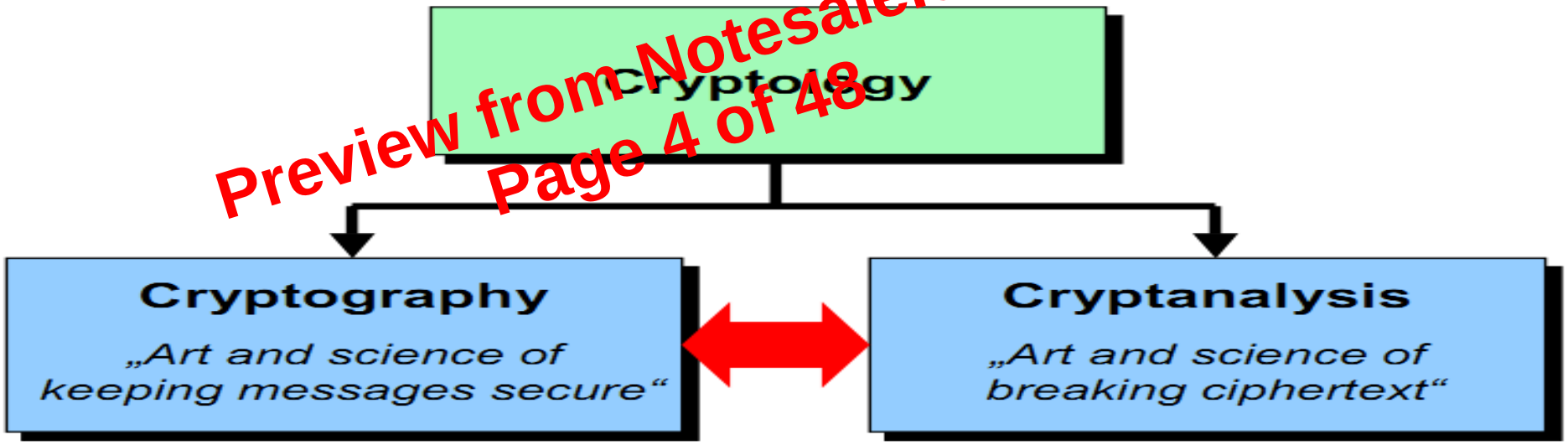
DEFINITIONS AND BASIC PRINCIPLES



Cryptology is a branch of mathematics

Cryptology

- The art and science of keeping messages secury is **cryptography**, and it is practiced by **cryptographers**.
- **Cryptanalysts** are practitioners of **cryptanalysis**, the art and science of breaking ciphertext; that is seeing through the disguise.
- The branch of mathematics encompassing both cryptography and cryptanalysis is **cryptology** an its practitioners are **cryptologists**.
- Modern cryptologists are generally trained in **theoretical mathematics** – they have to be.

CRYPTANALYSIS

„La Cryptographie militaire"

- Author: Auguste Kerckhoffs, born 1835 at Nuth, Holland
- **Good cryptographic algorithms are found only through thorough cryptanalysis!**
- Kerckhoffs deduced the following **six requirements** for selecting usable field ciphers:

1) the system should be, if not theoretically unbreakable, unbreakable in practice
2) Compromise of the system should not inconvenience the correspondents
3) The key should be remembrable without notes and should be easily changeable
4) The cryptograms should be transmissible by telegraph
5) the apparatus or documents should be portable and operable by a single person
6) the systems should be easy, neither requiring knowledge of a long list of rules nor involving mental strain.

E) Modular arithmetic

a) Multiplicative inverse
b) Euler totient function

Elliptic curve arithmetic

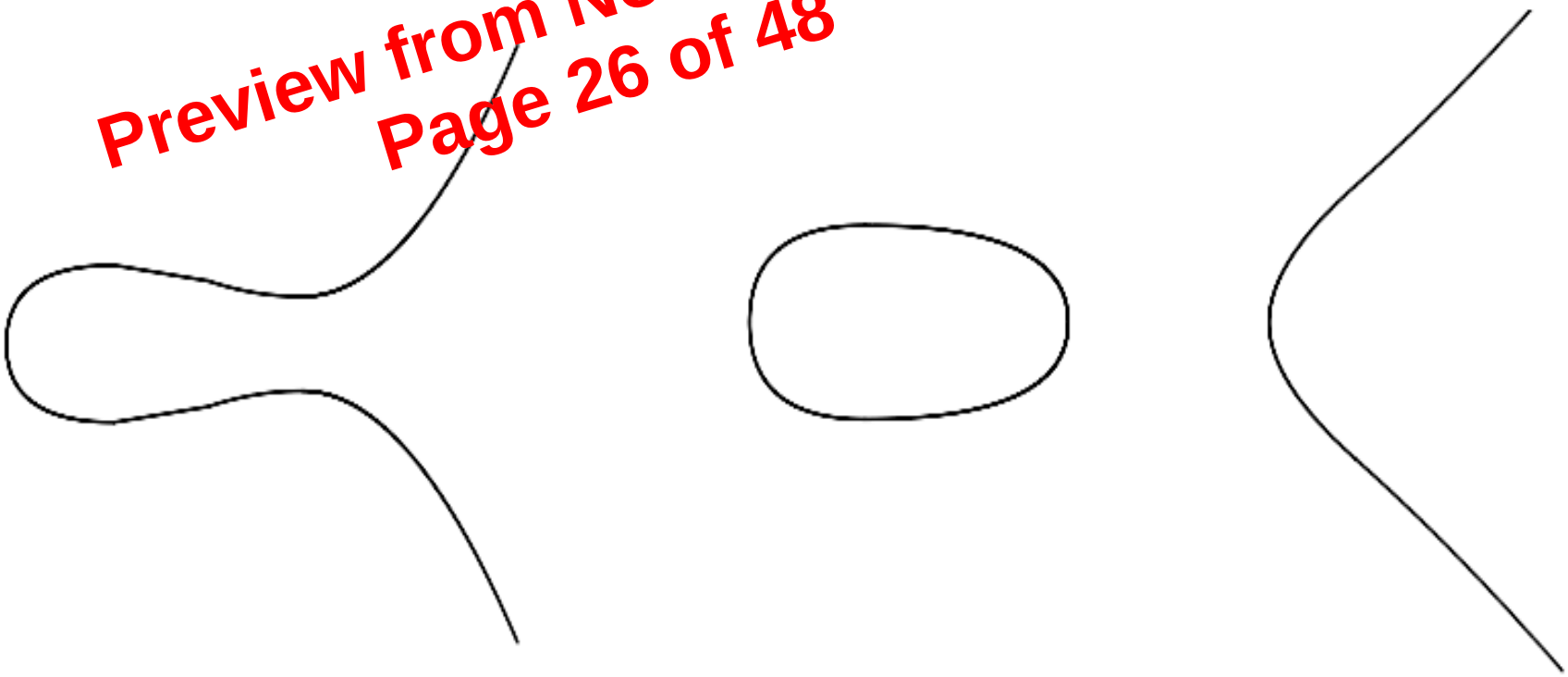
General form:

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

Condition for distinct single roots:

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

GENERAL SHAPE



$E_1 : Y^2 = X^3 - 3X + 3$

$E_2 : Y^2 = X^3 - 6X + 5$

Mathematical Description of Geometrical Transform

Line g: $y = s \cdot x - y_0$

with $s = \dfrac{y_Q - y_P}{x_Q - x_P}$

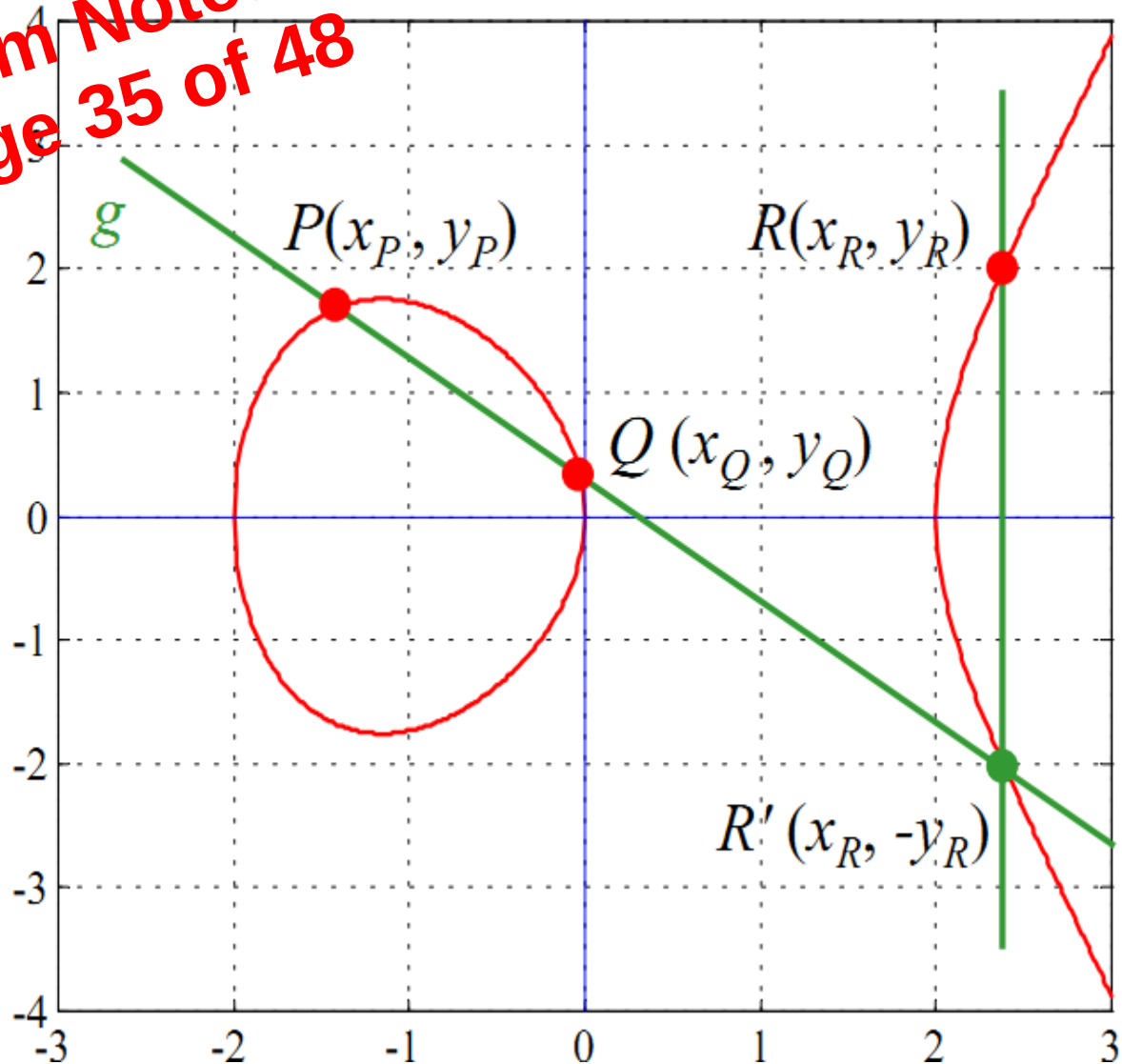
$$y_0 = y_P - s \cdot x_P$$

Intersection with curve:

$$(s \cdot x - y_0)^2 = x^3 + ax + b$$

Coordinates of point R:

$$x_R = s^2 - x_P - x_Q$$
$$y_R = -(s \cdot x_R + y_0)$$



ELLIPTIC CURVES – ADDITION IN FINITE FIELDS

- P = (9, 7) and Q = (1, 8)
- P + Q mod 13
- The slope, λ is given as

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{8 - 7}{1 - 9} = \frac{1}{-8} = \frac{1}{5} = 8$$

- Note that the additive inverse of -8 = 5 and the multiplicative inverse of 1/5 = 5^{-1} = 8 in mod 13 arithmetic

Task 3 – Iterate a Point on the Elliptic Curve

- Iterate the point P(2,4) lying on $y^2 = x^3 + x + 6 \mod 11$:
- Compute $P^2 = P * P$ by doubling the point P

$$s = \frac{dy}{dx} = \frac{3x_P^2 + a}{2y_P}$$

$$y_0 = y_P - s \cdot x_P$$

$$x_R = s^2 - 2x_P$$
$$y_R = -(s \cdot x_R + y_0)$$

- Compute $P^3 = P * P * P = P^2 * P$ by point addition

$$s = \frac{y_Q - y_P}{x_Q - x_P}$$

$$y_0 = y_P - s \cdot x_P$$

$$x_R = s^2 - x_P - x_Q$$
$$y_R = -(s \cdot x_R + y_0)$$

- All operations are computed in GF_{11}