congruence to a power with a positive integer exponent:

(vi) $a \equiv b \pmod{m} \Longrightarrow a + c \equiv b + c \pmod{m}$ and $a - c \equiv b - c \pmod{m}$.

(vii) $a \equiv b \pmod{m} \Longrightarrow ac \equiv bc \pmod{m}$.

(viii) $a \equiv b \pmod{m} \Longrightarrow a^n \equiv b^n \pmod{m}$.

The repeated application of these relations yields the useful law:

(ix) Let f be a polynomial with integer coefficients. Then

$$a \equiv b \pmod{m} \Longrightarrow f(a) \equiv f(b) \pmod{m}.$$

We illustrate the efficiency of the above rules with a few examples.

Examples. **E1** Demonstrate that any natural number n satisfies

$$17 \mid 3^{3n+1}5^{2n+1} + 2^{5n+1}11^n.$$

Solution: We have to show

$$3^{3n+1}5^{2n+1} + 2^{5n+1}11^n \equiv 0 \pmod{17}.$$

We replace the left-hand side with congruent expressions till we obtain 0:

$$\begin{aligned} 3^{3n+1}5^{2n+1} + 2^{5n+1}11^n &= 3 \cdot 27^n \cdot 5 \cdot 25^n + 2 \cdot 32^n \cdot 11^n \equiv \\ &\equiv 15(-7)^n 8^n + 2(-2)^n(-6)^n = \\ &= 15(-56)^n + 2(12)^n \equiv 15(-5)^n + 2(-5)^n = \\ &= 17(-5)^n \equiv 0 \pmod{17}. \end{aligned}$$

E2 Give a new proof for the divisibility $a - b \mid a^n - b^n$.

Solution: Clearly, we can restrict ourselves to the case $a - b > 0$. Applying (viii), we have

$$a \equiv b \pmod{a-b} \Longrightarrow a^n \equiv b^n \pmod{a-b}.$$

E3 Verify that $2^{32}+1$ is a composite number. (Cf. with Exercise 1.4.4 and Section 5.2.)

Solution: We establish the divisibility $641 \mid 2^{32} + 1$ relying on

$$641 = 5^4 + 2^4 = 5 \cdot 2^7 + 1.$$

We infer

$$-1 \equiv 5 \cdot 2^7 \pmod{641} \quad \text{and} \quad 5^4 \equiv -2^4 \pmod{641}.$$

Raising the first congruence to the fourth power and substituting the result into the second one, we obtain

$$1 = (-1)^4 \equiv 5^4 \cdot 2^{28} \equiv -2^4 \cdot 2^{28} = -2^{32} \pmod{641},$$

so $641 \mid 2^{32} + 1$.

We have seen that concerning addition, subtraction, and multiplication, congruences behave like equalities. There is a big difference for division, however; two congruences **must not** be divided. First of all, the results of the divisions are not always integers, and then the congruence between the fractional quotients makes no sense since only integers can appear in congruences. But even if the quotients are integers, the congruence obtained after the division will not necessarily be true. For example,

$$28 \equiv 46 \pmod 6 \quad \text{and} \quad 2 \equiv 2 \pmod 6 \quad \text{but} \quad 14 \not\equiv 23 \pmod 6.$$

Concerning division of congruences, we should be aware that also a fraction means a division. Therefore we must not replace the numerator or denominator of a fraction with an integer value even when the new fraction is an integer. E.g.

$$45 \equiv 35 \pmod{10} \quad \text{and} \quad 15 \equiv 5 \pmod{10} \quad \text{but} \quad 3 = \frac{45}{15} \not\equiv \frac{35}{5} = 7 \pmod{10}.$$

After clarifying what is forbidden, let us see what we are allowed to do. We shall deal only with the special case when division is just cancellation. The following theorem states that in performing the cancellation, we *have to change the modulus*:

Theorem 2.1.3. *Let $d = (c, m)$. Then $ac \equiv bc \pmod m$ if and only if $a \equiv b \left(\bmod \frac{m}{d}\right)$.* ♣

Proof. By the definition of congruence, we have

$$ac \equiv bc \pmod{m} \iff m \mid (a-b)c,$$

which is equivalent to the divisibility

$$\frac{m}{d} \,\Big|\, (a-b)\frac{c}{d}. \tag{2.1.1}$$

Since $(m/d, c/d) = 1$, (2.1.1) holds if and only if

$$\frac{m}{d} \,\Big|\, a-b, \quad \text{i.e.} \quad a \equiv b \left(\text{mod } \frac{m}{d}\right). \qquad \square$$

An important special case of Theorem 2.1.3 is when c and the modulus are coprime. Then the congruence remains valid with the same modulus after cancellation by c:

Theorem 2.1.3A.

$$ac \equiv bc \pmod{m},\ (c,m) = 1 \Longrightarrow a \equiv b \pmod{m}.$$

Exercises 2.1

1. Prove $23 \mid 61^{k+1} + 11^k 7^{2k} 3^{3k} 2^{5k+3}$.

2. What are the last three digits of $999^{777^{888}}$ (in decimal representation)?

3. Give a new proof using congruences for the divisibility rules by 9 and 11 (Exercise 1.1.14) and for their generalizations in other number systems (Exercise 1.2.14).

4. True or false?

   (a) $k \mid n,\ a \equiv b \pmod{n} \Longrightarrow a \equiv b \pmod{k}$.

   (b) $k \mid n,\ a \equiv b \pmod{k} \Longrightarrow a \equiv b \pmod{n}$.

   (c) $a \equiv b \pmod{n}, a \equiv b \pmod{k} \iff a \equiv b \pmod{kn}$.

   (d) $a \equiv b \pmod{n}, a \equiv b \pmod{k} \iff a \equiv b \pmod{[k,n]}$.

   (e) $a \equiv b \pmod{n} \iff ka \equiv kb \pmod{kn}$.

   (f) $a \equiv b \pmod{n}, c \equiv d \pmod{k} \Longrightarrow ac \equiv bd \pmod{kn}$.

   (g) $a^2 \equiv b^2 \pmod{n} \Longrightarrow a \equiv \pm b \pmod{n}$.

   (h) $a^2 \equiv b^2 \pmod{101} \Longrightarrow a \equiv \pm b \pmod{101}$.

5. There are several digits that can not be the last one in the decimal representation of a square. How many such digits can be found in the number system of base 101?

6. Comment on the following "theorem" and "proof" of Professor Donkey Monkey:

   "Theorem: For any integer $n > 3$, we have $\binom{n}{4} \equiv \binom{n+1}{4} \pmod{4}$.

Proof: Since $n+1 \equiv n-3 \pmod 4$ holds for every n,

$$\binom{n}{4} = \frac{n(n-1)(n-2)(n-3)}{1\cdot 2\cdot 3\cdot 4} \equiv$$
$$\equiv \frac{n(n-1)(n-2)(n+1)}{1\cdot 2\cdot 3\cdot 4} = \binom{n+1}{4} \pmod 4 \text{."}$$

7. Verify: $m \mid a-b \Longrightarrow m^2 \mid a^m - b^m$.
8. Assuming $3 \nmid a$ and $(6,n)=1$, prove $a^n \equiv b^n \pmod{3^n} \Longrightarrow a \equiv b \pmod{3^n}$.
9. Let $p>2$ be a prime and $1 \le k \le p{-}1$. Verify the following congruences modulo p:
   (a) $\binom{p}{k} \equiv 0$
   (b) $\binom{p-1}{k} \equiv (-1)^k$
   (c) $\binom{p-2}{k} \equiv (-1)^k(k+1)$.
10. Determine all primes p for which the remainder of $\binom{3p}{p}$ when divided by p is $p-2$.

* 11. Let p be a prime. Prove the following congruences modulo p:
   (a) $\binom{n}{p} \equiv \left\lfloor \frac{n}{p} \right\rfloor$
   (b) $\binom{n}{kp} \equiv \binom{\lfloor n/p \rfloor}{k}$
   (c) $\binom{n}{p^k} \equiv \left\lfloor \frac{n}{p^k} \right\rfloor$.

2.2. Residue Systems and Residue Classes

We mentioned the notion of a residue class modulo m after Theorem 2.1.2: it is the set of all integers giving the same remainder when divided by m.

Definition 2.2.1. Given the modulus m, the set of integers congruent to a is called the *residue class* represented by a. ♣

Notation: $(a)_m$. If there is no ambiguity, we can omit the index m referring to the modulus.

Thus, the residue class $(a)_m$ is an infinite arithmetic progression in both directions with difference m and a being one of its elements. There are m residue classes mod m, and each contains infinitely many numbers. By the definition, $(a)_m = (c)_m$ if and only if $a \equiv c \pmod m$.

Example. $(23)_7 = \{\dots, -5, 2, 9, 16, 23, 30, \dots\} = (100)_7$.

Definition 2.2.2. Given the modulus m, choosing one element from each residue class, we obtain a *complete residue system* modulo m. ♣

Example. $\{33, -5, 11, -11, -8\}$ is a complete residue system modulo 5.

We use mostly the following complete residue systems:

(A) Least non-negative residues: $0, 1, \dots, m-1$.

(B) Residues of least absolute value:

$$0, \pm 1, \pm 2, \dots, \pm \frac{m-1}{2}, \qquad \text{for } m \text{ odd}$$

and

$$0, \pm 1, \pm 2, \dots, \pm \frac{m-2}{2}, \frac{m}{2}, \qquad \text{for } m \text{ even}$$

(in the latter, $m/2$ can be replaced by $-m/2$).

We can apply the following simple criterion to check whether or not given numbers form a complete residue system:

Theorem 2.2.3. *A set of integers forms a complete residue system modulo m if and only if*

(i) *their number is m and*

(ii) *they are pairwise incongruent modulo m.* ♣

Proof. Let C_m be a complete residue system modulo m. Since there are m residue classes and we picked one element from each class, C_m contains exactly m numbers. Further, we took each number from a different residue class, hence the elements of C_m are pairwise incongruent modulo m.

Conversely, consider m integers pairwise incongruent modulo m. Then they belong to distinct residue classes. Since their number is m, they represent m residue classes, i.e. all classes are represented. Thus, these integers form a complete residue system modulo m. □

Multiplying a complete residue system by an integer coprime to the modulus and then adding an arbitrary integer yields a complete residue system again:

Theorem 2.2.4. *If* $r_1, r_2, \dots, r_m$ *is a complete residue system modulo m,* $(a, m) = 1$*, and b is any integer, then*

$$ar_1 + b, ar_2 + b, \dots, ar_m + b$$

is a complete residue system modulo m. ♣

Proof. Since the new system has m elements, it is enough to show, by Theorem 2.2.3, that the elements are pairwise incongruent mod m. We have to prove that $ar_i + b \equiv ar_j + b \pmod{m}$ implies $i = j$. Subtracting b from both sides, we obtain $ar_i \equiv ar_j \pmod{m}$. Since $(a, m) = 1$, by Theorem 2.1.3A, we can cancel a: $r_i \equiv r_j \pmod{m}$, and so $i = j$, indeed. □

Note that for $(a, m) \neq 1$, the integers $ar_i + b$ never form a complete residue system; see Exercise 2.2.11.

We examine now the distribution of the integers coprime to the modulus in the residue classes. It turns out that in a residue class, either all elements, or no elements are coprime to the modulus:

Let $a \equiv b \pmod{m}$. Then $(a, m) = 1$ if and only if $(b, m) = 1$.

We prove a stronger assertion in the next theorem:

Theorem 2.2.5.

$$a \equiv b \pmod{m} \Longrightarrow (a,m) = (b,m). \qquad ♣$$

Proof. By the assumption, $b = a + mc$ for some integer c.

On the right-hand side, both a and m are divisible by (a,m), hence $(a,m) \mid b$. This means that (a,m) is a common divisor of b and m, hence $(a,m) \mid (b,m)$.

We get the converse divisibility $(b,m) \mid (a,m)$ similarly, and so $(a,m) = (b,m)$. □

The residue classes with elements coprime to the modulus play an important role in the sequel:

Definition 2.2.6. A residue class $(a)_m$ is called a *reduced* residue class (mod m) if $(a,m) = 1$. ♣

As mentioned previously, Theorem 2.2.5 implies that if some element of a residue class is coprime to the modulus, then every element in the residue class has this property. Therefore Definition 2.2.6 does not depend on which number was picked to represent the residue class $(a)_m$.

We introduce now one of the most important functions in number theory:

Definition 2.2.7 (Euler's function φ)**.** For n given, $\varphi(n)$ counts how many integers of $1, 2, \ldots, n$ are coprime to n. ♣

Example. $\varphi(1) = 1$, $\varphi(10) = 4$, $\varphi(n) = n - 1$ if and only if n is a prime.

Clearly, $\varphi(n)$ is also the number of reduced residue classes modulo n.

We can easily compute $\varphi(n)$ from the standard form of n; we shall discuss this formula in Section 2.3.

Next, we define the notion of a reduced residue system analogously to the complete residue system:

Definition 2.2.8. Given the modulus m, choosing one element from each *reduced* residue class, we obtain a *reduced residue system* modulo m. ♣

Example. $\{17, -5, 11, -11\}$ is a reduced residue system modulo 12.

The simplest way to obtain a reduced residue system is to select the elements coprime to the modulus from the least non-negative remainders or from the remainders of least absolute value.

Now, we prove the analogues of Theorems 2.2.3 and 2.2.4 for reduced residue systems.

Theorem 2.2.9. *A set of integers forms a reduced residue system modulo m if and only if*

(i) *their number is $\varphi(m)$*

(ii) *they are pairwise incongruent modulo m and*

(iii) *each of them is coprime to m.* ♣

Proof. Let R_m be a reduced residue system modulo m. Since there are $\varphi(m)$ reduced residue classes and we picked one element from each, R_m contains exactly $\varphi(m)$ elements. Further, because we took each element from a different residue class, the elements of R_m are pairwise incongruent modulo m. Finally, every element of R_m is coprime to m, since they were chosen from reduced residue classes.

Conversely, consider $\varphi(m)$ pairwise incongruent integers modulo m that are coprime to m. The pairwise incongruence and the relative primeness guarantee that they belong to distinct reduced residue classes. Since their number is $\varphi(m)$, they represent $\varphi(m)$ reduced residue classes, i.e. all classes are represented. Thus, these integers form a reduced residue system modulo m. □

Theorem 2.2.10. *If $r_1, r_2, \dots, r_{\varphi(m)}$ is a reduced residue system modulo m and $(a,m) = 1$, then*

$$ar_1, ar_2, \dots, ar_m$$

is also a reduced residue system modulo m. ♣

Proof. We check criteria (i)–(iii) of Theorem 2.2.9.

(i) The new system has $\varphi(m)$ elements.

(ii) $ar_i \equiv ar_j \pmod{m}, (a,m) = 1 \Longrightarrow r_i \equiv r_j \pmod{m} \Longrightarrow i = j.$

(iii) $(a,m) = 1,\ (r_i,m) = 1 \Longrightarrow (ar_i,m) = 1.$ □

Note that for $(a,m) \neq 1$, the integers ar_i never form a reduced residue system, and moreover none of them is coprime to m.

Adding an integer b to the elements of a reduced residue system will not, in general, yield a reduced residue system, a significant difference from the complete residue systems. See Exercise 2.2.12.

Exercises 2.2

We assume everywhere that the modulus $m \geq 2$.

1. Determine the modulus m knowing that the integers below are elements of a reduced residue system:

   (a) 2 and 14

   (b) 18, 78, and 178

   (c) a and $-a$.

2. In how many (a) complete (b) reduced residue systems does every element a_i satisfy $0 \leq a_i \leq 5m + 1$?

3. Given m, characterize those arithmetic progressions that are infinite in both directions and contain modulo m

   (a) a residue class

   (b) a complete residue system?

4. For which $m \geq 2$ can we find a complete residue system consisting of

   (a) odd numbers

   (b) composite numbers

   (c) squares

   (d) integers ending with 1357 (in decimal representation)

   (e) consecutive elements of a geometric series

   S* (f) repunits (i.e. every digit is 1 in decimal system)

   S* (g) powers?

5. For which $m \geq 2$ can we find a reduced residue system consisting of

   (a) multiples of 15

   (b) numbers not divisible by 15

   (c) squares

   (d) integers ending with 1357 (in decimal representation)

   (e) powers?

6. True or false?

   (a) If $r_1, r_2, \dots, r_k$ is a reduced residue system modulo 7, then it is a reduced residue system modulo 14.

   (b) If $r_1, r_2, \dots, r_k$ is a reduced residue system modulo 14, then it is a reduced residue system modulo 7.

7. (a) What is the remainder of the sum of elements of a complete residue system modulo m?

   (b) Let m be even, and $a_1, a_2, \dots, a_m$ and $b_1, b_2, \dots, b_m$ be two complete residue systems modulo m. Prove that $a_1 + b_1, \dots, a_m + b_m$ *never* is a complete residue system modulo m. What can we say for m odd?

   (c) Examine the analogous questions for reduced residue systems instead of complete residue systems.

S 8. (a) There are m trees around a circular clearing with a squirrel in each tree. The squirrels want to get together in one tree, but they are allowed to move only the following way: every minute, any two squirrels may jump to an adjacent tree. For which values of m can they gather in one tree?

   (b) What happens if we modify the admissible step so that the two squirrels must jump to the adjacent trees in opposite directions (i.e. one of them clockwise, and the other counterclockwise).

* 9. (a) Determine all m for which $0, 0+1, 0+1+2, \dots, 0+1+2+\dots+(m-1)$ form a complete residue system mod m.

   (b) For which m does there exist a complete residue system $a_1, \dots, a_m$ mod m so that $a_1,\ a_1 + a_2,\ a_1 + a_2 + a_3, \dots, a_1 + a_2 + a_3 + \dots + a_m$ is also a complete residue system mod m?

10. Let $k \mid m$. True or false?

    (a) Every residue class mod k is the union of residue classes mod m.

    (b) Every reduced residue class mod k is the union of reduced residue classes mod m.

    * (c) Every reduced residue class mod k contains a subset that is a reduced residue class mod m.

    (d) Every reduced residue system mod k can be extended to a reduced residue system mod m.

    * (e) Every reduced residue system mod m contains a reduced residue system mod k.

11. Let $r_1, r_2, \dots, r_m$ be a complete residue system modulo m, $(a, m) \neq 1$, and b arbitrary.

    (a) Prove that $ar_1 + b, \dots, ar_m + b$ is never a complete residue system modulo m.

    (b) How many residue classes modulo m are represented by the elements $ar_1 + b$, $\dots$, $ar_m + b$ altogether?

S* 12. Let $r_1, r_2, \dots, r_{\varphi(m)}$ be a reduced residue system modulo m.

    (a) Determine all integers a such that the numbers ar_1, $\dots$, $ar_{\varphi(m)}$ are pairwise incongruent modulo m.

    (b) Find all integers b such that the numbers $r_1 + b, \dots, r_{\varphi(m)} + b$ form a reduced residue system modulo m.

S* 13. For which integers m and k do there exist a complete residue system a_1, $\dots$, a_m modulo m and a complete residue system $b_1, \dots, b_k$ modulo k so that the numbers $a_i b_j$ form a complete residue system modulo mk?

S 14. Let a and b be positive integers.

    (a) Prove that

    $$T = \{\, ib + ja \mid i = 1, 2, \dots, a, j = 1, 2, \dots, b \,\}$$

    is a complete residue system modulo ab if and only if $(a, b) = 1$.

    (b) Let r_1, $\dots$, $r_{\varphi(a)}$ and s_1, $\dots$, $s_{\varphi(b)}$ be reduced residue systems modulo a and modulo b. Prove that

    $$R = \{\, r_i b + s_j a \mid i = 1, 2, \dots, \varphi(a), j = 1, 2, \dots, \varphi(b) \,\}$$

    is a reduced residue system modulo ab if and only if $(a, b) = 1$.

    (c) Demonstrate that if $(a, b) = 1$, then $\varphi(ab) = \varphi(a)\varphi(b)$.

2.3. Euler's Function φ

We introduced Euler's function φ in Definition 2.2.7: If n is a positive integer, then $\varphi(n)$ is the number of integers coprime to n among the integers $1, 2, \dots, n$.

This implies immediately that there are $\varphi(m)$ reduced residue classes modulo m and a reduced residue system consists of $\varphi(m)$ integers.

We prove now a formula for $\varphi(n)$ from the standard form of n:

Theorem 2.3.1. *Let the standard form of n be*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} = \prod_{i=1}^{r} p_i^{\alpha_i}, \qquad \text{where} \qquad \alpha_i > 0.$$

Then

$$\varphi(n) = \left(p_1^{\alpha_1} - p_1^{\alpha_1-1}\right) \dots \left(p_r^{\alpha_r} - p_r^{\alpha_r-1}\right) = \prod_{i=1}^{r} \left(p_i^{\alpha_i} - p_i^{\alpha_i-1}\right). \qquad \clubsuit$$

This formula for $\varphi(n)$ is valid only if the exponents α_i in the standard form of n are positive (in contrast e.g. to the formula for $d(n)$ in Theorem 1.6.3 which remains valid even if we allow 0 to occur among the exponents α_i). Some equivalent forms of the formula are:

$$\varphi(n) = \prod_{i=1}^{r} p_i^{\alpha_i-1}(p_i - 1) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) = n \prod_{\substack{p \mid n \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right).$$

We give two proofs of Theorem 2.3.1. A third one can be derived from Exercise 6.5.4b. Also, Exercises 2.2.14 and 2.6.10 contain two further verifications of assertion II which is the key step in the first proof.

First proof. We infer the theorem from the two propositions below:

(I) If p is a prime (and $\alpha > 0$), then $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

(II) If $(a, b) = 1$, then $\varphi(ab) = \varphi(a)\varphi(b)$.

These imply the theorem: It follows from II by induction on the number of factors that if the integers $a_1, \dots, a_r$ are *pairwise* coprime, then $\varphi(a_1 \dots a_r) = \varphi(a_1) \dots \varphi(a_r)$. Applying this for $a_i = p_i^{\alpha_i}$ and substituting the value for $\varphi(p_i^{\alpha_i})$ obtained in I, we arrive at the desired formula.

We start with the verification of I. An integer is coprime to p^α if and only if it is not divisible by p. Hence, we obtain the coprime integers to p^α among $1, 2, \dots, p^\alpha$, if we discard the multiples of p. We thus discard $p, 2p, \dots, p^{\alpha-1}p$, which are $p^\alpha/p = p^{\alpha-1}$ numbers. This implies that $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ integers remain.

Now, we turn to the proof of II. (As indicated earlier, two other methods are available in Exercises 2.2.14 and 2.6.10.)

The number $\varphi(ab)$ is the number of positive integers not greater than ab that are coprime to ab, i.e. are relatively prime to both a and b.

Denoting the smallest positive elements of the reduced residue classes modulo a by $r_1, r_2, \dots, r_{\varphi(a)}$, we enumerate all positive integers not greater than ab and coprime to a:

$$\begin{array}{cccc} r_1 & r_2 & \dots & r_{\varphi(a)} \\ a+r_1 & a+r_2 & \dots & a+r_{\varphi(a)} \\ 2a+r_1 & 2a+r_2 & \dots & 2a+r_{\varphi(a)} \\ \vdots & \vdots & & \vdots \\ (b-1)a+r_1 & (b-1)a+r_2 & \dots & (b-1)a+r_{\varphi(a)} \end{array} \tag{2.3.1}$$

We have to select those numbers from (2.3.1) that are coprime also to b.

Consider an arbitrary column of the table. For example, the integers in column i are

$$r_i, a+r_i, 2a+r_i, \dots, (b-1)a+r_i. \tag{2.3.2}$$

These numbers were obtained from the complete residue system 0, 1, …, $b-1$ modulo b by multiplying the elements by a coprime to b and then adding r_i. By Theorem 2.2.4, (2.3.2) is a complete residue system modulo b, so every column of table (2.3.1) is a complete residue system modulo b.

Since a complete residue system modulo b contains $\varphi(b)$ elements coprime to b, there are $\varphi(b)$ numbers relatively prime to b in each column of (2.3.1).

The number of columns in (2.3.1) is $\varphi(a)$, so the table has altogether $\varphi(a)\varphi(b)$ elements coprime to b.

This means that there are $\varphi(a)\varphi(b)$ numbers among the positive integers not greater than ab that are coprime both to a and b, i.e. to ab. By definition, this value equals $\varphi(ab)$, hence $\varphi(ab)=\varphi(a)\varphi(b)$, indeed. □

Second proof. We use the Inclusion and Exclusion formula.

We have to determine, how many numbers are coprime to n among $1, 2, \dots, n$, that is, how many are divisible by none of the primes p_1, p_2, …, p_r.

Thus we have to delete those "bad" numbers from 1, 2, …, n which are divisible by one or more primes p_j.

Consider first those elements that are multiples of a given p_j (disregarding whether or not they are divisible by some other prime factors of n). Clearly, there are n/p_j such integers.

Now we count those numbers that are divisible by a given set of primes p_j (not caring again whether or not they are multiples of some other prime factors of n). An integer is divisible by both of two (distinct) primes if and only if it is divisible by their product. Hence, $n/(p_1p_2)$ elements are divisible by both p_1 and p_2, $n/(p_1p_3p_7)$ elements are divisible by each of p_1, p_3, and p_7, etc.

Thus, the Inclusion and Exclusion formula yields

$$\varphi(n) = n - \frac{n}{p_1} - \frac{n}{p_2} - \dots - \frac{n}{p_r} + \frac{n}{p_1p_2} + \frac{n}{p_1p_3} + \dots + \frac{n}{p_{r-1}p_r} - \frac{n}{p_1p_2p_3} - \dots \tag{2.3.3}$$

A simple direct calculation verifies that the right-hand side of (2.3.3) is equal to the product

$$n\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right),$$

which is an alternative version of the formula in the theorem. □

Exercises 2.3

1. Verify that $\varphi(n)$ is even for every $n > 2$.
2. Find all values of n for which $\varphi(n)$ is (a) 2 (b) 4 (c) 14 (d) 60.
3. Which is the smallest n for which $\varphi(n)$ is divisible by
   (a) 2^{10}
   (b) 3^{10}?
4. Determine all possible values of $\varphi(100n)/\varphi(n)$ for n a positive integer.
5. Prove the following propositions.
   (a) $k \mid n \Longrightarrow \varphi(k) \mid \varphi(n)$.
   (b) $\varphi\big((a,b)\big) \mid \big(\varphi(a),\varphi(b)\big)$ and $\big[\varphi(a),\varphi(b)\big] \mid \varphi\big([a,b]\big)$.
   (c) $\varphi\big((a,b)\big) = \big(\varphi(a),\varphi(b)\big) \iff \big[\varphi(a),\varphi(b)\big] = \varphi\big([a,b]\big)$.
6. Show that $\varphi(a)/\varphi(b) = a/b$ holds if and only if a and b have exactly the same prime factors.
7. Let $n > 2$. True or false?
   (a) If $\big(n,\varphi(n)\big) = 1$, then n is an odd squarefree number.
   (b) If n is an odd squarefree number, then $\big(n,\varphi(n)\big) = 1$.

* 8. Prove that for every positive integer k there exists an n satisfying $\big(n,\varphi(n)\big) = k$.

9. Verify that $\varphi(n) + d(n) \le n + 1$ holds for every n. When do we have equality?
10. (a) Demonstrate that if $(a,b) \ne 1$, then $\varphi(ab) > \varphi(a)\varphi(b)$ (thus equality is never true in this case).
    (b) In the first proof of Theorem 2.3.1, the key step was the verification of II, i.e. of $(a,b) = 1 \Longrightarrow \varphi(ab) = \varphi(a)\varphi(b)$. Where does the argument fail if a and b are not coprime?
    (c) Show that
    $$\varphi(ab)\varphi\big((a,b)\big) = (a,b)\varphi(a)\varphi(b)$$
    holds for every a and b.
11. (a) Prove that $n - \varphi(n) \ge \sqrt{n}$ if n is composite. When is equality true?
    (b) Find those n for which $n - \varphi(n)$ is
    (b1) 1
    (b2) 6

(b3) 7

(b4) 10.

12. Which *integers* occur in the range of the function $n/\varphi(n)$?

13. Prove that $\varphi(n^2) = \varphi(k^2)$ holds only for $n = k$.

14. Verify $\sum_{d|n} \varphi(d) = n$.

15. Show that $\varphi(n) \to \infty$ if $n \to \infty$.

* 16. Demonstrate that for every positive integer k there exists an n satisfying $\varphi(n) = \varphi(n+k)$.

* 17. Exhibit 1000 distinct integers where the function φ assumes the same value.

S* 18. Determine all n satisfying $\varphi(n!) = k!$ for some k.

S* 19. For which m can a reduced residue system mod m form an arithmetic progression?

2.4. The Euler–Fermat Theorem

Theorem 2.4.1 (Euler–Fermat Theorem).

$$(a, m) = 1 \Longrightarrow a^{\varphi(m)} \equiv 1 \pmod{m}. \qquad \clubsuit$$

Proof. Let $r_1, r_2, \dots, r_{\varphi(m)}$ be a reduced residue system modulo m.

Since $(a, m) = 1$, $ar_1, \dots, ar_{\varphi(m)}$ is also a reduced residue system modulo m.

This means that to every $1 \le i \le \varphi(m)$, there exists exactly one $1 \le j \le \varphi(m)$ satisfying $ar_i \equiv r_j \pmod{m}$. Denote this r_j by s_i:

$$\begin{aligned} ar_1 &\equiv s_1 \pmod{m}, \\ ar_2 &\equiv s_2 \pmod{m}, \\ &\vdots \\ ar_{\varphi(m)} &\equiv s_{\varphi(m)} \pmod{m}. \end{aligned} \tag{2.4.1}$$

Here $s_1, \dots, s_{\varphi(m)}$ is a permutation of the numbers $r_1, \dots, r_{\varphi(m)}$.

Multiplying the congruences in (2.4.1), we obtain

$$a^{\varphi(m)} r_1 r_2 \dots r_{\varphi(m)} \equiv s_1 s_2 \dots s_{\varphi(m)} \pmod{m},$$

or

$$a^{\varphi(m)} r_1 r_2 \dots r_{\varphi(m)} \equiv r_1 r_2 \dots r_{\varphi(m)} \pmod{m}. \tag{2.4.2}$$

We can cancel every r_i in (2.4.2), since $(r_i, m) = 1$, which yields the desired congruence $a^{\varphi(m)} \equiv 1 \pmod{m}$. □

An important special case is when the modulus is a prime p. Then $\varphi(p) = p - 1$ and we obtain:

Theorem 2.4.1A (First form of Fermat's Little Theorem). *If p is a prime and* $(a, p) = 1$, *then* $a^{p-1} \equiv 1 \pmod{p}$.

Note that for a prime p, the conditions $(a, p) = 1$, $p \nmid a$, and $a \not\equiv 0 \pmod{p}$ are equivalent.

From Theorem 2.4.1A, it is easy to get a congruence valid for every a:

Theorem 2.4.1B (Second form of Fermat's Little Theorem). *If p is a prime, then $a^p \equiv a \pmod{p}$ holds for every a.*

Proof. If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$ by Theorem 2.4.1A. Multiplying this congruence by a, we obtain the desired $a^p \equiv a \pmod{p}$.

If $p \mid a$, then $a \equiv 0 \pmod{p}$. Raising this to the pth power (or multiplying it by a^{p-1}), we get $a^p \equiv 0 \pmod{p}$, hence also $a^p \equiv a \pmod{p}$ holds. □

Remarks: (1) The converse of the Euler–Fermat Theorem (Theorem 2.4.1) is also true, i.e. $(a, m) = 1$ is not only a sufficient, but also a *necesssary* condition for $a^{\varphi(m)} \equiv 1 \pmod{m}$. In fact, the following stronger proposition holds: There exists an exponent $k > 0$ such that $a^k \equiv 1 \pmod{m}$ *only* if a and m are coprime. Namely, $a^k \equiv 1 \pmod{m}$ implies $(a^k, m) = (1, m) = 1$ by Theorem 2.2.5, hence also $(a, m) = 1$ must hold.

(2) The second form of Fermat's Little Theorem (Theorem 2.4.1B) has no natural generalization for arbitrary modulus m, i.e. there exists no simple variant of the general Euler–Fermat Theorem that would be valid for every a (see Exercise 2.4.15).

(3) As their names indicate, Theorems 2.4.1A and B are due to Fermat. Both variants can be verified directly, without relying on Theorem 2.4.1. Form B can be proven by induction (on a), and form A follows easily (see Exercise 2.4.16). Theorem 2.4.1 was found by Euler as a generalization of Fermat's Little Theorem.

(4) The adjective "little" serves to distinguish this result from Fermat's Last Theorem which is a very famous and only recently solved problem of mathematics. We shall treat this topic in Chapter 7.

Exercises 2.4

1. Prove $n \mid 2^{n!} - 1$ for any odd n.
2. Determine the last two digits of 1793^{8642} (in decimal representation).
3. Verify that $n^{20} + 4n^{44} + 8n^{80}$ is a multiple of 13 for every n.
4. Show that if n is any integer, then at least one of $n^6 + 13$ and $n^2 + 21$ is a composite number.
5. Prove $1703601900 \mid a^{62} - a^2$ for every a.
6. Verify the following propositions:

   (a) $11 \mid a^{30} + b^{30} + c^{30} \implies 11^{30} \mid a^{30} + b^{30} + c^{30}$.

   (b) $9 \mid a^{30} + b^{30} + c^{30} \implies 9^{15} \mid a^{30} + b^{30} + c^{30}$.

7. Show that $a^{88} - b^{88}$ is *not* divisible by 23 if and only if exactly one of a and b is divisible by 23.
8. Let p be a prime and $r_1, \dots, r_p$ be a complete residue system mod p. Prove that also $r_1^{2p-3}, \dots, r_p^{2p-3}$ is a complete residue system mod p.
9. (a) Let p be a prime, a an integer, and i and j positive integers satisfying $i \equiv j \pmod{p-1}$. Prove $a^i \equiv a^j \pmod{p}$.

   (b) How can we generalize the assertion in (a) for arbitrary m (instead of primes)?
10. True or false? (With decimal notation and powers with positive integer exponents.)

    (a) Infinitely many powers of 133 terminate with the string 133.

    (b) Infinitely many powers of 134 terminate with the string 134.

    (c) Infinitely many powers of 136 terminate with the string 136.
11. Show that an infinite arithmetic progression of distinct positive integers $a, a+d, \dots, a+kd, \dots$ contains infinitely many powers of a (with positive integer exponents) if and only if $d/(a,d)$ and a are coprime.
12. Give a new solution to Exercise 1.3.12a using the Euler–Fermat Theorem.
13. Verify that every positive odd divisor of $n^2 + 1$ is of the form $4k + 1$.
14. Assume that 19 divides $a^{40} + b^{40}$. Show that then 19 must divide both a and b, as well.
15. Verify the following propositions and investigate their relation to Fermat's Little Theorem.

    (a) $a^{\varphi(m)+1} \equiv a \pmod{m}$ holds for every a if and only if m is squarefree.

    (b) $a^m \equiv a^{m-\varphi(m)} \pmod{m}$ holds for every m and a.

    (c) $a^{1729} \equiv a \pmod{1729}$ holds for every a.
16. Give a direct proof of both versions of Fermat's Little Theorem: First verify Theorem 2.4.1B by induction and then deduce Theorem 2.4.1A.

2.5. Linear Congruences

This section deals with the simplest type of congruences with variables (or congruence equations), the linear congruences.

Definition 2.5.1. Let a and b be integers and m a positive integer. The congruence $ax \equiv b \pmod{m}$ is called a *linear congruence*, and by a *solution* of it we mean an integer s which substituted into x makes the congruence valid. ♣

Clearly, if s is a solution, then every other element of the residue class $(s)_m$ is a solution, too. Hence, to find all solutions, it is enough to check a complete residue system to see which elements of it satisfy the congruence; then all solutions are the integers congruent to them.

Therefore the number of solutions of a linear congruence is defined as how many *pairwise incongruent* integers satisfy the congruence, i.e. what is the number of *residue* *classes* the solutions come from, or (again in a slightly different formulation) how many elements of a complete residue system make the congruence valid. The same applies for congruences of higher degree as well, thus we define this convention immediately for the general case.

Definition 2.5.2. Let f be a polynomial with integer coefficients. The *number of solutions* of the congruence $f(x) \equiv 0 \pmod{m}$ is how many elements s of a complete residue system modulo m satisfy $f(s) \equiv 0 \pmod{m}$. ♣

Since $u \equiv v \pmod{m} \implies f(u) \equiv f(v) \pmod{m}$, this notion does not depend on which complete residue system modulo m we considered.

Returning to linear congruences, we want to answer the following questions arising for equations in general:

(i) What is a necessary and sufficient condition for solvability?

(ii) How many solutions do we have?

(iii) How can we describe or characterize all solutions?

(iv) Which methods yield these solutions?

We discuss solvability first.

Theorem 2.5.3. *The congruence $ax \equiv b \pmod{m}$ is solvable if and only if $(a, m) \mid b$.* ♣

Proof. The solvability of $ax \equiv b \pmod{m}$ means that $as \equiv b \pmod{m}$ for some s.

This is equivalent to the existence of an integer t satisfying $as + mt = b$, i.e. s and t are a solution of the linear Diophantine equation $ax + my = b$.

Hence, the linear congruence $ax \equiv b \pmod{m}$ is solvable if and only if the linear Diophantine equation $ax + my = b$ is solvable.

The necessary and sufficient condition for the solvability of the latter is $(a, m) \mid b$, by Theorem 1.3.6. Thus the same criterion applies for the solvability of $ax \equiv b \pmod{m}$. □

We see from the proof that the linear congruence $ax \equiv b \pmod{m}$ and the linear Diophantine equation $ax + my = b$ can be deduced from each other. (Moreover, the linear Diophantine equation $ax + my = b$ can also be transformed into the linear congruence $my \equiv b \pmod{|a|}$ if $a \neq 0$.)

Based on this, every result obtained for linear congruences can be used also for linear Diophantine equations and vice versa.

We should be aware, however, of the significant differences: The solutions of a linear congruence are integers (or rather residue classes), whereas the solutions of a linear Diophantine equation are *pairs* of integers; the number of solutions of a congruence is finite, but a linear Diophantine equation has infinitely many solutions, etc.

In the next theorem, we determine the number of solutions of a linear congruence, and also see how we can get all solutions from a given one.

Theorem 2.5.4. (I) *If $ax \equiv b \pmod{m}$ is solvable, then there are (a, m) solutions.*

(II) *Let $(a, m) = d$, $m = dm_1$, and s be a solution of $ax \equiv b \pmod{m}$. Then*

$$s, \quad s + m_1, \quad s + 2m_1, \quad \ldots, \quad s + (d-1)m_1 \tag{2.5.1}$$

are pairwise incongruent modulo m, satisfy the congruence, and every solution is congruent to one of them modulo m. ♣

Proof. We verify the two assertions simultaneously.

We assumed that s was a solution, so

$$as \equiv b \pmod{m}\,. \tag{2.5.2}$$

An integer t is a solution if and only if

$$at \equiv b \pmod{m}\,. \tag{2.5.3}$$

Using (2.5.2), formula (2.5.3) is equivalent to

$$at \equiv as \pmod{m}\,. \tag{2.5.4}$$

By Theorem 2.1.3, (2.5.4) is equivalent to

$$t \equiv s \left(\mathrm{mod}\ \frac{m}{(m,a)}\right) \quad \text{or} \quad t \equiv s \pmod{m_1}\,.$$

We can rewrite this as

$$t = s + km_1, \tag{2.5.5}$$

with some integer k.

This means that the numbers t in (2.5.5) give all solutions of $ax \equiv b \pmod{m}$.

Thus, we have to prove that these integers t in (2.5.5) belong to d distinct residue classes and (2.5.1) lists a representative from each class.

When do two such t fall into the same residue class modulo m? Let

$$t' = s + k'm_1 \quad \text{and} \quad t'' = s + k''m_1.$$

Then

$$t' \equiv t'' \pmod{m} \iff k'm_1 \equiv k''m_1 \pmod{m} \iff k' \equiv k'' \pmod{d}\,. \tag{2.5.6}$$

Here, we first subtracted s from $t' \equiv t'' \pmod{m}$, then cancelled m_1 and changed the modulus to $m/(m_1, m) = m/m_1 = d$, according to Theorem 2.1.3.

Implication (2.5.6) means that two integers t fall into the same residue class modulo m if and only if the relevant two integers k are congruent modulo d.

Thus, if k assumes the values $0, 1, \ldots, d-1$, then the integers

$$t = s + km_1, \quad \text{or} \quad s, s + m_1, \ldots, s + (d-1)m_1$$

occurring in (2.5.1) are just the representatives of the relevant residue classes modulo m. □

The most important special case of the linear congruence $ax \equiv b \pmod{m}$ is when $(a, m) = 1$. Then $(a, m) \mid b$ holds automatically, so the congruence is solvable, by Theorem 2.5.3, and it has $(a, m) = 1$ (pairwise incongruent) solutions, by Theorem 2.5.4.

We state this important result as a theorem:

Theorem 2.5.5. *If* $(a, m) = 1$*, then the congruence* $ax \equiv b \pmod{m}$ *is solvable for every* b *and the number of solutions is* 1. ♣

We make some general preliminary remarks concerning methods for finding the solutions.

(A) In general, it is advisable to check by the criterion of Theorem 2.5.3 whether the congruence is solvable at all.

(B) If $(a, m) = 1$, then the congruence is satisfied by the elements of just one residue class, so if we find somehow a solution, then we are done. Also, in the general case, it is sufficient to guess a single solution because we can easily obtain all solutions by Theorem 2.5.4/II.

(C) In most cases, the best start is to reduce the original linear congruence to one where the coefficient of x and the modulus are coprime. We can do this as follows. If $ax \equiv b \pmod{m}$ is solvable, then $(a, m) \mid b$. Let $d = (a, m)$, then

$$a = da_1, \quad m = dm_1, \quad b = db_1, \quad \text{and} \quad (a_1, m_1) = 1.$$

Hence, we can divide the congruence by d (including also the modulus): $ax \equiv b \pmod{m}$ is equivalent to $a_1x \equiv b_1 \pmod{m_1}$ and here $(a_1, m_1) = 1$. (Looking at the corresponding Diophantine equations, this just means that $ax + my = b$ is divided by d to yield $a_1x + m_1y = b_1$.)

The word "equivalent" in the previous paragraph should remind us that though the two congruences are satisfied by the same integers, we have to group them into residue classes of different moduli: mod m at the first congruence and mod m_1 at the second one. As a consequence, the two congruences will differ also in the number of solutions (for $d > 1$).

We turn now to the detailed discussion of a few methods for finding the solutions of a linear congruence. Each will be illustrated by an example.

M1 *Trial.* We check each element of a complete residue system modulo m to see if it satisfies the congruence. (This should be applied only for very small moduli.)

E1 $23x \equiv 11 \pmod{5}$. To make calculations simpler, it is worthwhile to replace the coefficients with congruent numbers having smaller (absolute) value before substituting into x: $3x \equiv 1 \pmod{5}$ or $-2x \equiv 1 \pmod{5}$. Testing the numbers 0, 1, 2, 3, 4 (or 0, ± 1, ± 2), we obtain that the residue class $x \equiv 2 \pmod{5}$ is the only solution. (Since $(23, 5) = 1$ implies that there is only one solution, after finding it we do not have to check more numbers.)

M2 *Diophantine equation.* We reduce the linear congruence to a Diophantine equation as seen in the proof of Theorem 2.5.3, and then reconstitute its solutions into solutions of the congruence.

E2 $18x \equiv 38 \pmod{28}$. The corresponding Diophantine equation is $18x + 28y = 38$. Dividing by 2, we obtain $9x + 14y = 19$. Following the proof of Theorem 1.3.6, we write the gcd of 9 and 14 in form $9u + 14v$. From the Euclidean algorithm or after a few trials, we have $9 \cdot (-3) + 14 \cdot 2 = 1$. Multiplying by 19, we obtain $9 \cdot (-57) + 14 \cdot 38 = 19$, so $x = -57, y = 38$ is a solution of the equation $9x + 14y = 19$.

Returning to the congruence $18x \equiv 38 \pmod{28}$, this means that $x = -57$ is a solution. We find all solutions by Theorem 2.5.4/II: $x \equiv -57 \pmod{28}$ and $x \equiv -43 \pmod{28}$. (The representatives -57 and -43 can be replaced by any others, e.g. by -1 and 13.)

Note that to solve a linear Diophantine equation, it is more convenient to apply the procedure described in Section 7.1 that characterizes all solutions immediately in a parametric form. (Actually, also this is a variant of the Euclidean algorithm.)

M3 *Euler–Fermat Theorem.* We reduce the congruence $ax \equiv b \pmod{m}$ to $a_1x \equiv b_1 \pmod{m_1}$ where $(a_1, m_1) = 1$, as seen in remark (C). T hen $a_1^{\varphi(m_1)} \equiv 1 \pmod{m_1}$ by the Euler–Fermat Theorem. Therefore $x = a_1^{\varphi(m_1)-1}b_1$ is a solution:

$$a_1 \cdot a_1^{\varphi(m_1)-1}b_1 = a_1^{\varphi(m_1)}b_1 \equiv b_1 \pmod{m_1}.$$

Hence, $x = a_1^{\varphi(m_1)-1}b_1$ is a solution of the original congruence, too. Finally, we can obtain all solutions from Theorem 2.5.4/II.

E3 $36x \equiv 81 \pmod{21}$. Here $(36, 21) = 3$, hence we can reduce the problem to the congruence $12x \equiv 27 \pmod{7}$. Decreasing the coefficients, we obtain $-2x \equiv -1 \pmod{7}$. Its solution is $x = (-2)^{6-1}(-1) \equiv 4 \pmod{7}$. Thus, all solutions of the original congruence are $x \equiv 4, 11, 18 \pmod{21}$.

Reducing the coefficients in the congruence $12x \equiv 27 \pmod{7}$, we may choose the least non-negative remainders instead of the ones with least absolute value. Then we get $5x \equiv 6 \pmod{7}$ and $x \equiv 5^5 \cdot 6 \pmod{7}$.

Since $(12, 7) = 1$, $12x \equiv 27 \pmod{7}$ has a unique solution modulo 7, i.e. $5^5 \cdot 6 \equiv 4 \pmod{7}$ For a direct verification, one should not compute the actual value of 5^5 but rather take the remainders modulo 7 while raising to powers:

$$5^2 = 25 \equiv 4 \pmod{7}, \quad 5^4 \equiv 4^2 \equiv 2 \pmod{7}, \quad 5^5 \equiv 5 \cdot 2 \equiv 3 \pmod{7},$$

hence $6 \cdot 5^5 \equiv 6 \cdot 3 \equiv 4 \pmod{7}$.

M4 *Tricks.* Multiplying or dividing the congruence by well-chosen integers coprime to the modulus, we get equivalent congruences till finally we can easily read the solution(s).

E4 Consider $80x \equiv 32 \pmod{108}$. Here $(80, 108) = 4$, so we can reduce the problem to solve $20x \equiv 8 \pmod{27}$.

As $(4, 27) = 1$, cancelling 4 yields an equivalent congruence: $5x \equiv 2 \pmod{27}$.

We show two methods of how to get rid of the coefficient 5 in $5x \equiv 2 \pmod{27}$.

I. Division: We can replace 2 on the right-hand side by -25: $5x \equiv -25 \pmod{27}$. Since $(5, 27) = 1$, we can cancel the 5: $x \equiv -5 \pmod{27}$.

II. Multiplication: We multiply by a suitable number to change the coefficient of x into an integer congruent to 1 (or -1) modulo 27. (This multiplier is then automatically coprime to 27 guaranteeing equivalence.) We can multiply our congruence $5x \equiv 2$

(mod 27) by 11: $55x \equiv 22 \pmod{27}$ and since $55 \equiv 1 \pmod{27}$ we obtain $x \equiv 22 (\equiv -5)$ (mod 27).

So the solutions of the original congruence are $x \equiv -5, 22, 49, 76 \pmod{108}$.

Comparing the above methods, M3 or M4 could seem to be the easiest to apply at first sight. It turns out, however, that only M2 works for large moduli. This will be treated in Section 5.7.

Exercises 2.5

1. Solve Examples E1–E4 with every method M2–M4.

2. Solve the following congruences:

   (a) $24x \equiv 60 \pmod{51}$

   (b) $100x \equiv 88 \pmod{116}$

   (c) $555x \equiv 5555 \pmod{55555}$

   (d) $(2^k + 1)x \equiv 2^{k+1} + 1 \pmod{2^{k+2} + 1}$

   (e) $10x^{39} + 8x^{20} + 9x^3 + 7x \equiv 0 \pmod{19}$

   (f) $13x^{41} \equiv 27 \pmod{100}$.

3. Determine the two smallest positive integers which when multiplied by 13 will have last digit 3 and next to last digit 4 in the number system of base seven.

4. Compute the last two digits of 3^{279} (in decimal representation).

5. Check (each of) the following conditions to see if they are sufficient for the solvability of the congruence $ax \equiv b \pmod{m}$.

   (a) $(a, m) \mid (a, b)$

   (b) $(a, b) \mid (a, m)$

   (c) a, m, b is an arithmetic progression

   (d) a, m, b is a geometric series

   (e) a, b, m is an arithmetic progression

   (f) a, b, m is a geometric series.

6. True or false?

   (a) The number of solutions of $ax \equiv b \pmod{m}$ is at most b if $b > 0$.

   (b) If $ax \equiv b \pmod{m}$ is solvable, then $a^2x \equiv b^2 \pmod{m^2}$ is solvable.

   (c) If both $a_1x \equiv b_1 \pmod{m_1}$ and $a_2x \equiv b_2 \pmod{m_2}$ are solvable, then $a_1a_2x \equiv b_1b_2 \pmod{m_1m_2}$ is solvable.

S 7. Let a and m be fixed and denote the number of solutions of $ax \equiv b \pmod{m}$ by $f(b)$. Compute $\sum_{b=1}^{m} f(b)$.

2.6. Simultaneous Systems of Congruences

A simultaneous system of congruences means that several congruence conditions with different moduli are imposed on the same variable:

$$f_1(x) \equiv 0 \pmod{m_1}, \quad f_2(x) \equiv 0 \pmod{m_2}, \quad \ldots, \quad f_k(x) \equiv 0 \pmod{m_k}$$

where $f_1, \ldots, f_k$ are polynomials with integer coefficients.

Clearly, a necessary condition for the solvability of such a system is that each congruence should be solvable. Thus, after solving the individual congruences, we have to study only the (special linear) systems of the form

$$x \equiv c_1 \pmod{m_1}, \quad x \equiv c_2 \pmod{m_2}, \quad \ldots, \quad x \equiv c_k \pmod{m_k}.$$

We consider first systems with two congruences.

Theorem 2.6.1. (I) *The simultaneous system of congruences*

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \end{aligned} \tag{2.6.1}$$

is solvable if and only if

$$(m_1, m_2) \mid c_1 - c_2.$$

(II) *If solvable, the solutions form a residue class modulo $[m_1, m_2]$. Or, putting it into another form: if s is a solution, then all solutions t are given by*

$$t \equiv s \pmod{[m_1, m_2]}, \quad \textit{or} \quad t = s + k[m_1, m_2], \quad \textit{where } k \textit{ is an integer.} \qquad \clubsuit$$

The proof will yield a method for finding the solutions; one has to solve a linear Diophantine equation (or, equivalently, a linear congruence).

Proof. I. By the definition of congruences, (2.6.1) can be transformed into

$$x = c_1 + z_1 m_1, \quad x = c_2 + z_2 m_2 \tag{2.6.2}$$

where z_1 and z_2 are integers.

Condition (2.6.2) is equivalent to

$$c_1 + z_1 m_1 = c_2 + z_2 m_2. \tag{2.6.3}$$

Rearranging (2.6.3), we obtain

$$c_1 - c_2 = z_2 m_2 - z_1 m_1. \tag{2.6.4}$$

This means that the system of congruences (2.6.1) can be reduced to the linear Diophantine equation (2.6.4).

By Theorem 1.3.6, it is solvable if and only if $(m_1, m_2) \mid c_1 - c_2$, hence the same applies for (2.6.1).

As we indicated before the proof, we also obtained a method of finding the solutions: we have to solve Diophantine equation (2.6.4) or a corresponding congruence.

II. Let s be a solution so

$$\begin{aligned} s &\equiv c_1 \pmod{m_1}, \\ s &\equiv c_2 \pmod{m_2}. \end{aligned} \tag{2.6.5}$$

An integer t is a solution if and only if

$$t \equiv c_1 \pmod{m_1}, \qquad t \equiv c_2 \pmod{m_2}. \tag{2.6.6}$$

Using (2.6.5), condition (2.6.6) is equivalent to

$$t \equiv s \pmod{m_1} \qquad t \equiv s \pmod{m_2}. \tag{2.6.7}$$

Rewrite (2.6.7) as divisibilities and apply the properties of lcm (Theorem 1.6.6/II):

$$\left.\begin{matrix} m_1 \mid t-s \\ m_2 \mid t-s \end{matrix}\right\} \iff [m_1, m_2] \mid t-s \iff t \equiv s \pmod{[m_1, m_2]}. \qquad \square$$

The most importamt special case is when the moduli m_1 and m_2 in system (2.6.1) are coprime. Then $(m_1, m_2) \mid c_1 - c_2$ holds automatically, so the system of congruences is solvable and the solutions form a unique residue class modulo $m_1 m_2$. We state this important result as a theorem:

Theorem 2.6.1A. *If $(m_1, m_2) = 1$, then the simultaneous system of congruences*

$$x \equiv c_1 \pmod{m_1}$$
$$x \equiv c_2 \pmod{m_2}$$

is solvable for arbitrary c_1 and c_2, and the solutions form a single residue class modulo $m_1 m_2$.

Theorem 2.6.1A implies that if m_1 and m_2 are coprime, then the remainder of a number when divided by m_1 is independent of its remainder mod m_2. For example, the last digits of an integer give its remainder modulo a power of 10 and they provide no information on the remainder, say, modulo 3, 7, or 13, since these moduli are coprime to 10.

Turning to systems consisting of more than two congruences, we deal only with the case when the moduli are *pairwise* coprime (see Exercise 2.6.13 for the general case). This result was known by the Chinese mathematician Sun Tsu about 2000(!) years ago, therefore it is generally referred to as the Chinese Remainder Theorem.

Theorem 2.6.2 (Chinese Remainder Theorem). *Let $m_1, \ldots, m_k$ be pairwise coprime. Then the system of congruences*

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \\ &\vdots \\ x &\equiv c_k \pmod{m_k} \end{aligned} \tag{2.6.8}$$

is solvable for any integers $c_1, \ldots, c_k$, and the solutions form one residue class modulo $m_1 m_2 \ldots m_k$. ♣

First proof. We can easily obtain the result from Theorem 2.6.1A by induction on k.

The case $k = 2$ is just Theorem 2.6.1A.

Assume now that the statement is true for systems of $k-1$ congruences, and consider the system (2.6.8) of k congruences. The integers satsifying the first $k-1$ congruences constitute one residue class modulo $m_1 m_2 \dots m_{k-1}$ by the induction hypothesis, so we can replace the first $k-1$ congruences by the congruence $x \equiv c \pmod{m_1 m_2 \dots m_{k-1}}$ with a suitable integer c. Thus, (2.6.8) is equivalent to the system

$$\begin{aligned} x &\equiv c \pmod{m_1 m_2 \dots m_{k-1}} \\ x &\equiv c_k \pmod{m_k} \end{aligned} \tag{2.6.9}$$

Applying Theorem 2.6.1A to (2.6.9), we obtain just the statement for k. □

Second proof. We show a new argument for solvability and we produce a solution in an explicit form (in a certain sense).

The procedure reminds us somewhat of the construction of the interpolation polynomials by Lagrange.

We consider first the special case of (2.6.8) when one c_i is 1 and all other c_j are 0, and then use this result to solve the general case.

Let us see the details. Let

$$M = m_1 \dots m_k \quad \text{and} \quad M_i = \frac{M}{m_i}, \quad i = 1, 2, \dots, k.$$

Since the moduli $m_1, \dots, m_k$ are pairwise coprime,

$$(M_i, m_i) = 1, \quad i = 1, 2, \dots, k. \tag{2.6.10}$$

I. We fix an index $1 \le i \le n$ and solve the problem in the special case when $c_i = 1$ and $c_j = 0$ for $j \ne i$ in (2.6.8).

The congruences $x \equiv 0 \ \big(\text{mod } m_j\big)$ mean that x is a multiple of every m_j with $j \ne i$. The moduli m_j are pairwise coprime, hence equivalently x is a multiple of the product M_i of the numbers m_j: $x = M_i z$.

Substituting this in the remaining congruence $x \equiv 1 \pmod{m_i}$, we obtain

$$M_i z \equiv 1 \pmod{m_i}. \tag{2.6.11}$$

This a linear congruence for z that is solvable by (2.6.10).

Let b_i be a solution of (2.6.11). Then $x = b_i M_i$ is a solution of (2.6.8).

II. We consider now the general case with arbitrary c_i in (2.6.8). We show that

$$x = c_1 b_1 M_1 + \dots + c_k b_k M_k \quad (\text{where } M_i b_i \equiv 1 \pmod{m_i}, i = 1, \dots, k) \tag{2.6.12}$$

is a solution of (2.6.8).

Let us check for example the congruence $x \equiv c_3 \pmod{m_3}$. Since $b_3 M_3 \equiv 1 \pmod{m_3}$ and all the other M_j are divisible by m_3, therefore the right-hand side of (2.6.12)

$$c_1 b_1 M_1 + \dots + c_k b_k M_k \equiv c_3 b_3 M_3 \equiv c_3 \pmod{m_3}.$$ □

An important corollary of Theorem 2.6.2 is that any congruence with a composite modulus can be reduced to congruences with prime power moduli. If the standard form of m is $m = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, then the congruence

$$f(x) \equiv 0 \pmod{m} \tag{2.6.13}$$

is equivalent to the system

$$\begin{aligned} f(x) &\equiv 0 \left(\bmod\ p_1^{\alpha_1}\right) \\ f(x) &\equiv 0 \left(\bmod\ p_2^{\alpha_2}\right) \\ &\ \vdots \\ f(x) &\equiv 0 \left(\bmod\ p_r^{\alpha_r}\right). \end{aligned} \tag{2.6.14}$$

We solve every congruence of (2.6.14) separately. If some of them are not solvable, then (2.6.13) is not solvable either. If all of them are solvable, then consider a solution of each, say $h_1, \dots, h_r$. Now, solving the system

$$\begin{aligned} x &\equiv h_1 \left(\bmod\ p_1^{\alpha_1}\right) \\ x &\equiv h_2 \left(\bmod\ p_2^{\alpha_2}\right) \\ &\ \vdots \\ x &\equiv h_r \left(\bmod\ p_r^{\alpha_r}\right), \end{aligned}$$

we get a solution of the original congruence (2.6.13). We obtain all solutions by considering all possible solution systems $h_1, \dots, h_r$ for the congruences (2.6.14).

Example E1. Solve the congruence

$$10x^{84} + 3x + 7 \equiv 0 \pmod{245}. \tag{2.6.15}$$

By the above, (2.6.15) is equivalent to the system

$$10x^{84} + 3x + 7 \equiv 0 \pmod{5} \tag{2.6.16}$$

$$10x^{84} + 3x + 7 \equiv 0 \pmod{49}. \tag{2.6.17}$$

(2.6.16) is identical to $3x + 7 \equiv 0 \pmod{5}$ since $10 \equiv 0 \pmod{5}$. The only solution of this linear congruence is

$$x \equiv 1 \pmod{5}. \tag{2.6.16a}$$

In looking for the solutions of (2.6.17), we distinguish two cases:

(i) $(x, 49) = 1$

(ii) $(x, 49) \neq 1$.

In case (i),

$$x^{84} = x^{2\varphi(49)} \equiv 1 \pmod{49},$$

by the Euler–Fermat Theorem. Thus (2.6.17) is equivalent to $3x + 17 \equiv 0 \pmod{49}$ in this case. This has one solution

$$x \equiv -22 \pmod{49}. \tag{2.6.17a}$$

In case (ii), $7 \mid x$. Then $x^{84} \equiv 0 \pmod{49}$. Thus (2.6.17) is equivalent to $3x + 7 \equiv 0 \pmod{49}$ in this case. The only solution (satisfying also the condition $7 \mid x$) is

$$x \equiv 14 \pmod{49}. \tag{2.6.17b}$$

Thus, the solutions of (2.6.15) are obtained from the systems

(2.6.16a) $$x \equiv 1 \pmod{5}.$$

(2.6.17a) $$x \equiv -22 \pmod{49}.$$

and

(2.6.16a) $$x \equiv 1 \pmod{5}.$$

(2.6.17b) $$x \equiv 14 \pmod{49}.$$

To determine the solutions, we can use the procedure in the proof of Theorem 2.6.1, but it is often more convenient to apply the following method.

From the congruence (2.6.17a)—using the larger modulus—-we have:

(2.6.18) $$x = 49z - 22.$$

Substituting (2.6.18) into (2.6.16a), we get

$$49z - 22 \equiv 1 \pmod{5}.$$

We find that

(2.6.19) $$z \equiv 2 \pmod{5} \quad \text{so} \quad z = 5w + 2.$$

Substituting (2.6.19) back into (2.6.18), we obtain $x = 245w + 76$. Thus the solution of the first system of congruences is $x \equiv 76 \pmod{245}$.

Proceeding similarly, the solution of the second system is $x \equiv 161 \pmod{245}$.

Thus all solutions of (2.6.15) are

$$x \equiv 76 \pmod{245} \quad \text{and} \quad x \equiv 161 \pmod{245}.$$

Finally, we discuss an application of the Chinese Remainder Theorem in computer science. Many operations in computers are composed of a sequence of additions, subtractions, and multiplications of integers. Therefore, it is essential to know how quickly these basic steps can be performed.

Consider e.g. addition. Using the usual representation in a number system, the addition of digits cannot be done independently since overflows influence the result significantly. In the so-called *remainder number systems*, however, we can perform the operations with the "digits." i.e. remainders, absolutely independently. This is mostly used if there are many parallel processors available.

The main point of the method is the following. Assume that only integers with absolute value less than N can occur during the operations. (This is no restriction since every computer can display and work with numbers only up to a given limit.) Let $m = p_1 \dots p_r$ be the product of the first r (positive) primes, and choose r to satisfy $m > 2N$.

Then every integer with absolute value less than N is equal to its remainder of least absolute value modulo m. And this can be represented by the system of remainders modulo p_i, which will be the digits in the remainder number system.

The digits actually are a simultaneous system of congruences where the moduli p_i are pairwise coprime, hence the remainder modulo m, i.e. the original number itself, can be uniquely reconstructed.

Adding or multiplying two numbers, we have to add or multiply the corresponding remainders (i.e. digits), there is no overflow, and the operations can be performed independently for the various moduli. From the system of the remainders modulo p_i thus obtained, we have to determine the remainder modulo m, i.e. the number itself.

Example E2. As an illustration, let $N = 1000$, and we execute the multiplication $27 \cdot 34$ in the remainder number system.

We can take

$$m = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2310.$$

The remainders of 27 when divided by the primes 2, 3, 5, 7, and 11 are 1, 0, 2, 6, and 5, so the representation of 27 in the remainder number system is

$$27 = (1, 0, 2, 6, 5).$$

Similarly,

$$34 = (0, 1, 4, 6, 1).$$

To do the multiplication $27 \cdot 34$, we multiply the corresponding digits (there is no overflow), reduce the products modulo p_i, and solve the resulting system of congruences:

$$27 \cdot 34 = (1 \cdot 0, 0 \cdot 1, 2 \cdot 4, 6 \cdot 6, 5 \cdot 1) = (0, 0, 3, 1, 5).$$

The solution of the system

$$\begin{aligned} x &\equiv 0 \pmod{2} \\ x &\equiv 0 \pmod{3} \\ x &\equiv 3 \pmod{5} \\ x &\equiv 1 \pmod{7} \\ x &\equiv 5 \pmod{11} \end{aligned}$$

is

$$x \equiv 918 \pmod{2310}.$$

Thus, $27 \cdot 34 = 918$.

If we perform more operations, we can keep working with the form in the remainder number system and convert only the final result into the usual representation of numbers.

We mention that systems of congruences can similarly be applied also to solve systems of linear equations (with rational coefficients). The main point of the method is that the system of equations is handled modulo various prime moduli, and from the solutions obtained we determine the solution modulo the product of these primes. This yields the solution wanted if certain conditions are satisfied and sufficiently many moduli are used. The advantage of the method in contrast with the traditional Gaussian elimination is that no too large (or too small) numbers can occur here, and thus there is no danger of overflow.

Exercises 2.6

(We use decimal representation unless stated otherwise.)

1. (a) A centipede wants to count its feet knowing that their number does not exceed 250. Counting them in elevens and in fifteens, 5 and 3 are left out. How many feet has the centipede?

   (b) Another centipede tries this method, too. It counts its feet by twelves and fifteens and finds that 4 and 8 are left out. Prove that it made a miscalculation.

2. The last digit of an integer in number system with base 20 is "eleven". What can be its last digit with base (a) 9 (b) 8?

3. Solve the congruences:

   (a) $2x^{20} + 3x + 4 \equiv 0 \pmod{176}$

   (b) $21x^{66} + 16x^{30} + 11x + 6 \equiv 0 \pmod{333}$

   (c) $3x^9 + 5x + 7 \equiv 0 \pmod{105}$.

4. Let a, b, and c be pairwise coprime integers greater than 1. What is the remainder

   (a) of $a^{\varphi(b)} + b^{\varphi(a)}$ modulo ab

   (b) of $a^{\varphi(bc)} + b^{\varphi(ac)} + c^{\varphi(ab)}$ modulo abc?

5. Determine the last three digits of 1234^{9876}.

6. I thought of an integer between 200 and 2000. Adding its 501st and 201st power to the original number, the sum will terminate in 998. Which number did I think of?

7. Which are those (a) two digit (b) three digit positive integers whose squares terminate in the same two and three digits, respectively?

8. (a) How many 21-digit positive integers have the property that every power of them terminates with the same 20 digits as the original number?

   (b) How many 21-digit positive integers have the property that every *odd* power of them terminates with the same 20 digits as the original number?

S 9. What will be the exact time (in hours and minutes) $39^{38^{37}}$ minutes after midnight?

10. (a) Let $(a, b) = 1$, and $r_1, \dots, r_{\varphi(a)}$ and $s_1, \dots, s_{\varphi(b)}$ be reduced residue systems modulo a and modulo b. For $i = 1, \dots, \varphi(a)$, $j = 1, \dots, \varphi(b)$, denote by c_{ij} a solution of the system

$$x \equiv r_i \pmod{a}$$
$$x \equiv s_j \pmod{b}\,.$$

   Show that the c_{ij} form a reduced residue system modulo ab. Use only the *definition* of the reduced residue system (Definition 2.2.8) during the proof, and do not rely on Theorem 2.2.9 or on part (b) of this exercise.

   (b) Give a new proof for $(a, b) = 1 \implies \varphi(ab) = \varphi(a)\varphi(b)$.

11. Verify that there are arbitrarily large gaps in the sequence of squarefree numbers. That is, for any K, there exist K consecutive positive integers none of which is squarefree.

* 12. (a) Prove that the following two systems are solvable for any positive integers a, b, and c.

(a1) $x \equiv a + b \pmod{c}$
$x \equiv b + c \pmod{a}$
$x \equiv c + a \pmod{b}$

(a2) $x \equiv ab \pmod{c}$
$x \equiv bc \pmod{a}$
$x \equiv ca \pmod{b}$.

(b) Show that

$$x \equiv b \pmod{c}, \qquad x \equiv c \pmod{a}, \qquad x \equiv a \pmod{b}$$

is solvable if and only if $(a, b) = (b, c) = (c, a)$.

* 13. Demonstrate that the system

$$x \equiv c_1 \pmod{m_1}, \quad x \equiv c_2 \pmod{m_2}, \quad \dots, \quad x \equiv c_k \pmod{m_k}$$

(where the moduli m_i are not necessarily pairwise coprime) is solvable if and only if $(m_i, m_j) \mid c_i - c_j$ for every $1 \le i < j \le k$.

14. Does there exist a polynomial $f(x)$ with integer coefficients for which the congruence $f(x) \equiv 0 \pmod{30}$ has exactly 14 solutions?

15. (a) Prove that there exist integers forming both a complete residue system modulo n and a reduced residue system modulo k if and only if $\varphi(k) = n$ and $(k, n) = 1$.

** (b) Prove that there exist integers forming a reduced residue system both modulo n and modulo k if and only if $\varphi(n) = \varphi(k)$.

16.* (a) Verify that for any distinct integers a_1, a_2, and a_3, there exist infinitely many positive numbers n such that $a_1 + n$, $a_2 + n$, and $a_3 + n$ are pairwise coprime.

(b) Find distinct integers a_1, a_2, a_3, and a_4 such that the numbers $a_i + n$, $i = 1, 2, 3, 4$ are not pairwise coprime for any n.

* (c) Demonstrate that for any distinct integers a_1, a_2, a_3, and a_4, there exist infinitely many positive numbers n such that $(a_i + n, a_j + n) \le 2$ for every $i \ne j$.

* (d) Verify that for any distinct integers a_1, a_2, a_3, and a_4, there exist infinitely many positive numbers n such that $(a_i + n, a_j + n, a_k + n) = 1$ for all $1 \le i < j < k \le 4$.

* (e) Do the statements in (c) and (d) remain valid if we increase the number of integers a_i from four to five or six?

2.7. Wilson's Theorem

Theorem 2.7.1 (Wilson's Theorem). *If p is a (positive) prime, then $(p-1)! \equiv -1 \pmod{p}$.* ♣

Since the numbers $1, 2, \dots, p-1$ form a reduced residue system modulo p and the product of the elements of every reduced residue system gives the same remainder modulo p, we can rewrite Wilson's Theorem in the following form:

If p is a (positive) prime, then the product of the elements of a reduced residue system is congruent to -1 modulo p.

We discuss generalizations for composite moduli and connections with group theory in Exercise 2.7.1 and in Section 2.8.

Proof. The theorem is clearly true for $p = 2$ and $p = 3$.

We show that for $p \geq 5$, the numbers $2, 3, \dots, p-2$ can be paired so that the product of the two elements in every pair is congruent to 1 modulo p. This implies the theorem since then $2 \cdot 3 \cdot \dots \cdot (p-2) \equiv 1 \pmod{p}$, hence

$$(p-1)! = 2 \cdot 3 \cdot \dots \cdot (p-2) \cdot 1 \cdot (p-1) \equiv 1 \cdot 1 \cdot (p-1) \equiv -1 \pmod{p}.$$

We illustrate the pairing first for $p = 11$. The mate of 2 is obtained from the congruence $2x \equiv 1 \pmod{11}$. Its only solution is $x \equiv 6 \pmod{11}$, so 2 is matched with 6. Here, 2 and 6 correspond to each other mutually as $2 \cdot 6 = 6 \cdot 2 \equiv 1 \pmod{11}$.

Continuing similarly, we obtain the pairs 3–4, 5–9, and 7–8. Thus

$$10! = (2 \cdot 6) \cdot (3 \cdot 4) \cdot (5 \cdot 9) \cdot (7 \cdot 8) \cdot 1 \cdot 10 \equiv 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot (-1) = -1 \pmod{11}.$$

Let us see how this works in general. We have to verify the following facts to obtain a perfect match:

(i) To every integer $2 \leq a \leq p-2$, there exists exactly one $b = f(a)$ satisfying

$$ab \equiv 1 \pmod{p} \quad \text{and} \quad 2 \leq b \leq p-2.$$

(ii) If $f(a) = b$, then $f(b) = a$, so a and b are assigned mutually to each other.

(iii) $f(a) \neq a$, so no element is the partner of itself.

(i) Since $(a, p) = 1$, the congruence $ax \equiv 1 \pmod{p}$ is solvable and has exactly one solution b in the complete residue system $0, 1, 2, \dots, p-1$. If $x = 0, 1$, or $p-1$, then $ax \equiv 0, a$, or $-a \pmod{p}$, thus $ax \not\equiv 1 \pmod{p}$ for these values of x. Hence, b falls in the interval $2 \leq b \leq p-2$, as required.

(ii) The condition $f(a) = b$ means $ab \equiv 1 \pmod{p}$. The value of $f(b)$ is the solution of the congruence $by \equiv 1 \pmod{p}$. Clearly, $y = a$ is a solution and we know from (i) that there is exactly one solution in the interval $2 \leq y \leq p-2$. Hence, necessarily $f(b) = a$.

(iii) The condition $b = a$ would mean $a^2 \equiv 1 \pmod{p}$. Considering the corresponding divisibility and using the prime property of p, we obtain

$$p \mid (a-1)(a+1) \Longrightarrow p \mid a-1 \text{ or } p \mid a+1 \Longrightarrow a \equiv \pm 1 \pmod{p}.$$

This, however, contradicts the condition $2 \leq a \leq p-2$. □

For further proofs of Wilson's Theorem, see the note after Theorem 3.1.2 and Exercise 3.3.6.

Exercises 2.7

(Primes are assumed to be positive.)

1. *Generalizations of Wilson's Theorem for composite moduli.* Let m be composite. What is the remainder modulo m of

   (a) $(m-1)!$

   * (b) $\big(\varphi(m)\big)!$

   * (c) the product of all elements of a reduced residue system?

2. Which integers $m > 6$ satisfy $(m-6)! \equiv 1 \pmod{m}$?

3. Let $a_1, \ldots, a_m$ and $b_1, \ldots, b_m$ be any two permutations of $1, 2, \ldots, m$.

   (a) Show that if $m > 2$ is a prime, then there exist i and j, $i \neq j$ satisfying
   $$m \mid a_i b_i - a_j b_j .$$

   * (b) Prove the same assertion if m is composite.

4. Let p be a prime of the form $4k-1$. Prove
   $$\Big(\frac{p-1}{2}\Big)! \equiv \pm 1 \pmod{p}.$$

5. Verify
   $$p^p \mid (p^2-1)! - p^{p-1}$$
   for any prime p.

6. Let $p > 3$ be a prime. What is the remainder of $3(p-3)!$ modulo p?

7. What is the remainder of 99! when divided by 10100?

8. Compute the possible values of $\big(n!+3, (n+2)!+6\big)$ if n is a positive integer.

9. For which m does there exist a (a) complete (b) reduced residue system of numbers of the form $k!$?

10. Let $a_1, \ldots, a_{30}$ be a reduced residue system modulo 31. Prove
    $$31 \mid (a_1 a_2 a_3)^3 + (a_4 a_5 \ldots a_{30})^{27}.$$

11. Let $p > 2$ be a prime and construct an arithmetic progression of $p-1$ integers. What can the remainder of the product of its elements modulo p be?

12. Solve the congruence $x!\,(z-x)! \equiv 1 \pmod{z}$ where $0 < x < z$ are integers.

* 13. For which primes p is $(p-1)!+1$ a power of p (with positive integer exponents)?

2.8. Operations with Residue Classes

We define an addition and a multiplication for residue classes modulo m and investigate their properties. We assume throughout that the modulus $m > 1$ is fixed.

Definition 2.8.1. The *sum* and *product* of the residue classes $(a)_m$ and $(b)_m$ are the residue classes $(a+b)_m$ and $(ab)_m$, i.e.

$$(a)_m + (b)_m = (a+b)_m \quad \text{and} \quad (a)_m(b)_m = (ab)_m. \qquad ♣$$

We have to verify that we have defined the operations so that both addition and multiplication assign a *unique* residue class to any two given residue classes.

The difficulty is that addition and multiplication of residue classes were defined using representatives, thus we have to clarify that the resulting residue classes do not depend on which representatives in the initial two classes were chosen.

Consider addition. We have to show that if $(a)_m = (a')_m$ and $(b)_m = (b')_m$, then $(a+b)_m = (a'+b')_m$. This holds since

$$\left.\begin{array}{lll}(a)_m = (a')_m & \Longrightarrow & a \equiv a' \pmod{m}\\ (b)_m = (b')_m & \Longrightarrow & b \equiv b' \pmod{m}\end{array}\right\} \Longrightarrow a+b \equiv a'+b' \pmod{m}$$
$$\Longrightarrow (a+b)_m = (a'+b')_m.$$

We can argue similarly about multiplication.

We must be aware that there are many operations on the integers that cannot be defined for residue classes using representatives. We illustrate this by an example; for some further examples see Exercise 2.8.6.

Let a and b be integers and denote by $\max(a,b)$ the larger one (or their common value if $a = b$). This maximum assigns a unique integer to any two integers, so it is a well defined operation on the integers.

Among the residue classes modulo m, however, the specification $\max\big((a)_m,(b)_m\big) = \big(\max(a,b)\big)_m$ does not define an operation, since the right-hand side of the equality (may) give different residue classes if we represent $(a)_m$ and/or $(b)_m$ with another element. For example, let the modulus be $m = 9$ and consider the two residue classes $A = (3)_9 = (12)_9$ and $B = (10)_9 = (1)_9$. Then $\max(A,B)$ would be $\big(\max(3,10)\big)_9 = (10)_9$ on the one hand and $\big(\max(12,1)\big)_9 = (12)_9$ on the other hand but $(10)_9 \neq (12)_9$.

We turn now to study the most important properties of addition and multiplication defined on the residue classes.

We can easily derive that most properties valid among the integers hold also for the residue classes:

Theorem 2.8.2. *Among the residue classes modulo m,*

- *addition is* associative *and* commutative
- $(0)_m$ *is a* zero element, *i.e.* $(0)_m + (a)_m = (a)_m + (0)_m = (a)_m$ *holds for every* $(a)_m$
- *the* negative *of* $(a)_m$ *is* $(-a)_m$, *i.e.* $(-a)_m + (a)_m = (a)_m + (-a)_m = (0)_m$
- *multiplication is* associative *and* commutative

- $(1)_m$ *is an* identity element, *i.e.* $(1)_m(a)_m = (a)_m(1)_m = (a)_m$ *holds for every* $(a)_m$
- *the* distributive law *is valid.* ♣

Proof. Each statement follows immediately from the definition of the operations and from the corresponding property of the integers. We illustrate this for the commutative law for addition:

$$(a)_m + (b)_m = (a+b)_m = (b+a)_m = (b)_m + (a)_m$$

(we applied the definition of addition for residue classes in the first and third equalities and the commutative law for the addition of integers in the second equality). □

Summarizing the properties listed in Theorem 2.8.2, the residue classes modulo m form a *commutative ring with identity element* with respect to addition and multiplication.

We mention that—as in every ring—also *subtraction* can be performed for residue classes, i.e. to any $(a)_m$ and $(b)_m$, there exists exactly one $(c)_m$ satisfying $(a)_m = (b)_m + (c)_m$; we obtain this $(c)_m$ as $(a)_m + (-b)_m$. (We can verify the existence of subtraction also by relying on subtraction among the integers; then we have $(c)_m = (a-b)_m$.)

We examine now which residue classes have a *multiplicative inverse* (or "reciprocal"), i.e. for which $(a)_m$ does there exist a residue class $(c)_m$ satisfying

$$(c)_m(a)_m = (a)_m(c)_m = (1)_m? \tag{2.8.1}$$

Condition (2.8.1) is equivalent to $(ac)_m = (1)_m$, i.e. to $ac \equiv 1 \pmod{m}$ which means that the linear congruence $ax \equiv 1 \pmod{m}$ is solvable. By Theorem 2.5.3, this holds if and only if $(a,m) \mid 1$, or $(a,m) = 1$. This is exactly the case when $(a)_m$ is a reduced residue class. Thus, we have proved:

Theorem 2.8.3. *Among the residue classes modulo m, exactly the reduced residue classes have a multiplicative inverse.* ♣

We note that for any associative operation, every element can have only one inverse. Thus, the inverse of a reduced residue class is unique, as well. (This follows also from Theorem 2.5.5.)

A *field* is a commutative ring (with at least two elements) that has an identity element and every non-zero element has an inverse. By Theorem 2.8.3, the residue classes satisfy these requirements if and only if every non-zero residue class is reduced, i.e. m is a prime. This gives the result:

Theorem 2.8.4. *The residue classes modulo m form a field if and only if m is a prime.* ♣

It can occur that the product of two non-zero residue classes is the zero residue class, e.g. $(5)_{10}(4)_{10} = (0)_{10}$. A residue class $(a)_m \neq (0)_m$ is called a *zero divisor* if

$$\text{there exists some } (b)_m \neq (0)_m \text{ satisfying } (a)_m(b)_m = (0)_m. \tag{2.8.2}$$

Thus, $(4)_{10}$ and $(5)_{10}$ are zero divisors in the previous example.

Theorem 2.8.5. *A residue class* $(a)_m \neq (0)_m$ *is a zero divisor if and only if* $(a)_m$ is not *a reduced residue class, i.e.* $(a,m) \neq 1$. ♣

The condition $(a)_m \neq (0)_m$ means $m \nmid a$ or $(a, m) < m$ for the representative a.

Proof. Rephrasing the definition in (2.8.2), the residue class $(a)_m \neq (0)_m$ is a zero divisor if and only if

(2.8.3) there exists some $b \not\equiv 0 \pmod{m}$ satisfying $ab \equiv 0 \pmod{m}$.

Since $x \equiv 0 \pmod{m}$ is always a solution of $ax \equiv 0 \pmod{m}$, (2.8.3) means that $ax \equiv 0 \pmod{m}$ has more solutions. The number of solutions is (a, m), hence $(a)_m \neq (0)_m$ is a zero divisor if and only if $(a, m) > 1$. □

We see from Theorem 2.8.5 that residue classes modulo m contain a zero divisor if and only if m is composite.

Finally, we touch briefly some group theoretic connections of the residue classes.

A set G is called a *group* if an associative operation with an identity element is defined on G and every element has an inverse. If the operation is commutative we have a *commutative* or *Abelian* group.

Thus, the residue classes modulo m form a commutative group under addition, and the same is true for the reduced residue classes with respect to multiplication (this follows from the fact that the product of two reduced classes and the inverse of a reduced class is a reduced class again).

The Euler–Fermat Theorem can be considered as a special case of a general theorem for groups: For any element a of a finite group G, $a^{|G|}$ is the identity element (where $|G|$ denotes the number of elements in the group). This general result can be verified similarly to the Euler–Fermat Theorem for commutative groups (see Exercise 2.8.7) and follows from *Lagrange's Theorem* for arbitrary G.

Generalizing Wilson's theorem, we can ask which element of a finite commutative group will be equal to the product of all its elements (see Exercise 2.8.8).

Exercises 2.8

1. For which m does there exist a non-zero residue class that is the negative of itself?
2. Consider the ring of the residue classes modulo 100.
   (a) What is the multiplicative inverse of the residue class (13)?
   (b) What is the number of zero divisors?
   (c) How many zero divisor pairs belong to (40), i.e. how many residue classes $(b) \neq (0)$ satisfy $(40)(b) = (0)$?
   (d) Does there exist a residue class (c) satisfying $(35)(c) = (90)$?
3. How many residue classes modulo m are their own multiplicative inverses if m is
   (a) 47
   (b) 30
   (c) 800
   * (d) arbitrary?

4. Consider the ring of residue classes modulo a composite m.
   (a) Show that if (a) is a zero divisor, then $(a)(c)$ is a zero divisor or (0) for any (c).
   (b) Demonstrate that if $(a)(c)$ is a zero divisor, then at least one of (a) and (c) is a zero divisor.
   (c) Determine all m where the sum of any two zero divisors is a zero divisor or (0).
   (d) Compute the sum and product of all zero divisors.
   (e) For which m does there exist an $(a) \neq (0)$ satisfying $(a)^2 = (0)$?

5. (a) Let H be the set of those residue classes modulo 20 that are "divisible" by 4, i.e.

$$H = \{(0)_{20}, (4)_{20}, (8)_{20}, (12)_{20}, (16)_{20}\}.$$

   Prove that H is a field under the addition and multiplication of residue classes.

   (b) Let K be the set of those residue classes modulo 40 that are divisible by 4, i.e.

$$K = \{(0)_{40}, (4)_{40}, \dots, (36)_{40}\}.$$

   Verify that K is a commutative ring under the addition and multiplication of residue classes, but it is not a field, it has no identity element, and every nonzero element is a zero divisor.

S* (c) Generalize the problem (as far as possible).

6. Examine in detail whether it is possible to define the following operations for residue classes modulo m using their positive representatives.
   (a) Gcd: $\gcd\big((a)_m, (b)_m\big) = \big(\gcd(a, b)\big)_m$
   (b) Third power: $(a)_m^3 = (a^3)_m$
   (c) Cube root: $\sqrt[3]{(a)_m} = (\sqrt[3]{a})_m$
   (d) Arithmetic mean: $\big((a)_m + (b)_m\big)/2 = \big((a + b)/2\big)_m$
   (e) Exponentiation: $(a)_m^{(b)_m} = \big(a^b\big)_m$.

7. *Generalization of the Euler–Fermat Theorem.* In a finite commutative group G, let $|G|$ denote the number of elements and e be the identity element. Prove that $a^{|G|} = e$ holds for any $a \in G$.

* 8. *Generalization of Wilson's Theorem.* In a finite commutative group G, let e be the identity element and P the product of all elements. Show that if G contains exactly one element $c \neq e$ satisfying $c^2 = e$, then $P = c$, and $P = e$ in all other cases.