Gauss's Lemma

Example

Determine if $x^2 \equiv 39 \mod 83$ has a solution.

By Theorem 11.3, Theorem 11.4, Theorem 11.5, and Theorem 11.6, we have that:

$$\begin{aligned}
\left(\frac{39}{83}\right) &= \left(\frac{3}{83}\right) \cdot \left(\frac{13}{83}\right) \quad \text{by Theorem 11.3 (C)} \\
&= -\left(\frac{83}{3}\right) \cdot \left(\frac{83}{13}\right) \quad \text{by Theorem 11.4} \\
&= -\left(\frac{2}{3}\right) \cdot \left(\frac{5}{13}\right) \quad \text{by Theorem 11.3 (A)} \\
&= \left(\frac{13}{5}\right) \quad \text{by Theorem 11.4 and Theorem 11.6} \\
&= \left(\frac{3}{5}\right) \text{by Theorem 11.3 (A)} \\
&= -1
\end{aligned}$$

Theorem : Gauss's Lemma (12.1)

Suppose that p is an odd prime, $(a, p) = 1$, and there are among the least residues modulo p of

$$a, \qquad 2a, \qquad 3a, \qquad \ldots, \qquad \frac{p-1}{2} \cdot a$$

Exactly g that are strictly greater than $\frac{p-1}{2}$. Then,

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

Proof. Let $r_1, r_2, \ldots, r_k$ denote the least residues of p

$$a, \qquad 2a, \qquad 3a, \qquad \ldots, \qquad \frac{p-1}{2} \cdot a$$

That are less than or equal to $\frac{p-1}{2}$. Then, let $s_1, s_2, \ldots, s_g$ denote those that are greater than $\frac{p-1}{2}$. Note that no two of the r's are congruence modulo p. Suppose that two were. Then, we would have for some k_1 and k_2 that

$$k_1 a \equiv k_2 a \mod p, \qquad 0 \leq k_1, k_2 \leq \frac{p-1}{2}$$

Since $(a, p) = 1$, it follows that $k_1 = k_2$. For the same reason, no two of the s's are congruent modulo p. Now, consider the set of numbers

$$r_1, \quad r_2, \quad \ldots, r_k, \quad p - s_1, \quad p - s_2, \quad \ldots, \quad p - s_g$$

Each integer n in the set satisfies $1 \leq n \leq \frac{p-1}{2}$ and there are $\frac{p-1}{2}$ elements in the set.

Suppose that for some i and j that we have

$$\begin{aligned} r_i &\equiv p - s_j \mod p \\ r_i + s_j &\equiv 0 \mod p \end{aligned}$$

Note that $r_i \equiv ta \mod p$ and $s_j \equiv ua \mod p$ for some t and u with

$$1 \leq t, u \leq \frac{p-1}{2}$$

Therefore, we would have that

$$\begin{aligned} (t+u)\, a &\equiv 0 \mod p \\ t + u &\equiv 0 \mod p \end{aligned}$$

This is impossible since $2 \leq t + u \leq p - 1$. Thus, all the elements in the following set are distinct

$$r_1, \quad r_2, \quad \ldots, r_k, \quad p - s_1, \quad p - s_2, \quad \ldots, \quad p - s_g$$

Consequently, the elements are a rearrangement of the elements in

$$1, \qquad 2, \qquad \ldots, \qquad \frac{p-1}{2}$$

Therefore, we have that

$$\begin{aligned} r_1 r_2 \cdots r_k\, (p - s_1) \cdots (p - s_g) &\equiv 1 \times 2 \times \cdots \times \frac{p-1}{2} \mod p \\ (-1)^g\, r_1 r_2 \cdots r_k \cdot s_1 s_2 \cdots s_g &\equiv \left(\frac{p-1}{2}\right)! \mod p \\ (-1)^g\, a^{\left(\frac{p-1}{2}\right)} \left(\frac{p-1}{2}\right)! &\equiv \left(\frac{p-1}{2}\right)! \mod p \end{aligned}$$

The common factor is relatively prime to p, thus

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

$\square$

Example

Determine whether $x^2 \equiv 7 \mod 23$ has a solution.

We have that $\frac{p-1}{2} = \frac{23-1}{2} = 11$. The multiples of 7 are:

$$7, 14, 21, 28, 35, 42, 49, 56, 63, 70, 77$$

These have the least residues modulo 23 of

$$7, 14, 21, 5, 12, 19, 3, 10, 17, 1, 8$$

Of these, 5 (14, 21, 12, 19, 17) are strictly larger than $\frac{p-1}{2} = 11$. Then, $(-1)^5 = -1$. Therefore, by Theorem 12.1, 7 is a quadratic nonresidue modulo 23.