Imaginary quadratic orders with given prime factor of class number

Alexander Rostovtsev, St. Petersburg State Polytechnic University,
rostovtsev@ssl.stu.neva.ru

Abstract

Abelian class group Cl(D) of imaginary quadratic order with odd squarefree discriminant D is used in public key cryptosystems, based on discrete logarithm problem in class group and in cryptosystems, based on isogenies of elliptic curves. Discrete logarithm problem in Cl(D) is hard if #Cl(D) is prime or has large prime divisor. But no algorithms for generating such D are known.

We propose probabilistic algorithm that gives discriminant of imaginary quadratic order with subgroup of given prime order l. Algorithm is based on properties of Hilbert class field polynomial H_D for elliptic curve $E(\mathbb{F}_{p^l})$ over field of p^l elements. Let trace of Frobenius endomorphism is T, discriminant of Frobenius endomorphism $D = T^2 - 4p^l$ and $j(E(\mathbb{F}_{p^l})) \notin \mathbb{F}_p$. Then $\deg(H_D) = \#\mathrm{Cl}(O_D)$ and $\#\mathrm{Cl}(D) \equiv 0 \pmod{l}$. If Diophantine equation $D = T^2 - 4p^l$ with variables $l < O(\sqrt[4]{|D|})$, prime p and T has solution only for $l = 1$, then class number is prime.

1. Class group of imaginary quadratic order

Let $a, b, c \in \mathbb{Z}$ and $Q = (a, b, c) = \{ax^2 + bxy + cy^2\}$ — integral quadratic form of discriminant $D = b^2 - 4ac$. Form Q is positive definite if $D < 0$ and $a > 0$.

If variables x, y run through $\mathbb{Z}$, Q runs through subset of $\mathbb{Z}$. Equivalent forms have equal sets of values (possibly permuted). It is sufficient to consider forms with $(a, b, c) = 1$, D is not perfect square and $a > 1$. If Q is positive definite form, then $Q(x, y) \geq 0$ and $Q = 0$ if and only if $x = 0$ and $y = 0$. All considered forms are positive definite.

Equivalent forms have the same discriminant. Equivalence partitions set of forms with given discriminant into finite set of classes. For given D pair (a, b) completely defines the quadratic form: $c = \dfrac{b^2 - D}{4a}$.

Product of 2×2 integral matrices is integral matrix. Such matrix is invertible if and only if its discriminant is ± 1. Matrix group with integral elements contains subgroup $\mathrm{SL}_2(\mathbb{Z})$ with discriminant 1. Infinite group $\mathrm{SL}_2(\mathbb{Z})$ is generated by matrices $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ for $n \in \mathbb{Z}$.

Forms $(a, b, c) = \{ax^2 + bxy + cy^2\}$ and $(a', b', c') = \{a'u^2 + b'uv + c'v^2\}$ are equivalent if and only if there exists matrix $L \in \mathrm{SL}_2(\mathbb{Z})$ such that $\begin{pmatrix} x \\ y \end{pmatrix} = L \begin{pmatrix} u \\ v \end{pmatrix}$. Multiplying vector by matrix can be considered as transformation of coefficients

of the form. Applying matrices S, T to given positive definite form, one can obtain uniquely defined reduced quadratic form (a, b, c) with properties

1. $0 < a \le c$;
2. $-a < b \le a$;
3. if $a = c$ then $b > 0$.

Let $D < 0$ is discriminant of quadratic form. Define complex number $\xi = \sqrt{D}$ for $-D \equiv 0 \pmod 4$ and $\xi = \frac{1+\sqrt{D}}{2}$ for $-D \equiv 3 \pmod 4$. Imaginary quadratic order O_D of discriminant D is ring $\mathbb{Z}[\xi]$. Joining those two cases, we can write $O_D = \mathbb{Z}\left[\frac{D+\sqrt{D}}{2}\right]$. Fields of fractions for quadratic orders of discriminant D and f^2D for integer conductor f are the same, but $O_D \supset O_{f^2D}$. Hence there exists maximal quadratic order for given field of fractions. Order with squarefree discriminant is maximal.

Ideal of quadratic order is subset $\mathsf{A} \subseteq O_D$ such that if $\alpha, \beta \in \mathsf{A}$, then $\alpha \pm \beta \in \mathsf{A}$, and $\alpha x \in \mathsf{A}$ for arbitrary $x \in O_D$. Ideal $\mathsf{A} \subseteq O_D$ defines quotient ring O_D/A, it is finite if $\mathsf{A} \ne (0)$. Norm $N(\mathsf{A})$ of nonzero ideal A is $\#O_D/\mathsf{A}$. Norm is the smallest positive integer contained in A. Ideal $(\alpha) = \alpha O_D$ for $\alpha \in O_D$ is principal. Generally ideal of quadratic order is generated by two elements: $\mathsf{A} = a\mathbb{Z} + \mathbb{Z}(b + \xi)$, where $a, b \in \mathbb{Z}$ and there exists such $c \in \mathbb{Z}$, that $b^2 - 4ac = D$. So there is one-to-one correspondence between non-zero ideals of O_D and quadratic forms of discriminant D. We use short designation $\mathsf{A} = (a, b)$ instead of $\mathsf{A} = a\mathbb{Z} + \mathbb{Z}(b + \xi)$. $N(a, b) = a$.

Set of ideals admits commutative and associative multiplication:

$(a\mathbb{Z} + \mathbb{Z}(b + \xi))(c\mathbb{Z} + \mathbb{Z}(d + \xi)) = ac\mathbb{Z} + c\mathbb{Z}(b + \xi) + a\mathbb{Z}(d + \xi) + \mathbb{Z}(b + \xi)(d + \xi))$

(ideal in the right side of the equation is generated by at most two elements). So set of ideals of order O_D form commutative monoid with identity $O_D = (1)$.

Norm of ideal is multiplicative function: $N(\mathsf{AB}) = N(\mathsf{A})N(\mathsf{B})$. If ideal cannot be represented as product of two proper ideals, it is prime. Hence ideals with prime norm are the prime ones. Generally ring O_D does not possess unique factorization, for example, $21 = 3 \cdot 7 = (1+\sqrt{-20})(1-\sqrt{-20})$ because prime ideal is not necessary principal. But each ideal can be uniquely represented as product of prime ideals, so O_D is Dedekind domain. So

$$(3) = (3, 1+\sqrt{-21})(3, 1-\sqrt{-21}),\ (7) = (7, 1+\sqrt{-21})(7, 1-\sqrt{-21}),$$

$$(1+\sqrt{-21}) = (3, 1+\sqrt{-21})(7, 1+\sqrt{-21}),\ (1-\sqrt{-21}) = (3, 1-\sqrt{-21})(7, 1-\sqrt{-21}).$$

Define ideal equivalence: $\mathsf{A} \sim \mathsf{B}$, if there exists pair of non-zero quadratic integers $\alpha, \beta \in O_D$ such that $\alpha\mathsf{A} = \beta\mathsf{B}$. Hence all principal non-zero ideals are equivalent. Equivalence partitions set of ideals into classes. Each class can be represented by reduced ideal with the smallest norm. Equivalence of ideals corresponds to equivalence of quadratic forms, and there is bijection between reduced quadratic forms and reduced ideals.

Multiplication of ideals induces multiplication in set of classes, and this set is Abelian group Cl(D). Its identity element is ideal (1, 1) for odd D and (1, 0) for even D. If A is ideal then $\mathsf{A}^{\#\mathrm{Cl}(D)}$ is principal ideal.

Reduced quadratic form (a, b, c) corresponds to ideal (a, b) and has inverse (a, $-b$, c) only if $a \neq 1$ and $a \neq c$, otherwise $(a, b)^{-1} = (a, b)$. Case $a = 1$ corresponds to identity in class group. In the case $a = c$ quadratic form (a, b, a) has order two in class group. Notice that form (a, b, a) is possible if its discriminant $D = b^2 - 4a^2 = (b + 2a)(b - 2a)$ is product of different integers ($b - 2a \neq \pm 1$ since $-a < b \leq a$). So class number #Cl(D) is odd if D is prime or degree of prime. Imaginary quadratic orders have #Cl(D) = 1 for $-D \in$ {3, 4, 7, 8, 11, 12, 16, 19, 27, 28, 43, 67, 163}.

There are no known effective algorithms for computing #Cl(D). There exists estimation $\#\mathrm{Cl}(D) = O(\sqrt{|D|})$ and explicit formula for #Cl(D) as sum of infinite Dirichlet's series. D. Shanks presented algorithm for computing class number with two stages. 1. Find approximation for #Cl(D) and estimate search interval. 2. Search the class number using giant step – baby step algorithm.

Experiments show that partial sum S_n of n first terms of Dirichlet's series is near to #Cl(D) (error $\frac{\#\mathrm{Cl}(D) - S_n}{\#\mathrm{Cl}(D)}$ is near to $\frac{\log n}{n}$). So for $n = O(\sqrt[6]{|D|})$ complexity of each stage is $O(\sqrt[6]{|D|})$ and the whole complexity is $O(\sqrt[6]{|D|})$.

Any ideal is product of prime ideals. Probability that an ideal has prime divisor with small norm is more than probability that prime divisor has large norm. So we can take set of prime ideals with small norms and try to represent an ideal as product of taken prime ideals. This leads to subexponential algorithm for computing class number with complexity $O(\exp(c\sqrt{\ln|D| \ln\ln|D|}))$ [2].

2. Modular functions, elliptic curves and class field polynomial

Let $L = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ be a lattice in complex plane $\mathbb{C}$ with basis [ω_1, ω_2], $\mathrm{Im}(\omega_2/\omega_1) > 0$. Then there exists quotient group $\mathbb{C}/L$. Define equivalent lattices: $L \sim M$, if $L = \alpha M$ for some $\alpha \in \mathbb{C}^*$. Two lattices with bases [ω_1', ω_2'] and [ω_1, ω_2] coincide if and only if $\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Due to

equivalence, lattice can be defined by single parameter τ: $L = \mathbb{Z} + \tau\mathbb{Z}$, $\mathrm{Im}(\tau) > 0$. Matrix transforms parameter τ: $\begin{pmatrix} a & b \\ c & d \end{pmatrix}(\tau) = \frac{a\tau + b}{c\tau + d}$.

Since group $\mathrm{SL}_2(\mathbb{Z})$ is generated by matrices S, T, arbitrary lattice can be transformed to equivalent lattice so that $-1/2 < \mathrm{Re}(\tau) \le 1/2$, $\mathrm{Re}(\tau)^2 + \mathrm{Im}(\tau)^2 \ge 1$, $\mathrm{Im}(\tau) \ge \frac{\sqrt{3}}{2}$.

Modular function f is defined as meromorphic function of complex variable τ, that maps upper half plane to plane $\mathbb{C}$ so that $f(\tau) = f\left(\frac{a\tau + b}{c\tau + d}\right)$ for any matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$.

Modular functions for given lattice form subfield in field $\mathbb{C}((\tau))$ of meromorphic functions. In practice for speeding-up the convergence of Laurent series for modular function, usually Fourier transform $q = e^{2\pi i\tau}$ is used instead of τ. The "simplest" modular function is $j(q) = q^{-1} + 744 + \ldots \in \mathbb{Z}((q))$ — Laurent series with integer coefficients. Any modular function is rational function of $j(q)$. Hence complex number $j(\tau)$ defines lattice up to equivalence.

Elliptic curve $E(K)$:

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

is set of points $(X, Y, Z) \in K\backslash(0, 0, 0)$, satisfying this equations under equivalence $(X, Y, Z) = (uX, uY, uZ)$ for any $u \ne 0$ and there is no point on elliptic curve such that all three partial derivatives are zero. Elliptic curve points form Abelian group under addition with zero element $P_\infty = (0, 1, 0)$. Elliptic curve isomorphism can be defined as multiplication $L\begin{pmatrix} X \\ Y \\ Z \end{pmatrix}$, where matrix L is invertible over K. Elliptic curve over algebraically closed field up to isomorphism can be determined by its invariant $j \in K(a_1, a_2, a_3, a_4, a_6)$.

If $K = \mathbb{C}$, then elliptic curve as Abelian group is isomorphic to quotient group $\mathbb{C}/L$ for some lattice L, so there is bijection between lattices and elliptic curves. Elliptic curve isomorphism corresponds to lattice equivalence and elliptic curve invariant j is the image of lattice invariant $j(\tau)$ in field K (this is possible only if τ is element of imaginary quadratic field [3]).

If field characteristic is 2, then linear change of variables gives $a_1 \ne 0$ or $a_3 \ne 0$ (but not both of them). If $a_1 = 0$, then $j = 0$.

In cryptographic applications elliptic curve $E(\mathbb{F}_{p^l})$ is considered over finite field $\mathbb{F}_{p^l}$ of p^l elements, $l \ge 1$. Frobenius map $\pi_l(X, Y, Z) = \left(X^{p^l}, Y^{p^l}, Z^{p^l}\right)$

keeps the elliptic curve equations, keeps all points over field $\mathbb{F}_{p^l}$ and changes other points (over algebraic closure of field $\mathbb{F}_{p^l}$). Frobenius map satisfies equation $\pi_l^2 - T\pi_l + p^l = 0$, where T is trace and $D = T^2 - 4p^l < 0$ is discriminant of this map. Twisted curves have traces with the same absolute value and different signs.

Number of elliptic curve points $E(\mathbb{F}_{p^l})$ is finite and equals

$$\#E(\mathbb{F}_{p^l}) = p^l + 1 - T.$$

Discriminant D up to sign determines T and hence determines $\#E(\mathbb{F}_{p^l})$.

Let $O_D = \mathbb{Z}\left[\frac{D+\sqrt{D}}{2}\right]$ is imaginary quadratic order for given discriminant D of Frobenius map, #Cl(D) is its class number and $\{(a_i, b_i, c_i)\}$, $1 \le i \le h_D$ is set of reduced quadratic forms (or set of reduced ideals in class group). Let $\tau_i = \frac{b_i + \sqrt{D}}{2a_i}$. Function $j(\tau)$ can be computed with small error for all i as partial sum of Laurent series. Irreducible over $\mathbb{Q}$ (and $\mathbb{Q}[\sqrt{D}]$) Hilbert class field polynomial is defined as

$$H_D(X) = \prod_{i=1}^{\#Cl(D)} (X - j(\tau_i)) \in \mathbb{Z}[X].$$

Its roots are algebraic integers. Joining the root j of H_D to $\mathbb{Q}$ or to $\mathbb{Q}[\sqrt{D}]$ gives field extensions of the same degree, and $\mathbb{Q}[\sqrt{D}, j]$ is class field — maximal unramified Abelian extension. Elliptic curve over prime finite field $\mathbb{F}_p$ with trace T up to isomorphism and up to twisted curve is determined by its invariant j as a root of $H_D(X)$ (mod p). So to find j-invariant one needs computing D, Cl(D), $H_D(X)$, factoring $H_D(X)$ (mod p) and taking a root as required j-invariant. This is common method for elliptic curve generation with given p and T.

Theorem 1. Let l is prime, $p \ne l$ is prime or degree of prime, and class field polynomial has no roots in $\mathbb{F}_p$. Elliptic curve $\mathbb{F}_{p^l}$ with $j \in \mathbb{F}_{p^l} \setminus \mathbb{F}_p$ and Frobenius discriminant $D = T^2 - 4p^l$ exists if class number #Cl(D) has factor l.

Proof. Let $q = p^l$, p is prime or degree of prime. If class field polynomial $H_D(X)$ has a root j in $\mathbb{F}_{p^l}$, then $H_D(X)$ factors completely over $\mathbb{F}_{p^l}$ and there exists elliptic curve $E(\mathbb{F}_{p^l})$ with invariant j and Frobenius discriminant $D = T^2 - 4p^l$. Back, if there is elliptic curve $E(\mathbb{F}_{p^l})$ with Frobenius discriminant D, then its invariant is a root of polynomial $H_D(X)$. Hence class field polynomial splits

completely over $\mathbb{F}_{p^l}$. Since $p \neq l$, class field polynomial gives separable extension of field of characteristic p.

Notice that if l is prime and class field polynomial splits over $\mathbb{F}_{p^l}$, it may split already over prime field $\mathbb{F}_p$. Then $j \in \mathbb{F}_p$ and class number possibly has no factor l. **n**

Theorem 1 can be explained in terms of quadratic orders. If $D = T^2 - 4p^l$ then we have factorization $p^l = \left(\frac{T+\sqrt{D}}{2}\right)\left(\frac{T-\sqrt{D}}{2}\right)$. Reduction modulo p gives existence of $\sqrt{D} \pmod p$, so $\left(\frac{D}{p}\right)=1$. Ideal (p^l) splits as product of two principal ideals. Hence ideal (p) also splits in O_D as product of two prime ideals. Its factors can be principal or not. Any ideal powered by class number becomes principal. If factors of ideal (p) are not principal and l is prime, then l divides class number.

3. Class group with subgroup of given prime order

Class group of imaginary quadratic order is used in public key cryptosystems of two types. The first one is based on discrete logarithm problem directly in class group [1]. The second one is based on computing isogenies between elliptic curves [5] (number of possible j-invariants divides class number for Frobenius discriminant).

If class number has largest prime divisor r, then complexity of computing discrete logarithms in class group does not exceed $O(\sqrt{r})$ due to Pollard's algorithm [4]. So in cryptographic applications it is likely that class number is large prime or it has large prime divisor.

To construct digital signature algorithm, similar to DSS, it is necessary to compute prime class number or its large prime divisor. But there are no known effective methods for prime D to recognize primality of class number. It is known that if $D = f^2D'$, discriminant D' has class number 1, conductor f is odd prime, then $\#\mathrm{Cl}(D) = f - \left(\frac{D}{f}\right)$, where $\left(\frac{D}{f}\right)$ is Jacobi symbol. So one can obtain required prime divisor l of group order as $l = \frac{f \pm 1}{2}$. But it is hard to find squarefree discriminant with given prime factor of class number.

Assume that class field polynomial has a root $j \in \mathbb{F}_p$, i.e. $j(E(\mathbb{F}_{p^l})) \in \mathbb{F}_p$ for prime l. Then Frobenius automorphism $\pi_1(x, y) = (x^p, y^p)$ satisfies equation ${\pi_1}^2 - T_1\pi_1 + p = 0$ with discriminant $D_1 = {T_1}^2 - 4p$. Let $\alpha, \overline{\alpha}$ be roots of the equation. Then $\#E(\mathbb{F}_p) = p + 1 - \alpha - \overline{\alpha}$ and $\#E(\mathbb{F}_{p^l}) = p^l + 1 - \alpha^l - \overline{\alpha}^l$. Frobenius map

$\pi_l(x,y)=(x^{p^l},y^{p^l})$ has discriminant $D=(\alpha^l+\overline{\alpha}^l)^2-4p^l$. According to theorem 1 imaginary quadratic order O_D may have class number with no factor l. If p is small, set of possible traces T_1 is small too. So it is not hard to test whether D has representation $D=(\alpha^l+\overline{\alpha}^l)^2-4p^l$.

Example 1. Consider elliptic curve $E(\mathbb{F}_{2^l})$

$$y^2 + xy = x^3 + a_2x^2 + a_6 \ (a_2 \in \mathbb{F}_2,\ a_6 \neq 0),$$

with invariant $j = a_6^{-1}$, map $a_2 \to a_2 + 1$ gives the twisted curve.

If $P = (x, y) \in E(\mathbb{F}_{2^l})$, then $-P = (x, x + y)$. Hence $2P = P_\infty$ if and only if $x = 0$. Point $(0, y)$ of order 2 always exists and corresponds equation $y^2 = a_6$, $y=a_6^{2^{l-1}}$. Point of order 4 exists, if equation $2P = (0, y)$ is solvable for $E(\mathbb{F}_{2^l})$. For $P = (u, v)$ we have equation $\lambda^2 + \lambda + a_2 = 0$, $\lambda=\frac{u^2+v}{u}$. This equation is solvable if and only if $a_2 = 0$. Notice that elliptic curve $E_1(\mathbb{F}_2)$: $y^2 + xy = x^3 + a_2x^2 +1$ has 2 points if $a_2 = 1$ and has 4 points if $a_2 = 0$, its Frobenius trace is ±1. Hence the curve $E(\mathbb{F}_{2^l})$ has subgroup isomorphic to curve $E_1(\mathbb{F}_2)$ with the same a_2. Frobenius discriminant $D = T^2 - 4\cdot2^l$ for curve $E(\mathbb{F}_{2^l})$ is odd if trace T is odd.

Let $q = 2^{11}$, $T = 55$, $\#E(\mathbb{F}_{2^{11}}) = q + 1 - T = 1994 = 2\cdot997$, $D = T^2 - 4q = -5167$ is prime, $\#\mathrm{Cl}(D) = 33$. Computing Hilbert class field polynomial and reduction its coefficients modulo 2 gives:

$$H_D = 1 + X^2 + X^3 + X^5 + X^6 + X^7 + X^8 + X^9 + X^{12} + X^{13} + X^{16} + X^{21} + X^{23} + X^{26} + X^{27} + X^{29} + X^{31} + X^{33}.$$

Its factorization over $\mathbb{F}_2$ is

$$H_D = (1 + X^2 + X^4 + X^6 + X^7 + X^9 + X^{11})(1 + X^2 + X^3 + X^4 + X^5 + X^7 + X^8 + X^{10} + X^{11})(1 + X^2 + X^4 + X^6 + X^9 + X^{10} + X^{11}).$$

All irreducible divisors of class field polynomial over prime field have degree 11 and factor completely over field $\mathbb{F}_{2^{11}}$. For discriminant $D = T^2 - 4\cdot2^{11}$ class number has factor 11. Similarly for any odd $T = 1, 3, \ldots, 89$ ($T = 89$ is maximum that gives $D < 0$) class number has factor 11. **n**

Conversion of theorem 1 gives probabilistic algorithm that generates imaginary quadratic order with given prime factor l of class number.

Algorithm 1. (Computes discriminant of imaginary quadratic order that probably has class number with given prime factor l).

1. Choose small prime $p \neq l$ (for example, $p = 2$), compute $D = T^2 - 4p^l < 0$ for integer T relatively prime to p. If $p = 2$, then T must be odd.

2. Find all elliptic curves over $\mathbb{F}_p$ and corresponding traces T_1 of Frobenius automorphisms $\pi_1(x, y) = (x^p, y^p)$. Find roots $\alpha, \overline{\alpha}$ of corresponding equations for π_1.
3. For all different absolute traces T_1 test that $D \neq p^l + 1 - \alpha^l - \overline{\alpha}^l$.
4. Return: D. **n**

Algorithm 1 gives true result if there exists elliptic curve $E(\mathbb{F}_{p^l})$ with given trace T (this existence is not tested). And result can be wrong if there is no such elliptic curve. But if l is sufficiently large, probability of mistake is negligibly small.

Notice that $|D|$ growths as exponential of l. So obtained discriminant for large l can be extremely large.

Example 2. Discriminant $D = -45402459391 = 97184015999^2 - 4 \cdot 2^{71}$ gives class number $5^2 \cdot 53 \cdot 71$, $D = -39281659711 = 24296033999 - 4 \cdot 2^{67}$ gives class number $2^5 \cdot 3 \cdot 19 \cdot 67$. **n**

From theorem 1 we deduce

Corollary 2. Let $D < 0$ is prime. Assume that exponential Diophantine equation $D = T^2 - 4p^l$ with three variables l, p, T and prime p, for $l < O(\sqrt[4]{|D|})$ has solution only for $l = 1$. Then class number $\#\mathrm{Cl}(D)$ is prime.

Proof. $\#\mathrm{Cl}(D) = O(\sqrt{|D|})$. If $\#\mathrm{Cl}(D)$ is composite, it has factor $l < \sqrt{\#\mathrm{Cl}(D)}$ and there exists elliptic curve $E(\mathbb{F}_{p^l})$ with required Frobenius discriminant $D = T^2 - 4p^l$. But Diophantine equation has no such solutions, so class number must be prime. **n**

This algorithm can be used to deduce whether imaginary quadratic order has non-prime class number: if representation $D = T^2 - 4p^l$ for large $|D|$ exists, then class number is probably composite and has factor l. This observation can simplify computation of class number with Shanks algorithm.

Algorithm 1 can be generalized. Quadratic order O_D has ideal with norm p^l if there exists quadratic form (p^l, b, c) with discriminant D. So we have $b^2 - 4p^l c = D$. This ideal is principle if there exists representation $4p^l = A^2 - DB^2$ for integers A, B. Hence instead of equation $D = T^2 - 4p^l$ we can consider equation $D = T^2 - 4p^l S$ for integer S. Here again D is a square modulo p.

References

1. J. Buchmann and H. Williams. A key-exchange system based on imaginary quadratic fields // Journal of Cryptology, v. 1, 1988, pp. 107–118.

2. H. Cohen. A Course in Computational Algebraic Number Theory, Springer–Verlag, 1993.
3. S. Lang. Elliptic functions, Springer–Verlag, 1987.
4. J. Pollard. Monte Carlo methods for index computation (mod p) // Mathematics of Computation, v. 32, 1978, pp. 918–924.
5. A. Rostovtsev and A. Stolbunov. Public key cryptosystem based on isogenies // Cryptology e-print archive, report 2006/145, 2006.