신 용 수 교수지도

석사학위청구논문

A Proof of Quadratic Reciprocity Law and its applications

2010

성신여자대학교 교육대학원

교육학과 수학교육전공

태 희 정

A Proof of Quadratic Reciprocity Law and its applications

신 용 수 교수지도

이 논문을 석사학위논문으로 제출함.

2010년 5월

성신여자대학교 교육대학원
교육학과 수학교육전공
태 희 정

인 준 서

태희정의 석사학위 논문으로 인준함.

심사위원 윤 기 헌 印

심사위원 신 용 수 印

심사위원 정 해 남 印

성신여자대학교 교육대학원

논 문 개 요

p가 홀수인 소수이고, a는 p와 서로소인 정수일 때, Legendre symbol 즉, $\left(\frac{a}{p}\right)$을 정의할 수 있다. 또한 $(-1)^{\frac{q-1}{2}}\left(\frac{q}{p}\right)$과 $(-1)^{\frac{p-1}{2}}\left(\frac{p}{q}\right)$가 같아지는 경우가 존재하는데 이러한 경우는 위의 두 식이 modulo pq에 대해 ± 1이 되는 경우이다. 그리고 이것은 p와 q가 모두 modulo 4에 대해 1이 되는 경우뿐이다.

이 논문에서는 Theorem과 Lemma를 사용하여 여러 가지 증명이 소개된 Quadratic Reciprocity Law를 새롭게 상세 증명하고, 이와 관련된 몇 가지 예제를 제시하였다.

목 차

1. **Introduction**

Let p be an odd prime number and $a \in \mathbb{Z}$ such that $(a, p) = 1$ where $\mathbb{Z}$ is the set of all integers. Then we define the Legendre symbol as

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if the congruence } x^2 \equiv a \pmod{p} \text{ has a solution,} \\ -1 & \text{otherwise.} \end{cases}$$

We say that a is ***a quadratic residue modulo*** p when $\left(\frac{a}{p}\right) = 1$. Otherwise, a is called ***a quadratic nonresidue***.

It is well-known that

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

which is called Euler's criterian ([3]).

Moreover, the following theorem:

Theorem 1.1. (Quadratic Reciprocity Law) *If p and q are distinct odd prime numbers, then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

has been proved by C.F. Gauss in ([1]).

Since then, more than 190 proofs have been announced (see [4]). In ([2]), Kim also proved this theorem.

In this thesis, we prove this result based on the ideas in ([2]).

2. **Quadratic Reciprocity Law**

Define a set Φ by

$$\Phi = \left\{ a : 1 \leq a \leq \frac{pq-1}{2},\ \gcd(a,\, pq) = 1 \right\},$$

and then let

$$A = \prod_{a \in \Phi} a.$$

Theorem 2.1 (Theorem11.3 (Euler's Criterion), [3])**.** *Let p be an odd prome and let a be a positive integer not divisible by p. Then*

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

Theorem 2.2 (Theorem6.1 (Wilson's Theorem), [3])**.** *If p is prime, then*

$$(p-1)! \equiv -1 \pmod{p}.$$

Lemma 2.3. $A \equiv (-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \pmod{p}$ *and* $A \equiv (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) \pmod{q}$.

Proof. Set

$$S = \left\{ a : 1 \leq a \leq \frac{pq-1}{2},\ \gcd(a,\, p) = 1 \right\}, \quad T = \left\{ q \cdot 1, \cdots, q \cdot \frac{p-1}{2} \right\}.$$

Note that, for every $1 \leq i \leq \frac{p-1}{2}$,

$$(p, i) = 1 \Rightarrow (p, qi) = 1 \qquad (\because (p, q) = 1).$$

Moreover, since

$$\begin{aligned}\frac{pq-1}{2} - q\cdot i &= \frac{(pq-1)-q\cdot 2i}{2} \\ &\geq \frac{(pq-1)-q\cdot(p-1)}{2} \qquad \left(\because 1 \leq i \leq \frac{p-1}{2}\right) \\ &= \frac{q-1}{2} \\ &> 0,\end{aligned}$$

we have

$$qi < \frac{pq-1}{2},$$

for such i, that is,

$$T \subseteq S.$$

For every element $qi \in T$, since $1 \leq i \leq \frac{p-1}{2}$, i.e., $(i,p)=1$,

we have

$$(qi, pq) = q \neq 1,$$

and so,

$$T \cap \Phi = \varnothing.$$

Hence

$$T \subset S - \Phi.$$

Conversely, for every $a \in S-\Phi$, we have

$$(a,p) = 1 \qquad (\because a \in S), \text{ and}$$

$$(a,pq) \neq 1 \qquad (\because a \notin \Phi).$$

Thus $(a, pq) = q$, that is, $q \mid a$ and $a = qi$ for some $i \in \mathbb{Z}$.

Furthermore, since

$$\begin{aligned}\frac{pq-1}{2} &= q \cdot \frac{p-1}{2} + \frac{q-1}{2} \\ &< q \cdot \frac{p-1}{2} + q \qquad \left(\because q - \frac{q-1}{2} = \frac{q+1}{2} > 0\right) \\ &= q \cdot \frac{p+1}{2},\end{aligned}$$

we see that $a = qi$ and $1 \leq i \leq \frac{p-1}{2}$, that is, $a \in T$, as we wanted.

In other words, $T = S - \Phi$, and $S = T \dot{\cup} \Phi$ is a disjoint union of T and Φ.

Thus, by Theorem 2.1,

$$\begin{aligned}\prod_{a \in S} a &= \prod_{a \in T} a \cdot \prod_{a \in \Phi} a \\ &= \left[q^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!\right] \cdot A \qquad (2.1) \\ &\equiv \left(\frac{q}{p}\right) \left(\frac{p-1}{2}\right)! \cdot A \pmod{p}.\end{aligned}$$

Note that

$$(aq + r, a) = (a, r)$$

for every integers a, q, and r in $\mathbb{Z}$. Hence

$$(i + p \cdot k, p) = (i, p) = 1$$

for any $i = 1, 2, \ldots, p-1$ and $k \in \mathbb{Z}$. Moreover, note that

for any $k \in \mathbb{Z}$

$$(1 + pk)(2 + pk) \cdots ((p-1) + pk)$$

$$\equiv (p-1)! \pmod{p}.$$

On the other hand, since

$$\frac{pq-1}{2} = \frac{q-1}{2} \cdot p + \frac{p-1}{2},$$

and

$$\begin{array}{lllll}
1, & 2, & \cdots, & p-1, & p, \\
1+p, & 2+p, & \cdots, & (p-1)+p, & 2p, \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
1+\frac{q-3}{2}p, & 2+\frac{q-3}{2}p, & \cdots, & (p-1)+\frac{q-3}{2}p, & \frac{q-1}{2}p, \\
1+\frac{q-1}{2}p, & 2+\frac{q-1}{2}p, & \cdots, & \frac{p-1}{2}+\frac{q-1}{2}p, &
\end{array}$$

we have

$$\begin{aligned}
\prod_{a\in S} a = (p-1)!\times & \\
& (1+p)\cdots((p-1)+p)\times\cdots\times \\
& \left(1+\left(\frac{q-3}{2}\right)p\right)\times\cdots\times\left((p-1)+\left(\frac{q-3}{2}\right)p\right)\times \\
& \left(1+\left(\frac{q-1}{2}\right)p\right)\times\cdots\times\left(\left(\frac{p-1}{2}\right)+\left(\frac{q-1}{2}\right)p\right) \qquad (2.2)\\
& \equiv [(p-1)!]^{\frac{q-1}{2}}\left(\frac{p-1}{2}\right)! \pmod p \\
& \equiv (-1)^{\frac{q-1}{2}}\left(\frac{p-1}{2}\right)! \pmod p \qquad (\because \text{Theorem 2.2}).
\end{aligned}$$

It follows from equations (2.1) and (2.2) that

$$\left(\frac{q}{p}\right)\left(\frac{p-1}{2}\right)!\cdot A \equiv (-1)^{\frac{q-1}{2}}\left(\frac{p-1}{2}\right)! \pmod p. \qquad (2.3)$$

Since $\left(\left(\frac{p-1}{2}\right)!, p\right) = 1$, we can rewrite equation (2.3)

as

$$\left(\frac{q}{p}\right)\cdot A \equiv (-1)^{\frac{q-1}{2}} \pmod p,$$

which follows that

$$A \equiv \left(\frac{q}{p}\right)(-1)^{\frac{q-1}{2}} \pmod{p}. \tag{2.4}$$

Since equation (2.4) holds for any distinct primes,

$$A \equiv \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}} \pmod{q}$$

holds, which completes the proof. □

Remark 2.4. It follows from Lemma 2.3 that

$$\begin{aligned}
&(-1)^{\frac{q-1}{2}}\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{q}\right) = \pm 1 \\
&\Leftrightarrow \begin{cases} A \equiv 1 \pmod{p} \\ A \equiv 1 \pmod{q} \end{cases} \quad \text{or} \quad \begin{cases} A \equiv -1 \pmod{p} \\ A \equiv -1 \pmod{q} \end{cases} \\
&\Leftrightarrow \quad A \equiv 1 \text{ or } -1 \pmod{pq}.
\end{aligned}$$

Theorem 2.5 (Theorem4.12 (Chinese Remainder Theorem), [3])**.** *Let $m_1, m_2, \cdots, m_r$ be pairwise relatively prime positive integers. Then the system of congruences*

$$\begin{aligned}
x &\equiv a_1 \pmod{m_1}, \\
x &\equiv a_2 \pmod{m_2}, \\
&\vdots \\
x &\equiv a_r \pmod{m_r},
\end{aligned}$$

has a unique solution modulo $M = m_1 m_2 \cdots m_r$.

Theorem 2.6 (Theorem 4.11, [3])**.** *Let p be prime. The positive integer a is its own inverse modulo p if and only if $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$.*

Lemma 2.7. *If p is an odd prime and a is a positive integer not divisible by p, then the congruence $x^2 \equiv a \pmod{p}$ has either no solution or exactly two incongruent solutions.*

Proof. Assume $x^2 \equiv a \pmod{p}$ has a solution $x \equiv \alpha \pmod{p}$ for some $\alpha \in \mathbb{Z}$.

Let $x \equiv \beta \pmod{p}$ be another solution of the system.

Then

$$x^2 \equiv \alpha^2 \equiv \beta^2 \equiv a \pmod{p}$$

$$\Rightarrow p \mid (\alpha^2 - \beta^2)$$

$$\Rightarrow p \mid (\alpha - \beta) \qquad \text{or} \qquad p \mid (\alpha + \beta).$$

In other words,

$$\alpha \equiv \pm\beta \pmod{p}.$$

Now suppose

$$\beta \equiv -\beta \pmod{p}.$$

Then

$$p \mid \beta - (-\beta) = 2\beta$$

$$\Rightarrow p \mid \beta \qquad (\because\ (p, 2) = 1)$$

$$\Rightarrow p \mid a \qquad (\because\ \beta^2 \equiv a \pmod{p}),$$

which is a contradiction.

Therefore $x^2 \equiv a \pmod{p}$ has two incongruent solutions

$$x^2 \equiv \pm\alpha \pmod{p},$$

which completes proof. □

Lemma 2.8. *$A \equiv 1$ or $-1 \pmod{pq}$ if and only if $p \equiv q \equiv 1 \pmod{4}$.*

Proof. It follows from Lemma 2.7 that

$$x^2 \equiv 1 \pmod{p}$$

and

$$x^2 \equiv 1 \pmod{q}$$

have two distinct solutions $x \equiv \pm 1 \pmod{p}$ and $x \equiv \pm 1 \pmod{q}$, respectively.

Hence, by Theorem 2.5 and Lemma 2.7,

$$x^2 \equiv 1 \pmod{pq}$$

has four incongruent solutions, let $x \equiv 1,\ -1,\ N,\ -N \pmod{pq}$.

Without loss of generality, we may assume

$$1 < N < \frac{pq-1}{2}.$$

Moreover, by Theorem 2.1 and Theorem 2.5, the following congruence

$$x^2 \equiv -1 \pmod{pq}$$

has four incongruent solutions if and only if

$$x^2 \equiv -1 \pmod{p} \quad \text{and}$$

$$x^2 \equiv -1 \pmod{q}$$

have two incongruent solutions, respectively if and only if

$$p \equiv q \equiv 1 \pmod{4}.$$

Let $x \equiv \alpha \pmod{pq}$ be a solution of $x^2 \equiv -1 \pmod{pq}$ for some $\alpha \in \mathbb{Z}$.

Note that

$$\alpha^2 \equiv (-\alpha)^2 \equiv -1 \pmod{pq} \quad \text{and}$$

$$(\alpha N)^2 \equiv (-\alpha N)^2 \equiv \alpha^2 N^2 \equiv \alpha^2 \equiv -1 \pmod{pq}.$$

Hence $x \equiv \pm\alpha, \pm\alpha N \pmod{pq}$ are all solutions of $x^2 \equiv -1 \pmod{pq}$.

In fact, without loss of generality, we may assume

$$1 < \alpha < \frac{pq-1}{2}.$$

Note that

$$1 < \alpha N < \frac{pq-1}{2} \quad \text{or}$$

$$\frac{pq-1}{2} < \alpha N < pq - 1.$$

Furthermore, by Lemma 2.7, $\alpha \not\equiv -\alpha \pmod{pq}$ and $\alpha N \not\equiv -\alpha N \pmod{pq}$.

Assume $\alpha \equiv \pm\alpha N \pmod{pq}$. Then $N \equiv \pm 1 \pmod{pq}$ since $(\alpha, pq) = 1$, which is a contradiction.

Thus $x \equiv \pm\alpha, \pm\alpha N \pmod{pq}$ are four incongruent solutions of

$$x^2 \equiv -1 \pmod{pq}.$$

Recall $\Phi = \left\{ a \in \mathbb{Z} \mid 1 \leq a \leq \frac{pq-1}{2}, (a, pq) = 1 \right\}$.

Then for any $a \in \Phi$, there exists integers $a', a'' \in \mathbb{Z}$ such that $aa' \equiv 1 \pmod{pq}$ and $aa'' \equiv -1 \pmod{pq}$ respectively.

Note that for any $a \in \Phi$, there exists unique $a' \in \{a' \in \mathbb{Z} \mid 1 \leq a \leq pq-1, (a, pq) = 1\}$ such that $aa' \equiv 1$ or $-1 \pmod{pq}$, respectively.

Assume $\frac{pq-1}{2} < a' \leq pq - 1$ and let $a'' = pq - a'$.

Then,

$$-pq + 1 \leq -a' < -\frac{pq-1}{2} \Rightarrow 1 \leq pq - a' < \frac{pq+1}{2} \Rightarrow 1 \leq a'' \leq \frac{pq-1}{2}.$$

In other words, if $aa' \equiv 1 \pmod{pq}$ and $\frac{pq-1}{2} < a' \leq pq - 1$, then there exists an integer $a'' \in \mathbb{Z}$ such that

$$aa'' \equiv -1 \pmod{pq}$$

and

$$1 \leq a'' \leq \frac{pq-1}{2}.$$

Similarly, one can show that if $aa' \equiv -1 \pmod{pq}$ and $\frac{pq-1}{2} \leq a' < pq-1$, then there exists an integer $a'' \in \mathbb{Z}$ such that

$$aa'' \equiv 1 \pmod{pq}$$

and

$$1 \leq a'' \leq \frac{pq-1}{2}.$$

Thus, for each a in Φ, there exist unique $a' \in \Phi$ such that

$$aa' \equiv 1 \text{ or } -1 \pmod{pq},$$

and hence the correspondence $a \mapsto a'$ is a permutation of Φ.

Writing

$$\Psi = \{a \in \Phi : a = a'\} = \{a \in \Phi : a^2 \equiv \pm 1 \pmod{pq}\}.$$

Then, $\prod_{a \in \Phi - \Psi} a \equiv \pm 1 \pmod{pq}$,

and hence

$$\begin{aligned} A &= \prod_{a \in \Phi} a \\ &= \left(\prod_{a \in \Psi} a \right) \left(\prod_{a \in \Phi - \Psi} a \right) \\ &\equiv \pm \left(\prod_{a \in \Psi} a \right) \pmod{pq}. \end{aligned}$$

Note that, by Theorem 2.1 $p \not\equiv 1$ or $q \not\equiv 1 \pmod 4$, then $a^2 \not\equiv -1 \pmod{pq}$ for every $a \in \mathbb{Z}$ with $(a, pq) = 1$. Hence, we have $\Psi = \{1, N\}$, and so

$$\begin{aligned} A &\equiv \prod_{a\in\Phi} a \equiv \pm \prod_{a\in\Psi} a \pmod{pq} \\ &\equiv \pm(1\cdot N) \pmod{pq} \\ &\equiv \pm N \neq \pm 1 \pmod{pq} \qquad \left(\because \left(\frac{-1}{pq}\right) = -1\right), \end{aligned}$$

which follows that $p \equiv q \equiv 1 \pmod 4$.

Thus if $A \equiv \pm 1 \pmod{pq}$, then, by Theorem 2.1, -1 is a quadratic residue modulo p and q, respectively.

Conversely, assume $p \equiv q \equiv 1 \pmod 4$. Note that $\left(\frac{1}{p}\right) = \left(\frac{-1}{p}\right) = 1$.

$$\begin{aligned} A &\equiv \prod_{a\in\Phi} a \equiv \pm \prod_{a\in\Psi} a \pmod{pq} \\ &\equiv \pm(1\cdot N)(\alpha\cdot \alpha N) \quad \text{or} \\ &\equiv \pm(1\cdot N)(\alpha\cdot -\alpha N) \\ &\equiv \pm(1\cdot N\cdot \alpha\cdot \alpha N) \\ &\equiv \pm 1 \pmod{pq}, \end{aligned}$$

which completes the proof. □

Proof of Theorem 1.1. By Remark 2.4 and Lemma 2.8, $p \equiv q \equiv 1$ if and only if

$$(-1)^{\frac{q-1}{2}}\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{q}\right),$$

and hence

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

In other words, either $p \equiv 3 \pmod 4$ or $q \equiv 3 \pmod 4$ if and only

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

Note that there are four possibilities for (p, q) as $(1, 1), (1, -1), (-1, 1)$, and $(-1, -1)$.

First assume $(p, q) = (1, 1)$, that is, $p \equiv q \equiv 1 \pmod 4$.

Then we have

$$\begin{aligned}
\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) &= (-1)^{\frac{p-1}{2}}(-1)^{\frac{q-1}{2}} \\
&= 1 && \left(\because 2 \mid \left(\tfrac{p-1}{2}\right), 2 \mid \left(\tfrac{q-1}{2}\right)\right) \\
&= \left((-1)^{\frac{p-1}{2}}\right)^{\frac{q-1}{2}} && \left(\because 2 \mid \left(\tfrac{p-1}{2}\right), 2 \mid \left(\tfrac{q-1}{2}\right)\right) \\
&= (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.
\end{aligned}$$

Now assume either $p \equiv 3 \pmod 4$ or $q \equiv 3 \pmod 4$. If $p \equiv 3 \pmod 4$, $q \equiv 1 \pmod 4$, then

$$(-1)^{\frac{p-1}{2}}\left(\frac{p}{q}\right) = (-1)(-1)^{\frac{q-1}{2}}\left(\frac{q}{p}\right)$$

and so

$$\begin{aligned}
\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) &= (-1)(-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{q-1}{2}} \\
&= (-1)^{\frac{p+1}{2}} \cdot (-1)^{\frac{q-1}{2}} \\
&= 1 \times 1 && \left(\because 2 \mid \left(\tfrac{p+1}{2}\right) \text{ and } 2 \mid \left(\tfrac{q-1}{2}\right)\right) \\
&= 1 \\
&= \left((-1)^{\frac{p-1}{2}}\right)^{\frac{q-1}{2}} && \left(\because 2 \mid \left(\tfrac{q-1}{2}\right)\right) \\
&= (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.
\end{aligned}$$

Using the same idea as before, if $p \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 4$, then one can show that

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1 = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Now Suppose $p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$. Then

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

Hence

$$\begin{aligned} \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) &= (-1)(-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{q-1}{2}} \\ &= -1 && \left(\because 2 \nmid \left(\tfrac{p-1}{2}\right), 2 \nmid \left(\tfrac{q-1}{2}\right)\right) \\ &= \left((-1)^{\frac{p-1}{2}}\right)^{\frac{q-1}{2}} && \left(\because 2 \nmid \left(\tfrac{p-1}{2}\right), 2 \nmid \left(\tfrac{q-1}{2}\right)\right) \\ &= (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}, \end{aligned}$$

which completes the proof.

□

3. **Some Examples**

In this section, with notation as in the proofs of Lemma 2.3 and 2.8, we shall give some examples which show that both

$$A \equiv 1 \pmod{pq} \quad \text{and} \quad A \equiv -1 \pmod{pq}$$

can occur for some primes p and q.

The following two Examples 3.1 and 3.2 are about the case $p \equiv q \equiv 1 \pmod 4$.

Example 3.1.

$$x^2 \equiv 1 \pmod{5 \cdot 13}.$$

Note that $5 \equiv 13 \equiv 1 \pmod 4$. Because $65 = 5 \cdot 13$, to find the four incongruent solutions we solve the congruences

$$x^2 \equiv 1 \pmod 5 \quad \text{and} \quad x^2 \equiv 1 \pmod{13}.$$

The solutions of these congruences are

$$x \equiv \pm 1 \pmod 5 \quad \text{and} \quad x \equiv \pm 1 \pmod{13}.$$

Using Theorem 2.5, we have $M = 5 \cdot 13 = 65$, $M_1 = 65/5 = 13$, and $M_2 = 65/13 = 5$. To determine y_1, we solve $13y_1 \equiv 1 \pmod 5$, or equivalently, $3y_1 \equiv 1 \pmod 5$. This yields $y_1 \equiv 2 \pmod 5$. We find y_2 by solving $5y_2 \equiv 1 \pmod{13}$; this gives $y_2 \equiv -5 \equiv 8 \pmod{13}$.

Case 1. $x \equiv 1 \pmod 5, \qquad x \equiv 1 \pmod{13}.$

$$\begin{aligned} x &\equiv 1 \cdot 13 \cdot 2 + 1 \cdot 5 \cdot 8 \\ &\equiv 66 \equiv 1 \pmod{65}. \end{aligned}$$

Case 2. $x \equiv 1 \pmod 5, \qquad x \equiv -1 \pmod{13}.$

$$\begin{aligned} x &\equiv 1 \cdot 13 \cdot 2 + (-1) \cdot 5 \cdot 8 \\ &\equiv -14 \pmod{65}. \end{aligned}$$

Case 3. $x \equiv -1 \pmod 5, \qquad x \equiv 1 \pmod{13}.$

$$\begin{aligned} x &\equiv (-1) \cdot 13 \cdot 2 + 1 \cdot 5 \cdot 8 \\ &\equiv 14 \pmod{65}. \end{aligned}$$

Case 4. $x \equiv -1 \pmod 5, \qquad x \equiv -1 \pmod{13}.$

$$\begin{aligned} x &\equiv (-1)\cdot 13 \cdot 2 + (-1)\cdot 5 \cdot 8 \\ &\equiv -66 \equiv -1 \pmod{65}. \end{aligned}$$

From Cases $1 \sim 4$ we obtain four incongruent solutions as follows, i.e.,

$$x = \pm 1,\ \pm 14 \pmod{65}.$$

Now consider the following quadratic congruence:

$$x^2 \equiv -1 \pmod{5 \cdot 13}.$$

To find the four incongruent solutions we solve the congruences

$$x^2 \equiv -1 \equiv 4 \pmod 5 \quad \text{and} \quad x^2 \equiv -1 \equiv 12 \pmod{13}.$$

The solutions of these congruences are

$$x \equiv \pm 2 \pmod 5 \quad \text{and} \quad x \equiv \pm 5 \pmod{13}.$$

Using the same M, M_1, M_2, y_1, and y_2 as above, one can obtain four incongruent solutions as the follows, i.e.,

$$x = \pm 8,\ \pm 18 \pmod{65}.$$

$$\begin{aligned} \Phi &= \{a \in \mathbb{Z} \mid 1 \le a \le 32, (a, 65) = 1\} \\ &= \{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 14, 16, 17, \\ &\qquad 18, 19, 21, 22, 23, 24, 27, 28, 29, 31, 32\}. \end{aligned}$$

If $aa' \equiv 1 \pmod{65}$ and $1 \le a' \le 32$, then there exists an integer $a'' \in \mathbb{Z}$ such that $aa'' \equiv -1 \pmod{65}$ and $32 \le a'' \le 64$, or vice versa.

a	1	2	3	4	6	7	8	9	11	12	14	16
a'	1	33	22	49	11	28	57	29	6	38	14	61
a''	64	32	43	16	54	37	8	36	59	27	51	4
a	17	18	19	21	22	23	24	27	28	29	31	32
a'	23	47	41	31	3	17	19	53	7	9	21	63
a''	42	18	24	34	62	48	46	12	58	56	44	2

TABLE 1

It is from Table 1 that

$$\begin{aligned}\Psi &= \{a \in \Phi : a = a'\} \\ &= \{a \in \Phi : a^2 \equiv \pm 1 \pmod{65}\} \\ &= \{1, 8, 14, 18\}.\end{aligned}$$

Hence,

$$\begin{aligned}\prod_{a \in \Phi - \Psi} a &\equiv 2 \cdot 3 \cdot 4 \cdot 6 \cdot 7 \cdot 9 \cdot 11 \cdot 12 \cdot 16 \cdot 17 \cdot 19 \cdot \\ &\quad 21 \cdot 22 \cdot 23 \cdot 24 \cdot 27 \cdot 28 \cdot 29 \cdot 31 \cdot 32 \\ &\equiv -1 \pmod{65},\end{aligned}$$

and so

$$\begin{aligned}A &= \prod_{a \in \Phi} a \\ &= \left(\prod_{a \in \Psi} a\right)\left(\prod_{a \in \Phi - \Psi} a\right) \\ &\equiv -\left(\prod_{a \in \Psi} a\right) \\ &\equiv -(1 \cdot 8 \cdot 14 \cdot 18) \\ &\equiv -2016 \\ &\equiv -1 \pmod{65}.\end{aligned}$$

Example 3.2. Now consider the following quadratic congruence:

$$x^2 \equiv 1 \pmod{13 \cdot 17}.$$

Note that $13 \equiv 17 \equiv 1 \pmod 4$. Because $221 = 13 \cdot 17$, to find the four incongruent solutions we solve the congruences

$$x^2 \equiv 1 \pmod{13} \quad \text{and} \quad x^2 \equiv 1 \pmod{17}.$$

The solutions of these congruences are

$$x \equiv \pm 1 \pmod{13} \quad \text{and} \quad x \equiv \pm 1 \pmod{17}.$$

Using Theorem 2.5, we have $M = 13 \cdot 17 = 221$, $M_1 = 221/13 = 17$, and $M_2 = 221/17 = 13$ To determine y_1, we solve $17y_1 \equiv 1 \pmod{13}$, or equivalently, $4y_1 \equiv 1 \pmod{13}$. This yields $y_1 \equiv 10 \pmod{13}$. We find y_2 by solving $13y_2 \equiv 1 \pmod{17}$; this gives $y_2 \equiv 4 \pmod{17}$.

Case 1. $x \equiv 1 \pmod{13}, \qquad x \equiv 1 \pmod{17}.$

$$\begin{aligned} x &\equiv 1 \cdot 17 \cdot 10 + 1 \cdot 13 \cdot 4 \\ &\equiv 222 \\ &\equiv 1 \pmod{221}. \end{aligned}$$

Case 2. $x \equiv 1 \pmod{13}, \qquad x \equiv -1 \pmod{17}.$

$$\begin{aligned} x &\equiv 1 \cdot 17 \cdot 10 + (-1) \cdot 13 \cdot 4 \\ &\equiv 118 \equiv -103 \pmod{221}. \end{aligned}$$

Case 3. $x \equiv -1 \pmod{13}, \qquad x \equiv 1 \pmod{17}.$

$$\begin{aligned} x &\equiv (-1) \cdot 17 \cdot 10 + 1 \cdot 13 \cdot 4 \\ &\equiv -118 \equiv 103 \pmod{221}. \end{aligned}$$

Case 4. $x \equiv -1 \pmod{13}, \qquad x \equiv -1 \pmod{17}.$

$$\begin{aligned} x &\equiv (-1) \cdot 17 \cdot 10 + (-1) \cdot 13 \cdot 4 \\ &\equiv -222 \equiv -1 \pmod{221}. \end{aligned}$$

From Cases $1 \sim 4$, we obtain four incongruent solutions as follows, i.e.,

$$x = \pm 1, \ \pm 103 \pmod{221}.$$

Now consider the following quadratic congruence:

$$x^2 \equiv -1 \pmod{13 \cdot 17}.$$

To find the four incongruent solutions we solve the congruences

$$x^2 \equiv -1 \equiv 12 \pmod{13} \quad \text{and} \quad x^2 \equiv -1 \equiv 16 \pmod{17}.$$

The solutions of these congruences are

$$x \equiv \pm 5 \pmod{13} \quad \text{and} \quad x \equiv \pm 4 \pmod{17}.$$

Using the same M, M_1, M_2, y_1, and y_2 as above, one can obtain four incongruent solutions as the follows, i.e.,

$$x = \pm 21, \ \pm 47 \pmod{221}.$$

$$\begin{aligned}\Phi =& \{a \in \mathbb{Z} \mid 1 \le a \le 110, (a, 221) = 1\} \\ =& \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 14, 15, 16, 18, 19, 20, \\ & 21, 22, 23, 24, 25, 27, 28, 29, 30, 31, 32, 33, 35, 36, 37, 38, 40, \\ & 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 53, 54, 55, 56, 57, 58, 59, 60, \\ & 61, 62, 63, 64, 66, 67, 69, 70, 71, 72, 73, 74, 75, 76, 77, 79, 80, \\ & 81, 82, 83, 84, 86, 87, 88, 89, 90, 92, 93, 94, 95, 96, 97, 98, 99, 100, \\ & 101, 103, 105, 106, 107, 108, 109, 110\}.\end{aligned}$$

If $aa' \equiv 1 \pmod{221}$ and $1 \le a' \le 110$, then there exists an integer $a'' \in \mathbb{Z}$ such that $aa'' \equiv -1 \pmod{221}$ and $110 \le a'' \le 220$, or vice versa.

It is from Table 2 that

$$\begin{aligned}\Psi &= \{a \in \Phi : a = a'\} \\ &= \{a \in \Phi : a^2 \equiv \pm 1 \pmod{221}\} \\ &= \{1, 21, 47, 103\}.\end{aligned}$$

a	1	2	3	4	5	6	7	8	9	10	11	12
a'	1	111	74	166	177	37	158	83	172	199	201	129
a''	220	110	147	55	44	184	63	138	49	22	20	92
a	14	15	16	18	19	20	21	22	23	24	25	27
a'	79	59	152	86	128	11	200	211	173	175	168	131
a''	142	162	69	135	93	210	21	10	48	46	53	90
a	28	29	30	31	32	33	35	36	37	38	40	41
a'	150	61	140	164	76	67	120	43	6	35	105	124
a''	71	160	81	57	145	154	101	178	215	186	116	97
a	42	43	44	45	46	47	48	49	50	53	54	55
a'	100	36	216	167	197	174	198	212	84	196	176	217
a''	121	185	5	54	24	47	23	9	137	25	45	4
a	56	57	58	59	60	61	62	63	64	66	67	69
a'	75	190	141	15	70	29	82	214	38	144	33	205
a''	146	31	80	206	151	192	139	7	183	77	188	16
a	70	71	72	73	74	75	76	77	79	80	81	82
a'	60	193	132	109	4	165	32	155	14	163	191	62
a''	161	28	89	112	217	56	189	66	207	58	30	159
a	83	84	86	87	88	89	90	92	93	94	95	96
a'	8	50	18	47	108	149	194	209	202	87	114	99
a''	213	171	203	174	113	72	27	12	19	134	107	122
a	97	98	99	100	101	103	105	106	107	108	109	110
a'	180	106	96	42	186	103	40	98	126	88	73	219
a''	41	115	125	179	35	118	181	123	95	133	148	2

TABLE 2

Hence,

$$\begin{aligned}\prod_{a\in\Phi-\Psi} a \equiv\ & 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7\cdot 8\cdot 9\cdot 10\cdot 11\cdot 12\cdot 14\cdot 15\cdot 16\cdot\\ & 18\cdot 19\cdot 20\cdot 22\cdot 23\cdot 24\cdot 25\cdot 27\cdot 28\cdot 29\cdot 30\cdot 31\cdot 32\cdot 33\cdot\\ & 35\cdot 36\cdot 37\cdot 38\cdot 40\cdot 41\cdot 42\cdot 43\cdot 44\cdot 45\cdot 46\cdot 48\cdot 49\cdot 50\cdot\\ & 53\cdot 54\cdot 55\cdot 56\cdot 57\cdot 58\cdot 59\cdot 60\cdot 61\cdot 62\cdot 63\cdot 64\cdot 66\cdot 67\cdot\\ & 69\cdot 70\cdot 71\cdot 72\cdot 73\cdot 74\cdot 75\cdot 76\cdot 77\cdot 79\cdot 80\cdot 81\cdot 82\cdot 83\cdot\\ & 84\cdot 86\cdot 87\cdot 88\cdot 89\cdot 90\cdot 92\cdot 93\cdot 94\cdot 95\cdot 96\cdot 97\cdot 98\cdot 99\cdot\\ & 100\cdot 101\cdot 105\cdot 106\cdot 107\cdot 108\cdot 109\cdot 110\\ \equiv\ & 1 \pmod{221},\end{aligned}$$

and thus

$$\begin{aligned} A &= \prod_{a\in\Phi} a \\ &= \left(\prod_{a\in\Psi} a\right)\left(\prod_{a\in\Phi-\Psi} a\right) \\ &\equiv \left(\prod_{a\in\Psi} a\right) \\ &\equiv (1\cdot 21\cdot 47\cdot 103) \\ &\equiv 101,661 \\ &\equiv 1 \pmod{221}. \end{aligned}$$

Now we shall give some different examples from Examples 3.1 and 3.2. In other worlds, we shall consider the cases either $p \not\equiv 1 \pmod 4$ or $q \not\equiv 1 \pmod 4$ in the following 4 examples.

The following two Examples 3.3 and 3.4 are about the case

$$p \equiv 1 \pmod 4, \quad \text{and} \quad q \equiv 1 \pmod 4.$$

Example 3.3. The follow example shows the case $A \equiv N \pmod{pq}$.

$$x^2 \equiv 1 \pmod{5\cdot 7}.$$

Note that $5 \equiv 1, 7 \equiv 3 \pmod 4$. Because $35 = 5\cdot 7$, to find the four incongruent solutions we solve the congruences

$$x^2 \equiv 1 \pmod 5 \quad \text{and} \quad x^2 \equiv 1 \pmod 7.$$

The solutions of these congruences are

$$x \equiv \pm 1 \pmod 5 \quad \text{and} \quad x \equiv \pm 1 \pmod 7.$$

Using Theorem 2.5, we have $M = 5 \cdot 7 = 35$, $M_1 = 35/5 = 7$, and $M_2 = 35/7 = 5$ To determine y_1, we solve $7y_1 \equiv 1 \pmod 5$, or equivalently, $2y_1 \equiv 1 \pmod 5$. This yields $y_1 \equiv -2 \equiv 3 \pmod 5$. We find y_2 by solving $5y_2 \equiv 1 \pmod 7$; this gives $y_2 \equiv 3 \pmod 7$.

Case 1. $x \equiv 1 \pmod 5, \qquad x \equiv 1 \pmod 7.$

$$\begin{aligned} x &\equiv 1 \cdot 7 \cdot 3 + 1 \cdot 5 \cdot 3 \\ &\equiv 36 \\ &\equiv 1 \pmod{35}. \end{aligned}$$

Case 2. $x \equiv 1 \pmod 5, \qquad x \equiv -1 \pmod 7.$

$$\begin{aligned} x &\equiv 1 \cdot 7 \cdot 3 + (-1) \cdot 5 \cdot 3 \\ &\equiv 6 \pmod{35}. \end{aligned}$$

Case 3. $x \equiv -1 \pmod 5, \qquad x \equiv 1 \pmod 7.$

$$\begin{aligned} x &\equiv (-1) \cdot 7 \cdot 3 + 1 \cdot 5 \cdot 3 \\ &\equiv -6 \pmod{35}. \end{aligned}$$

Case 4. $x \equiv -1 \pmod 5, \qquad x \equiv -1 \pmod 7.$

$$\begin{aligned} x &\equiv (-1) \cdot 7 \cdot 3 + (-1) \cdot 5 \cdot 3 \\ &\equiv -36 \equiv -1 \pmod{35}. \end{aligned}$$

From Cases $1 \sim 4$, we obtain two incongruent solutions as follows, i.e.,

$$x = \pm 1, \ \pm 6 \pmod{35}.$$

Now consider the following quadratic congruence:

$$x^2 \equiv -1 \pmod{5 \cdot 7}.$$

Note that $(\frac{-1}{5}) \equiv (-1)^{\frac{5-1}{2}} = 1$ and $(\frac{-1}{7}) \equiv (-1)^{\frac{7-1}{2}} = -1$. Hence $x^2 \equiv -1 \pmod 5$ has two incongruent solutions and $x^2 \equiv -1 \pmod 7$ has no solution.

The solutions of $x^2 \equiv -1 \pmod 5$ are $x \equiv \pm 2 \pmod 5$ and $x^2 \equiv -1 \pmod{35}$ has no solution.

$$\Phi = \{a \in \mathbb{Z} \mid 1 \le a \le 17, (a, 35) = 1\}$$

$$= \{1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17\}.$$

If $aa' \equiv 1 \pmod{35}$ and $1 \le a' \le 17$, then there exists an integer $a'' \in \mathbb{Z}$ such that $aa'' \equiv -1 \pmod{35}$ and $17 \le a'' \le 34$, or vice versa.

a	1	2	3	4	6	8	9	11	12	13	16	17
a'	1	18	12	9	6	22	4	16	3	27	11	33
a''	34	17	23	26	29	13	31	19	32	8	24	2

TABLE 3

It is from Table 3 that

$$\begin{aligned}\Psi =& \{a \in \Phi : a = a'\}\\ =& \{a \in \Phi : a^2 \equiv \pm 1 \pmod{35}\}\\ =& \{a \in \Phi : a^2 \equiv 1 \pmod{35}\}\\ & \left(\because \left(\frac{-1}{5}\right) = 1 \text{ and } \left(\frac{-1}{7}\right) = -1\right)\\ =& \{1, 6\}.\end{aligned}$$

Hence,

$$\begin{aligned}\prod_{a \in \Phi - \Psi} a &\equiv 2 \cdot 3 \cdot 4 \cdot 8 \cdot 9 \cdot 11 \cdot 12 \cdot 13 \cdot 16 \cdot 17\\ &\equiv 806,547,456\\ &\equiv 1 \pmod{35},\end{aligned}$$

and so

$$\begin{aligned} A &= \prod_{a\in\Phi} a \\ &= \left(\prod_{a\in\Psi} a\right)\left(\prod_{a\in\Phi-\Psi} a\right) \\ &\equiv \left(\prod_{a\in\Psi} a\right) \\ &\equiv (1\cdot 6) \\ &\equiv 6 \pmod{35}. \end{aligned}$$

Example 3.4. The follow example shows the case $A \equiv -N \pmod{pq}$.

$$x^2 \equiv 1 \pmod{5\cdot 11}.$$

Note that $5 \equiv 1, 11 \equiv 3 \pmod 4$. Because $55 = 5\cdot 11$, to find the four incongruent solutions we solve the congruences

$$x^2 \equiv 1 \pmod 5 \quad \text{and} \quad x^2 \equiv 1 \pmod{11}.$$

The solutions of these congruences are

$$x \equiv \pm 1 \pmod 5 \quad \text{and} \quad x \equiv \pm 1 \pmod{11}.$$

Using Theorem 2.5, we have $M = 5\cdot 11 = 55$, $M_1 = 55/5 = 11$, and $M_2 = 55/11 = 5$ To determine y_1, we solve $11y_1 \equiv 1 \pmod 5$, This yields $y_1 \equiv 1 \pmod 5$. We find y_2 by solving $5y_2 \equiv 1 \pmod{11}$; this gives $y_2 \equiv -2 \equiv 9 \pmod{11}$.

Case 1. $x \equiv 1 \pmod 5, \qquad x \equiv 1 \pmod{11}.$

$$\begin{aligned} x &\equiv 1 \cdot 11 \cdot 1 + 1 \cdot 5 \cdot 9 \\ &\equiv 56 \equiv 1 \pmod{55}. \end{aligned}$$

Case 2. $x \equiv 1 \pmod 5, \qquad x \equiv -1 \pmod{11}.$

$$\begin{aligned} x &\equiv 1 \cdot 11 \cdot 1 + (-1) \cdot 5 \cdot 9 \\ &\equiv -34 \equiv 21 \pmod{55}. \end{aligned}$$

Case 3. $x \equiv -1 \pmod 5, \qquad x \equiv 1 \pmod{11}.$

$$\begin{aligned} x &\equiv (-1) \cdot 11 \cdot 1 + 1 \cdot 5 \cdot 9 \\ &\equiv 34 \equiv -21 \pmod{55}. \end{aligned}$$

Case 4. $x \equiv -1 \pmod 5, \qquad x \equiv -1 \pmod{11}.$

$$\begin{aligned} x &\equiv (-1) \cdot 11 \cdot 1 + (-1) \cdot 5 \cdot 9 \\ &\equiv -56 \equiv -1 \pmod{55}. \end{aligned}$$

Now Cases $1 \sim 4$, we obtain four incongruent solutions as follows, i.e.,

$$x = \pm 1, \ \pm 21 \pmod{55}.$$

Now consider the following quadratic congruence:

$$x^2 \equiv -1 \pmod{5 \cdot 11}.$$

Note that $(\frac{-1}{5}) \equiv (-1)^{\frac{5-1}{2}} = 1$ and $(\frac{-1}{11}) \equiv (-1)^{\frac{11-1}{2}} = -1$. Hence $x^2 \equiv -1 \pmod 5$ has two incongruent solutions and $x^2 \equiv -1 \pmod{11}$ has no solution. The solution of $x^2 \equiv -1 \pmod 5$ is $x \equiv \pm 2 \pmod 5$ and $x^2 \equiv -1 \pmod{55}$ has no solution.

$$\begin{aligned} \Phi &= \{a \in \mathbb{Z} \mid 1 \le a \le 27, (a, 55) = 1\} \\ &= \{1, 2, 3, 4, 6, 7, 8, 9, 12, 13, 14, 16, 17, 18, 19, 21, 23, 24, 26, 27\}. \end{aligned}$$

If $aa' \equiv 1 \pmod{55}$ and $1 \leq a' \leq 27$, then there exists an integer $a'' \in \mathbb{Z}$ such that $aa'' \equiv -1 \pmod{55}$ and $27 \leq a'' \leq 54$, or vice versa.

a	1	2	3	4	6	7	8	9	12	13
a'	1	28	37	14	46	8	7	49	23	17
a''	54	27	18	41	9	47	48	6	32	38
a	14	16	17	18	19	21	23	24	26	27
a'	4	31	13	52	29	19	12	39	36	53
a''	51	24	42	3	26	36	43	16	19	2

TABLE 4

It is from Table 4. that

$$\begin{aligned}\Psi =&\{a \in \Phi : a = a'\}\\ =&\{a \in \Phi : a^2 \equiv \pm 1 \pmod{55}\}\\ =&\{a \in \Phi : a^2 \equiv 1 \pmod{55}\}\\ &\left(\because \left(\frac{-1}{5}\right) = 1 \text{ and } \left(\frac{-1}{11}\right) = -1\right)\\ =&\{1, 21\}.\end{aligned}$$

Hence,

$$\begin{aligned}\prod_{a \in \Phi - \Psi} a \equiv& 2 \cdot 3 \cdot 4 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 12 \cdot 13 \cdot 14 \cdot\\ & 16 \cdot 17 \cdot 18 \cdot 19 \cdot 23 \cdot 24 \cdot 26 \cdot 27\\ \equiv& -1 \pmod{55},\end{aligned}$$

and so

$$\begin{aligned} A &= \prod_{a\in\Phi} a \\ &= \left(\prod_{a\in\Psi} a\right)\left(\prod_{a\in\Phi-\Psi} a\right) \\ &\equiv -\left(\prod_{a\in\Psi} a\right) \\ &\equiv -(1\cdot 21) \\ &\equiv -21 \pmod{55}. \end{aligned}$$

The following two Examples 3.5 and 3.6 is about the case

$$p \equiv q \equiv 3 \pmod 4.$$

Example 3.5.

$$x^2 \equiv 1 \pmod{7\cdot 11}.$$

Note that $7 \equiv 11 \equiv 3 \pmod 4$. Because $77 = 7\cdot 11$, to find the four incongruent solutions we solve the congruences

$$x^2 \equiv 1 \pmod 7 \quad \text{and} \quad x^2 \equiv 1 \pmod{11}.$$

The solutions of these congruences are

$$x \equiv \pm 1 \pmod 7 \quad \text{and} \quad x \equiv \pm 1 \pmod{11}.$$

Using Theorem 2.5, we have $M = 7\cdot 11 = 77$, $M_1 = 77/7 = 11$, and $M_2 = 77/11 = 7$ To determine y_1, we solve $11y_1 \equiv 1 \pmod 7$, or equivalently, $4y_1 \equiv 1 \pmod 7$. This yields $y_1 \equiv 2 \pmod 7$. We find y_2 by solving

$7y_2 \equiv 1 \pmod{11}$; this gives $y_2 \equiv -3 \equiv 8 \pmod{11}$.

Case 1. $x \equiv 1 \pmod 7, \qquad x \equiv 1 \pmod{11}$.

$$\begin{aligned} x &\equiv 1 \cdot 11 \cdot 2 + 1 \cdot 7 \cdot 8 \\ &\equiv 78 \equiv 1 \pmod{77}. \end{aligned}$$

Case 2. $x \equiv 1 \pmod 7, \qquad x \equiv -1 \pmod{11}$.

$$\begin{aligned} x &\equiv 1 \cdot 11 \cdot 2 + (-1) \cdot 7 \cdot 8 \\ &\equiv -34 \pmod{77}. \end{aligned}$$

Case 3. $x \equiv -1 \pmod 7, \qquad x \equiv 1 \pmod{11}$.

$$\begin{aligned} x &\equiv (-1) \cdot 11 \cdot 2 + 1 \cdot 7 \cdot 8 \\ &\equiv 34 \pmod{77}. \end{aligned}$$

Case 4. $x \equiv -1 \pmod 7, \qquad x \equiv -1 \pmod{11}$.

$$\begin{aligned} x &\equiv (-1) \cdot 11 \cdot 2 + (-1) \cdot 7 \cdot 8 \\ &\equiv -78 \equiv -1 \pmod{77}. \end{aligned}$$

From Cases $1 \sim 4$, we obtain four incongruent solutions as follows, i.e.,

$$x = \pm 1, \ \pm 34 \pmod{77}.$$

Now consider the following quadratic congruence.

$$x^2 \equiv -1 \pmod{7 \cdot 11}$$

Note that $(\frac{-1}{7}) \equiv (-1)^{\frac{7-1}{2}} = -1$ and $(\frac{-1}{11}) \equiv (-1)^{\frac{11-1}{2}} = -1$. Hence $x^2 \equiv -1 \pmod 7$ and $x^2 \equiv -1 \pmod{11}$ has no solution. Thus, $x^2 \equiv -1$

(mod 77) has no solution.

$$\begin{aligned}\Phi &= \{a \in \mathbb{Z} \mid 1 \le a \le 38, (a, 77) = 1\} \\ &= \{1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 13, 15, 16, 17, 18, 19, \\ &\qquad 20, 23, 24, 25, 26, 27, 29, 30, 31, 32, 34, 36, 37, 38\}.\end{aligned}$$

If $aa' \equiv 1 \pmod{77}$ and $1 \le a' \le 38$, then there exists an integer $a'' \in \mathbb{Z}$ such that $aa'' \equiv -1 \pmod{77}$ and $38 \le a'' \le 76$ or vice versa.

a	1	2	3	4	5	6	8	9	10	12
a'	1	39	26	58	31	13	29	60	54	45
a''	76	38	51	19	46	64	48	17	23	32
a	13	15	16	17	18	19	20	23	24	25
a'	6	36	53	68	30	73	27	67	61	37
a''	71	41	24	9	47	4	50	10	16	37
a	26	27	29	30	31	32	34	36	37	38
a'	3	20	8	18	5	65	34	15	25	75
a''	74	57	69	59	72	12	43	62	52	2

Table 5

It is from Table 5. that

$$\begin{aligned}\Psi =& \{a \in \Phi : a = a'\} \\ =& \{a \in \Phi : a^2 \equiv \pm 1 \pmod{77}\} \\ =& \{a \in \Phi : a^2 \equiv 1 \pmod{77}\} \\ & \left(\because \left(\frac{-1}{7}\right) = \left(\frac{-1}{11}\right) = -1\right) \\ =& \{1, 34\}.\end{aligned}$$

Hence,

$$\begin{aligned}\prod_{a\in\Phi-\Psi} a \equiv & 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 8\cdot 9\cdot 10\cdot 12\cdot 13\cdot \\ & 15\cdot 16\cdot 17\cdot 18\cdot 19\cdot 20\cdot 23\cdot 24\cdot 25\cdot \\ & 26\cdot 27\cdot 29\cdot 30\cdot 31\cdot 32\cdot 36\cdot 37\cdot 38 \\ \equiv & 1 \pmod{77},\end{aligned}$$

and thus

$$\begin{aligned}A &= \prod_{a\in\Phi} a \\ &= \left(\prod_{a\in\Psi} a\right)\left(\prod_{a\in\Phi-\Psi} a\right) \\ &\equiv \left(\prod_{a\in\Psi} a\right) \\ &\equiv (1\cdot 34) \\ &\equiv 34 \pmod{77}.\end{aligned}$$

Example 3.6.

$$x^2 \equiv 1 \pmod{7\cdot 19}.$$

Note that $7 \equiv 19 \equiv 3 \pmod 4$. Because $133 = 7\cdot 19$, to find the four incongruent solutions we solve the congruences

$$x^2 \equiv 1 \pmod 7 \quad \text{and} \quad x^2 \equiv 1 \pmod{19}.$$

The solutions of these congruences are

$$x \equiv \pm 1 \pmod 7 \quad \text{and} \quad x \equiv \pm 1 \pmod{19}.$$

Using Theorem 2.5, we have $M = 7 \cdot 19 = 133$, $M_1 = 133/7 = 19$, and $M_2 = 133/19 = 7$ To determine y_1, we solve $19y_1 \equiv 1 \pmod 7$, or equivalently, $5y_1 \equiv 1 \pmod 7$. This yields $y_1 \equiv 3 \pmod 7$. We find y_2 by solving $7y_2 \equiv 1 \pmod{19}$; this gives $y_2 \equiv -8 \equiv 11 \pmod{19}$.

Case 1. $x \equiv 1 \pmod 7, \qquad x \equiv 1 \pmod{19}.$

$$\begin{aligned} x &\equiv 1 \cdot 19 \cdot 3 + 1 \cdot 7 \cdot 11 \\ &\equiv 134 \equiv 1 \pmod{133}. \end{aligned}$$

Case 2. $x \equiv 1 \pmod 7, \qquad x \equiv -1 \pmod{19}.$

$$\begin{aligned} x &\equiv 1 \cdot 19 \cdot 3 + (-1) \cdot 7 \cdot 11 \\ &\equiv -20 \pmod{133}. \end{aligned}$$

Case 3. $x \equiv -1 \pmod 7, \qquad x \equiv 1 \pmod{19}.$

$$\begin{aligned} x &\equiv (-1) \cdot 19 \cdot 3 + 1 \cdot 7 \cdot 11 \\ &\equiv 20 \pmod{133}. \end{aligned}$$

Case 4. $x \equiv -1 \pmod 7, \qquad x \equiv -1 \pmod{19}.$

$$\begin{aligned} x &\equiv (-1) \cdot 19 \cdot 3 + (-1) \cdot 7 \cdot 11 \\ &\equiv -134 \equiv -1 \pmod{133}. \end{aligned}$$

From Cases $1 \sim 4$, we obtain four incongruent solutions as follows, i.e.,

$$x = \pm 1, \ \pm 20 \pmod{133}.$$

Now consider the following quadratic congruence:

$$x^2 \equiv -1 \pmod{7 \cdot 19}.$$

Note that $(\frac{-1}{7}) \equiv (-1)^{\frac{7-1}{2}} = -1$ and $(\frac{-1}{19}) \equiv (-1)^{\frac{19-1}{2}} = -1$. Hence $x^2 \equiv -1 \pmod 7$ and $x^2 \equiv -1 \pmod{19}$ has no solution. Thus, $x^2 \equiv -1 \pmod{133}$ has no solution.

$$\begin{aligned}\Phi &= \{a \in \mathbb{Z} \mid 1 \le a \le 66, (a, 133) = 1\} \\ &= \{1, 2, 3, 4, 5, 6, 8, 9, 10, 11, 12, 13, 15, 16, 17, \\ &\quad 18, 20, 22, 23, 24, 25, 26, 27, 29, 30, 31, 32, 33, 34, 36, \\ &\quad 37, 39, 40, 41, 43, 44, 45, 46, 47, 48, 50, 51, 52, 53, 54, \\ &\quad 55, 58, 59, 60, 61, 62, 64, 65, 66\}\end{aligned}$$

If $aa' \equiv 1 \pmod{133}$ and $1 \le a' \le 66$, then there exists an integer $a'' \in \mathbb{Z}$ such that $aa'' \equiv -1 \pmod{133}$ and $66 \le a'' \le 132$, or vice versa.

a	1	2	3	4	5	6	8	9	10	11	12	13
a'	1	67	89	100	80	111	50	74	40	121	122	41
a''	132	66	44	33	53	22	83	59	93	12	11	92
a	15	16	17	18	20	22	23	24	25	26	27	29
a'	71	25	47	37	20	127	81	61	16	87	69	78
a''	62	108	86	96	113	6	52	72	117	46	64	55
a	30	31	32	33	34	36	37	39	40	41	43	44
a'	102	103	79	129	90	85	18	37	10	13	99	130
a''	31	30	54	4	43	48	115	96	123	120	34	3
a	45	46	47	48	50	51	52	53	54	55	58	59
a'	68	107	17	97	8	60	110	128	101	114	39	124
a''	65	26	116	36	125	73	23	5	32	29	94	9
a	60	61	62	64	65	66						
a'	51	24	114	106	88	131						
a''	82	109	19	27	45	2						

Table 6

It is from Table 6 that

$$\begin{aligned}\Psi =&\{a \in \Phi : a = a'\}\\ =&\{a \in \Phi : a^2 \equiv \pm 1 \pmod{133}\}\\ =&\{a \in \Phi : a^2 \equiv 1 \pmod{133}\}\\ &\left(\because \left(\frac{-1}{7}\right) = \left(\frac{-1}{19}\right) = -1\right)\\ =&\{1, 20\}.\end{aligned}$$

Hence,

$$\begin{aligned}\prod_{a\in\Phi-\Psi} a \equiv& 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 8\cdot 9\cdot 10\cdot 11\cdot 12\cdot 13\cdot 15\cdot 16\cdot 17\cdot 18\cdot\\ & 22\cdot 23\cdot 24\cdot 25\cdot 26\cdot 27\cdot 29\cdot 30\cdot 31\cdot 32\cdot 33\cdot 34\cdot 36\cdot\\ & 37\cdot 39\cdot 40\cdot 41\cdot 43\cdot 44\cdot 45\cdot 46\cdot 47\cdot 48\cdot 50\cdot 51\cdot 52\cdot\\ & 53\cdot 54\cdot 55\cdot 58\cdot 59\cdot 60\cdot 61\cdot 62\cdot 64\cdot 65\cdot 66\\ \equiv& -1 \pmod{133},\end{aligned}$$

and thus

$$\begin{aligned}A =& \prod_{a\in\Phi} a\\ =& \left(\prod_{a\in\Psi} a\right)\left(\prod_{a\in\Phi-\Psi} a\right)\\ \equiv& -\left(\prod_{a\in\Psi} a\right)\\ \equiv& -(1\cdot 20)\\ \equiv& -20 \pmod{133}.\end{aligned}$$

4. **Some Applications of Quadratic Reciprocity Law.**

We shall give some applications of Quadratic Reciprocity Law in this section. Before we give examples, we introduce the follow two known theorems (see, [3]).

Theorem 4.1 (Theorem11.4, [3]). *Let p be an odd prime and a and b be integers not divisible by p. Then*

(1) *if* $a \equiv b \pmod{p}$, *then* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(2) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

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

Theorem 4.2 (Theorem11.6, [3]). *If p is an odd prime, then*

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

Example 4.3. Let $p = 21$ and $q = 25$. Because $p \equiv q \equiv 1 \pmod 4$, by Theorem 1.1,

$$\begin{aligned}
\left(\frac{5}{19}\right) &= (-1)^{\frac{5-1}{2}\cdot\frac{19-1}{2}}\left(\frac{19}{5}\right) && (\because \text{Theorem 1.1})\\
&= \left(\frac{19}{5}\right)\\
&= \left(\frac{4}{5}\right) && (\because \text{Theorem 4.1 (1)})\\
&= \left(\frac{2^2}{5}\right)\\
&= 1 && (\because \text{Theorem 4.1 (3)}).
\end{aligned}$$

Example 4.4. Let $p = 19$ and $q = 23$. Because $p \equiv q \equiv 3 \pmod 4$, by Theorem 1.1, we know that

$$\begin{aligned}
\left(\frac{19}{23}\right) &= (-1)^{\frac{19-1}{2}\cdot\frac{23-1}{2}}\left(\frac{23}{19}\right) && (\because \text{Theorem 1.1})\\
&= -\left(\frac{23}{19}\right)\\
&= -\left(\frac{4}{19}\right) && (\because \text{Theorem 4.1 (1)})\\
&= -\left(\frac{2^2}{19}\right)\\
&= -1 && (\because \text{Theorem 4.1 (3)}).
\end{aligned}$$

Hence the quadratic congruence $x^2 \equiv 19 \pmod{23}$ has no solution.

Example 4.5. Now we will calculate $\left(\frac{437}{1001}\right)$.

Since $437 = 19 \cdot 23$, by Theorem 4.1 (2), we have

$$\left(\frac{437}{1001}\right) = \left(\frac{19\cdot 23}{1001}\right) = \left(\frac{19}{1001}\right)\left(\frac{23}{1001}\right).$$

To evaluate two Legendre symbols on the right side of this equality, we use Theorem 1.1. Because $1001 \equiv 1 \pmod 4$, we see that

$$\begin{aligned}
\left(\frac{19}{1001}\right) &= (-1)^{\frac{19-1}{2}\cdot\frac{1001-1}{2}}\left(\frac{1001}{19}\right) && (\because \text{Theorem 1.1})\\
&= \left(\frac{1001}{19}\right)\\
&= \left(\frac{13}{19}\right) && (\because \text{Theorem 4.1 (1)})\\
&= (-1)^{\frac{13-1}{2}\cdot\frac{19-1}{2}}\left(\frac{19}{13}\right) && (\because \text{Theorem 1.1})\\
&= \left(\frac{19}{13}\right)\\
&= \left(\frac{6}{13}\right) && (\because \text{Theorem 4.1 (1)})\\
&= \left(\frac{2}{13}\right)\left(\frac{3}{13}\right)\\
&= -\left(\frac{3}{13}\right) && (\because \text{Theorem 4.2})\\
&= -(-1)^{\frac{3-1}{2}\cdot\frac{13-1}{2}}\left(\frac{13}{3}\right) && (\because \text{Theorem 1.1})\\
&= -\left(\frac{13}{3}\right)\\
&= -\left(\frac{1}{3}\right) && (\because \text{Theorem 4.1 (1)})\\
&= -1.
\end{aligned}$$

Likewise,

$$\begin{aligned}
\left(\frac{23}{1001}\right) &= (-1)^{\frac{23-1}{2}\cdot\frac{1001-1}{2}}\left(\frac{1001}{23}\right) && (\because \text{Theorem 1.1})\\
&= \left(\frac{1001}{23}\right)\\
&= \left(\frac{12}{23}\right) && (\because \text{Theorem 4.1 (1)})\\
&= \left(\frac{2^2}{23}\right)\left(\frac{3}{23}\right)\\
&= \left(\frac{3}{23}\right) && (\because \text{Theorem 4.1 (3)})\\
&= (-1)^{\frac{3-1}{2}\cdot\frac{23-1}{2}}\left(\frac{23}{3}\right) && (\because \text{Theorem 1.1})\\
&= -\left(\frac{23}{3}\right)\\
&= -\left(\frac{2}{3}\right) && (\because \text{Theorem 4.1 (1)})\\
&= -(-1) && (\because \text{Theorem 4.2})\\
&= 1.
\end{aligned}$$

Therefore,

$$\begin{aligned}
\left(\frac{437}{1001}\right) &= \left(\frac{19}{1001}\right)\left(\frac{23}{1001}\right)\\
&= (-1)\cdot 1\\
&= -1.
\end{aligned}$$

References

[1] C. F.Gauss, *Disquisitiones Arithmeticae(trans. A.A.Clarke)*, Yale University Press, New Haven, 1966.

[2] Sey Y. Kim, *An Elementary Proof of the Quadratic Reciprocity Law*, The American Mathematical Monthly, Vol. 111, No.1.(Jan.,2004), pp.48-50.

[3] R. Kenneth H, *Elementary Number Theory and Its Applications*, Fifth Edition Addison-Wesley 1992.

[4] F. Lemmermeyer, *Reciprocity Laws*, Springer-Verlag, Berlin, 2000.

[5] Wolfram, *Mathematica 7*, Wolfram Research 2008.

ABSTRACT

A Proof of Quadratic Reciprocity Law and its applications

Tae Hee-jung
Major in Mathematics Education
Graduate School of Education
Sungshin Women's University
Supervised by Shin, Yong Su Ph. D.

More than 190 proofs of Quadratic Reciprocity Law have been announced. In this thesis, introduce another proof of Quadratic Reciprocity Law and give some applications and examples of the result.