18.781 Theory of Numbers

Problem Set 6

Official Solutions

April 5, 2026

Contents

Disclaimer

This document contains the official solutions to Problem Set 6 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 §3.1 #6

Problem (§3.1 #6)

(a) List the quadratic residues of each of the primes 7, 13, 17, 29, 37.

(b) For any positive integer n, define $F(n)$ to be the minimum value of $\left|n^2 - 17x\right|$, where x runs over all integers. Prove that $F(n)$ is either 0 or a power of 2.

Proof. (a) The required quadratic residues are

mod 7:	$1, 2, 4,$
mod 13:	$1, 3, 4, 9, 10, 12,$
mod 17:	$1, 2, 4, 8, 9, 13, 15, 16,$
mod 29:	$1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28,$
mod 37:	$1, 3, 4, 7, 9, 10, 11, 12, 16, 21, 25, 26, 27, 28, 30, 33, 34, 36.$

(b) Note that $F(n)$ is the minimal distance from n^2 to the closest multiple of 17. For each $n \in \mathbb{N}$, write $n^2 = 17q + r$ for some unique integers $q \geq 0$ and $0 \leq r < 17$, per the division algorithm. Then

$$\left|n^2 - 17x\right| = |17q + r - 17x| = |17(q - x) + r|,$$

is some number $\equiv r \pmod{17}$, and as such the only such cases that can minimize the above quantity are when

- $q = x$, so $\left|n^2 - 17x\right| = r$, as if $q > x$ then $|17(q - x) + r| = 17(q - x) + r > r$; or
- $q = x - 1$, so $\left|n^2 - 17x\right| = 17 - r$, as if $q < x - 1$ then $|17(q - x) + r| = 17(x - q) - r > 17 - r$.

Therefore $F(n) = \min(r, 17 - r)$, where r is the unique integer such that $n^2 \equiv r \pmod{17}$ and $0 \leq r < 17$. Working modulo 17, we see that $r \in Q_{17} := \{0, 1, 2, 4, 8, 9, 13, 15, 16\}$ since Q_{17} is the set of quadratic residues modulo 17, by part (a). Then $F(n)$ can only attain the values in the set $\{\min(r, 17-r) \mid r \in Q_{17}\} = \{0, 1, 2, 4, 8\}$. Thus $F(n)$ is either 0 or a power of 2.

■

Remark 1. *Note that for an odd prime p, the number of* **nonzero** *residues is $p-1$. The number of* **nonzero** *quadratic residues modulo p is $(p-1)/2$, so the number of* **nonzero** *quadratic nonresidues modulo p is $(p-1)/2$ as well.*

2 §3.1 #7

Problem (§3.1 #7)

Which of the following congruences have solutions? How many?

(a) $x^2 \equiv 2 \pmod{61}$

(c) $x^2 \equiv -2 \pmod{61}$

Solution. Note 61 is an odd prime.

(a) We calculate

$$\left(\frac{2}{61}\right) = (-1)^{(61^2-1)/8} = (-1)^{(61-1)(61+1)/8} = (-1)^{15\cdot 31} = (-1)^{\text{odd integer}} = -1,$$

so $x^2 \equiv 2 \pmod{61}$ has no solutions.

(c) We calculate

$$\left(\frac{-2}{61}\right) = \left(\frac{-1}{61}\right)\left(\frac{2}{61}\right) = (-1)^{(61-1)/2}\left(\frac{2}{61}\right) = (-1)^{30}\left(\frac{2}{61}\right) = -1,$$

so $x^2 \equiv -2 \pmod{61}$ has no solutions.

The exercise is complete. ■

Remark 2. *This exercise is a simple exercise in using properties of the Legendre symbol. Keep in mind the following properties!*

Theorem (Theorem 3.1)

Let p be an odd prime. Then

(1) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$,

(2) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$,

(3) $a \equiv b \pmod{p}$ implies that $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$,

(4) If $(a, p) = 1$ then $\left(\frac{a^2}{p}\right) = 1$, $\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$,

(5) $\left(\frac{1}{p}\right) = 1$, $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.

Theorem (Theorem 3.3)

If p is an odd prime and $(a, 2p) = 1$, then

$$\left(\frac{a}{p}\right) = (-1)^t, \quad \text{where } t = \sum_{j=1}^{(p-1)/2} \left[\frac{ja}{p}\right]; \quad \text{also } \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

3 §3.1 #10

Problem (§3.1 #10)
Prove that if p is an odd prime then $x^2 \equiv 2 \pmod{p}$ has solutions if and only if $p \equiv 1$ or $\equiv 7 \pmod{8}$.

Proof. Suppose p is an odd prime.

($\implies$) Suppose $x^2 \equiv 2 \pmod{p}$ has solutions. Then by Theorem 3.3,

$$1 = \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8},$$

so $(p^2-1)/8$ is even. Thus, p^2-1 is divisible by 16, so $p^2-1 \equiv 0 \pmod{16}$. Since p is odd, write $p = 2k+1$ for some $k \in \mathbb{Z}$. Then $p^2-1 = 4k^2+4k = 4k(k+1)$, and $p^2-1 \equiv 4k(k+1) \equiv 0 \pmod{16}$ implies

$$k(k+1) \equiv 0 \pmod{4}.$$

Since k and $k+1$ are consecutive integers, only one of k or $k+1$ is even, and the one that is even must be divisible by 4; otherwise, $k(k+1)$ is only divisible by 2 and not 4. If $4 \mid k$, then $k = 4\ell$ for some $\ell \in \mathbb{Z}$ and $p = 2k+1 = 8\ell+1 \equiv 1 \pmod{8}$; if $4 \mid (k+1)$, then $k = 4k-1$ for some $\ell \in \mathbb{Z}$ and $p = 2k+1 = 8\ell-1 \equiv -1 \pmod{8} \equiv 7 \pmod{8}$.

($\impliedby$) Suppose that $p \equiv 1 \pmod{8}$ or $p \equiv 7 \pmod{8}$. In the former case, $p-1$ is divisible by 8 and $p+1$ is even (i.e., divisible by 2), so $p^2-1 = (p-1)(p+1)$ is divisible by 16. Similarly, in the latter case, $p+1$ is divisible by 7 and $p-1$ is even (i.e., divisible by 2), so $p^2-1 = (p-1)(p+1)$ is divisible by 16. In either case, p^2-1 is divisible by 16, so $\left(p^2-1\right)/8$ is even. Then

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = (-1)^{\text{even integer}} = 1,$$

which implies $x^2 \equiv 2 \pmod{p}$ has solutions. ∎

Remark 3. *Equivalently, this exercise shows that if p is an odd prime, then*

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{8} \text{ or } p \equiv 7 \pmod{8}, \\ -1 & \text{if } p \equiv 3 \pmod{8} \text{ or } p \equiv 5 \pmod{8}. \end{cases}$$

One can compare this with

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4}, \\ -1 & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

4 §3.1 #12

Problem (§3.1 #12)
Denote quadratic residues by r, nonresidues by n. Prove that $r_1 r_2$ and $n_1 n_2$ are residues and that rn is a nonresidue for any odd prime p. Give a numerical example to show that the product of two nonresidues is not necessarily a quadratic residue modulo 12.

Proof. Let p be an odd prime. If r_1 and r_2 are quadratic residues modulo p, then $\left(\frac{r_1}{p}\right) = 1 = \left(\frac{r_2}{p}\right)$. Therefore,

$$\left(\frac{r_1 r_2}{p}\right) = \left(\frac{r_1}{p}\right)\left(\frac{r_2}{p}\right) = 1 \cdot 1 = 1,$$

so $r_1 r_2$ is a quadratic residue modulo p. If n_1 and n_2 are quadratic nonresidues modulo p, then $\left(\frac{n_1}{p}\right) = -1 = \left(\frac{n_2}{p}\right)$. Therefore,

$$\left(\frac{n_1 n_2}{p}\right) = \left(\frac{n_1}{p}\right)\left(\frac{n_2}{p}\right) = -1 \cdot -1 = 1,$$

so $n_1 n_2$ is a quadratic residue modulo p. Moreover, rn is quadratic nonresidue modulo p since

$$\left(\frac{rn}{p}\right) = \left(\frac{r}{p}\right)\left(\frac{n}{p}\right) = 1 \cdot (-1) = -1.$$

The set of quadratic residues modulo 12 is

$$\{0, 1, 4, 9\}.$$

Now 2 and 3 are quadratic nonresidues modulo 12, and their product $6 = 2 \cdot 3$ is still a quadratic nonresidue modulo 12. ■

Remark 4. *This exercise uses the multiplicative property of Legendre symbols modulo an odd prime p. See Theorem 3.1(2).*

5 §3.1 #15

Problem (§3.1 #15)
Show that if p is a prime of the form $4k+1$ then the sum of the quadratic residues $\pmod p$ in the interval $[1, p)$ is $p(p-1)/4$.

Proof. Let p be a prime of the form $4k+1$. Then

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = (-1)^{4k} = 1,$$

so -1 is a quadratic residue modulo p. Thus, if a is a quadratic residue modulo p, then so is $-a$ because

$$\left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right) = 1 \cdot 1 = 1.$$

In other words, $p-a$ is also a quadratic residue modulo p if a is a quadratic residue modulo p. Let Q be the set of all quadratic residues modulo p. We count the number of distinct pairs $\{a, p-a\}$ where a is a quadratic residue modulo p. We first make the following claim.

Claim 5. *For an odd prime p, there are $(p-1)/2$ nonzero quadratic residues modulo p.*

Using Claim 5, there are $(p-1)/4$ distinct pairs of quadratic residues modulo p, and each pair sums to $a+(p-a) = p$. Thus the required sum is $p \cdot (p-1)/4 = p(p-1)/4$.

We now prove Claim 5

Proof of Claim 5. Note if $x^2 \equiv y^2 \pmod p$, then $p \mid (x-y)(x+y)$ implies $x \equiv y \pmod p$ or $x \equiv -y \pmod p$. Now for all $x \in \{1, \ldots, p-1\}$, $x \neq p-x$ because p is odd, so $\{x, p-x\}$ is a pair for all such x. Then $\{x, p-x\}$ yields the same quadratic residue modulo p, and each pair yields a unique quadratic residue modulo p. There are $(p-1)/2$ such pairs, so there are $(p-1)/2$ quadratic residues modulo p. ■

The proof is complete. ■

Remark 6. *Pairing arguments are common in number theory. (Recall the proof of Wilson's theorem.) Pairing quadratic residues is another example of this method.*

6 §3.1 #23

Problem (§3.1 #23)
Show that if p is an odd prime and $(a, p) = 1$, then $x^2 \equiv a \pmod{p^\alpha}$ has exactly $1 + \left(\frac{a}{p}\right)$ solutions.

Proof. Suppose p is an odd prime and let $(a, p) = 1$. Note that $a \neq 0$. Let $\alpha > 0$ be an integer.

First, suppose $\left(\frac{a}{p}\right) = -1$. By definition, the congruence $x^2 \equiv a \pmod{p}$ has no solutions. The $x^2 \equiv a \pmod{p^\alpha}$ has no solutions (i.e., $1 + \left(\frac{a}{p}\right) = 0$ solutions) as well since otherwise if x_0 is a solution, then $p \mid p^\alpha \mid \left(x_0^2 - a\right)$ implies that $x_0^2 \equiv a \pmod{p}$.

Then suppose $\left(\frac{a}{p}\right) = 1$. We show that the congruence

$$x^2 \equiv a \pmod{p^\alpha}$$

has $1 + \left(\frac{a}{p}\right) = 2$ solutions. The congruence $x^2 \equiv a \pmod{p}$ has two solutions by Claim 5, say x_1 and x_2. The roots x_1 and x_2 are both nonsingular, i.e., $2x_1 \not\equiv 0 \pmod{p}$ and $2x_2 \not\equiv 0 \pmod{p}$; otherwise, $p \mid 2x_1$ (resp. $p \mid 2x_2$), which is impossible since p is an odd prime and $(x_1, p) = (x_2, p) = 1$. By $\alpha - 1$ repeated applications of Hensel's lemma, x_1 and x_2 lift to $x_1^{(\alpha)}$ and $x_2^{(\alpha)}$, which are solutions to $x^2 \equiv a \pmod{p^\alpha}$. Importantly, in each iteration $k \in \{1, \ldots, \alpha - 1\}$, the solutions $x_1^{(k+1)}$ and $x_2^{(k+1)}$ do not coincide modulo p^{k+1}; otherwise,

$$x_1^{(k+1)} \equiv x_2^{(k+1)} \pmod{p^{k+1}}$$

implies $p \mid p^{k+1} \mid \left(x_1^{(k+1)} - x_2^{(k+1)}\right)$, so $x \equiv x_1^{(k+1)} \pmod{p} \equiv x_2^{(k+1)} \pmod{p} \equiv x_2 \pmod{p}$, contrary to x_1 and x_2 being two distinct solutions to $x^2 \equiv a \pmod{p}$. Therefore, $x_1^{(\alpha)}$ and $x_2^{(\alpha)}$ are the two and only two solutions of the congruence $x^2 \equiv a \pmod{p^\alpha}$, as required. ∎

7 §3.2 #6

Problem (§3.2 #6)
Decide whether $x^2 \equiv 150 \pmod{1009}$ is solvable or not.

Proof. Now $1009 \equiv 1 \pmod 8$, so Problem 3 (cf. §3.1 #10) implies

$$\left(\frac{2}{1009}\right) = 1.$$

We compute

$$\left(\frac{150}{1009}\right) = \left(\frac{2}{1009}\right)\left(\frac{3}{1009}\right)\left(\frac{25}{1009}\right) = \left(\frac{3}{1009}\right).$$

By quadratic reciprocity,

$$\left(\frac{3}{1009}\right) = (-1)^{(3-1)(1009-1)/4}\left(\frac{1009}{3}\right) = (-1)^{2\cdot 252}\left(\frac{1}{3}\right) = 1,$$

so $x^2 \equiv 150 \pmod{1009}$ is solvable (i.e., it has a solution). ∎

Remark 7. *The quadratic reciprocity law makes computation of the Legendre symbol fairly simple.*

Theorem (The Gaussian reciprocity law, Theorem 3.4)
If p and q are distinct odd primes, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\{(p-1)/2\}\{(q-1)/2\}}.$$

Remark 8. *An important consequence of quadratic reciprocity is the following: if p and q are distinct odd primes*

- *and are $\equiv 3 \pmod 4$, then one of $x^2 \equiv p \pmod q$ and $x^2 \equiv q \pmod p$ is solvable and the other is not;*
- *and at least one is $\equiv 1 \pmod 4$, then both are solvable or both are not.*

8 §3.2 #8

Problem (§3.2 #8)
Find all primes p such that $\left(\frac{10}{p}\right) = 1$.

Solution. By definition of the Legendre symbol, it suffices to consider odd p. The primes p are all of the form

$$p \equiv 3, 9, 23, 31, 35, 39 \pmod{40}.$$

Note that $1 = \left(\frac{10}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{5}{p}\right)$, so we find all primes p such that $\left(\frac{2}{p}\right) = 1 = \left(\frac{5}{p}\right)$ or $\left(\frac{2}{p}\right) = -1 = \left(\frac{5}{p}\right)$. By quadratic reciprocity and enumerating the quadratic residues modulo 5,

$$\begin{aligned}\left(\frac{5}{p}\right) &= (-1)^{(5-1)(p-1)/4}\left(\frac{p}{5}\right)\\ &= \left(\frac{p}{5}\right)\\ &= \begin{cases} 1 & \text{if } p \equiv 1 \pmod 5 \text{ or } p \equiv 4 \pmod 5,\\ -1 & \text{if } p \equiv 2 \pmod 5 \text{ or } p \equiv 3 \pmod 5.\end{cases}\end{aligned}$$

By Problem 3 (cf. §3.1 #10),

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 8 \text{ or } p \equiv 7 \pmod 8,\\ -1 & \text{if } p \equiv 3 \pmod 8 \text{ or } p \equiv 5 \pmod 8.\end{cases}$$

- In the former case, we solve the system

$$\begin{aligned} p &\equiv a \pmod 5,\\ p &\equiv b \pmod 8,\end{aligned}$$

  for $a \in \{1, 4\}$ and $b \in \{1, 7\}$. The Chinese remainder theorem gives

$$p \equiv 1, 31, 9, 39 \pmod{40}.$$

- In the latter case, we solve the system

$$\begin{aligned} p &\equiv a \pmod 5,\\ p &\equiv b \pmod 8,\end{aligned}$$

  for $a \in \{2, 3\}$ and $b \in \{3, 5\}$. The Chinese remainder theorem gives

$$p \equiv 27, 37, 3, 13 \pmod{40}.$$

The solution is complete. ■

9 §3.2 #9

Problem (§3.2 #9)
Find all primes q such that $\left(\frac{5}{q}\right) = -1$.

Solution. By definition of the Legendre symbol, it suffices to consider odd q. The primes q are all of the form

$$q \equiv 2, 3 \pmod 5 \quad \text{and} \quad q \neq 2.$$

By quadratic reciprocity and enumerating the quadratic residues modulo 5,

$$\begin{aligned}\left(\frac{5}{p}\right) &= (-1)^{(5-1)(p-1)/4}\left(\frac{p}{5}\right) \\ &= \left(\frac{p}{5}\right) \\ &= \begin{cases} 1 & \text{if } p \equiv 1 \pmod 5 \text{ or } p \equiv 4 \pmod 5, \\ -1 & \text{if } p \equiv 2 \pmod 5 \text{ or } p \equiv 3 \pmod 5. \end{cases}\end{aligned}$$

The exercise is complete. ■

10 §3.2 #11

Problem (§3.2 #11)
If a is a quadratic nonresidue of each of the odd primes p and q, is $x^2 \equiv a \pmod{pq}$ solvable?

Proof. Suppose that a is a quadratic nonresidue modulo p and q, where p and q are both odd. Suppose for the sake of contradiction that $x^2 \equiv a \pmod{pq}$ has a solution, say x_0. Hence, $p \mid pq \mid \left(x_0^2 - a\right)$, so x_0 is a solution to $x^2 \equiv a \pmod{p}$, contrary to the fact that a is a quadratic nonresidue modulo p. ■