MATH 2170-19W Problem Set 8

April 1, 2019

Due: in class, Wednesday, April 03, 2019

$g = 2$ 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.

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

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

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

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

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

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 $\log_2(13)$.

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

[3] **Question 5.** Suppose that p is a prime and $(a,p) = 1 = (b,p)$.
[Recall the formula for $\left(\dfrac{ab}{p}\right)$.]
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.

[20] TOTAL