MAT2120 Number Theory
Problems III

Suhyun Park (20181634)

Department of Computer Science and Engineering, Sogang University

1. Solve the congrugence $8x^5 \equiv 3 \pmod{13}$ 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
$\operatorname{ind}_2 a$	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

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

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 $q = \frac{p-1}{2}$.

Proof. Recall that, if p is odd prime, then

$$\left(\frac{-1}{p}\right) = 1 \qquad \text{if and only if } p \equiv 1 \pmod{4}.$$

Note that

$$\left(\frac{p-a}{p}\right) = \left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right) = \left(\frac{a}{p}\right).$$

Claim p : odd prime, then $\sum_{k=1}^{p-1}\left(\frac{k}{p}\right)=0$. Thus,

$$\begin{aligned} 0 &= \left(\frac{1}{p}\right)+\left(\frac{2}{p}\right)+\cdots+\left(\frac{p-1}{p}\right) \\ &= 2\left[\left(\frac{1}{p}\right)+\left(\frac{2}{p}\right)+\cdots+\left(\frac{q}{p}\right)\right] \qquad \text{where } q=\frac{p-1}{2}. \end{aligned}$$

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 $p \equiv \pm 3 \pmod 8$.

Proof. By Gauss's Lemma, $\left(\frac{2}{p}\right)=(-1)^s$ where s is the number of least positive residues mod p of the integers $1\cdot 2,\ 2\cdot 2,\ 3\cdot 2,\ \cdots,\ \frac{p-1}{2}\times 2$ that are greater than $\frac{p}{2}$.

Since all of these integers are less than p, we need only count these greater than $\frac{p}{2}$ to find. Note that the integers $2j$ where $1 \le j \le \frac{p-1}{2}$ are less than $\frac{p}{2}$ whem $j \le \frac{p}{4}$.

Thus $\exists \left\lfloor \frac{p}{4} \right\rfloor$ integers in the set less that $\frac{p}{2}$. By Gauss's lemma,

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p-1}{2}-\left\lfloor \frac{p}{4}\right\rfloor}.$$

To prove the theorem, it suffice to show that $\frac{p-1}{2}-\left\lfloor \frac{p}{4}\right\rfloor \equiv \frac{p^2-1}{8} \pmod 2$ for every odd integer p.

Note that it holds for a positive integer p if and only if it holds for $p+8$. It can be checked that it holds for $p \equiv \pm 1$, $p \equiv \pm 3 \pmod 8$. Hence we conclude that it holds for every odd integer p.

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

Proof. By Problem 3, 2 is a quadratic residue of 1999; hence there exists integer x such that $x^2 \equiv 2 \pmod{1999}$, hence

$$\begin{aligned} x^2 &\equiv 2 \pmod{1999} \\ \Rightarrow \left(x^2\right)^{999} &\equiv 2^{999} \pmod{1999} \\ \Rightarrow x^{1998} = x^{\phi(1999)} &\equiv 2^{999} \pmod{1999} \\ \Rightarrow 1 &\equiv 2^{999} \pmod{1999} \\ \Rightarrow 0 &\equiv 2^{999}-1 \pmod{1999}. \end{aligned}$$

Therefore 1999 divides $2^{999} - 1$.

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,

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

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 $1\cdot 6, 2\cdot 6, 3\cdot 6, \cdots, \frac{19-1}{2}\cdot 6$ 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

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

Proof. Note that

$$
\begin{aligned}
\sqrt{5}F_p &= \left(\frac{1+\sqrt{5}}{2}\right)^p - \left(\frac{1-\sqrt{5}}{2}\right)^p \\
\Rightarrow \sqrt{5}2^p f_p &= \left(1+\sqrt{5}\right)^p - \left(1-\sqrt{5}\right)^p \\
&= \sum_{r=0}^{p} \binom{p}{r} \sqrt{5}^r - \sum_{r=0}^{p} \binom{p}{r} \left(-\sqrt{5}\right)^r \\
&= 2\left[\binom{p}{1}\sqrt{5} + \binom{p}{3}\sqrt{5}^3 + \cdots + \binom{p}{p}\sqrt{5}^p\right],
\end{aligned}
$$

thus

$$
2^{p-1}F_p = \binom{p}{1} + 5\binom{p}{3} + \cdots + 5^{\frac{p-1}{2}}\binom{p}{p}.
$$

Since $p \mid \binom{p}{k}$ for $1 \le k \le p-1$ and $\binom{p}{p} = 1$, we can see that

$$
2^{p-1}F_p \equiv 5^{\frac{p-1}{2}} \pmod{p}.
$$

Note that, by Fermat, $2^{p-1} \equiv 1 \pmod{p}$ and by Euler, $5^{\frac{p-1}{2}} \equiv \left(\frac{5}{p}\right) \pmod{p}$, hence $F_p \equiv \left(\frac{5}{p}\right) \pmod{p}$. Note also that, by the quadratic reciprocity, $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$. Hence

$$
F_p \equiv \left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \begin{cases} 1 \pmod{p} & p = \pm 1 \pmod{5}, \\ -1 \pmod{p} & p = \pm 2 \pmod{5}. \end{cases}
$$

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

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

Proof. If $p \equiv 1 \pmod 4$,

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{3}, \\ -1 & \text{if } p \equiv 2 \pmod{3}. \end{cases}$$

Similarity, if $p \equiv -1 \pmod 4$,

$$\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = \begin{cases} -1 & \text{if } p \equiv 1 \pmod{3}, \\ 1 & \text{if } p \equiv 2 \pmod{3}. \end{cases}$$

Hence it is clear that

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

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

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

Proof. Note that

$$\begin{aligned} \left(\frac{-3}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) \\ &= (-1)^{\frac{p-1}{2}}(-1)^{\frac{3-1}{2}\frac{p-1}{2}}\left(\frac{p}{3}\right) \\ &= \left(\frac{p}{3}\right). \end{aligned}$$

Hence, if $p \equiv 1 \pmod 6$, then $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1$, and if $p \equiv -1 \pmod 6$, then $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{-1}{3}\right) = -1$.