Processamento Paralelo

AULA 3A

Programa para Paralelização Algoritmo Pollard Rho

Professor: Luiz Augusto Laranjeira
luiz.laranjeira@gmail.com

Agenda

- Rápido Apanhado sobre Curvas Elípticas
- Criptografia de Curvas Elípticas
- Criptoanálise – Algoritmo Pollard Rho
- Programa – Algoritmo Pollard Rho

Motivation

Elliptic Curves Over Real Numbers

Ellipitic Curves over Real Numbers

- Elliptic curves are not ellipses. They are so named because they are described by cubic equations, such as those used to calculate the circumference of an ellipse:

$$y^2 + axy + by = x^3 + cx^2 + dx + e$$

- For our purposes we can limit ourselves to equations of the form: (these equations are said to be cubic, or of degree 3)

$$y^2 = x^3 + ax + b \qquad or \qquad y = \sqrt{x^3 + ax + b}$$

- So, this curve is symmetric about the x axis, y = 0.

Ellipitic Curves over Real Numbers

- An elliptic curve is said to have a *point at infinity* or the *zero point,* denoted *O*.

- The elliptic curve is the set of points E(*a*, *b*) composed of all the points (*x*, *y*) that satisfy the equation

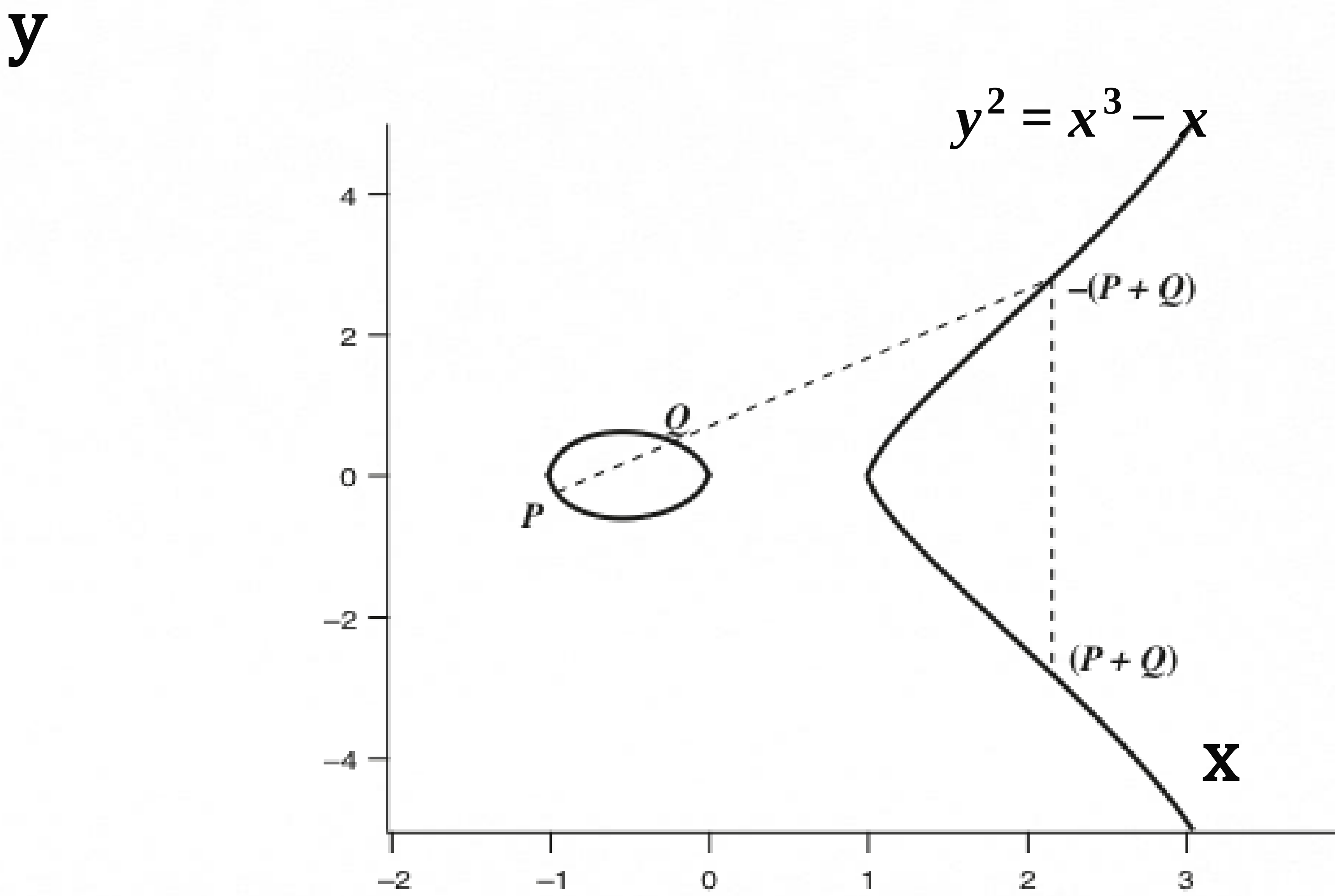
$$y^2 = x^3 + ax + b$$

- It can be shown that a group can be defined based on the set E(*a*, *b*), for specific values of *a* and *b* if:

$$4a^3 + 27b^2 \neq 0$$

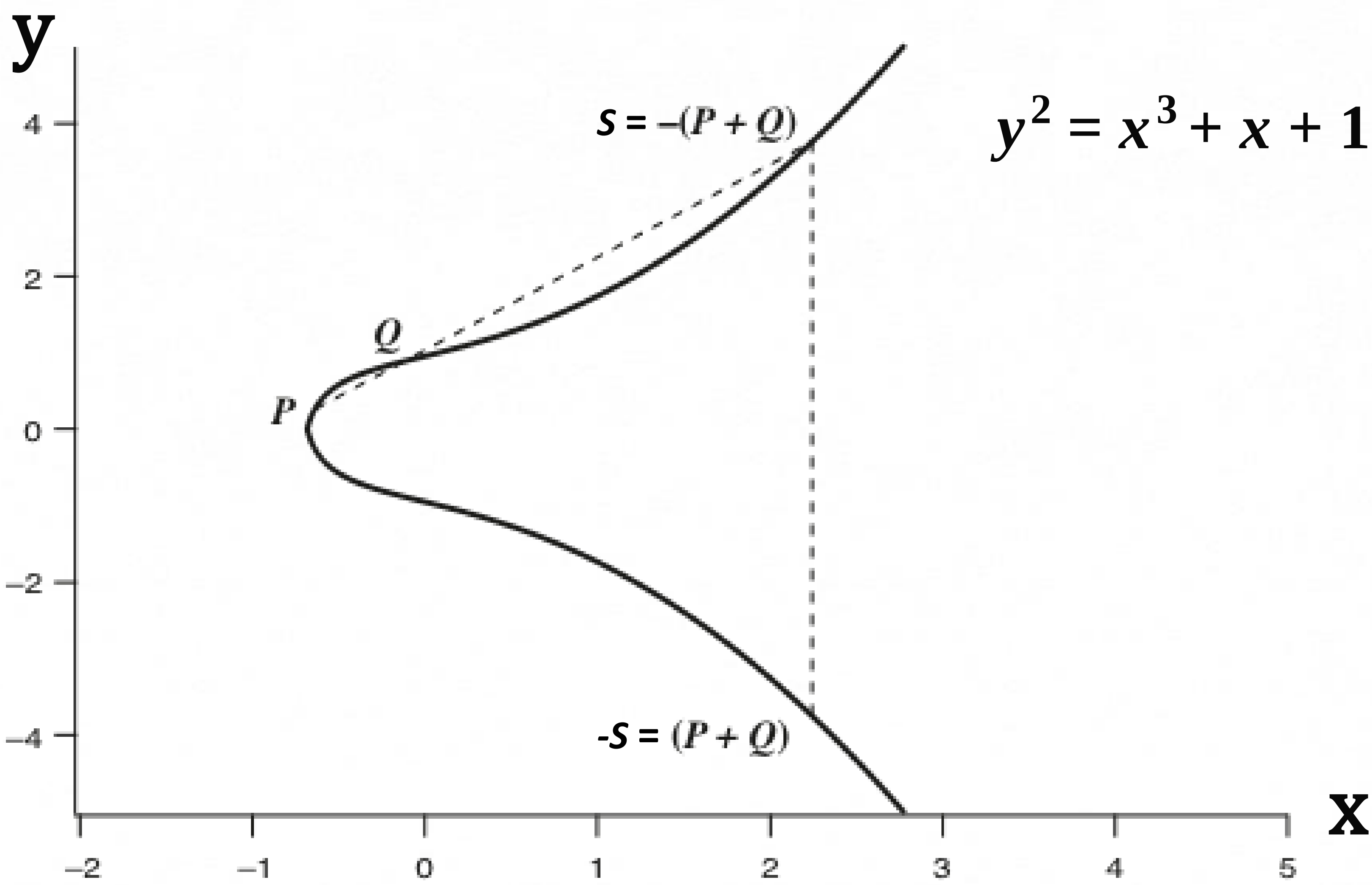
Ellipitic Curves over Real Numbers

E(-1, 0)   a = -1, b = 0



Elliptic Curves over Real Numbers

E(1, 1)   a = 1, b = 1



(b) $y^2 = x^3 + x + 1$

Geometric Description of Addtion

If three points on an elliptic curve lie on a straight line, their sum is O. From this the following rules result:

1. O is the additive identity → $O = -O$ For any point P on the elliptic curve, $P + O = P$.

2. The negative of a point $P = (x, y)$ is the point $-P$ with coordinates $-P = (x, -y)$. These two points can be joined by a vertical line.

3. Given two points P e Q, $P \neq Q$, a straight between them finds a third (unique) point S such that $S = -(P + Q)$.

4. To double a point P, draw the tangent line and find the point of intersection S. Then $P + P = 2P = -S$.

Geometric Description of Addtion

$$S + (P + Q) = O \quad \rightarrow \quad S = -(P + Q)$$

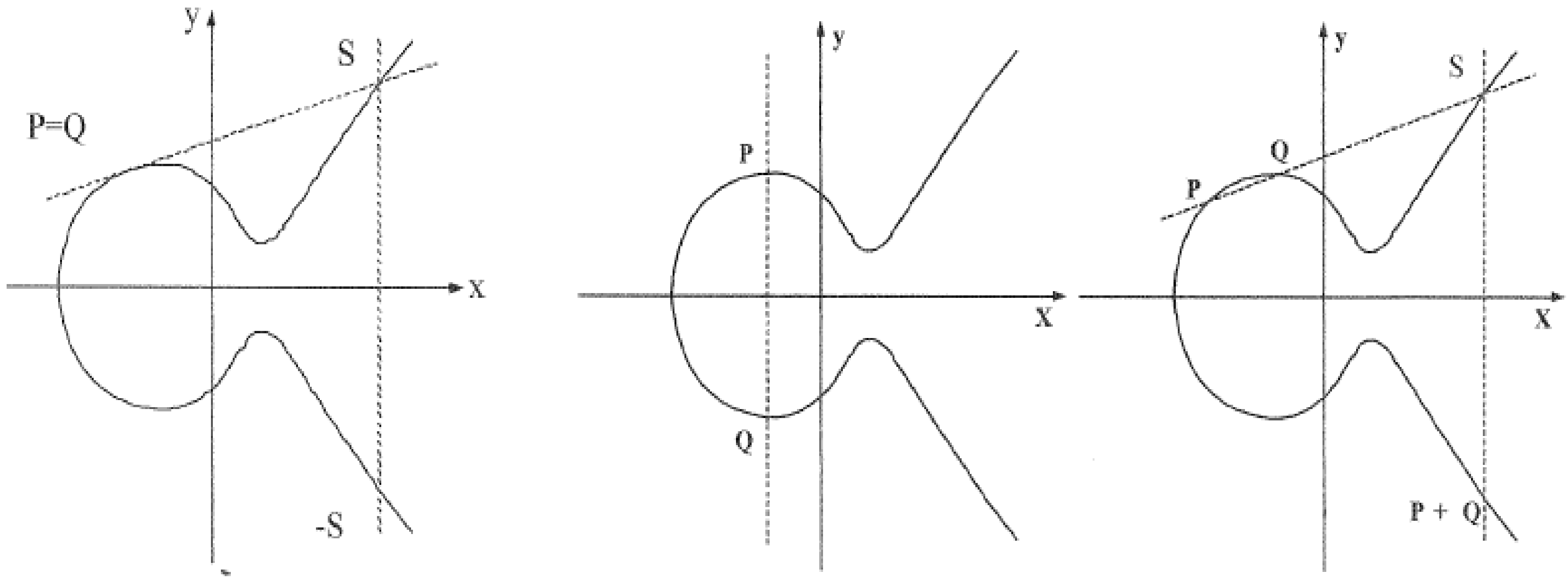


Figure 1 Figure 2 Figure 3.

$P = Q \;\rightarrow\; S = -2P$

$-S = 2P$

$P = -Q \;\rightarrow (P + Q) = O$

connecting line is vertical,

S is in the infinite: $S = O$

$P \neq Q,\ P \neq -Q$

$-S = (P + Q)$

Algebraic Description of Addition

- Given two distinct points $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$, $P \neq -Q$, the slope of the line that joins them is given by:

$$\Delta = \frac{(y_Q - y_P)}{(x_Q - x_P)}$$

- There is exactly one point where this line intercepts the elliptic curve, $S = -(P + Q)$. After some manipulation we get the sum of these two points $R = P + Q$ as:

$$x_R = \Delta^2 - x_P - x_Q$$

$$y_R = -y_P + \Delta(x_P - x_R)$$

Algebraic Description of Addition

- We also need to add a point to itself: *P + P = 2P = R*.
  For $y_P \neq 0$ the expressions are:

$$x_R = \left(\frac{3{x_P}^2 + a}{2y_P}\right)^2 - 2x_P$$

$$y_R = \left(\frac{3{x_P}^2 + a}{2y_P}\right)^2 * (x_P - x_R) - y_P$$

Elliptic Curves of Interest

- Elliptic curve cryptography uses curves whose variables and coefficients are elements of a finite field.
- There is no geometric interpretation for such curves.
- Two families of elliptic curves are used in cryptographic applications:

Prime curves over Z_p

- **Use a cubic equation in which the variables and coefficients all take on values in the set of integers from 0 through $p - 1$ and in which calculations are performed modulo p.**
- **Best for software applications.**

Binary curves over $GF(2^m)$

- Variables and coefficients all take on values in $GF(2^m)$ and calculations are performed over $GF(2^m)$.
- Best for hardware applications: a lot of bit-fiddling, but a powerful cryptosystem can be created with few logic gates.

Elliptic Curves Over Z_p

$Z_p = \{ 0, 1, 2, 3, 4, 5, \ldots, p-1, p-2, p-1 \}$

Elliptic Curves Over Z_p

- Coefficients and variables $\in$ Z_p, arithmetic modulo *p*.
- The algebraic interpretation used for elliptic curve arithmetic over real numbers does carry readily over.
- The elliptic curve is the set of points $E_p(a, b)$ composed of all the points (x, y) that satisfy the equation

$$y^2 \bmod p = (x^3 + ax + b) \bmod p$$

- It can be shown that a group can be defined based on the set $E_p(a, b)$, for specific values of *a* and *b* if:

$$(4a^3 + 27b^2) \bmod p \neq 0 \bmod p$$

Points (other than O) on the Elliptic Curve $E_{23}(1, 1)$

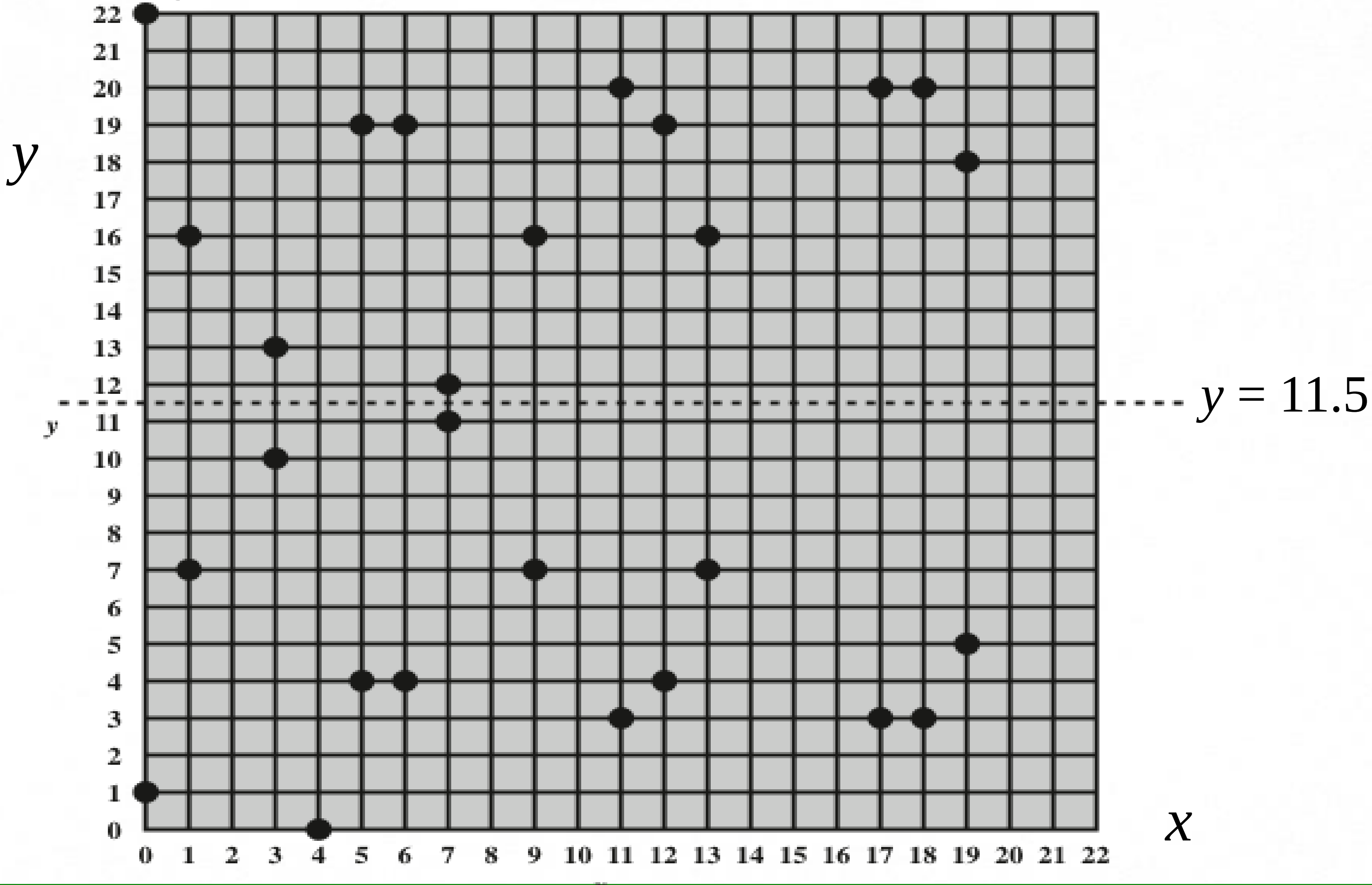
$$y^2 = x^3 + x + 1 \qquad p = 23 \qquad a = b = 1$$

(0, 1)	(6, 4)	(12, 19)
(0, 22)	(6, 19)	(13, 7)
(1, 7)	(7, 11)	(13, 16)
(1, 16)	(7, 12)	(17, 3)
(3, 10)	(9, 7)	(17, 20)
(3, 13)	(9, 16)	(18, 3)
(4, 0)	(11, 3)	(18, 20)
(5, 4)	(11, 20)	(19, 5)
(5, 19)	(12, 4)	(19, 18)

All points on the Elliptic Curve $E_{23}(1, 1)$: 27 points

The Elliptic Curve $E_{23}(1, 1)$

$y^2 = x^3 + x + 1 \qquad p = 23 \qquad a = b = 1$



Rules for Addtion in $E_p(a, b)$

1. $P + O = P$
2. If $P = (x_P, y_P)$, then $-P = (x_P, -y_P)$ and $P - P = O$
3. Given two points $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$, $P \neq -Q$, $P \neq Q$, the sum of these two points $R = P + Q$ is given by:

$$x_R = (\lambda^2 - x_P - x_Q) \bmod p \qquad \lambda = \frac{(y_Q - y_P)}{(x_Q - x_P)} \, mod\ p$$

$$y_R = (\lambda(x_P - x_R) - y_P) \bmod p$$

4. If $P = (x_P, y_P)$, then $R = 2P$ $\quad \lambda = \left(\frac{3{x_P}^2 + a}{2y_P}\right) mod\ p$

   $R = (x_R, y_R)$, as above

5. Multiplication is defined as repeated addition, example:

   $4P = P + P + P + P$

Examples: Addtion in $E_{23}(1, 1)$
$$y^2 = x^3 + x + 1$$

1. $P = (3, 10)$, $Q = (9, 7)$ $\quad P + Q = (x_R, y_R) = ?$

$$\lambda = \left(\frac{7-10}{9-3}\right) \bmod 23 = \left(\frac{-3}{6}\right) \bmod 23 = \left(\frac{-1}{2}\right) \bmod 23 = 11$$
$$x_R = (11^2 - 3 - 9) \bmod 23 = 109 \bmod 23 = 17$$
$$y_R = (11(3 - 17) - 10) \bmod 23 = -164 \bmod 23 = 20$$

$P + Q = (17, 20)$

multiplicative inverses used to perform division in Z_p:
$$y = \frac{1}{x} \quad \text{if} \quad xy = 1 \pmod{p}$$

2. $2P = (x_R, y_R) = ?$

$$\lambda = \left(\frac{3(3^2) + 1}{2 \times 10}\right) \bmod 23 = \left(\frac{5}{20}\right) \bmod 23 = \left(\frac{1}{4}\right) \bmod 23 = 6$$
$$x_R = (6^2 - 3 - 3) \bmod 23 = 30 \bmod 23 = 7$$
$$y_R = (6(3 - 7) - 10) \bmod 23 = (-34) \bmod 23 = 12$$

$2P = (7, 12)$

Agenda

- Rápido Apanhado sobre Curvas Elípticas
- Criptografia de Curvas Elípticas
- Criptoanálise – Algoritmo Pollard Rho
- Programa – Algoritmo Pollard Rho

ECC Encryption/Decryption

- Several approaches using elliptic curves have been analyzed.
- Must first embed a message character or number m as a point $P_m = (x, y)$ on the elliptic curve.
- What gets encrypted is the point P_m.
- The encryption operation corresponds to a mapping of the point P_m to the ciphertext C_m, which comprehends two points on the curve.
- The decryption operation corresponds to unmapping the ciphertext C_m to recover the point P_m on the curve.
- Must then revert the embedding of $P_m = (x, y)$ into m.

ECC Encryption/Decryption

- Select a suitable curve and a point G. Here G is the point on the curve with the <u>largest</u> order. G (the base point) is also called the *order of the curve* (n), and must be a prime number. $nG = O$

- User A chooses a private key n_A and generates a public key $P_A = n_A * G$. Same for user B: n_B and $P_B = n_B * G$.

- To encrypt and send a msg P_m to B, A chooses a random positive integer k, and uses B's public key P_B to produce the ciphertext C_m consisting of the pair of points:

$$C_m = \{C_1, C_2\} = \{kG, P_m + kP_B\}$$ **k < order(G)**

- To decrypt C_m, B multiplies the first point in the pair by B's secret key n_B and then subtracts the result from the second point:

$$C_2 - n_B C_1 = (P_m + kP_B) - n_B(kG) = P_m + k(n_B G) - n_B(kG) = P_m$$

“Breaking” ECC Encryption

- To encrypt and send a msg P_m to B, A picks a random positive integer k, and uses B’s public key P_B to produce the ciphertext C_m consisting of the pair of points:

$$C_m = \{C_1 , C_2\} = \{ kG, P_m + kP_B \} \qquad \boldsymbol{k < \text{order}(G)}$$

- In practice, given $C_1 = kG$, it suffices to find k
- Calling C_1 as Q and G as P, we would get $Q = kP$
- So, given P and Q, we need to find the value of k

Agenda

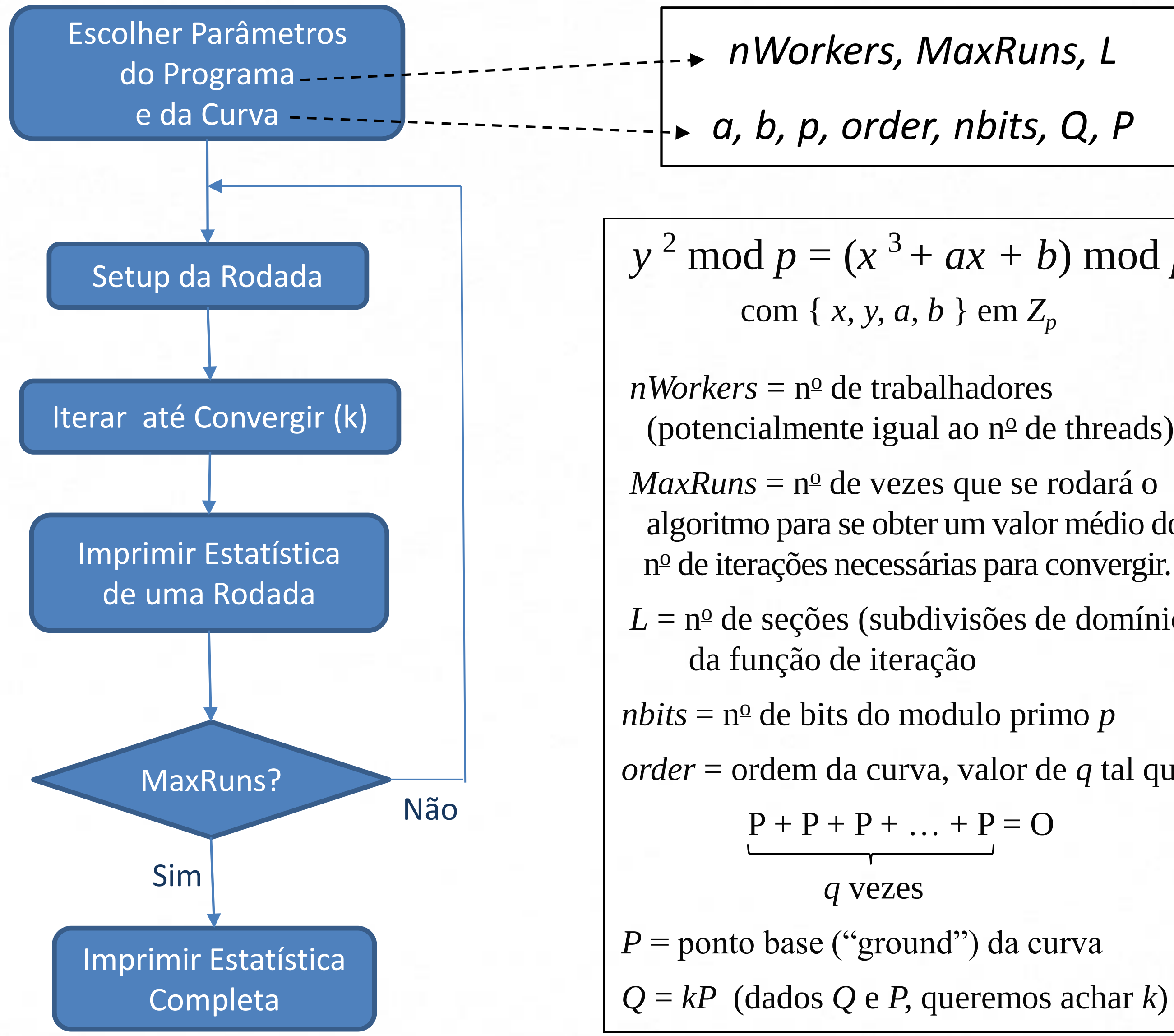
- Rápido Apanhado sobre Curvas Elípticas
- Criptografia de Curvas Elípticas
- Criptoanálise – Algoritmo Pollard Rho
- Programa – Algoritmo Pollard Rho

Professor vai compartilhar texto com a descrição do algoritmo na versão simples (1 thread) e na versão paralela (N threads)

Agenda

- Rápido Apanhado sobre Curvas Elípticas
- Criptografia de Curvas Elípticas
- Criptoanálise – Algoritmo Pollard Rho
- Programa – Algoritmo Pollard Rho

Diagrama de Blocos



$$y^2 \bmod p = (x^3 + ax + b) \bmod p$$

com $\{ x, y, a, b \}$ em Z_p

nWorkers = nº de trabalhadores (potencialmente igual ao nº de threads)

MaxRuns = nº de vezes que se rodará o algoritmo para se obter um valor médio do nº de iterações necessárias para convergir.

L = nº de seções (subdivisões de domínio) da função de iteração

nbits = nº de bits do modulo primo *p*

order = ordem da curva, valor de *q* tal que

$$\underbrace{P + P + P + \ldots + P}_{q \text{ vezes}} = O$$

P = ponto base (“ground”) da curva

$Q = kP$ (dados Q e P, queremos achar k)