Exercises 7.5

Brief solutions at end of Exercises. Complete solutions at

www.oup.co.uk/companion/NumberTheory

1. Evaluate the following Legendre and Jacobi symbols:

   (i) $\left(\frac{3}{7}\right)$ (ii) $\left(\frac{3}{49}\right)$

   Is 3 a quadratic residue of 49?

2. Evaluate the following Jacobi symbols:

   (a) $\left(\frac{26}{27}\right)$ (b) $\left(\frac{12}{115}\right)$ (c) $\left(\frac{128}{1001}\right)$ (d) $\left(\frac{72}{5183}\right)$

   [Prime factorization of $1001 = 7\times11\times13$ and $5183 = 71\times73$]

3. Evaluate the following Jacobi symbols:

   (a) $\left(\frac{11}{211}\right)$ (b) $\left(\frac{17}{135}\right)$ (c) $\left(\frac{231}{1025}\right)$ (d) $\left(\frac{333}{403}\right)$

4. Prove that $\left(\frac{a^k}{n}\right) = \left(\frac{a}{n}\right)^k$ where a and n are relatively prime integers and n is an odd integer greater than 1 and k is a positive integer.

5. Prove Corollary (7.26).

6. Prove the following results for $n>1$ is an odd integer:

   (a) $\left(\frac{-1}{n}\right) = \begin{cases} 1 & \text{if } n \equiv 1 \pmod 4 \\ -1 & \text{if } n \equiv 3 \pmod 4 \end{cases}$ (b) $\left(\frac{2}{n}\right) = \begin{cases} 1 & \text{if } n \equiv \pm1 \pmod 8 \\ -1 & \text{if } n \equiv \pm3 \pmod 8 \end{cases}$

7. (i) Let $n>1$ and a be integers. Show that $(n-a)^2 \equiv a^2 \pmod n$.

   (ii) Determine the quadratic residues of 35.

8. Let a, $m>1$ and $n>1$ be relatively prime integers where m and n are odd. Prove that $\left(\frac{a}{mn}\right)=\left(\frac{a}{m}\right)\times\left(\frac{a}{n}\right)$.

9. Show that $\left(\frac{a}{p^{2m}}\right)=1$ for any natural number m.

10. Let a and b be odd integers. Prove the following where $\left(\ \right)$ are algebraic brackets:

(a) $\left(\frac{a-1}{2}\right)+\left(\frac{b-1}{2}\right)\equiv\left(\frac{ab-1}{2}\right)\pmod 2$

(b) $\left(\frac{a^2-1}{8}\right)+\left(\frac{b^2-1}{8}\right)\equiv\left(\frac{[ab]^2-1}{8}\right)\pmod 2$

11. Prove Lemma (7.23) (a) and (b). [Hint: Use the results of previous question.]

12. Prove Proposition (7.24) (b).

13. **Prove GLQR (7.25).

Brief Solutions

2. (i) –1 (ii) 1 No
3. (a) –1 (b) –1 (c) 1 (d) 1
4. (a) 1 (b) 1 (c) –1 (d) 1
7. (ii) 1, 4, 9, 11, 14, 15, 16, 21, 25, 29, 30