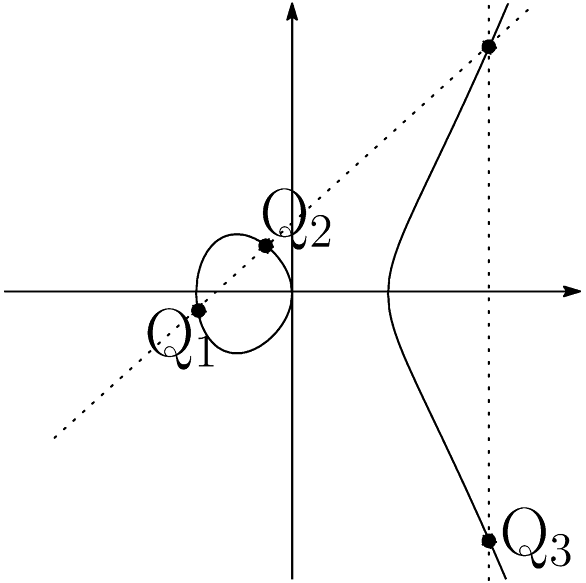
Elliptic Curves and Cryptography (6)

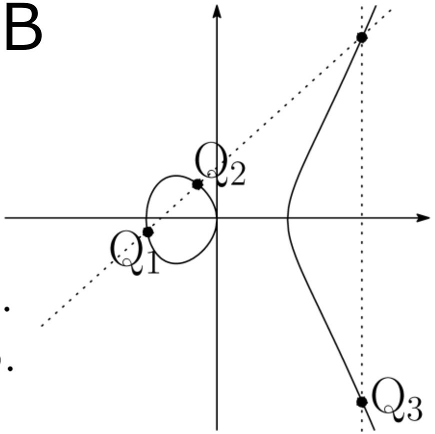
Group Law

- From points Q_1,Q_2 on an elliptic curve, we can create a new point Q_3.
- We write $\mathbf{Q_3 = Q_1 \oplus Q_2}$.
- We define $\mathbf{Q \oplus \infty = Q}$.



Elliptic Curves and Cryptography (7)

Elliptic Curve $Y^2 = X^3 + AX + B$



(1) If Q_1 or $Q_2 = \infty$,
- If $Q_1 = \infty$, put $Q_3 = Q_2$.
- If $Q_2 = \infty$, put $Q_3 = Q_1$.

(2) Otherwise, put $Q_1(S_1, T_1)$ and $Q_2(S_2, T_2)$.
- If $S_1 = S_2$ and $T_1 \neq T_2$, put $Q_3 = \infty$.
- Otherwise, define $Q_3(S_3, T_3)$ by

$$S_3 = K^2 - S_1 - S_2$$

$$T_3 = K(S_1 - S_3) - T_1$$

$$K = \begin{cases} (T_2 - T_1)/(S_2 - S_1) & \text{if } S_1 \neq S_2 \\ (3S_1^2 + A)/(2T_1) & \text{if } S_1 = S_2. \end{cases}$$

Elliptic Curves and Cryptography (8)

- Given two points Q_1 and Q_2 on the elliptic curve, there is a law (**Group Law**) creating a new point Q_3.
- Everything is calculated in terms of usual four operations of coordinates.
- We can also define the **Group Law for mod P points**.

Elliptic Curves and Cryptography (9)

- For a mod P point Q, we define

$$\mathbf{[K]Q} = Q \oplus \cdots \oplus Q \quad (K-1 \text{ times}).$$

- [K]Q is an analogue of the exponential A^K (mod P).
- Using [K]Q instead of A^K, we can construct cryptosystems.

$\Rightarrow$ **Elliptic Curve Cryptography (ECC)**

2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103 107 109 113 127 131 137 139 149 151 157 163 167 173 179 181 191 193 197 199

Summary of Week 4

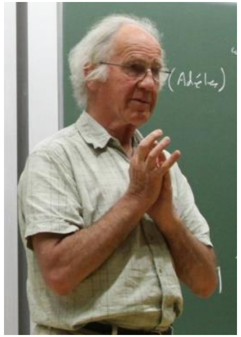
- Basics on Cryptography, Carsar cipher
- The use of Modular Arithmetic in Cryptography.
  - Discrete Logarithm Problem
  - Integer Factorization
- The RSA Cryptosystems
- Elliptic Curve Cryptography (ECC)

Plan of Week 5

We will learn more advanced **laws of prime numbers** for **elliptic curves**.

Let's explore attractive theorems and conjectures on elliptic curves!

See you next week!



Bryan John Birch (1931-)

Peter Swinnerton-Dyer (1927-)

https://en.wikipedia.org/wiki/Bryan_John_Birch
https://en.wikipedia.org/wiki/Peter_Swinnerton-Dyer