18.781 Theory of Numbers

Problem Set 5

Official Solutions

March 23, 2026

Contents

Disclaimer

This document contains the official solutions to Problem Set 5 of the Spring 2026 edition of 18.781 Theory of Numbers. While carefully proofread, all errors, typos, and omissions are mine alone. Please email allenees@mit.edu should you have any questions or concerns. All references made herein refer to Niven and Montgomery's *An Introduction to the Theory of Numbers*, 5th edition.

1 §2.8 #8

Problem (§2.8 #8)

Use Theorem 2.37 to determine how many solutions each of the following congruences has:

(a) $x^{12} \equiv 16 \pmod{17}$

(b) $x^{48} \equiv 9 \pmod{17}$

(c) $x^{20} \equiv 13 \pmod{17}$

(d) $x^{11} \equiv 9 \pmod{17}$.

Solution. Let $p = 17$. When $(a, p) = (a, 17) = 1$, the congruence $x^n \equiv a \pmod{17}$ has $(n, p-1) = (n, 16)$ solutions or no solutions according to

$$a^{(p-1)/(n,p-1)} = a^{16/(n,16)} \equiv 1 \pmod{17}$$

or not, by Theorem 2.37.

(a) Here $n = 12$ and $a = 16$, and $(a, 17) = (16, 17) = 1$. Since $a^{16/(n,16)} \equiv 16^4 \pmod{17} \equiv 1 \pmod{17}$, there are

$$(n, 16) = (12, 16) = 4 \text{ solutions.}$$

(b) Here $n = 48$ and $a = 9$, and $(a, 17) = (9, 17) = 1$. Since $a^{16/(n,16)} \equiv 9 \pmod{17} \not\equiv 1 \pmod{17}$, there are

$$\text{no solutions.}$$

(c) Here $n = 20$ and $a = 13$, and $(a, 17) = (13, 17) = 1$. Since $a^{16/(n,16)} \equiv 13^4 \pmod{17} \equiv 1 \pmod{17}$, there are

$$(n, 16) = (12, 16) = 4 \text{ solutions.}$$

(d) Here $n = 11$ and $a = 9$, and $(a, 17) = (9, 17) = 1$. Since $a^{16/(n,16)} \equiv 9^{16} \pmod{17} \equiv 1 \pmod{17}$, there is

$$(n, 16) = (11, 16) = 1 \text{ solution.}$$

The exercise is complete. ■

Theorem (Theorem 2.37)

If p is a prime and $(a, p) = 1$, then the congruence $x^n \equiv a \pmod{p}$ has $(n, p-1)$ solutions or no solution according as

$$a^{(p-1)/(n,p-1)} \equiv 1 \pmod{p}$$

or not.

2 §2.8 #13

Problem (§2.8 #13)
Show that the numbers $1^k, 2^k, \ldots, (p-1)^k$ form a reduced residue system $\pmod p$ if and only if $(k, p-1) = 1$.

Proof. Let g be a primitive root modulo p, which exists by Theorem 2.41. Then $g, g^2, \ldots, g^{p-1}$ form a reduced residue system modulo p.

($\Longrightarrow$) Suppose that the numbers $1^k, 2^k, \ldots, (p-1)^k$ form a reduced residue system modulo p. Therefore, for any $a \in \{1, \ldots, p-1\}$ there exists some unique $b \in \{1, \ldots, p-1\}$ such that

$$b^k \equiv a \pmod p.$$

Since g is a primitive root modulo p, the above statement is equivalent to saying that for any $i \in \{1, \ldots, p-1\}$ there exists some unique $j \in \{1, \ldots, p-1\}$ (where $a = g^i$ and $b = g^j$) such that $g^{jk} = \left(g^j\right)^k \equiv g^i \pmod p$. Multiplying the congruence by g^{p-1-i} gives

$$g^{jk+p-1-i} \equiv g^{p-1} \pmod p \equiv 1 \pmod p,$$

so Lemma 2.31 implies that $(p-1) \mid (jk + p - 1 - i)$ since g has order $p-1$ modulo p. In particular,

$$jk - i \equiv jk + (p-1) - i \pmod{p-1} \equiv 0 \pmod{p-1},$$

which gives $jk \equiv i \pmod{p-1}$. By Theorem 2.17, there exists a solution j when $(k, p-1) \mid i$. This must hold for all $i \in \{1, \ldots, p-1\}$, so we must have $(k, p-1) = 1$. Moreover, j is unique since $(k, p-1) = 1$.

($\Longleftarrow$) Suppose that $(k, p-1) = 1$. By Theorem 2.17, since $1 = (k, p-1) \mid i$ for all $i \in \{1, \ldots, p-1\}$, the congruence $jk \equiv i \pmod{p-1}$ has a unique solution j. There exists some $q \in \mathbb{Z}$ such that $q(p-1) = jk - i$. Thus

$$g^{jk-i} \equiv \left(g^{p-1}\right)^q \pmod p \equiv 1 \pmod p,$$

so multiplying the congruence by g^i gives

$$\left(g^j\right)^k = g^{jk} \equiv g^i \pmod p.$$

But $\left\{g, g^2, \ldots, g^{p-1}\right\} = \{1, 2, \ldots, p-1\}$, and for each $i \in \{1, \ldots, p-1\}$ there exists a unique $j \in \{1, \ldots, p-1\}$ such that the above congruence holds. Thus, $1^k, 2^k, \ldots, (p-1)^k$ form a reduced residue system modulo p. ∎

Lemma (Lemma 2.31)
If a has order $h \pmod m$, then the positive integers k such that $a^k \equiv 1 \pmod m$ are precisely those for which $h \mid k$.

Theorem (Theorem 2.41)
There exists a primitive root modulo m if and only if $m = 1$, 2, 4, p^α, or $2p^\alpha$, where p is an odd prime.

Remark 1. *§2.8 #32 (Problem 5) is a generalized version of this problem; write $m = p$, $n = \phi(p) = p - 1$, and write $r_i = i$ for all $i \in \{1, \ldots, p-1\}$.*

3 §2.8 #14

Problem (§2.8 #14)
Suppose that a has order $h \pmod p$, and that $a\overline{a} \equiv 1 \pmod p$. Show that $\overline{a}$ also has order h. Suppose that g is a primitive root $\pmod p$, and that $a \equiv g^i \pmod p$, $0 \leqslant i < p-1$. Show that $\overline{a} = g^{p-1-i} \pmod p$.

Proof. Since a has order h modulo p, $a^h \equiv 1 \pmod p$ and $a^n \not\equiv 1 \pmod p$ for all integers $1 \leq n < h$. Let

$$r_n \equiv \overline{a}^n \pmod p.$$

be the residue of $\overline{a}^n$ modulo p. Multiplying the congruence by a^n gives

$$a^n r_n \pmod p \equiv a^n \overline{a}^n \pmod p \equiv 1 \pmod p.$$

If $n = h$, we have $r_h \equiv a^h r_h \pmod p \equiv 1 \pmod p$; if $1 \leq n < h$, then $r_n \not\equiv a^n r_n \equiv 1 \pmod p$, so $\overline{a}$ has order h.

Now let g be a primitive root modulo p so that $a \equiv g^i \pmod p$ for some $i \in \{1, \ldots, p-1\}$. Then $\overline{a} \equiv g^j$ for some $j \in \{1, \ldots, p-1\}$, and

$$1 \pmod p \equiv a\overline{a} \pmod p \equiv g^i g^j \pmod p \equiv g^{i+j} \pmod p.$$

Since g has order $p-1$ modulo p, Lemma 2.31 implies that $(p-1) \mid (i+j)$. Thus, $k(p-1) = i+j$ for some $k \in \mathbb{Z}$. But $2 \leq i+j < 2p$, so we must have $i+j = p-1$. In other words, $j = p-1-i$. ∎

4 §2.8 #18

Problem (§2.8 #18)
Show that if g and g' are primitive roots modulo an odd prime p, then gg' is not a primitive root of p.

Proof. Suppose g and g' are primitive roots modulo an odd prime p. By definition,

$$\begin{aligned} g^{p-1} &\equiv 1 \pmod{p}, \\ (g')^{p-1} &\equiv 1 \pmod{p}. \end{aligned}$$

Since p is odd, $x = g^{(p-1)/2}$ (resp. $x' = (g')^{(p-1)/2}$) is a solution to the congruence $x^2 \equiv 1 \pmod{p}$ (resp. $(x')^2 \equiv 1 \pmod{p}$). But the only such solutions are when $x \equiv 1 \pmod{p}$ (resp. $x' \equiv 1 \pmod{p}$) or when $x \equiv -1 \pmod{p}$ (resp. $x' \equiv -1 \pmod{p}$), by Lemma 2.10. However, $x \equiv 1 \pmod{p}$ (resp. $x' \equiv 1 \pmod{p}$) is impossible since otherwise $g^{(p-1)/2} \equiv 1 \pmod{p}$ (resp. $(g')^{(p-1)/2} \equiv 1 \pmod{p}$) implies that g (resp. g') is not a primitive root modulo p. Thus

$$\begin{aligned} g^{(p-1)/2} &\equiv -1 \pmod{p}, \\ (g')^{(p-1)/2} &\equiv -1 \pmod{p}, \end{aligned}$$

and hence

$$\begin{aligned} (gg')^{(p-1)/2} &\equiv g^{(p-1)/2}(g')^{(p-1)/2} \pmod{p} \\ &\equiv (-1)(-1) \pmod{p} \\ &\equiv 1 \pmod{p}, \end{aligned}$$

so gg' is not a primitive root modulo p. ∎

Lemma (Lemma 2.10)
Let p be a prime number. Then $x^2 \equiv 1 \pmod{p}$ if and only if $x \equiv \pm 1 \pmod{p}$.

Remark 2. *The spirit of this problem is similar to §2.8 #21 on Problem Set 4.*

5 §2.8 #32

Problem (§2.8 #32)
Let $r_1, r_2, \ldots, r_n$ be a reduced residue system modulo m ($n = \phi(m)$). Show that the numbers $r_1^k, r_2^k, \ldots, r_n^k$ form a reduced residue system $\pmod m$ if and only if $(k, \phi(m)) = 1$. (H)

Proof. ($\implies$) If $m = 2$, the statement holds trivially, so suppose $m > 2$. Towards the contrapositive, suppose that $(k, \phi(m)) > 1$. Therefore, there exists some prime p such that $p \mid (k, \phi(m))$, so $p \mid k$ and $p \mid \phi(m)$. Write the prime factorization $m = \prod_{q \text{ prime}} q^{\alpha(q)}$, so

$$\phi(m) = \prod_{q \text{ prime}} \phi\left(q^{\alpha(q)}\right)$$

and $p \mid \phi\left(q^{\alpha(q)}\right)$ for some prime q. Thus $\phi\left(q^{\alpha(q)}\right)/q \in \mathbb{Z}$ is well-defined, as is $k/p \in \mathbb{Z}$.

- If $q \neq 2$, then there exists a primitive root g modulo $q^{\alpha(q)}$ by Theorem 2.41. If we let $x = g^{\phi\left(q^{\alpha(q)}\right)/p}$, then

$$x^k \equiv g^{\phi\left(q^{\alpha(q)}\right)k/p} \pmod{q^{\alpha(q)}} \equiv \left(g^{\phi\left(q^{\alpha(q)}\right)}\right)^{k/p} \pmod{q^{\alpha(q)}} \equiv 1^{k/p} \pmod{q^{\alpha(q)}} \equiv 1 \pmod{q^{\alpha(q)}}.$$

- If $q = 2$, then we must have $p = 2$ and $p \mid k$ means that k is even. If we let $x = -1$, then $x^k \equiv 1 \pmod{q^{\alpha(q)}}$.

Consider the system of congruences $y \equiv x \pmod{q^{\alpha(q)}}$ and $y \equiv 1 \pmod{m/q^{\alpha(q)}}$. Now $\left(q^{\alpha(q)}, m/q^{\alpha(q)}\right) = 1$, so the Chinese remainder theorem gives an unique solution y modulo m satisfying

$$y^k \equiv 1 \pmod m, \tag{1}$$
$$y \not\equiv 1 \pmod m, \tag{2}$$
$$(y, m) = 1. \tag{3}$$

The congruence (1) follows from Theorem 2.3(c) because

$$y^k \equiv x^k \pmod{q^{\alpha(q)}} \equiv 1 \pmod{q^{\alpha(q)}},$$
$$y^k \equiv 1^k \pmod{m/q^{\alpha(q)}} \equiv 1 \pmod{m/q^{\alpha(q)}}.$$

If congruence (2) was false, Theorem 2.3(c) implies that $y \equiv 1 \pmod{q^{\alpha(q)}} \equiv g^{\phi\left(q^{\alpha(q)}\right)/p} \pmod{q^{\alpha(q)}}$ or $1 \equiv -1 \pmod{2^{\alpha(2)}}$, a contradiction since g is a primitive root modulo $q^{\alpha(q)}$ and $m > 2$. If (3) was false, then $p' \mid (y, m)$ for some prime p', so $p' \mid y \mid y^k$ and yet $y^k \equiv 1 \pmod m$ implies $p' \mid m \mid \left(y^k - 1\right)$. Take any r_i. We then have $(yr_i, m) = 1$, so $yr_i = r_j$ for some j. Now $r_j \equiv yr_i \pmod m \not\equiv r_i \pmod m$ and yet $r_j^k \equiv (yr_i)^k \pmod m \equiv r_i^k \pmod m$. It follows that the numbers $r_1^k, r_2^k, \ldots, r_n^k$ do not form a reduced residue system modulo m.

($\impliedby$) Suppose that $(k, \phi(m)) = 1$. For all $i \in \{1, \ldots, n\}$, we have $\left(r_i^k, m\right) = 1$ because $(r_i, m) = 1$; if for some $x, y \in \mathbb{Z}$, $r_i x + my = 1$ is an integer linear combination of r_i and m, then expanding $1 = (r_i x + my)^k$ gives an integer linear combination of r_i^k and m. Now it suffices to show that $r_1^k, r_2^k, \ldots, r_n^k$ are distinct. To this end, suppose that $r_i^k \equiv r_j^k \pmod m$. Since $(k, \phi(m)) = 1$, there exists some $\overline{k} \in \mathbb{Z}$ such that $k\overline{k} \equiv 1 \pmod{\phi(m)}$. Thus, there exists some $q \in \mathbb{Z}$ such that $q\phi(m) = k\overline{k} - 1$, or equivalently $k\overline{k} = q\phi(m) + 1$. Then

$$r_i \equiv r_i^{q\phi(m)+1} \pmod m \equiv r_i^{k\overline{k}} \pmod m \equiv r_j^{k\overline{k}} \pmod m \equiv r_j^{q\phi(m)+1} \pmod m \equiv r_j \pmod m,$$

so we must have $r_i \equiv r_j \pmod m$ and hence $i = j$. Hence, $r_1^k, r_2^k, \ldots, r_n^k$ form a reduced residue system modulo m. ∎

Remark 3. *This generalizes §2.8 #13 (Problem 2).*

6 §2.11 #1

Problem (§2.11 #1)
Prove that the multiplicative group modulo 9 is isomorphic to the additive group modulo 6.

Proof. Let R_9 and C_6 be the multiplicative group modulo 9 and additive group modulo 6 with binary operations $\odot$ and $\oplus$, respectively. Define $C_6 = \{0, 1, 2, 3, 4, 5\}$ and $R_9 = \{1, 2, 4, 5, 7, 8\}$. Let $\phi\colon R_9 \to C_6$ be a function defined by

$$\begin{aligned} 1 &\mapsto 0, & 2 &\mapsto 1, & 4 &\mapsto 2, \\ 5 &\mapsto 5, & 7 &\mapsto 4, & 8 &\mapsto 3. \end{aligned}$$

This is clearly a one-to-one-correspondence by construction, so now we need only check that

$$\phi(a \odot b) = \phi(a) \oplus \phi(b)$$

for any $a, b \in R_9$. For the sake of brevity, define

$$\begin{aligned} a^{\oplus n} &= \underbrace{a \oplus \cdots \oplus a}_{n \text{ times}}, \\ a^{\odot n} &= \underbrace{a \odot \cdots \odot a}_{n \text{ times}}. \end{aligned}$$

We see that 1 is a generator for C_6 and 2 is a generator for R_9 (since 2 is a primitive root modulo 9). Therefore any element of C_6 (resp. R_9) is of the form $1^{\oplus n}$ (resp. $2^{\otimes n}$) for some $n \in \{0, 1, 2, 3, 4, 5\}$. Since $\phi(2) = 1$

$$\phi\left(2^{\odot n}\right) = \phi(2)^{\oplus n} = 1^{\oplus n}$$

for all $n \in \{0, 1, 2, 3, 4, 5\}$, and hence

$$\phi\left(2^{\odot n} \odot 2^{\odot m}\right) = \phi\left(2^{\odot(n+m)}\right) = 1^{\oplus(n+m)} = 1^{\oplus n} \oplus 1^{\oplus m} = \phi\left(2^{\odot n}\right) \oplus \phi\left(2^{\odot n}\right),$$

as desired. ∎

Remark 4. *The key insight in this problem is noting that both R_9 and C_6 are cyclic, and thus they must both have a generator g_R and g_C, respectively. Now g_C must be 1 and g_R is a primitive root modulo 9, so it must be 2. Then any element of R_9 and C_6 can be written using g_R and g_C, so the group isomorphism boils down to mapping g_R iterated n times in R_9 to g_C iterated n times in C_6.*

7 §2.11 #3

Problem (§2.11 #3)
Prove that any two cyclic groups of order m are isomorphic.

Proof. Let G and H be two cyclic groups of order m with generators a_G and a_H. In other words,

$$G = \left\{ e_G \coloneqq a_G^0, a_G^1, a_G^2, \ldots, a_G^{m-1} \right\},$$
$$H = \left\{ e_H \coloneqq a_H^0, a_H^1, a_H^2, \ldots, a_H^{m-1} \right\}.$$

Let $\phi \colon G \to H$ be such that $\phi(a_G^n) = a_H^n$ for all $n \in \{0, \ldots, m-1\}$. This is clearly a one-to-one correspondence, and

$$\phi\left(a_G^n a_G^{n'}\right) = \phi\left(a_G^{n+n'}\right) = a_H^{n+n'} = a_H^n a_H^{n'} = \phi\left(a_G^n\right)\phi\left(a_G^{n'}\right)$$

for any $n, n' \in \{0, \ldots, m-1\}$. Thus ϕ is a group isomorphism. ■

Remark 5. *Again, like the previous problem the group isomorphism is motivated by mapping the generator of one group to the generator of the other group.*

8 §2.11 #5

Problem (§2.11 #5)
If a is an element of order r of a group G, prove that $a^k = e$ if and only if $r \mid k$.

Proof. Let $a \in G$ have order r. Then $a^r = e$ and $a^n \neq e$ for all integers $1 \leq n < r$.

($\implies$) Suppose $a^k = e$. Then $k \geq r$. The division algorithm gives unique $q, r' \in \mathbb{Z}$ such that $k = qr + r'$, where $0 \leq r' < q$. Then

$$e = a^k = a^{qr+r'} = (a^r)^q a^{r'} = e^q a^{r'} = a^{r'}.$$

By definition, this forces $r' = 0$, so $k = qr$ and hence $r \mid k$.

($\impliedby$) Suppose $r \mid k$. Then there exists some $m \in \mathbb{Z}$ such that $rm = k$. Then

$$a^k = a^{rm} = (a^r)^m = e^m = e,$$

as desired. ■

9 §2.11 #6

Problem (§2.11 #6)
What is the smallest positive integer m such that the multiplicative group modulo m is not cyclic?

Solution. The smallest positive integer is

$$\boxed{m = 8.}$$

Recall that R_m (the multiplicative group modulo m) is cyclic if and only if $m = 1$, 2, 4, p^α, or $2p^\alpha$, where p is an odd prime. (A primitive root can serve as a generator of a cyclic group, and if there is no primitive root, then there is no generator, so Theorem 2.41 applies). The smallest positive m that is not of that form is $m = 8$. ■

10 §2.11 #11

Problem (§2.11 #11)

Let G consist of a, b, c, d, e, f and let $\oplus$ be defined by the following table.

$\oplus$	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	e	d	f	b	c
b	b	f	e	d	c	a
c	c	d	f	e	a	b
d	d	c	a	b	f	e
f	f	b	c	a	e	d

Show that G is a noncommutative group.

Proof. First we show G is a group.

- By inspection from the table, G is closed under $\oplus$ since for any $x, y \in G$ we also have $x \oplus y \in G$.
- The associative law holds by inspection, i.e., $x \oplus (y \oplus z) = (x \oplus y) \oplus z$ for all $x, y, z \in G$.
- By inspection, $e \in G$ is the unique identity; $x \oplus e = e \oplus x = x$ for all $x \in G$, and no other element satisfies this.
- Each element in G has a unique inverse in G since each row and column has one and only one e.

For noncommutativity, we need only exhibit $x, y \in G$ such that $x \oplus y \neq y \oplus x$. There are many; for example, take $x = a$ and $y = b$ and we see that

$$x \oplus y = a \oplus b = d \neq f = b \oplus a = y \oplus x,$$

as desired. ■