1. Use Gauss's lemma to calculate $(\frac{5}{23})$.

Consider the multiples of 5 up to $\frac{23-1}{2} = 11$ times 5. These are the integers $5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55$. The least residues mod 23 of these integers are $5, 10, 15, 20, 2, 7, 12, 17, 22, 4, 9$. Of these least residues, exactly 5 exceed $\frac{23}{2} = 11.5$. So $(\frac{5}{23}) = (-1)^5 = -1$.

2. (a) Prove that $4^n \equiv 4 \bmod 12$ for all integers $n \geq 1$.

(b) If p is a prime of the form $4^n + 1$, then is 3 a quadratic residue or nonresidue mod p ?

(a) $4^2 \equiv 16 \equiv 4 \bmod 12$. $4^3 \equiv 4 \cdot 4^2 \equiv 4 \cdot 4 \equiv 4 \bmod 12$, $4^4 \equiv 4 \cdot 4^3 \equiv 4 \cdot 4 \equiv 4 \bmod 12$, and so on. The best way to write this up is induction, but the above is acceptable too.

(b) Let p be an odd prime. We know (from class) that 3 is a quadratic residue mod p if and only if p is of the form $12k+1$ or $12k+11$. If p is of the form 4^n+1, then by part (a), $p \equiv 4+1 \equiv 5 \bmod 12$. In other words, it is of the form $12k + 5$. Thus 3 is a quadratic non-residue mod p

3. Let p be an odd prime. Use Quadratic Reciprocity to calculate $(\frac{127}{311})$. Note that 127 and 311 are both primes.

$(\frac{127}{311}) = (\frac{311}{127})(-1)^{\frac{311-1}{2}\frac{127-1}{2}} = -(\frac{311}{127}) = -(\frac{57}{127}) = -(\frac{3}{127})(\frac{19}{127}) = -(\frac{127}{3})(\frac{127}{19})(-1)^{\frac{127-1}{2}\frac{3-1}{2}}(-1)^{\frac{127-1}{2}\frac{19-1}{2}}$
$= -(\frac{127}{3})(\frac{127}{19}) = -(\frac{1}{3})(\frac{13}{19}) = -(\frac{13}{19}) = -(\frac{19}{13})(-1)^{\frac{13-1}{2}\frac{19-1}{2}} = -(\frac{6}{13}) = -(\frac{3}{13})(\frac{2}{13}) = (\frac{3}{13})$, where we used $(\frac{2}{13}) = -1$ since $13 = 8k + 5$. Continuing with the calculation, $(\frac{3}{13}) = (\frac{13}{3})(-1)^{\frac{13-1}{2}\frac{3-1}{2}} = (\frac{13}{3}) = (\frac{1}{3}) = 1$.

Final answer, $(\frac{127}{311}) = 1$.

4. Use Quadratic Reciprocity to determine when 5 is a quadratic residue mod p and when it is not.

$(\frac{5}{p}) = (\frac{p}{5})(-1)^{\frac{5-1}{2}\frac{p-1}{2}} = (\frac{p}{5})$. The quadratic residues of 5 are 1 and 4. Thus $(\frac{p}{5}) = 1$ if and only if $p \equiv 1 \bmod 5$ or $p \equiv 4 \bmod 5$. In summary,

$$(\frac{5}{p}) = \begin{cases} 1 & \text{if and only if } \ p = 5k+1 \text{ or } \ p = 5k+4 \\ -1 & \text{if and only if } \ p = 5k+2 \text{ or } \ p = 5k+3. \end{cases}$$