MATH 467 FACTORIZATION AND PRIMALITY TESTING, FALL 2024, PRACTICE EXAM 2 SOLUTIONS.

Mid-term Exam 2 will on Monday 3rd November. 9:05-9:55, 133 Erickson.

1. Show that 2 is a primitive root modulo 11 and draw up a table of discrete logarithms to this base modulo 11. Hence, or otherwise, find all solutions to the following congruences, (i) $x^6 \equiv 7 \pmod{11}$, (ii) $x^{48} \equiv 9 \pmod{11}$, (iii) $x^7 \equiv 8 \pmod{11}$.

y	1	2	3	4	5	6	7	8	9	10
2^y	2	4	8	5	10	9	7	3	6	1
x	1	2	3	4	5	6	7	8	9	10
$\text{dlog}_2 x$	10	1	8	2	4	9	7	3	6	5

(i) This is equivalent to $6y \equiv 7 \pmod{10}$. Since $(6,10) = 2 \nmid 7$ there is no solution. (ii) $48y \equiv 6 \pmod{10}$, $24y \equiv 3 \pmod{5}$ $1 \le y \le 10$, $y \equiv 2 \pmod{5}$, $y \equiv 2$ or $7 \pmod{10}$, $x \equiv 4$ or $7 \pmod{11}$ (iii) $7y \equiv 3 \pmod{10}$, $y \equiv 9 \pmod{10}$, $x \equiv 6 \pmod{11}$.

2. Let g be a primitive root modulo p. Prove that no k exists satisfying $g^{k+2} \equiv g^{k+1} + 1 \equiv g^k + 2 \pmod{p}$.

If $p = 2$, then $g = 1$ and we would have $1 \equiv 2 \pmod{2}$ which is impossible. If $p > 2$ we have $g^{k+1}(g-1) \equiv 1 \pmod{p}$ and $g^k(g-1) \equiv 1 \pmod{}$. Thus $1 \equiv g\big(g^k(g-1)\big) \equiv g \pmod{p}$ which is also impossible.

3. Find all primes p such that $x^2 \equiv 13 \pmod{p}$ has a solution.

We have $1 = \left(\frac{13}{p}\right)_L = \left(\frac{p}{13}\right)_L$. Thus any prime p which is a QR modulo p. The QR modulo p are $1, 4, 9, 3, 12, 10$. Thus any prime $p \equiv 1, 3, 2, 9, 10$ or $12 \pmod{13}$.

4. Evaluate the following Legendre symbols, showing your working (i) $\left(\frac{-1}{103}\right)_L$,

We have $\left(\frac{-1}{103}\right)_L = (-1)^{(102)/2} = -1$
by Euler's criterion.

(ii) $\left(\frac{2}{103}\right)_L$.

(ii) $103 \equiv 7 \pmod{8}$, so $(103^2 - 1)/8$ is even and
$\left(\frac{2}{103}\right)_L = 1$.

(iii) $\left(\frac{7}{103}\right)_L$.

By the law of quadratic reciprocity
$\left(\frac{7}{103}\right)_L = -\left(\frac{103}{7}\right)_L = -\left(\frac{5}{7}\right)_L = -\left(\frac{7}{5}\right)_L =$
$-\left(\frac{2}{5}\right)_L = +1$.