MATH 467 FALL 2024, PRACTICE EXAM 2, SOLUTIONS.

Mid-term Exam 2 will be on Wednesday 30th October. 9:05-9:55, 012 Walker.

1. Suppose that p, q and r are distinct primes. Prove that

$$p^{(q-1)(r-1)} + q^{(r-1)(p-1)} + r^{(p-1)(q-1)} \equiv 2 \pmod{pqr}.$$

By the Fermat-Euler theorem we have $q^{(r-1)(p-1))} = (q^{p-1})^{r-1} \equiv 1 \pmod p$ and likewise $r^{(p-1)(q-1)} \equiv 1 \pmod p$. Hence $p^{(q-1)(r-1)} + q^{(r-1)(p-1)} + r^{(p-1)(q-1)} \equiv 2 \pmod p$, and so also $\pmod q$ and $\pmod r$.

2. Solve the simultaneous congruences $x \equiv 4 \pmod{19}, x \equiv 5 \pmod{31}$. Solve $31a \equiv 1 \pmod{19}$ and $19b \equiv 1 \pmod{31}$. By Euclid's algorithm, $1 = 8.31 - 13.19$, Thus $a = 8$, $b \equiv -13 \equiv 18 \pmod{31}$. $19.31 = 589$. Hence $x \equiv 4.8.31 + 5.18.19 \equiv 346 \pmod{589}$

3. (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
$\mathrm{dlog}_2 x$	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) $7y \equiv 3 \pmod{10}$, $y \equiv 9 \pmod{10}$, $x \equiv 6 \pmod{11}$.

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

$103 \equiv 7 \pmod 8$, 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
$\left(\frac{7}{103}\right)_L = -\left(\frac{103}{7}\right)_L = -\left(\frac{5}{7}\right)_L = -\left(\frac{7}{5}\right)_L =$
$-\left(\frac{2}{5}\right)_L = +1$.