Sec 2.3, p71: 30
*Show that if \( n \equiv 7 \mod 8 \), then \( n \) is not the sum of 3 squares.

**Answer.** If \( x \) is odd, we have shown that \( x^2 \equiv 1 \mod 8 \), while for even \( x \), we have \( x^2 \equiv 0 \mod 8 \) or \( x^2 \equiv 4 \mod 8 \). Thus, if we compute the possibilities for the sum of three squares mod 8, we get the possibilities \((0, 1, or 4) + (0, 1, or 4) + (0, 1, or 4) \mod 8 \). Thus, the only possibilities are 0,1,2, 3, 4, 5, 6 mod 8. Therefore, there is no way to get 7 mod 8 as the sum of three squares.

* How many final 0’s in the decimal expansion of 1,000! For example, the number 1,006,500 has 2 final 0’s.

**Answer.** The number is the highest power of 10 dividing 1,000!. This is the same as the highest power of 5 dividing 1,000!, since there are more factors of 2 than of 5. The required answer is therefore

\[
[1000/5] + [1000/5^2] + \ldots = 200 + 40 + 8 + 1 = 249
\]

Sec. 5.3, p 233/1, *2, 6, *10

**Answer.** 2. We have \( x = r^2 - s^2 \), \( y = 2rs \), \( z = r^2 + s^2 \). for a primitive triple. if \( r \) or \( s \equiv 0 \mod 3 \), then \( 3 \mid y \). If not, we have \( r \) and \( s \equiv \pm 1 \mod 3 \), Therefore \( r^2 \) and \( s^2 \equiv 1 \mod 3 \).

Thus \( x \equiv 1 - 1 = 0 \mod 3 \) giving the result. The analysis for 5 is similar. Here, if \( r \) or \( s \) is divisible by 5, then \( y \) will be. If not, \( r \) and \( s \equiv \pm 1 \) or \( \pm 2 \mod 5 \). So \( r^2 \) and \( s^2 \equiv 1 \) or 4 mod 5. The four possibilities for \((r^2, s^2)\) are \((1,1)\), \((1,4)\), \((4,1)\), and \((4,4)\). \( r^2 + s^2 \equiv 0 \mod 5 \) in cases 2 and 3, while \( r^2 - s^2 \equiv 0 \mod 5 \) in cases 1 and 4. In any case, one of \( x \) and \( z \) is divisible by 5. Note: if \((x, y, z)\) is not primitive, then it is a multiple of a primitive triple, so the result holds here too.

**Answer.** 10. If \( x^2 + y^2 = z^4 \), with any two of \( x, y, z \) relatively prime. Then \((x, y, z^2)\) is a primitive Pythagorean triple. So for some \((r, s)\), we have \( x = r^2 - s^2 \), \( y = 2rs \), \( z^2 = r^2 + s^2 \).

This makes \((r,s,z)\) a Pythagorean triple. We know that there are infinitely many solutions for \( z^2 = r^2 + s^2 \). Using any \((r,s)\) so found, we use it to find a solution to the given equation. Therefore there are infinitely many solution to the given equation. If \( r \) and \( s \) have different parities, and are relatively prime, then we know that \((x, y, z^2) = 1 \). So \((x, y, z) = 1 \)

*In \( \mathbb{Z}_p \), the order of an element \( a \neq 0 \) is the least positive integer \( n \) such that \( a^n = 1 \). Show that in \( \mathbb{Z}_{11} \), the order of any element is a divisor of 10. (Hint: Use Fermat’s little theorem for this.) List all the elements of \( \mathbb{Z}_{11} \) and compute the order of each of them.

**Answer.** If \( e \) is the order of \( a \), then \( a^e \equiv 1 \mod 11 \). We also know that \( a^{10} \equiv 1 \mod 11 \).
Now we divide 10 by \(e\) to get a remainder \(r\): \(10 = eq + r\) with \(0 \leq r < e\). Therefore

\[
1 \equiv a^{10} = a^{eq+r} = (a^e)^q a^r \equiv 1^q a^r \equiv a^r \mod 11.
\]

Since \(r < e\) and \(e\) was the least positive number such that \(a^e \equiv 1\mod 11\), \(r\) cannot be positive. Since \(0 \leq r\) is follows that \(r = 0\) and \(e|10\).

For the second part, we list all the non-zero elements of \(\mathbb{Z}_{11}\) with their orders. We know that the orders can be 1, 2, 5, or 10. 1 has order 1, and \(-1\) has order 2, since the only solutions of \(x^2 = 1\) in \(\mathbb{Z}_{11}\) are \(\pm1\). The following table gives the elements and their orders. Note that if \(a\) has order 5, then \(-a\) must have order 10. Note also that any square cannot have order 10, since its fifth power is 1. This simplifies the computation whose result is given in the following table.

<table>
<thead>
<tr>
<th>(a)</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Order of (a)</td>
<td>1</td>
<td>10</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>5</td>
<td>2</td>
</tr>
</tbody>
</table>