UNIVERSITY OF NEW SOUTH WALES

SCHOOL OF MATHEMATICS AND STATISTICS

Assignment

Number Theory

Author:
Adam J. Gray

Student Number:
3329798

Question 1

Part a

Prove the following theorem.

Theorem 1. *Let n be an integer for which $\mathbb{U}_n$ admits primitive roots and suppose $(a, n) = 1$. Then the congruence $x^k \equiv a \mod n$ has a solution if and only if*

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

where $d = (k, \phi(n))$. Furthermore, if it has solutions, then it has exactly d solutions in $\mathbb{U}_n$.

Proof. Let $g \in \mathbb{U}_n$ be a primitive root. Now as $(a, n) = 1$ and g is a primitive root, there must exist an r such that

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

Now it suffices to consider $x \in \{g^1, g^2, \ldots, g^{\phi(n)}\}$ because if $(x, n) \neq 1$ then $(x^k, n) \neq 1$ for all k, which conflicts with $(a, n) = 1$.
So there exists an s such that $g^s \equiv x \mod n$. We can now write

$$\begin{aligned} & x^k \equiv a \mod n \\ \Leftrightarrow \quad & g^{sk} \equiv g^r \mod n \\ \Leftrightarrow \quad & sk \equiv r \mod \phi(n) \qquad (1) \end{aligned}$$

Now (1) has a solution if and only if $(k, \phi(n)) \mid r$, that is if and only if $d \mid r$. Also if a solution exists there are clearly d such solutions.
We now wish to show $d \mid r \Leftrightarrow a^{\frac{\phi(n)}{d}} \equiv 1 \mod n$. Note that

$$a^{\frac{\phi(n)}{d}} \equiv g^{\phi(n)\frac{r}{d}} \mod n$$

and because $\text{ord}_n(g) = \phi(n)$ we have that

$$g^{\phi(n)\frac{r}{d}} \equiv 1 \mod n,$$

if and only if $d \mid r$. That is to say $a^{\frac{\phi(n)}{d}} \equiv 1 \mod n$ if and only if $d \mid r$.
So we have shown that a solution to

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

exists if and only if

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

and that if a solution exists, there are exactly d solutions. □

Part b

Prove the following lemma.

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

Proof. See that

$$(\phi(p), 3) = (6k - 2, 3) \\ = 1. \tag{2}$$

From the lemma above we have that $x^3 \equiv a \mod p$ has d solutions if

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

where $d = (\phi(p), 3)$. The uniqueness of the solution is therefore guaranteed by (2).
We just have to show that $a^{\phi(p)} \equiv 1 \mod p$ for all a, but Euler's theorem guarantees that this must be the case for $(a, p) = 1$. As p is prime this is true for all $a \in \mathbb{Z}_p$, except 0. So for all $a \in \mathbb{Z}_p$, $a \not\equiv 0 \mod p$ there is a solution. When $a \equiv 0 \mod p$ it is clear that $x \equiv 0 \mod p$ is a solution. So we have shown that for primes of the form $p = 6k + 1$, $x^3 \equiv a \mod p$ has a *unique* solution for all a. □

Question 2

Suppose q and $p = 2q + 1$ are both prime, with $q > 2$. Prove that $2q$ is the only element in $\mathbb{Z}_p$ which is a quadratic non-residue, but not a primitive root. Hence find all the primitive roots in $\mathbb{Z}_{23}$.

Solution

If g is a primitive root $\mod p$ then it must be that $g^{\frac{p-1}{2}} \equiv -1 \mod p$, but Euler's criterion tells us that g must therefore be a a quadratic non-residue. That is to say, all primitive roots must be quadratic non-residues.
The number of primitive roots of $\mathbb{Z}_p$ is

$$\begin{aligned}\phi(\phi(p)) &= \phi(\phi(2q + 1)) \\ &= \phi(2q) \\ &= \phi(2)\phi(q) \\ &= q - 1. \end{aligned} \tag{3}$$

From the lectures it is know that the number of quadratic residues (and hence non-residues) mod p is

$$\frac{p-1}{2} = q. \tag{4}$$

So from (3) and (4) we can conclude that there must be precisely one quadratic non-residue which is not a primitive root in $\mathbb{Z}_p$.
Consider $2q$ and note that $2q \equiv -1 \mod p$ so, $2q$ cannot possibly be a primitive root. We can also see that

$$\begin{aligned}(-1)^{\frac{p-1}{2}} &\equiv (-1)^q \\ &\equiv (-1)\end{aligned}$$

as we have $q > 2$, so by Euler's criterion we $2q$ must be a quadratic non-residue.
So we have shown that $2q$ is the only quadratic non-residue in $\mathbb{Z}_p$.
We now consider $\mathbb{Z}_{23}$ and note that $23 = 11*2+1$ and that 11 is a prime. This means we can apply the above result to list all the primitive roots in $\mathbb{Z}_{23}$. They are $\{5, 7, 10, 11, 14, 15, 17, 19, 20, 21\}$.

Question 3

Part a

Show that for any positive integer n, the number $4n+2$ is the sum of three squares, exactly two of which are odd.

Solution

From the lectures it is known that a number, m, can be written as the sum of three squares if and only if it cannot be written in the form $m = 4^{\alpha}(8k+7)$, where $\alpha, k \in \mathbb{Z}$. So if we let $m = 4n+2$ it suffices to show that $4 \nmid m$ and $m \not\equiv 7 \mod 8$.
Clearly $4n+2 \equiv 2$ or $6 \mod 8$. Additionally $4n+2 \equiv 2 \mod 4$. So $m \not\equiv 7 \mod 8$ and $4 \nmid m$, therefore it must be possible to write m as the sum of three squares.
Now we wish to show that two of the squares must be odd. Note that for even x, we must have $x^2 \equiv 0 \mod 4$ and for odd x we must have $x^2 \equiv 1 \mod 4$. Then if we have

$$m \equiv 2 \equiv x^2 + y^2 + z^2 \mod 4$$

we must have that exactly two of $\{x^2, y^2, z^2\}$ are congruent $1 \mod 4$, that is, two of the numbers must be odd. $\square$

Part b

Deduce that every odd positive integer can be expressed in the form $a^2 + b^2 + 2c^2$.

Solution

From the above statement we know that for any positive $n \in \mathbb{Z}$, $4n+2 = x^2+y^2+z^2$, for some positive integers $\{x, y, z\}$, and that exactly one of these integers is even. Without loss of generality suppose z is even. Then

$$\begin{aligned} 2(2n+1) &= x^2 + y^2 + z^2 \\ 2n+1 &= \frac{x^2+y^2}{2} + 2c^2 \end{aligned}$$

where $c = \frac{z}{2}$.
Let

$$d = \frac{x^2+y^2}{2},$$

where x and y are odd, so that it suffices to show that d can be written as the sum of two integer squares. Note that

$$\begin{aligned} d &= \frac{x^2+y^2}{2} \\ &= \underbrace{\left(\frac{x+y}{2}\right)^2}_{\in\mathbb{Z}} + \underbrace{\left(\frac{x-y}{2}\right)^2}_{\in\mathbb{Z}} \end{aligned}$$

and since x and y are both odd, $\frac{x+y}{2}$ and $\frac{x-y}{2}$ are both integers. Letting

$$a = \frac{x+y}{2}$$

and

$$b = \frac{x-y}{2}$$

we have shown that we can write $d = a^2 + b^2$ and hence have shown that we can write

$$2n + 1 = a^2 + b^2 + 2c^2$$

for some integers, $\{a, b, c\}$ and n a positive integer.
For completeness it remains only to tie up one edge case when we wish to write 1 as the sum of three squares, but this is clearly achieved with $a = 1, b = 0, c = 0$.

Acknowledgements

Thank you to Kent Yang for mentioning a technique which reduced a larger proof by cases argument in Question 3, Part a, to a single, short, modulus argument.
Thank you to Roberto Riedig for pointing out an extra case to consider in my solution for Question 1, Part b.