# PMATH 340 Number Theory, Solutions to the Exercises for Chapter 4

**1:** Determine whether $10 \in Q_{37}$ in each of the following four ways.

(a) For each $k \in P = \{1, 2, \cdots, 18\}$, find $k^2 \bmod 37$ and hence determine $Q_{37}$.

(b) For each $k \in P$, find $10^k \bmod 37$, and hence determine $\left(\frac{10}{37}\right)$ using Euler's Criterion.

(c) For each $k \in P$, find $10k$, determine $|10P \cap N|$, then find $\left(\frac{10}{37}\right)$ using Gauss' Lemma.

(d) Use Quadratic Reciprocity to calculate $\left(\frac{10}{37}\right)$.

Solution: For parts (a), (b) and (c) we make a table modulo 37.

| $k$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $k^2$ | 1 | 4 | 9 | 16 | 25 | 36 | 12 | 27 | 7 | 26 | 10 | 33 | 21 | 11 | 3 | 34 | 30 | 28 |
| $10^k$ | 10 | 26 | 1 | 10 | 26 | 1 | 10 | 26 | 1 | 10 | 26 | 1 | 10 | 26 | 1 | 10 | 26 | 1 |
| $10k$ | 10 | $-17$ | $-7$ | 3 | 13 | $-14$ | $-4$ | 6 | 16 | $-11$ | $-1$ | 9 | $-18$ | $-8$ | 2 | 12 | $-15$ | $-5$ |

(a) From the list of values of $k^2$ we see that $Q_{37} = \{1, 3, 47, 9, 10, 11, 12, 16, 21, 25, 26, 27, 28, 30, 33, 34, 36\}$.

(b) From the list of values of $10^k$ we see that $10^{18} = 1 \in U_{37}$ and so by Euler's Criterion $\left(\frac{10}{37}\right) = (-1)^{18} = 1$.

(c) From the last row we see that $|10P \cap N| = 10$ so by Gauss' Lemma $\left(\frac{10}{37}\right) = (-1)^{|10P \cap N|} = (-1)^{10} = 1$.

(d) Using Quadratic Reciprocity and the fact that for odd primes $p$, $\left(\frac{2}{p}\right) = 1 \iff p = \pm 1 \bmod 8$, we have $\left(\frac{10}{37}\right) = \left(\frac{2}{37}\right)\left(\frac{5}{37}\right) = -\left(\frac{5}{37}\right) = -\left(\frac{37}{5}\right) = -\left(\frac{2}{5}\right) = 1$. We conclude that 10 is most definitely in $Q_{37}$.

**2:** (a) Find $\left(\frac{19}{53}\right)$.

Solution: $\left(\frac{19}{53}\right) = \left(\frac{53}{19}\right) = \left(\frac{15}{19}\right) = \left(\frac{3}{19}\right)\left(\frac{5}{19}\right) = -\left(\frac{19}{3}\right)\left(\frac{19}{5}\right) = -\left(\frac{1}{3}\right)\left(\frac{4}{5}\right) = -1$.

(b) Find $\left(\frac{71}{127}\right)$.

Solution: $\left(\frac{71}{127}\right) = -\left(\frac{127}{71}\right) = -\left(\frac{56}{71}\right) = -\left(\frac{2}{71}\right)^3\left(\frac{7}{71}\right) = -\left(\frac{2}{71}\right)\left(\frac{7}{71}\right) = -\left(\frac{7}{71}\right) = \left(\frac{71}{7}\right) = \left(\frac{1}{7}\right) = 1$.

(c) Find $\left(\frac{649}{967}\right)$.

Solution: $\left(\frac{649}{697}\right) = \left(\frac{11}{697}\right)\left(\frac{59}{697}\right) = \left(\frac{967}{11}\right)\left(\frac{967}{59}\right) = \left(\frac{-1}{11}\right)\left(\frac{23}{59}\right) = -\left(\frac{23}{59}\right) = \left(\frac{59}{23}\right) = \left(\frac{13}{23}\right) = \left(\frac{23}{13}\right) = \left(\frac{10}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{5}{13}\right) = -\left(\frac{5}{13}\right) = -\left(\frac{13}{5}\right) = -\left(\frac{3}{5}\right) = -\left(\frac{5}{3}\right) = -\left(\frac{2}{3}\right) = 1$.

**3:** (a) Determine whether $569 \in Q_{2600}$.

Solution: Note that $2600 = 2^3 \cdot 5^2 \cdot 13$. We have $569 \in Q_8$ since $569 = 1 \bmod 8$. Also, $\left(\frac{569}{5}\right) = \left(\frac{4}{5}\right) = \left(\frac{2}{5}\right)^2 = 1$ so $569 \in Q_5$ and hence $569 \in Q_{25}$. Finally, $\left(\frac{569}{13}\right) = \left(\frac{10}{13}\right) = 1$ (from our solution to part (c) of problem 2), so $569 \in Q_{13}$. Thus $569 \in Q_{2600}$.

(b) Determine whether 84168 is a square (a quadratic residue) modulo 75924.

Solution: Note that $75924 = 2^2 \cdot 3^3 \cdot 19 \cdot 37$. We have $84168 = 0 = 0^2 \bmod 4$, so 84168 is a square mod 4, and $84168 = 9 = 3^2 \bmod 27$, so it is a square modulo 27, and $\left(\frac{84168}{19}\right) = \left(\frac{-2}{19}\right) = \left(\frac{-1}{19}\right)\left(\frac{2}{19}\right) = 1$ so $84168 \in Q_{19}$, and $84168 = 30 \bmod 37$ so $84168 \in Q_{37}$ by our solution to part (a) of question 1. Thus 84168 is a square modulo 75924. (We remark that $84168 \notin Q_{75925}$ since $84168 \notin U_{75924}$).

**4:** (a) Find all of the primes $p$ with $2 < p < 100$ such that $\left(\frac{11}{p}\right) = 1$.

Solution: Modulo 11, the squares are $1^2 = 1$, $2^2 = 4$, $3^2 = 9$, $4^2 = 5$ and $5^2 = 3$, so $Q_{11} = \{1,3,4,5,9\}$. Let $p$ be an odd prime with $p \neq 11$. Since $Q_{11} = \{1,3,4,5,9\}$, we have $\left(\frac{p}{11}\right) = 1 \iff p = 1,3,4,5$ or $9 \bmod 11$, and by Quadratic Reciprocity we have

$$\left(\frac{11}{p}\right) = \begin{cases} \left(\frac{p}{11}\right) \text{, if } p = 1 \bmod 4 \\ -\left(\frac{p}{11}\right) \text{, if } p = 3 \bmod 4 \end{cases}$$

and so

$$\begin{aligned} \left(\frac{11}{p}\right) = 1 &\iff (p = 1 \bmod 4 \text{ and } p = 1,3,4,5,9 \bmod 11) \text{ or } (p = 3 \bmod 4 \text{ and } p = 2,6,7,8,10 \bmod 11) \\ &\iff (p = 1,25,37,5,9 \bmod 44) \text{ or } (p = 35,39,7,19,43 \bmod 44) \\ &\iff p = 1,5,7,9,19,25,35,37,39 \text{ or } 43 \bmod 44. \end{aligned}$$

For $p < 100$ we must have

$$p = 1,5,7,9,19,25,35,37,39,43,45,49,51,53,63,69,79,81,83,87,89,93,95 \text{ or } 97$$

and picking out the primes in this list gives $p = 5,7,19,37,43,53,79,83,89$ or $97$.

(b) Find all of the primes $p$ with $2 < p < 100$ such that $\left(\frac{-10}{p}\right) = 1$.

Solution: We have $\left(\frac{-10}{p}\right) = \left(\frac{-2}{p}\right)\left(\frac{5}{p}\right)$. We know that $\left(\frac{-2}{p}\right) = 1 \iff p = 1$ or $3 \bmod 8$, and we have $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = 1 \iff p = 1$ or $4 \bmod 5$ (since $Q_5 = \{1,4\}$), and so

$$\begin{aligned} \left(\frac{-10}{p}\right) = 1 &\iff (p = 1 \text{ or } 3 \bmod 8 \text{ and } p = 1 \text{ or } 4 \bmod 5) \text{ or } (p = 5 \text{ or } 7 \bmod 8 \text{ and } p = 2 \text{ or } 3 \bmod 5) \\ &\iff (p = 1,9,11 \text{ or } 19 \bmod 40) \text{ or } (p = 37,13,7 \text{ or } 23) \\ &\iff (p = 1,7,9,11,13,19,23 \text{ or } 37 \bmod 40). \end{aligned}$$

For $p < 100$ we must have

$$p = 1,7,9,11,13,19,23,37,41,47,49,51,53,59,63,77,81,87,89,91,93 \text{ or } 99$$

and picking out the primes in this list gives $p = 7,11,13,19,23,37,41,47,53,59$ or $89$.

**5:** Let $p$ be an odd prime, let $a,b,c \in \mathbf{Z}_p$ with $a \neq 0$, and let $d = b^2 - 4ac \in \mathbf{Z}_p$. Show that when $d = 0$ the quadratic equation $ax^2 + bx + c = 0$ has exactly one solution $x \in \mathbf{Z}_p$, and when $d \neq 0$ so $d \in U_p$, if $d \notin Q_p$ then $ax^2 + bx + c = 0$ has no solution $x \in \mathbf{Z}_p$, and if $d \in Q_p$ then $ax^2 + bx + c = 0$ has exactly 2 distinct solutions $x \in \mathbf{Z}_p$.

Solution: Recall that $\mathbf{Z}_p$ is a field. Since $\mathbf{Z}_p$ has no has no zero divisors, for $u, e \in \mathbf{Z}_p$ we have

$$u^2 = e^2 \iff u^2 - e^2 = 0 \iff (u-e)(u+e) = 0 \iff \big(u - e = 0 \text{ or } u + e = 0\big) \iff u = \pm e.$$

Also, since $0 \neq a \in \mathbf{Z}_p$ it follows that $a$ is a unit in $\mathbf{Z}_p$. Since $p$ is an odd prime, we also have $0 \neq 2, 4 \in \mathbf{Z}_p$ so that 2 and 4 are also units in $\mathbf{Z}_p$. Thus we have

$$\begin{aligned} ax^2 + bx + c = 0 &\iff x^2 + \tfrac{b}{a}x + \tfrac{c}{a} = 0 \\ &\iff \big(x + \tfrac{b}{2a}\big)^2 - \tfrac{b^2}{4a^2} + \tfrac{c}{a} = 0 \\ &\iff \big(x + \tfrac{b}{2a}\big)^2 = \tfrac{b^2 - 4ac}{4a^2} \\ &\iff 4a^2\big(x + \tfrac{b}{2a}\big)^2 = d. \end{aligned}$$

When $d = 0$ we have

$$ax^2 + bx + c = 0 \iff 4a^2\big(x + \tfrac{b}{2a}\big)^2 = 0 \iff \big(x + \tfrac{b}{2a}\big)^2 = 0 \iff x + \tfrac{b}{2a} = 0 \iff x = -\tfrac{b}{2a}$$

so the equation $ax^2 + bx + c = 0$ has exactly one solution $x \in \mathbf{Z}_p$, namely $x = -\frac{b}{2a}$. Suppose that $d \neq 0$. If $d \notin Q_p$ then we cannot have $4a^2\big(x + \frac{b}{2a}\big)^2 = d$ because $4a^2\big(x + \frac{b}{2a}\big)^2 \in Q_p$, and so the equation $ax^2 + bx + c = 0$ has no solution $x \in \mathbf{Z}_p$. Suppose that $d \in Q_p$, say $d = e^2$ with $0 \neq e \in Z_p$. Then we have

$$ax^2 + bx + c = 0 \iff 4a^2\big(x + \tfrac{b}{2a}\big)^2 = e^2 \iff 2a\big(x + \tfrac{b}{2a}\big) = \pm e \iff x + \tfrac{b}{2a} = \pm\tfrac{e}{2a} \iff x = -\tfrac{b}{2a} \pm \tfrac{e}{2a}.$$

Finally we note that the two solutions $x_1 = \frac{b}{2a} + \frac{e}{2a}$ and $x_2 = \frac{b}{2a} - \frac{e}{2a}$ are distinct because $x_1 - x_2 = \frac{e}{a} \neq 0$.