1 Modular arithmetics

Theorem 1 (Division algorithm)**.** Given any integers a and b, with $a > 0$, there exist unique integers q and r such that $a = qb + r$, $0 \le r < a$.

Theorem 2. If $g = (b, c)$, there exist unique integers x and y such that $g = bx + cy$. The result could generalize to greatest common divisor of more than two integers.

Theorem 3. If $g = (b, c)$, then g is the least positive linear combination of b and c, and g is divisible by every common divisor. $\implies$ if 1 is a linear combination of b and c, then $(b, c) = 1$.

Theorem 4 (Basic identities)**.** Let a, b, c, d denote integers, then

1. $a \equiv b \pmod{m}$ & $c \equiv d \pmod{m} \implies ac \equiv bd \pmod{m}$
2. $a \equiv b \pmod{m} \implies ac \equiv bc \pmod{mc}$

Theorem 5. Let f denote a polynomial taking integral coefficients. If $a \equiv b \pmod{m}$, then $f(a) \equiv f(b) \pmod{m}$.

Theorem 6. We have:

1. $ax \equiv ay \pmod{m} \iff x \equiv y \pmod{\frac{m}{(a,m)}}$
2. $ax \equiv ay \pmod{m}$ & $(a, m) = 1 \implies x \equiv y \pmod{m}$
3. $x \equiv y \pmod{m_i}$ for $i = 1, \dots, r \iff x \equiv y \pmod{[m_1, \dots, m_r]}$

Theorem 7. If $b \equiv c \pmod{m}$, then $(b, m) = (c, m)$.

2 Primes

Definition: If $x \equiv y \pmod{m}$, then y is called a **residue** of x *modulo m*. A set of integers x_i is called a **complete residue system** *modulo m* if for every integer y there exists unique x_j such that $y \equiv x_j \pmod{m}$.
Definition: A **reduced residue system** *modulo m* is a set of integers r_i such that $(r_i, m) = 1$, $r_i \not\equiv r_j \pmod{m}$ if $i \ne j$, and such that every x prime to m is congruent *modulo m* to some member r_k in the set.
Definition: The number $\phi(m)$ is the number of positive integers $\le m$ and coprime to m.

Theorem 8 (Properties of ϕ)**.** We have:

1. $\phi(p) = p - 1$ for prime p.
2. $\phi(p^r) = p^r - p^{r-1}$ for prime p.
3. $\phi(mn) = \phi(m)\phi(n)$ if $(m, n) = 1$.

Theorem 9. Let $(a, m) = 1$. Let $\{r_i\}$ be a complete/reduced residue system *modulo m*, then $\{ar_i + b\}$ is a complete/reduced residue system *modulo m* respectively.

Theorem 10. a has an inverse $\pmod{n} \iff (a, n) = 1$

Theorem 11 (Fermat's theorem)**.** Let p denote a prime. If $p \not| a$ then $a^{p-1} \equiv 1 \pmod{p}$. For every integer a, $a^p \equiv a \pmod{p}$.

Theorem 12 (Euler's generalization of Fermat's theorem)**.** If $(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \pmod{m}$.

Theorem 13 (Failure of converse of Fermat's)**.** There are composite numbers n(e.g.$n = 531 = 3 * 11 * 17$) such that $a^{n-1} \equiv 1 \pmod{n} \forall a \in [1, n-1] \cap \mathbb{Z}, (a, n) = 1$

Theorem 14 (Wilson's theorem)**.** If p is a prime, then $(p-1)! \equiv -1 \pmod{p}$.

Theorem 15 (Converse of Wilson's)**.** If $(p-1)! \equiv -1 \pmod{p}$, then p is a prime.

Theorem 16 (Contrapositive of Fermat's)**.** If $\exists a \in [1, n-1] \cap \mathbb{Z}$ for which $a^{n-1} \not\equiv 1 \pmod{n}$, then n is not a prime.

Theorem 17. Let p be a prime number, then $x^2 \equiv -1 \pmod{p}$ has solutions $\iff p = 2 \vee p \equiv 1 \pmod{4}$.

3 Solution of congruences

Theorem 18. Suppose $n > 0$. Let $d = (a, n)$, then $ax \equiv b \pmod{n}$ has a solution $\iff d | b$. The solution is unique modulo $\frac{n}{d}$. There are d solutions modulo n.

Theorem 19 (Chinese remainder theorem)**.** Let $m_1, \dots, m_r$ denote a set of integers pairwise relatively prime. Let $a_1, \dots, a_r$ denote a set of integers. The system of

$$x \equiv a_i \pmod{m_i}$$

has a solution unique *modulo* $m_1 \dots m_r$.
One solution is constructed as $x_0 = \sum_{j=1}^{r} \frac{m}{m_j} b_j a_j$, where $m = \prod_{i=1}^{r} m_i$ and $b_j \frac{m}{m_j} \equiv 1 \pmod{m_j}$.

Remark: Chinese remainder theorem asserts that $\mathbb{Z}/\prod_{n_i} \mathbb{Z}$ is isomorphic to $\oplus_i \mathbb{Z}/n\mathbb{Z}$
Remark: If the moduli of the initial system are not coprime, factorize the moduli until all new moduli become coprime. Ignore duplicate terms. Claim no solution if inconsistency observed. If modulo a and modulo a^p occur, keep the one with higher power.
Definition: Let m denote a positive integer and a any integer such that $(a, m) = 1$. Let h be the smallest integer such that $a^h \equiv 1 \pmod{m}$. We say that the **order** of a modulo m is h.
Definition: If g has order $\phi(m)$ modulo m, then g is called a **primitive root** modulo m.

Theorem 20. If $(a, m) = 1$, then the order of a modulo m divides $\phi(m)$.

Theorem 21. If a has order h modulo m, then a^k has order $\frac{h}{(h,k)}$ modulo m.

Theorem 22. If a has order h modulo m, and b has order k modulo m, and if $(h, k) = 1$, then ab has order hk modulo m.

Theorem 23. n has a primitive root $\iff n$ is of the form $1, 2, 4, p^\alpha, 2p^\alpha$ for odd prime p.

Theorem 24. If n has a primitive root, then n has $\phi(\phi(n))$ primitive roots.

Theorem 25. If a is a primitive root modulo n. then $a^k \equiv a^j \pmod{n} \iff k \equiv j \pmod{\phi(n)}$. If b is not a primitive root but invertible modulo n, then $b^s \equiv b^t \pmod{n} \iff s \equiv t \pmod{h}$, where h is order of b modulo n.

Theorem 26. If a is a primitive root modulo n, then RRS(n) is a cyclic group generated by a.

Theorem 27. RRS(2^k)=$\{\pm 3^j : 0 \le j \le 2^{k-2}\} = \{\pm 5^j : 0 \le j \le 2^{k-2}\}$

Remark: We can now solve $x^m = c \pmod{n}$ for general n, by replacing modulo n by a system of moduli of prime factorization of n, which is equivalent by Chinese remainder theorem. For odd prime powers, solve the congruence by primitive root. For 2^k. solve by previous theorem. Combine the resultant linear congruences solved by CRT to form the final result.

4 Quadratic reciprocity

Theorem 28 (Hensel's lemma)**.** Suppose that $f(x)$ is a polynomial with integral coefficients. If $f(a) \equiv 0 \pmod{p^j}$ and $f'(a) \not\equiv 0 \pmod{p}$, then $\exists! t \pmod{p}$ such that $f(a + tp^j) \equiv 0 \pmod{p^{j+1}}$. To get this p, solve the linear congruence

$$tf'(a) \equiv -\frac{f(a)}{p^j} \pmod{p}$$

Definition: For all a such that $(a, m) = 1$, a is called a **quadratic residue** modulo m if the congruence $x^2 \equiv a \pmod{m}$ has a solution, otherwise a quadratic nonresidue modulo m.

Theorem 29. Let p be an odd prime, we have

1. a is QR modulo $p \iff a$ is QR modulo p^e $\forall e \ge 1$
2. Set of QR modulo $p = \{1^2, 2^2, \dots, (\frac{p-1}{2})^2\}$
3. If u is a primitive root modulo p, then set of QR modulo $p = \{u^{2k} : k \in \mathbb{Z}\}$

Definition: If p denotes an odd prime, then the **Legendre** symbol $\left(\frac{a}{p}\right)$ is defined to be 1 if a is a quadratic residue modulo p, -1 if a is a quadratic nonresidue modulo p, and 0 if $a | p$.

Theorem 30. Let p be an odd prime, then

1. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$
2. $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$
3. $a \equiv b \pmod{p} \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
4. If $(a, p) = 1$ then $\left(\frac{a^2}{p}\right) = 1$, $\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$
5. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. i.e. -1 is QR modulo $p \iff p \equiv -1 \pmod{4}$
6. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. i.e.2 is QR modulo $p \iff p \equiv 1, 7 \pmod{8}$

Theorem 31 (The Gaussian reciprocity law)**.** If p and q are distinct odd primes, then

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

Another way to state this is: If p and q are distinct odd primes of the form $4k + 3$, then one of the congruences $x^2 \equiv p \pmod{q}$ and $x^2 \equiv q \pmod{p}$ is solvable and the other is not. Otherwise, both congruences are simultaneously solvable or not solvable.

Theorem 32. For $n \in \mathbb{Z}$, we define set $S_2^n(a) = \{(x, y) \in \mathbb{Z}_n \times \mathbb{Z}_n : x^2 + y^2 \equiv a \pmod{n}\}$, then $\forall a \in U_n$ such that $S_2^n(a)$ is not empty, the cardinality is same, independent of choice of a. The result generalizes from sum of two squares to sum of arbitrarily many squares.

Theorem 33. For prime p, we have $|S_2^p(a)| = p - (-1)^{\frac{p-1}{2}}$ if $a \ne 0$, and $p + (-1)^{\frac{p-1}{2}}(p-1)$ if $a = 0$.

Theorem 34 (Characterization of Pythagorean triples)**.** (a, b, c) is a primitive triplet if $(a, b, c) = 1$ and $(a, b, c) = (s^2 - t^2, 2st, s^2 + t^2)$ for some relatively prime s, t with $s > t$ and $s \not\equiv t \pmod{2}$.

Theorem 35 (Chord and tangent argument)**.** Given a rational point on unit circle, draw any secant line through the rational point with rational slope, the other intersection is also a rational point, and all rational points could be found in this approach.

5 Diophantine equations

Theorem 36. For any $a, b \in \mathbb{Z}^+$, the equation $x^2 + y^2 + z^2 = 4^a(8b + 7)$ has no integral solution.

Theorem 37. $y^2 = x^3 + 7$ has no integral solution, but it has an integral solution for any modulo m.

Theorem 38. The system: $x^4 + y^4 = z^2, xyz \ne 0$ has no integral solution.

Theorem 39 (Fermat's descent)**.** Suppose the above equation has an integral solution (x, y, z), we are able to form another solution (x', y', z') such that $z' < z$. Since the descent is infinite, we obtain a contradiction.

6 Pell's equation

6.1 General setup

Diophantine equation of the form $x^2 - dy^2 = 1$. In general form, Diophantine equation of the form $x^2 - dy^2 = n$.
If $d < 0$, there are finitely many solutions to be found by trial. If d is a perfect square, we could factor into two linear Diophantine equations. We focus on the non-trivial case that $d > 0$ and d is not a perfect square.

6.2 Specific case: $n = 1$

Theorem 40. Let (a, b) be a solution such that $a + b\sqrt{d} > 1 \implies a > 1, b > 0$

Theorem 41. If $(x, y), (a, b)$ are two solutions such that $x, y, a, b \ge 0$, then $a + b\sqrt{d} < x + y\sqrt{d} \implies a < x \cap b < y \iff a < x \cup b < y$

Remark: $x+y\sqrt{d}=a+b\sqrt{d} \iff x=a\cap y=b$.
Remark: $(x+y\sqrt{d})(a+b\sqrt{d})=(xa+dyb)+(xb+ya)\sqrt{d}$. We could verify that if $(x,y)(a,b)$ are two solutions, then $(xa+dyb, xb+ya)$ is another solution. Therefore, for a given solution (a,b), the coefficients of $(a+b\sqrt{d})^k, k\in\mathbb{Z}$ is another solution.
Definition: The minimal solution of $x^2-dy^2=1$ is the solution (x,y) such that $x>0, y>0$ and for all solution (a,b) such that $a>0, b>0$, we have $x+y\sqrt{d}<a+b\sqrt{d}$.

Theorem 42. All solutions of special Pell's equation is in the form $\pm(x+y\sqrt{d})^k, k\in\mathbb{R}$

Theorem 43. Special Pell's equation has a non-trivial solution.

6.3 Diophantine approximation

Suppose $d>0$ is not a perfect square, then $\sqrt{d}$ is irrational. Suppose for special Pell's equation we have solution (x,y), then $x^2-dy^2=1 \implies \frac{x}{y}=\sqrt{d+\frac{1}{y^2}}\approx\sqrt{d}$. We have $\frac{x}{y}$ as a rational approximation of $\sqrt{d}$.

Theorem 44 (Dirichlet)**.** For arbitrary irrational α, there exists infinitely many $\frac{p}{q}\in\mathbb{Q}$ such that $|\alpha-\frac{p}{q}|<\frac{1}{2q^2}$

Remark: The infinite sequence of rational approximations is contained in the sequence of finite convergent of the continued fraction of α
Remark: By Harmitz, the bound $\frac{1}{2q^2}$ could be improved to $\frac{1}{\sqrt{5}q^2}$, and it is the tightest.

6.4 Continued fraction

Definition: We apply the recursive algorithm to generate continued fraction representation for a real number α_0: Take $a_0=\lfloor\alpha_0\rfloor$, then take $\alpha_1=\frac{1}{\alpha_0-a_0}$, which is greater than 1. Recursively take a_i and α_i, then we express the continued fraction of α_0 as $[a_0,a_1,\dots]$, and we have $\alpha_0=a_0+\frac{1}{a_1+\frac{1}{a_2+\dots}}$
Remark: For rational number, the continued fraction representation is finite.
Definition: For any continued fraction $C=[a_0,a_1,\dots]$, its finite truncation $C_i=[a_0,a_1,\dots,a_i]$ is called a convergent of C.

Theorem 45. Consider a continued fraction $C=[a_0,a_1,a_2,\dots]$, we define a sequence of p_i and q_i recursively: $p_{-1}=1, p_0=a_0, p_n=a_np_{n-1}+p_{n-2}; q_{-1}=0, q_0=1, q_n=a_nq_{n-1}+q_{n-2}$. We then have:

1. $C_i=\frac{p_i}{q_i}$
2. $p_nq_{n-1}-q_np_{n-1}=(-1)^{n-1}$
3. $C_n-C_{n-1}=\frac{(-1)^{n-1}}{q_nq_{n-1}} \implies$ convergence
4. $p_nq_{n-2}-p_{n-2}q_n=(-1)^{n-2}a_n$
5. $C_n-C_{n-2}=\frac{(-1)^{n-2}a_n}{q_nq_{n-2}}$
6. $C_1>C_3>C_5>\dots>C_{2n+1}$
7. $C_2<C_4<C_6<\dots<C_{2n}$
8. $|C-C_n|<\frac{1}{q_nq_{n+1}}<\frac{1}{q_n^2} \implies$ converge to C

Remark: For irrational number, the continued fraction representation is infinite and unique. Different irrational numbers have different continued fraction representations. Any recurring infinite continued fraction must be a quadratic irrational (root of a degree 2 polynomial) and converse also holds.
Remark: Take any two consecutive convergent C_i, C_{i+1}, at least one of them satisfies the bound imposed by Dirichlet. Take any three consecutive convergent C_k, C_{k+1}, C_{k+2}, at least one of them satisfies the bound imposed by Harmitz.

Theorem 46 (Dirichlet)**.** If a rational number $\frac{p}{q}$ satisfies the bound of theorem 44, then $\frac{p}{q}=\frac{p_i}{q_i} \implies \frac{p}{q}$ must be a convergent of α.

Theorem 47. If $\alpha\in\mathbb{R}$ could be approximated by infinitely many rational numbers $\frac{p}{q}$ such that $|\alpha-\frac{p}{q}|<\frac{1}{q^2}$, then α is irrational.

Theorem 48. If $d>0$ and d is not a perfect square, then $\sqrt{d}=[a_0,\overline{a_1,a_2,\dots,a_{k-1},2a_0}]$ where k is the period of recurrence.

Theorem 49. All positive solutions of $x^2-dy^2=\pm1$ are of the form (p_n,q_n), where $\frac{p_n}{q_n}$ is a convergent of $\sqrt{d}$.

Theorem 50. If k is even, then $x^2-dy^2=-1$ has no solution and all solutions of $x^2-dy^2=1$ are given by (p_{kr-1},q_{kr-1}) for $r=1,2,\dots$

Theorem 51. If k is odd, then all solutions of $x^2-dy^2=-1$ are given by (p_{kr-1},q_{kr-1}), for $r=1,3,5,\dots$ and all solutions of $x^2-dy^2=1$ are given by (p_{kr-1},q_{kr-1}) for $r=2,4,6,\dots$.

6.5 Transcendental numbers

Definition: A number is algebraic if it is a solution of some polynomial with integral coefficients. It is algebraic with degree d, where d is the minimal possible degree of polynomial that admits the number as a root.
Definition: A number is transcendental if it is not algebraic.

Theorem 52 (Liouville)**.** Suppose α is an algebraic number of degree $d>1$, then there is a positive real number A depending on α such that $|\alpha-\frac{p}{q}|>\frac{A}{q^\alpha}$, for all $\frac{p}{q}\in\mathbb{Q}$.

Remark: Say we want $|\alpha-\frac{p}{q}|<\epsilon$ for some very small ϵ, then we must have $\frac{A}{q^\alpha}<\epsilon \implies (\frac{A}{\epsilon})^{\frac{1}{\alpha}}<q$. This implies that a good rational approximation to any algebraic number must have a very large denominator.

6.6 General case: $n\in\mathbb{Z}$

Theorem 53. Fix a non-trivial positive solution (a,b) of $x^2-dy^2=1$, which is guaranteed to exist, then for each nonzero n, every integral solution of $x^2-dy^2=n$ could be obtained from the coefficients of $(x'+y'\sqrt{d})(a+b\sqrt{d})^k$, where (x',y') is a solution of $x^2-dy^2=n$ such that $|x'|\le\frac{\sqrt{|n|}}{2}(\sqrt{u}+\frac{1}{\sqrt{u}})$ and $|y'|\le\frac{\sqrt{|n|}}{2\sqrt{d}}(\sqrt{u}+\frac{1}{\sqrt{u}})$, where $u=a+b\sqrt{d}$

Remark: If $n>0$, then the second constraint could be replaced by $|y'|\le\frac{\sqrt{|n|}}{2\sqrt{d}}(\sqrt{u}-\frac{1}{\sqrt{u}})$

7 Binary quadratic form

7.1 Representability

Definition: We say $n\in\mathbb{Z}$ is represented by (a,b,c) if $ax^2+bxy+cy^2=n$ has integral solutions. If further $\gcd(x,y)=1$, we say (a,b,c) properly represents n.
Definition: Discriminant Δ of (a,b,c) is defined as $\Delta=b^2-4ac$.
Definition: f is definite if $f(x,y)>0$ (or $f(x,y<0)$) for all $(x,y)\in\mathbb{Z}^2$. Semidefinite if the inequality is not strict. Indefinite if not definite or semidefinite.

Theorem 54. f is definite $\iff \Delta<0$. Positive definite if $a>0$. Negative definite if $a<0$.

Theorem 55. $\Delta\equiv b^2 \pmod 4 \iff \Delta\equiv 0/1 \pmod 4$

Theorem 56. n is represented by $f \iff \frac{n}{d^2}$ is properly represented by $\frac{1}{d^2}f$, where $d=\gcd(x,y)$.

Theorem 57. Suppose $\Delta\in\mathbb{Z}$ and $\Delta\equiv 0/1 \pmod 4$. There is a binary quadratic form with discriminant Δ which properly represents $n \iff \Delta$ is a quadratic residue modulo $4|n|$.

Corollary: An odd prime p is properly represented by a binary quadratic form with discriminant $\Delta \iff \left(\frac{\Delta}{p}\right)=1$

7.2 Equivalence and reduced form

Definition: The representation matrix of a form $f=(a,b,c)$ is $M_f=\begin{bmatrix}a & \frac{b}{2}\\ \frac{b}{2} & c\end{bmatrix}$. Let $X=(x,y)^T$, then $f(x,y)=X^TM_fX$.
Definition: Two forms f and g are equivalent if we could fix $A\in SL_2(\mathbb{Z})$ such that $g(X)=f(AX) \iff X^TM_gX=X^TA^TM_fAX \iff M_g=A^TM_fA$.

Theorem 58. Equivalence of forms is an equivalence relation which defines equivalence classes in S_Δ. In fact, $SL_2(\mathbb{Z})$ acts on S_Δ by form equivalence.

Definition: n is represented by $f \iff n$ is represented by g.
Definition: We say $f(x,y)=(a,b,c)$ is reduced if $-|a|<b\le|a|\le|c|$, and $|a|<|c|$ if $b=|a|$, and $b\ge0$ if $|a|=|c|$.

Theorem 59. We fix $\Delta\equiv 0/1 \pmod 4$, suppose f is a reduced form with discriminant Δ, then if $\Delta<0$, a,c have same sign and $|a|\le\sqrt{-\frac{\Delta}{3}}$. If $\Delta>0$, then a,c have opposite signs and $|a|\le\frac{\sqrt{\Delta}}{2}$. In either case, there are only finitely many such reduced forms.

Theorem 60. Every equivalence class has at least one reduced form. Therefore, there are finitely many equivalence classes in S_Δ.

Remark: It may happen that two distinct reduced forms are equivalent. Indeed, this happens when $\Delta>0$.
Remark: $SL_2(\mathbb{Z})$ is generated by $T=\begin{bmatrix}1&1\\0&1\end{bmatrix}$ and $S=\begin{bmatrix}0&-1\\1&0\end{bmatrix}$, where for $f=(a,b,c)$, the effect to apply S,T are $S:(a,b,c)\to(c,-b,a)$, $T^m:(a,b,c)\to(a,b+2am,am^2+bm+c)$ for $m\in\mathbb{Z}$

Theorem 61 (Reduction algorithm)**.** Given any form (a,b,c), iterate until it is reduced:

1. If $b\notin(-|a|,|a|]$, find the unique integer m such that $b+2am$ is within the range, apply T^m.
2. If now $|a|=|c|$ and $b\ge0$, it is reduced. If now $b<0$ and $|a|=|c|$, apply S and it is reduced.
3. If $|c|<|a|$, apply S, if b is within the range, it is reduced. Else, back to step 1.

Remark: The algorithm is guaranteed to terminate because there is descent in coefficient of x^2.

Theorem 62. Suppose $\Delta<0$ and $f,g\in S_\Delta$ are reduced, then $f\cong g \iff f=g$ (No equivalence between two distinct reduced forms with negative discriminant.)

Theorem 63. If f is a positive definite reduced form in S_Δ, then the smallest positive integral values represented by f are $a\le c\le a+c-|b|$

Corollary: If $\Delta<0$, then the class number of S_Δ is the number of reduced forms.

Theorem 64 (Dirichlet)**.** For prime $p>3, p\equiv3 \pmod 4$, we have $h(-p)=-\frac{1}{p}\sum_{n=1}^{p-1}\left(\frac{n}{p}\right)n$

7.3 Form composition

We wish to define composition $*$ such that if two forms f_1,f_2 could respectively represent c_1,c_2, then f_1*f_2 could represent c_1c_2.
Definition: For $f=(a,b,c)$, $g=(a',b',c')\in S_\Delta$, if $\gcd(a,a',\frac{b+b'}{2})=1$, then composition $f*g$ is defined as $(aa',B,\frac{B^2-\Delta}{4aa'})$, where B is the unique solution (up to modulo, for computation, take arbitrary value) to the system

$$\begin{cases}a'B\equiv a'b & \pmod{2aa'}\\ aB\equiv ab' & \pmod{2aa'}\\ \frac{b+b'}{2}B\equiv\frac{bb'+\Delta}{2} & \pmod{2aa'}\end{cases}$$

Definition: f is primitive if $\gcd(a,b,c)=1$.

Theorem 65. The set of primitive equivalence classes, together with binary form composition, forms a group.

Remark: Primitive equivalence class is well-defined. It is impossible for a primitive form to be equivalent to a non-primitive form.
Remark: Identity in the group is defined by $f_0=$

$$\begin{cases}(1,1,\frac{1-\Delta}{4}) & \Delta\equiv1 \pmod 2\\ (1,0,-\frac{\Delta}{4}) & \Delta\equiv0 \pmod 2\end{cases}$$

Remark: $(a,b,c)^{-1}=(a,-b,c)$