Geoffrey Thomas
18.781 pset 6
Collaborators: Liz Denys

3-2 6. Yes, because

$$\left(\frac{150}{1009}\right) = \left(\frac{25}{1009}\right)\left(\frac{6}{1009}\right) = 1 \cdot \left(\frac{2}{1009}\right)\left(\frac{3}{1009}\right) = (-1)^{((1008+1)^2-1)/8}\left(\frac{1009}{3}\right) = 1 \cdot 1 = 1$$

3-2 7. First, 13 is a quadratic residue of 2. Then considering odd primes, 13 is of the form $4k+1$, so $x^2 \equiv 13 \pmod{p}$ has a solution when $x^2 \equiv p \pmod 1$3 does. The only odd prime that is a quadratic residue of 13 is 3.

3-2 8. 2 is clearly inadmissible. Therefore, $\left(\frac{10}{p}\right) = \left(\frac{5}{p}\right)\left(\frac{2}{p}\right) = \left(\frac{p}{5}\right)(-1)^{(p^2-1)/8}$.

3-2 9. 2 is inadmissible. For all other primes, $\left(\frac{5}{q}\right) = \left(\frac{q}{5}\right)$, so any prime congruent to a quadratic nonresidiue modulo 5, specifically any prime ccongruent to 2 or 3 modulo 5, satisfies this equation.

3-2 13.

3-2 16. Since the order of any residue divides 2^{2^n}, any non-primitive root is also a quadratic residue. Therefore we can determine whether 3 is a primitive root simply by calculating $\left(\frac{3}{p}\right)$, which is 1 if $n = 1$ and $\left(\frac{p}{3}\right)$for $n > 1$. In the latter case, $p - 1$ is a square and is therefore congruent to a quadratic residue modulo 3, the only one of which is 1. So $p \equiv 2 \pmod 3$, which is not a quadratic residue, so 3 is a primitive root.

3-2 20.

3-3 3. $\left(\frac{11}{61}\right) = \left(\frac{61}{11}\right) = \left(\frac{5}{11}\right) = \left(\frac{11}{5}\right) = \left(\frac{1}{5}\right) = 1.$
$\left(\frac{42}{97}\right) = \left(\frac{2}{97}\right)\left(\frac{21}{97}\right) = (-1)^{(97^2-1)/8}\left(\frac{97}{21}\right) = 1 \cdot \left(\frac{13}{21}\right) = -1.$
$\left(\frac{-43}{97}\right) = \left(\frac{43}{79}\right) = \left(\frac{79}{43}\right) = -\left(\frac{7}{43}\right) = \left(\frac{43}{7}\right) = \left(\frac{1}{7}\right) = 1.$
$\left(\frac{31}{103}\right) = -\left(\frac{103}{31}\right) = -\left(\frac{10}{31}\right) = -1.$

3-3 5. These are Legendre symbols for p n odd prime, so we can therefore analyze the sum by noting that half of the residues are quadratic, and so the 1s and -1s cancel yielding 0.

3-3 13.

3-3 14. $\left(\frac{a}{p}\right) = \left(\frac{p}{a}\right)$. We know that $x = b$ satisfies $x^2 \equiv p \pmod{a}$, so the Jacobi symbol is 1.

3-3 17. $s(0,p) = \sum_{n=1}^{p}\left(\frac{n^2}{p}\right) = \sum_{n=1}^{p-1} 1 + 0 = p - 1.$

$\sum_{a=1}^{p}\sum_{n=1}^{p}\left(\frac{n(n+a)}{p}\right)$, by part 5 of theorem 3.6, is equivalent to $\sum_{a=1}^{p}\sum_{n=1}^{p}\left(\frac{na}{p}\right) = \sum_{a=1}^{p}\sum_{n=1}^{p}\left(\frac{n}{p}\right)\left(\frac{a}{p}\right)$. There are $(p-1)/2$ quadratic residues modulo p and as many nonresidues, and one residue equivalent to zero. Therefore, of this summation of p^2 terms, $(p-1)^2/2$ of the terms have both Jacobi symbols evaluate the same nonzero value and therefore equal 1, as many have different nonzero values and equal -1, and the remaining $2p - 1$ terms are zero. So the sum is zero.

3-3 20.
```
x^2 - n^2 = a mod p
(x+n)(x-n) = a mod p
u(u-2n) = a mod p
```

3-4 1. positive definite, negative definite, indefinite, positive definite, indefinite, positive definite

3-4 4. $(3+2\sqrt{2})^k = \sum_{i=0}^{[k/2]} \binom{k}{2i} 9^{k-i}8^i + \sum_{i=0}^{[(k-1)/2]} \binom{k}{2i+1} 9^{k-i}8^i \cdot 6\sqrt{2}$, by splitting odd and even indices from the original binomial expansion. To expand $(3-2\sqrt{2})$, we need only negate the odd-indexed terms, which yields $x_k - y_k\sqrt{2}$.

$$\left(3+2\sqrt{2}\right)^k \left(3-2\sqrt{2}\right)^k = \left(x_k + y_k\sqrt{2}\right)\left(x_k - y_k\sqrt{2}\right)$$
$$(9-8)^k = x_k^2 - 2y_k^2$$

so $x_k^2 - 2y_k^2 = 1$ for all positive k.

$$\begin{aligned}\left(3+2\sqrt{2}\right)^{k+1} &= \left(3+2\sqrt{2}\right)^k \left(3+2\sqrt{2}\right)\\ x_{k+1} + y_{k+1}\sqrt{2} &= \left(x_k + y_k\sqrt{2}\right)\left(3+2\sqrt{2}\right)\\ &= 3x_k + 4y_k + (2x_k + 3y_k)\sqrt{2}\end{aligned}$$

We can demonstrate $(x_k, y_k) = 1$ by induction. This is true of the base case $k = 1$; then at each step $(x_{k+1}, y_{k+1}) = (3x_k + 4y_k, 2x_k + 3y_k) = (x_k, y_k) = 1$. In addition, since the recursive formula only includes a summation of previous terms and the initial terms are positive, both sequences are strictly increasing. Therefore for any k we can generate a unique pair x_k, y_k such that $x_k^2 - 2y_k^2 = 1$.

3-4 7. The solutions to a quadratic equation are

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

both roots of which are rational iff $\sqrt{b^2-4ac}$ is rational, i.e., if the discriminant. It is not possible for one root to be rational and the other not.

4.

$$\begin{aligned}&\left(x_1^2 + dy_1^2\right)\left(x_2^2 + dy_2^2\right)\\ =&x_1^2x_2^2 + dx_1^2y_2^2 + dx_2^2y_1^2 + d^2y_1^2y_2^2\\ =&\left(x_1x_2 + dy_1y_2\right)^2 + d\left(x_1y_2 - y_1x_2\right)^2\end{aligned}$$