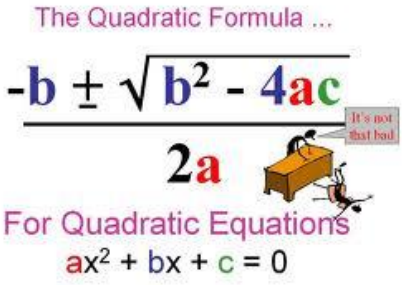
3. QUADRATIC CONGRUENCES

§3.1. Quadratics Over a Finite Field

We're 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 is non-zero) 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 $(2x + 1)(2x + 3) \equiv 11 (\text{mod } 83)$.

Simplifying, we get $4x^2 + 8x - 8 \equiv 0 (\text{mod } 83)$.
Since 4 is coprime with 83 we can divide by 4 to get

$$x^2 + 2x - 2 \equiv 0 (\text{mod } 83).$$

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 (in fact we only need to go half-way), 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 these values of x and we'll 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:

x	0	±1	±2	±3	±4	±5	±6	±7
$\mathbf{x^2}$	0	1	4	9	16	25	9	22

x	±8	±9	±10	±11	±12	±13
$\mathbf{x^2}$	10	0	19	13	9	7

So while certain numbers have 2 square roots, 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:

$x = \dfrac{-b + \sqrt{b^2 - 4ac}}{2a}$ where $\sqrt{b^2 - 4ac}$ represents all (possibly more than 2) square roots of $b^2 - 4ac$.

Example 2: Solve the quadratic $x^2 + 8x + 7 \equiv 0 (\text{mod } 27)$.
Solution: From the quadratic formula we get

$$x \equiv \frac{-8 + \sqrt{64 - 28}}{2}$$
$$\equiv \frac{-8 + \sqrt{36}}{2}$$
$$\equiv -4 + \sqrt{9}\ .$$

Now ± 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:

$$x = -16, -10, -7, -1, 2, 8 \text{ that is}$$
$$x = 2, 8, 11, 17, 20, 26.$$

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

Example 3: Solve the quadratic $3x^2 + 2x + 2 \equiv 0 (\text{mod } 27)$.
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. ± 13.

Hence $x \equiv \frac{11}{6}$ or $\frac{-15}{6}$.

The problem is that 6^{-1} doesn't 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's multiply the equation $3x^2 + 2x + 2 \equiv 0 (\text{mod } 27)$ by 12.
This gives $36x^2 + 24x + 24 \equiv 0 (\text{mod } 27)$.

Completing the square we get:

$$(6x + 2)^2 \equiv 4 - 24 \equiv -20 \equiv 7 (\text{mod } 27).$$

Hence $6x + 2 \equiv 13 (\text{mod } 27)$ or $6x + 2 \equiv -13 (\text{mod } 27)$.
We now have two linear congruences to solve.

The first gives $6x \equiv 11 (\text{mod } 27)$ which has no solutions since 11 is not divisible by 3.
The second gives $6x \equiv -15 \equiv 12 (\text{mod } 27)$.

Now we can divide by 6 *but the modulus changes*.
We get $x \equiv 2 (\text{mod } 9)$.
We have to divide the modulus by the GCD (6, 27) = 3.
So, modulo 27 we get three solutions:
$x \equiv 2 (\text{mod } 27)$, $x \equiv 11 (\text{mod } 27)$ and $x \equiv 20 (\text{mod } 27)$.
This seems fine, but if we check them in the original equation only $x \equiv 20$ works! What did we do wrong?

Note that all three solutions satisfy the congruence $36x^2 + 24x + 24 \equiv 0 (\text{mod } 27)$. What has happened in multiplying through by 24 is that we've introduced 'spurious' solutions. Remember when you had to solve equations with surds, and you squared both sides of the equation, 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 wanted. 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 don't work.

There's a myth that when we solve an equation we're finding the solutions. Not at all! If we start with the equation, and end up with a set of values, all we've 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 as a rule. 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 isn't reversible, such as squaring both sides of an equation, or multiplying by a number that doesn't have an inverse, we should say to ourselves "we'll probably get some spurious solutions – we'd better check at the end".

§3.2. 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's coprime to the modulus then there'll 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's better to break the problem down to ones involving prime powers – it's a lot less work. (5) 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 some techniques for deciding whether or not there are any square roots.

§3.3. The Legendre Function

So, solving a quadratic equation $ax^2 + bx + c \equiv 0 (\text{mod } m)$ boils down to finding square roots in $\mathbb{Z}_m$. There are three levels of questions about square roots.

- Is there a square root?
- How many square roots are there?
- What are the square roots?

We begin by considering the question of existence, Since $(-x)^2 = x^2$ about half the elements of $\mathbb{Z}_m$, or even less, are squares. For small m the simplest thing is to generate a table of squares.

Example 4: The table of squares modulo 13 is:

x	0	1	2	3	4	5	6	7	8	9	10	11	12
$\mathbf{x^2}$	0	1	4	9	3	12	10	10	12	3	9	4	1

so 7 of the 13 elements have square roots. Clearly we only ever need to go half way,

Example 5: The table of squares modulo 16 is:

x	0	1	2	3	4	5	6	7	8
$\mathbf{x^2}$	0	1	4	9	0	9	4	1	0

so only 4 of the 16 elements have square roots.

The **Legendre function** is a map from $\mathbb{Z} \times \mathbb{Z}^+$ to $\mathbb{Z}_2$ defined by:

$$(a \mid m) = \begin{cases} 0 \text{ if } x^2 \equiv a \pmod{m} \text{ has a solution} \\ 1 \text{ if } x^2 \equiv a \pmod{m} \text{ has no solution} \end{cases}.$$

As well as addition and multiplication in $\mathbb{Z}_2$ we use the Boolean operation $\vee$ where $0 \vee 0 = 0$ and

$$0 \vee 1 = 1 \vee 0 = 1,\ 1 \vee 1 = 1.$$

[**NOTE:** We could write $a \vee b$ as $a + b + ab$ for all a, b.]

Adrien-Marie Legendre [1752 – 1833] was a French mathematician. The caricature shown here is the only known portrait. There is a portrait of Legendre that you find in many mathematics books, but in 2005 it was discovered to be that of the *wrong* Legendre. The mathematician Legendre is known for many things in mathematics, such as Legendre polynomials. He investigated quadratic congruences and introduced a notation, now known as the Legendre symbol, for studying when numbers have a square root for a given modulus.

An unflattering portrait of Legendre.

We shall prove the following properties of the Legendre function.

(QR1) If $a \equiv b \pmod{m}$ then $(a \mid m) = (b \mid m)$.

(QR2) If m, n are coprime then $(a \mid mn) = (a \mid m) \vee (a \mid n)$.

(QR3) If $0 \leq a < 2^n$ and a is odd then $(a \mid 2^n) = 0$ if and only if $a \equiv 1 \pmod{8}$.

(QR4) If p is an odd prime, not dividing a, then $(a \mid p^n) = (a \mid p)$.

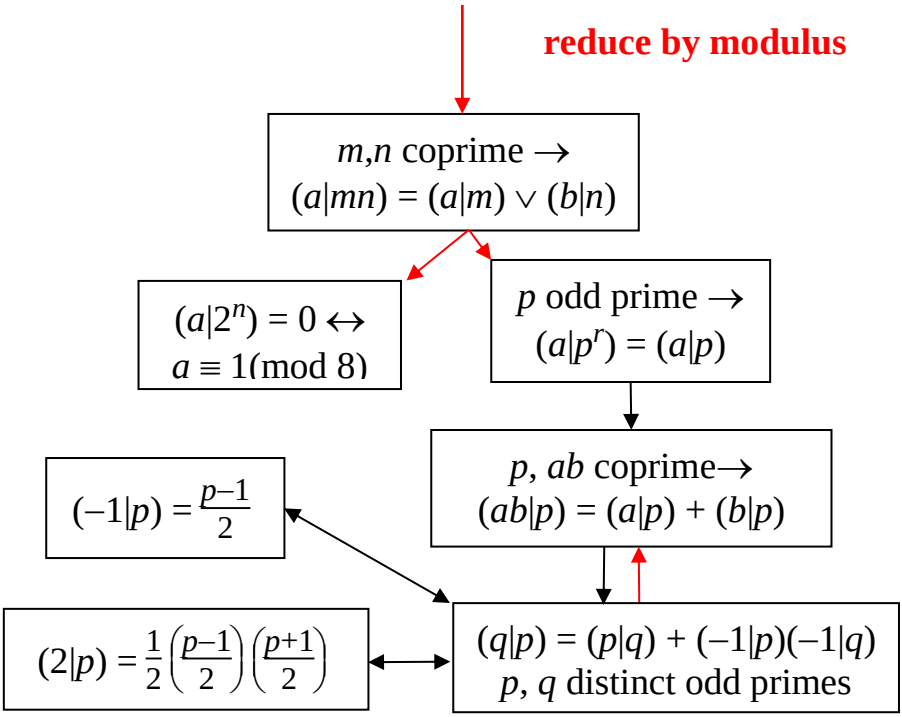
(QR5) If p is prime and GCD$(p, ab) = 1$ then $(ab \mid p) = (a \mid p) + (b \mid p)$.

(QR6) **(GAUSS RECIPROCITY THEOREM)**:

If p, q are different odd primes then $(q \mid p) = (p \mid q) + (-1 \mid p).(-1 \mid q)$.

(QR7) If p is an odd prime $(-1 \mid p) = \dfrac{p-1}{2}$.

(QR8) If p is an odd prime $(2 \mid p) = \dfrac{1}{2}\left(\dfrac{p-1}{2}\right)\left(\dfrac{p+1}{2}\right)$.



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

Example 6: Find (165 | 76).
Solution: (165 | 76) = (13 | 76) by (1).
= (13 | 4) $\vee$ (13 | 19) by (Q2).
Now (13 | 4) = (1 | 4) by (QR1)
= 0.
And (13 | 19) = (19 | 13) + (–1 | 13)(–1 | 19) by (Q6)
Now (19 | 13) = (6 |13) by (QR1).
(–1 | 13) = 0 by (QR7).
(–1 | 19) = 1 by (QR7).
(6 | 13) = (2 | 13) + (3 | 13) by (QR5).
(2 | 13) = 1 by (QR8).
(3 | 13) = (13 | 3) + (–1 | 3)(–1 | 13) by (QR6).
(13 | 3) = (1 | 3) by (QR1) = 0.
(–1 | 3) = 1 by (QR7).
(–1 | 13) = 0 by (QR7).
Hence (3 | 13) = 0.
Hence (19 | 13) = (6 | 13) = 1.
Hence (13 | 19) = 1.
Hence (165 | 76) = 1.

Theorem 1 [QR1]: If $a \equiv b \pmod{m}$ then $(a \mid m) = (b \mid m)$.
Proof: This follows directly from the definition of the Legendre function.

In the next few sections we/ll prove these results. However you'll need to know some basic group theory and know the definition of a ring.

§3.4. The Structure of the Group $\mathbb{Z}_m$

The integers modulo m form a finite **commutative ring**, $\mathbb{Z}_m$ and its **units** (elements with multiplicative inverses) form a finite abelian group $\mathbb{Z}_m^{\#}$ under multiplication. Consequently, both are isomorphic to a direct sum, or product, of cyclic groups. We denote the cyclic group of order n by C_n.

$\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z} = \{a + m\mathbb{Z} \mid a \in \mathbb{Z}\}$ 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 2: If $(m, n) = 1$ then $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \oplus \mathbb{Z}_n$.
Proof: $\phi:\mathbb{Z}_{mn} \to \mathbb{Z}_m \oplus \mathbb{Z}_n$ defined by $\phi(a) = (a, a)$ is an isomorphism. It's clearly a ring homomorphism.
If $a \in \ker \phi$ then m, n both divide a and, being coprime, their product mn divides a. Hence ϕ is 1-1.

It might appear that this isn't onto because we don't seem to be getting elements (a, b) where $a \neq b$. But remember that a is an integer representing integers modulo mn, m, and n. So, when a is reduced modulo m or n it will usually be the case that we get different remainders.

So, why is ϕ onto? This is simply because $\mathbb{Z}_{mn}$ and $\mathbb{Z}_m \oplus \mathbb{Z}_n$ both have order mn and ϕ is 1-1.

If R is a commutative ring we define $\mathbf{R^2}$ to be $\{r^2 \mid r \in R\}$.
[**NOTE:** The usual definition of R^2 is the set of all sums of products of elements of R. This is always a ring. With this definition it is usually not.]

Theorem 3 [QR2]: If GCD(m, n) = 1 then ($a \mid mn$) = (a, m) $\vee$ (a, n).
Proof: Under the above isomorphism ϕ: $\mathbb{Z}_{mn}^2 \to (\mathbb{Z}_m \oplus \mathbb{Z}_n)^2 = \mathbb{Z}_m^2 \oplus \mathbb{Z}_n^2$.
So ($a \mid mn$) = 0 if and only if ($a \mid m$) = ($b \mid n$) = 0, that is if and only if ($a \mid m$) $\vee$ ($a \mid n$) = 0.

§3.5. 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 GCD(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 $\{x \in \mathbb{Z} \mid 1 \le x < m$ and GCD(x, m) = 1$\}$ is denoted by $\boldsymbol{\varphi(m)}$. The function φ is called the **Euler φ-function**. Hence $|\mathbb{Z}_m^{\#}| = \varphi(m)$.

Theorem 5: If GCD(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 GCD(a, p) = 1 then $a^{p-1} \equiv 1 \pmod{p}$.

Theorem 6: If m, n are coprime, $\mathbb{Z}_{mn}^{\#} \cong \mathbb{Z}_m^{\#} \times \mathbb{Z}_n^{\#}$.
Proof: $a \to (a, a)$ is an isomorphism.
$(r, s)^{-1} = (r^{-1}, s^{-1})$, each existing if the other one does.
Corollary: If GCD(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, …, $p^n - 1$, exactly p^{n-1} are multiples of p and so $p^n - p^{n-1}$ elements are coprime with p.

§3.6. The Structure of the Group $\mathbb{Z}_{p^n}^{\#}$

Theorem 8:

$\mathbb{Z}_2^{\#} = \{1\} \cong 1$.
$\mathbb{Z}_4^{\#} = \{1, 3\} \cong C_2$.
If $n \geq 3$, $\mathbb{Z}^{\#}_{2^n} = \langle 3 \rangle \times \langle -1 \rangle \cong C_{2^{n-2}} \times C_2$.

Proof:
(1) The order of 3 in $\mathbb{Z}^{\#}_{2^n}$ is 2^{n-2}:
$3^{2^{r+1}} = 9^{2^r} = (1 + 2^3)^{2^r} = 1 + 2^{r+3} + \tfrac{1}{2}\, 2^r(2^r - 1).2^9 + \ldots \equiv 1 + 2^{r+3} \pmod{2^{r+4}}$.
Hence $3^{2^{n-3}}$ is not congruent to 1 mod 2^n but $3^{2^{n-2}}$ is.
(2) Suppose $3^k \equiv -1 \pmod{2^n} \equiv -1 \pmod 8$. However $3^k \equiv 1$ or 3 (mod 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 $q \mid p - 1$, $|\{x^q = 1\}| \leq q$ 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 (WILSON'S THEOREM): If p is prime then $(p - 1)! \equiv -1 (\text{mod } p)$.

Proof: It is clearly true if $p = 2$ so suppose that p is odd. In the group $\mathbb{Z}_p^{\#}$, $(p - 1)!$ is the product of all the elements. Being cyclic of even order there are just two elements that equal their squares, namely ± 1. All other elements will cancel with their inverse and so $(p - 1)! = 1.(-1) = -1$.

Theorem 11: If p is odd, $\mathbb{Z}^{\#}{}_{p^n} = \langle 1 + p \rangle \times \langle a \rangle$ for some a.

$$\cong C_{p^{n-1}} \times C_{p-1}.$$

Proof:
$$\begin{aligned}(1 + p)^{p^r} &= 1 + p^{r+1} + \tfrac{1}{2} p^r(p^r - 1)p^2 + \ldots \\ &\equiv 1 + p^{r+1} \ (\text{mod } p^{r+2}) \\ &\equiv 1 \ (\text{mod } p^{r+1})\end{aligned}$$

Hence $(1 + p)^{p^{n-2}}$ is not congruent to 1 (mod p^n) but

$$(1 + p)^{p^{n-1}} \equiv 1 \ (\text{mod } p^n).$$

Hence $1 + p$ has order p^{n-1} in $\mathbb{Z}^{\#}{}_{p^n}$.

Now $|\mathbb{Z}^{\#}{}_{p^n}| = p^{n-1}(p - 1)$ and so $\langle 1 + p \rangle$ is a Sylow p-subgroup.

Hence $\mathbb{Z}^{\#}{}_{p^n} = \langle 1 + p \rangle \times B$ where $|B| = p - 1$.

Consider the homomorphism f: $\mathbb{Z}^{\#}{}_{p^n} \to \mathbb{Z}_p^{\#}$ defined by $f(a) = a$.

The image of f is $\mathbb{Z}_p^{\#}$ and the kernel is $S = \{1 + kp \mid k = 0, 1, \ldots, p^{n-1} - 1\}$.
Now $(1 + p)^r \equiv 1 (\text{mod } p)$ 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 $B \cong \mathbb{Z}^{\#}_{p^n} / \langle 1 + p \rangle \cong \mathbb{Z}_p^{\#}$ which is cyclic, so $B \cong C_{p-1}$.

Theorem 12 [QR3}: If $0 \leq a < 2^n$ and a is odd then $(a \mid 2^n) = 0$ if and only if
$a \equiv 1 \text{ (mod } 8)$.
Proof: Let $G = \mathbb{Z}^{\#}_{2^n}$. Then $G = \langle 3 \rangle \times \langle -1 \rangle$ so $G^2 = \langle 9 \rangle \subseteq \{1 + 8k \mid k = 0, 1, \ldots, 2^{n-3} - 1\}$.
Since both have 2^{n-3} elements they are equal.
Hence $(a \mid 2^n) = 0$ if and only if $a \equiv 1 (\text{mod } 8)$.

Theorem 13 [QR4]: If p is an odd prime and GCD$(p, a) = 1$ then $(a \mid p^n) = (a \mid p)$.
Proof: Let $G = \mathbb{Z}^{\#}_{p^n} = \langle 1 + p \rangle \times \langle a \rangle$ where a has order $p - 1$.
Then $G^2 = \langle 1 + p \rangle \times \langle a^2 \rangle$.

Theorem 14 [QR5]: If p is prime and GCD$(p, ab) = 1$ then $(ab \mid p) = (a \mid p) + (b \mid p)$.
Proof: $\mathbb{Z}_p^{\#}$ is an abelian group under multiplication.
$\theta: \mathbb{Z}_p^{\#} \to \mathbb{Z}_p^{\#}$ defined by $\theta(x) = x^2$ is a homomorphism.
$\ker \theta = \{\pm 1\}$.
$\text{im } \theta = (\mathbb{Z}_p^{\#})^2$.
So $(\mathbb{Z}_p^{\#})^2$ is a subgroup of index 2.

Hence $\mathbb{Z}_p^{\#}/(\mathbb{Z}_p^{\#})^2 \cong \mathbb{Z}_2$.
So the map $a \to (a \mid p)$ 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 15 [QR7]: If p is an odd prime $(-1 \mid p) \equiv \frac{p-1}{2}$ (mod 2).
Proof: $\mathbb{Z}_p^{\#}$ is cyclic of order $p - 1$, say $\langle a \rangle$.
$(a^{1/2(p-1)})^2 = 1$, 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.

§3.7. The Quadratic Reciprocity Theorem

Theorem 16: For all $b \in \mathbb{Z}_p^{\#}$, $b^{1/2(p-1)} = (-1)^{(b \mid p)}$.
Proof: $\mathbf{Z}_p^{\#}$ 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 and 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 $\mathbf{M_p^q}$ be this number, modulo 2.

Theorem 17: $M_p^q = (q \mid p)$.

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 $qb_1, \ldots, qb_M$ are in B (all distinct).

Hence $-qb_1, \ldots, -q_M$ are all in A (all distinct).

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

If $qa_i = -qb_j$ 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 $qa_1, \ldots, qa_{h-M}, -qb_1, \ldots, -qb_M$ is a permutation of A.

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

Theorem 18: $M_p{}^q \equiv \sum_{i=1}^{h} \left[\frac{iq}{p}\right] + \frac{(q-1)(p^2-1)}{8} \pmod 2$

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 15, 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 $\sum_{i\in A} r_i = \sum_{i\in A_0} r_i + \sum_{i\in A_1} r_i \equiv \frac{p^2-1}{8} \pmod 2$.

Moreover $\sum_{i\in A} i = \frac{p^2-1}{8}$.

Now $q\sum_{i\in A} i = p\sum_{i\in A}\left[\frac{iq}{p}\right] + Mp + \sum_{i\in A} r_i$

Hence $(q-1)\left(\frac{p^2-1}{8}\right) \equiv p\left(M + \sum_{i\in A}\left[\frac{iq}{p}\right]\right) (\mathrm{mod}\, 2)$

Since p is odd the result follows.

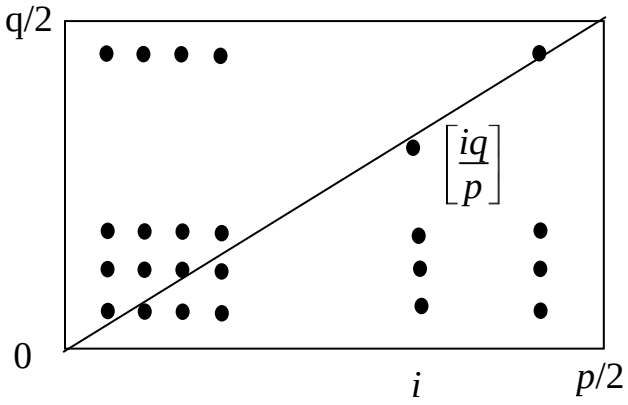
Theorem 19 [QR8]: If p is an odd prime $(2 \mid p) = \frac{1}{2}\left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right)$.

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

Theorem 20 (EISENSTEIN):

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

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



Since $p \neq q$ no lattice points lie on the diagonal.

The number of lattice points in the lower triangle is $\sum_{i=1}^{\frac{p-1}{2}}\left\lfloor \frac{iq}{p} \right\rfloor$ and the number in the upper triangle is $\sum_{i=1}^{\frac{q-1}{2}}\left\lfloor \frac{ip}{q} \right\rfloor$.

Theorem 21 [QR6]: (GAUSS' RECIPROCITY THEOREM):
If p, q are different odd primes then $(q \mid p) = (p \mid q) + (-1 \mid p)(-1 \mid q)$.
Proof: $(p \mid q) + (q \mid p) \equiv \sum_{i=1}^{\frac{q-1}{2}}\left\lfloor \frac{ip}{q} \right\rfloor + \sum_{i=1}^{\frac{p-1}{2}}\left\lfloor \frac{iq}{p} \right\rfloor \equiv \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right) \equiv (-1 \mid p)(-1 \mid q).$

§3.8. The Number of Square Roots

The next level of enquiry about square roots modulo m is to ask "how many square roots there are?" We denote the number of square roots of a mod m by $\#(a \mid m)$. If p is an odd prime and $0 \neq a \in \mathbb{Z}_p$ with a square root in $\mathbb{Z}_p$ then it has exactly two square roots. This is because $\mathbb{Z}_p$ is a field and so the quadratic $x^2 - 1$ has two zeros. Alternatively, $\mathbb{Z}_p^{\#}$ is a cyclic group of even order $p - 1$ and so has exactly one element of order 2, namely -1. The two square roots have the form $\pm x$. We can generalise this to the case where the modulus is a power of p.

Theorem 22: If p is an odd prime, coprime to a and $(a \mid p^n) = 0$ then $\#(a \mid p^n) = 2$.
Proof: Suppose p is an odd prime not dividing a.

Suppose that there exists x such that $x^2 \equiv a \pmod{p^n}$.
If $y^2 \equiv a \pmod{p^n}$ then $(x - y)(x + y) \equiv 0 \pmod{p^n}$.
Since p is odd then p can't divide both factors, so either $p^n \mid x - y$ or p $\mid x + y$.
Hence $x \equiv \pm y \pmod{m}$ and so a has exactly two square roots modulo p^n.

Theorem 23: If m, n are coprime then $\#(a \mid mn) = \#(a \mid m).\#(a \mid n)$.
Proof: In $\mathbb{Z}_m \times \mathbb{Z}_n$, $(a, b)^2 = (c, d)$ if and only if $a^2 = c$ and $b^2 = d$.
Hence the number of square roots of $(c, d) = \#(c \mid m).\#(c \mid d)$.
But $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ and so the result follows.

Example 7: Find $\#(100 \mid 6615)$.
Solution: $\#(100 \mid 6615) = \#(100 \mid 3^3.5.7^2)$
$= \#(100 \mid 3^3).\#(100 \mid 5).\#(100 \mid 7^2)$ by Theorem 22
$= 2^3 = 8$ by Theorem 21.

Theorem 24: Suppose a is odd.
(1) If $2n + 1 < m$ then $\#(2^{2n+1}.a \mid 2^m) = 0$.
(2) If $n < m$ then $\#(2^{2n}a^2 \mid 2^{2m}) = \begin{cases} 2^{n+2} \text{ if } n \le m - 2 \\ 2^{n+1} \text{ if } n = m - 1 \end{cases}$.
(3) If $n \le m$ then $\#(2^{2n}a^2 \mid 2^{2m+1}) = \begin{cases} 2^{n+2} \text{ if } n \le m - 1 \\ 2^n \text{ if } n = m \end{cases}$.

Proof:

(1) Let $x = 2^r u$ where u is odd and suppose that $x^2 \equiv 2^{2n+1}.a \pmod{2^m}$.

Hence $2^{2r}u^2 - 2^{2n+1}.a \equiv 0 \pmod{2^m}$.

If $2r < 2n + 1$ then $2^{2r}(u^2 - 2^{2(n-r)}.a) \equiv 0 \pmod{2^m}$.

Hence $u^2 - 2^{2(n-r)+1}.a$, which is odd, is divisible by 2^{m-2r}.

But if $2r = m$ then $x^2 \equiv 0 \pmod{m}$, a contradiction.

So $u^2 - 2^{2(n-r)+1}$ is even, a contradiction.

If $2r > 2n + 1$ then $2^{2n+1}(2^{2(r-n)-1}.u^2 - a) \equiv 0 \pmod{2^m}$.

Hence $2^{2(r-n)-1}.u^2 - a$, which is odd, is divisible by 2^{m-2n-1}.

But $m - 2n - 1 > 0$ so $2^{2(r-n)-1}.u^2 - a$ is even, a contradiction.

(2) Let $x = 2^r u$ where u is odd and suppose that $x^2 \equiv a^2 2^{2n} \pmod{2^{2m}}$.

Then $2^{2r}u^2 - 2^{2n}a^2$ is divisible by 2^{2m}.

Clearly $r = n$.

Hence $2^{2n}(u^2 - a^2)$ is divisible by 2^{2m} and so $u^2 \equiv a^2 \pmod{2^{2(m-n)}}$.

If $n \leq m - 2$, then $2(m - n) \geq 4$ and so $\mathbb{Z}_2{}^{2(m-n)\#} \cong C_2 \times C_2{}^{2(m-n)-1}$.

This has 4 elements whose square is 2.

It follows that there are 4 possibilities for u, modulo $2^{2(m-n)}$.

So there are $4.2^n = 2^{n+2}$ possibilities modulo 2^{2m-n}.

Hence $\#(a^2 2^n \mid 2^m) = 2^{n+2}$.

If $n = m - 1$ then $2(m - n) = 2$ and so $\mathbb{Z}_{2^{2(m-n)^\#}} = \mathbb{Z}_4^{\#} \cong C_2$.
This has 2 elements whose square is 2.
It follows that there are 2 possibilities for u, modulo $2^{2(m-n)}$.
So there are $2.2^n = 2^{n+1}$ possibilities modulo 2^{2m-n}.
Hence $\#(a^2 2^{2n} \mid 2^{2m+1}) = 2^{n+1}$.

(3) The proof is similar.

Example 8: Find $\#(a \mid m)$ for $a < m \leq 1024$ where a, m are powers of 2.
Solution:

#(a | m)	**1**	**2**	**4**	**8**	**16**	**32**	**64**	**128**	**256**	**512**	**1024**
1		1	2	4	4	4	4	4	4	4	4
2			0	0	0	0	0	0	0	0	0
4				2	4	8	8	8	8	8	8
8					0	0	0	0	0	0	0
16						4	8	16	16	16	16
32							0	0	0	0	0
64								8	16	32	32
128									0	0	0
256										16	32
512											0

§3.9. 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 root modulo mn.

Example 9: Find the square roots of 4 modulo 91.

Solution: $91 = 7.13$.

The square roots of 4 mod 7 are ± 2, that is, 2, 5.

The square roots of 4 mod 13 are ± 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 $x_1 = -1$.

$7x \equiv 1 \pmod{13} \equiv 14 \pmod{13}$ gives $x_2 = 2$. (Note we are justified in dividing by 7 as it is coprime to the modulus.)

So take $x = 13.(-1).2 + 7.11.2 = 128 \equiv 37$.

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 ± pair for the first modulus.

Example 10: Find the square roots of 15 modulo 71^2.
Solution: We know from theorem 21 that there are two solutions.
Suppose $x^2 \equiv 15 (\text{mod } 71^2)$.
Hence $x^2 \equiv 15 (\text{mod } 71)$.
We solve this by examining squares mod 71, up to 35^2 and discover that
$x \equiv \pm 21 (\text{mod } 71)$.
If $x \equiv 21 (\text{mod } 71)$ then $x = 21 + 71k$ for some integer k.
Thus $x^2 \equiv 21^2 + 71^2k^2 + 2.21.71k (\text{mod } 71^2)$
$\equiv 441 + 2982k (\text{mod } 71^2)$.
Therefore $441 + 2982k \equiv 15 (\text{mod } 71^2)$.
and so $2982k \equiv -426 (\text{mod } 71^2)$.
Hence $1491k \equiv -213 (\text{mod } 71^2)$
and so $21k \equiv -3 (\text{mod } 71)$, on dividing by 71.
Thus $7k \equiv -1 \equiv 70 (\text{mod } 71)$ and so $k \equiv 10 (\text{mod } 71)$.
This gives $x \equiv 21 + 10.71 \equiv 731$.
The other square root is clearly $-731 \equiv 4310 (\text{mod } 71^2)$.
So the square roots of 15 modulo 71^2 are 731 and 4310.

If the modulus is a large prime we can only find the two square roots by searching. We need to compute squares of elements of $\mathbb{Z}_p$ up to $\left(\frac{p-1}{2}\right)^2$.

EXERCISES FOR CHAPTER 3

Exercise 1: Solve $5x^2 + 7x + 12 \equiv 0 (\text{mod } 17)$.

Exercise 2: Solve $x^2 + x + 1 \equiv 0 (\text{mod } 23)$.

Exercise 3: Show that if p is a prime of the form $3n + 2$ then $x^2 + x + 1 \equiv 0 (\text{mod } p)$ has no solutions.
[**HINT:** Do you recognise the polynomial $x^2 + x + 1$ in relation to the cube roots of 1?]

Exercise 4: Find (125 | 196).

Exercise 5: Find (527 | 1093).

Exercise 6: Find (217 | 1093).

Exercise 7: Find (65 | 256).

Exercise 8: If p, q, r, s are distinct odd primes find #(9 | $pq^2r^3s^4$).

SOLUTIONS FOR CHAPTER 3

Exercise 1: $x \equiv \dfrac{-7 \pm \sqrt{49 - 240}}{10}$

$$\equiv \frac{-7 \pm \sqrt{-191}}{10}$$

$$\equiv \frac{-7 \pm \sqrt{13}}{10}$$

Now, mod 17, the squares are as follows:

x	0	1	2	3	4	5	6	7	8
$\mathbf{x^2}$	0	1	4	9	16	13	2	15	13

Hence $x \equiv \dfrac{-7 \pm 5}{10} \equiv \dfrac{-12}{10}, \dfrac{-2}{10} \equiv \dfrac{-6}{5}, \dfrac{-1}{5} \equiv 10, 9.$

Exercise 2: $x = \dfrac{-1 \pm \sqrt{-3}}{2} \equiv \dfrac{-1 \pm \sqrt{20}}{2}$.

Now, mod 23, the squares are as follows:

x	0	1	2	3	4	5	6	7	8	9	10	11
$\mathbf{x^2}$	0	1	4	9	16	2	13	3	18	12	8	6

Since 20 has no square root mod 23, there are no solutions.

Exercise 3: If $x^2 + x + 1 \equiv 0 (\text{mod } p)$ then $x^3 - 1 = (x - 1)(x^2 + x + 1) \equiv 0 (\text{mod } p)$.

But clearly $p \neq 3$ and so $x \equiv 1$ is not a solution to the quadratic. Hence x is an element of order 3 in $Z_p^{\#}$. Thus, $p - 1$ is a multiple of 3, a contradiction.

Exercise 4: $(125 \mid 196) = (125 \mid 4.49)$

$= (125 \mid 4) + (125 \mid 49) + (125 \mid 4).(125 \mid 49).$

$(125 \mid 4) = (1 \mid 4) = 1.$

$(125 \mid 49) = (27 \mid 49)$

$= (27 \mid 7^2)$

$= (27 \mid 7)$

$= (6 \mid 7)$

$= (-1 \mid 7)$

$= \frac{6}{2}$

$= 3$

$= 1 \pmod 2.$

$\therefore (125 \mid 196) = 1 + 1 + 1.1 = 1 \pmod 2.$

[This means that 125 is not a square mod 196.]

Exercise 5: (629 | 1093) = (17.37 | 1093)

= (17 | 1093) + (37 | 1093).

(17 | 1093) = (1093 | 17) + (–1 | 17)(–1 | 17)(–1 | 1093) by Gauss reciprocity

(1093 | 17) = (5 | 17)

= (17 | 5) + (–1 | 17)(–1 | 5) by Gauss reciprocity

= (2 | 5) + 8 + 2

= 1 + 0 + 0 (mod 2)

= 1.

(37 | 1093) = (1093 | 37) + (–1 | 37)(–1 | 1093) by Gauss reciprocity

= (20 | 37) + 18.546

= (20 | 37) mod 2

= (5 | 37) + 2(2 | 37)

= (5 | 37)

= (37 | 5) + (–1 | 5)(–1 | 37)

= (2 | 5) + 2.18

= (2 | 5)

= ½ 2.3

= 3

= 1

∴ (629 | 1093) = 1 + 1

= 0.

[This means that 629 is a square mod 1093.]

Exercise 6:

(217 | 1093) = (7.31 | 1093)

= (7 | 1093) + (31 | 1093), since 1093 is prime and GCD(1, 31) = 1

= (1093 | 7) + (–1 | 7)(–1 | 1093) by Gauss reciprocity

= (1 | 7) + 3.546

= 0 (mod 2)

[This means that 217 is a square mod 1093.]

Exercise 7: $(65 \mid 2^8) = 0$ if and only if $65 \equiv 1 \pmod 8$.
Hence $(65 \mid 256) = 0$.
[This means that 65 is a square root mod 258.]

Exercise 8: Clearly 9 is a square modulo any prime.
$\therefore \#(9 \mid pq^2r^3s^4) = \#(9 \mid p).\ \#(9 \mid q^2).\ \#(9 \mid r^3).\ \#(9 \mid s^4).$
$= 2^4 = 16.$