

An Encoding for the Theta Model of Elliptic Curves

Nafissatou Diarra^{$1(\boxtimes)$} and Emmanuel Fouotsa²

 ¹ Cheikh Anta Diop University, Dakar, Senegal fifiramatou@gmail.com
 ² The University of Bamenda, Bamenda, Cameroon emmanuelfouotsa@yahoo.fr

Abstract. The use of elliptic curves in cryptography requires to be able to transform an information (generally a bit string) to a point of an elliptic curve. This transformation, called encoding, must be such that the encoded message can be easily and uniquely recovered from the corresponding point. In this paper we propose a new encoding that maps an element of \mathbb{F}_q to a point on the theta model for elliptic curves $E_{\lambda}: 1 + x^2 + y^2 + x^2y^2 = \lambda^2 xy$ recently introduced in [9]. In particular, we show that this new encoding is efficiently computable (deterministic and polynomial-time). We also present a Sage software implementation to ensure the correctness of the encoding on this curve.

Keywords: Theta model \cdot Elliptic curves \cdot Deterministic encoding

1 Introduction

Many elliptic curve-based cryptographic schemes require to hash into the group of points of an elliptic curve, such as password-based authentication protocols (SPEKE (Simple Password Exponential Key Exchange), PAK (Password Authenticated Key exchange)), as well as various signature schemes based on the hardness of the DLP (Discrete Logarithm Problem). The main idea for constructing a hash function into elliptic curves is the following: the image of a message (an arbitrary string) m by the hash function F is F(m) = f(h(m)), where h is a classical hash function and f is an encoding function that maps a point of \mathbb{F}_q to an element of the curve. But a problem arises: given any elliptic curve E over any finite field \mathbb{F}_q , how to construct, in a *deterministic* way, a nonzero point of the curve? Some authors have proposed algorithms to answer this question. But before 2006, only probabilistic solutions were known. The paper [3] of Boney and Franklin in 2001 was one of the first that required hashing into (supersingular) elliptic curves; in fact, the public key of their identity-based

This work is supported by the Pole of research in Mathematics with Applications to Information Security (PRMAIS, SubSaharan Africa) sponsored by Simons Foundation and LIRIMA-MACISA Project.

 [©] ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2018
 C. M. F. Kebe et al. (Eds.): InterSol 2018, LNICST 249, pp. 224-235, 2018. https://doi.org/10.1007/978-3-319-98878-8_21

encryption is a point on the curve. In 2006, Shallue and Van de Woestjine proposed the first algorithm [15] that maps in a deterministic way an element of \mathbb{F}_q (with odd characteristic) to a point of any elliptic curve over \mathbb{F}_q . Their algorithm is based on the Skalba's equality theorem and requires to compute a square root in \mathbb{F}_q ; but it can construct only (q-4)/8 points of the curve.

In 2009, Icart defined a new encoding function [13] for Weierstrass form of elliptic curves, based on a very simple idea: intersect the line y = ux + v with the equation of the curve. He showed that his algorithm works in $O \log^3(q)$ operations in \mathbb{F}_q and conjectured (it was proven later by Tibouchi and Fouque [12]) that the size of the image set is approximately $\frac{5}{8}$ of the size of the curve.

Some authors have also proposed constructions of encoding functions for special families of elliptic curves, such as Hessian curves (by Farashahi in [10]), Edwards curves (elligator functions by Bernstein et al. in [1]), or Huff curves (by Diarra *et al.* in [8]).

Our goal on this paper is to continue this line of research, by proposing an encoding function for the theta model for elliptic curves E_{λ} : $1+x^2+y^2+x^2y^2 = \lambda^2 xy$, recently introduced by Fouotsa and Diao [6]. In particular, we will show that this new encoding is efficiently computable (deterministic and polynomial-time).

The rest of the paper is structured as follows: In Sect. 2, we recall a special mathematical concept needed in the work. We briefly define elliptic curves and present the theta model for elliptic curves. together with an overview of main existing encodings into elliptic curves. The Sect. 3 describes our new encoding on the theta model and describes its properties. A numerical example is given with a code written with the Sage software to ensure the correctness of the encoding. We conclude our work in Sect. 4.

2 Preliminaries

2.1 Quadratic Character

Let $p \neq 2$ be a prime and $\mathbb{F}_{p^n} = \mathbb{F}_q$ the finite field of $q = p^n$ elements (where $n \geq 1$ is an integer). An element $a \in \mathbb{F}_q$ is a quadratic residue if there exists $r \in \mathbb{F}_q$ s.t. $a \equiv r^2 \mod q$. We define the quadratic character as follows: $\chi : \mathbb{F}_q \to \mathbb{F}_q : a \mapsto \chi(a) = a^{(q-1)/2}$; it verifies: $\chi(a) = 1$ if a is a non-zero quadratic residue, $\chi(a) = 0$ if a = 0 and $\chi(a) = -1$ otherwise. The following properties are also verified: $\chi(ab) = \chi(a) \cdot \chi(b)$ for any $a, b \in \mathbb{F}_q$; $\chi(a^2) = 1$ for any $a \in \mathbb{F}_q^*$; and if $q \equiv 3 \mod 4$, $\chi(-1) = -1$, $\chi(\chi(a)) = \chi(a)$, for any $a \in \mathbb{F}_q$. If $q \equiv 1 \mod 4$, then $\chi(-1) = 1$.

2.2 The Theta Model for Elliptic Curves

Elliptic Curves. An elliptic curve E over a field \mathbb{K} is the set of solution in $\mathbb{A}^2(\overline{\mathbb{K}})$ of the equation

$$E: y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6, \text{ with } (a_1, a_2, a_3, a_4, a_6) \in \mathbb{K}^5 \quad (1)$$

together with a rational point \mathcal{O} and the condition $\Delta \neq 0$ where $\Delta = -d_2^2 d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6$ with $d_2 = a_1^2 + 4a_2, d_4 = 2a_4 + a_1, d_6 = a_3^2 + 4a_6, d_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$.

The quantity Δ is called the discriminant of E and the condition $\Delta_E \neq 0$ ensures that the curve E is smooth. In the set of point of an elliptic curve, it is very easy to set an additive group structure using the chord-and-tangent method (see [16] for complete details). When an elliptic curve is defined over a finite field, the resulting group presents a difficult mathematical problem known as the Discrete Logarithm Problem stated as follows: Given a point Q multiple of another given point P, find the integer n such that Q = nP. This problem justifies the use of elliptic curves in cryptography for the construction of several secure cryptosystems. The model of elliptic curve given by Eq. (1) is called the Weierstrass model and is the commonly used in the literature. Several other models exists in the literature such as the Edwards model [7], Hessian curves [14], Huff curves [5] and the Jacobi curves [2,4] including the theta model recently introduced by Fouotsa and Diao [6]. Although these curves are birationally equivalent to each other, in an algorithmic point of view and for security and efficiency purposes, careful choices need to be made on which model of elliptic to use in cryptography.

The Theta Model. This model of elliptic curves was proposed by Fouotsa and Diao [9]. The model is obtained from theta functions and the equation is given as follows E_{λ} : $1 + x^2 + y^2 + x^2y^2 = \lambda^2 xy$. They showed that their model is birationally equivalent to the Weierstrass model $v^2 = u^3 - (1 + c^4)u^2 - 4c^4u + 4c^4(1 + c^4)$. This model enjoys many other properties such as unified formulas (addition and doubling of points use the same formulas) and presents competitive addition formulas over binary fields. More details can be found in [6,9].

2.3 Existing Encodings for Elliptic Curves

In this section, we give a short overview of existing methods to encode into elliptic curves.

Trivial Encoding: For an elliptic curve $E_{a,b}$: $y^2 = x^3 + ax + b$ over the field \mathbb{F}_q , the simplest way to construct a point of $E_{a,b}$ from an element of \mathbb{F}_q is to use the trivial encoding, also known as the *try-and-increment* method. The idea is to pick a *x*-coordinate and try to deduce the *y*-coordinate by computing a square root: choose a random element $u \in \mathbb{F}_q^*$ and compute $u^3 + au + b$; and then test whether $u^3 + au + b$ is a square in \mathbb{F}_q . If it is the case, then returns

 $(x, y) = (u, \pm \sqrt{u^3 + au + b})$ as a point of the curve. Otherwise, one can choose another u in \mathbb{F}_q and try again. But this method has at least one drawback as it cannot *run in constant time*: the number of operations depends on the input u. In practice the input u is the message m we want to hash; thus running this algorithm can allow the attacker to guess some information about m.

Icart's Encoding: Let $q \equiv 2 \mod 3$. The map $x \mapsto x^3$ is a bijection and then computation of a cubic root can be done as an exponentiation. In [13], Icart defined a new encoding function, based on the following idea: intersect the line y = ux + v with the Weierstrass curve $E_{a,b}$: $y^2 = x^3 + ax + b$, with $a, b \in \mathbb{F}_q$. He defined the encoding function:

$$f_{a,b}: \mathbb{F}_q \to E_{a,b}$$
$$u \mapsto f_{a,b}(u) = (x, ux + v)$$

where $x = (v^2 - b - \frac{u^6}{27})^{1/3} + \frac{u^2}{3}$ and $v = (3a - u^4)/6u$.

As shown in the paper, this function presents many interesting properties. In fact, it can be implemented in polynomial time with $O(\log^3 q)$ operations. The inverse function $f_{a,b}^{-1}$ is also computable in polynomial time. Icart also showed that $|f_{a,b}^{-1}(P)| \leq 4$, given a point P on the elliptic curve.

Other Existing Encodings: There exist many other encodings for special families of elliptic curves, such as supersingular curves (by Boneh and Franklin in [3]), Hessian curves (by Farashahi in [10]), Edwards curves (Elligator functions by Bernstein *et al.* in [1]), Huff curves (by Diarra *et al.* in [8]), etc.

3 A New Encoding for the Theta Model

3.1 The Algorithm

In this section, we propose a deterministic algorithm that given an element r (with additional conditions) of \mathbb{F}_q , constructs a point on $E_{\lambda}(\mathbb{F}_q)$. From this algorithm, we define the new encoding function which does not cover all points of \mathbb{F}_q , unless we make some additional hypothesis on the underlying field \mathbb{F}_q . Nevertheless, we can send all elements of \mathbb{F}_q that are not in the set of definition (there are at most 6 such points) of the encoding to the point at infinity.

Algorithm 1. Encode-Theta-Model

$$\begin{array}{ll} \text{Input} &: q \text{ be a prime power, } c \in \mathbb{F}_q \text{ s.t. } c(1-c^4)(1+c^4) \neq 0, \, u \in \mathbb{F}_q \text{ s.t. } \chi(u) = -1, \\ & r \in \mathcal{R} = \{r \in \mathbb{F}_q : \, 4ur^2c^6 \neq (1-c^4)(1+3c^4), \, 4ur^2c^6 \neq \\ & -(1-c^4)^4, (4ur^2c^6)(1+3c^4) \neq (1-c^4)^3 \} \subseteq \mathbb{F}_q \end{array} \\ \begin{array}{ll} \text{Output: A point } (x_\lambda, y_\lambda) \\ & v = c \cdot \left(\frac{4ur^2c^6 + (1-c^4)(3+c^4)}{4ur^2c^6 + (1-c^4)(-3c^4-1)}\right); \\ & \varepsilon = \chi \left((c^2 - v^2)(1-c^2v^2)\right); \\ & X = \frac{1}{2} \left((1+\varepsilon)v + (1-\varepsilon) \left(\frac{(-c^4-1)(v+c) - c(1-c^4)}{2c^3(v+c) + 1-c^4}\right)\right); \\ & Y = -\varepsilon \sqrt{\frac{c^2 - X^2}{1-c^2X^2}}; \\ & x_\lambda = \frac{X+1}{X-1}; \\ & y_\lambda = \frac{Y-1}{Y+1}; \\ \mathbf{return } (x_\lambda, y_\lambda); \end{array}$$

Theorem 1. The output $(x_{\lambda}, y_{\lambda})$ of Algorithm 1 is a point of the curve E_{λ} : $1 + x^2 + y^2 + x^2 y^2 = \lambda^2 xy$, where $\lambda^2 = \frac{4(1+c^2)}{1-c^2}$ and $\lambda(\lambda^2 - 4)(\lambda^2 + 1) \neq 0$.

Proof. 1. v is well-defined from the definition of \mathcal{R} .

- 2. Let us show that $\varepsilon \neq 0$. Suppose that $\varepsilon = 0 \Leftrightarrow \mathbf{c^2} = \mathbf{v^2}$ or $\mathbf{c^2v^2} = \mathbf{1}$.
 - (a) $\mathbf{c^2} = \mathbf{v^2} \Rightarrow c = \pm v \Rightarrow 4(1 c^4)(1 + c^4) = 0$ (impossible by the choice of c) or $4ur^2c^6 = (1 c^4)^2$ (impossible since u is not a square).
 - (b) $\mathbf{c^2 v^2} = \mathbf{1} \Rightarrow cv = \pm \mathbf{1} \Rightarrow 4ur^2 c^6 = (c^2 + 1)^4$ or $4ur^2 c^6 = (c-1)^4 (c+1)^4$; this is impossible since u is not a square.

So $\varepsilon \neq 0$ and then $\varepsilon = \pm 1$.

3. Let us show that X, Y are well-defined. For this, we consider the two cases $\varepsilon = 1, \varepsilon = -1$ and show that the quantity $\frac{c^2 - X^2}{1 - c^2 X^2}$ is a square. $\varepsilon = 1 \Rightarrow X = v$ and $\chi \left(\frac{c^2 - X^2}{1 - c^2 X^2}\right) = \chi \left(\frac{c^2 - v^2}{1 - c^2 v^2}\right) = \varepsilon = 1$; so X and Y are well-defined. $\varepsilon = -1 \Rightarrow X = -\frac{(-c^4 - 1)(v + c) - c(1 - c^4)}{2c^3(v + c) + 1 - c^4}$. Now let $H(X) = \frac{c^2 - X^2}{1 - c^2 X^2} = \frac{(c - X)(c + X)}{1 - c^2 X^2}$; we want to express H(X) in term of H(v) and use the value $\chi(H(v)) = \chi \left(\frac{c^2 - v^2}{1 - c^2 v^2}\right) = \varepsilon = -1$. Now to have an expression of H(X) in terms of H(v), we compute separately the value of c - X, c + X and $1 - c^2 X^2$ and find that:

$$\begin{bmatrix} 2c^3(v+c) + (1-c^4) \end{bmatrix} (c-X) = (v+c)(c^4-1), \\ \begin{bmatrix} 2c^3(v+c) + (1-c^4) \end{bmatrix} (c+X) = (v+c)(3c^4+1) + 2c(1-c^4), \\ \text{and } \begin{bmatrix} 2c^3(v+c) + (1-c^4) \end{bmatrix}^2 (1-c^2X^2) = (1-c^2v^2)(c^4-1)^2. \\ \text{This leads to} \end{bmatrix}$$

$$H(X) = \frac{(v+c)(c^4-1)\left[(v+c)(3c^4+1)+2c(1-c^4)\right]}{(1-c^2v^2)(c^4-1)^2}$$
$$= \frac{H(v)}{c-v}\left(\frac{(v+c)(3c^4+1)+2c(1-c^4)}{c^4-1}\right)$$

Since $(v+c)(3c^4+1)+2c(1-c^4) = 2c\left(\frac{8ur^2c^6(1+c^4)}{4ur^2c^6+(1-c^4)(-3c^4-1)}\right)$ and $(c-v)(c^4-1) = 4c\left(\frac{(1-c^4)^2(1+c^4)}{4ur^2c^6+(1-c^4)(-3c^4-1)}\right)$, then we can rewrite H(X) as follows:

$$H(X) = H(v) \left(\frac{4ur^2c^6}{(1-c^4)^2}\right)$$

and thus $\chi(H(X)) = \chi(H(v)) \cdot \chi \left[(4ur^2c^6)(1-c^4)^2 \right] = -\chi(u) = 1$. In other words, $\frac{c^2 - X^2}{1 - c^2 X^2}$ is a square and Y is well-defined.

4. Since X and Y are well-defined (for both cases $\varepsilon = 1$ and $\varepsilon = -1$), we can compute $Y^2 = \frac{c^2 - X^2}{1 - c^2 X^2} \Rightarrow X^2 + Y^2 = c^2(1 + X^2 Y^2)$. Now we have to show that x_{λ} and y_{λ} verify the relation $1 + x_{\lambda}^2 + y_{\lambda}^2 + x_{\lambda}^2 y_{\lambda}^2 - \lambda^2 x_{\lambda} y_{\lambda} = 0$, where $\lambda^2 = \frac{4(1 + c^2)}{1 - c^2}$. In fact, we have: $1 + x_{\lambda}^2 + y_{\lambda}^2 + x_{\lambda}^2 y_{\lambda}^2 - \lambda^2 x_{\lambda} y_{\lambda} = 1 + (\frac{X+1}{X-1})^2 + (\frac{Y-1}{Y+1})^2 + (\frac{X+1}{X-1})^2 (\frac{Y-1}{Y+1})^2 - \lambda^2 (\frac{X+1}{X-1}) (\frac{Y-1}{Y+1})$ $= \frac{1}{(X-1)^2(Y+1)^2} \left[2(X^2 + 1)((Y+1)^2 + (Y-1)^2) - \lambda^2(X^2 - 1)(Y^2 - 1) \right]$ $= \frac{1}{(X-1)^2(Y+1)^2} \left[4(1 + X^2Y^2 + c^2(1 + X^2Y^2)) - \frac{4(1+c^2)}{1 - c^2} (1 + X^2Y^2 - c^2(1 + X^2Y^2)) \right]$ $= \frac{4}{(1 - c^2)(X-1)^2(Y+1)^2} \left[(1 - c^2)(1 + X^2Y^2 + c^2(1 + X^2Y^2)) - (1 + c^2)(1 + X^2Y^2 - c^2(1 + x^2Y^2)) \right]$ = 0. Moreover λ verifies $\lambda(\lambda^2 - 4)(\lambda^2 + 1) \neq 0$ from the conditions on c.

Definition 1. The encoding function for the theta model for elliptic curves is the function

$$f_{\lambda} : \mathcal{R} \subseteq \mathbb{F}_q \to E_{\lambda}(\mathbb{F}_q)$$
$$r \mapsto (x_{\lambda}, y_{\lambda}),$$

where x_{λ} and y_{λ} are defined by Algorithm 1. If $r \in \mathbb{F}_q \setminus \mathcal{R}$, we set $f_{\lambda}(r) = \mathcal{O}_o$.

3.2 Size of the Set \mathcal{R}

- Our encoding covers a subset \mathcal{R} of \mathbb{F}_q ; this means that only elements of \mathcal{R} can be encoded. And from the definition of \mathcal{R} , it is easy to see that at most 6 elements of \mathbb{F}_q can not be encoded, that is $card(\mathbb{F}_q \setminus \mathcal{R}) \leq 6$. Since in practice q (the size of the field) is much greater than 6, thus we can state that our encoding f_{λ} covers a great proportion of \mathbb{F}_q . For example, for q = 503 (see the Appendix for the complete example), we find that $card(\mathcal{R}) = 501$ and thus f covers more than 99% of \mathbb{F}_q .
- To cover \mathbb{F}_q (that is $\mathcal{R} = \mathbb{F}_q$), one can choose an element $c \in \mathbb{F}_q$ such that $\chi\left((1-c^4)(1+3c^4)\right) = 1$ and -1 is a square (for example when $q \equiv 2 \mod 3$), and then $\mathcal{R} = \mathbb{F}_q$.
- Remark 1. The choice of c (and u) does not have any impact on the runningtime of the algorithm, since one must choose a suitable c (and u) before starting the algorithm. When $q \equiv 3 \mod 4$, one can choose u = -1; if $q \equiv 5 \mod 8$, one can choose u = 2.
- Compared to many existing encodings, we do not put any requirements on q (the authors of [13] proposed for example to choose $q \equiv 2 \mod 3$, in order to compute efficiently cubic roots).

3.3 Properties of Our Encoding

Lemma 1 (Polynomial time).

The function f_{λ} can be implemented in deterministic polynomial time, with approximately $O(\log^3(q))$ operations over \mathbb{F}_q .

- *Proof.* The function f_{λ} is deterministic in the sense that, once the parameters q, c and u are fixed, then any input $r \in \mathcal{R}$ will always give the same output $P = (x_{\lambda}, y_{\lambda})$. In fact, the algorithm does not involve any random value.
- To show that the algorithm is also computable in polynomial time, we must evaluate its complexity. Globally, the computation of $P = (x_{\lambda}, y_{\lambda})$ requires some inversions, some multiplications, one computation of the quadratic character χ and one square root computation. The computation of χ can be replaced by an exponentiation (to test if *a* is square, just compute *a* to the exponent (q-1)/2), which requires $O(\log^3(q))$ operations. Computing a square root in \mathbb{F}_q requires $O(\log^3(q))$ operations when $q \equiv 3 \mod 4$; and more generally, it can be done in probabilistic polynomial time by using the Tonelli-Shanks algorithm. The inversions can be made efficiently by using extended Euclid algorithm or avoided by using projective coordinates (excepted for the last two inversions in x_{λ} and y_{λ}). So globally, we can expect our algorithm to run in polynomial time (with approximatively $O(\log^3(q))$ operations). \Box

From definition (1) and from Algorithm (1), it is easy to see that given any point $P \in \text{Im}(f_{\lambda})$ such that $f_{\lambda}(r) = P$ (for a certain $r \in \mathcal{R}$), we have $f_{\lambda}^{-1}(P) = \{r, -r\}$. This results from the fact that the definition of the encoding f_{λ} only involves r^2 . Hence, if $f_{\lambda}(r) = P$, then $f_{\lambda}(-r) = P$ also. And one can show that r, -r are the only points in the set $f_{\lambda}^{-1}(P)$ (like in [1] or in [8], this property of f_{λ} is called *almost-injectivity*). Moreover, we can invert f_{λ} as follows.

Lemma 2 (Inverting f_{λ}).

Given a point $P = (x_{\lambda}, y_{\lambda}) \in Im(f_{\lambda})$, we can compute its preimage $r \in \mathcal{R}$ as follows:

$$\begin{aligned} - & if \ \chi(y_{\lambda}) = -1, \ then \ r = \frac{1}{2c^3} \sqrt{\frac{c(x-1)(3+c^4) + (1+x)(1+3c^4)}{u[x(1-c)+1+c]}} \ ; \\ - & if \ \chi(y_{\lambda}) = 1, \ then \ r = \frac{1}{2c^3(1-c^4)} \sqrt{\frac{(1+x)(5c^4-1) + c(1-x)(3+c^4)}{u[(1-c^4)(1+x+c(x-1))]}}. \end{aligned}$$

The proof is similar to those in [1,8].

Remark 2. Encodings into elliptic curves can be used in several ways. For example, Bernstein *et al.* [1] used an almost-injective encoding, namely Elligator-2, to make uniform strings indifferentiable from random. When the encoding function is well-distributed, it can be used to design an indifferentiable hash function into $E(\mathbb{F}_q)$. We can use these two applications for our encoding, since it is:

- almost-injective: injective when restricted to a certain subset S of \mathbb{F}_q . In fact, we can characterize the image set of f_{λ} and show that given a point P in $\operatorname{Im}(f_{\lambda}), f_{\lambda}^{-1}(P) \in \{r, -r\}$ for some $r \in \mathbb{F}_q$. When \mathbb{F}_q is a prime field, one can just set $S = \{0, 1, \ldots, \frac{q-1}{2}\}$;
- and *well-distributed*: in [11], Farashahi *et al.* showed that any deterministic encoding into elliptic curves can be transformed into a well-distributed one.

Example 1. We consider an example with the following parameters: q = 503, we set u = -1 and c = 3. A code for the implementation is given in appendix as well as the outputs for this example.

4 Conclusion

In this work, we described the first known encoding for the theta model for elliptic curves E_{λ} : $1 + x^2 + y^2 + x^2y^2 = \lambda^2xy$. And we showed that this new encoding is efficiently computable (deterministic and polynomial-time). A numerical example is also given to ensure the correctness of our encoding. Like existing encodings for other models of curves, our encoding has some interesting features, like almost-injectivity and inversibility. Such properties can be used to design indifferentiable hash functions in the group of points of the curve, or to design IBE-schemes.

A An Implementation of Theta-Model-Encoding in Sage

```
class ThetaModel():
    def init(self,q,u,c): ##assuming q is prime
    self.F=FiniteField(q,'a')
         self.q=q
         self.u=u
         self c=c
    def verificationParameters(self):
         F=self.F
         q=self.q
         u=self.u
         c=self.c
         if F.characteristic()==2:
             print 'Error: The characteristic is egal to', F.characteristic()
             return False
         else:
             if (F(c).is_zero() is True) or (F(1-c<sup>4</sup>).is_zero() is True) or (F(1+c<sup>4</sup>).is_zero() is True):
                  print 'Error: bad value for c
                  return False
             else:
                 if (F(u).is_zero() is True) or (F(u).is_square() is True):
print 'Error: u={} is zero or is a square'.format(u)+' in the finite field of {} elements'.format(F.order())
                      return False
                  else:
                       return True
    def setOfDefinition(self,value):
        F=self.F
         c=self.c
         u=self.u
         r=F(value)
         if (F(4*u*r*r*(c^6)-(1-c^4)*(1+3*c^4)).is_zero() is True) or
         ( F(4+u*r*r*(c^6)+(1-c^4)'4).is_zero() is True ) or ( F(4+u*r*r*(c^6)*(1+3*(c^4))-(1-c^4)^3).is_zero() is True):
    print 'r={} is not in the set of definition'.format(r)
             return False
         else:
            return True
    def quadraticCharacter(self,value):
         F=self.F
         try:
             residu=value.is square()
         except:
             residu=F(value).is_square()
         if residu is True:
             return 1
         else:
             return -1
    def encodeTheta(self,value):
         if self.verificationParameters() is True:
             if self.setOfDefinition(value) is True:
                  F=self.F
                  r=F(value)
                  c=self.c
                  u=self.u
                  v=F( c*(4*u*r*r*(c^6)+(1-c^4)*(3+c^4))/(4*u*r*r*(c^6)+(1-c^4)*(-3*(c^4)-1)) );
                  e=self.quadraticCharacter((c*c-v*v)*(1-c*c*v*v));
X=F( v*(e+1)/2 + (((-c^4-1)*(v+c)-c*(1-c^4))/(2*(c^3)*(v+c)+1-c^4))*(e-1)/2 );
                  trv:
                       a=F((c*c-X*X)/(1-c*c*X*X))
                       root=a.square_root()
Y=-e*root
                       x=(X+1)/(X-1)
                       y=(Y-1)/(Y+1)
                       return (F(x),F(y))
                  except:
                       print 'Error when computing the square root of f(x)'
                       return {}
```

B Example with q = 503, u = -1, c = 3:.

t=ThetaModel()	r= 4 ====>(x,y)= (212, 73)	r= 17 ====>(x,y)= (283, 123)
t.init(501,-1,3)	r= 5 ====>(x,y)= (307, 100)	r= 18 ====>(x,y)= (327, 188)
if t.verificationParameters() is True:	r= 6 ====>(x,y)= (23, 298)	r= 19 ====>(x,y)= (411, 365)
for i in t.F:	r= 7 ====>(x,y)= (42, 171)	r= 20 ====>(x,y)= (480, 265)
if t.setOfDefinition(i) is True:	r= 8 ====>(x,y)= (311, 239)	r= 21 ====>(x,y)= (25, 485)
print 'r=',i,'====>(x,y)=',	r= 9 ====>(x,y)= (491, 332)	r= 22 ====>(x,y)= (386, 153)
t.encodeTheta(i)	r= 10 ====>(x,y)= (415, 385)	r= 23 ====>(x,y)= (176, 404)
	r= 11 ====>(x,y)= (125, 490)	r= 24 ====>(x,y)= (368, 142)
	r= 12 ====>(x,y)= (330, 470)	r= 25 ====>(x,y)= (121, 62)
r= 0 ====>(x,y)= (430, 121)	r= 13 ====>(x,y)= (328, 205)	r= 26 ====>(x,y)= (40, 422)
r= 1 ====>(x,y)= (441, 382)	r= 14 ====>(x,y)= (315, 483)	r= 27 ====>(x,y)= (461, 50)
r= 2 ====>(x,y)= (386, 240)	r= 15 ====>(x,y)= (77, 31)	r= 28 ====>(x,y)= (318, 46)
r= 3 ====>(x,y)= (283, 274)	r= 16 ====>(x,y)= (352, 369)	r= 29 ====>(x,y)= (170, 76)

r≡	30 ====>(x,y)=	(217, 310)	r≡	120 :
r≡	31 ====>(x,y)=	(171, 12)	r≡	121 :
r=	32 ====>(x,y)=	(187, 49)	r=	122 :
r=	33 ====>(x,y)=	(436, 313)	r=	123 -
r=	34 ====>(x, y)=	(31, 98)	r=	124
r=	35 ====>(x,y)	(43, 350)	-	105 -
1-	30>(x,y)-	(200 72)	1-	100 -
r=	36 ====>(x,y)=	(302, 73)	T.=	120 -
r=	37 ====>(x,y)=	(490, 125)	r=	127 -
r=	38 ====>(x,y)=	(338, 435)	r=	128 -
r≡	39 ====>(x,y)=	(124, 141)	r≡	129 :
r≡	40 ====>(x,y)=	(378, 387)	r≡	130 =
r=	41 ====>(x, y)=	(416, 457)	r=	131 :
- r=	42 ====>(x, y)=	(63 32)	- r=	132
	42>(x,y)	(96 51)	-	122 -
1-	43>(x,y)-	(80, 51)	T	100 -
T=4	44 IS NOT IN THE	Set of definition	T.=	134 -
r=	45 ====>(x,y)=	(470, 330)	r=	135 -
r≡	46 ====>(x,y)=	(259, 352)	r≡	136 =
r≡	47 ====>(x,y)=	(153, 460)	r≡	137 :
r≡	48 ====>(x,y)=	(318, 339)	r≡	138 =
r=	49 ====> (x, y) =	(237, 69)	r=	139 :
r=	50 ====>(x, y)=	(220, 380)	r=	140 =
r≡	51 ====>(x y)=	(442 330)	r=	141 :
	51 = (x, y) = (x, y	(112, 000)		140 -
r=	52 ====>(x,y)=	(213, 100)	T.=	142 '
r=	53 ====>(x,y)=	(495, 110)	r=	143 •
r=	54 ====>(x,y)=	(393, 8)	r=	144 •
r=	55 ====>(x,y)=	(185, 164)	r=	145 =
r≡	56 ====>(x,y)=	(287, 364)	r≡	146 •
r=	57 ====>(x,y)=	(378, 13)	r≡	147 :
r=	58 ====>(x,y)=	(472, 405)	r=	148 :
r=	59 ====>(x, y)=	(232, 304)	r=	149 =
r=	60 ====>(v v)=	(51, 310)	r=	150 -
	61>(x,y)	(016 120)	-	161 -
1-	01>(x,y)-	(210, 139)	T	101 .
r=	62 ====>(x,y)=	(258, 199)	r=	152 -
r=	63 ====>(x,y)=	(60, 476)	r=	153 -
r=	64 ====>(x,y)=	(258, 91)	r=	154 =
r=	65 ====>(x,y)=	(382, 441)	r=	155 :
r≡	66 ====>(x,y)=	(352, 259)	r≡	156 :
r=	67 ====>(x,y)=	(350, 117)	r=	157 :
r=	68 ====>(x, y)=	(109, 149)	r=	158 -
- r=	69 ====>(x, y)=	(102 336)	- r=	159
	70 ====>(x,y)	(467, 275)	-	160 -
1-	70>(x,y)-	(405, 454)	1-	100 -
r=	71>(x,y)=	(425, 154)	T.=	101 -
r=	72 ====>(x,y)=	(339, 318)	r=	162 -
r=	73 ====>(x,y)=	(231, 209)	r=	163 -
r=	74 ====>(x,y)=	(379, 362)	r=	164 =
r≡	75 ====>(x,y)=	(116, 334)	r≡	165 :
r=	76 ====>(x,y)=	(252, 502)	r=	166 =
r=	77 ====> (x, y) =	(149, 109)	r=	167 :
r=	78 ====>(x, y)=	(235, 278)	r=	168 -
- r=	79 ====>(x, y)=	(466 338)	- r=	169
	90 ====>(x,y)=	(460, 330)		170 -
1-	80>(x,y)-	(407, 410)	T	170 .
r=	81 ====>(x,y)=	(10, 123)	T.=	1/1 '
r=	82 ====>(x,y)=	(495, 471)	r=	172 -
r=	83 ====>(x,y)=	(141, 215)	r=	173 -
r=	84 ====>(x,y)=	(470, 157)	r=	174 =
r=	85 ====>(x,y)=	(127, 94)	r=	175 :
r=	86 ====>(x,y)=	(334, 490)	r=	176 :
r=	87 ====>(x, y)=	(311, 181)	r=	177 -
r≡	88 =====>(x y)=	(301 409)	r=	178
r=	89 ====>(x y)=	(458, 67)	- r=	179
1-	00>(x,y)-	(440, 471)	1-	100
	01 ====:\(x, y)=	(360 253)		181 -
	00 =====>(x,y)=	(250, 200)	1 - 	100 '
T.a.	52>(x,y)=	(300, 43)	T=	102
r=	90 ====>(x,y)=	(304, 245)	r=	183 -
r=	94 ====>(x,y)=	(322, 192)	r=	184 :
r≡	95 ====>(x,y)=	(173, 33)	r≡	185 :
r≡	96 ====>(x,y)=	(18, 342)	r≡	186 :
r=	97 ====>(x,y)=	(410, 179)	r=	187 :
r=	98 ====>(x.v)=	(485, 25)	r=	188 :
r=	99 ====>(x, y)=	(190, 488)	r=	189
r=	100 ====>(x - y)-	(475 161)	- r=	190 -
	101 ====>(x,y)	(225 122)	r=	101 -
T.a.	100 (X, Y)	- (220, 122)	T=	100
r=	102 ====>(x,y)=	(8, 393)	r=	192 -
r=	103 ====>(x,y)=	(73, 382)	r=	193 :
r≡	104 ====>(x,y)=	= (342, 18)	r≡	194 :
r≡	105 ====>(x,y)=	= (69, 237)	r≡	195 :
r≡	106 ====>(x,y)=	(442, 157)	r≡	196 :
r≡	107 ====>(x,v)=	(443, 27)	r=	197 :
r=	108 ====>(x.v)=	(403, 290)	r=	198 =
r=	109 ====>(y y)=	(12, 453)	- r=	199
r=	110 ====>(x - y)-	(148 214)	r=	200 -
	111 ====>(x,y)=	(201 420)	1 - 	200 1
I.a.	110 (X, Y)	- (200, 400)	T=	201 1
r=	112 ====>(x,y)=	= (269, 48b)	r=	202 -
r=	113 ====>(x,y)=	(135, 361)	r=	203 =
r≡	114 ====>(x,y)=	= (250, 401)	r≡	204 =
r=	115 ====>(x,y)=	(369, 493)	r=	205 :
r≡	116 ====>(x,y)=	(305, 376)	r≡	206 =
r≡	117 ====>(x,v)=	(167, 143)	r=	207 =
r=	118 ====>(y.v)=	(493, 369)	r=	208 =
n=	119 ====>(x,y)	(212 441)	- r=	209
	(A, y)"	·, ····/	÷	

120	>(x,y)=	(125, 116)
121	====>(x,y)=	(38, 235)
122	====>(x,y)=	(490, 334)
123	====>(x,y)=	(196, 337)
124	====>(x,y)=	(263, 43)
125	====>(x,y)=	(324, 93)
126	====>(x,y)=	(357, 77)
127	====>(x,y)=	(337, 290)
128	====>(x,y)=	(337, 196)
129	====>(x,y)=	(164, 185)
130	====>(x,y)=	(460, 153)
131	====>(x,y)=	(14, 224)
132	====>(x,y)=	(245, 412)
133	====>(x,y)=	(110, 495)
134	====>(x,y)=	(271, 91)
135	====>(x,y)=	(478, 18)
136	====>(x,y)=	(151, 134)
137	====>(x,y)=	(435, 189)
138	====>(x,y)=	(467, 279)
139	====>(x,y)=	(404, 483)
140	====>(x,y)=	(489, 279)
141	====>(x,y)=	(409, 301)
142	====>(x,v)=	(493, 259)
143	====>(x,y)=	(315, 176)
144	====>(x,y)=	(28, 478)
145	====>(x,y)=	(237, 226)
146	====>(x,y)=	(157, 442)
147	====>(x, y)=	(465 268)
148	====>(x,y)=	(394 354)
149	====>(x,y)=	(460 240)
150	>(x,y)-	(198 202)
151	>(x,y)-	(100, 202)
151	>(x,y)-	(202, 198)
102	>(x,y)-	(105, 400)
153	>(x,y)=	(01, 339)
154	>(x,y)=	(76, 454)
155	====>(x,y)=	(240, 386)
156	====>(x,y)=	(213, 100)
157	====>(x,y)=	(143, 250)
158	====>(x,y)=	(224, 36)
159	====>(x,y)=	(51, 86)
160	====>(x,y)=	(435, 338)
161	====>(x,y)=	(215, 132)
162	====>(x,y)=	(411, 390)
163	====>(x,y)=	(376, 305)
164	====>(x,y)=	(275, 355)
165	====>(x v)=	(316 349)
	. (2,))	(010, 040)
166	====>(x,y)=	(307, 166)
166 167	====>(x,y)= ====>(x,y)=	(307, 166) (272, 294)
166 167 168	====>(x,y)= ====>(x,y)= ====>(x,y)=	(307, 166) (272, 294) (502, 252)
166 167 168 169	>(x,y)= >(x,y)= >(x,y)= >(x,y)=	(307, 166) (272, 294) (502, 252) (485, 161)
166 167 168 169 170	>(x,y)= >(x,y)= >(x,y)= >(x,y)= >(x,y)=	(307, 166) (272, 294) (502, 252) (485, 161) (463, 118)
166 167 168 169 170 171	>(x,y)= >(x,y)= >(x,y)= >(x,y)= >(x,y)=	(307, 166) (272, 294) (502, 252) (485, 161) (463, 118) (381, 38)
166 167 168 169 170 171 172	>(x,y)= >(x,y)= >(x,y)= >(x,y)= >(x,y)= >(x,y)=	(307, 166) (272, 294) (502, 252) (485, 161) (463, 118) (381, 38) (217, 86)
166 167 168 169 170 171 172 173	>(x,y)= >(x,y)= >(x,y)= >(x,y)= >(x,y)= >(x,y)= >(x,y)=	(307, 166) (272, 294) (502, 252) (485, 161) (463, 118) (381, 38) (217, 86) (476, 60)
166 167 168 169 170 171 172 173 174	<pre>>:(x,y)= >:::>(x,y)= >:::>(x,y)=</pre>	(307, 166) (307, 166) (272, 294) (502, 252) (485, 161) (463, 118) (381, 38) (217, 86) (476, 60) (264, 317)
166 167 168 169 170 171 172 173 174 175		(307, 166) (272, 294) (502, 252) (485, 161) (463, 118) (381, 38) (217, 86) (476, 60) (264, 317) (333, 427)
166 167 168 169 170 171 172 173 174 175 176	<pre>>:(x,y)= >:(x,y)= >:(x,y)</pre>	(307, 166) (272, 294) (502, 252) (465, 161) (463, 118) (381, 38) (217, 86) (476, 60) (264, 317) (333, 427) (88, 81)
166 167 168 169 170 171 172 173 174 175 176	<pre>>(x,y)= >(x,y)= >(x,y)= >>(x,y)= >>(x,y)= >>(x,y)= >>(x,y)= >>(x,y)= >>(x,y)= >>(x,y)= >>>(x,y)= >>>(x,y)= >>>(x,y)= >>>(x,y)= >>>>(x,y)= >>>>(x,y)= >>>>(x,y)= >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>></pre>	(307, 166) (272, 294) (502, 252) (485, 161) (463, 118) (381, 38) (217, 86) (476, 60) (264, 317) (333, 427) (88, 81) (288, 175)
166 167 168 169 170 171 172 173 174 175 176 177		(307, 166) (272, 294) (502, 252) (485, 161) (463, 118) (381, 38) (217, 86) (476, 60) (244, 317) (333, 427) (88, 81) (298, 175) (67, 458)
166 167 168 169 170 171 172 173 174 175 176 177 178	$\begin{array}{c} & \cdots \\ & (x, y) = \\ & \cdots \\ $	(307, 166) (272, 294) (502, 252) (485, 161) (463, 118) (381, 38) (217, 86) (264, 317) (333, 427) (388, 81) (298, 175) (67, 458) (281, 119)
166 167 168 169 170 171 172 173 174 175 176 177 178 179 180	$ \begin{array}{c} & (x,y) \\ & (x,y) $	(337, 166) (377, 166) (372, 294) (502, 252) (485, 161) (485, 161) (485, 161) (485, 161) (485, 161) (485, 161) (485, 161) (381, 38) (217, 86) (217, 86) (217, 86) (217, 86) (233, 427) (88, 81) (298, 175) (67, 458) (281, 119) (238, 466)
166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181	$ \begin{array}{c} & (x,y) \\ & (x,y) $	(212, 342) (307, 166) (272, 294) (502, 252) (485, 161) (465, 118) (381, 38) (217, 86) (476, 60) (264, 317) (333, 427) (68, 81) (298, 175) (67, 458) (281, 119) (338, 466) (199, 258)
166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182	$\begin{array}{c} & & (x,y) = \\ & & (x,y)$	(212, 342) (307, 166) (272, 294) (502, 252) (485, 161) (463, 118) (381, 38) (217, 86) (476, 60) (264, 317) (333, 427) (333, 427) (88, 81) (298, 175) (67, 458) (281, 119) (338, 466) (199, 258)
166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183	$ \begin{array}{c} & (z, y) \\ & (z, y) \\ & (x, y) \\ & ($	(212, 342) (307, 166) (272, 294) (502, 252) (485, 161) (463, 118) (381, 38) (217, 86) (274, 38) (217, 86) (274, 317) (333, 427) (388, 81) (288, 81) (288, 175) (281, 119) (338, 466) (362, 288) (362, 288) (324, 288)
166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184	$ \begin{array}{c} & & (x,y) \\ & & & $	(237, 166) (277, 294) (502, 252) (485, 161) (463, 118) (381, 38) (217, 86) (476, 60) (264, 317) (333, 427) (88, 81) (298, 175) (67, 458) (281, 119) (338, 466) (199, 258) (382, 288) (128, 14)
166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185	$\begin{array}{c} & & & (x,y) \\ & & & & (x,y) \\$	(212, 342) (307, 166) (272, 294) (502, 252) (485, 161) (463, 118) (381, 38) (217, 86) (274, 38) (274, 86) (274, 317) (333, 427) (38, 41) (298, 175) (38, 466) (138, 466) (139, 258) (362, 288) (362, 288) (364, 222) (384, 422) (384, 422) (385, 357)
166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185	$ \begin{array}{c} & & (x,y) \\ & & & & (x$	(237, 166) (277, 294) (502, 252) (485, 161) (463, 118) (381, 38) (217, 86) (476, 60) (264, 317) (333, 427) (88, 81) (298, 175) (67, 458) (281, 119) (338, 466) (199, 258) (362, 288) (128, 14) (384, 222) (98, 357) (990, 403)
1666 1677 1688 1699 1700 1711 1722 1733 1744 1755 1766 1777 1788 1799 1800 1811 1822 1833 1844 1855 1865	$\begin{array}{c} & & & & & \\ & & & & & & \\ & & & & & & $	(212, 342) (307, 166) (272, 294) (502, 252) (485, 161) (463, 118) (281, 38) (217, 86) (476, 60) (264, 317) (284, 317) (288, 81) (298, 175) (67, 458) (281, 119) (281, 119) (281, 119) (282, 288) (122, 14) (384, 466) (199, 258) (362, 288) (128, 14) (384, 222) (98, 357) (290, 403) (466, 189)
166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187	$\begin{array}{c} & & (x,y) \\ & &$	(212, 342) (307, 166) (272, 294) (502, 252) (485, 161) (463, 118) (381, 38) (217, 86) (274, 38) (217, 86) (274, 38) (284, 317) (333, 427) (383, 427) (384, 427) (384, 428) (384, 428) (128, 14) (384, 222) (98, 387) (290, 403) (466, 189)
1666 167 168 169 170 171 172 173 174 175 176 177 178 180 181 182 183 184 185 186 187 188	$\begin{array}{c} & & (x,y) \\ & &$	(212, 342) (207, 166) (272, 294) (502, 252) (485, 161) (463, 118) (381, 38) (217, 86) (274, 38) (274, 86) (284, 317) (333, 427) (88, 81) (298, 175) (67, 458) (281, 119) (284, 119) (284, 119) (284, 119) (284, 222) (98, 357) (290, 403) (486, 189) (186, 239)
166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189	$\begin{array}{c} & & & (x,y) \\ & & & & (x,y)$	(212, 342) (307, 166) (272, 294) (502, 252) (485, 161) (463, 118) (381, 38) (217, 86) (476, 60) (264, 317) (333, 427) (383, 427) (384, 317) (388, 81) (298, 175) (388, 427) (388, 427) (388, 428) (199, 258) (382, 288) (128, 14) (384, 222) (98, 357) (290, 403) (486, 189) (104, 69) (104, 69)
166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190	$\begin{array}{c} & & & (x,y) \\ & & & & (x,y)$	(237, 166) (277, 294) (502, 252) (485, 161) (463, 118) (381, 38) (217, 86) (274, 36) (274, 317) (284, 317) (284, 317) (294, 175) (67, 458) (281, 119) (233, 466) (199, 258) (384, 422) (98, 357) (290, 403) (486, 189) (186, 239) (186, 239) (186, 239) (186, 128) (374, 126) (374, 126) (374, 126) (374, 126) (375,
166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190	$\begin{array}{c} & & & & & & \\ & & & & & & \\ & & & & & $	(212, 342) (307, 166) (272, 294) (502, 252) (485, 161) (463, 118) (381, 38) (217, 86) (476, 60) (264, 317) (333, 427) (88, 81) (298, 175) (67, 458) (281, 119) (338, 466) (199, 258) (362, 288) (128, 14) (384, 422) (98, 357) (290, 403) (466, 189) (138, 69) (364, 128) (132, 124) (364, 128)
166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191	$\begin{array}{c} & & & (x,y) \\ & & & &$	(207, 166) (272, 294) (502, 252) (485, 161) (463, 118) (381, 38) (217, 86) (274, 38) (217, 86) (264, 317) (284, 317) (67, 458) (298, 175) (67, 458) (298, 175) (67, 458) (298, 175) (67, 458) (298, 175) (67, 458) (281, 119) (338, 466) (199, 258) (362, 288) (128, 14) (364, 222) (98, 357) (290, 403) (466, 189) (186, 239) (186, 239) (186, 239) (182, 124) (46, 87)
166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192	$\begin{array}{c} \\ & = & (x,y) \\ \\ & = & (x,y) \\ & = & (x,y) \\ \\ & = & (x,y) \\ & = & (x,y) \\ \\ & = & (x,$	(212, 342) (237, 166) (272, 294) (502, 252) (485, 161) (463, 118) (381, 38) (217, 86) (274, 38) (274, 86) (284, 317) (333, 427) (88, 81) (298, 175) (67, 458) (281, 119) (338, 466) (199, 258) (362, 288) (128, 14) (384, 422) (98, 357) (290, 403) (466, 189) (136, 69) (36, 128) (132, 124) (46, 87) (225, 268)
166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 182 183 184 186 187 188 189 190 191 192 193	$\begin{array}{c} & & & & & & \\ & & & & & & \\ & & & & & $	(225, 244) (307, 166) (272, 294) (502, 252) (485, 161) (463, 118) (381, 38) (217, 86) (274, 38) (217, 86) (274, 38) (284, 317) (333, 427) (388, 41) (388, 427) (388, 427) (388, 427) (388, 427) (388, 427) (388, 428) (199, 258) (382, 288) (128, 14) (384, 222) (98, 357) (290, 403) (466, 189) (104, 69) (36, 128) (103, 124) (46, 87) (225, 268) (263, 117)
166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194	$\begin{array}{c} & & & (x,y) \\ & & & & (x,$	(212, 342) (237, 166) (272, 294) (502, 252) (485, 161) (463, 118) (381, 38) (217, 86) (274, 38) (274, 86) (284, 317) (284, 317) (283, 175) (67, 458) (284, 317) (284, 317) (284, 317) (284, 317) (284, 317) (284, 317) (284, 317) (284, 317) (384, 466) (139, 258) (324, 466) (139, 258) (128, 14) (384, 222) (98, 357) (296, 327) (136, 128) (132, 124) (465, 87) (225, 268) (263, 117) (475, 25)
166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 196 197 197 197 198 197 198 197 198 197 198 199 197 198 197 198 199 198 198 199 198 199 199	$\begin{array}{c} & & & & & & \\ & & & & & & \\ & & & & & $	(225, 244) (237, 166) (272, 294) (502, 252) (485, 161) (463, 118) (281, 38) (217, 86) (274, 38) (284, 38) (284, 38) (284, 38) (284, 317) (333, 427) (388, 41) (288, 317) (288, 317) (288, 317) (288, 317) (384, 466) (128, 14) (384, 422) (384, 428) (364, 128) (134, 428) (134, 42
166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 1890 191 192 193 194 195 196 197 197 192 193 194 195 196 197 197 197 197 197 197 197 197	$\begin{array}{c} & & & & & & \\ & & & & & & \\ & & & & & $	(212, 342) (237, 166) (272, 294) (502, 252) (485, 161) (463, 118) (381, 38) (217, 86) (476, 60) (264, 317) (333, 427) (88, 81) (298, 175) (67, 458) (281, 119) (284, 119) (284, 119) (384, 426) (128, 14) (384, 422) (384, 422) (384, 222) (384, 2
166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 197 198	$\begin{array}{c} & & & & & & \\ & & & & & & \\ & & & & & $	(225, 244) (307, 166) (272, 294) (502, 252) (485, 161) (463, 118) (381, 38) (217, 86) (264, 317) (333, 427) (88, 81) (298, 175) (67, 458) (281, 119) (384, 466) (199, 258) (362, 288) (128, 14) (384, 422) (98, 357) (290, 403) (466, 189) (136, 293) (104, 69) (36, 128) (132, 124) (46, 87) (225, 268) (225, 268) (263, 117) (475, 25) (487, 229) (404, 176) (328, 265)
1666 1677 1688 1699 1700 1711 1722 1733 1744 1755 1766 1777 1788 1799 1800 1811 1822 1833 1844 1855 1866 1877 1888 1890 1911 1922 1933 1944 1955 1966 1977 1988 1997	$\begin{array}{c} & & & (x,y) \\ & & & (x,$	(212, 242) (237, 166) (272, 294) (502, 252) (485, 161) (463, 118) (381, 38) (217, 86) (274, 38) (217, 86) (274, 317) (284, 317) (298, 175) (67, 458) (281, 119) (238, 466) (199, 258) (384, 222) (98, 357) (290, 403) (486, 189) (186, 239) (104, 69) (36, 128) (132, 124) (465, 877) (225, 268) (265, 117) (475, 25) (487, 229) (404, 176) (328, 265) (328, 265
1666 1677 1688 1699 1700 1711 1722 1733 1744 1755 1766 1777 1788 1799 1800 1811 1822 1833 1844 1855 1866 1877 1888 1890 1901 1912 1933 1946 1977 1988 1999 2000	$\begin{array}{c} & & & (x,y) \\ & & & &$	(212, 342) (237, 166) (272, 294) (502, 252) (485, 161) (463, 118) (381, 38) (217, 86) (274, 38) (284, 317) (333, 427) (88, 81) (298, 175) (67, 458) (281, 119) (338, 466) (199, 258) (338, 466) (199, 258) (362, 288) (128, 14) (384, 422) (98, 357) (290, 403) (466, 189) (136, 229) (104, 69) (36, 128) (132, 124) (467, 225) (487, 225) (487, 225) (487, 225) (487, 229) (404, 176) (328, 265) (82, 390) (104, 226)
1666 1677 1688 1699 1700 1711 1722 1733 1744 1755 1766 1777 1788 1799 1800 1811 1822 1833 1844 1855 1866 1877 1988 1990 1911 1922 1933 1944 1957 1968 1979 1970 1971 1972 1973 1974 1975 1975 1975 1975 1975 1975 1975 1975	$\begin{array}{c} & & & (x,y) \\ & & & &$	(227, 294) (502, 252) (485, 161) (463, 118) (381, 38) (217, 86) (477, 60) (264, 317) (67, 458) (298, 175) (67, 458) (298, 175) (290, 403) (466, 189) (184, 222) (404, 169) (36, 128) (132, 124) (467, 25) (404, 176) (328, 265) (52, 390) (104, 226) (104,
1666 1677 1688 1699 1700 1711 1722 1733 1744 1755 1766 1777 1788 1799 1800 1811 1822 1833 1844 1855 1866 1877 1888 1899 1900 1914 1955 1966 1977 1988 1999 2000 2012 202	$\begin{array}{c} & & (x,y) \\ & & & &$	(212, 342) (237, 166) (272, 294) (502, 252) (485, 161) (463, 118) (381, 38) (217, 86) (274, 38) (284, 317) (333, 427) (88, 81) (298, 175) (67, 458) (284, 119) (338, 466) (199, 258) (338, 466) (199, 258) (324, 466) (198, 357) (299, 403) (466, 189) (136, 128) (132, 124) (465, 87) (255, 268) (263, 117) (475, 25) (487, 129) (104, 226) (104, 22
1666 1677 1688 1699 1700 1711 1722 1733 1744 1755 1760 1777 1788 1799 1800 1811 1822 1833 1844 1855 1866 1877 1888 1899 1900 1911 1922 1933 1944 1955 1966 1977 1982 1992 2000 2012 2022 2033	$\begin{array}{c} & & (x,y) \\ & &$	(225, 246) (237, 166) (272, 294) (502, 252) (485, 161) (463, 118) (281, 38) (217, 86) (274, 38) (264, 317) (333, 427) (38, 41) (288, 31) (298, 175) (281, 119) (384, 466) (199, 258) (382, 466) (199, 258) (382, 288) (128, 14) (384, 422) (384, 222) (364, 128) (132, 124) (46, 87) (225, 266) (235, 126) (475, 25) (487, 229) (404, 176) (328, 266) (322, 226) (322, 226) (322, 220) (488, 190) (342, 8)
1666 1677 1688 1699 1700 1711 1722 1733 1744 1755 1767 1777 1788 1800 1811 1822 1833 1844 1855 1860 1811 1922 1933 1944 1956 1971 1938 1990 2001 2020 2030 204	$\begin{array}{c} & & & (x,y) \\ & & & &$	(227, 294) (502, 252) (485, 161) (502, 252) (485, 161) (463, 118) (381, 38) (217, 86) (274, 38) (284, 317) (284, 317) (288, 317) (288, 317) (288, 317) (288, 317) (288, 317) (288, 317) (288, 317) (288, 317) (284, 317) (338, 466) (139, 258) (328, 148) (328, 466) (139, 258) (328, 466) (139, 258) (328, 466) (139, 258) (328, 222) (384, 222) (485, 176) (322, 268) (104, 256) (104, 226) (104, 226) (10
1666 167 168 169 170 171 172 173 174 175 176 176 177 178 179 180 181 182 183 184 185 186 187 190 191 192 193 194 195 196 197 192 203 204 205	$\begin{array}{c} & & & & & & & \\ & & & &$	(212, 342) (307, 166) (272, 294) (502, 252) (485, 161) (463, 118) (381, 38) (217, 86) (374, 86) (264, 317) (333, 427) (88, 81) (298, 175) (67, 458) (281, 119) (338, 466) (199, 258) (362, 288) (128, 14) (384, 222) (98, 357) (290, 403) (466, 189) (138, 228) (132, 124) (46, 87) (225, 268) (225, 268) (225, 268) (263, 117) (36, 128) (132, 124) (46, 87) (225, 268) (263, 117) (328, 225) (487, 229) (404, 176) (328, 265) (82, 380) (104, 226) (229, 220) (482, 190) (342, 16)
1666 1677 1688 1699 1700 1711 1722 1733 1744 1755 1766 1777 1788 1800 1811 1822 1833 1844 1855 1866 1877 1888 1890 1911 1922 1933 1944 1955 1966 1977 1988 1999 2000 2011 2022 2033 2044	$\begin{array}{c} & & & (x,y) \\ & & &$	(212, 242) (237, 166) (272, 294) (502, 252) (485, 161) (463, 118) (381, 38) (217, 86) (274, 38) (217, 86) (274, 317) (284, 317) (298, 175) (67, 458) (281, 119) (284, 175) (67, 458) (281, 119) (283, 466) (199, 258) (384, 222) (98, 357) (290, 403) (486, 189) (136, 229) (132, 124) (466, 87) (265, 117) (475, 25) (467, 229) (404, 176) (228, 266) (228, 265) (328, 265) (328, 266) (342, 229) (404, 176) (328, 265) (328, 265) (328, 265) (328, 265) (328, 220) (482, 376)
1666 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207	$\begin{array}{c} & & & (x,y) \\ & & & & (x,$	(212, 342) (307, 166) (272, 294) (502, 252) (485, 161) (463, 118) (381, 38) (217, 86) (274, 38) (284, 317) (333, 427) (88, 81) (298, 175) (67, 458) (281, 119) (338, 466) (199, 258) (362, 288) (128, 14) (338, 466) (128, 14) (338, 466) (128, 12) (342, 12) (464, 189) (136, 239) (104, 69) (364, 128) (136, 128) (132, 124) (467, 25) (487, 229) (404, 176) (328, 265) (229, 200) (342, 28) (161, 475) (344, 116) (348, 375) (480, 205)
166 167 168 169 170 171 172 173 174 175 176 177 178 177 178 177 178 177 178 177 178 177 178 177 178 180 181 182 183 184 185 186 187 190 191 192 193 194 192 193 194 192 193 194 192 193 194 192 193 194 192 193 194 192 193 194 192 193 194 192 193 194 194 195 196 197 197 198 197 197 198 197 197 198 197 197 198 197 197 198 197 197 198 197 197 198 197 198 198 197 198 198 198 198 198 198 198 198 199 199	$\begin{array}{c} & & (x,y) \\ & & & (x,y) \\$	(237, 166) (277, 294) (502, 252) (485, 161) (463, 118) (381, 38) (217, 86) (274, 38) (217, 86) (264, 317) (333, 427) (88, 81) (298, 175) (67, 458) (298, 175) (67, 458) (298, 175) (67, 458) (298, 175) (67, 458) (298, 175) (67, 458) (298, 175) (67, 458) (281, 119) (333, 466) (199, 258) (364, 228) (128, 14) (364, 228) (134, 222) (404, 176) (326, 228) (104, 69) (35, 128) (132, 124) (465, 87) (225, 268) (226, 217) (475, 25) (404, 176) (328, 265) (52, 390) (104, 226) (228, 220) (488, 190) (342, 228) (161, 475) (403, 196)

	210	====>(x y)=	(278 381)
	011	>(x,y)	(175 022)
r=	211	>(x,y)=	(175, 236)
r=	212	====>(x,y)=	(375, 467)
r≡	213	====>(x,y)=	(401, 167)
r=	214	====>(x,y)=	(288, 371)
r≡	215	====>(x y)=	(87 46)
	216	>(x, y)-	(071 100)
	210	>(x,y)-	(271, 133)
T	211	>(x,y)-	(511, 519)
r=	218	====>(x,y)=	(50, 491)
r≡	219	====>(x,y)=	(186, 181)
r≡	220	====>(x,y)=	(10, 244)
r=	221	====>(x,y)=	(146, 426)
r=	222	====>(x,y)=	(31, 77)
- r=	223	====>(x, y)=	(117 263)
<u> </u>	004	>(n,j)	(110, 110)
T	224	>(x,y)-	(440, 110)
r=	225	====>(x,y)=	(189, 435)
r≡	226	====>(x,y)=	(502, 2)
r≡	227	====>(x,y)=	(441, 212)
r=	228	====>(x,y)=	(465, 122)
r=	229	====>(x,y)=	(279, 489)
- r=	230	====>(x, y)=	(483 315)
	200	> (x,y)-	(17, 000)
r=	231	>(x,y)=	(17, 220)
r=	232	====>(x,y)=	(91, 271)
r≡	233	====>(x,y)=	(94, 127)
r≡	234	====>(x,y)=	(169, 387)
r=	235	====>(x,y)=	(453, 42)
r=	236	====>(x,y)=	(15, 45)
r=	237	====>(x,y)=	(116, 125)
- r=	238	====>(x, y)=	(20 99)
	200	> (x,y)-	(20, 33)
r=	239	>(x,y)=	(357, 96)
r≡	240	====>(x,y)=	(310, 217)
r≡	241	====>(x,y)=	(346, 61)
r≡	242	====>(x,y)=	(226, 104)
r=	243	====>(x,y)=	(73, 212)
r=	244	====>(x y)=	(471 440)
	246	>(x,y)	(160 12)
T	240	>(x,y)-	(109, 13)
r=	246	====>(x,y)=	(412, 232)
r=	247	====>(x,y)=	(32, 63)
r=	248	====>(x,y)=	(332, 461)
r≡	249	====>(x,y)=	(478, 28)
r≡	250	====>(x,y)=	(82, 365)
r=	251	====>(x,y)=	(16, 274)
r=	252	====>(x,y)=	(16, 274)
r=	253	====>(x,y)=	(82, 365)
- r=	254	====>(x, y)=	(478 28)
	201	>(x,y)	(220, 461)
T	200	>(x,y)-	(332, 401)
r=	256	====>(x,y)=	(32, 63)
r=	257	====>(x,y)=	(412, 232)
r=	258	====>(x,y)=	(169, 13)
r= r=	258 259	====>(x,y)= ====>(x,y)=	(169, 13) (471, 440)
r= r= r=	258 259 260	>(x,y)= >(x,y)= >(x,y)=	(169, 13) (471, 440) (73, 212)
r= r= r= r=	258 259 260 261	====>(x,y)= ====>(x,y)= ====>(x,y)= ====>(x,y)=	(169, 13) (471, 440) (73, 212) (226, 104)
r= r= r= r=	258 259 260 261 262	====>(x,y)= ====>(x,y)= ====>(x,y)= ====>(x,y)=	(169, 13) (471, 440) (73, 212) (226, 104) (346, 61)
r= r= r= r= r=	258 259 260 261 262 263	====>(x,y)= ====>(x,y)= ====>(x,y)= ====>(x,y)= ====>(x,y)=	(169, 13) (471, 440) (73, 212) (226, 104) (346, 61) (310, 217)
r= r= r= r= r=	258 259 260 261 262 263 263	====>(x,y)= ====>(x,y)= ====>(x,y)= ====>(x,y)= ====>(x,y)=	(169, 13) (471, 440) (73, 212) (226, 104) (346, 61) (310, 217) (257, 98)
r= r= r= r= r= r=	258 259 260 261 262 263 264	====>(x,y)= ====>(x,y)= ====>(x,y)= ====>(x,y)= ====>(x,y)= ====>(x,y)=	(169, 13) (471, 440) (73, 212) (226, 104) (346, 61) (310, 217) (357, 98)
r= r= r= r= r= r=	258 259 260 261 262 263 264 265	====>(x,y)= ====>(x,y)= ====>(x,y)= ====>(x,y)= ====>(x,y)= ====>(x,y)=	(169, 13) (471, 440) (73, 212) (226, 104) (346, 61) (310, 217) (357, 98) (20, 99)
r= r= r= r= r= r= r=	258 259 260 261 262 263 264 265 266	<pre>>(x,y)= >(x,y)= ></pre>	(169, 13) (471, 440) (73, 212) (226, 104) (346, 61) (310, 217) (357, 98) (20, 99) (116, 125)
r= r= r= r= r= r= r= r=	258 259 260 261 262 263 264 265 265 266 267	<pre>>(x,y)= >(x,y)= ></pre>	(169, 13) (471, 440) (73, 212) (226, 104) (346, 61) (310, 217) (357, 98) (20, 99) (116, 125) (15, 45)
r= r= r= r= r= r= r= r= r=	258 259 260 261 262 263 264 265 266 266 267 268	<pre>>(x,y)= >(x,y)= >(x,y)= >>>(x,y)= >>>>(x,y)= >>>>(x,y)= >>>>(x,y)= >>>>>(x,y)= >>>>>(x,y)= >>>>>>>>>(x,y)= >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>></pre>	(169, 13) (471, 440) (73, 212) (226, 104) (346, 61) (310, 217) (357, 98) (20, 99) (116, 125) (15, 45) (453, 42)
r= r= r= r= r= r= r= r= r= r=	258 259 260 261 262 263 264 265 266 266 267 268 269	<pre>>>(x,y)= >>>(x,y)= >>>>(x,y)= >>>>(x,y)= >>>>>(x,y)= >>>>>(x,y)= >>>>>>>>>>(x,y)= >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>></pre>	(169, 13) (471, 440) (73, 212) (226, 104) (346, 61) (310, 217) (357, 98) (20, 99) (116, 125) (15, 45) (453, 42) (169, 387)
r= r= r= r= r= r= r= r= r= r=	258 259 260 261 262 263 264 265 266 266 266 267 268 269 270	<pre>>>(x,y)= >>>(x,y)= >>>>(x,y)= >>>>>(x,y)= >>>>>(x,y)= >>>>>(x,y)= >>>>>(x,y)= >>>>>>>>>>(x,y)= >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>></pre>	(169, 13) (471, 440) (73, 212) (226, 104) (346, 61) (310, 217) (357, 98) (20, 99) (116, 125) (15, 45) (453, 42) (169, 387) (94, 127)
r= r= r= r= r= r= r= r= r= r=	258 259 260 261 262 263 264 265 266 266 267 268 269 270 271	<pre>>>(x, y)= >>(x, y)= >>>(x, y)= >>>(x, y)= >>>(x, y)= >>>>(x, y)= >>>>(x, y)= >>>>>>>>>(x, y)= >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>></pre>	(169, 13) (471, 440) (73, 212) (226, 104) (346, 61) (310, 217) (357, 98) (20, 99) (116, 125) (15, 45) (453, 42) (169, 387) (94, 127) (94, 127)
r= r= r= r= r= r= r= r= r= r= r=	258 259 260 261 262 263 264 265 266 267 268 269 270 271 272	$\begin{array}{c} \\ & = &$	(169, 13) (471, 440) (73, 212) (226, 104) (346, 61) (310, 217) (357, 98) (20, 99) (116, 125) (15, 45) (453, 42) (169, 387) (94, 127) (91, 271) (91, 271)
r= r= r= r= r= r= r= r= r= r= r=	258 259 260 261 262 263 264 265 266 267 268 269 270 271 272	$ \begin{array}{c} \\ & \\ \\ & \\ \\ & \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ $	(169, 13) (471, 440) (73, 212) (226, 104) (346, 61) (310, 217) (357, 98) (20, 99) (116, 125) (15, 45) (453, 42) (169, 387) (94, 127) (91, 271) (17, 228)
r= r= r= r= r= r= r= r= r= r= r= r= r=	258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273	$\begin{array}{c} & & & \\$	(169, 13) (471, 440) (73, 212) (226, 104) (346, 61) (310, 217) (357, 98) (20, 99) (116, 125) (15, 45) (453, 42) (169, 387) (94, 127) (91, 271) (17, 228) (483, 315)
r= r= r= r= r= r= r= r= r= r= r= r= r= r	258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274	$\begin{array}{c} & & & (x,y) = \\ & & & ($	(169, 13) (471, 440) (73, 212) (226, 104) (346, 61) (310, 217) (357, 98) (20, 99) (116, 125) (15, 45) (453, 42) (169, 387) (94, 127) (91, 271) (17, 228) (483, 315) (279, 489)
r= r= r= r= r= r= r= r= r= r= r= r= r= r	258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275	$\begin{array}{c} & & & (x,y) = \\ & & & ($	$\begin{array}{llllllllllllllllllllllllllllllllllll$
r= r= r= r= r= r= r= r= r= r= r= r= r= r	258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276	$\begin{array}{c} & & & & & & \\ & & & & & & \\ & & & & & $	$\begin{array}{c} (169, 13) \\ (471, 440) \\ (73, 212) \\ (226, 104) \\ (346, 61) \\ (310, 217) \\ (357, 98) \\ (20, 99) \\ (116, 125) \\ (15, 45) \\ (453, 42) \\ (169, 387) \\ (453, 42) \\ (169, 387) \\ (94, 127) \\ (91, 271) \\ (17, 228) \\ (483, 315) \\ (279, 489) \\ (465, 122) \\ (441, 212) \end{array}$
r= r= r= r= r= r= r= r= r= r= r= r= r= r	258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277	$\begin{array}{c} & & & (x,y) = \\ & & & (x,y) = \\ & & & (x,y) = \\ & &$	(169, 13) (471, 440) (73, 212) (226, 104) (346, 61) (310, 217) (357, 98) (20, 99) (116, 125) (15, 45) (453, 42) (169, 387) (94, 127) (91, 271) (17, 228) (485, 315) (279, 489) (465, 122) (461, 212)
r= r= r= r= r= r= r= r= r= r= r= r= r= r	258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278	$\begin{array}{c} & & & & & & \\ & & & & & & \\ & & & & & $	(169, 13) (471, 440) (73, 212) (226, 104) (346, 61) (310, 217) (357, 98) (20, 99) (116, 125) (15, 45) (453, 42) (169, 127) (91, 271) (91, 271) (91, 271) (91, 271) (91, 271) (91, 271) (92, 483, 315) (279, 489) (465, 122) (441, 212) (502, 2) (189, 435)
r= r= r= r= r= r= r= r= r= r= r= r= r= r	258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279	<pre>>>(x, y)= >>>(x, y)= >>>>(x, y)= >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>></pre>	(169, 13) (471, 440) (73, 212) (226, 104) (346, 61) (310, 217) (357, 98) (20, 99) (116, 125) (15, 45) (453, 42) (169, 337) (94, 127) (91, 271) (17, 228) (465, 122) (483, 315) (279, 489) (465, 122) (484, 1212) (502, 2) (189, 435)
r= r= r= r= r= r= r= r= r= r= r= r= r= r	258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 277	$ \begin{array}{c} \\ & \longrightarrow (x, y) = \\ \\ & \longrightarrow (x, y) = \\ \\ & (x, y$	(165, 13) (471, 440) (73, 212) (226, 104) (346, 61) (310, 217) (357, 98) (20, 99) (116, 125) (15, 45) (15, 45) (15, 45) (169, 327) (17, 228) (483, 315) (279, 489) (445, 122) (441, 212) (502, 2) (158, 435) (440, 110) (417, 262)
r= r= r= r= r= r= r= r= r= r= r= r= r= r	258 259 260 261 262 263 264 265 266 267 270 271 272 273 274 275 276 277 278 279 280	$ \begin{array}{c} \\ & \longrightarrow (x, y) = \\ \\ & \longrightarrow (x, y) = \\ & $	(169, 13) (471, 440) (73, 212) (226, 104) (346, 61) (310, 217) (357, 98) (20, 99) (116, 125) (15, 45) (169, 337) (94, 127) (91, 271) (17, 228) (465, 122) (483, 315) (279, 489) (465, 122) (484, 121) (502, 2) (189, 435) (440, 110) (117, 253)
r= r= r= r= r= r= r= r= r= r= r= r= r= r	258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281	$ \begin{array}{c} \\ & \longrightarrow (x, y) = \\ \\ & \longrightarrow (x, y) = \\ & $	(165, 13) (467, 140) (73, 212) (226, 104) (310, 217) (340, 61) (357, 98) (20, 99) (116, 125) (15, 45) (453, 42) (116, 125) (453, 42) (116, 125) (453, 42) (116, 125) (463, 412) (463, 412) (502, 2) (189, 435) (412, 912) (502, 2) (189, 435) (412, 912) (502, 2) (189, 435) (117, 263) (117,
r= r= r= r= r= r= r= r= r= r= r= r= r= r	258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 277 278 277 278 279 280 281 282	$\begin{array}{c} & & & (x,y) = \\ & & & ($	(169, 13) (471, 440) (73, 212) (226, 104) (346, 61) (310, 217) (357, 98) (20, 99) (116, 125) (15, 45) (169, 387) (94, 127) (91, 271) (17, 228) (483, 315) (279, 489) (465, 122) (441, 212) (441, 212) (441, 212) (117, 263) (31, 77) (31, 77)
r= r= r= r= r= r= r= r= r= r= r= r= r= r	258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 277 278 279 280 281 282 283	$\begin{array}{c} \\ & & \\ \\ \\ & & \\ \\ \\ & & \\ \\ \\ & & \\ \\ \\ & \\ \\ \\ & \\ \\ \\ & \\ \\ \\ & \\ \\ \\ & \\ \\ \\ & \\ \\ \\ & \\ \\ \\ & \\ \\ \\ & \\$	(165, 13) (471, 440) (73, 212) (226, 104) (346, 61) (310, 217) (357, 98) (20, 99) (16, 125) (15, 45) (453, 42) (165, 387) (94, 127) (91, 271) (17, 228) (483, 315) (279, 489) (465, 122) (441, 212) (502, 2) (189, 435) (117, 283) (31, 77) (146, 426) (10, 244)
r= r= r= r= r= r= r= r= r= r= r= r= r= r	258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 282 283 284	$\begin{array}{c} \\ & \longrightarrow (x,y) = \\ \\ & \longrightarrow (x,y) = \\ & ($	(169, 13) (471, 440) (73, 212) (226, 104) (346, 61) (310, 217) (357, 98) (20, 99) (116, 125) (15, 45) (169, 387) (94, 127) (91, 271) (17, 228) (483, 315) (279, 489) (441, 212) (502, 2) (188, 435) (440, 110) (117, 263) (31, 77) (146, 426) (108, 181)
r= r= r= r= r= r= r= r= r= r= r= r= r= r	258 259 260 261 262 263 264 265 266 267 270 271 272 273 274 275 276 277 278 277 278 279 280 281 282 283 284 285	$\begin{array}{c} \\ & & \\ \\ & \\ \\ & & \\ \\ & & \\ \\ & & \\ \\ & \\ \\ & & \\ \\ \\ & & \\ \\ & \\ \\ & \\ \\ & \\ \\ & \\ \\ \\ & \\ \\ \\ & \\ \\ \\ & \\ \\ \\ & \\$	(165, 13) (467, 140) (73, 212) (226, 104) (310, 217) (357, 98) (20, 99) (16, 125) (15, 45) (453, 42) (164, 127) (91, 217) (17, 228) (483, 315) (279, 483) (465, 122) (441, 212) (502, 2) (188, 435) (31, 77) (146, 426) (10, 244) (180, 418) (117, 283) (31, 77)
r= r= r= r= r= r= r= r= r= r= r= r= r= r	258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 277 278 279 280 281 282 283 284 285	$\begin{array}{c} \\ & = & (x, y) = \\ & = & (x, y) =$	(169, 13) (471, 440) (73, 212) (226, 104) (346, 61) (310, 217) (357, 98) (20, 99) (116, 125) (15, 45) (169, 387) (169, 387) (169, 387) (169, 387) (17, 228) (483, 315) (279, 489) (465, 122) (483, 315) (279, 489) (412, 212) (502, 2) (188, 435) (440, 110) (117, 263) (31, 77) (146, 426) (10, 244) (158, 181) (50, 491) (571, 379)
r= r= r= r= r= r= r= r= r= r= r= r= r= r	258 259 260 261 262 263 264 265 266 267 270 271 272 273 273 274 275 276 277 278 279 280 281 282 283 284 285 286	$\begin{array}{c} \\ & = & (x, y) = \\ & = & (x, y) =$	(165, 13) (467, 140) (73, 212) (226, 104) (310, 217) (357, 98) (20, 99) (116, 125) (15, 45) (453, 42) (164, 1427) (91, 271) (17, 228) (483, 315) (279, 489) (465, 122) (502, 2) (189, 435) (412, 122) (502, 2) (189, 435) (117, 283) (31, 77) (146, 426) (117, 283) (31, 77) (146, 426) (10, 244) (10, 244) (10, 244) (117, 263) (31, 77) (146, 426) (10, 244) (371, 379) (371, 379)
r= r= r= r= r= r= r= r= r= r= r= r= r= r	258 259 260 261 262 263 264 266 267 268 269 270 271 272 273 274 275 276 277 277 278 279 280 281 282 283 284 285 284 285 286 287	$\begin{array}{c} \\ & & \\ \\ \\ & & \\ \\ \\ & & \\ \\ \\ & & \\ \\ \\ & & \\ \\ \\ & \\ \\ & \\ \\ \\ & \\ \\ \\ & \\ \\ \\ & \\ \\ \\ & \\ \\ \\ & \\ \\ \\ & \\ \\ \\ & \\ \\ \\ \\ \\ \\ & \\$	(169, 13) (467, 440) (73, 212) (226, 104) (310, 217) (346, 61) (357, 98) (20, 99) (116, 125) (15, 45) (453, 42) (169, 387) (169, 387) (169, 387) (17, 228) (483, 315) (277, 489) (465, 122) (484, 212) (502, 2) (189, 435) (444, 212) (502, 2) (188, 161) (10, 244) (10, 243) (10, 244) (10, 244) (10, 244) (10, 244) (10, 244) (10, 244) (10, 217) (271, 199) (27, 49) (27, 49)
r= r= r= r= r= r= r= r= r= r= r= r= r= r	258 259 260 261 262 263 264 265 265 266 267 268 269 270 271 272 273 274 277 273 274 277 278 279 277 278 279 280 281 282 283 284 285 286 287 288 285 286 287 285 286 287 282 285 286 287 280 281 282 283 284 285 285 286 285 270 271 272 275 276 277 277 277 277 277 277 277 277 277	$\begin{array}{c} \\ & & \\ \\ & \\ \\ & & \\ \\ & \\ \\ & \\ \\ & \\ \\ & \\ \\ & \\ \\ \\ & \\ \\ \\ & \\ \\ \\ & \\ \\ \\$	(165, 13) (467, 140) (73, 212) (226, 104) (310, 217) (330, 217) (357, 98) (20, 99) (116, 125) (15, 45) (453, 42) (164, 154) (453, 42) (453, 42) (465, 127) (463, 127) (464, 127) (464, 127) (464, 127) (465, 122) (502, 2) (188, 435) (117, 228) (441, 212) (502, 2) (188, 435) (117, 248) (31, 77) (146, 426) (10, 244) (10, 244) (117, 263) (31, 77) (146, 426) (10, 244) (371, 379) (377, 137) (377, 137)
L= L= L= L= L= L= L= L= L= L= L= L= L= L	2258 259 260 260 262 263 264 265 266 267 268 269 270 271 272 273 274 275 277 278 277 277 278 277 277 278 279 280 281 282 283 284 285 286 287 288 286 287 287 288 286 287 287 287 288 286 287 287 287 288 286 287 287 287 288 286 287 287 288 286 287 288 286 287 288 286 287 288 286 287 277 277 277 277 277 277 277 277 277	$\begin{array}{c} \\ & = &$	(169, 13) (471, 440) (73, 212) (226, 104) (310, 217) (346, 61) (310, 217) (357, 98) (20, 99) (116, 125) (453, 42) (169, 387) (169, 387) (17, 228) (483, 315) (277, 489) (485, 122) (482, 217) (17, 228) (483, 315) (279, 489) (485, 122) (484, 127) (189, 435) (444, 127) (189, 435) (444, 127) (189, 435) (444, 127) (189, 435) (444, 127) (189, 435) (446, 110) (117, 263) (31, 77) (146, 426) (10, 244) (10, 245) (10, 247) (10, 247) (11, 253) (11, 277) (12, 277) (12, 277) (12, 277) (13, 377) (14, 277) (14, 277) (
r= r= r= r= r= r= r= r= r= r= r= r= r= r	2258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 277 278 277 278 277 278 280 281 282 283 284 285 284 285 284 285 284 285 284 285 284 285 284 285 284 285 284 285 284 285 284 285 284 285 284 285 284 285 284 285 284 285 285 285 285 285 285 285 285 285 285	$\begin{array}{c} \\ & = &$	(165, 13) (167, 13) (247, 144) (226, 104) (226, 104) (236, 104) (237, 98) (20, 99) (105, 127) (357, 98) (20, 99) (20, 99) (216, 125) (15, 45) (453, 42) (165, 387) (94, 127) (91, 271) (17, 228) (483, 315) (279, 489) (483, 315) (279, 489) (483, 122) (502, 2) (188, 435) (177, 288) (441, 212) (502, 2) (188, 435) (177, 489) (417, 212) (504, 412) (177, 213) (31, 77) (146, 426) (10, 244) (371, 379) (271, 199) (87, 46) (288, 371) (403, 171)
r= r= r= r= r= r= r= r= r= r= r= r= r= r	2258 2259 2260 261 262 263 264 265 266 267 270 271 277 277 277 277 277 277 277 277 277	$\begin{array}{c} \\ & = & (x, y) = \\ & = & (x, y) =$	(165, 13) (471, 440) (73, 212) (226, 104) (346, 61) (340, 217) (357, 98) (20, 99) (116, 125) (453, 42) (165, 357) (453, 42) (165, 357) (445, 42) (165, 357) (47, 228) (483, 315) (277, 489) (485, 122) (441, 212) (502, 2) (189, 435) (440, 110) (117, 263) (31, 77) (146, 426) (10, 244) (186, 181) (50, 491) (371, 379) (271, 199) (271, 199) (271, 199) (271, 167) (375, 467)
L= L= L= L= L= L= L= L= L= L= L= L= L= L	2258 2259 260 261 262 263 264 265 266 267 268 270 271 272 273 274 2775 277 277 277 277 277 277 277 277 27	$\begin{array}{c} \\ & = & (x, y) = \\ & = & (x, y) =$	(165, 13) (167, 13) (471, 440) (346, 61) (326, 104) (346, 61) (310, 217) (357, 98) (20, 99) (116, 125) (15, 45) (453, 42) (165, 387) (94, 127) (91, 271) (17, 228) (483, 315) (279, 489) (483, 315) (279, 489) (483, 122) (502, 2) (188, 435) (117, 228) (441, 212) (502, 2) (188, 435) (117, 288) (31, 77) (146, 422) (31, 77) (146, 428) (31, 77) (146, 428) (31, 77) (146, 428) (31, 77) (146, 428) (371, 379) (271, 199) (87, 46) (288, 371) (375, 467) (175, 238)
r= r= r= r= r= r= r= r= r= r= r= r= r= r	2258 2259 2260 261 262 263 264 265 266 267 270 271 272 273 274 2772 2773 2774 2775 2776 2777 2778 2779 2830 283 284 285 283 284 285 286 287 283 284 285 285 286 287 285 286 287 285 286 287 285 286 287 285 286 287 285 286 287 285 286 287 285 286 287 287 287 287 287 287 287 287 287 287	$\begin{array}{c} \\ & = & (x, y) = \\ & = & (x, y) =$	(165, 13) (471, 440) (73, 212) (226, 104) (236, 61) (310, 217) (357, 98) (20, 99) (116, 125) (15, 45) (453, 42) (165, 337) (94, 127) (17, 228) (465, 315) (27, 483) (41, 212) (502, 2) (189, 435) (441, 122) (502, 2) (10, 244) (10, 244) (10, 244) (10, 244) (10, 245) (10, 244) (10, 245) (10, 244) (10, 245) (10, 246) (10, 247) (10, 247) (10, 247) (10, 247) (10, 247) (10, 247) (117, 228) (11, 127) (117, 128) (11, 127) (117, 128) (11, 127) (117, 128) (11, 127) (117, 128) (117, 127) (117, 128) (117, 127) (117, 128) (117, 127) (117, 128) (117, 127) (117, 128) (117, 128) (11
L= L= L= L= L= L= L= L= L= L= L= L= L= L	2258 2259 2260 2261 2262 2263 2264 2265 2267 2267 2271 2772 2773 2774 2775 2776 2777 2778 2779 280 281 282 283 284 285 288 288 288 288 288 288 288 288 288	$\begin{array}{c} \\ & = & (x, y) = \\ & = & (x, y) =$	(166, 13) (167, 13) (471, 440) (346, 61) (326, 104) (346, 61) (310, 217) (357, 98) (20, 99) (116, 125) (15, 45) (453, 42) (453, 42) (453, 42) (445, 142) (445, 142) (445, 142) (445, 142) (445, 142) (445, 142) (445, 142) (445, 142) (445, 142) (445, 142) (502, 2) (148, 435) (117, 228) (311, 77) (146, 122) (314, 77) (146, 124) (314, 77) (146, 124) (314, 77) (146, 143) (314, 77) (146, 144) (371, 379) (271, 199) (87, 46) (288, 371) (375, 376) (271, 197) (375, 467) (175, 238) (276, 381) (276, 381) (276, 381) (276, 381) (278, 371)
L= L= L= L= L= L= L= L= L= L= L= L= L= L	2258 2259 2260 261 262 263 264 265 266 267 270 277 277 277 277 277 277 277 277 27	$\begin{array}{c} \\ & = & (x, y) = \\ & = & (x, y) =$	(165, 13) (471, 440) (73, 212) (226, 104) (236, 61) (340, 61) (357, 98) (20, 99) (116, 125) (15, 45) (15, 45) (15, 45) (165, 337) (94, 127) (17, 228) (483, 315) (27, 48) (412, 217) (427, 483) (441, 212) (502, 2) (189, 435) (441, 212) (189, 435) (441, 212) (10, 244) (10, 24
L= L= L= L= L= L= L= L= L= L= L= L= L= L	2588 2609 2611 2622 263 2644 2655 2666 2677 2688 2699 2700 2711 2772 2773 2774 2775 2776 2776 2777 2779 2800 2812 2742 2779 2800 2812 2742 2779 2800 2812 2742 2779 2800 2812 2829 2829 2829 2829 2829 2829 2829	$\begin{array}{c} \\ & = & (x, y) = \\ & = & (x, y) =$	(166, 13) (167, 13) (471, 440) (346, 61) (326, 104) (346, 61) (310, 217) (357, 98) (20, 99) (116, 125) (15, 45) (453, 42) (453, 42) (412, 212) (502, 2) (443, 315) (432, 312) (444, 212) (502, 2) (444, 212) (502, 2) (444, 212) (502, 2) (443, 315) (435, 412) (435, 422) (441, 212) (502, 2) (443, 315) (172, 288) (311, 72) (172, 288) (311, 72) (371, 379) (371, 379) (271, 199) (47, 46) (371, 379) (271, 197) (401, 167) (375, 367) (402, 117) (401, 167) (375, 367) (402, 117) (401, 167) (375, 361) (402, 117) (403, 167) (375, 361) (403, 196) (480, 206)
L= L= L= L= L= L= L= L= L= L= L= L= L= L	2258 2259 260 261 262 263 264 265 266 267 270 271 272 273 274 275 276 277 2778 277 2778 277 2778 277 2778 277 277	$\begin{array}{c} \\ & &$	(165, 13) (471, 440) (73, 212) (226, 104) (236, 61) (310, 217) (357, 98) (20, 99) (116, 125) (15, 45) (15, 45) (15, 45) (15, 45) (165, 327) (445, 422) (169, 327) (17, 228) (448, 315) (441, 212) (502, 2) (189, 435) (444, 212) (502, 2) (189, 435) (444, 212) (502, 2) (189, 435) (444, 212) (502, 2) (189, 435) (444, 212) (502, 2) (189, 435) (441, 212) (502, 2) (189, 435) (441, 212) (502, 2) (189, 435) (441, 212) (503, 491) (317, 71) (317, 71) (316, 426) (317, 71) (317, 467) (317, 467) (375, 467) (175, 238) (380, 487) (480, 195)
L= L= L= L= L= L= L= L= L= L= L= L= L= L	2258 2259 260 261 262 263 264 265 266 267 268 267 270 277 277 277 277 277 277 277 277 27	$\begin{array}{c} \\ & &$	(166, 13) (167, 140) (73, 212) (226, 104) (346, 61) (310, 217) (357, 98) (20, 99) (116, 125) (15, 45) (453, 42) (453, 42) (412, 127) (91, 271) (17, 228) (443, 315) (279, 489) (465, 122) (441, 212) (502, 2) (441, 212) (502, 2) (443, 315) (445, 122) (441, 212) (502, 2) (148, 435) (117, 238) (417, 128) (437, 137) (271, 199) (87, 46) (271, 199) (87, 46) (273, 374) (271, 197) (401, 167) (375, 374) (402, 1167) (375, 374) (403, 196) (480, 205) (480, 205) (480, 205) (480, 205) (480, 205)
L= L= L= L= L= L= L= L= L= L= L= L= L= L	2258 2559 260 261 262 263 264 265 266 267 268 266 267 271 272 273 2774 2773 2774 2775 2776 2777 2788 2779 280 281 282 283 284 285 288 288 288 288 288 288 288 288 288	$ \begin{array}{c} \\ & = & (x, y) = \\ & = & (x, y) $	(165, 13) (467, 140) (73, 212) (226, 104) (236, 61) (310, 217) (357, 98) (20, 99) (116, 125) (15, 45) (15, 45) (15, 45) (169, 327) (17, 228) (483, 315) (483, 315) (441, 212) (502, 2) (189, 435) (441, 212) (502, 2) (189, 435) (417, 263) (317, 379) (271, 199) (371, 379) (271, 199) (371, 467) (175, 238) (380, 487) (430, 195) (334, 472) (435, 195) (334, 472) (435, 195) (334, 472) (435, 195) (334, 472) (435, 195) (334, 472) (335, 487) (334, 472) (336, 487) (334, 472) (336, 487) (334, 415) (334, 415) (33

r= 300	====>(x,y)=	(342,	28)	r= 368	<pre>8 ====>(x,y)=</pre>	(478, 18)	r=	436 ====>(x,y):	= (350, 117)
r= 301	====>(x,v)=	(488.	190)	r= 369) ====>(x, y)=	(271, 91)	r=	437 ====>(x, y)	= (352, 259)
r = 302	====>(x, y)=	(229	220)	r = 370) ====>(x y)=	(110 495)	r=	438 ====>(x y);	= (382 441)
n= 202	>(x,y)	(104	226)	x= 271	>(x,y)	(245 412)		420 ====>(x,y)	- (258 01)
1- 303	>(x,y)-	(10-1,	220)	- 270	·> (x, y)-	(14 004)	1-	400> (x, y)	- (200, 31)
r= 304	>(x,y)=	(02,	390)	r= 3/2	=====>(x,y)=	(14, 224)	r=	440 ====>(x,y)	= (60, 476)
r= 305	=====>(x,y)=	(328,	265)	r= 373	3 ====>(x,y)=	(460, 153)	r=	441 ====>(x,y)	= (258, 199)
r= 306	====>(x,y)=	(404,	176)	r= 374	L ====⇒(x,y)=	(164, 185)	r=	442 ====>(x,y):	= (216, 139)
r= 307	====>(x,y)=	(487,	229)	r= 375	5 ====>(x,y)=	(337, 196)	r=	443 ====>(x,y):	= (51, 310)
r= 308	====>(x,y)=	(475,	25)	r= 376	S ====>(x,y)=	(337, 290)	r=	444 ====>(x,y):	= (232, 304)
r= 309	====>(x,v)=	(263.	117)	r= 377	' ====>(x, y)=	(357, 77)	r=	445 ====>(x,v)	= (472, 405)
r = 310	====>(x, y)=	(225	268)	r = 378	====>(x y)=	(324 93)	r=	446 ====>(x y)	= (378 13)
n= 211	>(x,y)	(16	97)	x= 270	(x, y) = ((062 /2)		447 ====>(x,y)	= (297, 264)
1= 311	>(x,y)-	(40,	(01)	1= 313	,>(x,y)-	(203, 43)	1-	447>(x,y)	- (287, 304)
r= 312	=====>(x,y)=	(132,	124)	r= 380) ====>(x,y)=	(196, 337)	r=	448 ====>(x,y)	= (185, 164)
r= 313	====>(x,y)=	(36,	128)	r= 381	====>(x,y)=	(490, 334)	r=	449 ====>(x,y):	= (393, 8)
r= 314	====>(x,y)=	(104,	69)	r= 382	2 ====>(x,y)=	(38, 235)	r=	450 ====>(x,y):	= (495, 110)
r= 315	====>(x,y)=	(186,	239)	r= 383	8 ====>(x,y)=	(125, 116)	r=	451 ====>(x,y):	= (213, 166)
r= 316	====>(x,v)=	(466.	189)	r= 384	=====>(x,v)=	(212, 441)	r=	452 ====>(x, y)	= (442, 330)
r = 317	====>(x, y)=	(290	403)	r= 385	====>(x y)=	(493 369)	r=	453 ====>(x y);	= (220 380)
x= 210	>(x,y)	(00	260)	x= 200	>(x,y)	(167, 142)		4E4 ====>(x,y)	- (227, 60)
1= 310	>(x,y)-	(90,	357)	1= 300	(x,y)-	(107, 143)	1-	454>(X,y)	- (237, 09)
r= 319	=====>(x,y)=	(384,	222)	r= 387	====>(x,y)=	(305, 376)	r=	455 ====>(x,y)	= (318, 339)
r= 320	====>(x,y)=	(128,	14)	r= 388	8 ====>(x,y)=	(369, 493)	r=	456 ====>(x,y):	= (153, 460)
r= 321	====>(x,y)=	(362,	288)	r= 389) ====>(x,y)=	(250, 401)	r=	457 ====>(x,y):	= (259, 352)
r= 322	====>(x,y)=	(199,	258)	r= 390) ====>(x,y)=	(135, 361)	r=	458 ====>(x,y):	= (470, 330)
r= 323	====>(x,v)=	(338.	466)	r= 391	====>(x,v)=	(289, 486)	r=	459 is not in the	e set of definition
r = 324	====>(x, y)=	(281.	119)	r= 392	P ====>(x y)=	(291 430)	r=	460 ====>(x y)	(86 51)
r = 325	===>(x,y)	(67	458)	r = 303	$(x,y) = \sum_{x \in Y} (x,y) = \sum_$	(148 214)	r=	461 ====>(x,y)	= (63, 32)
n= 206	>(x,y)-	(00)	175)	n= 20/	(x, y) = (x, y) = (x, y)	(10, 452)	1-	460 ====>(x,y)	= (00, 02) = (016 057)
I= 320	>(x,y)=	(298,	1/5)	r= 394	= ====>(x,y)=	(12, 455)	r=	462 ====>(x,y)	= (410, 407)
r= 327	====>(x,y)=	(88,	81)	r= 395	====>(x,y)=	(403, 290)	r=	463 ====>(x,y)	= (378, 387)
r= 328	====>(x,y)=	(333,	427)	r= 396	5 ====>(x,y)=	(443, 27)	r=	464 ====>(x,y):	= (124, 141)
r= 329	====>(x,y)=	(264,	317)	r= 397	′ ====>(x,y)=	(442, 157)	r=	465 ====>(x,y):	= (338, 435)
r= 330	====>(x,y)=	(476,	60)	r= 398	8 ====>(x,y)=	(69, 237)	r=	466 ====>(x,y):	= (490, 125)
r= 331	====>(x,y)=	(217,	86)	r= 399	====>(x,y)=	(342, 18)	r=	467 ====>(x,y):	= (382, 73)
r = 332	====>(x, y)=	(381	38)	r = 400) ====>(x y)=	(73 382)	r=	468 ====>(x y);	= (43 350)
r= 333	===>(x,y)	(463	118)	r = 401	====>(x, y)=	(8 303)		469 ====>(x, y);	= (31 98)
- 224	>(x,y)-	(405,	1(1)	1- 401	·> (x, y)-	(005 100)	1-	400> (x, y)	- (426 212)
r= 334	>(x,y)=	(405,	161)	r= 402	=====>(x,y)=	(225, 122)	r=	470 ====>(x,y)	= (436, 313)
r= 335	====>(x,y)=	(502,	252)	r= 403	3 ====>(x,y)=	(475, 161)	r=	471 ====>(x,y)	= (187, 49)
r= 336	====>(x,y)=	(272,	294)	r= 404	↓ ====>(x,y)=	(190, 488)	r=	472 ====>(x,y):	= (171, 12)
r= 337	====>(x,y)=	(307,	166)	r= 405	5 ====>(x,y)=	(485, 25)	r=	473 ====>(x,y):	= (217, 310)
r= 338	====>(x,y)=	(316,	349)	r= 406	6 ====>(x,y)=	(410, 179)	r=	474 ====>(x,y):	= (170, 76)
r= 339	====>(x,y)=	(275.	355)	r= 407	' ====>(x, y)=	(18, 342)	r=	475 ====>(x,y)	= (318, 46)
r = 340	====>(x, y)=	(376	305)	r = 408	====>(x y)=	(173 33)	r=	476 ====>(x y)	= (461 50)
n= 2/1	>(x,y)	(411	200)	x= 400	(x, y) = ((200, 100)		477 ====>(x,y)	- (40, 400)
1= 341	>(x,y)-	(411,	390)	1= 403	,>(x,y)-	(322, 192)	1-	477>(X,y)	- (40, 422)
r= 342	=====>(x,y)=	(215,	132)	r= 410) ====>(x,y)=	(304, 245)	r=	478 ====>(x,y)	= (121, 62)
r= 343	====>(x,y)=	(435,	338)	r= 411	====>(x,y)=	(350, 43)	r=	479 ====>(x,y)	= (368, 142)
r= 344	====>(x,y)=	(51,	86)	r= 412	2 ====>(x,y)=	(360, 253)	r=	480 ====>(x,y):	= (176, 404)
r= 345	====>(x,y)=	(224,	36)	r= 413	8 ====>(x,y)=	(440, 471)	r=	481 ====>(x,y):	= (386, 153)
r= 346	====>(x,y)=	(143,	250)	r= 414	====>(x,y)=	(458, 67)	r=	482 ====>(x,y):	= (25, 485)
r= 347	====>(x,v)=	(213.	100)	r= 415	5 ====>(x,v)=	(301, 409)	r=	483 ====>(x.v)	= (480, 265)
r = 348	====>(x, y)=	(240	386)	r = 416	====>(x y)=	(311 181)	r=	484 ====>(x y);	= (411 365)
r= 349	====>(x,y)=	(78	454)	r= 417	(x, y)=	(334 490)	r=	485 ====>(* *)	= (327 188)
1= 349	>(x,y)-	(10,	404)	1- 417	>(x,y)-	(334, 450)	1-	400>(X,y)	- (327, 188)
r= 350	>(x,y)=	(0/,	(600)	r= 416	>(x,y)=	(121, 94)	r=	400 ====>(X, y):	- (203, 123)
r= 351	====>(x,y)=	(189,	466)	r= 419) ====>(x,y)=	(470, 157)	r=	487 ====>(x,y):	= (352, 369)
r= 352	====>(x,y)=	(202,	198)	r= 420) ====>(x,y)=	(141, 215)	r=	488 ====>(x,y):	= (77, 31)
r= 353	====>(x,y)=	(198,	202)	r= 421	====>(x,y)=	(495, 471)	r=	489 ====>(x,y):	= (315, 483)
r= 354	====>(x,y)=	(460,	240)	r= 422	2 ====>(x,y)=	(16, 123)	r=	490 ====>(x,y):	= (328, 205)
r= 355	====>(x,v)=	(394.	354)	r= 423	3 ====>(x,y)=	(457, 416)	r=	491 ====>(x,v)	= (330, 470)
r= 356	====>(x y)=	(465	268)	r= 424	(x y)=	(466 338)	r=	492 ====>(x y)	= (125 490)
r= 257	- (x,y)=	(157	442)	- 125	· (x, y)=	(235, 279)		403 ====>(x,y)	= (415 385)
1- 357	>(x,y)=	(007	112/	1 420	>(x,y)=	(140, 100)	r=	404>(x,y)	- (401 220)
r= 358	>(x,y)=	(237,	220)	r= 426	>(x,y)=	(149, 109)	r=	494 ====>(x,y)	= (491, 332)
r= 359	====>(x,y)=	(28,	478)	r= 427	====>(x,y)=	(252, 502)	r=	495 ====>(x,y):	= (311, 239)
r= 360	====>(x,y)=	(315,	176)	r= 428	8 ====>(x,y)=	(116, 334)	r=	496 ====>(x,y):	= (42, 171)
r= 361	====>(x,y)=	(493,	259)	r= 429) ====>(x,y)=	(379, 362)	r=	497 ====>(x,y):	= (23, 298)
r= 362	====>(x,y)=	(409,	301)	r= 430) ====>(x,y)=	(231, 209)	r=	498 ====>(x,v)	= (307, 100)
r= 363	====>(x,v)=	(489.	279)	r= 431	====>(x,v)=	(339, 318)	r=	499 ====>(x.v)	= (212, 73)
r = 364	====>(x,v)=	(404	483)	r= 432	(x, v)=	(425, 154)	r=	500 ====>(x y)	= (283, 274)
r= 365	====>(x,y)=	(467	279)	r= 499	$(x,y)^{-}$	(467 375)		501 ====>(x, y)	= (386, 240)
1- 305	>(x,y)=	(407,	100)	1 400	,(x,y)=	(100, 220)	r=	500>(x,y)	- (000, 240)
r= 366	>(x,y)=	(435,	103)	r= 434	=====>(x,y)=	(102, 336)	r=	502 ====>(x,y)	= (441, 382)
r= 367	====>(x,y)=	(151,	134)	r= 435	, ====>(x,y)=	(109, 149)			

References

- Bernstein, D.J., Hamburg, M., Krasnova, A., Lange, T.: Elligator: elliptic-curve points indistinguishable from uniform random strings. In: Gligor, V., Yung, M. (eds.) ACM CCS (2013)
- Billet, O., Joye, M.: The Jacobi model of an elliptic curve and side-channel analysis. In: Fossorier, M., Høholdt, T., Poli, A. (eds.) AAECC 2003. LNCS, vol. 2643, pp. 34–42. Springer, Heidelberg (2003). https://doi.org/10.1007/3-540-44828-4_5

- Boneh, D., Franklin, M.: Identity-based encryption from the weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-44647-8_13
- Chudnovsky, D.V., Chudnovsky, G.V.: Sequences of numbers generated by addition in formal groups and new primality and factorization tests. Adv. Appl. Math. 7(4), 385–434 (1986)
- Devigne, J., Joye, M.: Binary huff curves. In: Kiayias, A. (ed.) CT-RSA 2011. LNCS, vol. 6558, pp. 340–355. Springer, Heidelberg (2011). https://doi.org/10. 1007/978-3-642-19074-2_22
- Diao, O., Fouotsa, E.: Arithmetic of the level four theta model of elliptic curves. Afrika Mathematica 26(3), 283–301 (2015)
- Edwards, H.M.: A normal form for elliptic curves. Bull. Am. Math. Soc. 44, 393–422 (2007). http://www.ams.org/bull/2007-44-03/S0273-0979-07-01153-6/home. html
- Diarra, N., Sow, D., Ould Cheikh Khlil, A.Y.: On indifferentiable deterministic hashing into elliptic curves. Eur. J. Pure Appl. Math. 10(2), 363–391 (2017). (MathScinet: MR3607082) (ZentralBlattMath: Zbl 06701281)
- Fouotsa, E., Diao, O.: A theta model for elliptic curves. Mediterr. J. Math. 14, 65 (2017). https://doi.org/10.1007/s00009-017-0840-y
- Farashahi, R.R.: Hashing into Hessian curves. In: Nitaj, A., Pointcheval, D. (eds.) AFRICACRYPT 2011. LNCS, vol. 6737, pp. 278–289. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-21969-6_17
- Farashahi, R.R., Fouque, P.-A., Shparlinski, I.E., Tibouchi, M., Voloch, J.F.: Indifferentiable deterministic hashing to elliptic and hyperelliptic curves. Math. Comput. 82(281), 491–512 (2013)
- Fouque, P.-A., Tibouchi, M.: Estimating the size of the image of deterministic hash functions to elliptic curves. In: Abdalla, M., Barreto, P.S.L.M. (eds.) LATIN-CRYPT 2010. LNCS, vol. 6212, pp. 81–91. Springer, Heidelberg (2010). https:// doi.org/10.1007/978-3-642-14712-8_5
- Icart, T.: How to hash into elliptic curves. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 303–316. Springer, Heidelberg (2009). https://doi.org/10. 1007/978-3-642-03356-8_18
- Smart, N.P.: The Hessian form of an elliptic curve. In: Koç, Ç.K., Naccache, D., Paar, C. (eds.) CHES 2001. LNCS, vol. 2162, pp. 118–125. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-44709-1_11
- Shallue, A., van de Woestijne, C.E.: Construction of rational points on elliptic curves over finite fields. In: Hess, F., Pauli, S., Pohst, M. (eds.) ANTS 2006. LNCS, vol. 4076, pp. 510–524. Springer, Heidelberg (2006). https://doi.org/10. 1007/11792086_36
- 16. Washington, L.C.: Elliptic Curves. Number Theory and Cryptography. Discrete Mathematics and Applications. Chapman and Hall, Boca Raton (2008)