15. Gauss Lemma

Let p be an odd prime. Recall that the set

$$S = \{\, k \in \mathbb{Z} \,|\, -(p-1)/2 \leq k \leq (p-1)/2 \,\}$$

is a complete residue system modulo p.

Theorem 15.1 (Gauss's Lemma)**.** *Let p be an odd prime and let a be an integer coprime to p. Let μ be the number of elements of the set*

$$\{\, ka \,|\, 1 \leq k \leq \frac{p-1}{2} \,\}$$

which are equivalent modulo p to a negative element of S.

Then

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

Proof. We may assume that a is coprime to p. Note that ka is equivalent to a unique element of S. Let r_1, r_2, ..., be the positive elements of S and $-s_1$, $-s_2$, ..., the negative elements of S, we get this way.

Note that no two r's are equal and no two s's are equal. Suppose that an r is equal to an s, that is, $r_i = s_j$. By assumption we may find m_i and m_j such that $m_i a \equiv r_i$ and $m_j a \equiv -s_j$. In this case

$$\begin{aligned}(m_i + m_j)a &= m_i a + m_j a \\ &\equiv r_i - s_j \mod p \\ &= 0.\end{aligned}$$

As a is coprime to p, $m_i + m_j$ is divisible by p. On the other hand

$$\begin{aligned}m_i + m_j &\leq (p-1)/2 + (p-1)/2 \\ &= p-1,\end{aligned}$$

which is impossible.

Thus all of the $(p-1)/2$ numbers r_i and s_j are distinct. As there are $(p-1)/2$ such numbers between 1 and $(p-1)/2$, it follows that the numbers r_i and s_j are precisely the numbers between 1 and $(p-1)/2$.

Therefore

$$\begin{aligned}a \cdot (2a) \cdot (3a) \ldots (p-1)/2a &\equiv r_1 \cdot r_2 \cdot r_3 \ldots)(-s_1 \cdot -s_2 \cdot -s_3 \ldots) \mod p \\ &= (-1)^{\mu}(r_1 \cdot r_2 \cdot r_3 \ldots)(s_1 \cdot s_2 \cdot s_3 \ldots) \\ &= (-1)^{\mu} 1 \cdot 2 \cdot 3 \cdot 4 \cdot \ldots (p-1)/2 \\ &= (-1)^{\mu}((p-1)/2)!.\end{aligned}$$

But

$$a \cdot (2a) \cdot (3a) \ldots (p-1)/2a = a^{(p-1)/2}((p-1)/2)!.$$

Cancelling the common factorial from both sides we get

$$\left(\frac{a}{p}\right) = a^{(p-1)/2}$$
$$= (-1)^{\mu}. \qquad \square$$

Example 15.2. *Is 3 a quadratic residue modulo 37?*

We have to consider the first 18 multiples of 3. They are

3 6 9 12 15 18 21 24 27 30 33 36 39 42 45 48 51 54.

These are equivalent to the following elements of S:

3 6 9 12 15 18 −16 −13 −10 −7 −4 −1 2 5 8 11 14 17.

Six of these are negative and so $\mu = 6$. Therefore

$$\left(\frac{3}{37}\right) = (-1)^6$$
$$= 1.$$

Thus 3 is a quadratic residue modulo 37.

Note that we do indeed get every integer from 1 to 18, up to sign.

Definition 15.3. *If r is a real number $\llcorner r \lrcorner$ is the largest integer smaller than r.*

$$\llcorner\sqrt{2}\lrcorner = 1, \qquad \llcorner e \lrcorner = 2 \qquad \text{and} \qquad \llcorner \pi \lrcorner = 3.$$

Theorem 15.4. *If p is an odd prime then 2 is a quadratic residue of p if and only if p is congruent to 1 or −1 modulo 8.*

Succintly,

$$\left(\frac{a}{p}\right) = (-1)^{(p^2-1)/8}.$$

Proof. We use (15.1). Consider the first $(p-1)/2$ multiples of 2 . Roughly half of these multiples lie in the interval $(0, p/2)$ and the other half in the interval $(p/2, p)$. The ones in the interval $(p/2, p)$ are equivalent to the negative elements of S. Now

$$2k < \frac{p}{2} \qquad \text{if and only if} \qquad k < \frac{p}{4}.$$

Thus

$$\lfloor \frac{p}{4} \rfloor$$

multiples lie in the interval $(0, p/2)$. The rest lie in the interval $(p/2, p)$ and so

$$\mu = \frac{p-1}{2} - \lfloor \frac{p}{4} \rfloor.$$

We now consider cases.

If $p = 8k + 1$ then

$$\mu = \frac{(8k + 1 - 1)}{2} - \lfloor \frac{8k + 1}{4} \rfloor = 4k - 2k = 2k.$$

If $p = 8k + 3$ then

$$\mu = \frac{(8k + 3 - 1)}{2} - \lfloor \frac{8k + 3}{4} \rfloor = 4k + 1 - 2k = 2k + 1.$$

If $p = 8k + 5$ then

$$\mu = \frac{(8k + 5 - 1)}{2} - \lfloor \frac{8k + 5}{4} \rfloor = 4k + 2 - 2k - 1 = 2k + 1.$$

If $p = 8k + 7$ then

$$\mu = \frac{(8k + 7 - 1)}{2} - \lfloor \frac{8k + 7}{4} \rfloor = 4k + 3 - 2k - 1 = 2k + 2.$$

Thus μ is even if and only if $p \equiv \pm 1 \mod 8$. Thus 2 is a quadratic residue if and only if $p \equiv \pm 1 \mod 8$.

Finally note that $(p^2 - 1)/8$ is even if and only if $p \equiv \pm 1 \mod 8$. □

Definition 15.5. *If $m > 1$ is an integer and $(a, m) = 1$ then we say that a is a **primitive root** if the order of a is equal to $\varphi(m)$.*

Recall that the order t is the smallest natural number such that $a^t \equiv 1 \mod m$; the order always divides $\varphi(m)$.

Example 15.6. *Is 2 a primitive root of 13?*

Let t be the order of 2. We want to decide if $t = \varphi(13) = 12$. t has to divide 12, so that $t = 1$, 2, 3, 4, 6 or 12. $2^1 = 2 \neq 1 \mod 13$ and so $t \neq 1$. $2^2 = 4 \neq 1 \mod 13$ and so $t \neq 2$. $2^3 = 8 \neq 1 \mod 13$ and so $t \neq 3$. $2^4 = 16 \equiv 3 \mod 13$ and so $t \neq 4$. Finally $2^6 = 4 \cdot 3 = 12 \mod 13$. Thus $t \neq 6$. By a process of elimination $t = 12$ and so 2 is a primitive root.

Theorem 15.7.

(1) *If $p = 4q + 1$ where q is an odd prime then 2 is a primitive root.*

(2) *If $p = 2q + 1$ where q is a prime of the form $4k + 1$ then 2 is a primitive root.*

(3) *If $p = 2q + 1$ where q is a prime of the form $4k - 1$ then -2 is a primitive root.*

Proof. We first prove (1). If t is the order of 2 then t divides $p - 1 = 4q$. So $t = 1$, 2, 4, q, $2q$ or $4q$. Now if $t = 1$, 2 or 4 then $2^4 \equiv 1 \mod p$, so that p divides 15. But then $p = 3$, which is too small, or $p = 5$ so that $q = 1$, which is not prime.

Otherwise either $t = 4q$ or $t|(2q)$, so that it suffices to show $2^{2q} \neq 1 \mod p$. Suppose that $q = 2k + 1$. Then

$$\begin{aligned} p &= 4q + 1 \\ &= 4(2k + 1) + 1 \\ &= 8k + 5. \end{aligned}$$

Therefore

$$\begin{aligned} 2^{2q} &= 2^{(p-1)/2} \\ &= \left(\frac{2}{p}\right) \mod p \\ &= -1, \end{aligned}$$

as $p \equiv 5 \mod 8$.

Parts (b) and (c) are proved in a similar fashion. □