MATH 2170-19W Problem Set 8

April 4, 2019

Solutions

$g = 2$ is a primitive root modulo 19.

Use the following table to assist you in the solution of the first two questions and 4(a). The most efficient solutions involve the use of the table and the application of theory; numerically correct solutions involving long computations will not receive full credit.

t	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
g^t	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1

Question 1.

For all parts, note that $\phi(19) = 18$.

[2] (a) Find the least positive residue of 12^6 modulo 19 (efficiently, using the given information!).

Solution: $12 \equiv 2^{15} \pmod{19}$, $15 * 6 = 90 \equiv 18 \pmod{18}$, and so $12^6 \equiv 2^{18} \equiv 1 \pmod{19}$.

[2] (b) Find the number of solutions to $x^{15} \equiv 12 \pmod{19}$.

Solution: $(15, 18) = 3$ and $18/3 = 6$, and by (a), $12^6 \equiv 1 \pmod{19}$, so by Theorem 2.37, the congruence has 3 solutions $\pmod{19}$.

[3] (c) Find all the solutions to $x^{15} \equiv 12 \pmod{19}$.

Solution: From (a) we are looking for the solutions to $x^{15} = (2^t)^{15} \equiv 2^{15} \pmod{19}$, and therefore solutions to $15t \equiv 15 \pmod{18}$. $(15, 18) = 3$, so this is equivalent to $5t \equiv 5 \pmod{6}$, and $(5, 6) = 1$ so we can cancel and get $t \equiv 1 \pmod{6}$. Thus the three solutions for t are $t \equiv 1, 7, 13 \pmod{18}$, and so the solutions to the original congruence are $x \equiv 2, 14, 3$.

[2] **Question 2.** Evaluate $\left(\frac{7}{19}\right)$ and $\left(\frac{8}{19}\right)$ using the results of the table. No marks will be given for any other method.

Solution: $7 \equiv 2^6 \pmod{19}$, an even exponent, so 7 is a square $\pmod{19}$, that is, $\left(\frac{7}{19}\right) = 1$.

$8 \equiv 2^3 \pmod{19}$, an odd exponent, so 8 is not a square $\pmod{19}$, that is, $\left(\frac{8}{19}\right) = -1$.

Comments: You *must* demonstrate through your solutions of these two questions your understanding of the use of primitive roots and their powers in solving problems like these.

[4] **Question 3.** Evaluate the Legendre symbol $\left(\frac{79}{103}\right)$, using the theory of quadratic reciprocity.

Remark: There are several correct pathways to a solution.
Solution:

$$\left(\frac{79}{103}\right) = \left(\frac{103}{79}\right)(-1)^{\frac{102}{2}\frac{78}{2}} = -\left(\frac{24}{79}\right) = -\left(\frac{4}{79}\right)\left(\frac{2}{79}\right)\left(\frac{3}{79}\right) =$$

$$= -(1)(-1)^{\frac{79^2-1}{8}}\left(\frac{79}{3}\right)(-1)^{\frac{78}{2}\frac{2}{2}} = -(1)(1)(-1)\left(\frac{1}{3}\right) = 1$$

We know that $\frac{79^2-1}{8}$ is even since $79 \equiv 7 \pmod 8$.
[Here we are making use of the following: $\frac{1^2-1}{8} = 0$, $\frac{3^2-1}{8} = 1$, $\frac{5^2-1}{8} = 3$, and $\frac{7^2-1}{8} = 6$.]

Question 4. Let g be a primitive root modulo p, p a prime.
If $(a,p) = 1$, define $\log_g(a)$ to be the unique t, $1 \le t < p$, such that $g^t \equiv a \pmod p$.
Suppose that $(a,p) = 1 = (b,p)$.

[2] (a) For $p = 19$, evaluate $\log_2(13)$.

Solution: From the table, $\log_2(13) = 5$.

[2] (b) Prove that for any $n > 0$, $\log_g(a^n) \equiv n\log_g(a) \pmod{\phi(p)}$;

Proof: Let $t = \log_g(a)$, so $g^t \equiv a \pmod p$.
Then $g^{tn} \equiv a^n \pmod p$, and so $tn \equiv \log_g(a^n) \pmod{\phi(p)}$,
that is, $n\log_g(a) \equiv \log_g(a^n) \pmod{\phi(p)}$. ∎

[3] **Question 5.** Suppose that p is a prime and $(a,p) = 1 = (b,p)$.
[Recall the formula for $\left(\frac{ab}{p}\right)$.]
Show that ab is a quadratic residue modulo p if both a and b are quadratic residues modulo p *or* if neither a nor b is a quadratic residue modulo p, and that ab is a quadratic non-residue modulo p if exactly one of a or b is a quadratic non-residue modulo p.

Proof: $\left(\frac{a}{p}\right) = \pm 1$ since $(a,p) = 1$, and similarly for b.
$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.
There are two cases: $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ and $\left(\frac{a}{p}\right) = -\left(\frac{b}{p}\right)$.
In the first case, the product is 1 and ab is a quadratic residue $\pmod p$, and in the second case, the product is -1 and ab is a quadratic non-residue $\pmod p$, ∎

[20] TOTAL