Section 3.2, problem 17.

Note that if 7 does not divide \(a\) then the congruence
\[
19a^2 \equiv b^2 \pmod{7}
\]
gives that 19 is a square mod 7 which is false. Therefore we must have \(7|a\) which implies that \(7|b\). It follows that \(7^2|a^2\) and \(7^2|b^2\) so in particular
\[
19a^2 \equiv b^2 \pmod{7^2}.
\]

Section 3.2, problem 20.

Note that \(2y^2 + 3\) is congruent to 3 modulo 8 if \(y\) is even, and congruent to 5 modulo 8 if \(y\) is odd. Therefore there exists a prime \(p\) which is congruent to \(\pm 3\) modulo 8 dividing \(2y^2 + 3\). On the other hand, if \((x^2 - 2)/(2y^2 + 3)\) is an integer then this prime must also divide \(x^2 - 2\). This gives that 2 is a square modulo \(p\) which is a contradiction since then we must have \(p \equiv \pm 1 \pmod{8}\).

Section 3.2: problem 22.

We are trying to count the number of solutions to the congruence
\[
ax^2 + by^2 \equiv 1 \pmod{p},
\]
where \(a\) and \(b\) are relatively prime to \(p\). For this note that for any given value \(x\) the number of \(y\)'s such that \((x, y)\) is a solution to the congruence is equal to
\[
1 + \left(\frac{b}{p}\right) \left(\frac{1 - ax^2}{p}\right).
\]
Note that this includes the case when \(1 - ax^2 \equiv 0 \pmod{p}\) since in this case there is exactly one choice of \(y\) giving a solution. Therefore the number of solutions to equation 1.2 is given by
\[
\sum_{x=0}^{p-1} \left(1 + \left(\frac{b}{p}\right) \left(\frac{1 - ax^2}{p}\right)\right) = p + \left(\frac{b}{p}\right) \sum_{x=0}^{p-1} \left(\frac{1 - ax^2}{p}\right).
\]
On the other hand if \(a'\) denotes a number such that \(aa' \equiv 1 \pmod{p}\) then we have
\[
1 - ax^2 \equiv (-a)(x^2 - a') \pmod{p}
\]
so
\[
\left(\frac{1 - ax^2}{p}\right) = \left(\frac{-a}{p}\right) \left(\frac{x^2 - a'}{p}\right).
\]
From this we conclude that we can rewrite the count in equation 1.3 as

\[ p + \left( \frac{-ab}{p} \right) \sum_{x=0}^{p-1} \left( \frac{x^2 - a'}{p} \right). \]

To prove that the number of solutions to equation 1.2 is equal to

\[ p - \left( \frac{-ab}{p} \right) \]

it therefore suffices to show that

\[ \sum_{x=0}^{p-1} \left( \frac{x^2 - a'}{p} \right) = -1. \]

This we do as follows. Note that by a similar reasoning to the above, the number of solutions to the equation

(1.3) \[ x^2 - y^2 \equiv a' \pmod{p} \]

is equal to

\[ p + \sum_{x=0}^{p-1} \left( \frac{x^2 - a'}{p} \right). \]

Therefore it suffices to show that the number of solutions to equation 1.4 is \( p - 1 \). This we can do as follows. Set

\[ u = x - y, \quad v = x + y. \]

Note that since \( p \) is odd, there exists an integer \( 2' \) such that \( 22' \equiv 1 \pmod{p} \). From this we get that

\[ x = 2'(u + v), \quad y = 2'(v - u). \]

We therefore get a bijection between the set of solutions to equation 1.4 and the set of solutions to

(1.4) \[ uv \equiv a' \pmod{p}. \]

But this last equation clearly has \( p - 1 \) solutions, since for any \( u \) not divisible by \( p \) there exists a unique \( v \) such that \( uv \equiv a' \pmod{p} \).