18.781 Theory of Numbers

Problem Set 3

Official Solutions

February 27, 2026

Contents

Disclaimer

This document contains the official solutions to Problem Set 3 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 §2.3 #8

Problem (§2.3 #8)
Find the smallest positive integer giving remainders 1, 2, 3, 4, and 5 when divided by 3, 5, 7, 9, and 11, respectively.

Solution. We aim to find the smallest positive integer x satisfying the simultaneous congruences

$$\begin{aligned} x &\equiv 1 \pmod 3, \\ x &\equiv 2 \pmod 5, \\ x &\equiv 3 \pmod 7, \\ x &\equiv 4 \pmod 9, \\ x &\equiv 5 \pmod{11}. \end{aligned}$$

Now all integers satisfying $x \equiv 4 \pmod 9$ also satisfy $x \equiv 1 \pmod 3$. Thus, we drop the first congruence as it is redundant. One verifies that all the moduli are pairwise prime. The Chinese remainder theorem then guarantees a solution modulo $3465 = 5 \cdot 7 \cdot 9 \cdot 11$. Now the numbers $b_1 = 2$, $b_2 = 3$, $b_3 = 4$, and $b_4 = 8$ satisfy the congruences

$$\begin{aligned} \left(\frac{m}{5}\right) b_1 = 693 b_1 \equiv 3 b_1 &\equiv 1 \pmod 5, \\ \left(\frac{m}{7}\right) b_2 = 495 b_2 \equiv 5 b_2 &\equiv 1 \pmod 7, \\ \left(\frac{m}{9}\right) b_3 = 385 b_3 \equiv 7 b_3 &\equiv 1 \pmod 9, \\ \left(\frac{m}{11}\right) b_4 = 315 b_4 \equiv 7 b_4 &\equiv 1 \pmod{11}. \end{aligned}$$

The construction of the solution x_0 in the Chinese remainder theorem then gives

$$x_0 \equiv \left(\frac{m}{5}\right) b_1 \cdot 2 + \left(\frac{m}{7}\right) b_2 \cdot 3 + \left(\frac{m}{9}\right) b_3 \cdot 4 + \left(\frac{m}{11}\right) b_4 \cdot 5 \pmod m \equiv 25987 \pmod{3465} \equiv 1732 \pmod{3465},$$

so 1732 is the smallest positive integer satisfying the simultaneous congruences. ■

Remark 1. *To apply the Chinese remainder theorem, one must first check that the moduli are all pairwise prime.*

Theorem (Chinese remainder theorem, Theorem 2.18)
Let $m_1, \ldots, m_r$ denote r positive integers that are relatively prime in pairs, and let $a_1, \ldots, a_r$ denote any r integers. Then the congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

have common solutions. If x_0 is one such solution, then an integer x satisfies the congruences if and only if x is of the form $x = x_0 + km$ for some integer k. Here $m = m_1 m_2 \cdots m_r$.

2 §2.3 #18

Problem (§2.3 #18)
Given any positive integer k, prove that there are k consecutive integers each divisible by a square > 1.

Proof. Let k be any positive integer. Let $p_1, \ldots, p_k$ be the first k primes. Then $p_1^2, \ldots, p_k^2$ are all pairwise prime. We wish to find k consecutive integers $n+1, \ldots, n+k$ such that

$$n + i \equiv 0 \pmod{p_i^2}$$

for all $i \in \{1, \ldots, k\}$. The Chinese remainder theorem then applies and implies that there exists some integer n modulo $p_1^2 \cdots p_k^2$ such that n satisfies the above k simultaneous congruences. In other words, $p_i^2 \mid (n+i)$ for all $i \in \{1, \ldots, k\}$, so $n+1, \ldots, n+k$ are k consecutive integers that are divisible by a square > 1. ∎

Remark 2. *We could explicitly construct what n is, but all we need is the existence of such a n. This existence is guaranteed by the Chinese remainder theorem.*

3 §2.3 #20

Problem (§2.3 #20)
Let m_1 and m_2 be arbitrary positive integers, and let a_1 and a_2 be arbitrary integers. Show that there is a simultaneous solution of the congruences $x \equiv a_1 \pmod{m_1}$, $x \equiv a_2 \pmod{m_2}$, if and only if $a_1 \equiv a_2 \pmod{g}$, where $g = (m_1, m_2)$. Show that if this condition is met, then the solution is unique modulo $[m_1, m_2]$.

Proof. Let m_1, m_2, a_1, and a_2 be arbitrary integers. We prove the first claim.

($\implies$) Suppose there exists some integer x such that

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}. \end{aligned}$$

By definition, $m_1 \mid (x - a_1)$ and $m_2 \mid (x - a_2)$. Then putting $g = (m_1, m_2)$ we have $g \mid (x - a_1)$ and $g \mid (x - a_2)$ (since $g \mid m_1$, $g \mid m_2$, and transitivity). But

$$a_1 - a_2 = (x - a_2) - (x - a_1)$$

is now a difference of two multiples of g and is hence a multiple of g. In other words, $g \mid (a_1 - a_2)$, so

$$a_1 \equiv a_2 \pmod{g}.$$

($\impliedby$) Put $g = (m_1, m_2)$ again, and suppose that $a_1 \equiv a_2 \pmod{g}$. By definition, there exists some $k \in \mathbb{Z}$ such that $gk = a_1 - a_2$. We want to find a solution to the simultaneous congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}. \end{aligned}$$

If x is a solution of the first congruence, then $x = a_1 + m_1 t$ for some $t \in \mathbb{Z}$. If x is a solution of the second congruence as well, then $a_1 + m_1 t \equiv a_2 \pmod{m_2}$. In particular, $a_1 - a_2 \equiv -m_1 t \pmod{m_2}$. Write $m_1 = g m_1'$ and $m_2 = g m_2'$ for $(m_1', m_2') = 1$. Recall that $gk = a_1 - a_2$. Then we obtain $gk \equiv -g m_1' t \pmod{g m_2'}$, and dividing by g gives

$$m_1' t \equiv -k \pmod{m_2'}.$$

Now since $(m_1', m_2') = 1$, there exists a multiplicative inverse t of m_1' modulo m_2'. Then such a t gives the solution $x = a_1 + m_1 t$.

Now suppose that x and y are integers that satisfy

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_1}, \end{aligned} \qquad \begin{aligned} y &\equiv a_1 \pmod{m_1}, \\ y &\equiv a_2 \pmod{m_1}. \end{aligned}$$

Then in particular $x \equiv y \pmod{m_1}$ and $x \equiv y \pmod{m_2}$, so $m_1 \mid (x - y)$ and $m_2 \mid (x - y)$. Thus $[m_1, m_2] \mid (x - y)$, so

$$x \equiv y \pmod{[m_1, m_2]},$$

and the solution is unique modulo $[m_1, m_2]$. ∎

4 §2.3 #25

Problem (§2.3 #25)
If m and k are positive integers, prove that the number of positive integers $\leqslant mk$ that are prime to m is $k\phi(m)$.

Proof. Partition the set of all positive integers $\leq mk$ into k subsets

$$\begin{aligned}\mathscr{S}_1 &= \{1, \ldots, m\},\\ \mathscr{S}_2 &= \{m+1, \ldots, 2m\},\\ &\vdots\\ \mathscr{S}_k &= \{(k-1)m+1, \ldots, mk\}\end{aligned}$$

of size m each. By definition, there are exactly $\phi(m)$ integers of $\mathscr{S}_1$ that are prime to m; enumerate them by

$$\left\{x_1, \ldots, x_{\phi(m)}\right\},$$

so $(x_i, m) = 1$ for any $i \in \{1, \ldots, \phi(m)\}$. But Theorem 1.9 implies that

$$1 = (x_i, m) = (x_i + am, m)$$

for any such i and any integer a. In particular, choosing $a = 1, \ldots, k-1$ imply that there are exactly $\phi(m)$ integers of $\mathscr{S}_a$ that are prime to m for all $a \in \{1, \ldots, k-1\}$. Thus, the total number of integers $\leq mk$ is simply the sum across all k subsets, which is $k\phi(m)$. ■

5 §2.3 #26

Problem (§2.3 #26)
Show that $\phi(mn) = n\phi(m)$ if every prime that divides n also divides m.

Proof. Let m and n be integers, and suppose every prime that divides n also divides m. Therefore, if $p \mid mn$, then $p \mid m$ (since by Theorem 1.15 we have $p \mid m$ or $p \mid n$, and both imply $p \mid m$). By Theorem 2.19 we have

$$\phi(m) = m \prod_{p \mid m} \left(1 - \frac{1}{p}\right)$$

and

$$\begin{aligned}
\phi(mn) &= mn \prod_{p \mid mn} \left(1 - \frac{1}{p}\right) \\
&= mn \prod_{p \mid m} \left(1 - \frac{1}{p}\right) \\
&= n \left(m \prod_{p \mid m} \left(1 - \frac{1}{p}\right) \right) \\
&= n\phi(m),
\end{aligned}$$

as desired. ■

Remark 3. *The Euler totient function ϕ is what we call a* multiplicative function *because for any two positive integers m and n that are relatively prime we have $\phi(mn) = \phi(m)\phi(n)$. However, ϕ is* **not** completely multiplicative *because the relation does not hold for all positive integers m and n; take $m = 4$ and $n = 6$, for example. Then*

$$\phi(mn) = \phi(24) = 24(1 - 1/2)(1 - 1/3) = 8,$$

but

$$\phi(m)\phi(n) = \phi(4)\phi(6) = 4(1 - 1/2)6(1 - 1/2)(1 - 1/3) = 4.$$

Theorem (Theorem 2.19)
If m_1 and m_2 denote two positive, relatively prime integers, then $\phi(m_1 m_2) = \phi(m_1)\phi(m_2)$. Moreover, if m has the canonical factorization $m = \prod p^{\alpha}$, then $\phi(m) = \prod_{p \mid m} (p^{\alpha} - p^{\alpha - 1}) = m \prod_{p \mid m} (1 - 1/p)$.

6 §2.3 #44

Problem (§2.3 #44)

Prove the following generalization of Euler's theorem:

$$a^m \equiv a^{m-\phi(m)} \pmod{m}$$

for any integer a.

Proof. Let m and a be integers. By the fundamental theorem of arithmetic, m has prime divisors $p_1, \ldots, p_r$, and its unique prime factorization is of the form

$$m = \prod_{i=1}^{r} {p_i}^{\alpha(p_i)}.$$

We show for all $i \in \{1, \ldots, r\}$ that

$$a^m \equiv a^{m-\phi(m)} \pmod{p_i^{\alpha(p_i)}}.$$

If the above r congruences simultaneously hold, then the Chinese remainder theorem implies $a^m \equiv a^{m-\phi(m)} \pmod{m}$. To this end, fix an $i \in \{1, \ldots, r\}$ and consider the above congruence. There are two cases: $p_i \nmid a$ and $p_i \mid a$.

Suppose $p_i \nmid a$. Then $\left(p_i^{\alpha(p_i)}, a\right) = 1$, so Euler's theorem gives

$$a^{\phi\left(p_i^{\alpha(p_i)}\right)} \equiv 1 \pmod{p_i^{\alpha(p_i)}}.$$

We have this handy lemma.

Lemma 4

Let m and n be positive integers. If $m \mid n$, then $\phi(m) \mid \phi(n)$.

Since $p_i^{\alpha(p_i)} \mid m$, Lemma 4 gives $\phi\left(p_i^{\alpha(p_i)}\right) \mid \phi(m)$. Thus, there exists some integer k such that

$$\phi\left(p_i^{\alpha(p_i)}\right) k = \phi(m).$$

Hence

$$a^{\phi(m)} \equiv \left(a^{\phi\left(p_i^{\alpha(p_i)}\right)}\right)^k \equiv 1 \pmod{p_i^{\alpha(p_i)}}.$$

As such, $p_i^{\alpha(p_i)} \mid \left(a^{\phi(m)} - 1\right)$. But $\left(a^{\phi(m)} - 1\right) \mid a^{m-\phi(m)}\left(a^{\phi(m)} - 1\right) = a^m - a^{m-\phi(m)}$, so $p_i^{\alpha(p_i)} \mid \left(a^m - a^{m-\phi(m)}\right)$ and

$$a^m \equiv a^{m-\phi(m)} \pmod{p_i^{\alpha(p_i)}}.$$

Suppose $p_i \mid a$. Write $a = p_i s$ for some integer $q \geq 1$ and $m = p_i^{\alpha(p_i)} t$ for some integer $t \geq 1$. Then note that

$$a^m = (p_i q)^m = (p_i q)^{p_i^{\alpha(p_i)} t} = p_i^{p_i^{\alpha(p_i)}} q^{p_i^{\alpha(p_i)} t} = p_i^{\alpha(p_i)} p_i^{p_i^{\alpha(p_i)} - \alpha(p_i)} q^{p_i^{\alpha(p_i)} t},$$

where $p_i^{\alpha(p_i)} - \alpha(p_i) \geq 0$ because $p_i^{\alpha(p_i)} \geq \alpha(p_i)$. Therefore, $p_i^{\alpha(p_i)} \mid a^m$, which means

$$a^m \equiv 0 \pmod{p_i^{\alpha(p_i)}}.$$

On the other hand, since $\left(p_i^{\alpha(p_i)}, t\right) = 1$, we have

$$\phi(m) = \phi\left(p_i^{\alpha(p_i)} t\right) = \phi\left(p_i^{\alpha(p_i)}\right)\phi(t) = \left(p_i^{\alpha(p_i)} - p_i^{\alpha(p_i)-1}\right)\phi(t) = p_i^{\alpha(p_i)-1}(p_i - 1)\,\phi(t),$$

so

$$m - \phi(m) = p_i^{\alpha(p_i)} t - p_i^{\alpha(p_i)-1}(p_i - 1)\,\phi(t) = p_i^{\alpha(p_i)-1}\left(p_i t - (p_i - 1)\phi(t)\right).$$

But $p_i^{\alpha(p_i)-1} \geq \alpha(p_i)$ as well, so

$$a^{m-\phi(m)} = (p_i s)^{m-\phi(m)} = p_i^{p_i^{\alpha(p_i)-1}(p_i t-(p_i-1)\phi(t))} s^{m-\phi(m)}$$

has a factor of $p_i^{\alpha(p_i)}$. Therefore, $p_i^{\alpha(p_i)} \mid a^{m-\phi(m)}$, which means

$$a^{m-\phi(m)} \equiv 0 \pmod{p_i^{\alpha(p_i)}}.$$

Hence

$$a^m \equiv a^{m-\phi(m)} \pmod{p_i^{\alpha(p_i)}}.$$

Now we prove Lemma 4.

Proof of Lemma 4. Suppose $m \mid n$. Then every prime p that divides m also divides n (i.e., if $p \mid m$, then $p \mid n$). Then

$$\phi(m) = m \prod_{p \mid m} \left(1 - \frac{1}{p}\right)$$

divides

$$n \prod_{p \mid n} \left(1 - \frac{1}{p}\right) = \phi(n)$$

since $m \mid n$ and $\prod_{p \mid m}\left(1 - \frac{1}{p}\right) \mid \prod_{p \mid n}\left(1 - \frac{1}{p}\right)$. ■

The proof is complete. ■

Theorem (Euler's theorem, Theorem 2.8)
If $(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \pmod{m}$.

7 §2.3 #45

Problem (§2.3 #45)
Find the number of solutions of $x^2 \equiv x \pmod{m}$ for any positive integer m.

Solution. Let m be any positive integer. By the fundamental theorem of arithmetic, m has prime divisors $p_1, \ldots, p_r$, and its unique prime factorization is of the form

$$m = \prod_{i=1}^{r} {p_i}^{\alpha(p_i)}.$$

Let x be a solution. By the Chinese remainder theorem, the solutions to $x^2 \equiv x \pmod{m}$ correspond to solutions to the r simultaneous congruences

$$\begin{aligned} x^2 &\equiv x \pmod{p_1^{\alpha(p_1)}}, \\ &\vdots \\ x^2 &\equiv x \pmod{p_r^{\alpha(p_r)}}. \end{aligned}$$

Fix some $i \in \{1, \ldots, r\}$ and consider the congruence $x^2 \equiv x \pmod{p_i^{\alpha(p_i)}}$, or $x(x-1) \equiv 0 \pmod{p_i^{\alpha(p_i)}}$. Then we have $p_i^{\alpha(p_i)} \mid x(x-1)$. But $(x, x-1) = 1$ (why?), so either $p_i^{\alpha(p_i)} \mid x$ or $p_i^{\alpha(p_i)} \mid (x-1)$. Equivalently, we have either $x \equiv 0 \pmod{p_i^{\alpha(p_i)}}$ or $x \equiv 1 \pmod{p_i^{\alpha(p_i)}}$, so the congruence $x^2 \equiv x \pmod{p_i^{\alpha(p_i)}}$ gives two choices of $a_i \in \{0, 1\}$ where

$$x \equiv a_i \pmod{p_i^{\alpha(p_i)}}.$$

This holds for any $i \in \{1, \ldots, r\}$, so the total number of choices of $a_1, \ldots, a_r$ for all r congruences simultaneously (and hence $x^2 \equiv x \pmod{m}$) is 2^r. Each choice of $a_1, \ldots, a_r$ gives rise to a unique solution to $x^2 \equiv x \pmod{m}$, so there are 2^r solutions to $x^2 \equiv x \pmod{m}$, where r is the number of distinct prime factors of m. ■

Remark 5. *To see $(x, x-1) = 1$, note the integer linear combination $x - (x-1) = 1$ and Theorem 1.4.*

8 §2.4 #4

Problem (§2.4 #4)
Show that the Carmichael number 561 is composite by showing that it is not a spsp(2).

Proof. Note that $560 = 561 - 1 = 2^4 \cdot 35$. Since $35 = 1 + 2 + 2^5$, we have

$$2^{35} = 2^{1+2+2^5} = 2 \cdot 2^2 \cdot 2^{32}.$$

By repeatedly squaring, we obtain

$$\begin{aligned}
2 &\equiv 2 \pmod{561},\\
2^2 &\equiv 4 \pmod{561},\\
2^4 &\equiv 16 \pmod{561},\\
2^8 &\equiv 256 \pmod{561},\\
2^{16} &\equiv 256^2 \pmod{561}\\
&\equiv 460 \pmod{561},\\
2^{32} &\equiv 460^2 \pmod{561},\\
&\equiv 103 \pmod{561}.
\end{aligned}$$

Then repeatedly squaring again gives

$$\begin{aligned}
2^{35} &\equiv 2 \cdot 4 \cdot 103 \equiv 263 \pmod{561},\\
2^{70} &\equiv 263^2 \equiv 166 \pmod{561},\\
2^{140} &\equiv 166^2 \equiv 67 \pmod{561},\\
2^{280} &\equiv 67^2 \equiv 1 \pmod{561},\\
2^{560} &\equiv 1^2 \equiv 1 \pmod{561}.
\end{aligned}$$

Suppose for the sake of contradiction that 561 is prime. Then $x^2 \equiv 1 \pmod{561}$ if and only if $x \equiv \pm 1 \pmod{561}$ by Lemma 2.10. But from the above calculation, we pick $x = 67$; clearly $67^2 \equiv 1 \pmod{561}$, but $67 \not\equiv \pm 1 \pmod{561}$. Therefore, 561 must be composite. ■

Remark 6. *The hint in the problem about showing that* 561 *is not* spsp(2) *suggests that we take* 2 *to be our base. We then follow the* strong pseudoprime test.

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

9 §2.4 #9

Problem (§2.4 #9)
Show that if $x^2 \equiv 1 \pmod{m}$ but $x \not\equiv \pm 1 \pmod{m}$, then $1 < (x-1, m) < m$, and that $1 < (x+1, m) < m$.

Proof. Suppose $x^2 \equiv 1 \pmod{m}$ and $x \not\equiv \pm 1 \pmod{m}$. Then

$$(x-1)(x+1) \equiv 0 \pmod{m}. \tag{1}$$

We prove this in four parts.

(I) Suppose that $(x-1, m) = 1$. Then there exists some integer y such that $(x-1)y \equiv 1 \pmod{m}$. We multiply congruence (1) by y to obtain

$$(x+1) \equiv 0 \pmod{m},$$

contrary to $x \not\equiv -1 \pmod{m}$. Thus $(x-1, m) > 1$.

(II) Suppose that $(x+1, m) = 1$. Then there exists some integer y such that $(x+1)y \equiv 1 \pmod{m}$. We multiply congruence (1) by y to obtain

$$(x-1) \equiv 0 \pmod{m},$$

contrary to $x \not\equiv 1 \pmod{m}$. Thus $(x+1, m) > 1$.

(III) Suppose that $(x-1, m) = m$. In particular, $m \mid (x-1)$, so $x \equiv 1 \pmod{m}$, a contradiction. Thus $(x-1, m) < m$.

(IV) Suppose that $(x+1, m) = m$. In particular, $m \mid (x+1)$, so $x \equiv -1 \pmod{m}$. Again, $(x+1, m) < m$.

Combining all four inequalities gives $1 < (x-1, m) < m$ and $1 < (x+1, m) < m$. ■