Number theory Assignment 1

Edward McDonald

Question 1

For this question, let n be a positive integer such that $\mathbb{U}_n$ has primitive roots (That is, $n = 1, 2, 4$, a power of an odd prime or double a power of an odd prime). We also let a be an integer coprime to n.

Part a

Theorem 1 *$a \in \mathbb{U}_n$ is a kth power in $\mathbb{U}_n$ that is, there is a number $x \in \mathbb{U}_n$ with $x^k \equiv a \mod n$ if and only if*

$$a^{\frac{\varphi(n)}{d}} \equiv 1 \mod n$$

where φ is Euler's totient function and $d := (\varphi(n), k) := \gcd(\varphi(n), k)$.

Proof First suppose that a is a kth power modulo n. So choose x such that

$$a \equiv x^k \mod n.$$

Note that x must be coprime to n due our assumption that a is coprime to n. Then simply raise a to the power $\varphi(n)/d$. So we have

$$a^{\frac{\varphi(n)}{d}} \equiv x^{\frac{\varphi(n)k}{d}} \mod n.$$

However the right hand side is $x^{\varphi(n)}$ raised to the power k/d. k/d is a whole number since $d|k$. By Euler's theorem, $x^{\varphi(n)} \equiv 1 \mod n$. Hence,

$$a^{\frac{\varphi(n)}{d}} \equiv 1 \mod n.$$

Conversely, suppose that

$$a^{\frac{\varphi(n)}{d}} \equiv 1 \mod n$$

and we wish to find x such that $a \equiv x^k \mod n$.

By assumption, $\mathbb{U}_n$ has a primitive element (a generator). Let α be such a primitive element, and choose r such that

$$\alpha^r \equiv a \mod n.$$

Raise both sides to the power $\varphi(n)/d$, to find

$$\alpha^{\frac{r\varphi(n)}{d}} \equiv a^{\frac{\varphi(n)}{d}} \equiv 1 \mod n.$$

Since α is a primitive element, it must have minimal order $\varphi(n)$. Hence, we must have

$$\varphi(n) | \frac{r\varphi(n)}{d}$$

So choose $t \in \mathbb{Z}$ such that

$$t\varphi(n) = \frac{r\varphi(n)}{d}.$$

Hence $r = td$. Recall that $d = (\varphi(n), k)$. So by Bezout's lemma, there are integers p and q such that $d = p\varphi(n) + qk$.

Thus,

$$\begin{aligned} a &\equiv \alpha^r \\ &\equiv \alpha^{td} \\ &\equiv \alpha^{tp\varphi(n)+tqk} \\ &\equiv \alpha^{tp\varphi(n)}\alpha^{tqk} \\ &\equiv \alpha^{tqk} \mod n. \end{aligned}$$

So put $x = \alpha^{tq}$ and then $a \equiv x^k \mod n$. $\square$

We now wish to find the *number* of solutions to the equation $x^k \equiv a \mod n$, provided that it has solutions. Note that any two solutions, x and y are related by a kth root of unity modulo n: since if $x^k \equiv y^k \mod n$, then xy^{-1} is a kth root of unity. Hence, given a solution x we can find all solutions as $x\zeta$, where ζ is a kth root of unity.

So to find the number of solutions to the equation, we simply need to find the number of kth roots of unity modulo n.

Lemma 2 *There are $(\varphi(n), k)$ kth roots of unity in $\mathbb{U}_n$.*

Proof Consider the group homomorphism $\psi : \mathbb{U}_n \to \mathbb{U}_n$ given by $x \mapsto x^k$. Le α be a primitive element for $\mathbb{U}_n$. The image of ψ is then

$$\{1, \alpha^k, \alpha^{2k}, \alpha^{3k}, \dots\}$$

This is a subgroup of $\mathbb{U}_n$, let its size be r. r must divide the size of $\mathbb{U}_n$, $r|\varphi(n)$, and r is the smallest positive integer such that $\alpha^{kr} \equiv 1 \mod n$.

So kr is the smallest multiple of k divisible by $\varphi(n)$. Hence $kr = \mathrm{lcm}(k, \varphi(n))$. So $r = \varphi(n)/(\varphi(n), k)$.

So the image of ψ has size $r = \varphi(n)/(k, \varphi(n))$.

Hence the kernel of ψ has size $(k, \varphi(n))$ by the first isomorphism theorem.

The kernel of ψ is exactly the numbers x in $\mathbb{U}_n$ such that $x^k \equiv 1 \mod n$, so there are $(k, \varphi(n))$ kth roots of unity in $\mathbb{U}_n$. $\square$

By the above argument, if the equation $x^k \equiv a \mod n$ has solutions then there are exactly $(k, \varphi(n))$ solutions.

Part b

Corollary 3 *If p is a prime of the form $6k - 1$, then the equation $x^3 \equiv a \mod p$ has a unique solution for every a.*

Proof In the case when $(a, p) \neq 1$, then $a \equiv 0 \mod p$, and so the equation $x^3 \equiv a \mod p$ has a unique solution $x = 0$. The solution is unique because the ring $\mathbb{Z}_p$ is a domain and cannot have nonzero nilpotent elements.

For $(a,p)=1$, we can use the results in part a.

Put $p=6k-1$. Then $\varphi(p)=6k-2=2(3k-1)$. So $\varphi(p)$ cannot be a multiple of 3, since $3k-1$ is one less than a multiple of 3. Hence, $(3,\varphi(p))=1$. Now by Euler's theorem

$$a^{\varphi(p)/(3,\varphi(p))} \equiv a^{\varphi(p)} \equiv 1 \mod p.$$

Therefore, the equation $x^3 \equiv a \mod p$ has a solution, and the number of solutions is $(\varphi(p),3)=1$.

That is, for any a the equation $x^3 \equiv a \mod p$ has a unique solution. □

Question 2

For question 2, suppose that q is an odd prime such that $p := 2q+1$ is also prime. For example, $q=11$ and $p=23$.

Lemma 4 *There are $q-1$ primitive roots modulo p, q quadratic residues and q quadratic non residues.*

Proof The set $\mathbb{U}_p$ has $\varphi(\varphi(p))$ primitive roots. Since $p=2q+1$ is prime, $\varphi(p)=2q$. As q is odd, we can compute $\varphi(2q)=\varphi(2)\varphi(q)=q-1$. Hence, there are $\varphi(\varphi(p))=q-1$ primitive roots for $\mathbb{U}_n$.

By Theorem 1.2 in chapter 1 of the course notes, exactly half of the numbers in $\mathbb{U}_p$ are quadratic residues. Hence, the number of quadratic residues is half of $2q+1-1$. So the number of quadratic residues is q, and there must also be q quadratic non residues.

Lemma 5 *A quadratic residue is never a primitive root.*

Proof Suppose that n is an integer, and a is a quadratic residue in $\mathbb{U}_n$. So $a \equiv x^2 \mod n$ for some $x \in \mathbb{U}_n$. If a is a primitive root, then there is some k such that $x \equiv a^k \mod n$. Hence $a^k \equiv a^{2k} \mod n$ and so $a^k \equiv 1 \mod n$. Hence $x \equiv 1 \mod n$, so $a \equiv 1 \mod n$ and a cannot be a primitive root. □

Since every primitive root is a quadratic non residue, and here are $q-1$ primitive elements in $\mathbb{U}_p$ and q quadratic non residues: there must be exactly one number in $\mathbb{U}_n$ that is a quadratic non residue but not a primitive element.

Theorem 6 $2q \in \mathbb{U}_n$ *is not a primitive element.*

Proof Since $p=2q+1$, $2q \equiv -1 \mod p$. Hence $2q$ has minimal order 2, and so cannot be a primitive element for $\mathbb{U}_n$. □

Theorem 7 $2q$ *is a quadratic non residue modulo p.*

Proof Since $2q \equiv -1 \mod p$, we simply need to show that -1 is not a quadratic residue modulo p.

By the corollary to Wilson's theorem in the course notes, -1 is a quadratic residue modulo a prime p precisely when $p \equiv 1 \mod 4$.

However, since q is odd, we cannot have $2q+1 \equiv 1 \mod 4$. Hence p is not equal to 1 modulo 4. So -1 is not a quadratic residue modulo p. □

We have therefore shown that the unique quadratic non residue that is not a primitive element in $\mathbb{U}_p$ is $2q$.

Corollary 8 *The primitive roots of* $\mathbb{U}_{23}$ *are* $5, 7, 10, 11, 14, 15, 17, 19, 20, 21$

Proof We simply need to find the quadratic non residues that are not -1, since 23 is a prime of the form $2q+1$ for an odd prime $q = 11$. We have already shown that there must be $q - 1 = 10$ primitive roots.

So we simply need to find a single primitive root, then all of the odd powers of that primitive root that are not -1 are the remaining primitive roots since even powers are quadratic residues.

Consider 5. We can show that 5 is a primitive root by showing that it it not a quadratic residue. So we compute the Legendre symbol:

$$\left(\frac{5}{23}\right) = \left(\frac{23}{5}\right)$$

by quadratic reciprocity, since $5 \equiv 1 \mod 4$. The right hand side is $\left(\frac{3}{5}\right)$. By quadratic reciprocity, this is $\left(\frac{5}{3}\right) = \left(\frac{-1}{3}\right)$.

However by the corollary to Wilson's theorem, $\left(\frac{-1}{3}\right) = -1$. Hence 5 is not a quadratic residue modulo 23 and since $5 \neq -1$, we can conlude that 5 is a primitive element.

Odd powers of 5 are easily computed since $5^2 \equiv 2 \mod 23$. Hence the odd powers of 5 are.

$$\begin{aligned}
5^3 &\equiv 10 \\
5^5 &\equiv 20 \\
5^7 &\equiv 17 \\
5^9 &\equiv 11 \\
5^{11} &\equiv 22 \equiv -1 \\
5^{13} &\equiv 21 \\
5^{15} &\equiv 19 \\
5^{17} &\equiv 15 \\
5^{19} &\equiv 7 \\
5^{21} &\equiv 14
\end{aligned}$$

where the congruences are modulo 23 .So excluding $5^{11} \equiv -1$, these are the primitive elements of $\mathbb{U}_{23}$. $\square$

Question 3

Part a

Theorem 9 *Every number of the form* $4n + 2$ *for some integer* n *is expressible as a sum of three squares, exactly* 2 *of which are odd.*

Proof By theorem 1.10 in the course notes, a number can be expressed as a sum of three squares unless it is of the form $4^\alpha(8k + 7)$ for some integers α, k. Since $4n + 2$ is not divisible by 4, we need only show that $4n + 2$ is not congruent to 7 modulo 8.

Suppose that $4n + 2 \equiv 7 \mod 8$

$$\begin{aligned}
&4n + 2 \equiv 7 \mod 8 \\
\Rightarrow\ &4n \equiv 5 \mod 8
\end{aligned}$$

But then $5 = 4n - 8k$ for some integer k. This is impossible because 5 is odd. Hence, $4n + 2$ is expressible as a sum of three squares.

Suppose that $4n + 2 = a^2 + b^2 + c^2$. We cannot have all a, b, c being even, because then $4|a^2 + b^2 + c^2$ but $4n + 2$ is not divisible by 4. Similarly, if exactly one of a, b, c is odd, then $a^2 + b^2 + c^2$ is odd, but $4n + 2$ is not odd. Similarly, if all of a, b, c are odd then $4n + 2$ is odd.

Hence, the only possible case is that exactly two of a, b, c are even. $\square$

Part b

Theorem 10 *Every odd positive integer can be expressed in the form $a^2 + b^2 + 2c^2$ for integers a, b, c.*

Proof Suppose that $2n + 1$ is any odd positive integer. Then by the preceding theorem there are integers r, s, t such that

$$4n + 2 = (2r)^2 + (2s + 1)^2 + (2t + 1)^2.$$

Divide through by 2 and expand, so that we have

$$2n + 1 = 2r^2 + 2s^2 + 2t^2 + 2s + 2t + 1.$$

Note the identity,

$$(s + t)^2 + (s - t)^2 = 2s^2 + 2t^2.$$

So we can express $2n + 1$ as

$$2n + 1 = 2r^2 + (s - t)^2 + (s + t)^2 + 2s + 2t + 1.$$

Recognise that $(s + t)^2 + 2s + 2t + 1 = (s + t + 1)^2$, so

$$2n + 1 = 2r^2 + (s - t)^2 + (s + t + 1)^2.$$

This gives the desired decomposition. $\square$.