MAT2120 Number Theory
Homework, November 7th

Suhyun Park (20181634)

Department of Computer Science and Engineering, Sogang University

Lemma 1 (Gauss's Lemma). *p : odd prime. $p \nmid a$. If s is the number of least positive residues mod p of the integers $a, 2a, 3a, \cdots, \frac{p-1}{2}a$ that are greater than $\frac{p}{2}$, then $\left(\frac{a}{p}\right) = (-1)^s$.*

Proof. Let

$$\begin{aligned} z &= a \cdot 2a \cdot 3a \times \cdots \times \frac{p-1}{2}a \\ &= a^{\frac{p-1}{2}} \left[1 \cdot 2 \cdot 3 \times \cdots \times \frac{p-1}{2}\right]. \end{aligned}$$

Since a and p are coprime, $a, 2a, \cdots, \frac{p-1}{2}a$ are distinct modulo p.

If we define $f(x)$ to be

$$f(x) = \begin{cases} x & \text{if } 1 \le x \le \frac{p-1}{2} \\ p - x & \text{if } \frac{p+1}{2} \le x \le p-1 \end{cases}$$

then since s is the count of least positive residues mod p of the integers, it will count $\frac{p+1}{2} \le ka \le p-1$, hence

$$z = (-1)^s \left[f(1)\, f(2)\, f(3) \times \cdots \times f\left(\frac{p-1}{2}\right)\right].$$

Note that if, for some positive integer $1 \le n, m \le \frac{p-1}{2}$, $na \equiv \pm ma \pmod p$, then since a is coprime to p, $n \equiv m \pmod p$ ($\because 1 \le n, m \le \frac{p-1}{2}$). This gives that $f(a), f(2a), \cdots, f\left(\frac{p-1}{2}a\right)$ is just a rearrangement of $1, 2, \cdots, \frac{p-1}{2}$. Therefore since

$$z = a^{\frac{p-1}{2}} \left[1 \cdot 2 \cdot 3 \times \cdots \times \frac{p-1}{2}\right] = (-1)^s \left[1 \cdot 2 \cdot 3 \times \cdots \times \frac{p-1}{2}\right],$$

it is clear that $a^{\frac{p-1}{2}} = (-1)^s$. $\square$