**Theorem 50** Any finite field $\mathbb{F}$ has $p^n$ elements for some $n \geq 1$, where $p$ is a prime.

Proof. First note that $\mathbb{F}$ satisfies the axioms A, M and D and one other axiom: If $x \in \mathbb{F}$, with $x \neq 0$, there exists $y \in \mathbb{F}$ such that $xy = 1$.

Retain the axioms A for all of $\mathbb{F}$. We retain only part of the axioms M and D, as follows:

$\mathbb{F}$ is a finite set containing $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ with two binary operations, addition and scalar multiplication. Addition satisfies the axioms A from Lecture 9, SM Scalar multiplication:

- **SM0**: If $x \in \mathbb{F}$ and $\alpha \in \mathbb{Z}_p$, then $\alpha x \in \mathbb{F}$.
- **SM1**: $\alpha (\beta x) = (\alpha \beta) x$ for all $\alpha, \beta \in \mathbb{Z}_p$ and for all $x \in \mathbb{F}$.
- **SM2**: $1 \cdot x = x$ for all $x \in \mathbb{F}$, $1 \in \mathbb{Z}_p$.
- **SMD**: $(\alpha + \beta) x = \alpha x + \beta x$, for all $\alpha, \beta \in \mathbb{Z}_p$, and for all $x \in \mathbb{F}$

$$\alpha (x + y) = \alpha x + \alpha y, \text{ for all } \alpha \in \mathbb{Z}_p \text{ and for all } x, y \in \mathbb{F}.$$ 

It follows that $\mathbb{F}$ is now an vector space over the field $\mathbb{Z}_p$. Since $\mathbb{F}$ is finite, it is finite dimensional as $\mathbb{Z}_p$-vector space. Let $v_1, v_2, \ldots, v_n$ be a basis for $\mathbb{F}$ as $\mathbb{Z}_p$ vector space. Then every element of $\mathbb{F}$ can be uniquely written in the form

$$\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n,$$

where $\alpha_i \in \mathbb{Z}_p$. Hence there are exactly $p^n$ elements in $\mathbb{F}$.

This completes the proof.

I am including this only for information purposes. It is not impossibly difficult to prove ... I just won’t give a proof here. It is a remarkable result.

**Theorem 51** There is one and only one field $\mathbb{F}$ of order $p^n$ for every prime $p$ and for every integer $n \geq 1$, up to isomorphism. Thus every finite field has the form $\mathbb{Z}_p[x]_{\phi(x)}$, for some prime polynomial $f(x) \in \mathbb{Z}_p[x]$ of degree $n$.

I want to end this here by looking for a second at the fields of real and complex numbers. Consider first the ring $\mathbb{R}[x]$ of all polynomials with real coefficients. This is a perfectly standard ring with a Division Algorithm and hence a Euclidean Algorithm. It was the subject of Gauss’s PhD thesis which showed that the prime polynomials in $\mathbb{R}[x]$ are linear polynomials and certain quadratics $ax^2 + bx + c$ whose discriminant $\Delta = b^2 - 4ac < 0$). Indeed Gauss showed that every polynomial in $\mathbb{R}[x]$ is a product of linear and quadratic polynomials.

I want us here to look at one prime quadratic polynomial, $x^2 + 1 \in \mathbb{R}[x]$. This polynomial has no roots in $\mathbb{R}$ obviously and so is prime and by Theorem 48 $\mathbb{R}[x]_{x^2 + 1}$ is a field. It is clear that its
elements are the linear polynomials \(a + bx\), since every polynomial leads to such a polynomial on division by \(x^2 + 1\).

There is an obvious isomorphism between \(\mathbb{R}[x]_{x^2+1}\) and \(\mathbb{C}\) given by \(\varphi : a + bx \rightarrow a + ib\).

Hence we could have constructed \(\mathbb{C}\) as a collection of remainders of polynomials in \(\mathbb{R}[x]\) modulo \(x^2 + 1\). This would obviate the need to introduce the 'imaginary' number \(i = \sqrt{-1}\), as we needed to do to produce \(\mathbb{C}\). Thus the complex numbers are no more nor less imaginary than the so-called real numbers.

**Theorem 52** \(\mathbb{C} \cong \mathbb{R}[x]_{x^2+1}\).

**SQUARES AND QUADRATIC RECIPROCITY**

**Squares in** \(\mathbb{Z}_p\)

We will say that an element \(x \in \mathbb{Z}_p\), where \(p\) is a prime, is a square, if it is non-zero and if there is an element \(y\) such that \(x = y^2\). The historical term for square is Quadratic Residue, but I prefer to use the more natural term, square. Similarly, rather than speak about the Quadratic Non-residues, I will speak about non-squares. Thus an element \(x \in \mathbb{Z}_p\) is a non-square if \(x \neq 0\) and \(x\) is not a square.

If time permits, I will show you a beautiful proof that generators exists in \(\mathbb{Z}_p^*\), for any prime \(p > 2\). For now just believe it.

**Definition** Define \(S_p = \{x : x \neq 0 \text{ and } x = y^2, \text{ for } y \in \mathbb{Z}_p\}\). Similarly, define \(N_p = \mathbb{N} = \mathbb{Z}_p^* \setminus S\).

So we will refer to \(S\) as the squares in \(\mathbb{Z}_p\) and \(\mathbb{N}\) as the non-squares.

**Theorem 57** \(|S| = |N| = \frac{p-1}{2}\), if \(p \geq 3\).

Proof. Since

\[
\mathbb{Z}_p = \{0, 1, 2, \ldots, \frac{p-1}{2}, \frac{p+1}{2}, \ldots, p-1\} \\
\equiv \{0, 1, 2, \ldots, \frac{p-1}{2}, -\frac{p-1}{2}, \ldots, -1\} \pmod{p},
\]

it follows that

\[
S \subseteq \{1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2\}.
\]

Hence \(|S| \leq \frac{p-1}{2}\).

Suppose that \(1 \leq a, b \leq \frac{p-1}{2}\), and \(a^2 \equiv b^2 \pmod{p}\). Then \(p\) divides \(a^2 - b^2 = (a + b)(a - b)\) and so by Lemma 24, either \(p\) divides \(a + b\) or \(p\) divides \(a - b\). Since \(|a \pm b| < p\) it follows that \(a - b = 0\). Hence \(|S| = \frac{p-1}{2}\).
Since $Z_p$ is the disjoint union of $\{0\}$, $S$ and $N$ it follows that $|S| = |N| = \frac{p - 1}{2}$. Note that $N_2 = \emptyset$.

This completes the proof.

The squares in $Z_p$ are an extremely intriguing collection of numbers, numbers which held Gauss’s attention for most of his life. Here is a list of squares and non-squares for some different primes.

$S_2 : 1 \quad N_2 : \emptyset$

$S_3 : 1 \quad N_3 : 2$

$S_5 : 1, 4 \quad N_5 : 2, 3$

$S_7 : 1, 2, 4 \quad N_7 : 3, 5, 6$

$S_{11} : 1, 3, 4, 5, 9 \quad N_{11} : 2, 6, 7, 8, 10$

$S_{13} : 1, 3, 4, 9, 10, 12 \quad N_{13} : 2, 5, 6, 7, 8, 11$

$S_{17} : 1, 2, 4, 8, 9, 13, 15, 16 \quad N_{17} : 3, 5, 6, 7, 10, 11, 12, 14$

$S_{19} : 1, 4, 5, 6, 7, 9, 11, 16, 17 \quad N_{19} : 2, 3, 8, 10, 12, 13, 14, 15, 18$

$S_{23} : 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18 \quad N_{23} : 5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22.$

There are very many interesting properties of these numbers. For example, one can see that if we multiply any two elements of $S_p$ modulo $p$ we get an element of $S_p$. This, with some related (but different) properties of $N_p$, is a general property for every prime $p$.

There are other properties ... for example if we add the numbers in $S_p$ and $N_p$, we get the following situation:

\[
\begin{array}{ccc}
  p & \sum S_p & \sum N_p \\
  2 & 1 & 0 \\
  3 & 1 & 2 \\
  5 & 5 & 5 \\
  7 & 7 & 14 \\
 11 & 22 & 33 \\
 13 & 39 & 39 \\
 17 & 68 & 68 \\
 19 & 76 & 95 \\
 23 & 92 & 161 \\
\end{array}
\]

It seems to be true (and indeed it is true for every prime $p > 3$) that:

(i) Both the sum of the squares and the sum of the non-squares is a multiple of $p$ if $p \geq 5$.

(ii) If $p \equiv 1 \pmod{4}$ and $p \geq 5$ the sum of the non-squares is equal to the sum of the squares.
(iii) For $p \equiv -1 \pmod{4}$ with $p \geq 5$, the sum of the non-squares is strictly greater than the sum of the squares.

(i) and (ii) are true and relatively easy to prove. (iii) is also true, but there is no proof known which does not involve complex analysis and deep mathematics. This is curious given that it is a problem which can be stated so simply and appears to be completely elementary. This of course is not an unusual situation in the theory of numbers.