

MAT2120 Number Theory

Problems III

Suhyun Park (20181634)

Department of Computer Science and Engineering, Sogang University

1. Solve the congruence $8x^5 \equiv 3 \pmod{13}$ using the following table of indices for the prime 13 relative to the primitive root 2:

a	1	2	3	4	5	6	7	8	9	10	11	12
$\text{ind}_2 a$	12	1	4	2	9	5	11	3	8	10	7	6

Solution. Since $8x^5 \equiv 3 \pmod{13}$, $x^5 \equiv 2 \pmod{13}$.

Taking ind_2 on $x^5 \equiv 2 \pmod{13}$ gives

$$\begin{aligned}\text{ind}_2 x^5 &\equiv \text{ind}_2 2 \pmod{12} \\ \Leftrightarrow 5 \text{ind}_2 x &\equiv 1 \pmod{12} \\ \Leftrightarrow \text{ind}_2 x &\equiv 5 \pmod{12},\end{aligned}$$

therefore $x \equiv 6 \pmod{13}$.

2. Show that if p is a prime of the form $4k+1$, then $\left(\frac{1}{p}\right) + \left(\frac{2}{p}\right) + \cdots + \left(\frac{q}{p}\right) = 0$, where $q = \frac{p-1}{2}$.

TODO

3. Let p be an odd prime. Show that 2 is a quadratic residue of p if $p \equiv \pm 1 \pmod{8}$ and a quadratic nonresidue of p if $p \equiv \pm 3 \pmod{8}$.

TODO

4. Using problem 2 above, show that the prime 1999 divides $2^{999} - 1$.

TODO

5. Calculate $\left(\frac{6}{19}\right)$ using (a) Euler's criterion (b) Gauss's Lemma (c) the law of quadratic reciprocity.

(a) By Euler's criterion,

$$\begin{aligned}\left(\frac{6}{19}\right) &\equiv 6^{\frac{19-1}{2}} \equiv 6^9 \pmod{19} \\ &\equiv 6 \cdot (6^2)^4 \equiv 6 \cdot 36^4 \pmod{19} \\ &\equiv 6 \cdot (-2)^4 \equiv 6 \cdot 16 \pmod{19} \\ &\equiv 6 \cdot (-3) \equiv -18 \pmod{19} \\ &\equiv 1 \pmod{19},\end{aligned}$$

hence $\left(\frac{6}{19}\right) = 1$.

(b) By Gauss's Lemma,

$$\left(\frac{6}{19}\right) = (-1)^s$$

where s is the number of least positive integers mod 19 of the integers $1 \cdot 6, 2 \cdot 6, 3 \cdot 6, \dots, \frac{19-1}{2} \cdot 6$ that are greater than $\frac{19}{2}$. Note that

$$\begin{aligned}&\{1 \cdot 6, 2 \cdot 6, 3 \cdot 6, 4 \cdot 6, 5 \cdot 6, 6 \cdot 6, 7 \cdot 6, 8 \cdot 6, 9 \cdot 6\} \\ &= \{6, 12, 18, 24, 30, 36, 42, 48, 54\} \\ &\equiv \{6, 12, 18, 5, 11, 17, 4, 10, 16\} \pmod{19},\end{aligned}$$

hence $s = 6 \Rightarrow \left(\frac{6}{19}\right) = (-1)^6 = 1$.

(c) By the law of quadratic reciprocity,

$$\begin{aligned}
\left(\frac{6}{19}\right) &= \left(\frac{2}{19}\right) \left(\frac{3}{19}\right) \\
&= (-1)^{\frac{19^2-1}{8}} \times (-1)^{\frac{3-1}{2} \frac{19-1}{2}} \left(\frac{19}{3}\right) \\
&= (-1)^{45} \times (-1)^9 \left(\frac{1}{3}\right) \\
&= (-1) \times (-1) \times 1 \\
&= 1.
\end{aligned}$$

6. Let F_n denote the n -th Fibonacci number, and p an odd prime with $p \neq 5$. Show that

$$F_p \equiv \begin{cases} 1 \pmod{p} & \text{if } p \equiv \pm 1 \pmod{5}, \\ -1 \pmod{p} & \text{if } p \equiv \pm 2 \pmod{5}. \end{cases}$$

TODO

7. Show that if $p > 3$ is an odd prime, then

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{12}, \\ -1 & \text{if } p \equiv \pm 5 \pmod{12}. \end{cases}$$

TODO

8. Show that if $p > 3$ is an odd prime, then

$$\left(\frac{-3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{6}, \\ -1 & \text{if } p \equiv -1 \pmod{6}. \end{cases}$$

TODO