PMATH 340 Number Theory, Solutions to Assignment 3

1: Make a table showing some of the values of k^2, 3^k, $(-4)^k$ and $-4k$ modulo 31 for $1 \le k \le 15$, and then determine whether $-4 \in Q_{31}$ using each of the following 5 methods:

Solution: Here is the table

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
k^2	1	4	9	16	25	5	18	2	21	7	28	20	14	10	8
3^k	3	9	27	19	26	16	17	20	29	25	13	8	24	10	30
$(-4)^k$	-4	16	-2	8	-1										
$-4k$	-4	-8	-12	15	11	7	3	-1	-5	-9	-13	14	10	6	2

(a) From the list of values k^2 mod 31, determine whether $-4 \in Q_{31}$ using Definition 4.2.

Solution: Since $-4 = 27$ does not appear on the list of values k^2, we have $-4 \notin Q_{31}$. Note that although we only listed k^2 for $1 \le k \le 15$, this gives the complete list of squares in U_{31} because for $16 \le \ell \le 30$ we can write $\ell = -k$ mod 31 with $1 \le k \le 30$, and then we have $\ell^2 = (-k)^2 = k^2$ mod 31.

(b) From the list of values 3^k mod 31, determine whether $-4 \in Q_{31}$ using Note 4.8.

Solution: Since $3^k = 30 = -1$ mod 31, if we continued the list of powers of 3, the next 15 values would be $3^{15+k} = 3^{15}3^k = -3^k$ for $1 \le k \le 15$, ending wth $3^{30} = 1$. Thus $\text{ord}(3) = 30 = |\text{U}_{31}|$ so that $U_{31} = \langle 3 \rangle$. Since $-4 = 27 = 3^3$, by Note 4.8 we have $\left(\frac{-4}{31}\right) = (-1)^3 = -1$ so that $-4 \notin Q_{31}$.

(c) From the list of values $(-4)^k$ mod 31, determine whether $-4 \in Q_{31}$ using Theorem 4.11 (Euler's Criterion).

Solution: Since $(-4)^5 = -1$, Euler's Criterion gives $\left(\frac{-4}{31}\right) = (-4)^{(31-1)/2} = (-4)^{15} = \left((-4)^5\right)^3 = (-1)^3 = -1$ so that $-4 \notin Q_{31}$.

(d) From the list of values $-4k$ mod 31, determine whether $-4 \in Q_{31}$ using Theorem 4.12 (Gauss' Lemma).

Solution: The list of values $-4k$ is a list of the elements in $-4P$. We listed the elements as positive integers when they lie in P and as negative integers when they lie in N, so we see that $|-4P \cap N| = 7$ (indeed we have $-4P \cap N = \{-4, -8, -12, -1, -5, -9, -13, \}$). By Gauss' Lemma, $\left(\frac{-4}{31}\right) = (-1)^{|-4P\cap N|} = (-1)^7 = -1$ so that $-4 \notin Q_{31}$.

(e) Determine whether $-4 \in Q_{31}$ using Theorem 4.9 (The Multiplicative Property) and Theorem 4.14.

Solution: Since $31 = 3$ mod 4, it follows from Theorem 4.14 that $-1 \notin Q_{31}$, and so by the Multiplicative Property we have $\left(\frac{-4}{31}\right) = \left(\frac{-1}{31}\right)\left(\frac{2}{31}\right)^2 = (-1)(1) = -1$ so that $-4 \notin Q_{31}$.

2: (a) Determine whether $23 \in Q_{61}$.

Solution: Using various properties of the Legendre symbol, including quadratic reciprocity, we have

$$\left(\tfrac{23}{61}\right) = \left(\tfrac{61}{23}\right) = \left(\tfrac{15}{23}\right) = \left(\tfrac{3}{23}\right)\left(\tfrac{5}{23}\right) = -\left(\tfrac{23}{3}\right)\left(\tfrac{23}{5}\right) = -\left(\tfrac{2}{3}\right)\left(\tfrac{3}{5}\right) = -\left(\tfrac{2}{3}\right)\left(\tfrac{5}{3}\right) = -\left(\tfrac{2}{3}\right)^2 = -1,$$

and hence $23 \notin Q_{61}$.

(b) Determine whether $47 \in Q_{1111}$.

Solution: Note that $1111 = 11 \cdot 101$. We have

$$\begin{aligned}\left(\tfrac{47}{11}\right) &= \left(\tfrac{3}{11}\right) = -\left(\tfrac{11}{3}\right) = -\left(\tfrac{2}{3}\right) = 1\\ \left(\tfrac{47}{101}\right) &= \left(\tfrac{101}{47}\right) = \left(\tfrac{7}{47}\right) = -\left(\tfrac{47}{7}\right) = -\left(\tfrac{5}{7}\right) = -\left(\tfrac{7}{5}\right) = -\left(\tfrac{2}{5}\right) = 1.\end{aligned}$$

Since $47 \in Q_{11}$ and $47 \in Q_{101}$, it follows that $47 \in Q_n$.

(c) Determine whether $413 \in Q_{739}$.

Solution: We need to determine whether 739 is prime. Note that $28^2 = 784 > 739$, so it suffices to determine whether 739 has a prime factor p with $p < 28$. The primes $p < 28$ are 2, 3, 5, 7, 11, 13, 17, 19 and 23. The tests for divisibility by 2, 3, 5 and 11 (described in Example 2.31) show that these primes do not divide 739, so it remains to test the primes 7, 13, 17 and 19, which we do using long division: we find that

$$739 = 105 \cdot 7 + 4\ ,\ 739 = 13 \cdot 56 + 11\ ,\ 739 = 17 \cdot 43 + 8\ ,\ \text{and } 739 = 19 \cdot 38 + 17$$

so none of these primes is a factor of 739, and so 739 is prime.

We have $413 = 7 \cdot 59$ and so, using various properties of the Legendre symbol, we have

$$\begin{aligned}&\left(\tfrac{7}{739}\right) = -\left(\tfrac{739}{7}\right) = -\left(\tfrac{4}{7}\right) = -1\\ &\left(\tfrac{59}{739}\right) = -\left(\tfrac{739}{59}\right) = -\left(\tfrac{31}{59}\right) = \left(\tfrac{59}{31}\right) = \left(\tfrac{28}{31}\right) = \left(\tfrac{2}{31}\right)^2\left(\tfrac{7}{31}\right) = \left(\tfrac{7}{31}\right) = -\left(\tfrac{31}{7}\right) = -\left(\tfrac{3}{7}\right) = \left(\tfrac{7}{3}\right) = \left(\tfrac{1}{3}\right) = 1\\ &\left(\tfrac{413}{739}\right) = \left(\tfrac{7}{739}\right)\left(\tfrac{59}{739}\right) = (-1)(1) = -1.\end{aligned}$$

and hence $413 \notin Q_{739}$.

3: (a) Determine the number of quadratic residues in U_{400} (that is find $|Q_{400}|$).

Solution: Since $400 = 16 \cdot 25$ and $\gcd(16, 25) = 1$, we have $Q_{400} \cong Q_{16} \times Q_{25}$ by Theorem 4.3. We have $|U_{16}| = 8$, $|Q_{16}| = 2$, $|U_{25}| = 20$ and $|Q_{25}| = 10$ and so $|Q_{400}| = |Q_{16}|\,|Q_{25}| = 2 \cdot 10 = 20$.

(b) Determine the number of quadratic residues in $\mathbb{Z}_{400}$ (that is find $|S_{400}|$).

Solution: In $\mathbb{Z}_{16} \setminus U_{16} = \{0, 2, 4, 6, 8, 10, 12, 14\}$. we have

$$\begin{array}{ccccccccc} x & 0 & 2 & 4 & 6 & 8 & 10 & 12 & 14 \\ x^2 & 0 & 4 & 0 & 4 & 0 & 4 & 0 & 4 \end{array}$$

and hence $S_{16} = U_{16} \cup \{0, 4\}$ so that $|S_{16}| = |Q_{16} + 2| = 4$. In $\mathbb{Z}_{25} \setminus U_{25} = \{0, 5, 10, 15, 20\}$, we have

$$\begin{array}{cccccc} x & 0 & 5 & 10 & 15 & 20 \\ x^2 & 0 & 0 & 0 & 0 & 0 \end{array}$$

and hence $S_{25} = U_{25} \cup \{0\}$ so that $|S_{25}| = |U_{25} + 1| = 11$. Thus $|S_{400}| = |S_{16}|\,|S_{25}| = 4 \cdot 11 = 44$.

(c) Let $n = 10^6$. Find the number of solutions to $(x-1)(x-5) = 0$ in $\mathbb{Z}_n$.

Solution: Note that $10^6 = 2^6 \cdot 5^6$. Notice that $4\big|(x-1) \iff 4\big|(x-5)$ and that 8 cannot divide both $(x-1)$ and $(x-5)$, and so we have

$$\begin{aligned} (x-1)(x-5) = 0 \bmod 2^6 &\iff 2^6\big|(x-1)(x-5) \\ &\iff \big(2^4\big|(x-1) \text{ or } 2^4\big|(x-5)\big) \\ &\iff x = 1 \bmod 2^4 \text{ or } x = 5 \bmod 2^4 \\ &\iff x = 1, 17, 33, 49, 5, 21, 37 \text{ or } 53 \bmod 2^6 \end{aligned}$$

so there are 8 solutions to $(x-1)(x-5) = 0$ modulo 2^6. Also notice that 5 can only divide one of $(x-1)$ and $(x-5)$ and so we have

$$\begin{aligned} (x-1)(x-5) = 0 \bmod 5^6 &\iff 5^6\big|(x-1)(x-5) \\ &\iff 5^6\big|(x-1) \text{ or } 5^6\big|(x-5) \\ &\iff x = 1 \text{ or } 5 \bmod 5^6 \end{aligned}$$

so there are 2 solutions modulo 5^6. Thus there are $8 \cdot 2 = 16$ solutions in $\mathbb{Z}_n$.

4: (a) Prove that for primes $p>3$ we have $-3 \in Q_p \iff p=1 \bmod 6$.

Solution: We have $\left(\frac{-3}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)$. Recall, from Theorem 4.14, that

$$\left(\frac{-1}{p}\right)=\left\{\begin{array}{r} 1 \text{ , if } p=1 \bmod 4 \\ -1 \text{ , if } p=3 \bmod 4 \end{array}\right\} \quad \text{and} \quad \left(\frac{3}{p}\right)=\left\{\begin{array}{r} 1 \text{ , if } p=1 \text{ or } 11 \bmod 12 \\ -1 \text{ , if } p=5 \text{ or } 7 \bmod 12 \end{array}\right\}$$

and so

$$\begin{aligned}\left(\frac{-3}{p}\right)&=\left\{\begin{array}{r} 1 \text{ , if } (p=1 \bmod 4 \text{ and } p=1 \text{ or } 11 \bmod 12) \text{ or } (p=3 \bmod 4 \text{ and } p=5 \text{ or } 7 \bmod 12) \\ -1 \text{ , if } (p=1 \bmod 4 \text{ and } p=5 \text{ or } 7 \bmod 12) \text{ or } (p=3 \bmod 4 \text{ and } p=1 \text{ or } 11 \bmod 12) \end{array}\right\} \\ &=\left\{\begin{array}{r} 1 \text{ , if } p=1 \text{ or } 7 \bmod 12 \\ -1 \text{ , if } p=5 \text{ or } 11 \bmod 12 \end{array}\right\}=\left\{\begin{array}{r} 1 \text{ , if } p=1 \bmod 6 \\ -1 \text{ , if } p=5 \bmod 6 \end{array}\right\}\end{aligned}$$

(b) Find a set $S \subseteq U_{24}$ such that for all primes $p>3$ we have $6 \in Q_p \iff p \in S \bmod 24$.

Solution: Let p be prime with $p>3$. Note that $\left(\frac{6}{p}\right)=\left(\frac{-2}{p}\right)\left(\frac{-3}{p}\right)$. By Theorem 4.14 and Part (a), we have

$$\left(\frac{-2}{p}\right)=\left\{\begin{array}{r} 1 \text{ if } p=1,3 \bmod 8 \\ -1 \text{ if } p=5,7 \bmod 8 \end{array}\right\} \quad \text{and} \quad \left(\frac{-3}{p}\right)=\left\{\begin{array}{r} 1 \text{ if } p=1 \bmod 6 \\ -1 \text{ if } p=5 \bmod 6 \end{array}\right\}$$

It follows that

$$\begin{aligned}\left(\frac{6}{p}\right)&=\left\{\begin{array}{r} 1 \text{ if } (p=1,3 \bmod 8 \text{ and } p=1 \bmod 6) \text{ or } (p=5,7 \bmod 8 \text{ and } p=5 \bmod 6) \\ -1 \text{ if } (p=1,3 \bmod 8 \text{ and } p=5 \bmod 6) \text{ or } (p=5,7 \bmod 8 \text{ and } p=1 \bmod 6) \end{array}\right\} \\ &=\left\{\begin{array}{r} 1 \text{ if } (p=1,19 \bmod 24) \text{ or } (p=5,23 \bmod 24) \\ -1 \text{ if } (p=17,11 \bmod 24) \text{ or } (p=13,7 \bmod 24) \end{array}\right\}\end{aligned}$$

Thus we can take $S=\{1,5,19,23\}=\{\pm 1,\pm 5\} \in U_{24}$.

(c) Find a set $S \subseteq U_{28}$ such that for all primes $p>7$ we have $7 \in Q_p \iff p \in S \bmod 28$.

Solution: In U_7 we have $1^1=1$, $2^2=4$ and $3^3=2$ so that $Q_7=\{1,2,4\}$. Let p be a prime number with $p>7$. When $p=1 \bmod 4$ we have $\left(\frac{7}{p}\right)=\left(\frac{p}{7}\right)$, which is equal to 1 when $p \in \{1,2,4\} \bmod 7$. and when $p=3 \bmod 4$ we have $\left(\frac{7}{p}\right)=-\left(\frac{p}{7}\right)$, which is equal to 1 when $p \in \{3,5,6\} \bmod 7$. Thus

$$\begin{aligned} p \in Q_7 &\iff \big(p=1 \bmod 4 \text{ and } p \in \{1,2,4\} \bmod 7\big) \text{ or } \big(p=3 \bmod 4 \text{ and } p \in \{2,5,6\} \bmod 7\big) \\ &\iff \big(p \in \{1,9,25\} \bmod 28\big) \text{ or } \big(p \in \{3,19,27\} \bmod 28\big) \\ &\iff p \in \big\{1,3,9,19,25,27\big\} \bmod 28. \end{aligned}$$

Thus we can take $S=\big\{1,3,9,19,25,27\big\}=\big\{\pm 1,\pm 3 \pm 9\big\} \subseteq U_{28}$.