18.781 Theory of Numbers

Problem Set 10

Official Solutions

May 12, 2026

Contents

Disclaimer

This document contains the official solutions to Problem Set 10 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 §5.3 #10

Problem (§5.3 #10)

Prove that $x^2 + y^2 = z^4$ has infinitely many solutions with $(x, y, z) = 1$.

Proof. The equation $x^2 + y^2 = \left(z^2\right)^2$ has infinitely many solutions with $(x, y, z) = 1$ if and only if there are infinitely many Pythagorean triples x, y, and z^2 with $(x, y, z) = 1$. This holds with the parametrization

$$\boxed{\begin{aligned} x &= \left(r^2 - s^2\right) - (2rs)^2, \\ y &= 2\left(r^2 - s^2\right)(2rs), \\ z &= r^2 + s^2, \end{aligned}}$$

for integers r and s of opposite parity such that $r > s > 0$ and $(r, s) = 1$. First,

$$x^2 + y^2 = \left(\left(r^2 - s^2\right) - (2rs)^2\right)^2 + \left(2\left(r^2 - s^2\right)(2rs)\right)^2 = \left(\left(r^2 - s^2\right) + (2rs)^2\right)^2 = \left(r^2 + s^2\right)^2 = z^2,$$

so there are infinitely many Pythagorean triples x, y, and z^2. In particular, from above we have $z^2 = \left(r^2 - s^2\right) + (2rs)^2$. We first show that $\left(r^2 - s^2, 2rs\right) = 1$. Suppose that there exists some prime p such that $p \mid \left(r^2 - s^2\right)$ and $p \mid 2rs$, so $p \mid \left(\left(r^2 - s^2\right)^2 + (2rs)^2\right) = \left(r^2 + s^2\right)^2$. Thus $p \mid \left(r^2 + s^2\right)$. Note that $r^2 + s^2$ is odd since r and s have opposite parity, so $p \neq 2$. Now $p \mid \left(\left(r^2 + s^2\right) + \left(r^2 - s^2\right)\right) = 2r^2$, so $p \mid r$. Similarly, we have $p \mid \left(\left(r^2 + s^2\right) - \left(r^2 - s^2\right)\right) = 2s^2$, so $p \mid s$. Thus $p \mid (r, s)$, contrary to $(r, s) = 1$. Since $\left(r^2 - s^2, 2rs\right) = 1$, by Theorem 5.5 the Pythagorean triple x, y, z^2 is primitive, i.e., $\left(x, y, z^2\right) = 1$. Therefore, we have $(x, y, z) = 1$. Otherwise, if there exists some prime p such that $p \mid (x, y, z)$, then $p \mid x$, $p \mid y$, and $p \mid z$. Then $p \mid z^2$ so $p \mid \left(x, y, z^2\right)$, contrary to $\left(x, y, z^2\right) = 1$. ■

Remark 1. *The parametrization is obtained by applying Theorem 5.5 twice. By this theorem, such Pythagorean triples* x, y, z^2 *are parametrized by* $x = m^2 - n^2$, $y = 2mn$, $z^2 = m^2 + n^2$ *for integers* m *and* n *of opposite parity such that* $m > n > 0$ *and* m, n, z *is a Pythagorean triple. But this latter condition is parametrizable as* $m = r^2 - s^2$, $n = 2rs$, *and* $z = r^2 + s^2$ *for integers* r *and* s *of opposite parity such that* $r > s > 0$.

Theorem (Theorem 5.5)

The positive primitive solutions of $x^2 + y^2 = z^2$ with y even are $x = r^2 - s^2$, $y = 2rs$, and $z = r^2 + s^2$, where r and s are arbitrary integers of opposite parity with $r > s > 0$ and $(r, s) = 1$.

2 §5.3 #11

Problem (§5.3 #11)

Using Theorem 5.5, determine all solutions of the equation $x^2 + y^2 = 2z^2$.

Proof. We classify all primitive solutions x, y, z, since any other solution kx, ky, kz is attained by scaling a primitive solution by some $k \in \mathbb{Z}$. Since $2z^2$ is even, so is $x^2 + y^2$. Thus, x and y have the same parity since otherwise $x^2 + y^2$ is odd. Moreover, x and y must be both odd; otherwise, if they are both even, then $4 \mid \left(x^2 + y^2\right)$, so $4 \mid 2z^2$. This means $2 \mid z^2$, so z is even, contrary to $(x, y, z) = 1$.

A triple of integers x, y, z is a solution to $x^2 + y^2 = 2z^2$ if and only if it is a solution to the equation $(x + y)^2 + (x - y)^2 = 2\left(x^2 + y^2\right) = 4z^2$ if and only if it is a solution to

$$\left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 = z^2.$$

Thus with $u = (x + y)/2$, $v = (x - y)/2$, we solve the latter, and u and v are well defined since $x - y$ and $x + y$ are both even. By Theorem 5.5, the positive primitive solutions are given by $u = r^2 - s^2$, $v = 2rs$, and $z = r^2 + s^2$ for integers r and s of opposite parity such that $r > s > 0$ and $(r, s) = 1$. Therefore,

$$u = \frac{x+y}{2} = r^2 - s^2, \qquad v = \frac{x-y}{2} = 2rs,$$

which gives

$$\begin{aligned} x &= r^2 + 2rs - s^2, \\ y &= r^2 - 2rs - s^2, \\ z &= r^2 + s^2. \end{aligned}$$

Suppose that there exists some prime p such that $p \mid x$, $p \mid y$, and $p \mid z$. Hence $p \mid (x + y) = 2\left(r^2 - s^2\right)$. But $p \neq 2$ since x and y are odd, so $p \mid \left(r^2 - s^2\right)$. Since $p \mid z = \left(r^2 + s^2\right)$, $p \mid \left(\left(r^2 + s^2\right) + \left(r^2 - s^2\right)\right) = 2r^2$, so $p \mid r$. Similarly, we have $p \mid \left(\left(r^2 + s^2\right) - \left(r^2 - s^2\right)\right) = 2s^2$, so $p \mid s$. Thus $p \mid (r, s)$, contrary to $(r, s) = 1$. Thus $(x, y, z) = 1$, and

$$\boxed{\begin{aligned} x &= k\left(r^2 + 2rs - s^2\right), \\ y &= k\left(r^2 - 2rs - s^2\right), \\ z &= k\left(r^2 + s^2\right), \end{aligned}}$$

are solutions to $x^2 + y^2 = 2z^2$, where $k, r, s \in \mathbb{Z}$ are such that r, s have opposite parity, $r > s > 0$, and $(r, s) = 1$. ■

3 §5.3 #12

Problem (§5.3 #12)

Show that if $x = \pm\left(r^2 - 5s^2\right)$, $y = 2rs$, and $z = r^2 + 5s^2$ then $x^2 + 5y^2 = z^2$. This equation has the solution $x = 2$, $y = 3$, $z = 7$. Show that this solution is not given by any rational values of r, s.

Proof. Suppose that $x = \pm\left(r^2 - 5s^2\right)$, $y = 2rs$, and $z = r^2 + 5s^2$. Then

$$x^2 + 5y^2 = \left(r^2 - 5s^2\right)^2 + 5(2rs)^2 = r^4 + 10r^2s^2 + 25s^4 = \left(r^2 + 5s^2\right)^2 = z^2.$$

To show that the solution $x = 2$, $y = 3$, and $z = 7$ is not given by any rational values of r and s, we solve

$$\begin{aligned} 3 &= 2rs, \\ 7 &= r^2 + 5s^2, \end{aligned}$$

which gives solutions

$$(r,s) = \left(\frac{3}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right), \qquad (r,s) = \left(-\frac{3}{\sqrt{2}}, -\frac{1}{\sqrt{2}}\right),$$

$$(r,s) = \left(\sqrt{\frac{5}{2}}, \frac{3}{\sqrt{10}}\right), \qquad (r,s) = \left(-\sqrt{\frac{5}{2}}, -\frac{3}{\sqrt{10}}\right),$$

which are not rational. ∎

4 §5.6 #6

Problem (§5.6 #6)

Show that the curve $y^2 = x^3 - 3x - 2$ has an isolated double point. Use this double point to parametrize all rational points on the curve.

Proof. Let $f(x, y) = y^2 - x^3 + 3x + 2$, and define the notation

$$\Delta_{i,j}(x, y) = \frac{\partial^{i+j} f}{\partial x^i \partial y^j}(x, y).$$

A point $\mathbf{P} = (x_0, y_0)$ on the curve $\mathscr{C}_f(\mathbb{R})$ is a double point if and only if $\Delta_{i,j}\mathbf{P} = 0$ whenever $i + j < 2$. Therefore,

- $\Delta_{1,0}\mathbf{P} = \big(\partial f/\partial x\big)\mathbf{P} = 0$, i.e., $-3x_0^2 + 3 = 0$;
- $\Delta_{0,1}\mathbf{P} = \big(\partial f/\partial y\big)\mathbf{P} = 0$, i.e., $2y = 0$; and
- $\Delta_{0,0}\mathbf{P} = f\mathbf{P} = 0$, i.e., $y_0^2 - x_0^3 + 3x_0 + 2 = 0$.

The first and second condition imply that $x_0 = \pm 1$ and $y = 0$, respectively, and the third condition forces $x_0 = -1$, so $\mathbf{P} = (-1, 0)$ is the only double point. We set

$$p(x) = f(x, m(x+1)) = 2 + 3x - x^3 + m^2(x+1)^2.$$

Since $x_0 = -1$ is a double root of $p(x)$ and the sum of all three roots is m^2, the third root is $x_1 = m^2 + 2$. Therefore, $y_1 = m(x_1 + 1) = m^3 + 3m$, so the equations

$$\boxed{\begin{aligned} x &= m^2 + 2, \\ y &= m^3 + 3m, \\ m &= \frac{y}{x+1}, \end{aligned}}$$

determine a one-to-one correspondence between rational points (x, y) on the curve $\mathscr{C}_f(\mathbb{R})$ and m rational. ■

5 §5.6 #9

Problem (§5.6 #9)
The cubic curve $x^3+y^3=1$ contains the two rational points $(0,1)$ and $(1,0)$. Explain why the chord-and-tangent method does not yield any further points on this curve.

Proof. Let $f(x,y)=x^3+y^3-1$. The chord L passing through $(0,1)$ and $(1,0)$ has equation $y=-x+1$. Therefore, the intersection of this chord L with the curve $\mathscr{C}_f(\mathbb{R})$ gives the relation $x^3+(-x+1)^3-1=0$, or equivalently

$$x(x-1)=0.$$

This has solutions $(x,y)=(0,1)$ and $(x,y)=(1,0)$ again, i.e., the chord L meets $\mathscr{C}_f(\mathbb{R})$ at only these two points. ■

Remark 2. *We expect to find three points of intersection of L and $\mathscr{C}_f(\mathbb{R})$, counting multiplicity, because f has degree 3. This third point is located at the point at infinity. To find the third point of this intersection, consider the homogeneous polynomial $F(X,Y,Z)=X^3+Y^3-Z^3$ so that the affine points of $f(x,y)$ correspond precisely to when $Z=1$. The chord L has equation $X+Y=Z$ in projective space, and the intersection of $F(X,Y,Z)=0$ and $X+Y=Z$ becomes $X^3+Y^3=(X+Y)^3$, or equivalently $3XY(X+Y)=0$. The cases where $X=0$ and the $Y=0$ translate to affine points as before, but the case where $Z=X+Y=0$ is the point at infinity $(X:Y:Z)=(1:-1:0)$.*

6 §5.6 #14

Problem (§5.6 #14)
Apply the tangent method to the curve $x^3+y^3=7$, and thus construct a recurrence that gives a new solution of the equation $X^3+Y^3=7Z^3$ from a known one. Starting from the triple $(2,-1,1)$, show that this generates infinitely many distinct rational points on the curve $x^3+y^3=7$.

Proof. Let $f(x,y)=x^3+y^3-7$. Then $\partial f/\partial x=3x^2$ and $\partial f/\partial y=3y^2$. Suppose $(a,b)\in\mathscr{C}_f(\mathbb{Q})$ (i.e., (a,b) is a rational point of f). Then $f(a,b)=0$, and the tangent line of f at (a,b) is

$$0=\frac{\partial f}{\partial x}(a,b)(x-a)+\frac{\partial f}{\partial y}(a,b)(y-b)=3a^2(x-a)+3b^2(y-b)=3\left(a^2x+b^2y-\left(a^3+b^3\right)\right)=3\left(a^2x+b^2y-7\right).$$

The intersection of this line with the curve $\mathscr{C}_f(\mathbb{R})$ gives the relation $x^3+\left(\left(7-a^2x\right)/b^2\right)^3=7$, or equivalently,

$$(x-a)^2\left(\left(7-2a^3\right)x+14a-a^4\right).$$

The third point is thus $x=a\left(a^3+2b^2\right)/\left(a^3-b^3\right)$ which with $y=\left(7-a^2x\right)/b^2$ gives

$$x=\frac{a\left(a^3+2b^2\right)}{\left(a^3-b^3\right)}\quad\text{and}\quad y=-\frac{b\left(2a^3+b^3\right)}{\left(a^3-b^3\right)}. \tag{1}$$

Suppose that (X_n,Y_n,Z_n) is an integer solution of $X^3+Y^3=7Z^3$, where $Z_n\neq 0$, so that $(a,b)=(X_n/Z_n,Y_n/Z_n)\in\mathscr{C}_f(\mathbb{Q})$. Then (1) gives another rational point $(X_{n+1}/Z_{n+1},Y_{n+1}/Z_{n+1})$ such that

$$\begin{aligned}
\frac{X_{n+1}}{Z_{n+1}}&=\frac{(X_n/Z_n)\Big((X_n/Z_n)^3+2(Y_n/Z_n)^2\Big)}{(X_n/Z_n)^3-(Y_n/Z_n)^3}=\frac{X_n\left(X_n^3+2Y_n^3\right)}{Z_n\left(X_n^3-Y_n^3\right)},\\
\frac{Y_{n+1}}{Z_{n+1}}&=-\frac{(Y_n/Z_n)\Big(2(X_n/Z_n)^3+(Y_n/Z_n)^3\Big)}{(X_n/Z_n)^3-(Y_n/Z_n)^3}=-\frac{Y_n\left(2X_n^3+Y_n^3\right)}{Z_n\left(X_n^3-Y_n^3\right)},
\end{aligned}$$

Then the recurrences defined by

$$\begin{aligned}
X_{n+1}&=X_n\left(X_n^3+2Y_n^3\right),\\
Y_{n+1}&=-Y_n\left(2X_n^3+Y_n^3\right),\\
Z_{n+1}&=Z_n\left(X_{n-1}^3-Y_{n-1}^3\right),
\end{aligned}$$

is another solution to $X^3+Y^3=7Z^3$. Starting from $(X_0,Y_0,Z_0)=(2,-1,1)$, the recurrences

$$\boxed{\begin{aligned}
X_n&=\begin{cases}X_{n-1}\left(X_{n-1}^3+2Y_{n-1}^3\right) & \text{if } n\geq 1,\\ 2 & \text{if } n=0,\end{cases}\\
Y_n&=\begin{cases}-Y_{n-1}\left(2X_{n-1}^3+Y_{n-1}^3\right) & \text{if } n\geq 1,\\ -1 & \text{if } n=0,\end{cases}\\
Z_n&=\begin{cases}Z_{n-1}\left(X_{n-1}^3-Y_{n-1}^3\right) & \text{if } n\geq 1,\\ 1 & \text{if } n=0,\end{cases}
\end{aligned}}$$

give rational points $(X_n/Z_n, Y_n/Z_n)$ of f for all integers $n \geq 0$, provided that $Z_n \neq 0$. We show that this is the case and then prove that there are infinitely many distinct rational points on $\mathscr{C}_f(\mathbb{R})$. First, since $X_{n-1} \mid X_n$ for all integers $n \geq 1$ and $X_0 = 2$, we have

$$X_n \equiv 0 \pmod 2$$

for all integers $n \geq 0$. Similarly, since Y_0 and Z_n are odd, by induction we obtain

$$\begin{aligned} Y_n &\equiv 1 \pmod 2, \\ Z_n &\equiv 1 \pmod 2, \end{aligned}$$

for all integers $n \geq 0$. Then $X_n^3 + 2Y_n^3 \equiv 2 \pmod 4$ for all integers $n \geq 0$. Since

$$X_{n+1} = X_n \left(X_n^3 + 2Y_n^3\right) \equiv 2X_n \pmod 4,$$

the power of 2 in X_{n+1} is one more than the power of 2 in X_n. Thus $2^{n+1} \parallel X_n$. Since Z_n is always odd and thus does not share a factor of 2 with X_n and $2 \mid X_{n+1}/X_n$, we have $X_{n+1}/Z_{n+1} \neq X_n/Z_n$ for all integers $n \geq 0$. Hence, there are infinitely many distinct rational points. ∎

Remark 3. *The proof of this is similar to that of Theorem 5.16. One can show that for a general form of $x^3 + y^3 = c$, where $c \neq 0$ is a constant, that we must have the recurrences*

$$\boxed{\begin{aligned} X_n &= X_{n-1}\left(X_{n-1}^3 + 2Y_{n-1}^3\right), \\ Y_n &= -Y_{n-1}\left(2X_{n-1}^3 + Y_{n-1}^3\right), \\ Z_n &= Z_{n-1}\left(X_{n-1}^3 - Y_{n-1}^3\right), \end{aligned}}$$

for integers $n \geq 1$, with initial conditions (X_0, Y_0, Z_0) such that $X_0^3 + Y_0^3 = cZ_0^3$.

Theorem (Theorem 5.16)
The cubic curve $x^3 + y^3 = 9$ contains infinitely many rational points.