Quadratic Maths

The field $\mathbb{F}_p$

Theorem

For any prime number p, $\mathbb{F}_p = \mathbb{Z}/p$ is a field.

Proof

RTP that $\forall a \in \mathbb{F}_p$, a has a multiplicative inverse mod p. We argue by induction on $a \in \mathbb{F}_p$. Let $k = \min\{i \in \mathbb{Z} : ai \geq p\}$. Then $a(k-1) \leq p-1$ and so $p \leq ak \leq p + a - 1$. By the induction hypothesis $\exists l$ such that $(ak)l \equiv 1 \mod p$, and so $a^{-1} = kl$.

Theorem (Fermat)

For any $a \in \mathbb{F}_p^*$, $a^{p-1} = p$.

Proof

Consider the subgroup $\langle a \rangle$ generated by a,

$$\langle a \rangle = \{1, a, a^2, \ldots, a^{i-1}\},$$

where i is the order of a. By Lagrange's theorem, $i \mid p-1$, so $p - 1 = ik$ for some $k \in \mathbb{Z}$. Then $a^{p-1} = a^{ik} = 1^k = 1$ as required.

Theorem

$\mathbb{F}_p^*$ is cyclic of order $p-1$, i.e. $\mathbb{F}_p^* = C_{p-1}$.

Proof

See lecture notes.

Quadratic residues

A quadratic residue modulo p is an element $a \in \mathbb{F}_p^*$ such that the congruence $x^2 \equiv a \mod p$ is soluble.

The quadratic residues modulo p form a subgroup of $\mathbb{F}_p$. If p is an odd prime then there are precisely $(p-1)/2$ quadratic residues and $(p-1)/2$ non-residues modulo p. To prove this, consider the representation of $\mathbb{F}_p$ as the group generated by a primitive root g: $\mathbb{F}_p = \langle g \rangle = \{1, g, g^2, \ldots, g^{p-2}\}$.

We define the Legendre symbol $(\frac{a}{p})$ by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue} \pmod{p} \\ -1 & \text{if } a \text{ is a quadratic non-residue} \pmod{p}. \end{cases}$$

Theorem (Euler's criterion)

Let p be an odd prime, and $a \in \mathbb{F}_p$. Then

$$a^{(p-1)/2} = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue} \pmod{p} \\ -1 & \text{if } a \text{ is a quadratic non-residue} \pmod{p}. \end{cases}$$

In other words,

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

Proof

Let g be a primitive root of $\mathbb{F}_p$. Then $a = g^i$ for some i, and a is a quadratic residue $\bmod p$ if and only if i is even. Now $a^{(p-1)/2} = g^{i(p-1)/2}$ and therefore we need to prove that $h = g^{(p-1)/2} = -1$. But $h^2 = 1$ and $h \neq 1$, and since there are at most two square roots of unity, h must be equal to -1.

Theorem

Let p be an odd prime. Then -1 is a square modulo p if and only if $p \equiv 1 \pmod{4}$.

Proof

Apply Euler's criterion.

Theorem (Gauss' lemma)

Let p be an odd prime, and $a \in \mathbb{F}_p^*$. Consider the set of multiples of a,

$$a, 2a, 3a, \ldots, Pa$$

where $P = (p-1)/2$. Represent each of these elements of $\mathbb{F}_p$ by an integer in the range $(-p/2, p/2)$, and let ν be the number of negative integers in this list. Then $(\frac{a}{p}) = (-1)^\nu$.

Proof

Since $\mathbb{F}_p$ is a field, none of the entries in the list is zero, so they all lie in the set $\{\pm 1, \pm 2, \ldots, \pm P\}$. Also, no two of the numbers are equal, since $ka \equiv la \pmod{p}$ implies $k \equiv l \pmod{p}$, which implies that $k = l$ (since $1 \leq k, l \leq P$). Further, none of the numbers is equal to the negative of another one, since $ka \equiv -la \pmod{p}$ implies $k + l \equiv 0 \pmod{p}$, which is impossible.

Therefore, we have

$$(a)(2a)\ldots(Pa) \equiv (\pm 1)(\pm 2)\ldots(\pm P) \pmod{p}$$

where the number of minus signs on the right is equal to ν. Hence $a^P \equiv (-1)^\nu \pmod{p}$, and so by Euler's criterion

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

as required.

Theorem

For an odd prime p

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1 & \text{if } p \equiv \pm 3 \pmod 8. \end{cases}$$

Proof

Consider the set $\{2, 4, 6, \ldots, 2P\}$. By Gauss' lemma, 2 is a quadratic residue modulo p if and only if the number ν of these numbers which lie in the interval $(-p/2, 0)$ is even. But ν is just the number of even integers in the interval $[(p+1)/2, p-1]$.

Now suppose that $(p+1)/2$ is even, i.e. $p \equiv 3 \pmod 4$. Then

$$\nu = \frac{(p-1) - (p+1)/2}{2} + 1 = \frac{p+1}{4}$$

and so

$$\left(\frac{2}{p}\right) = (-1)^{(p+1)/4} = \begin{cases} 1 & \text{if } p \equiv 7 \pmod 8 \\ -1 & \text{if } p \equiv 3 \pmod 8. \end{cases}$$

Alternatively, if $(p+1)/2$ is odd, i.e. $p \equiv 1 \pmod 4$. Then

$$\nu = \frac{(p-1) - (p+3)/2}{2} + 1 = \frac{p-1}{4}$$

and so in this case

$$\left(\frac{2}{p}\right) = (-1)^{(p-1)/4} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 8 \\ -1 & \text{if } p \equiv 5 \pmod 8. \end{cases}$$

Combining these two cases gives the required result.

Theorem (Law of quadratic reciprocity)

For any two distinct odd primes p and q,

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

Proof

See lecture notes.

Quadratic forms

Definitions

A *binary quadratic form* is a polynomial of the form $ax^2 + bxy + cy^2$ with integer coefficients. We say that an integer n is *represented* by a binary quadratic form $ax^2 + bxy + cy^2$ if there are integers x and y such that $ax^2 + bxy + cy^2 = n$. Two quadratic forms $f(x, y)$ and $g(x, y)$ are said to be *equivalent* if there exists an element $A = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$ of $SL(2, \mathbb{Z})$ such that if we write

$$\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

then $g(x, y) = f(X, Y)$.

Theorem

Two equivalent binary quadratic forms represent the same set of integers.

Proof

If an integer n is represented by g then there exist x, y such that $g(x, y) = n$. But then let X, Y be defined by the equation above — then X and Y are integers and $f(X, Y) = g(x, y) = n$, so n is represented by f. Conversely, since A is invertible in $SL(2, \mathbb{Z})$ then any integer represented by f is also represented by g.

Theorem

A prime number p can be represented by a binary quadratic form f if and only if there is a binary form equivalent to f which is of the form $px^2 + dxy + ey^2$ for some integers d and e.

Proof

Obviously any form $px^2 + dxy + ey^2$ represents p, so if f is equivalent to such a binary quadratic form then f represents p.

Conversely, suppose f represents p. Then there exist x, y such that $f(x, y) = p$. To find a binary quadratic form $px^2 + dxy + ey^2$ which is equivalent to f we need to find an element A of $SL(2, \mathbb{Z})$ which takes $\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$ to $\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)$. Then if we let $g(x, y) = f(A(x, y))$ then $g(1, 0) = f(x, y) = p$ and so g must be of the required form. Now x and y must be coprime (since $\mathrm{hcf}(x, y) \mid p$). It follows by the Euclidean algorithm that there are integers a and b such that $ax + by = 1$. Then the matrix $\begin{pmatrix} x & -b \\ y & a \end{pmatrix}$ satisfies our requirements — it is in $SL(2, \mathbb{Z})$ and it sends $\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$ to $\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)$, as required.

Definition

The *discriminant* of a binary quadratic form $ax^2 + bxy + cy^2$ is $b^2 - 4ac$. The discriminant is invariant under the action of $SL(2, \mathbb{Z})$. A binary quadratic form has negative discriminant iff it is either positive or negative definite.

Reduced forms

Definition

A *reduced* binary quadratic form is one whose coefficients satisfy

$$\begin{array}{rrcr} \text{either} & c > a & \text{and} & -a < b \leq a \\ \text{or} & c = a & \text{and} & 0 \leq b \leq a. \end{array}$$

The reduction algorithm

Let the form $ax^2 + bxy + cy^2$, denoted (a, b, c), be positive definite. Then apply the following two operations alternately until the conditions for neither operation are satisfied:

1. If $c < a$, replace (a, b, c) by the equivalent form $(c, -b, a)$.
2. If $|b| > a$, replace (a, b, c) by the equivalent form (a, b_1, c_1), where $b_1 = b + 2ua$, the integer u being chosen such that $|b_1| \leq a$, and c_1 is chosen to satisfy $b_1^2 - 4ac_1 = b^2 - 4ac$.

Theorem

Any positive definite binary quadratic form is equivalent to a (unique) reduced form.

Proof

Apply the reduction algoithm. First we need to check that the forms produced by the algorithm are equivalent to the original form. That is, for each operation we need to find an element of $SL(2, \mathbb{Z})$ which takes the original form to the form produced by that operation. In operation 1, the required element is $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, and in operation 2 the required element is $\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$.

First note that a and c must always be greater than 0, since the form is positive definite. Now, in operation 1 we diminish a without affecting the value of $|b|$, and in operation 2 we diminish $|b|$ without affecting the value of a. Thus it is easy to see that in a finite number of steps we will reach a form satisfying $a \leq c$ and $|b| \leq a$.

Finally, if $b = -a$ we can apply operation 2 again to change b to $+a$, and if $a = c$, $|b| < 0$ then we can apply operation 1 one last time to make b positive. Then the resulting form is reduced.

Definition

For a negative integer d, the *class number* $C(d)$ of d is the number of equivalence classes of positive definite forms with discriminant d.

Theorem

For any $d < 0$, the class number $C(d)$ is finite.

Proof

$C(d)$ is equal to the number of reduced forms with discriminant d. Let $D = -d$. Then every such form (a, b, c) satisfies $a, c > 0$, $c \geq a$, $|b| \leq a$ and $4ac - b^2 = D$. Therefore $b^2 \leq a^2 \leq ac$, and so $3ac \leq D$. But there are only a finite number of positive integral values for a and c satisfying

this inequality, and for each such pair there are at most two suitable values for b. Hence there are only a finite number of reduced forms of discriminant d, and so $C(d)$ is finite.

Enumeration of reduced forms

To enumerate all the reduced forms of discriminant $D < 0$, notice first that $b^2 \leq ac \leq D/3$. Notice also that since $D = 4ac - b^2$ then b must be even if $D \equiv 0 \pmod 4$ and b must be odd if $D \equiv 3 \pmod 4$ (if $d \equiv 1 \pmod 4$). Therefore, choose all sufficiently small values of b of the correct parity, and for each such value factorize $ac = (D + b^2)/4$ in every possible way. Finally, reject those triples (a, b, c) which do not satisfy the conditions for a reduced form.

Theorem

A prime number p can be represented by some form of discriminant d if and only if $\exists q \in \mathbb{Z}/(4p)$ such that $q^2 \equiv d \pmod{4p}$.

Proof

Suppose that p is represented by some form of determinant d. Then p is represented by some form $px^2 + qxy + ry^2$, where $q^2 - 4pr = d$, and so $q^2 \equiv d \pmod{4p}$. Conversely, suppose that there exists such a q with $q^2 \equiv d \pmod{4p}$. Then there exists r such that $q^2 - 4pr = d$, and so the form $px^2 + qxy + ry^2$ has determinant d and represents p.