# ELEMENTARY NUMBER THEORY


## W W L CHEN




# Chapter 3

## CONGRUENCES

### 3.1. Introduction

Suppose that $m \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. Then we say that $a$ is congruent to $b$ modulo $m$, denoted by $a \equiv b \pmod{m}$, if $m \mid (a - b)$.

Suppose that $m \in \mathbb{N}$ and $c \in \mathbb{Z}$. Then by Theorem 1A, there exist unique $q, r \in \mathbb{Z}$ such that $c = mq + r$ and $0 \le r < m$. The number $r$ is called the residue of $c$ modulo $m$, and $c$ is said to belong to the residue class $r$ modulo $m$.

We make no notational distinction between numbers $r \in \mathbb{Z}$ and the residue classes $r$. We shall use the convention that whenever $r$ denotes a residue class, this will be explicitly stated in the text.

The following three results are simple consequences of our definition.

**THEOREM 3A.** *Suppose that $m \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. Then $a \equiv b \pmod{m}$ if and only if $a$ and $b$ belong to the same residue class modulo $m$.*

PROOF. Suppose that $a \equiv b \pmod{m}$. If $a$ belongs to the residue class $r$ modulo $m$, where $r \in \mathbb{Z}$ and $0 \le r < m$, then there exists $q_1 \in \mathbb{Z}$ such that $a = mq_1 + r$. Since $a \equiv b \pmod{m}$, there exists $q \in \mathbb{Z}$ such that $b = a + mq$. It follows that $b = m(q_1 + q) + r$, and so $b$ also belongs to the residue class $r$ modulo $m$.

Conversely, suppose that $a$ and $b$ belong to the same residue class $r$ modulo $m$, where $0 \le r < m$. Then there exist $q_1, q_2 \in \mathbb{Z}$ such that $a = mq_1 + r$ and $b = mq_2 + r$. It follows that $a - b = m(q_1 - q_2)$, and so $a \equiv b \pmod{m}$. ○

**THEOREM 3B.** *Suppose that $m \in \mathbb{N}$, and $a_1, a_2, b_1, b_2 \in \mathbb{Z}$. Suppose further that $a_1 \equiv b_1 \pmod{m}$ and $a_2 \equiv b_2 \pmod{m}$. Then*
*(i)* $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$*; and*
*(ii)* $a_1 a_2 \equiv b_1 b_2 \pmod{m}$.

PROOF. (i) is trivial. (ii) follows from $a_1a_2 - b_1b_2 = (a_1 - b_1)a_2 + b_1(a_2 - b_2)$. ○

**THEOREM 3C.** *Suppose that $m \in \mathbb{N}$, and $a, b, c \in \mathbb{Z}$ with $c \neq 0$.*
*(i) If $ac \equiv bc \pmod{m}$, then $a \equiv b \pmod{m/(c, m)}$.*
*(ii) If further that $(c, m) = 1$, then $a \equiv b \pmod{m}$.*

The proof is left as an exercise.

## 3.2. Sets of Residues

Suppose that $m \in \mathbb{N}$. Consider the set $M = \{0, 1, 2, \ldots, m - 1\}$. A set $S$ of $m$ integers is said to be a complete set of residues modulo $m$ if for every integer $a \in M$, there exists a unique element $x \in S$ such that $x \equiv a \pmod{m}$. It is easy to see that $S$ is a complete set of residues modulo $m$ if and only if $S$ contains exactly $m$ elements and $x \not\equiv y \pmod{m}$ for any distinct $x, y \in S$.

On the other hand, the subset $M^* = \{a \in M : (a, m) = 1\}$ has $\phi(m)$ elements. A set $T$ of $\phi(m)$ integers is said to be a reduced set of residues modulo $m$ if for every integer $a \in M^*$, there exists a unique element $x \in T$ such that $x \equiv a \pmod{m}$. It is easy to see that $T$ is a reduced set of residues modulo $m$ if and only if $T$ contains exactly $\phi(m)$ elements, all coprime to $m$, and $x \not\equiv y \pmod{m}$ for any distinct $x, y \in T$.

EXAMPLES. (i) The set $\{2, 4, 6\}$ is a complete set of residues modulo 3. The subset $\{2, 4\}$ is a reduced set of residues modulo 3.

(ii) Suppose that $p$ is prime. The set $\{1, 2, \ldots, p\}$ is a complete set of residues modulo $p$. The subset $\{1, 2, \ldots, p - 1\}$ is a reduced set of residues modulo $p$.

**THEOREM 3D.** *Suppose that $m \in \mathbb{N}$ and $k \in \mathbb{Z} \setminus \{0\}$, where $(k, m) = 1$.*
*(i) As $x$ runs through a complete set of residues modulo $m$, $kx$ runs through a complete set of residues modulo $m$.*
*(ii) As $x$ runs through a reduced set of residues modulo $m$, $kx$ runs through a reduced set of residues modulo $m$.*

PROOF. (i) Suppose that $S$ is a complete set of residues modulo $m$. If $x, y \in S$ and $x \not\equiv y \pmod{m}$, then it follows from Theorem 3C(ii) that $kx \not\equiv ky \pmod{m}$. Hence the set $\{kx : x \in S\}$ is a set of $m$ integers that are pairwise incongruent modulo $m$, and so is a complete set of residues modulo $m$.

(ii) Suppose that $T$ is a reduced set of residues modulo $m$. A similar argument shows that the set $\{kx : x \in T\}$ is a set of $\phi(m)$ integers that are pairwise incongruent modulo $m$. On the other hand, we know that $(kx, m) = 1$ whenever $(x, m) = 1$. It follows that the elements in the set $\{kx : x \in T\}$ are coprime to $m$, and so the set is a reduced set of residues modulo $m$. ○

**THEOREM 3E.** *Suppose that $a, b \in \mathbb{N}$, and $(a, b) = 1$.*
*(i) As $x$ runs through a complete set of residues modulo $a$ and $y$ runs through a complete set of residues modulo $b$, $bx + ay$ runs through a complete set of residues modulo $ab$.*
*(ii) As $x$ runs through a reduced set of residues modulo $a$ and $y$ runs through a reduced set of residues modulo $b$, $bx + ay$ runs through a reduced set of residues modulo $ab$.*

PROOF. (i) If $bx_1 + ay_1 \equiv bx_2 + ay_2 \pmod{ab}$, then $bx_1 \equiv bx_2 \pmod{a}$. It follows from Theorem 3C(ii) that $x_1 \equiv x_2 \pmod{a}$. Similarly $y_1 \equiv y_2 \pmod{b}$.

(ii) Since $(a, b) = 1$, we have $\phi(ab) = \phi(a)\phi(b)$. Suppose that $(x, a) = 1$ and $(y, b) = 1$. Then it is easy to check that

$$(bx + ay, a) = (bx, a) = (x, a) = 1.$$

Similarly,

$$(bx + ay, b) = (ay, b) = (y, b) = 1.$$

It follows easily that $(bx + ay, ab) = 1$. ○

## 3.3. Some Interesting Congruences

As an application of Theorem 3D, we prove the following famous result.

**THEOREM 3F.** (FERMAT-EULER) *Suppose that $m \in \mathbb{N}$ and $a \in \mathbb{Z} \setminus \{0\}$, where $(a, m) = 1$. Then $a^{\phi(m)} \equiv 1 \pmod{m}$.*

PROOF. Suppose that $r_1, \ldots, r_{\phi(m)}$ form a reduced set of residues modulo $m$. Then it follows from Theorem 3D that $ar_1, \ldots, ar_{\phi(m)}$ also form a reduced set of residues modulo $m$. Thus

$$r_1 \ldots r_{\phi(m)} \equiv (ar_1) \ldots (ar_{\phi(m)}) = a^{\phi(m)} r_1 \ldots r_{\phi(m)} \pmod{m}.$$

Clearly $(r_1 \ldots r_{\phi(m)}, m) = 1$. Hence $a^{\phi(m)} \equiv 1 \pmod{m}$, in view of Theorem 3C(ii). ○

A special case of Theorem 3F is the following.

**THEOREM 3G.** (FERMAT'S LITTLE THEOREM) *Suppose that $p$ is a prime and $a \in \mathbb{Z}$, where $p \nmid a$. Then $a^{p-1} \equiv 1 \pmod{p}$.*

## 3.4. Some Linear Congruences

Suppose that $f : \mathbb{Z} \to \mathbb{Z}$ is a given polynomial with integer coefficients, and $m \in \mathbb{N}$. By the number of solutions of the congruence $f(x) \equiv 0 \pmod{m}$, we mean the number of elements $x$ in a complete set of residues modulo $m$ for which the congruence holds; in other words, the number of incongruent numbers $x$ modulo $m$ for which the congruence holds.

Our first result concerns the simplest of congruences.

**THEOREM 3H.** *Suppose that $m \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. Then the congruence*

$$ax \equiv b \pmod{m} \tag{1}$$

*is soluble if and only if $(a, m) \mid b$. In this case, the number of solutions is equal to $(a, m)$, and the congruence is satisfied by precisely all the numbers in a certain residue class modulo $m/(a, m)$.*

PROOF. The result is trivial if $a = 0$, so suppose that $a \neq 0$. If (1) is soluble, then there exist $x_0, y_0 \in \mathbb{Z}$ such that $ax_0 + my_0 = b$, and so $(a, m) \mid b$. Conversely, suppose that $(a, m) \mid b$. Since

$$\left( \frac{a}{(a, m)}, \frac{m}{(a, m)} \right) = 1,$$

it follows from Theorem 3D that the integers

$$0, \frac{a}{(a,m)}, \frac{2a}{(a,m)}, \ldots, \left(\frac{m}{(a,m)} - 1\right)\frac{a}{(a,m)}$$

form a complete set of residues modulo $m/(a,m)$. Hence one of the numbers $x_0$ in the set

$$\left\{0, 1, \ldots, \frac{m}{(a,m)} - 1\right\}$$

must satisfy

$$\frac{a}{(a,m)}x_0 \equiv \frac{b}{(a,m)} \quad \left(\text{mod } \frac{m}{(a,m)}\right), \tag{2}$$

whence

$$ax_0 \equiv b \quad (\text{mod } m), \tag{3}$$

and so (1) is soluble.

Furthermore, if $x \equiv x_0$ (mod $m/(a,m)$), then (2) and hence also (3) hold with $x_0$ replaced by $x$. To show that the residue class $x_0$ modulo $m/(a,m)$ gives all the solutions, let $x$ be any solution of (1). Then $a(x - x_0) \equiv 0$ (mod $m$). It follows from Theorem 3C(i) that $x - x_0 \equiv 0$ (mod $m/(a,m)$). ◯

Our next result concerns simultaneous linear congruences.

**THEOREM 3J.** (CHINESE REMAINDER THEOREM) *Suppose that $n > 1$, and that the natural numbers $m_1, \ldots, m_n \in \mathbb{N}$ are pairwise coprime; in other words, $(m_i, m_j) = 1$ whenever $1 \le i < j \le n$. Then for any $a_1, \ldots, a_n \in \mathbb{Z}$, the simultaneous congruences*

$$\begin{aligned} x &\equiv a_1 \quad (\text{mod } m_1) \\ &\vdots \\ x &\equiv a_n \quad (\text{mod } m_n) \end{aligned}$$

*are satisfied by precisely the members of a unique residue class modulo $m_1 \ldots m_n$.*

Proof. For every $j = 1, \ldots, n$, write $q_j = m_1 \ldots m_{j-1}m_{j+1} \ldots m_n$. Then $(q_j, m_j) = 1$. It follows from Theorem 3H that there exists $k_j \in \mathbb{Z}$ such that $q_jk_j \equiv a_j$ (mod $m_j$). Now let

$$x_0 = \sum_{j=1}^{n} q_jk_j.$$

If $x \equiv x_0$ (mod $m_1 \ldots m_n$), then $x \equiv x_0 \equiv q_ik_i \equiv a_i$ (mod $m_i$) for every $i = 1, \ldots, n$. On the other hand, if $x$ is a solution to the simultaneous congruences, then $x \equiv a_i \equiv x_0$ (mod $m_i$) for every $i = 1, \ldots, n$. Hence $x \equiv x_0$ (mod $m_1 \ldots m_n$). ◯

## 3.5. Some Polynomial Congruences

Our first result follows from Fermat's little theorem.

**THEOREM 3K.** *Suppose that $p$ is prime. Then for any polynomial $f : \mathbb{Z} \to \mathbb{Z}$ with integer coefficients, there exists a polynomial $g : \mathbb{Z} \to \mathbb{Z}$ with integer coefficients and of degree less than $p$ such that $f(x) \equiv g(x)$ (mod $p$) for every $x \in \mathbb{Z}$.*

Proof. In view of Theorem 3B, it suffices to prove Theorem 3K for the polynomial $f(x) = x^n$, where $n$ is a fixed positive integer. It is not difficult to show that there exist $q, r \in \mathbb{Z}$ such that $n = (p-1)q + r$ and $1 \le r \le p-1$. If $p \nmid x$, then it follows from Theorem 3G that

$$x^n = (x^{p-1})^q x^r \equiv 1^q x^r \equiv x^r \pmod{p},$$

whence the result. If $p \mid x$, then $x \equiv 0 \pmod{p}$, so that $x^n \equiv 0 \equiv x^r \pmod{p}$. ◯

Having reduced the degree of the polynomial, we now show that in many cases, we cannot have too many solutions.

**THEOREM 3L.** (LAGRANGE) *Suppose that $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$ is a polynomial with integer coefficients. Suppose further that $p$ is prime, and $p \nmid a_n$. Then the congruence*

$$f(x) \equiv 0 \pmod{p} \tag{4}$$

*has at most $n$ solutions.*

Proof. The case $n = 0$ is trivial. The case $n = 1$ follows from Theorem 3H. Let $n > 1$ and assume that the result is true for all polynomials of degree $n - 1$. Suppose on the contrary that (4) has at least $n + 1$ incongruent solutions $x_0, x_1, \ldots, x_n$. Then

$$f(x) - f(x_0) = \sum_{k=1}^{n} a_k(x^k - x_0^k) = (x - x_0)\sum_{k=1}^{n} a_k(x^{k-1} + x^{k-2}x_0 + \ldots + x_0^{k-1}) = (x - x_0)g(x),$$

where $g(x) = a_n x^{n-1} + \ldots$. It follows that $(x_j - x_0)g(x_j) \equiv 0 \pmod{p}$ for every $j = 1, \ldots, n$, and so $g(x_j) \equiv 0 \pmod{p}$, contradicting the inductive hypothesis. ◯

On the other hand, if a polynomial has many solutions, then we can say quite a lot about its coefficients.

**THEOREM 3M.** *Suppose that $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$ is a polynomial with integer coefficients. Suppose further that $p$ is prime, and the congruence $f(x) \equiv 0 \pmod{p}$ has more than $n$ solutions. Then $p \mid a_j$ for every $j = 0, 1, \ldots, n$.*

Proof. Suppose on the contrary that some coefficient is not divisible by $p$. Let $k$ be the largest index such that $p \nmid a_k$. Then $k \le n$. On the other hand, since

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_{k+1}x^{k+1} \equiv 0 \pmod{p}$$

for every $x \in \mathbb{Z}$, it follows that the congruence

$$a_k x^k + a_{k-1}x^{k-1} + \ldots + a_0 \equiv 0 \pmod{p}$$

has more than $k$ solutions, contradicting Theorem 3L. ◯

We conclude this section by using polynomial congruences to prove an interesting congruence result.

**THEOREM 3N.** (WILSON) *For every prime $p$, we have*

$$(p-1)! \equiv -1 \pmod{p}.$$

Proof. The polynomial

$$f(x) = (x^{p-1} - 1) - \prod_{m=1}^{p-1}(x - m)$$

has degree at most $(p-2)$, but has $(p-1)$ roots modulo $p$, in view of Theorem 3G. It follows from Theorem 3M that all the coefficients are divisible by $p$. Note that the coefficient of $x^0$ is $-1 - (-1)^{p-1}(p-1)!$. ◯

Remark. We can also prove Wilson's theorem in the following way. The theorem is obvious if $p \leq 3$, so we assume that $p > 3$. Suppose that $x \not\equiv 0 \pmod{p}$. Then it follows from Theorem 3H that there exists a unique $x'$ modulo $p$ such that $xx' \equiv 1 \pmod{p}$. Moreover, if $x \equiv x' \pmod{p}$, then $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$. It follows that the numbers $2, 3, \ldots, p-2$ can be paired off into $(p-3)/2$ mutually reciprocal pairs modulo $p$, so that $(p-2)! \equiv 1 \pmod{p}$. The result follows easily.

## 3.6. Primitive Roots

Suppose that $a \in \mathbb{Z} \setminus \{0\}$ and $m \in \mathbb{N}$, where $(a, m) = 1$. Then there exist numbers $n \in \mathbb{N}$ such that

$$a^n \equiv 1 \pmod{m}. \tag{5}$$

For example, as shown in Theorem 3F, the number $n = \phi(m)$ satisfies the requirement. The smallest $n \in \mathbb{N}$ for which the congruence (5) holds is called the exponent to which $a$ belongs modulo $m$.

**THEOREM 3P.** *Suppose that $a \in \mathbb{Z} \setminus \{0\}$ and $m \in \mathbb{N}$, where $(a, m) = 1$. If $a$ belongs to the exponent $n$ modulo $m$, then the numbers $1, a, a^2, \ldots, a^{n-1}$ are incongruent modulo $m$.*

Proof. Suppose on the contrary that there exist $\ell, k \in \mathbb{Z}$ such that $0 \leq \ell < k \leq n-1$ and $a^\ell \equiv a^k \pmod{m}$. Then $a^{k-\ell} \equiv 1 \pmod{m}$. But $k - \ell < n$, and this contradicts the minimality of $n$. ◯

**THEOREM 3Q.** *Suppose that $a \in \mathbb{Z} \setminus \{0\}$ and $m \in \mathbb{N}$, where $(a, m) = 1$. Suppose further that $a$ belongs to the exponent $n$ modulo $m$, and $\ell, k \in \mathbb{N} \cup \{0\}$. Then $a^\ell \equiv a^k \pmod{m}$ if and only if $\ell \equiv k \pmod{n}$. In particular, $a^\ell \equiv 1 \pmod{m}$ if and only if $n \mid \ell$.*

Proof. There exist $u, v, r, s \in \mathbb{Z}$ with $0 \leq r, s < n$ such that $\ell = nu + r$ and $k = nv + s$. Since $\ell, k \geq 0$, it follows that $u, v \geq 0$. By Theorem 3A, we have $\ell \equiv k \pmod{n}$ if and only if $r = s$. On the other hand, we have

$$a^\ell = (a^n)^u a^r \equiv a^r \pmod{m}$$

and

$$a^k = (a^n)^v a^s \equiv a^s \pmod{m}.$$

By Theorem 3P, we have $a^r \equiv a^s \pmod{m}$ if and only if $r = s$. The result follows. ◯

An immediate consequence of Theorems 3F and 3Q is that the exponent to which $a$ belongs modulo $m$ is a divisor of $\phi(m)$. However, if the exponent to which $a$ belongs modulo $m$ is actually $\phi(m)$, then we say that $a$ is a primitive root modulo $m$.

A natural question is then to determine those values of $m \in \mathbb{N}$ for which primitive roots modulo $m$ exist. Thanks to Gauss, we have a complete answer to this interesting question.

## 3.7. A Theorem of Gauss

Our first task is to show that there are certain values of $m \in \mathbb{N}$ for which primitive roots modulo $m$ exist. We have the following three results.

**THEOREM 3R.** *Suppose that $p$ is prime. Then for every $n \in \mathbb{N}$ satisfying $n \mid (p-1)$, there are exactly $\phi(n)$ incongruent numbers modulo $p$ which belong to the exponent $n$ modulo $p$. In particular, there are $\phi(p-1) = \phi(\phi(p))$ primitive roots modulo $p$.*

PROOF. Suppose that $n \mid (p-1)$. Let $\psi(n)$ denote the number of incongruent numbers modulo $p$ which belong to the exponent $n$ modulo $p$. We shall show that $\psi(n) = \phi(n)$. To see this, let $\theta(n)$ denote the number of solutions of the congruence

$$x^n \equiv 1 \pmod{p}. \tag{6}$$

By Theorem 3Q, an integer $x$ is a solution of (6) if and only if the exponent $k$ to which $x$ belongs modulo $p$ satisfies $k \mid n$. Hence

$$\theta(n) = \sum_{k \mid n} \psi(k).$$

Note next that

$$x^{p-1} - 1 = (x^n - 1)(x^{p-1-n} + x^{p-1-2n} + \ldots + x^n + 1).$$

By Fermat's little theorem, the congruence

$$x^{p-1} - 1 \equiv 0 \pmod{p}$$

has exactly $p-1$ solutions. On the other hand, by Lagrange's theorem, the congruence (6) has at most $n$ solutions and the congruence

$$x^{p-1-n} + x^{p-1-2n} + \ldots + x^n + 1 \equiv 0 \pmod{p}$$

has at most $p-1-n$ solutions. It follows that (6) must have exactly $n$ solutions, and so

$$\sum_{k \mid n} \psi(k) = n.$$

It now follows from the Möbius inversion formula and Theorem 2R that

$$\psi(n) = \sum_{k \mid n} \mu(k) \frac{n}{k} = \phi(n).$$

This completes the proof. ○

**THEOREM 3S.** *Suppose that $p$ is an odd prime, and $g$ is a primitive root modulo $p$. Then there exists $t \in \mathbb{Z}$ such that the integer $u$, defined by the equation*

$$(g + pt)^{p-1} = 1 + pu,$$

*is not divisible by $p$. In this case, $g + pt$ is a primitive root modulo $p^r$ for every $r \in \mathbb{N}$.*

PROOF. Since $g^{p-1} = 1 + pq$ for some $q \in \mathbb{Z}$, it follows that there exist $r, s \in \mathbb{Z}$ such that

$$\begin{aligned} (g + px)^{p-1} &= 1 + pq + (p-1)g^{p-2}px + p^2 r \\ &= 1 + p(q - xg^{p-2} + ps) \\ &= 1 + py, \end{aligned} \tag{7}$$

where

$$y = q - xg^{p-2} + ps \equiv q - xg^{p-2} \pmod{p}.$$

As $x$ runs through a complete set of residues modulo $p$, so does $y$, in view of Theorem 3D. Hence there exists a value of $x$, say $t$, for which $p \nmid y$, and let $u$ be the corresponding value of $y$. It follows from (7) that for this value of $t$, we have

$$(g + pt)^{(p-1)p} = (1 + pu)^p = 1 + p^2 u + p^3 u' = 1 + p^2 u_2,$$

where $p \nmid u_2$. Similarly,

$$(g+pt)^{(p-1)p^2} = 1 + p^3 u_3,$$

where $p \nmid u_3$, and so on. Suppose that $(g+pt)$ belongs to the exponent $n$ modulo $p^r$, so that $(g+pt)^n \equiv 1 \pmod{p^r}$. Then clearly $(g+pt)^n \equiv 1 \pmod{p}$, and so $g^n \equiv 1 \pmod{p}$. Since $g$ is a primitive root modulo $p$, we must have $(p-1) \mid n$. On the other hand, $n \mid \phi(p^r) = p^{r-1}(p-1)$. Hence $n = p^{s-1}(p-1)$ for some integer $s$ satisfying $1 \le s \le r$. Recall now that

$$(g+pt)^n = (g+pt)^{(p-1)p^{s-1}} = 1 + p^s u_s,$$

where $p \nmid u_s$. It follows that

$$1 + p^s u_s \equiv 1 \pmod{p^r},$$

so that $p^s u_s \equiv 0 \pmod{p^r}$. We therefore must have $s = r$, and so $n = \phi(p^r)$. ○

**THEOREM 3T.** *Suppose that $p$ is an odd prime, and $g$ is an odd primitive root modulo $p^r$, where $r \in \mathbb{N}$. Then $g$ is a primitive root modulo $2p^r$.*

Remark. Note that since there exist primitive roots modulo $p^r$, there must exist odd primitive roots modulo $p^r$. To see this, note that if $h$ is an even primitive root modulo $p^r$, then $g = h + p^r$ is an odd primitive root modulo $p^r$.

Proof of Theorem 3T. Note first of all that every odd integer $x$ which satisfies $x^n \equiv 1 \pmod{p^r}$ clearly satisfies $x^n \equiv 1 \pmod{2p^r}$, and vice versa. It follows that if $g$ is an odd primitive root modulo $p^r$, then it belongs to the exponent $\phi(p^r)$ modulo $2p^r$. Note, however, that $\phi(p^r) = \phi(2p^r)$. ○

We are now in a position to determine precisely those values of $m \in \mathbb{N}$ for which primitive roots modulo $m$ exist. We prove the following beautiful result.

**THEOREM 3U.** (GAUSS) *Suppose that $m \in \mathbb{N}$ and $m > 1$. Then there exist primitive roots modulo $m$ if and only if $m = 2, 4, p^r, 2p^r$, where $p$ is an odd prime and $r \in \mathbb{N}$.*

Proof. For $m = 4$, it is easy to check that 3 is a primitive root. The existence of primitive roots to the other moduli follows from the previous three theorems.

Suppose now that $m = p_1^{u_1} \ldots p_r^{u_r}$, where the natural numbers $p_1 < \ldots < p_r$ are primes and the integers $u_i > 0$ for $i = 1, \ldots, r$. For every $i = 1, \ldots, r$, write $m_i = p_i^{u_i}$, so that $m = m_1 \ldots m_r$, and let $\ell = [\phi(m_1), \ldots, \phi(m_r)]$ be the least common multiple of $\phi(m_1), \ldots, \phi(m_r)$. Suppose now that $a \in \mathbb{Z} \setminus \{0\}$ and $(a, m) = 1$. For every $i = 1, \ldots, r$, we have by Theorem 3F that $a^{\phi(m_i)} \equiv 1 \pmod{m_i}$, so that $a^\ell \equiv 1 \pmod{m_i}$. It follows that $a^\ell \equiv 1 \pmod{m}$. We have to show that if $m$ is not one of the stated values, then

$$\ell < \phi(m) = \phi(m_1) \ldots \phi(m_r).$$

If $p$ is a prime, then $\phi(p^u) = p^{u-1}(p-1)$ is even if $p > 2$ or if $p = 2$ and $u \ge 2$, and so $\phi(p^u)$ is even whenever $p^u > 2$. It follows that if two of the values $m_1, \ldots, m_r$ exceed 2, then $\ell < \phi(m)$. It remains to show that there are no primitive roots modulo $2^u$, where $u \ge 3$. We shall do this by proving that for every odd integer $a$ and every integer $u \ge 3$, we have

$$a^{\frac{1}{2}\phi(2^u)} \equiv 1 \pmod{2^u}. \tag{8}$$

For $u = 3$, we note that $a^2 \equiv 1 \pmod{8}$. Suppose now that (8) holds for $u = k$; in other words, suppose that

$$a^{\frac{1}{2}\phi(2^k)} = 1 + 2^k t,$$

where $t \in \mathbb{Z}$. Squaring both sides, we obtain

$$a^{\phi(2^k)} = 1 + 2^{k+1}t + 2^{2k}t^2 \equiv 1 \pmod{2^{k+1}}.$$

This completes the proof, since $\phi(2^k) = \frac{1}{2}\phi(2^{k+1})$. ○

## Problems for Chapter 3

1. Prove that $7 \mid (3^{2n+1} + 2^{n+2})$ for every $n \in \mathbb{N}$.
2. Prove that every year, including a leap year, has a Friday 13th.
[Hint: For those who are superstitious, prove instead that every year, including a leap year, has a Sunday 1st. The two statements are the same!]
3. Prove that $5n^3 + 7n^5 \equiv 0 \pmod{12}$ for every $n \in \mathbb{Z}$.
4. Show that $1^2, 2^2, \ldots, m^2$ is not a complete set of residues modulo $m$ if $m > 2$.
5. Suppose that $a, b, p \in \mathbb{N}$ and $p$ is prime. Show that $(a+b)^p \equiv a^p + b^p \pmod{p}$.
6. Suppose that $a, b, p \in \mathbb{N}$ and $p > 2$ is prime. Show that if $a^p + b^p \equiv 0 \pmod{p}$, then we must have $a^p + b^p \equiv 0 \pmod{p^2}$.
7. Suppose that $p > 2$ is a prime. Show that $1^p + 2^p + \ldots + (p-1)^p \equiv 0 \pmod{p}$.
8. Find all $x \in \mathbb{Z}$ such that simultaneously $x \equiv 1 \pmod{2}$, $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$.
9. Suppose that $m \in \mathbb{N}$ and $a, b \in \mathbb{Z}$ such that $(a, m) = 1$. Prove that $\displaystyle\sum_{x=1}^{m} \left\{ \frac{ax+b}{m} \right\} = \frac{m-1}{2}$.
10. Suppose that $m_1, \ldots, m_k$ are integers greater than 1 and which are pairwise coprime, and write $m = m_1 \ldots m_k$. Suppose further that $x_1, \ldots, x_k, x$ run through complete sets of residues and $y_1, \ldots, y_k, y$ run through reduced sets of residues modulo $m_1, \ldots, m_k, m$ respectively. Prove that the fractions
$$\left\{ \frac{x_1}{m_1} + \ldots + \frac{x_k}{m_k} \right\} \qquad \text{and} \qquad \left\{ \frac{x}{m} \right\}$$
coincide, as do the fractions
$$\left\{ \frac{y_1}{m_1} + \ldots + \frac{y_k}{m_k} \right\} \qquad \text{and} \qquad \left\{ \frac{y}{m} \right\}.$$
11. Suppose that $a, m \in \mathbb{N}$ satisfy $(a, m) = 1$ and $m > 1$. Prove that
$$\sum_{\substack{y=1 \\ (y,m)=1}}^{m} \left\{ \frac{ay}{m} \right\} = \frac{\phi(m)}{2}.$$
[Hint: Denote the above sum by $S(m)$, and show that for every $d \in \mathbb{N}$, we have $S(d) = \displaystyle\sum_{\substack{x=1 \\ (x,d)=1}}^{d} \frac{x}{d}$.
Then consider the sum $\displaystyle\sum_{d \mid m} S(d)$, and use the Möbius inversion formula.]

12. The number $g = 10^{100}$ is called a googol. Show that there exist a googol consecutive integers each of which is divisible by the square of a prime.
[Hint: Use the Chinese remainder theorem.]
[Remark: Can you prove that there are arbitrarily long gaps between consecutive primes?]

13. Suppose that $p$ is a prime. Suppose further that $h$ and $k$ are non-negative integers such that $h + k = p - 1$. Prove that $h!k! + (-1)^h \equiv 0 \pmod{p}$.

14. Suppose that $p$ is a odd prime.
    (i) Prove that $1^2 3^2 5^2 \ldots (p-2)^2 \equiv 2^2 4^2 6^2 \ldots (p-1)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$.
    (ii) Deduce that $\left(\left[\dfrac{p-1}{2}\right]!\right)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$.

15. Suppose that $p$ is a prime, and that $n \in \mathbb{Z}$.
    (i) Prove that $\dbinom{n}{p} \equiv \left[\dfrac{n}{p}\right] \pmod{p}$.
    (ii) Suppose that $\alpha \in \mathbb{N}$ and $p^\alpha$ divides $\left[\dfrac{n}{p}\right]$. Prove that $p^\alpha$ also divides $\dbinom{n}{p}$.

16. Suppose that $n \in \mathbb{N}$, and that there exists $a \in \mathbb{Z}$ such that $n \mid (a^{n-1} - 1)$. Suppose further that $n \nmid (a^x - 1)$ whenever $1 \le x \le n-2$. Show that $n$ is prime.

17. Let

$$S_n(p) = \sum_{k=1}^{p-1} k^n,$$

where $p$ is an odd prime and $n$ is an integer greater than 1. Prove that $S_n(p) \equiv -1 \pmod{p}$ if $(p-1) \mid n$, and that $S_n(p) \equiv 0 \pmod{p}$ if $(p-1) \nmid n$.
[Hint: Let $g$ be a primitive root modulo $p$. Show that $S_n(p) \equiv \sum_{j=0}^{p-2} g^{jn} \pmod{p}$.]

18. Suppose that $p$ is a prime. Prove that the sum of the primitive roots modulo $p$ is congruent to $\mu(p-1)$ modulo $p$.

19. Suppose that $p > 3$ is a prime. Prove that the product of the primitive roots modulo $p$ is congruent to 1 modulo $p$.

20. Suppose that $p > 2$ is a prime.
    (i) Prove that for any integer $a > 1$, any odd prime divisor of $a^p - 1$ either divides $a - 1$ or is of the form $2px + 1$.
    (ii) Prove that for any integer $a > 1$, any odd prime divisor of $a^p + 1$ either divides $a + 1$ or is of the form $2px + 1$.
    (iii) Prove that there are infinitely many primes of the form $2px + 1$.
    (iv) Prove that any prime divisor of $2^{2^n} + 1$, where $n \in \mathbb{N}$, is of the form $2^{n+1}x + 1$.

21. Suppose that $a, n \in \mathbb{N}$ and $a > 1$. Prove that $n$ divides $\phi(a^n - 1)$.