18.781 Theory of Numbers

Problem Set 2

Official Solutions

February 20, 2026

Contents

Disclaimer

This document contains the official solutions to Problem Set 2 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 §2.1 #12

Problem (§2.1 #12)
Prove that 19 is not a divisor of $4n^2 + 4$ for any integer n.

Proof. We want to show that for all $n \in \mathbb{Z}$,

$$4n^2 + 4 \not\equiv 0 \pmod{19}.$$

Suppose for the sake of contradiction that some $n_0 \in \mathbb{Z}$ satisfies

$$4n^2 + 4 \equiv 4\left(n^2 + 1\right) \equiv 0 \pmod{19}.$$

Then since $(4, 19) = 1$ we can divide by 4 and obtain

$$n^2 + 1 \equiv 0 \pmod{19}.$$

But by Theorem 2.12, for any prime p the congruence $x^2 \equiv -1 \pmod{p}$ has solutions if and only if $p = 2$ or $p \equiv 1 \pmod{4}$, which 19 does not satisfy. ■

Remark 1. *It is important to recognize when you can divide both sides of a congruence (cf. Theorem 2.3).*

Theorem (Theorem 2.3) (a) $ax \equiv ay \pmod{m}$ if and only if $x \equiv y \pmod{m/(a, m)}$.

(b) If $ax \equiv ay \pmod{m}$ and $(a, m) = 1$, then $x \equiv y \pmod{m}$.

(c) $x \equiv y \pmod{m_i}$ for $i = 1, 2, \ldots, r$ if and only if $x \equiv y \pmod{[m_1, m_2, \ldots, m_r]}$.

Theorem (Theorem 2.12)
Let p denote a prime. Then $x^2 \equiv -1 \pmod{p}$ has solutions if and only if $p = 2$ or $p \equiv 1 \pmod{4}$.

2 §2.1 #17

Problem (§2.1 #17)
Show that $61! + 1 \equiv 63! + 1 \equiv 0 \pmod{71}$.

Proof. We first note that 71 is a prime. By Wilson's theorem,

$$70! \equiv -1 \pmod{71}.$$

But $70! = 63! \cdot 64 \cdot 65 \cdot 66 \cdot 67 \cdot 68 \cdot 69 \cdot 70$, so

$$\begin{aligned}
-1 &\equiv 70! \pmod{71} \\
&\equiv 63! \cdot 64 \cdot 65 \cdot 66 \cdot 67 \cdot 68 \cdot 69 \cdot 70 \\
&\equiv 63! \cdot (-7) \cdot (-6) \cdot (-5) \cdot (-4) \cdot (-3) \cdot (-2) \cdot (-1) \pmod{71} \\
&\equiv 63! \cdot (7) \cdot (6) \cdot (5) \cdot (4) \cdot (3) \cdot (2) \cdot (-1) \pmod{71} \\
&\equiv 63! \cdot (7) \cdot (6) \cdot (5) \cdot 2 \cdot 2 \cdot (3) \cdot (2) \cdot (-1) \pmod{71} \\
&\equiv 63! \cdot \underbrace{(6) \cdot 2 \cdot 2 \cdot (3)}_{72 \equiv 1 \pmod{71}} \cdot \underbrace{(7) \cdot (5) \cdot (2)}_{70 \equiv -1 \pmod{71}} \cdot (-1) \pmod{71} \\
&\equiv 63! \cdot 1 \cdot (-1) \cdot (-1) \pmod{71} \\
&\equiv 63! \pmod{71},
\end{aligned}$$

so $63! + 1 \equiv 0 \pmod{71}$. To show the other congruence, note that $63! = 61! \cdot 62 \cdot 63$, so

$$\begin{aligned}
-1 &\equiv 63! \pmod{71} \\
&\equiv 61! \cdot 62 \cdot 63 \pmod{71} \\
&\equiv 61! \cdot \underbrace{(-9) \cdot (-8)}_{72 \equiv 1 \pmod{71}} \pmod{71} \\
&\equiv 61! \pmod{71}.
\end{aligned}$$

Thus $61! + 1 \equiv 0 \pmod{71}$. ∎

Remark 2. *The natural theorem to apply is Wilson's theorem because of the appearance of the factorial. This exercise especially exemplifies the utility of congruences in reducing large factors.*

Theorem (Wilson's theorem, Theorem 2.11)
If p is a prime, then $(p-1)! \equiv -1 \pmod{p}$.

Remark 3. *The converse of Wilson's theorem is also true! Thus, p is a prime if and only if $(p-1)! \equiv -1 \pmod{p}$. It's a nice exercise to try and show this.*

3 §2.1 #25

Problem (§2.1 #25)
Prove that $n^{12} - a^{12}$ is divisible by 91 if n and a are prime to 91.

Proof. Suppose $(n, 91) = (a, 91) = 1$. The key thing to realize is that 91 is not prime; indeed, $91 = 7 \cdot 13$, and $[7, 13] = 91$. Thus, to show

$$n^{12} - a^{12} \equiv 0 \pmod{91},$$

we show both

$$n^{12} - a^{12} \equiv 0 \pmod{7},$$
$$n^{12} - a^{12} \equiv 0 \pmod{13}$$

by Theorem 2.3. By Fermat's little theorem,

$$n^6 \equiv 1 \pmod{7},$$
$$a^6 \equiv 1 \pmod{7},$$

so

$$n^{12} \equiv 1 \pmod{7},$$
$$a^{12} \equiv 1 \pmod{7},$$

and

$$n^{12} - a^{12} \equiv 0 \pmod{7}.$$

Similarly, Fermat's little theorem implies

$$n^{12} \equiv 1 \pmod{13},$$
$$a^{12} \equiv 1 \pmod{13},$$

so

$$n^{12} - a^{12} \equiv 0 \pmod{13}.$$

This completes the proof. ∎

Remark 4. *The important theorems here are Theorem 2.3 and Fermat's little theorem.*

Theorem (Fermat's theorem, Theorem 2.7)
Let p denote a prime. If $p \nmid a$ then $a^{p-1} \equiv 1 \pmod{p}$. For every integer a, $a^p \equiv a \pmod{p}$.

4 §2.1 #27

Problem (§2.1 #27)
Prove that $\frac{1}{5}n^5 + \frac{1}{3}n^3 + \frac{7}{15}n$ is an integer for every integer n.

Proof. Note

$$\frac{1}{5}n^5 + \frac{1}{3}n^3 + \frac{7}{15}n = \frac{3n^5 + 5n^3 + 7n}{15}.$$

To show this is an integer, we show $15 \mid \left(3n^5 + 5n^3 + 7n\right)$, or that

$$3n^5 + 5n^3 + 7n \equiv 0 \pmod{15}.$$

But $[3, 5] = 15$, so by Theorem 2.3, it suffices to show

$$3n^5 + 5n^3 + 7n \equiv 0 \pmod{3},$$
$$3n^5 + 5n^3 + 7n \equiv 0 \pmod{5}.$$

The first follows from $n^3 \equiv n \pmod{3}$ (Fermat's theorem), so

$$\begin{aligned} 3n^5 + 5n^3 + 7n &\equiv 2n^3 + n \pmod{3} \\ &\equiv 2n + n \pmod{3} \\ &\equiv 3n \pmod{3} \\ &\equiv 0 \pmod{3}. \end{aligned}$$

Similarly, the second follows from $n^5 \equiv n \pmod{5}$ (again by Fermat), so

$$\begin{aligned} 3n^5 + 5n^3 + 7n &\equiv 3n^5 + 2n \pmod{5} \\ &\equiv 3n + 2n \pmod{5} \\ &\equiv 5n \pmod{5} \\ &\equiv 0 \pmod{5}. \end{aligned}$$

This concludes the proof. ■

Remark 5. *You should always look for places where you can apply Fermat's theorem or Wilson's theorem!*

5 §2.1 #45

Problem (§2.1 #45)
Show that if p is prime then $\binom{p}{k} \equiv 0 \pmod{p}$ for $1 \leqslant k \leqslant p-1$.

Proof. Let p be a prime, and let $k \in \{1, \ldots, p-1\}$. Note that

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = n$$

for some integer n. Then $nk!(p-k)! = p!$ and applying mod p yields

$$nk!(p-k)! = p! \equiv 0 \pmod{p}.$$

Since $k \in \{1, \ldots, p-1\}$, $(k!, p) = ((p-k)!, p) = 1$ (can you convince yourself of this?), so Theorem 2.3 applies and we divide by $k!$ and $(p-k)!$. This yields

$$n \equiv 0 \pmod{p},$$

which is the result. ■

Remark 6. *This fundamental result is useful in advanced number theory. A frequent application of this is known as the* Freshmen's Dream *of*

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

Can you see how you can derive this result? (Hint: Use the binomial theorem.)

6 §2.1 #46

Problem (§2.1 #46)
For any prime p, if $a^p \equiv b^p \pmod{p}$, prove that $a^p \equiv b^p \pmod{p^2}$.

Proof. Let p be a prime, and suppose $a^p \equiv b^p \pmod{p}$. But Fermat's little theorem implies that

$$a^p \equiv a \pmod{p},$$
$$b^p \equiv b \pmod{p},$$

so we conclude

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

Therefore, there exists some $k \in \mathbb{Z}$ such that $a = b + kp$. Then we apply the binomial theorem and get

$$\begin{aligned} a^p &= (b+kp)^p \\ &= \sum_{i=0}^{p} \binom{p}{i} b^i (kp)^{p-i} \\ &= \sum_{i=0}^{p-2} \underbrace{\binom{p}{i} b^i (kp)^{p-i}}_{\text{divisible by } p^2} + \underbrace{\binom{p}{p-1} b^{p-1}(kp)}_{\text{divisible by } p^2} + \binom{p}{p} b^p. \end{aligned}$$

Taking mod p^2 yields

$$a^p \equiv b^p \pmod{p^2},$$

as desired. ∎

7 §2.1 #51

Problem (§2.1 #51)
Prove that $(p-1)! \equiv p-1 \pmod{1+2+\cdots+(p-1)}$ if p is a prime.

Proof. The claim follows easily for $p = 2$, so now suppose $p > 2$. Importantly, p is odd. Note

$$1+2+\cdots+(p-1) = \frac{p(p-1)}{2}.$$

Since $(p-1)/2 < p$ (if p were not odd, then $(p-1)/2$ would not be well defined), $((p-1)/2, p) = 1$. Moreover, $[(p-1)/2, p] = p(p-1)/2$, so by Theorem 2.3 it suffices to show both

$$(p-1)! \equiv p-1 \pmod{p},$$
$$(p-1)! \equiv p-1 \pmod{(p-1)/2}.$$

The first congruence is immediate from Wilson's theorem. Since $(p-1)/2$ is well defined, we write the second congruence as

$$(p-1)! \equiv 2 \cdot \frac{p-1}{2} \pmod{(p-1)/2},$$

from which it is clear that both sides of the congruence are divisible by $(p-1)/2$. (For the left, expand out $(p-1)!$.) ■

8 §2.2 #6

Problem (§2.2 #6)

How many solutions are there to each of the following congruences:

(a) $15x \equiv 25 \pmod{35}$;

(b) $15x \equiv 24 \pmod{35}$;

(c) $15x \equiv 0 \pmod{35}$?

Solution. We use Theorem 2.17.

(a) Since $(15, 35) = 5 \mid 25$, there are $(15, 35) = 5$ solutions.

(b) Since $(15, 35) = 5 \nmid 24$, there are no solutions.

(c) Since $(15, 35) = 5 \mid 0$, there are $(15, 35) = 5$ solutions.

The exercise is complete. ■

Remark 7. *Theorem 2.17 gives the complete classification of solutions to linear congruences. It is a good additional exercise to find all solutions. As an example, let's find all* 5 *solutions to* $15x \equiv 25 \pmod{35}$. *The proof of Theorem 2.17 suggests that we first divide by* $(15, 35) = 5$, *which gives*

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

Next, the proof suggests that we find a multiplicative inverse of 3 *modulo* 7*; that is, some integer* y *such that* $3y \equiv 1 \pmod{7}$. *Since* $(3, 7) = 1$, *the Euclidean algorithm should give us an integer linear combination* $3a + 7b = 1$, *from which we can take* mod 7. *The algorithm gives*

$$7 = 3 \cdot 2 + 1,$$
$$3 = 1 \cdot 3 + 0,$$

so $7 = 3 \cdot 2 + 1$ *and*

$$7 + 3 \cdot (-2) = 1.$$

This implies that $-2 \equiv 5 \pmod{7}$ *is our multiplicative inverse modulo* 7. *Multiplying* $3x \equiv 5 \pmod{7}$ *by* 5 *yields*

$$x \equiv 25 \pmod{7} \equiv 4 \pmod{7}.$$

Thus, $x = 4$ *is a solution to* $15x \equiv 25 \pmod{35}$. *There are four other solutions, all spaced out by* $35/(15, 35) = 7$, *so the complete set is*

$$x \in \{4, 11, 18, 25, 32\}.$$

Theorem (Theorem 2.17)

Let a, b, and $m > 0$ be given integers, and put $g = (a, m)$. The congruence $ax \equiv b \pmod{m}$ has a solution if and only if $g \mid b$. If this condition is met, then the solutions form an arithmetic progression with common difference m/g, giving g solutions mod m.

9 §2.2 #14

Problem (§2.2 #14)
Show that $\binom{p^\alpha}{k} \equiv 0 \pmod{p}$ for $0 < k < p^\alpha$.

Proof. We proceed with induction. Problem 5 (§2.2 #14) shows the claim for $\alpha = 1$. Now suppose the claim is true for $n = \alpha$ (i.e., for all $0 < k < p^\alpha$, $\binom{p^\alpha}{k} \equiv 0 \pmod{k}$). Using the same idea of *Freshmen's Dream* (cf. Remark 6) in §2.1 #45 (5),

$$(1+x)^{p^\alpha} = \sum_{k=0}^{p^\alpha} \binom{p^\alpha}{k} x^k \equiv 1 + x^{p^\alpha} \pmod{p}.$$

Then on the one hand,

$$\begin{aligned}(1+x)^{p^{\alpha+1}} &= \left((1+x)^{p^\alpha}\right)^p \\ &\equiv \left(1+x^{p^\alpha}\right)^p \pmod{p} \\ &\equiv 1 + x^{p^{\alpha+1}} \pmod{p}\end{aligned}$$

by *Freshmen's Dream* (cf. Remark 6) in §2.1 #45 (5). On the other hand,

$$(1+x)^{p^{\alpha+1}} = \sum_{k=0}^{p^{\alpha+1}} \binom{p^{\alpha+1}}{k} x^k = 1 + \sum_{k=1}^{p^{\alpha+1}-1} \binom{p^{\alpha+1}}{k} x^k + x^{p^{\alpha+1}}.$$

Comparing the two expansions for $(1+x)^{p^{\alpha+1}}$ gives

$$1 + \sum_{k=1}^{p^{\alpha+1}-1} \binom{p^{\alpha+1}}{k} x^k + x^{p^{\alpha+1}} \equiv 1 + x^{p^{\alpha+1}} \bmod p,$$

which implies that

$$\binom{p^{\alpha+1}}{k} \equiv 0 \pmod{p}$$

for all $0 < k < p^{\alpha+1}$. This completes the induction step. ∎

10 §2.2 #17

Problem (§2.2 #17)

Let the numbers c_i be defined by the power series identity

$$\left(1 + x + \cdots + x^{p-1}\right) / (1-x)^{p-1} = 1 + c_1 x + c_2 x^2 + \cdots.$$

Show that $c_i \equiv 0 \pmod{p}$ for all $i \geqslant 1$.

Proof. Note that

$$(1-x)^p \equiv 1 - x^p \pmod{p};$$

see *Freshmen's Dream* (cf. Remark 6) in §2.1 #45 (5). To use this, we observe that

$$1 + x + \cdots + x^{p-1} = \frac{1-x^p}{1-x},$$

and so

$$\frac{1-x^p}{(1-x)^p} = \frac{1 + x + \cdots + x^{p-1}}{(1-x)^{p-1}} = 1 + c_1 x + c_2 x^2 + \cdots.$$

Therefore,

$$1 - x^p = \left(1 + c_1 x + c_2 x^2 + \cdots\right)(1-x)^p.$$

Taking modulo p then gives

$$1 - x^p \equiv \left(1 + c_1 x + c_2 x^2 + \cdots\right)(1 - x^p) \pmod{p}.$$

For $i \geq 1$ and $i \neq p$, the coefficients of the x^i term on the left and right sides are 0 and c_i, respectively, modulo p, so $c_i \equiv 0 \pmod{p}$ for all $i \geq 1$ and $i \neq p$. For the $i = p$ case, the coefficient of the x^p term on the left and right sides are -1 and $-1 + c_p$, respectively, modulo p. Thus, $c_p \equiv 0 \pmod{p}$ as well. ∎

Remark 8. *You can also prove this more directly by multiplying everything out and comparing coefficients modulo p.*