Theorem 9.5: Gauss's Lemma

Let p be an odd prime and $\gcd(a,p)=1$

Let n be the number of integers in

$$S=\{a, 2a, 3a \dots \left(\tfrac{p-1}{2}\right)a\}$$

whose remainder when divided by p is larger than $p/2$.

Then

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

proof:

Because $\gcd(a,p)=1$, $a \in (\mathbb{Z}/p\mathbb{Z})^*$ so all of the numbers in S are different and nonzero modulo p. Compute all the remainders.

Let $r_1, r_2 \dots, r_m$ be the remainders with

$$0 < r_i < p/2$$

$s_1, s_2 \dots s_n$ be the remainders with

$$p/2 < s_i < p$$

Claim: $r_1, r_2 \dots r_m, p-s_1, p-s_2 \dots p-s_n$ are all of the integers $1, 2, \dots \frac{p-1}{2}$ in some order

① These are $\frac{p-1}{2}$ integers

② These are all between 1 and $\frac{p-1}{2}$

- r_i is clear since $\frac{p-1}{2} = \lfloor p/2 \rfloor$

- if $p/2 < s_i < p$

$$-p/2 > -s_i > -p$$
$$p/2 > p - s_i > 0$$

③ They are all different

- Suppose $r_i = p - s_j$ i.e. $r_i + s_v = p$

So $ua + va \equiv 0 \mod p$ $0 < u, v \leq \frac{p-1}{2}$

$$(u+v)a \equiv 0 \mod p$$
$$u+v \equiv 0 \mod p$$

but $0 < u+v \leq p-1$ so this is impossible

- Suppose $r_i = r_j$ then $ua \equiv va \mod p$, contradiction if $u \neq v$
- Similarly if $p-s_i = p-s_j$, then $s_i = s_j$.

Now if we have $\frac{p-1}{2}$ integers, all between 1 and $\frac{p-1}{2}$ inclusively, and all different, they must be $1, 2, 3 \ldots \frac{p-1}{2}$ in some order.

Therefore

$$\left(\frac{p-1}{2}\right)! = r_1 r_2 \ldots r_m (p-s_1)(p-s_2) \ldots (p-s_n)$$
$$\equiv r_1 r_2 \ldots r_m (-s_1)(-s_2) \ldots (-s_n) \mod p$$
$$\equiv (-1)^n r_1 r_2 \ldots r_m s_1 s_2 \ldots s_n \mod p$$

Since $r_1, r_2, \ldots, r_m, s_1, s_2, \ldots, s_n$ are the remainders for $a, 2a, 3a \ldots \left(\frac{p-1}{2}\right)a$, we have that the product

$$r_1 r_2 \dots r_m s_1 s_2 \dots s_n \equiv a \cdot 2a \cdot 3a \dots \left(\tfrac{p-1}{2}\right)a \mod p$$

since a number is congruent to its remainder modulo p. So

$$\left(\tfrac{p-1}{2}\right)! \equiv (-1)^n a \cdot 2a \cdot \dots \left(\tfrac{p-1}{2}\right) a \mod p$$
$$\equiv (-1)^n a^{\frac{p-1}{2}} \left(\tfrac{p-1}{2}\right)! \mod p$$

Now since $1, 2, 3 \dots \left(\frac{p-1}{2}\right) \in (\mathbb{Z}/p\mathbb{Z})^*$, $\left(\frac{p-1}{2}\right)! \in (\mathbb{Z}/p\mathbb{Z})^*$ too so we can cancel to get

$$1 \equiv (-1)^n a^{\frac{p-1}{2}} \mod p$$

Multiplying both sides by $(-1)^n$ and remembering that $(-1)^{2n} = 1$ we get

$$(-1)^n \equiv a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \mod p$$

where the last congruence is Euler's criterion

Now since both $(-1)^n$ and $\left(\frac{a}{p}\right)$ are equal to ± 1, we must have equality in $\mathbb{Z}$ (p cannot divide the difference) so

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

$\square$

We can now use this to show

Theorem 9.6

Let p be an odd prime, then

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \mod 8 \\ -1 & \text{if } p \equiv \pm 3 \mod 8 \end{cases}$$

proof: We use Gauss's Lemma and its notation: Here $a=2$, so

$$S = \{2, 4, 6, \dots, p-1\} \quad \text{this is } 2 \cdot \left(\frac{p-1}{2}\right)$$

Since each of these are $0 \leq s < p$, they are their own remainders. Therefore all we need is to count how many of these are greater than $P/2$. Since

$$n = \#\{s \in S;\ s > P/2\} = \frac{P-1}{2} - \#\{s \in S : s < P/2\}$$

we count instead those that are less than $P/2$.

We have that $s = 2k < P/2$ so $k < P/4$. We need to decide how many integers are such that $0 < k < P/4$ or really if that number is even or odd. Then we see if $\frac{P-1}{2}$ is even or odd and this will tell us if n is even or odd.

Let $p = 8m + r$, $r = 1, 3, 5, 7$ (r cannot be even otherwise p would be even, contradiction)

First look at $\frac{p-1}{2}$:

$$\frac{p-1}{2} = \frac{8m+r-1}{2} = 4m + \frac{r-1}{2}$$

$$= \begin{cases} 4m & \text{if } r=1 \\ 4m+1 & \text{if } r=3 \\ 4m+2 & \text{if } r=5 \\ 4m+3 & \text{if } r=7 \end{cases}$$

Now look at $\#\{s \in S : s < p/2\}$

$$= \#\{k \in \mathbb{Z} : 0 < k < p/4\}$$

$$= \left\lfloor \frac{p}{4} \right\rfloor$$

where $\lfloor x \rfloor$ is the floor function, giving the largest integer n with $n \leq x$.

$$\left\lfloor \frac{p}{4} \right\rfloor = \left\lfloor \frac{8m+r}{4} \right\rfloor$$

$$= \left\lfloor 2m + \frac{r}{4} \right\rfloor$$

$$= 2m + \left\lfloor \frac{r}{4} \right\rfloor$$

$$= \begin{cases} 2m & \text{if } r = 1,3 \\ 2m+1 & \text{if } r = 5,7 \end{cases}$$

so now

$$n = \begin{cases} 4m + 2m = 6m \equiv 0 \mod 2 & \text{if } r = 1 \\ 4m+1 + 2m = 6m+1 \equiv 1 \mod 2 & \text{if } r = 3 \\ 4m+2 + 2m+1 = 6m+3 \equiv 1 \mod 2 & \text{if } r = 5 \\ 4m+3 + 2m+1 = 6m+4 \equiv 0 \mod 2 & \text{if } r = 7 \end{cases}$$

and $\left(\frac{2}{p}\right) = (-1)^n = \begin{cases} 1 & \text{if } r = 1,7 \text{ OR } p \equiv \pm 1 \mod 8 \\ -1 & \text{if } r = 3,5 \text{ OR } p \equiv \pm 3 \mod 8 \end{cases}$

$\square$