3. QUADRATIC CONGRUENCES

§3.1. Quadratics Over a Field

We are all familiar with the quadratic equation in the context of real or complex numbers. The formula for the solutions to \( ax^2 + bx + c = 0 \) (where \( a \neq 0 \)) is:

\[
    x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.
\]

This is valid over any field provided 2 has an inverse under multiplication. For the fields \( \mathbb{Z}_p \) this only rules out \( \mathbb{Z}_2 \) and we ought not to be using a formula to solve an equation over \( \mathbb{Z}_2 \). Of course it may be that there are no square roots of \( b^2 - 4ac \), in which case the quadratic will have no solutions.

Example 1: Find two consecutive odd numbers whose product is 11 more than a multiple of 83.

Solution: We can set this problem up as a quadratic congruence. If the numbers are 2x + 1 and 2x + 3 then we want to solve the congruence \((2x + 1)(2x + 3) \equiv 11 \pmod{83}\). Simplifying, we get \(4x^2 + 8x - 8 \equiv 0 \pmod{83}\). Since 4 is coprime with 83 we can divide by 4 to get \(x^2 + 2x - 2 \equiv 0 \pmod{83}\). Hence \(x = \frac{-2 \pm \sqrt{12}}{2} \) and so \(x = -1 \pm \sqrt{3}\).

We need to find the square roots of 3 modulo 83. By squaring every number from 0 to 82, and reducing modulo 83, we can see that x = 13 and x = 70 are the square roots. (Note that 70 = -13, so we could write these as ±13). This gives the solutions for x as 12 and 69.

These correspond to the two pairs of consecutive numbers 25, 27 and 139, 141. Of course these are not the only solutions. We can add or subtract any multiple of 83 to the values of x and we will still have solutions. So, for example, x = 108 and 152 are also solutions to the quadratic giving two more pairs 217, 219 and 305, 307. There are, of course infinitely many solutions. But when we count solutions to a congruence equation we treat congruent solutions as the same. So this quadratic has just two solutions, as usual.

But if the modulus is not prime there can be more than two solutions by virtue of the fact that there can be more than two square roots. The squares mod 27 are given in the following table:

<table>
<thead>
<tr>
<th>x^2</th>
<th>0</th>
<th>±1</th>
<th>±2</th>
<th>±3</th>
<th>±4</th>
<th>±5</th>
<th>±6</th>
<th>±7</th>
<th>±8</th>
<th>±9</th>
<th>±10</th>
<th>±11</th>
<th>±12</th>
<th>±13</th>
</tr>
</thead>
<tbody>
<tr>
<td>x</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>9</td>
<td>16</td>
<td>25</td>
<td>9</td>
<td>22</td>
<td>10</td>
<td>0</td>
<td>19</td>
<td>13</td>
<td>9</td>
<td>7</td>
</tr>
</tbody>
</table>

So while certain numbers have 2 square roots, the other numbers have none at all. But 9 has as many as six square roots! So we must modify the quadratic formula if we want to apply it to quadratic congruences:
\[ x = \frac{-b + \sqrt{b^2 - 4ac}}{2a} \]  where \( \sqrt{b^2 - 4ac} \) represents all (possibly more than 2) the square roots of \( b^2 - 4ac \).

**Example 2:** Solve the quadratic \( x^2 + 8x + 7 \equiv 0 \pmod{27} \).

**Solution:** From the quadratic formula we get
\[ x \equiv \frac{-8 + \sqrt{64 - 28}}{2} \equiv \frac{-8 + 36}{2} \equiv -4 + \sqrt{9} \cdot \]

Now \( \pm 3 \) are certainly some of the square roots of 9 but, as we have seen, there are others. Since \( \sqrt{9} \equiv \pm 3, \pm 6, \pm 12 \) modulo 27 we get six solutions to our quadratic:
\[ x = -16, -10, -7, -1, 2, 8 \] that is
\[ x = 2, 8, 11, 17, 20, 26. \]

But there are other complications when the modulus is not prime. Consider the following example.

**Example 3:** Solve the quadratic \( 3x^2 + 2x + 2 \equiv 0 \pmod{27} \).

**Attempted solution:** The quadratic formula gives us
\[ x \equiv \frac{-2 + \sqrt{4 - 24}}{6} \]
\[ \equiv \frac{-2 + \sqrt{-20}}{6} \]
\[ \equiv \frac{-2 + \sqrt{7}}{6}. \]
From the above table we find that there are two square roots of 7 modulo 27, viz. \( \pm 13 \).
Hence \( x \equiv \frac{11}{6} \) or \( -\frac{15}{6} \). The problem is that \( 6^{-1} \) does not exist in \( \mathbb{Z}_{27} \) because 6 is not coprime to 27. (Beware cancelling by 3 in the second case as 3 doesn’t have an inverse either.) We seem to be stuck.

**A more enlightened, but nevertheless false solution:**
The quadratic formula is based on the technique of completing the square.
In order to complete the square let us multiply the equation \( 3x^2 + 2x + 2 \equiv 0 \pmod{27} \) by 12. This gives \( 36x^2 + 24x + 24 \equiv 0 \pmod{27} \).

Completing the square we get \( (6x + 2)^2 \equiv 4 - 24 \equiv -20 \equiv 7 \pmod{27} \).
Hence \( 6x + 2 \equiv 13 \pmod{27} \) or \( 6x + 2 \equiv -13 \pmod{27} \). We now have two linear congruences to solve.
The first gives \( 6x \equiv 11 \pmod{27} \) which has no solutions since 11 is not divisible by 3. The second gives \( 6x \equiv -15 \equiv 12 \pmod{27} \).

Now we can divide by 6 but the modulus changes. We get \( x \equiv 2 \pmod{9} \). We have to divide the modulus by the GCD (6, 27) = 3.

So, modulo 27 we get three solutions \( x \equiv 2 \pmod{27} \), \( x \equiv 11 \pmod{27} \) and \( x \equiv 20 \pmod{27} \). This seems fine, but if we check them in the original equation only \( x \equiv 20 \) works! What did we do wrong?
Correct Solution: Note that all three solutions satisfy the congruence 
$36x^2 + 24x + 24 \equiv 0 \pmod{27}$. What has happened in multiplying through by 24 is that we have introduced “spurious” solutions. Remember when you had to solve equations with surds and you squared both sides of the equation. Then often you found that some of the solutions you obtained didn’t work for the original equation. They worked for the squared equation but that’s not what we want. The reason was that squaring is not reversible because real numbers have two square roots.

We have the same situation here. Multiplying by 24 is not reversible since 24 is not coprime to 27. We have increased the set of solutions. What must we do?

The answer is that you must check your solutions and discard any spurious ones. In this case the correct procedure is to proceed exactly as we did but check the solutions and discard any that do not work.

There is a myth that when we solve an equation we are finding the solutions. Not at all. If we start with the equation and end up with a set of values what we really have done is to narrow the search. If $x$ satisfies the equation then it must be one of the numbers we obtain. But technically we should check them all.

Of course we’re lazy. We don’t bother checking. And usually we get away with it. Because if every step in our working is reversible then that amounts to a check. And that is mostly the case. But when we carry out a step that is not reversible, such as squaring both sides of an equation, or multiplying by a number that does not have an inverse, we should say to ourselves “we will probably get some spurious solutions – we’d better check at the end”.

§3.2. The Technique for Solving Quadratic Congruences

If the modulus is prime then we can use the quadratic formula (with the provisos mentioned above). If the modulus is a prime power we use the following procedure.

To solve the congruence $ax^2 + bx + c \equiv 0 \pmod{p^n}$:
1. Multiply by $4a$ to give $4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{p^n}$.
2. Complete the square to give $(2ax + b)^2 \equiv b^2 - 4ac \pmod{p^n}$.
3. Find the square roots of $b^2 - 4ac$ modulo $p^n$.
4. For each such square root $r$, solve the linear congruence $2ax + b \equiv r \pmod{p^n}$.
5. Check each solution found into the original quadratic to eliminate any spurious solutions.

NOTES:
1. It may not be necessary to multiply by $4a$ in step (1). Multiply by as little as possible to be able to complete the square. This will reduce the possibility of having spurious solutions.
2. If you do multiply by something and it is coprime to the modulus then there will be no spurious solutions and you can omit step (5).
3. Of course if the modulus is small it might be easier to simply try all possibilities.
4. The method works for any modulus, not just prime powers, but in those cases it is better to break the problem down to ones involving prime powers – it’s a lot less work. We discuss how to do this in the next section.
The hardest part, for a large modulus, is finding the square roots. There are some techniques we can use if the modulus is large but has small factors. And there are techniques for deciding whether or not there are any square roots.

§3.3. Square Roots to Composite Moduli

Suppose we want to solve the quadratic congruence \( x^2 \equiv a \pmod{mn} \), where \( m, n \) are coprime. Then we solve the separate congruences \( x^2 \equiv a \pmod{m} \) and \( x^2 \equiv a \pmod{n} \) and splice the results together using the Chinese Remainder Theorem.

Suppose the square roots modulo \( m_1 \) are \( a_1, a_2, ..., a_k \) and the square roots modulo \( n \) are \( b_1, b_2, ..., b_h \). Then there will be \( hk \) square roots modulo \( mn \). For each \( i, j \) we find \( x \) so that \( x \equiv a_i \pmod{m} \) and \( x \equiv b_j \pmod{n} \) and this will be the corresponding square roots modulo \( mn \).

Example 4: Find the square roots of 4 modulo 91.
Solution: 91 = 7 \times 13.
The square roots of 4 mod 7 are \( \pm 2 \), that is, 2, 5.
The square roots of 4 mod 13 are \( \pm 2 \), that is 2, 11.
For 2, 2 we want \( x \equiv 2 \pmod{7} \) and \( x \equiv 2 \pmod{13} \). Clearly this is \( x = 2 \).
For 2, 11 we want \( x \equiv 2 \pmod{7} \) and \( x \equiv 11 \pmod{13} \).
We must solve \( 7x \equiv 1 \pmod{13} \) and \( 13x \equiv 1 \pmod{7} \) to get the \( x_1, x_2 \) in the Chinese Remainder Theorem.
\( 13x \equiv 1 \pmod{7} \) reduces to \(-x \equiv 1 \pmod{7} \), giving \( x_1 = -1 \).
\( 7x \equiv 1 \pmod{13} \) \equiv 14(mod 13) gives \( x_2 = 2 \). (Note we are justified in dividing by 7 as it is coprime to the modulus.)
So take \( x = 13.(\pm 1)2 + 7.11.2 = 128 \equiv 37 \).
We can process the other two combinations in the same way, but not surprisingly we will get \(-2 \) and \(-37 \). So we can save effort by only selecting one from each \( \pm \) pair for the first modulus.

If we have a prime modulus, \( p \), then to find the square roots we must square each element, though because square roots come in \( \pm \) pairs we need only do this up to \( \frac{p-1}{2} \).
However before undertaking a great deal of work it is useful to know if there are any square roots. This we can do quite easily, even for large primes.

§3.4. The Legendre Function

The Legendre function is a map from \( \mathbb{Z} \times \mathbb{Z}^+ \) to \( \mathbb{Z}_2 \) defined by:
\[
(a \mid m) = \begin{cases} 
0 & \text{if } x^2 \equiv a \pmod{m} \text{ has a solution} \\
1 & \text{if } x^2 \equiv a \pmod{m} \text{ has no solution} 
\end{cases}
\]

We shall prove the following properties of the Legendre function.
(1) If \( a \equiv b \pmod{m} \) then \( (a \mid m) = (b \mid m) \).
(2) \( (0 \mid m) = (1 \mid m) = 0 \).
(3) If \( (m, n) = 1 \) then \( (a \mid mn) = (a \mid m) + (a \mid n) + (a \mid m)(a \mid n) \).
(4) If \( p \) is prime and \( 0 \leq a < p^n \) then \( (a \mid p^n) = 0 \) if and only if \( a = p^{3t}b \) for some \( b, t \) where \( (p, b) = 1 \) and \( (b \mid p^{n-2t}) = 0 \).

(5) If \( 0 \leq a < 2^n \) and \( a \) is odd then \( (a \mid 2^n) = 0 \) if and only if \( a \equiv 1 \pmod{8} \).

(6) If \( p \) is an odd prime and \( (p, a) = 1 \) then \( (a \mid p^n) = (a \mid p) \).

(7) If \( p \) is prime and \( (p, ab) = 1 \) then \( (ab \mid p) = (a \mid p) + (b \mid p) \).

(8) If \( p \) is an odd prime \( (2 \mid p) = \frac{p-1}{2} \cdot \frac{p+1}{2} \).

(9) (Gauss' Reciprocity Theorem):

\[
\text{If } p, q \text{ are different odd primes then } (q \mid p) = (p \mid q) + \left( \frac{-1}{p} \right)(q \mid q).
\]

(10) If \( p \) is an odd prime \( (-1 \mid p) = \frac{p-1}{2} \).

On the basis of these ten results we are able to find \( (n \mid m) \) quite efficiently.

**Example 5:** Find \( (165 \mid 76) \).

**Solution:** \( (165 \mid 76) = (13 \mid 76) \) by (1).

\[
= (13 \mid 4) + (13 \mid 19) + (13 \mid 4)(13 \mid 19) \text{ by (3)}.
\]

Now \( (13 \mid 4) = (1 \mid 4) \) by (1)

\[
= 0 \text{ by (2)}.
\]

And \( (13 \mid 19) = (19 \mid 13) + (-1 \mid 13)(-1 \mid 19) \).

Now \( (19 \mid 13) = (6 \mid 13) \) by (1).

\[
(-1 \mid 13) = 0 \text{ by (10)}.
\]

\[
(-1 \mid 19) = 1 \text{ by (10)}.
\]

\[
(6 \mid 13) = (2 \mid 13) + (3 \mid 13) \text{ by (7)}.
\]

\[
(2 \mid 13) = 1 \text{ by (8)}.
\]

\[
(3 \mid 13) = (13 \mid 3) + (-1 \mid 3)(-1 \mid 13) \text{ by (9)}.
\]

\[
(13 \mid 3) = (1 \mid 3) \text{ by (1)} = 0 \text{ by (2)}.
\]

\[
(-1 \mid 3) = 1 \text{ by (10)}.
\]

\[
(-1 \mid 13) = 0 \text{ by (10)}.
\]

Hence \( (3 \mid 13) = 0 \).

Hence \( (19 \mid 13) = (6 \mid 13) = 1 \).

Hence \( (13 \mid 19) = 1 \).

Hence \( (165 \mid 76) = 1 \).

**§3.5. The Structure of the Ring \( \mathbb{Z}_m \)**

\( \mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z} = \{a + m\mathbb{Z} \mid a \in \mathbb{Z}\} \) where each coset \( a + m\mathbb{Z} = \{a + mk \mid k \in \mathbb{Z}\} \).

We use the same symbol for the elements of \( \mathbb{Z} \) and their cosets.

**Theorem 1:** If \( (m, n) = 1 \) then \( \mathbb{Z}_{mn} \cong \mathbb{Z}_m \oplus \mathbb{Z}_n \).

**Proof:** \( a \rightarrow (a, a) \) is an isomorphism.

If \( R \) is a ring define \( R^2 \) to be \( \{r^2 \mid r \in R\} \).

**Theorem 2:** If \( (m, n) = 1 \) then \( (a \mid mn) = (a, m) + (a, n) + (a, m) (a, n) \).

**Proof:** Under the above isomorphism \( \mathbb{Z}_{mn}^2 \rightarrow (\mathbb{Z}_m \oplus \mathbb{Z}_n)^2 = \mathbb{Z}_m^2 \oplus \mathbb{Z}_n^2 \).

So \( (a \mid mn) = 0 \) if and only if \( (a \mid m) = (a \mid n) = 0 \).
Theorem 3: If \( p \) is prime and \( 0 \leq a < p^n \) then \((a \mid p^n) = 0\) if and only if \( a = p^{2t}b \) for some \( b, t \) where \((p, b) = 1\) and \((b \mid p^{n-2t}) = 0\).

Proof: Suppose \( a = p^s b \) where \((p, b) = 1\). Then \( s < r\).
Suppose \((a \mid p^n) = 0\). Then there exists \( x \) such that \( x^2 \equiv a \pmod{p^r} \) whence \( p^s \mid x^2 \).
Suppose \( s = 2t + 1 \). Then \( p^{t+1} \mid x \) whence \( p^{2t+2} (= p^{s+1}) \) divides \( x^2 \) and so divides \( a \), a contradiction.
Hence \( s \) is even, say \( 2t \). Then \( p^t \mid x \). Let \( x = p^t y \).
Then \( p^{2t} y^2 = p^{2t}b \pmod{p^n} \).
Hence \( y^2 \equiv b \pmod{p^{n-2t}} \). Conversely if \( y^2 \equiv b \pmod{p^{n-2t}} \) and \( a = p^{2t}b \) then \((p^t y)^2 = p^{2t}y^2 = p^{2t}b \equiv a \pmod{p^n}\).

§3.6. The Structure of the Group \( \mathbb{Z}_m^\# \)
Theorem 4: \( \mathbb{Z}_m^\# = \{ x \in \mathbb{Z}_m \mid (x, m) = 1 \} \).
Proof: \( xy \equiv 1 \pmod{m} \) has a solution for \( y \) if and only if \((x, m)\) divides 1, that is equals 1.
Corollary: \( \mathbb{Z}_p \) is a field if and only if \( p \) is prime.

The size of the set \( \{ x \in \mathbb{Z} \mid 1 \leq x < m \text{ and } (x, m) = 1 \} \) is denoted by \( \varphi(m) \). The function \( \varphi \) is called the Euler \( \varphi \)-function. Hence \( |\mathbb{Z}_m^\#| = \varphi(m) \).

Theorem 5: If \((a, m) = 1\) then \( a^{\varphi(m)} \equiv 1 \pmod{m} \).
Proof: From group theory, the order of \( a \) in \( \mathbb{Z}_m^\# \) divides \( |\mathbb{Z}_m^\#| = \varphi(m) \).
Corollary (Fermat): If \( p \) is prime and \((a, p) = 1\) then \( a^{p-1} \equiv 1 \pmod{p} \).

Theorem 6: If \((m, n) = 1\), \( \mathbb{Z}_{mn}^\# \equiv \mathbb{Z}_m^\# \times \mathbb{Z}_n^\# \).
Proof: \( a \rightarrow (a, a) \) is an isomorphism.
\((r, s)^{-1} = (r^{-1}, s^{-1})\), each existing if the other one does.
Corollary: If \((m, n) = 1\) then \( \varphi(mn) = \varphi(m)\varphi(n) \).

Theorem 7: If \( p \) is prime, \( \varphi(p^n) = p^{n-1}(p-1) \).
Proof: Of the \( p^n \) elements \( 0, 1, \ldots, p^n - 1 \), exactly \( p^{n-1} \) are elements of \( p \).

§3.7. The Structure of the Group \( \mathbb{Z}_{p^n}^\# \)
Theorem 8: \( \mathbb{Z}_{2^n}^\# = \{ 1 \} \equiv 1 \).
\[ \mathbb{Z}_{4}^\# = \{ 1, 3 \} \cong C_2. \]
If \( n \geq 3 \), \( \mathbb{Z}_{2^n}^\# = \langle 3 \rangle \times \langle -1 \rangle \equiv C_{2^{n-2}} \times C_2. \)

Proof:
(1) The order of \( 3 \) in \( \mathbb{Z}_{2^n}^\# \) is \( 2^{n-2} \):
\[ 3^{2^{n-1}} = 9^{2^r} = (1 + 2^3)^{2^r} = 1 + 2^{r+3} + \frac{1}{2}(2^{2^r} - 1)2^9 + \ldots \equiv 1 + 2^{r+3} \pmod{2^{r+4}}. \]
Hence \( 3^{2^{n-1}} \) is not congruent to \( 1 \) mod \( 2^n \) while \( 3^{2^{n-2}} \) is.
(2) Suppose \( 3^k \equiv -1 \pmod{2^n} \equiv -1 \pmod{8} \). However \( 3^k \equiv 1 \text{ or } 3 \pmod{8} \), a contradiction. Hence \( \langle 3 \rangle \cap \langle -1 \rangle = 1 \).
Theorem 9: If $p$ is prime, $\mathbb{Z}_p^\#$ is cyclic.

Proof: $|\mathbb{Z}_p^\#| = p - 1$. For each prime $q | p - 1$, $|[x^q = 1]| \leq q$ since the roots of a polynomial over a field is at most the degree. Hence every Sylow subgroup of $\mathbb{Z}_p^\#$ is cyclic and hence so is $\mathbb{Z}_p^\#$ itself.

Theorem 10: If $p$ is odd, $\mathbb{Z}_p^{p^n} = \langle 1 + p \rangle \times \langle a \rangle$ for some $a$.

Proof: $(1 + p)^{p^r} = 1 + p^{r+1} + \frac{1}{2} p^r(p^r - 1)p^2 + \ldots$ 
$\equiv 1 + p^{r+1} \pmod{p^{r+2}}$
$\equiv 1 \pmod{p^{r+1}}$
Hence $(1 + p)^{p^{n-2}}$ is not congruent to 1 (mod $p^n$) but $(1 + p)^{p^{n-1}} \equiv 1 \pmod{p^n}$.
Hence $1 + p$ has order $p^{n-1}$ in $\mathbb{Z}_p^{p^n}$.
Now $|\mathbb{Z}_p^{p^n}| = p^{n-1}(p - 1)$ and so $\langle 1 + p \rangle$ is a Sylow $p$-subgroup.
Hence $\mathbb{Z}_p^{p^n} = \langle 1 + p \rangle \times B$ where $|B| = p^{n-1}$.
Consider the homomorphism $f: \mathbb{Z}_p^{p^n} \to \mathbb{Z}_p^\#$ define by $f(a) = a$.
The image of $f$ is $\mathbb{Z}_p^\#$ and the kernel is $S = \{1 + kp | k = 0, 1, \ldots, p^{n-1} - 1\}$.
Now $(1 + p)^f \equiv 1 \pmod{p}$ so $\langle 1 + p \rangle \subseteq S$.
But both have $p^{n-1}$ elements and so they are equal. Hence $ker f = \langle 1 + p \rangle$.
Now $B \cong \mathbb{Z}_p^{p^n}/\langle 1 + p \rangle \cong \mathbb{Z}_p^\#$ which is cyclic, so $B \cong C_{p-1}$.

Theorem 11: If $0 \leq a < 2^n$ and $a$ is odd then $(a | 2^n) = 0$ if and only if $a \equiv 1 \pmod{8}$.

Proof: Let $G = \mathbb{Z}_2^{2^n}$. Then $G = \langle 3 \rangle \times \langle -1 \rangle$ so $G^2 = \langle 9 \rangle \subseteq \{1 + 8k | k = 0, 1, \ldots, 2^{n-3} - 1\}$.
Since both have $2^{n-3}$ elements they are equal.
Hence $(a | 2^n) = 0$ if and only if $a \equiv 1 \pmod{8}$.

Theorem 12: If $p$ is an odd prime and $(p, a) = 1$ then $(a | p^n) = (a | p)$.

Proof: Let $G = \mathbb{Z}_p^{p^n} = \langle 1 + p \rangle \times \langle a \rangle$ where $a$ has order $p - 1$.
Then $G^2 = \langle 1 + p \rangle \times \langle a^2 \rangle$.

Theorem 13: If $p$ is prime and $(p, ab) = 1$ then $(ab | p) = (a | p) + (b | p)$.

Proof: $\mathbb{Z}_p^\#$ is an abelian group under multiplication.
$\theta: x \to x^2$ is a homomorphism.
$\ker \theta = \{\pm 1\}$.
$im \theta = \mathbb{Z}_p^{#2}$.
So $\mathbb{Z}_p^{#2}$ is a subgroup of index 2.
Hence $\mathbb{Z}_p^\#/\mathbb{Z}_p^{#2} \cong \mathbb{Z}_2$.
So $a \to (a | p)$ is precisely the product of the projection of $\mathbb{Z}_p^\#$ onto $\mathbb{Z}_p^\#/\mathbb{Z}_p^{#2}$ and the isomorphism from $\mathbb{Z}_p^\#/\mathbb{Z}_p^{#2}$ onto $\mathbb{Z}_2$.

Theorem 14: If $p$ is an odd prime $(-1 | p) \equiv \frac{p-1}{2} \pmod{2}$.

Proof: $\mathbb{Z}_p^\#$ is cyclic of order $p - 1$, say $\langle a \rangle$. 

35
\[(a^{1/2(p-1)})^2 = 1, \text{ so } a^{1/2(p-1)} = \pm 1.\]

Since \(a\) has order \(p - 1\), \(a^{1/2(p-1)} = -1\).

If \(\frac{p-1}{2}\) is even then \((a^{1/4(p-1)})^2 = a^{1/2(p-1)} = -1\), and so \((-1 \mid p) = 0.\)

Conversely if \((-1 \mid p) = 0\), \(-1 = a^{2r}\) for some \(r\).

Hence \(2r \equiv \frac{p-1}{2} \pmod{p-1}\).

Since both \(2r\) and \(p - 1\) are even, \(\frac{p-1}{2}\) is even.

§3.8. The Reciprocity Theorem

**Theorem 15**: For all \(b \in \mathbb{Z}_p^\#\), \(b^{1/2(p-1)} = (-1)^{(b \mid p)}\).

**Proof**: \(\mathbb{Z}_p^\#\) is cyclic, say \(\langle a \rangle\) where \(a\) has order \(p - 1\). Let \(b = a^t\).

Then \(b^{1/2(p-1)} = a^{t/2(p-1)} = 1\) if and only if \(t\) is even, if and only if \((b \mid p) = 0.\)

Suppose \(p, q\) are distinct primes and suppose that \(p\) is odd. Let \(h = \frac{p-1}{2}\).

Partition \(\mathbb{Z}_p^\#\) into \(A = \{1, 2, \ldots, h\}\) and \(B = \{-1, -2, \ldots, -h\}\).

Multiplication by \(q\) is a permutation of \(\mathbb{Z}_p^\#\) that causes a certain number of elements of \(A\) to migrate to \(B\) with an equal number of elements of \(B\) migrating to \(A\). Let \(M_p^q\) be this number, modulo \(2\).

**Theorem 16**: \(M_p^q = (q \mid p)\).

**Proof**: Let \(M = M_p^q\) and let \(a_1, \ldots, a_{h-M}\) be the elements of \(A\) that stay in \(A\) and \(b_1, \ldots, b_M\) be the elements of \(A\) that migrate to \(B\).

Hence \(q b_1, \ldots, q b_M\) are in \(B\) (all distinct).

Hence \(-q b_1, \ldots, -q b_M\) are all in \(A\) (all distinct).

Moreover \(qa_1, \ldots, q_{h-M}\) are all in \(A\) (all distinct).

If \(qa_i = -q b_j\) for some \(i, j\), then \(q(a_i + b_j) = 0\), in which case \(a_i = -b_j\), a contradiction since both \(a_i\) and \(b_j\) are in \(A\).

Hence \(qa_1, \ldots, qa_{h-M}, -q b_1, \ldots, -q b_M\) is a permutation of \(A\).

Hence \(q^{M}(-1)^bh! = h!\) and so \(q^h = (-1)^M\) and so, by Theorem 15, \(M = (b \mid p)\).

**Theorem 17**: \(M_{pq} = \sum_{i=1}^{h} \left[ \left\lfloor \frac{iq}{p} \right\rfloor + \frac{(q-1)(p^2-1)}{8} \right] \pmod{2}\)

where \([x]\) denotes the integral part of \(x\).

**Proof**: Let \(a_1, \ldots, a_{h-M}, b_1, \ldots, b_M\) and \(A, B\) be as in Theorem 16, but regarded as elements of \(\mathbb{Z}_p^\#\).

Let \(A_0 = \{a_1, \ldots, a_{h-M}\}\) and \(A_1 = \{b_1, \ldots, b_M\}\). Then \(A = A_0 + A_1\).

If \(i \in A_0\) then \(iq = \left[ \frac{iq}{p} \right] p + r_i\) for some \(r_i \in A\).

If \(i \in A_1\) then \(iq = \left[ \frac{iq}{p} \right] p + p + s_i\) for some \(s_i \in B\).

From Theorem 13, \(A = \{r_i \mid i \in A_0\} + \{-r_i \mid i \in A_1\}\).
Hence \( \sum_{i \in A_0} r_i - \sum_{i \in A_1} r_i = \sum_{i=1}^h i = \frac{h(h + 1)}{2} = \frac{1}{2} \left( \frac{p-1}{2} \right) \left( \frac{p+1}{2} \right) = \frac{p^2 - 1}{8}. \)

Therefore \( \sum_{i \in A} r_i = \sum_{i \in A_0} r_i + \sum_{i \in A_1} r_i \equiv \frac{p^2 - 1}{8} \) (mod 2). Moreover \( \sum_{i \in A} i = \frac{p^2 - 1}{8}. \)

Now \( q \sum_{i \in A} i = p \sum_{i \in A} \left\lfloor \frac{iq}{p} \right\rfloor + Mp + \sum_{i \in A} r_i \)

Hence \( (q-1) \left( \frac{p^2 - 1}{8} \right) \equiv p \left( M + \sum_{i \in A} \left\lfloor \frac{iq}{p} \right\rfloor \right) \) (mod 2)

Since \( p \) is odd the result follows.

**Theorem 18:** If \( p \) is an odd prime \((2 \mid p) = \frac{1}{2} \left( \frac{p-1}{2} \right) \left( \frac{p+1}{2} \right). \)

**Proof:** \((2 \mid p) = M_p^2 \equiv 0 + \frac{p^2 - 1}{8}. \)

**Theorem 19 (Eisenstein):**

\[
\sum_{i=1}^{p-1} \left\lfloor \frac{iq}{p} \right\rfloor + \sum_{i=1}^{q-1} \left\lfloor \frac{ip}{q} \right\rfloor = \left( \frac{p-1}{2} \right) \left( \frac{p+1}{2} \right).
\]

**Proof:** The right-hand side is the number of points with integer coordinates in the following rectangle:

```
Since p ≠ q no lattice points lie on the diagonal.
```

The number of lattice points in the lower triangle is \( \sum_{i=1}^{p-1} \left\lfloor \frac{iq}{p} \right\rfloor \) and the number in the upper triangle is \( \sum_{i=1}^{q-1} \left\lfloor \frac{ip}{q} \right\rfloor \).
Theorem 20 (Gauss’ Reciprocity Theorem):
If p, q are different odd primes then \((q \mid p) = (p \mid q) + (-1 \mid p)(-1 \mid q)\).

Proof:
\[
(p \mid q) + (q \mid p) \equiv \sum_{i=1}^{q-1} \left[ \frac{ip}{q} \right] + \sum_{i=1}^{p-1} \left[ \frac{iq}{p} \right] \equiv \left( \frac{p-1}{2} \right) \left( \frac{q-1}{2} \right) \equiv (-1 \mid p)(-1 \mid q).
\]