18.781 Theory of Numbers

Problem Set 4

Official Solutions

March 13, 2026

Contents

1 §2.6 #4 2

2 §2.6 #9 3

3 §2.6 #10 4

4 §2.7 #3 5

5 §2.7 #10 6

6 §2.7 #11 7

7 §2.8 #5 8

8 §2.8 #7 9

9 §2.8 #20 10

10 §2.8 #21 12

Disclaimer

This document contains the official solutions to Problem Set 4 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 §2.6 #4

Problem (§2.6 #4)
Solve $x^2 + 5x + 24 \equiv 0 \pmod{36}$.

Solution. The solutions are

$$7, 15, 16, 24.$$

Let $f(x) = x^2 + 5x + 24$. Then $f'(x) = 2x + 5$. By the Chinese remainder theorem, we find solutions to

$$f(x) \equiv 0 \pmod{4},$$
$$f(x) \equiv 0 \pmod{9}.$$

We first solve $f(x) \equiv 0 \pmod{2}$. We see that $f(0) \equiv 0 \pmod{2}$ and $f(1) \equiv 0 \pmod{2}$.

- Note that $f'(0) = 5 \not\equiv 0 \pmod{2}$, so 0 is a nonsingular root. By Hensel's lemma, we take $\overline{f'(0)} = 1$ so that $a_0 = 0$ lifts to $a_1 = a_0 - f(0)\overline{f'(0)} = 0 - 24 \cdot 1 = -24 \equiv 0 \pmod{4}$.
- Note that $f'(1) = 7 \not\equiv 0 \pmod{2}$, so 1 is a nonsingular root. By Hensel's lemma, we take $\overline{f'(1)} = 1$ so that $a_0 = 1$ lifts to $a_1 = a_0 - f(1)\overline{f'(1)} = 1 - 30 \cdot 1 = -29 \equiv 3 \pmod{4}$.

We now solve $f(x) \equiv 0 \pmod{3}$. We see that $f(0) \equiv 0 \pmod{3}$ and $f(1) \equiv 0 \pmod{24}$.

- Note that $f'(0) = 5 \not\equiv 0 \pmod{3}$, so 0 is a nonsingular root. By Hensel's lemma, we take $\overline{f'(0)} = 2$ so that $a_0 = 0$ lifts to $a_1 = a_0 - f(0)\overline{f'(0)} = 0 - 24 \cdot 2 = -48 \equiv 6 \pmod{9}$.
- Note that $f'(1) = 7 \not\equiv 0 \pmod{3}$, so 1 is a nonsingular root. By Hensel's lemma, we take $\overline{f'(1)} = 1$ so that $a_0 = 1$ lifts to $a_1 = a_0 - f(1)\overline{f'(1)} = 1 - 30 \cdot 1 \equiv 7 \pmod{9}$.

Therefore, the system becomes

$$x \equiv 0 \pmod{4} \quad \text{or} \quad x \equiv 3 \pmod{4},$$
$$x \equiv 6 \pmod{9} \quad \text{or} \quad x \equiv 7 \pmod{9}.$$

Since $b_1 = 1$ and $b_2 = 7$ solves

$$9b_1 \equiv 1 \pmod{4} \quad \text{and} \quad 4b_2 \equiv 1 \pmod{9},$$

the Chinese remainder theorem constructively gives the solution

$$9b_1c_1 + 4b_2c_2 \equiv 9c_1 + 28c_2 \pmod{36}$$

for $c_1 \in \{0, 3\}$ and $c_2 \in \{6, 7\}$, giving the solutions as above. ∎

Remark 1. *This is a standard application of Hensel's lemma.*

Theorem (Hensel's lemma, Theorem 2.23)
Suppose that $f(x)$ is a polynomial with integral coefficients. If $f(a) \equiv 0 \pmod{p^j}$ and $f'(a) \not\equiv 0 \pmod{p}$, then there is a unique $t \pmod{p}$ such that $f\left(a + tp^j\right) \equiv 0 \pmod{p^{j+1}}$.

2 §2.6 #9

Problem (§2.6 #9)
Suppose that $f(a) \equiv 0 \pmod{p^j}$ and that $f'(a) \not\equiv 0 \pmod{p}$. Let $\overline{f'(a)}$ be an integer chosen so that $f'(a)\overline{f'(a)} \equiv 1 \pmod{p^j}$, and put $b = a - f(a)\overline{f'(a)}$. Show that $f(b) \equiv 0 \pmod{p^{2j}}$.

Proof. Suppose $\deg f = n$, and write the Taylor series expansion of f by

$$\begin{aligned} f\left(a + tp^j\right) &= f(a) + tp^j f'(a) + t^2 p^{2j} \frac{f''(a)}{2!} + \cdots + t^n p^{nj} \frac{f^{(n)}(a)}{n!} \\ &\equiv f(a) + tp^j f'(a) \pmod{p^{2j}} \end{aligned}$$

since $f^{(k)}(a)/k!$ is an integer for all integers $2 \leq k \leq n$. Suppose $t \in \mathbb{Z}$ is such that $f\left(a + tp^j\right) \equiv 0 \pmod{p^{2j}}$. (Here, we prove that t exists.) Then

$$f(a) + tp^j f'(a) \equiv 0 \pmod{p^{2j}}.$$

Since $f(a) \equiv 0 \mod p^j$ implies $p^j \mid f(a)$, so $f(a)/p^j$ is an integer and we divide the congruence by p^j to obtain

$$\begin{aligned} \frac{f(a)}{p^j} + tf'(a) &\equiv 0 \pmod{p^{2j}/\left(p^{2j}, p^j\right)} \\ &\equiv 0 \pmod{p^j}. \end{aligned}$$

In other words,

$$tf'(a) \equiv -\frac{f(a)}{p^j} \pmod{p^j}.$$

Then t exists since multiplying through by $\overline{f'(a)}$ and using $f'(a)\overline{f'(a)} \equiv 1 \pmod{p^j}$ gives

$$t \equiv -\frac{f(a)\overline{f'(a)}}{p^j} \pmod{p^j}.$$

We take this choice of t and see that

$$\begin{aligned} a + tp^j &\equiv a - f(a)\overline{f'(a)} \pmod{p^j} \\ &\equiv b \pmod{p^j}, \end{aligned}$$

so hence

$$\begin{aligned} f(b) &\equiv f\left(a + tp^j\right) \pmod{p^j} \\ &\equiv 0 \pmod{p^j}, \end{aligned}$$

as required. ∎

Remark 2. *This is essentially the same proof of Hensel's lemma. Suppose that you want to lift a root a a total of j times. Assuming calculations are polynomial, you would need to apply Hensel's lemma $O(j)$ times, i.e., linear. However, you can apply this statement $O(\log j)$ times since every time you lift the power doubles.*

3 §2.6 #10

Problem (§2.6 #10)
Let p be an odd prime, and suppose that $a \not\equiv 0 \pmod{p}$. Show that if the congruence $x^2 \equiv a \pmod{p^j}$ has a solution when $j = 1$, then it has a solution for all j.

Proof. Let $f(x) = x^2 - a$. We proceed by induction. The base case $j = 1$ holds by assumption. For our induction step, suppose that the proposition holds for some $j > 1$. Therefore, some $b \in \mathbb{Z}$ satisfies $f(b) \equiv 0 \pmod{p^j}$. Now

$$f'(b) = 2b \not\equiv 0 \pmod{p}$$

because $p \nmid 2b$; otherwise (if $p \mid 2b$), then $p \mid 2$ (which is impossible since p is odd) or $p \mid b$ (which is impossible since $p^j \mid f(b)$, i.e., $p^j \mid \left(b^2 - a\right)$, implies that $p \mid \left(b^2 - a\right)$, i.e., $a \equiv b^2 \equiv 0 \pmod{p}$, contrary to $a \not\equiv 0 \pmod{p}$). Hence Hensel's lemma applies; there exists a unique $t \pmod{p}$ such that $f\left(b + tp^j\right) \equiv 0 \pmod{p^{j+1}}$, as required. ■

4 §2.7 #3

Problem (§2.7 #3)
Prove that $x^{14} + 12x^2 \equiv 0 \pmod{13}$ has 13 solutions and so it is an identical congruence.

Proof. Let $f(x) = x^{14} + 12x^2$, and let $a \in \mathbb{Z}$. By Fermat's little theorem, $a^{13} \equiv a \pmod{13}$, so

$$\begin{aligned} f(a) &= a^{14} + 12a^2 \\ &\equiv a^{13}a + 12a^2 \pmod{13} \\ &\equiv a^2 + 12a^2 \pmod{13} \\ &\equiv 13a^2 \pmod{13} \\ &\equiv 0 \pmod{13}, \end{aligned}$$

so $f(x) \equiv 0 \pmod{13}$. Thus, $f(x)$ is an identical congruence and as such has 13 solutions. ■

5 §2.7 #10

Problem (§2.7 #10)
Write $1/1 + 1/2 + \cdots + 1/(p-1) = a/b$ with $(a, b) = 1$. Show that $p^2 \mid a$ if $p \geqslant 5$.

Proof. Recall that σ_{p-2} is the sum of all product numbers of $p-1$ distinct numbers of the set $\{1, \ldots, p-1\}$, i.e.,

$$\sigma_{p-2} = (p-1)! \sum_{i=1}^{p-1} \frac{1}{i}.$$

Let $a, b > 0$ be integers such that $(a, b) = 1$ and

$$\frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{p-1} = \frac{a}{b}.$$

Multiplying through by $b(p-1)!$ gives

$$a(p-1)! = b\sigma_{p-2}.$$

Now Wolstenholme's congruence ($\sigma_{p-2} \equiv 0 \pmod{p^2}$ for $p \geq 5$) implies that

$$a(p-1)! \equiv 0 \pmod{p^2}.$$

But $\left((p-1)!, p^2\right) = 1$ since otherwise there exists some prime q such that $q \mid \left((p-1)!, p^2\right)$; then $q \mid p^2$, which forces $q = p$, but now $p \mid (p-1)!$ is a contradiction because $(p-1)! \equiv -1 \pmod{p}$ by Wilson's theorem. Thus

$$\begin{aligned} a &\equiv 0 \pmod{p^2 / \left((p-1)!, p^2\right)} \\ &\equiv 0 \pmod{p^2}, \end{aligned}$$

which implies $p^2 \mid a$. ∎

Remark 3. *The condition $p \geq 5$ is necessary to apply Wolstenholme's congruence.*

Theorem (Wolstenholme's congruence)
If $p \geq 5$, then $\sigma_{p-2} \equiv 0 \pmod{p^2}$.

6 §2.7 #11

Problem (§2.7 #11)
Let p be a prime, $p \geqslant 5$, and suppose that the numbers σ_j are as in (2.7). Show that $\sigma_{p-2} \equiv p\sigma_{p-3} \pmod{p^3}$.

Proof. Let $f(x) = (x-1)(x-2)\cdots(x-p+1)$. Write

$$f(x) = x^{p-1} - \sigma_1 x^{p-2} + \cdots + \sigma_{p-3}x^2 - \sigma_{p-2}x + \sigma_{p-1},$$

where σ_j is the sum of all products of j distinct members of the set $\{1, \ldots, p-1\}$. Then

$$(p-1)! = f(p) = p^{p-1} - p^{p-2}\sigma_1 + \cdots - p^3\sigma_{p-4} + p^2\sigma_{p-3} - p\sigma_{p-2} + \sigma_{p-1}.$$

Since $\sigma_{p-1} = (p-1)!$ we get

$$0 = p^{p-1} - p^{p-2}\sigma_1 + \cdots - p^3\sigma_{p-4} + p^2\sigma_{p-3} - p\sigma_{p-2}.$$

We divide by p to obtain

$$0 = p^{p-2} - p^{p-3}\sigma_1 + \cdots - p^2\sigma_{p-4} + p\sigma_{p-3} - \sigma_{p-2}$$

Moreover, $p \mid \sigma_j$ for all integers $1 \leq j \leq p-2$ and $p \geq 5$, so $p - 3 \geq 2$. Applying modulo p^3 we obtain

$$\begin{aligned} 0 &= \underbrace{p^{p-2} - p^{p-3}\sigma_1 + \cdots - p^2\sigma_{p-4}}_{\equiv 0 \pmod{p^3}} + p\sigma_{p-3} - \sigma_{p-2} \\ &\equiv p\sigma_{p-3} - \sigma_{p-2} \pmod{p^3}, \end{aligned}$$

which yields $\sigma_{p-2} \equiv p\sigma_{p-3}$, as required. ∎

Remark 4. *Here we use the key fact that $\sigma_j \equiv 0 \pmod{p}$ for all integers $1 \leq j \leq p-2$.*

7 §2.8 #5

Problem (§2.8 #5)

Let p be an odd prime. Prove that a belongs to the exponent 2 modulo p if and only if $a \equiv -1 \pmod{p}$.

Proof. ($\Longrightarrow$) Suppose a belongs to the exponent 2 modulo p. By definition, we have $a^2 \equiv 1 \pmod{p}$. By Lemma 2.10, we have $a \equiv \pm 1 \pmod{p}$. But if $a \equiv 1 \pmod{p}$ then a belongs to the exponent 1 modulo p. Thus $a \equiv -1 \pmod{p}$.

($\Longleftarrow$) Suppose $a \equiv -1 \pmod{p}$. Then by Lemma 2.10 $a^2 \equiv 1 \pmod{p}$. We cannot have $a \equiv 1 \pmod{p}$ by assumption, so a belongs to the exponent 2 modulo p. ■

Lemma (Lemma 2.10)

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

8 §2.8 #7

Problem (§2.8 #7)
If p is an odd prime, how many solutions are there to $x^{p-1} \equiv 1 \pmod{p}$; to $x^{p-1} \equiv 2 \pmod{p}$?

Solution. Suppose p is an odd prime. For the congruence $x^{p-1} \equiv 1 \pmod{p}$ there are

$$\boxed{p-1 \text{ solutions.}}$$

The choice of $n = p-1$, $m = p$, and $a = 1$ in Corollary 2.42, with

$$\frac{\phi(m)}{(n, \phi(m))} = \frac{\phi(p)}{(p-1, \phi(p))} = \frac{p-1}{(p-1, p-1)} = 1$$

and

$$\begin{aligned} a^{\phi(m)/(n,\phi(m))} &\equiv 1^1 \pmod{p} \\ &\equiv 1 \pmod{p} \end{aligned}$$

imply that there are $(p-1, \phi(p)) = p-1$ solutions.

Now the choice of $n = p-1$, $m = p$, and $a = 2$ in Corollary 2.42 gives

$$\begin{aligned} a^{\phi(m)/(n,\phi(m))} &\equiv 2^1 \pmod{p} \\ &\not\equiv 1 \pmod{p}, \end{aligned}$$

which implies that the congruence $x^{p-2} \equiv 2 \pmod{p}$ has

$$\boxed{0 \text{ solutions,}}$$

as required. ■

Corollary (Corollary 2.42)
Suppose that $m = 1, 2, 4, p^\alpha$, or $2p^\alpha$, where p is an odd prime. If $(a, m) = 1$, then the congruence $x^n \equiv a \pmod{m}$ has $(n, \phi(m))$ solutions or no solution, according as

$$a^{\phi(m)/(n,\phi(m))} \equiv 1 \pmod{m}$$

or not.

Remark 5. *Alternatively, for all the $p-1$ integers $0 < a \leq p-1$ we have $a^{p-1} \equiv 1 \pmod{p}$ by Fermat's little theorem, and clearly $0^{p-1} \not\equiv 1 \pmod{p}$. Thus $x^{p-1} \equiv 1 \pmod{p}$ for $x \in \{1, \ldots, p-1\}$, i.e., $x^{p-1} \not\equiv 2 \pmod{p}$ for $x \in \{1, \ldots, p-1\}$. One can then check $x = 0$. This is another way of deducing that the former has $p-1$ solutions and the latter has 0 solutions.*

9 §2.8 #20

Problem (§2.8 #20)
Of the 101 integers in a complete residue system $\pmod{101^2}$ that are $\equiv 2 \pmod{101}$, which one is not a primitive root $\pmod{101^2}$?

Solution. This number is

8385.

Let $p = 101$ and $\alpha = 1$. By Theorem 2.41, there exists a primitive root modulo 101. Now by Euler's theorem $2^{100} = 2^{\phi(101)} \equiv 1 \pmod{101}$, so now we show that $2^n \not\equiv 1$ for any smaller power of n (i.e., $0 < n < \phi(101) = 100$). Suppose such an n exists, so $2^n \equiv 1 \pmod{101}$; by Lemma 2.31, $n \mid 100$. We iterate:

$$\begin{aligned} 2^1 &\equiv 2 \pmod{101}, & 2^2 &\equiv 4 \pmod{101}, & 2^4 &\equiv 16 \pmod{101}, \\ 2^5 &\equiv 32 \pmod{101}, & 2^{10} &\equiv 14 \pmod{101}, & 2^{20} &\equiv 95 \pmod{101}, \\ 2^{25} &\equiv 10 \pmod{101}, & 2^{50} &\equiv 100 \pmod{101}, & 2^{100} &\equiv 1 \pmod{101}. \end{aligned}$$

A number $\equiv 2 \pmod{101}$ is of the form $2 + 101k$ for some $k \in \mathbb{Z}$. Let h denote its order modulo 101^2. Since $1 \equiv (2+101k)^h \pmod{101^2}$, we have $1 \equiv (2+101k)^h \equiv 2^h \pmod{101}$, so $100 \mid h$ by Lemma 2.31. On the other hand, $h \mid \phi\left(101^2\right) = 100 \cdot 101$ by Lemma 2.31. Thus $h = 100$ or $h = 100 \cdot 101$. Suppose $h \neq 100 \cdot 101$ (i.e., $2+101k$ is not a primitive root modulo 101^2). Then $h = 100$; if we let $f(x) = x^{100} - 1$, then we want to find $a \in \mathbb{Z}$ such that

$$0 \equiv f(a) \pmod{101^2}.$$

Since $f(2) = 0$ and $f'(2) = 100 \cdot 2^{99} \not\equiv 0 \pmod{101}$ (since otherwise $101 \mid 100$ or $101 \mid 2^{99}$, both of which are impossible), Hensel's lemma implies that with the choice $\overline{f'(2)} = -2$ such that $f'(2)\overline{f'(2)} \equiv 1 \pmod{101}$, the solution

$$a = 2 - \left(2^{100} - 1\right)\overline{f'(2)} = 2^{101} = 2 \cdot 2^{100} \equiv 2 \pmod{101}$$

gives $f(a) \equiv 2^{101 \cdot 100} - 1 \equiv 0 \pmod{100}$, so 2^{101} is a primitive root modulo 101^2, and it is unique since it is nonsingular. From here, we compute $101 = 80 + 20 + 1$, $1024 = 101 \cdot 10 + 14$, and

$$\begin{aligned} 2^{10} &\equiv 1024 \pmod{101^2}, \\ 2^{20} &\equiv (101 \cdot 10 + 14)^2 \pmod{101^2} \\ &\equiv 2 \cdot 10 \cdot 101 \cdot 14 + 14^2 \pmod{101^2} \\ &\equiv 101 \cdot 282 - 6 \pmod{101^2}, \\ 2^{80} &\equiv (101 \cdot 282 - 6)^4 \pmod{101^2} \\ &\equiv 4 \cdot 101 \cdot 282 \cdot (-6)^3 + 6^4 \pmod{101^2} \\ &\equiv 101 \cdot 78 - 17 \pmod{101^2}, \\ 2^{101} &\equiv 2^{80} \cdot 2^{20} \cdot 2 \pmod{101^2}, \\ &\equiv (101 \cdot 78 - 17)(101 \cdot 282 - 6)(2) \pmod{101^2} \\ &\equiv 8385 \pmod{101^2}, \end{aligned}$$

as desired. ■

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 $h \mid k$.

Remark 6. *Technically, we did not have to use Theorem 2.41 to show that there exists primitive roots modulo* 101 *since in the proof we showed that* 2 *is a primitive root modulo* 101*, but in practice it's safer to first check if there is a primitive root before trying to find one.*

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 7. *The proof of this result mirrors that of Theorem 2.39.*

Theorem (Theorem 2.39)
If p is a prime then there exists $\phi\left(\phi\left(p^2\right)\right) = (p-1)\phi(p-1)$ primitive roots modulo p^2.

10 §2.8 #21

Problem (§2.8 #21)
Let g be a primitive root of the odd prime p. Show that $-g$ is a primitive root, or not, according as $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$.

Proof. Since g is a primitive root of p, by definition $g^{p-1} \equiv 1 \pmod p$ and $g^n \not\equiv 1 \pmod p$ for any integer $1 \leq n < p-1$. Since p is odd, $x = g^{(p-1)/2}$ is a solution to the congruence $x^2 \equiv 1 \pmod p$. But the only such solutions are when $x \equiv 1 \pmod p$ or when $x \equiv -1 \pmod p$, by Lemma 2.10; however, $x \equiv 1 \pmod p$ is impossible since otherwise $g^{(p-1)/2} \equiv 1 \pmod p$ implies that g is not a primitive root. Therefore,

$$g^{(p-1)/2} \equiv -1 \pmod p.$$

Suppose that $p \equiv 1 \pmod 4$. Then there exists some $k \in \mathbb{Z}$ such that $p = 4k+1$. Then

$$(-g)^{p-1} = (-g)^{4k} = g^{4k} = g^{p-1} \equiv 1 \pmod p$$

and for all integers $1 \leq n < p-1$, we have

$$(-g)^n = (-1)^n g^n \equiv \begin{cases} g^n \pmod p & \text{if } n \text{ is even,} \\ -g^n \pmod p & \text{if } n \text{ is odd.} \end{cases}$$

For n even, we see that $(-g)^n \equiv g^n \pmod p \not\equiv 1 \pmod p$. For n odd, then $g^n \not\equiv -1 \pmod p$; because g is a primitive root, $g^n \equiv -1 \pmod p$ only when $n = (p-1)/2 = 2k$, which is even. It follows that $(-g)^n \pmod p \equiv -g^n \not\equiv 1 \pmod p$. Therefore, $-g$ is a primitive root modulo p.

Now suppose that $p \equiv 3 \pmod 4$. Then there exists some $k \in \mathbb{Z}$ such that $p = 4k+3$. Then

$$(-g)^{(p-1)/2} = (-1)^{(p-1)/2} g^{(p-1)/2} = (-1)^{2k+1} g^{(p-1)/2} = -g^{(p-1)/2} \equiv 1 \pmod p,$$

so $-g$ is not a primitive root modulo p. ■

Remark 8. *One key property about a primitive root g modulo m is that the set $\{g^n \bmod m \mid n \in \{1, \ldots, \phi(m)\}\}$ is a complete reduced residue system modulo m. In other words, g generates all positive integers $1, \ldots, m$ that are coprime to m. In particular, this is the reason why $g^n \equiv -1 \pmod p$ only when $n = (p-1)/2$ and no other integers, as the set has $\phi(m)$ integers and there are only $\phi(m)$ integers in $1, \ldots, m$ that are coprime to m.*