Генерация эллиптических кривых. Лабораторные работы

2 марта 2024 г.

Лабораторная работа 1: Вычисление числа классов $h(D)$ для квадратичной формы с фундаментальным дискриминантом $D < 0$

Input: $D < 0$

1. $h := 1$;
2. $b := D \pmod 2$;
3. $B := \lfloor \sqrt{|D|/3} \rfloor$;
4. **repeat**
5. $\quad q := (b^2 - D)/4$;
6. $\quad a := b$;
7. $\quad$ **if** $a \leq 1$ **then**
8. $\quad\quad a := 2$;
9. $\quad$ **endif**
10. $\quad$ **repeat**
11. $\quad\quad$ **if** $a|q$ **then**

Лабораторная работа 1

12 **if** $a == b$ **or** $a^2 == b$ **or** $b == 0$ **then**
13 $h := h + 1;$
14 **else**
15 $h := h + 2;$
16 **endif**
17 **endif**
18 $a := a + 1;$
19 $a^2 > q;$
20 $b := b + 2;$
21 **until** $b > B$**;**
22 **return** h.

Лабораторная работа 2: Вычисление количества всех редуцированных форм с фундаментальным дискримимнантом $-D$ **Input:** $D > 0$

1. $r := \lfloor \sqrt{D/3} \rfloor$;
2. $b := D(\bmod 2)$;
3. **while** $b \leq r$ **do**
4. $\quad m := \frac{b^2+D}{4}$;
5. $\quad$ **for** $a|m$ **and** $a \leq \lfloor \sqrt{m} \rfloor$ **do**
6. $\quad\quad c := \frac{m}{a}$;
7. $\quad\quad$ **if** $b \leq a$ **then**
8. $\quad\quad\quad$ **if** $b == a$ **or** $c == a$ **then**
9. $\quad\quad\quad\quad$ store $[a, b, c]$;
10. $\quad\quad\quad$ **else**
11. $\quad\quad\quad\quad$ store $[a, \pm b, c]$;
12. $\quad\quad\quad$ **endif**
13. $\quad\quad$ **endif**
14. $\quad$ **endfor**
15. $\quad b := b + 2$
16. **endwhile**