Solutions to selected homework problems. Sections 4.5, 5.3-5.4

4.5.28. We have $b = [p-1, q-1] = [22, 46] = 2 \cdot 11 \cdot 23 = 506$. Next, we need to find d such that $13d \equiv 1 \pmod{506}$. Solving this we find $d = 39$. Thus, we have to find least residues of 228^{39} and 714^{39} modulo $23 \cdot 47 = 1081$. Applying the modular exponentiation algorithm from Section 4.4 we find

$$228^{39} \equiv 120 \pmod{1081}, \quad 714^{39} \equiv 507 \pmod{1081}.$$

Thus, the message was $120, 507$. Regrouping into two-digit numbers get $12, 05, 07$ which corresponds to "LEG".

5.3.14. $(-1/71) = -1$ since $71 \equiv 3 \pmod 4$ (see Theorem 5.7, part 5).

5.3.43. This is true. Here is the proof. We have

$$(-a/p) = (-1/p) \cdot (a/p) = -(a/p)$$

since $(-1/p)$ as $p \equiv 3 \pmod 4$. Therefore, exactly one of the Legendre symbols $(-a/p)$ and (a/p) is equal to 1.

5.4.14. $(19/67) = -(67/19) = -(10/19) = -(2/19)(5/19) = (5/19) = (19/5) = (4/5) = 1$.

5.4.37. We have $(5/p) = (p/5) = 1$ if and only if $p \equiv \pm 1 \pmod 5$. Since p is odd, this means that the last digit of p is either 1 or 9.