Problems IV

1. Prove that if an integer \( n \) is the sum of two squares, then \( n = 4q \) or \( n = 4q + 1 \) or \( n = 4q + 2 \) for some \( q \in \mathbb{Z} \). Deduce that 1234567 cannot be written as the sum of two squares.

**Solution:** Let \( n = a^2 + b^2 \) for \( a, b \in \mathbb{Z} \). By problem 15.5, we know that \( a^2 \) has a remainder of 1 or 0 modulo 4, and the same holds for \( b^2 \). Thus we have that

\[
n = 4m + 4k \\
= 4(m + k)
\]

or

\[
n = 4m + 1 + 4k \\
= 4(m + k) + 1
\]

or

\[
n = 4m + 1 + 4k + 1 \\
= 4(m + k) + 2
\]

In any event, we get our result by setting \( q = m + k \), which is certainly an integer. Now, since 1234567 = \( 4 \cdot 308641 + 3 \), we conclude that 1234567 cannot be written as a sum of two squares.

2. Let \( a \) be an integer. Prove that \( a^2 \) is divisible by 5 if and only if \( a \) is divisible by 5.

**Solution:** One direction scarce requires explanation: if 5 divides \( a \), then 5 divides any multiple of \( a \); in particular it divides \( a^2 \). So assume 5 divides \( a^2 \). We know that \( a = 5q + r \), where \( q, r \in \mathbb{Z} \) and \( r = 0, 1, 2, 3 \) or 4. This means that

\[
a^2 = (5q + r)^2 \\
= 25q^2 + 10r + r^2
\]
and since 5 divides $a^2$, it must divide $r^2 = a^2 - 25q^2 + 10r$ as well. Looking at the possible values of $r^2$ (0, 1, 4, 9, and 15), we see that $r^2$ must be 0, which forces $r = 0$. Thus $a$ is indeed divisible by 5.

3. Use the result of Question 2 to prove that there does not exist a rational number whose square is 5.

Solution: Suppose that $x$ is a rational square root of 5. By cancelling any common factors, we can write $x$ as $\frac{a}{b}$, where $a$ and $b$ are coprime integers (with $b \neq 0$). From the equation

$$\left(\frac{a}{b}\right)^2 = 5$$

we get that

$$a^2 = 5b^2$$

This means 5 divides $a^2$, and the previous problem shows that 5 divides $a$ as well. Writing $a = 5k$ for $k \in \mathbb{Z}$, we thus have

$$25k^2 = 5b^2$$

which we can divide to get

$$5k^2 = b^2$$

As before, this implies 5 divides $b$, contradicting $(a, b) = 1$. Therefore, no rational number can square to 5.

4. Prove there is no rational number whose square is 98.

Solution: Notice first that $98 = 7^2 \cdot 2$, so if $x^2 = 98$, then $(\frac{x}{7})^2 = 2$. The same reasoning applies if we start with a rational square root of 2, so (using that multiplying and dividing by an integer preserves rationality) we see that 98 has a rational square root if and only if 2 has a rational square root. Also, using the division theorem and the same reasoning as in problem 2, one can show that for any integer $a$, 2 divides $a$ if and only if 2 divides $a^2$. Thus we can use the exact same argument as in problem 3 (replacing 5 with 2 where necessary) to conclude that 2 has no rational root, which in turn means that 98 does not have one either.

6. Use the Euclidean algorithm to find the greatest common divisors of (i) 165 and 252, (ii) 4282 and 3480

(i) Solution: We have

$$252 = 165 + 87$$
$$165 = 87 + 78$$
$$87 = 78 + 9$$
$$78 = 8 \cdot 9 + 6$$
$$9 = 6 + 3$$
$$6 = 2 \cdot 3$$
so \((252, 165) = 3\).

(ii) **Solution:**

\[
\begin{align*}
4284 &= 3480 + 804 \\
3480 &= 4 \cdot 804 + 264 \\
804 &= 3 \cdot 264 + 12 \\
264 &= 22 \cdot 12
\end{align*}
\]

so \((4284, 3480) = 12\).

15. Solve the linear diophantine equations

(i) \(165m + 252n = 15\)

**Solution:** Tracing back through the equations in the Euclidean algorithm from the previous problem, we can write 3 as

\[
3 = 9 - 6 \\
= 9 - (78 - 8 \cdot 9) \\
= 9 \cdot (87 - 78) - 78 \\
= 9 \cdot 87 - 10 \cdot (165 - 87) \\
= 19 \cdot (252 - 165) - 10 \cdot 165 \\
= 252 \cdot 19 - 165 \cdot 29
\]

so \(165 \cdot (-145)252 \cdot 95 = 15\). The methods of chapter 18 then yield the general solution to \(165m + 252n = 15\): \(m = -145 + \frac{252}{3}q = -145 + 84q\), and \(n = 95 - \frac{165}{3}q = 95 - 55q\), for \(q \in \mathbb{Z}\).

(ii) \(165m + 252n = 20\)

**Solution:** Since 3 does not divide 20, there are no solutions.

(iii) \(4284m + 3480n = 60\)

**Solution:** Using the previous problem again, we get that \(12 = 4284 \cdot 13 + 3480 \cdot (-16)\), so a particular solution is \(4284 \cdot 65 + 3480 \cdot (-80)\). The general solution is then \(m = 65 - 290q\), \(n = -80 + 357q\), for \(q \in \mathbb{Z}\).

(iv) \(4284m - 3480n = 36\)

**Solution:** By the same method as part (iii), we get the particular solution \(m_0 = 39, n_0 = 48\). The same argument as in the previous parts, modified so that the signs work out, yields the general solution \(m = 39 - 290q, n = 48 - 357q \ (q \in \mathbb{Z})\).
16. Solve the linear diophantine equation

\[ 336m + 238n = 5558 \]

Prove that there is a unique pair of positive integers \( m \) and \( n \) satisfying this equation and find this solution.

**Solution:** One can show that \((336, 238) = 14\), and that \[336 \cdot 1985 + 238 \cdot (-2779) = 5558.\] This means that any solution to \(336m + 238n = 5558\) is of the form \(m = 1985 - 17q, n = -2779 + 24q\) for some \(q \in \mathbb{Z}\). Note that in order for \(m\) and \(n\) to be positive, we must have \(0 < 336m \leq 5558\), since if it’s larger, the only way to make the sum smaller so that it can add up to 5558 is to add a negative multiple of 238. We plug \(m = 1985 - 17q\) into the first inequality to get \(0 < 1985 - 17q\), which means \(q \leq \frac{1985}{17}\). On the other hand, \(336(1985 - q) \leq 5558\) implies that \(1985 - 17q \leq 14\), or \(\frac{1971}{17} \leq q\). The only integer between \(\frac{1971}{17}\) and \(\frac{1985}{17}\) is 116, so this is the only value of \(q\) possible. We can check that setting \(q = 116\) yields \(m = 13, n = 5\), which therefore must be the unique solution with \(m\) and \(n\) both positive.

17. Find all positive integers which satisfy the diophantine equation

\[ 12563m + 6052n = 9922169 \]

**Solution:** By the same process as in the previous problem, we find that the only positive solutions are \(m = 191, n = 1243\) and \(m = 547, n = 504\).