1. (Davenport, p.220, ex. 3.16) Assume that \(4k + 1\) and \(8k + 3\) are both primes. Then \(2^{8k+2} \equiv 1 \mod 8k + 3\) by Fermat’s little theorem. But \(8k + 2 = 2(4k + 1)\). Since \(4k + 1\) is prime, it suffices to show that \(2^{4k+1} \not\equiv 1 \mod 8k + 3\) in order to show that the order of 2 is \(8k + 2\) (notice that we used Lagrange’s theorem). Indeed, since \((\frac{2}{8k+3}) = (-1)^{\frac{(8k+3)^2-1}{8}} = -1\), we deduce that 2 is a quadratic nonresidue mod \(8k + 3\). Thus we cannot have \(2^{4k+1} \equiv 1 \mod 8k + 3\) because otherwise, if we multiply both sides with 2, then we get \(2^{4k+2} \equiv 2 \mod 8k + 3\), which would imply that 2 is a quadratic residue, a contradiction.

2. (Davenport, p.220, ex. 3.17) This time assume that \(4k\). We will find all \(p\). We will find a congruence describing all primes for which 5 is a quadratic residue. In other words, we aim to characterize all primes \(p\) such that \((\frac{5}{p}) = 1\). This follows from quadratic reciprocity because \(\frac{5}{p}\) is indeed a prime. We first claim that all primes \(p\) with \((\frac{5}{p}) = 1\) mod \(4\). By the law of quadratic reciprocity \((\frac{5}{p}) = (\frac{p}{5})\) when 5 \(\equiv 1 \mod 4\) in using the law of quadratic reciprocity, and the congruences 769 \(\equiv 1 \mod 3\) and 769 \(\equiv 4 \mod 5\) in evaluating the Legendre symbols at the end.

3. Recall that Pepin’s test tells the following: \(F_m = 2^{2m} + 1\) is prime if and only if \(3^{(F_m-1)/2} \equiv 1 \mod F_m\). You should use a calculator to check that the congruences \(3^{(F_3-1)/2} \equiv 1 \mod F_3\) and \(3^{(F_4-1)/2} \equiv 1 \mod F_4\) hold.

4. We will show that 3 is a primitive root of every Fermat prime. Let \(F_m\) is a Fermat prime. Then, by Pepin’s test, \(3^{2^{m-1}} \equiv 1 \mod F_m\). Suppose, for a contradiction that 3 is not a primitive root mod \(F_m = 2^{2m} + 1\). Then, since \(\varphi(F_m) = 2^{2m}\), we must have \(3^{2^d} \equiv 1 \mod F_m\) for some \(d \in \{1, 2, \ldots, 2^m - 1\}\). But then taking to the power \(2^{2m-1-d}\) of both sides (notice that taking to the power \(2^{m-1-d}\) makes sense since it is \(\geq 1\)) we get \(3^{2^d} \equiv 1 \mod F_m\), a contradiction.

5. We will find a congruence describing all primes for which 5 is a quadratic residue. In other words, we aim to characterize all primes \(p\) with \((\frac{5}{p}) = 1\). By the law of quadratic reciprocity \((\frac{5}{p}) = (\frac{p}{5})\) since 5 \(\equiv 1 \mod 4\). So, \(p\) should be a quadratic residue mod 5. So \(p\) must be congruent to either 1 or 4 mod 5.

6. Let \(p = 1 + 8 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23\). Using a number theory/arithmetic software like pari, it can be checked that \(p\) is indeed a prime. We first claim that all primes \(q\) with \(q < 24\) are quadratic residues mod \(p\). This follows from quadratic reciprocity because \((\frac{5}{q}) = (\frac{q}{5}) = (\frac{-1}{q}) (\frac{5}{q}) = (\frac{-1}{q}) (\frac{9}{q}) = (\frac{-1}{q}) (\frac{2}{q}) (\frac{3}{q}) = (\frac{-1}{q}) (\frac{2}{q}) (\frac{3}{q}) = 1 \cdot 1 \cdot 1 = 1\). So, all such \(q\)’s are quadratic residues. Observe that if \(m < 29\), then \(m\) is a product of such primes \(q\). Since product of quadratic residues is again a quadratic residue, we deduce that \(m\) must be a quadratic residue, too. Moreover, since any quadratic residue is a square of some primitive root, we conclude that none of these \(m\)’s can be a primitive root (a square of a primitive root cannot be a primitive root).

7. The Jacobi symbol \((\frac{1009}{2307}) = (\frac{1009}{3}) (\frac{1009}{709}) = (\frac{1}{3}) (\frac{240}{709}) = 1 \cdot (\frac{2^4}{709}) (\frac{3}{709}) (\frac{5}{709}) = (\frac{769}{3}) (\frac{769}{7}) = (\frac{1}{3}) (\frac{4}{7}) = 1 \cdot 1 = 1\). Note that we used the congruence 769 \(\equiv 1 \mod 4\) in using the law of quadratic reciprocity, and the congruences 769 \(\equiv 1 \mod 3\) and 769 \(\equiv 4 \mod 5\) in evaluating the Legendre symbols at the end.

8. We will find all \(n\)’s such that \((n, 15) = 1\) and \((\frac{15}{n})\) is 1. If \(n = 2\), then obviously \((\frac{15}{2}) = 1\). Now assume
\( n \) is odd. By the reciprocity law for the Jacobi symbol, we get \( \left( \frac{15}{n} \right) \left( \frac{n}{15} \right) = (-1)^{\frac{n-1}{2}} \frac{n-1}{2} = (-1)^{\frac{n-1}{2}}. \)

Thus \( \left( \frac{15}{n} \right) = \left( \frac{n}{15} \right) = (-1)^{\frac{n-1}{2}} \left( \frac{n}{3} \right) \left( \frac{n}{5} \right). \) So we have a product of three things. To get 1, either all of them must be 1, or exactly one of them must be 1 (and the others are -1). So there are 4 cases

**Case 1:** \( 1 \cdot 1 \cdot 1 \): In this case we have \( n \equiv 1 \mod 4, n \equiv 1 \mod 3, n \equiv 1 \text{ or } 4 \mod 5. \) Combining these using Chinese remainder theorem (since 3,4,5 are mutually coprime), we get \( n \equiv 1 \text{ or } 49 \mod 60. \)

**Case 2:** \( 1 \cdot (-1) \cdot (-1) \): In this case we have \( n \equiv 1 \mod 4, n \equiv 2 \mod 3, n \equiv 2 \text{ or } 3 \mod 5. \) Combining these using Chinese remainder theorem, we get \( n \equiv 17 \text{ or } 53 \mod 60. \)

**Case 3:** \( (-1) \cdot (-1) \cdot 1 \): In this case we have \( n \equiv 3 \mod 4, n \equiv 2 \mod 3, n \equiv 1 \text{ or } 4 \mod 5. \) Combining these using Chinese remainder theorem, we get \( n \equiv 11 \text{ or } 59 \mod 60. \)

**Case 4:** \( (-1) \cdot 1 \cdot (-1) \): In this case we have \( n \equiv 3 \mod 4, n \equiv 1 \mod 3, n \equiv 2 \text{ or } 3 \mod 5. \) Combining these using Chinese remainder theorem, we get \( n \equiv 7 \text{ or } 43 \mod 60. \)

So, any \( n \) that satisfies \( n \equiv 1, 7, 11, 17, 43, 49, 53, 59 \mod 60 \) will satisfy \( \left( \frac{15}{n} \right) = 1. \)

Now, in general, given \( m \) coprime to 15, write \( m = 2^a n \) where \( n \) is odd. Now, since \( \left( \frac{15}{2} \right) = 1, \) the \( \left( \frac{15}{m} \right) = \left( \frac{15}{n} \right). \) This characterizes all such \( m \) with \( \left( \frac{15}{m} \right) = 1. \)

9. By successive squaring, it is easy (but tedious) to see that \( 11^{864} \equiv 1 \mod 1729. \) Further, \( \left( \frac{11}{1729} \right) = \left( \frac{1729}{11} \right) (-1)^{\frac{n-1}{2}} \frac{1729-1}{2} = \left( \frac{1729}{11} \right) = \left( \frac{2}{11} \right) = (-1)^{\frac{n-1}{2}} = -1. \)

10. Suppose \( p \) is a prime \( > 5 \) and \( p = a^2 + 5b^2 \) for some \( a,b. \) Then, taking mod 5, we see that \( p \equiv 1 \text{ or } 4 \mod 5 \) (because these are the quadratic residues). Similarly, taking mod 4 gives us \( p \equiv 1 \mod 4 \) (note that \( p \) is a prime, so it cannot be congruent to 0 or 2 mod 4). These two congruences now imply that \( p \) is congruent to 1 or 9 mod 20 (again note that \( p \) is prime, so it cannot be congruent to some \( k \in \{1, 2, \ldots, 19\} \) with \( (k, 20) \neq 1. \)