# Część 6

# Kryptografia asymetryczna na krzywych eliptycznych

# GRUPA

**Grupę $(G, \circ)$ tworzy zbiór $G$ z operacją binarną $\circ$ spełniający następujące aksjomaty:**

**1*) $\forall\ a, b, c \in G : a \circ (b \circ c) = (a \circ b) \circ c$**

**(łączność operacji $\circ$)**

**2*) $\exists\ e \in G\ \forall\ a \in G : a \circ e = e \circ a = a$**

**(istnienie elementu tożsamościowego dla $\circ$)**

**3*) $\forall\ a \in G\ \exists\ a^{-1} \in G : a \circ a^{-1} = a^{-1} \circ a = e$**

**(istnienie elementu odwrotnego do elementu $a$)**

**Grupoid – wystarczy określenie $G$ i $\circ$**

**Półgrupa – spełnienie 1*)**

**Monoid - spełnienie 1*) i 2*)**

**Grupa $(G, \circ)$ jest grupą abelową (albo przemienną) wtedy, gdy dodatkowo:**

**4*) $\forall\ a, b \in G : a \circ b = b \circ a$**

**(przemienność operacji $\circ$)**

# WŁASNOŚCI GRUPY

Jeżeli wartość | G | (moc zbioru) jest skończona, to grupa G jest grupą skończoną, zaś liczba elementów tej grupy jest rzędem grupy.

Podgrupą H grupy G jest taki niepusty podzbiór H grupy G, który także z operacją $\circ$ tworzy grupę.
Jeżeli ponadto $H \neq G$, to H jest podgrupą właściwą grupy G.

$\exists\, a \in G\ \forall\, b \in G\ \exists\, i \in Z : b = a^i \Rightarrow$

G jest grupą cykliczną, zaś a jest generatorem grupy cyklicznej G

$$(a^i = a \circ a \circ \ldots \circ a)$$

a powyżej po prawej stronie występuje i razy

UWAGA: Z faktu, że $e \in G$ wynika, że $\exists\, i \in Z : e = a^i$, stąd grupą cykliczną może być wyłącznie grupa skończona.

Podgrupą cykliczną generowaną przez element $a \in G$ jest zbiór:

$< a > = \{ b \in G : b = a^i \}$, gdzie $i \in Z$

## WŁASNOŚCI GRUPY (cd.)

Rzędem elementu $a \in G$, oznaczanym jako ord (a), jest najmniejsza dodatnia liczba całkowita $t$ taka, że $a^t = e$. Jeżeli taka liczba nie istnieje, to ord (a) = $\infty$.

(G jest grupą) $\wedge$ ( $a \in G$ ) $\wedge$ ( $ord(a) = t < \infty$ ) $\Rightarrow$ $|< a >| = t$

### Twierdzenie Lagrange'a

Jeżeli G jest grupą skończoną i H jest podgrupą G, to $| H | \,|\, | G |$.
Wynika stąd, że jeśli $a \in G$, to $ord(a) \,|\, | G |$.

Każda podgrupa grupy cyklicznej G jest grupą cykliczną. Jeżeli G jest grupą cykliczną rzędu n, to G zawiera dokładnie jedną podgrupę rzędu d, gdzie d jest dodatnim dzielnikiem n.

Niech G będzie grupą i $a \in G$.
$ord(a) = t \Rightarrow ord(a^k) = t / gcd(t, k)$
(G jest grupą cykliczną rzędu n) $\wedge$ ( $d \mid n$ ) $\Rightarrow$ G zawiera dokładnie $\phi(d)$ elementów rzędu d (w szczególności $\phi(n)$ generatorów).

# WŁASNOŚCI GRUPY (cd.)

***Przykład 1:***

**Zbiór $Z_n$ z operacją *dodawania modulo n* tworzy skończoną przemienną grupę addytywną $(Z_n, +)$, gdyż:**

$$\forall\ a, b, c \in Z_n : (a + ( b + c ))(mod\ n) = (( a + b ) + c )(mod\ n)$$

**elementem tożsamościowym jest $e = 0$ :**

$$\forall\ a \in Z_n : (a + 0)\ (mod\ n) = (0 + a)\ (mod\ n) = a$$

**elementem odwrotnym do elementu *a* jest $-a = (n - a)\ (mod\ n)$ :**

$$\forall\ a \in Z_n : (a + (-a))\ (mod\ n) = ((-a) + a)\ (mod\ n) = (a + n - a)\ (mod\ n) = n\ (mod\ n) = 0$$

**a ponadto:**

$$\forall\ a, b \in Z_n : (a + b)\ (mod\ n) = (b + a)\ (mod\ n)$$

# WŁASNOŚCI GRUPY (cd.)

***Przykład 1 (cd.):***

**Rząd grupy $(Z_n, +)$ wynosi $n$.**

**Niech $n$ będzie liczbą parzystą. Wówczas podzbiór liczb parzystych należących do zbioru $Z_n$ (wraz z elementem tożsamościowym $e = 0$) tworzy podgrupę właściwą z operacją dodawania *modulo n*.**

**Generatorem grupy $(Z_n, +)$ jest element $a = 1$, natomiast generatorem cyklicznej podgrupy właściwej zawierającej liczby parzyste należące do $Z_n$, gdzie $n$ jest liczbą parzystą, jest element $a = 2$.**

**Uogólniony wniosek**

**Z twierdzenia Lagrange'a wynika, że każdy dzielnik liczby $n$ jest generatorem cyklicznej podgrupy właściwej, zaś jej elementami są wszystkie wielokrotności generatora < $n$ i liczba $0$.**

# WŁASNOŚCI GRUPY (cd.)

***Przykład 2:***

**Zbiór $Z^*_n$ z operacją *mnożenia modulo n* tworzy skończoną przemienną grupę multiplikatywną $(Z^*_n, .)$, gdyż:**

$\forall\ a, b, c \in Z^*_n : (a\ (\ b\ c\ ))(mod\ n) = ((\ a\ b\ )\ c\ )(mod\ n)$

**elementem tożsamościowym jest $e = 1$ :**

$$\forall\ a \in Z^*_n : (a \cdot 1)\ (mod\ n) = (1 \cdot a)\ (mod\ n) = a$$

**elementem odwrotnym do elementu $a$ jest $a^{-1}\ (mod\ n)$ :**

$\forall\ a \in Z^*_n : (a\ a^{-1})\ (mod\ n) = (a^{-1}\ a)\ (mod\ n) = 1$

**a ponadto:**

$\forall a, b \in Z^*_n : (a\ b)\ (mod\ n) = (b\ a)\ (mod\ n)$

**Rząd grupy $(Z^*_n, .)$ wynosi $\phi(n)$.**

# WŁASNOŚCI GRUPY (cd.)

***Przykład 3:***

**Niech *n = 19.***

$$Z^*_{19} = \{ 1, 2, 3, ..., 18 \} \qquad \phi(19) = 18$$

**Grupa $(Z^*_{19}, .)$ jest grupą cykliczną.**

**Dzielniki $\phi(19)$ to liczby: *1, 2, 3, 6, 9* i *18*.**

**Istnieje zatem *6* podgrup cyklicznych, odpowiednio rzędu: *1, 2, 3, 6, 9* i *18* (przy czym ostatnia z podgrup nie jest podgrupą właściwą, lecz jest tożsama z grupą $Z^*_{19}$).**

**Poniższa tabela przedstawia wszystkie podgrupy cykliczne $Z^*_{19}$ i ich generatory.**

| *Podgrupa* | *Generatory* | *Rząd d* | $\phi(d)$ |
|---|---|---|---|
| $\{ 1 \}$ | 1 | 1 | 1 |
| $\{ 1, 18 \}$ | 18 | 2 | 1 |
| $\{ 1, 7, 11 \}$ | 7, 11 | 3 | 2 |
| $\{ 1, 7, 8, 11, 12, 18 \}$ | 8, 12 | 6 | 2 |
| $\{ 1, 4, 5, 6, 7, 9, 11, 16, 17 \}$ | 4, 5, 6, 9, 16, 17 | 9 | 6 |
| $\{ 1, 2, 3, ...., 18 \}$ | 2, 3, 10, 13, 14, 15 | 18 | 6 |

## WŁASNOŚCI GRUPY (cd.)

***Przykład 4:***

**Niech *n = 15.***

$$Z^*_{15} = \{ 1, 2, 4, 7, 8, 11, 13, 14 \} \qquad \phi(15) = \phi(3) \bullet \phi(5) = 8$$

**Grupa $(Z^*_{15}, .)$ jest skończoną grupą multiplikatywną ale nie jest grupą cykliczną.**

**Dzielniki $\phi(15)$ to liczby: *1, 2, 4* i *8*.**

**Mimo że każdy z elementów grupy generuje pewną podgrupę cykliczną, to żaden nie jest generatorem grupy $(Z^*_{15}, .)$.**

**Poniższa tabela przedstawia wszystkie podgrupy cykliczne $Z^*_{15}$ i ich generatory.**

| *Podgrupa* | *Generatory* | *Rząd podgrupy (d)* | *φ(d)* |
|---|---|---|---|
| *{1}* | *1* | *1* | *1* |
| *{1, 4}* | *4* | *2* | *1* |
| *{1, 11}* | *11* | *2* | *1* |
| *{1, 14}* | *14* | *2* | *1* |
| *{1, 2, 4, 8}* | *2, 8* | *4* | *2* |
| *{1, 4, 7, 13}* | *7, 13* | *4* | *2* |

# WŁASNOŚCI GRUPY (finał)

**Czy każda grupa skończona jest grupą cykliczną?**

**NIE !!!**

# PIERŚCIEŃ

**Pierścień $(R, +, \times)$ tworzy zbiór $R$ z dwoma operacjami binarnymi, arbitralnie oznaczonymi jako $+$ (dodawanie) i $\times$ (mnożenie), spełniający następujące aksjomaty:**

**$(R, +)$ jest grupą przemienną z elementem tożsamościowym oznaczanym jako $0$ (element zerowy, neutralny):**

$$\forall\, a, b, c \in R : a \times (b \times c) = (a \times b) \times c$$

**(łączność operacji $\times$)**

$$\exists\ e \in R : (e \neq 0) \wedge (\forall\, a \in R: a \times e = e \times a = a)$$

**(istnienie elementu tożsamościowego dla $\times$, oznaczanego jako $1$)**

**Operacja $\times$ jest rozdzielna względem operacji $+$, tzn.:**

$$\forall\, a, b, c \in R:\ a \times (b + c) = (a \times b) + (a \times c)$$

$$\forall\, a, b, c \in R: (b + c) \times a = (b \times a) + (c \times a)$$

**Pierścień $(R, +, \times)$ jest pierścieniem przemiennym wtedy, gdy ponadto:**

$$\forall\, a, b \in R : a \times b = b \times a$$

**(przemienność operacji $\times$)**

# PIERŚCIEŃ (cd.)

**Element $a \in R$ pierścienia jest nazywany *elementem odwracalnym*, jeżeli istnieje element $b \in R$ taki, że $a \times b = 1$.**

**Zbiór elementów odwracalnych pierścienia $R$ tworzy z operacją $\times$ *grupę elementów odwracalnych R*.**

***Przykłady:***

**Zbiór $Z$ ze zwykłymi operacjami dodawania i mnożenia liczb całkowitych jest pierścieniem przemiennym.**

**Zbiór $Z_n$ z operacjami dodawania i mnożenia *modulo n* jest pierścieniem przemiennym.**

**Grupą elementów odwracalnych pierścienia $Z_n$ jest zbiór $Z^*_n$ .**

# CIAŁO

**Ciałem F** jest **pierścień przemienny**, którego wszystkie niezerowe elementy są elementami **odwracalnymi**.

**Charakterystyka** ciała wynosi **0**, jeżeli dla żadnego $m \geq 1$ wynik operacji **m**-krotnego dodawania elementów **1** nie jest równy elementowi **zerowemu**. W przeciwnym przypadku charakterystyka ciała jest równa najmniejszej dodatniej liczbie całkowitej **m** takiej, że:

$$\sum_{i=1}^{m} 1 = 0$$

Charakterystyka ciała $m \neq 0 \Rightarrow$ **m** jest **liczbą pierwszą**.

# CIAŁO SKOŃCZONE

**Ciało skończone** to ciało **F** zawierające skończoną liczbę elementów. Liczba ta jest **rzędem ciała skończonego**.

**F** jest ciałem skończonym $\Rightarrow$ **F** zawiera $p^m$ elementów, gdzie **p** jest pewną liczbą pierwszą, zaś **m** liczbą naturalną.

Dla każdej potęgi naturalnej liczby pierwszej $p^m$ istnieje unikalne (z dokładnością do **izomorfizmu**) ciało skończone rzędu $p^m$, oznaczane jako $F_{p^m}$ albo $GF(p^m)$ (**GF - Galois Field - ciało Galois**).

**Izomorfizm** oznacza (nieformalnie), że ciała są strukturalnie identyczne (mimo odmiennej reprezentacji elementów ciała). Stąd między innymi wynika, że każde ciało rzędu **p** jest **izomorficzne** z ciałem $Z_p$.

Niech $F_q$ będzie **ciałem skończonym** rzędu $q = p^m$.
Wtedy każde podciało ciała $F_q$ jest rzędu $p^n$, dla pewnego **n** będącego dodatnim dzielnikiem **m**.

# WŁASNOŚCI CIAŁA SKOŃCZONEGO

Jeżeli n jest dodatnim dzielnikiem m, to istnieje dokładnie jedno podciało ciała $F_q$ rzędu $p^n$.

Element $a \in F_q$ należy do podciała $F_p{}^n$ wtedy i tylko wtedy, gdy

$$a^{p^n} = a .$$

Niezerowe elementy ciała $F_q$ tworzą grupę z mnożeniem, nazywaną grupą multiplikatywną ciała $F_q$ i oznaczaną jako $F_q{}^*$.

$F_q{}^*$ jest grupą cykliczną rzędu $q-1$. Stąd $a^q = a$ dla wszystkich $a \in F_q$.

Jeżeli $a, b \in F_q$, gdzie $F_q$ jest ciałem skończonym charakterystyki p,

to $(a+b)^{p^t} = a^{p^t} + b^{p^t}$ dla wszystkich $t \geq 0$.

# PRZYKŁAD

## TEORIA: Istnieje ciało skończone GF($2^2$).

**Czy zbiór $Z_4 = \{0, 1, 2, 3\}$ z operacjami dodawania modulo 4 i mnożenia modulo 4 jest ciałem ?**

$Z_4$ z operacją dodawania modulo 4 jest grupą przemienną.

Operacja dodawania modulo 4 jest łączna.

Elementem tożsamościowym jest 0.

Elementami odwrotnymi są odpowiednio:

$0 \Leftrightarrow 0$, $1 \Leftrightarrow 3$, $2 \Leftrightarrow 2$.

Operacja dodawania modulo 4 jest przemienna.

Operacja mnożenia modulo 4 jest łączna.

Operacja mnożenia modulo 4 jest rozdzielna względem operacji dodawania modulo 4.

Elementem tożsamościowym jest 1.

Elementy 1 i 3 są odwracalne ($1^{-1} = 1$, $3^{-1} = 3$).

Element 2 nie jest odwracalny (ani nie jest tożsamościowym dla dodawania).

**Zbiór $Z_4 = \{0, 1, 2, 3\}$ z operacjami dodawania modulo 4 i mnożenia modulo 4 nie jest ciałem (ale jest pierścieniem przemiennym) !!!**

# KRZYWE ELIPTYCZNE „WKRACZAJĄ” DO KRYPTOLOGII

**W 1985 roku Neal Koblitz i Victor S. Miller zaproponowali wykorzystanie w kryptografii krzywych eliptycznych nad ciałem *K*, tzn. krzywych, dla których współrzędne punktów spełniają (w zależności od charakterystki ciała *K*, do którego należą współczynniki odpowiednich wielomianów, a także współrzędne punktów) następujące równania:**

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

$$y^2 + cy = x^3 + ax^2 + b \qquad (2)$$

$$y^2 + xy = x^3 + ax^2 + b \qquad (3)$$

$$y^2 = x^3 + ax^2 + bx + c \qquad (4)$$

***(dokładniej: krzywą eliptyczną jest zbiór wszystkich punktów spełniających jedną z powyższych zależności oraz element O, zwany “punktem w nieskończoności”).***

**Każda krzywa eliptyczna nad dowolnym ciałem *K* może być opisana równaniem:**

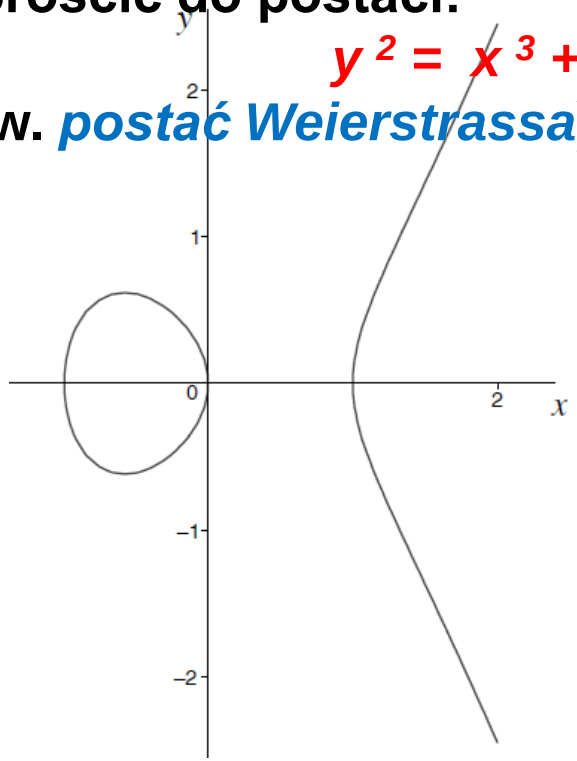
$$y^2 + axy + by = x^3 + cx^2 + dx + e$$

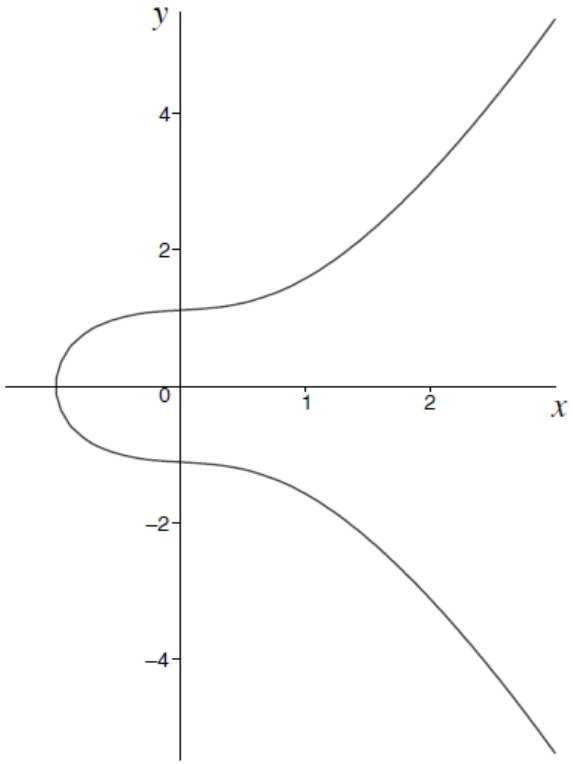
**(ten opis nie musi być jednoznaczny i nazywa się *modelem afinicznym krzywej eliptycznej*).**

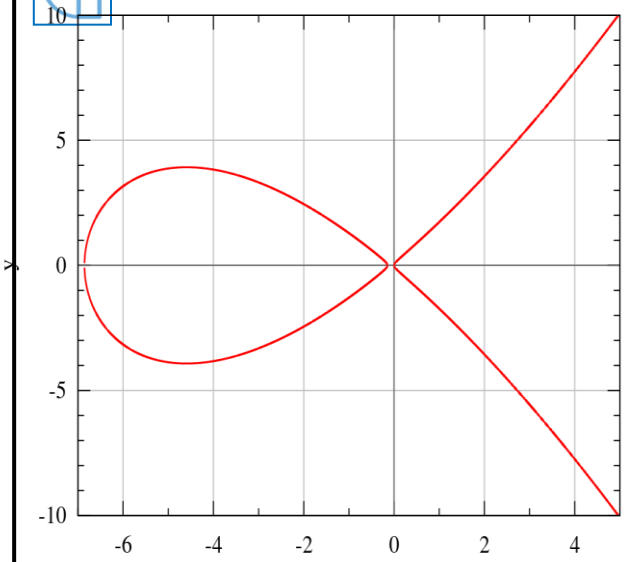
**Jeśli charakterystyka ciała $K \notin \{2, 3\}$, to powyższe równanie afiniczne można uprościć do postaci:**

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

**(jest to tzw. *postać Weierstrassa*).**






W 1987 roku Peter L. Montgomery „pochylił się” nad krzywymi eliptycznymi nad ciałem $K$ opisywanymi równaniem:

$$by^2 = x^3 + ax^2 + x,$$

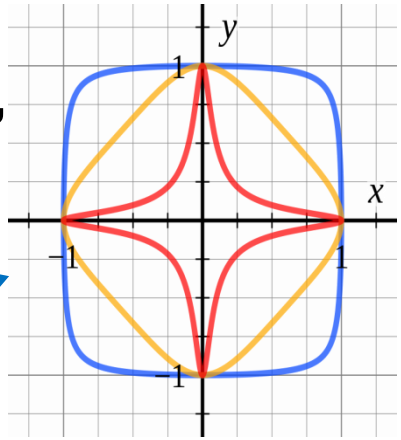
gdzie $b(a^2 - 4) \neq 0$

(jest to tzw. *postać Montgomery'ego*, która i tak ma swoją ekwiwalentną *krzywą Weierstrassa*).

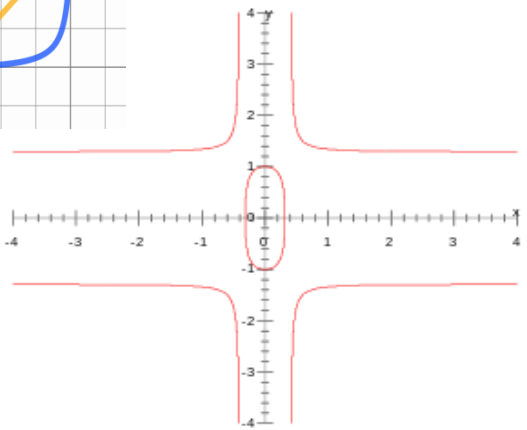
W 2007 roku Harold Edwards „zajął się” krzywymi eliptycznymi nad ciałem $K$ opisywanymi równaniem:

$$x^2 + y^2 = c^2(1 + dx^2y^2),$$

gdzie $cd(1 - c^4d) \neq 0$




(a zastosowania krzywych Edwardsa i skręconych (twisted) krzywych Edwardsa w kryptologii są badane intensywnie przez min. D.L.Bernsteina i T.Lange – głównie ze względu na efektywność implementacji sprzętowych).



# DODAWANIE PUNKTÓW NA KRZYWEJ ELIPTYCZNEJ

**Punkty krzywej eliptycznej *E* (wraz z punktem *O*) tworzą grupę przemienną (abelową) ze względu na dodawanie, które jest zdefiniowane następująco:**

**Niech będą dane punkty *P* i *Q* należące do krzywej *E*.**

***Definicja elementu przeciwnego i neutralnego (zera)***

**Jeżeli $P = O$, to $-P = O$, a ponadto dla każdego $Q \neq P$ zachodzi:**

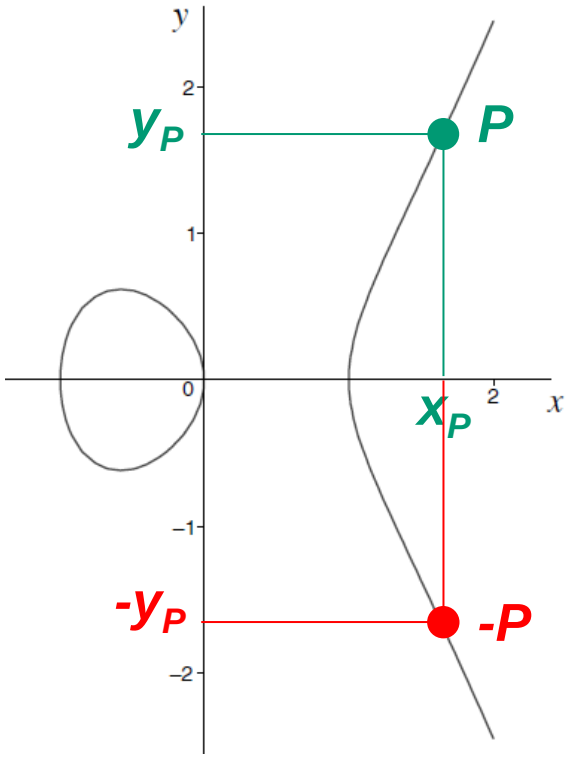
$$P + Q = Q.$$

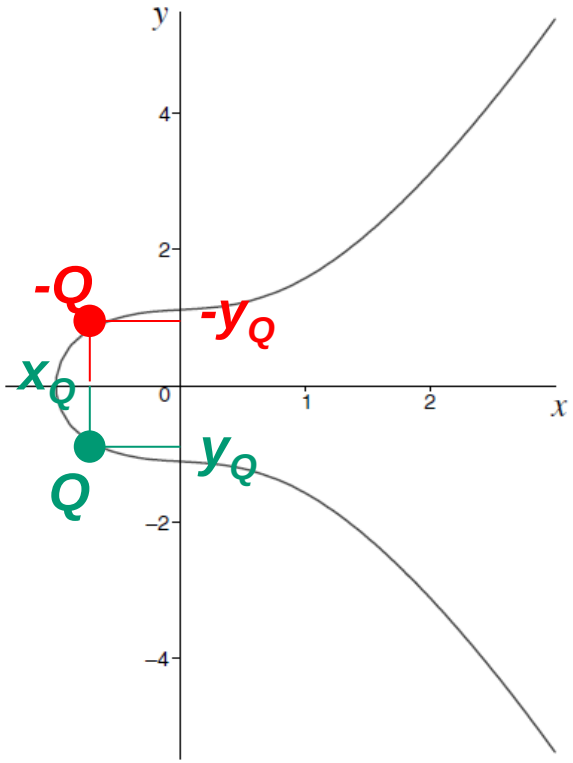
**Punkt *O* jest elementem tożsamościowym (neutralnym) tej grupy.**

**Jeżeli $P \neq O$ i jest określony parą współrzędnych $(x_P, y_P)$, to elementem przeciwnym, czyli punktem $-P$, jest punkt o współrzędnych $(x_P, -y_P)$ (także należący do krzywej *E*, co łatwo sprawdzić).**

**UWAGA: współrzędna $-y$ jest w ciele *K* elementem przeciwnym względem dodawania dla współrzędnej *y*.**

**Przykład dla $K = \mathbb{R}$**
**(zbiór liczb rzeczywistych z „klasycznym” dodawaniem i mnożeniem)**




$y^2 = x^3 - x$

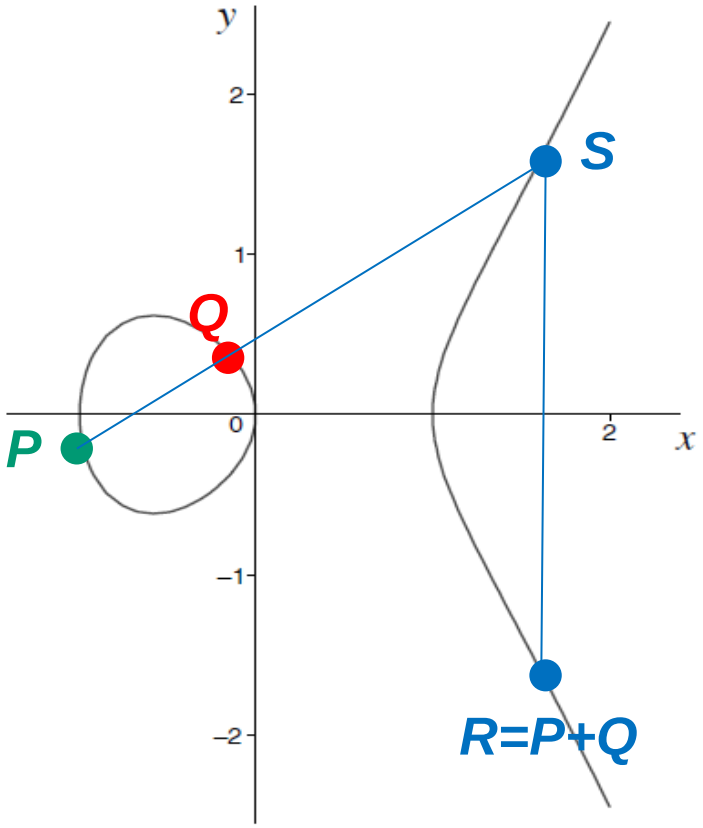
$y^2 = x^3 + 0.25x + 1.25$

## *Definicja dodawania dla punktów różnych od elementu neutralnego*

**Niech *P* ma współrzędne $(x_P,y_P)$, punkt *Q* ma współrzędne $(x_Q,y_Q)$, zaś punkt $R = P+Q$ ma współrzędne $(x_R,y_R)$.**

### *Przypadek 1:*

**Jeżeli $x_P \neq x_Q$, to prosta poprowadzona przez punkty *P* i *Q* przetnie krzywą eliptyczną dokładnie w jednym punkcie $S = -R$ o współrzędnych $(x_R,-y_R)$.**

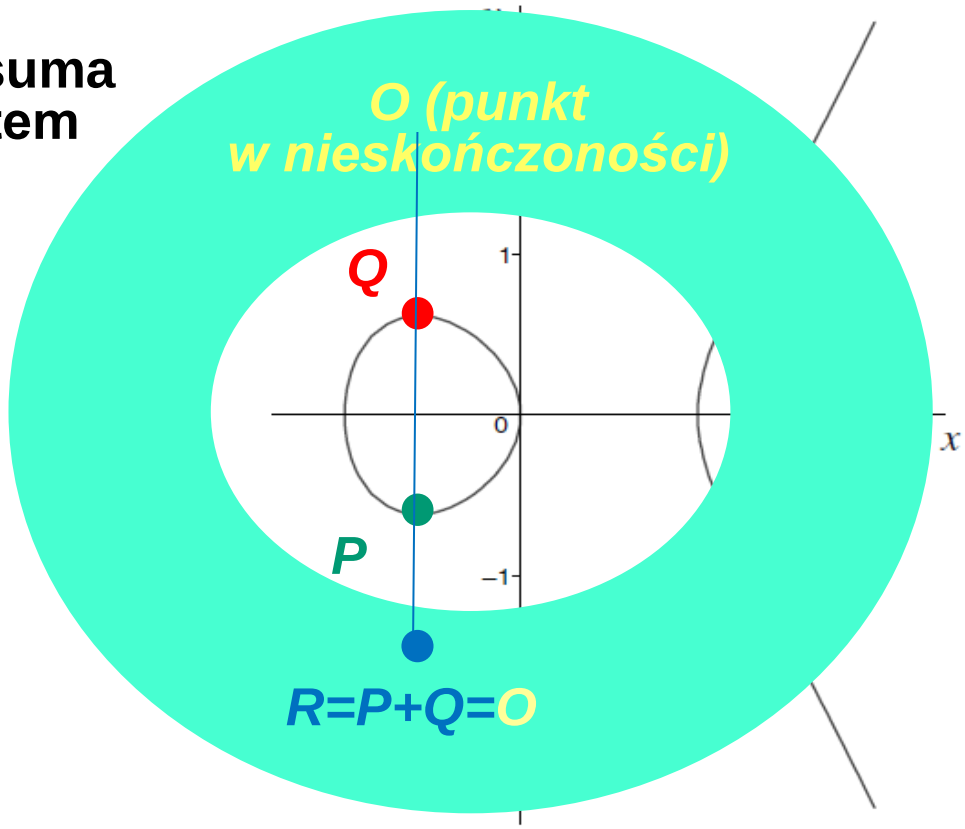



**Przykład dla *K* = *R***

## *Przypadek 2:*

**Jeżeli $x_P = x_Q$ oraz $y_P = - y_Q$ (a zatem wtedy, gdy $P = -Q$), to suma tych punktów musi być elementem neutralnym $O$, czyli "punktem w nieskończoności".**

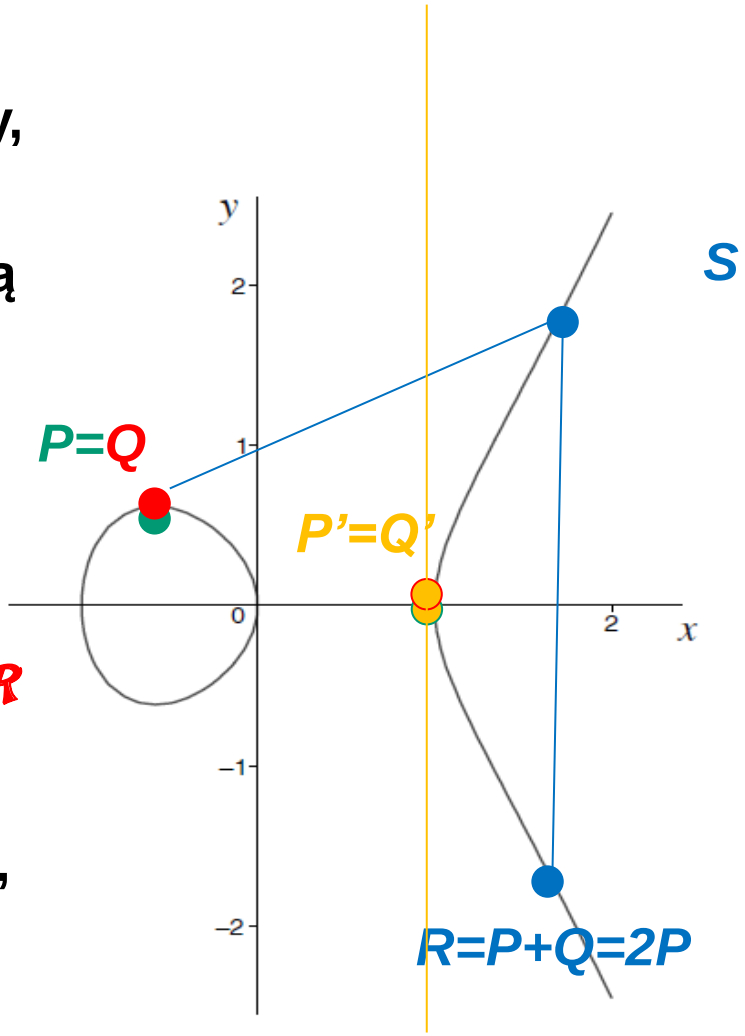
**Przykład dla $K = \mathbb{R}$**



## *Przypadek 3:*

**Jeżeli $x_P = x_Q$ oraz $y_P = y_Q$ (a zatem wtedy, gdy $P = Q$), to suma tych punktów jest wyznaczana jako punkt przeciwny do punktu $S$, w którym krzywą eliptyczną przecina prosta styczna do tej krzywej w punkcie $P = Q$.**

**Tak wyznaczony punkt $R = P+Q$ określa się także jako $R = 2P$.**




**Przykład dla $K = \mathbb{R}$**

## *Przypadek szczególny*

**Jeżeli $x_{P'} = x_{Q'}$ zaś $y_{P'} = y_{Q'} = 0$ (w ciele $K$), to styczna przetnie krzywą w „punkcie w nieskończoności", a zatem w tym przypadku $2P$ '$= O$ (!!!).**

Stosując „podwajanie” punktu i dodawanie punktów określa się mnożenie punktu przez skalar (liczbę całkowitą):

$R = kP = (P + P + ... + P)$ ($k$ składników sumy dla $k > 0$);
$R = -kP = -(P + P + ... + P)$;
$R = 0P = O$ („punkt w nieskończoności”).

Wprowadza się także pojęcie logarytmu dyskretnego na krzywej eliptycznej (*ECDL*):

jeżeli $R = kP$, to $log_P R = k$.

Tak, jak w każdej grupie, określa się rząd każdego punktu $ord(P)$ jako najmniejszą liczbę $k > 0$, dla której $kP=O$, oraz generator grupy $G$, czyli punkt, dla którego $ord(G)$ jest równy rzędowi grupy (liczbie punktów na krzywej).

Takich generatorów może być oczywiście w każdej grupie więcej niż jeden, albo grupa może nie posiadać żadnego generatora.

W kryptografii mają zastosowanie krzywe eliptyczne nad ciałami skończonymi $F_p^m$, dla których zaproponowano między innymi odpowiedniki algorytmów RSA, Diffiego-Hellmana, ElGamala i inne.

Podstawą ich konstrukcji jest konstatacja faktu, że odpowiednikiem operacji potęgowania w ciele skończonym $F_p$, jest operacja mnożenia przez stałą całkowitą punktów na krzywej eliptycznej $E$ nad pewnym ciałem $F_p^m$:

$$\{y = x^k, \text{ gdzie } x,y \in F_p\} \leftrightarrow \{Q = kP, \text{ gdzie } P,Q \in E\}.$$

Wyznaczenie takich ciał o odpowiednio dużej liczbie punktów leżących na danej krzywej $E$ nie jest zadaniem łatwym.

Z punktu widzenia zastosowań kryptograficznych „najciekawszymi" (jak dotąd) krzywymi eliptycznymi, czyli grupami addytywnymi, których elementami są punkty na krzywej, są:

- krzywe eliptyczne nad ciałem skończonym $F_p$, gdzie p jest liczbą pierwszą;
- krzywe eliptyczne nad ciałem skończonym $F_2^m$, gdzie m jest dowolną liczbą naturalną, czyli nad ciałem wielomianów stopnia (m-1) o współczynnikach z $Z_2$ (ze względu na reprezentację tych wielomianów przez m–bitowe ciągi binarne, krzywe te są atrakcyjne dla implementacji w „klasycznych" urządzeniach informatycznych).

# LICZBA PUNKTÓW NA KRZYWEJ ELIPTYCZNEJ (1/4)

## *Ślad Frobeniusa*

**Dla krzywej eliptycznej nad ciałem $F_p^m$ liczba punktów *#(E)* wynosi:**

$$\#(E) = p^m + 1 - t,$$

**gdzie liczba *t* to tzw. ślad Frobeniusa dla $q = p^m$.**

## *Twierdzenie Hasse'go 1*

**Dla krzywych eliptycznych *E* nad ciałem GF(p), gdzie p jest liczbą pierwszą, rząd grupy *#(E)* spełnia zależność:**

$$p+1-2\sqrt{p} \le \#(E) \le p+1+2\sqrt{p}$$

## *Twierdzenie Waterhouse'a 1*

**Każda liczba całkowita n z przedziału określonego w powyższym twierdzeniu jest rzędem pewnej grupy punktów na krzywej eliptycznej nad ciałem GF(p).**

# LICZBA PUNKTÓW NA KRZYWEJ ELIPTYCZNEJ (2/4)

## *Twierdzenie Hasse'go 2*

**Dla krzywych eliptycznych *E* nad ciałem GF($2^m$), gdzie m jest liczbą naturalną, rząd grupy *#(E)* spełnia zależność:**

$$2^m + 1 - 2\sqrt{2^m} \leq \#(E) \leq 2^m + 1 + 2\sqrt{2^m}$$

## *Twierdzenie Waterhouse'a 2*

**Niech *t* będzie liczbą całkowitą spełniającą zależność $|t| \leq 2\sqrt{2^m}$.**

**Istnieje krzywa eliptyczna rzędu nad ciałem GF($2^m$) wtedy i tylko wtedy, gdy zachodzi jeden z poniższych warunków:**

- ***t*** **jest liczbą nieparzystą**
- **m jest liczbą nieparzystą i (*t = 0* albo $t^2 = 2^{m+1}$)**
- **m jest liczbą parzystą i (*t = 0* albo $t^2 = 2^{m+2}$ albo $t^2 = 2^m$)**

# LICZBA PUNKTÓW NA KRZYWEJ ELIPTYCZNEJ (3/4)

## *Twierdzenie Hasse'go 3*

**Dla krzywych eliptycznych *E* nad ciałem $GF(p^m)$, gdzie p jest liczbą pierwszą zaś m jest liczbą naturalną, rząd grupy *#(E)* spełnia zależność:**

$$p^m + 1 - 2\sqrt{p^m} \leq \#(E) \leq p^m + 1 + 2\sqrt{p^m}$$

## *Twierdzenie Waterhouse'a 3*

**Niech *t* będzie liczbą całkowitą spełniającą zależność $|t| \leq 2\sqrt{p^m}$.**

**Istnieje krzywa eliptyczna rzędu $q=p^m+1-t$ nad ciałem $GF(p^m)$ wtedy i tylko wtedy, gdy zachodzi jeden z poniższych warunków:**

- ***t*** **jest liczbą nieparzystą**
- **m jest liczbą nieparzystą i (*t = 0* albo ($t^2 = 2q$ i *p = 2*) albo ($t^2 = 3q$ i *p = 3*))**
- **m jest liczbą parzystą i ((*t = 0* i $p \neq 1 \bmod 4$) albo ($t^2 = q$ i $p \neq 1 \bmod 3$) albo $t^2 = 4q$)**

# LICZBA PUNKTÓW NA KRZYWEJ ELIPTYCZNEJ (4/4)

Krzywa eliptyczna nad ciałem $GF(q=p^m)$, dla której $\#(E) = p^m+1-t$ , nazywa się krzywą supersingularną wtedy, gdy $p \mid t$ (co jest równoważne warunkowi $\#(E) \equiv 1 \bmod p$).

Z punktu widzenia „klasycznej" kryptografii krzywe supersingularne nie są bezpieczne i należy ich unikać w „klasycznych ECC" (natomiast takie krzywe są „przyjazne" z punktu widzenia systemów kryptograficznych wykorzystujących odwzorowania dwuliniowe – „pairings", tzw. PBC – Pairing Based Cryptosystems).

Krzywa eliptyczna nad ciałem $GF(q=p^m)$, dla której ślad Frobeniusa $t$ wynosi 1 (wtedy $\#(E) = q$), nazywa się krzywą anomalną.

Z punktu widzenia kryptografii krzywe anomalne nie są bezpieczne i należy ich unikać.

Dla punktu $P$ należącego do grupy addytywnej punktów na krzywej eliptycznej $E$ najmniejsza liczba całkowita $n$ taka, że $nP = O$, jest rzędem tego punktu $ord(P)$.

Z twierdzenia Lagrange'a wynika, że $ord(P) | \#(E)$.

Wartość $h = \#(E)/ord(P)$ określa się mianem kofaktora.

# GRUPY PUNKTÓW NA KRZYWYCH ELIPTYCZNYCH NAD $F_p$ (1/4)

Grupy te, to zbiory punktów $P = (x, y)$ spełniających równanie:

$$y^2 \bmod p = (x^3 + ax + b) \bmod p \qquad (x, y, a, b \in Z_p),$$

oraz punkt $O$ „w nieskończoności”.

Warunkiem istnienia grupy jest: $(4a^3 + 27b^2) \bmod p \neq 0$.

Punktem „przeciwnym” do punktu $P = (x, y)$ jest punkt $(x, p - y)$.

Współrzędne punktu $R = P + Q$, gdzie $P \neq Q$ i $P \neq -Q$, a ponadto oba punkty są różne od punktu $O$, określane są następująco:

$$s = (y_P - y_Q)(x_P - x_Q)^{-1} \bmod p,$$

gdzie $s$ jest nachyleniem prostej łączącej punkty $P$ i $Q$;

$$x_R = s^2 - x_P - x_Q \bmod p;$$
$$y_R = -y_P + s(x_P - x_R) \bmod p.$$

# GRUPY PUNKTÓW NA KRZYWYCH ELIPTYCZNYCH NAD $F_p$ (2/4)

**Współrzędne punktu $R = 2P$ określane są następująco:**

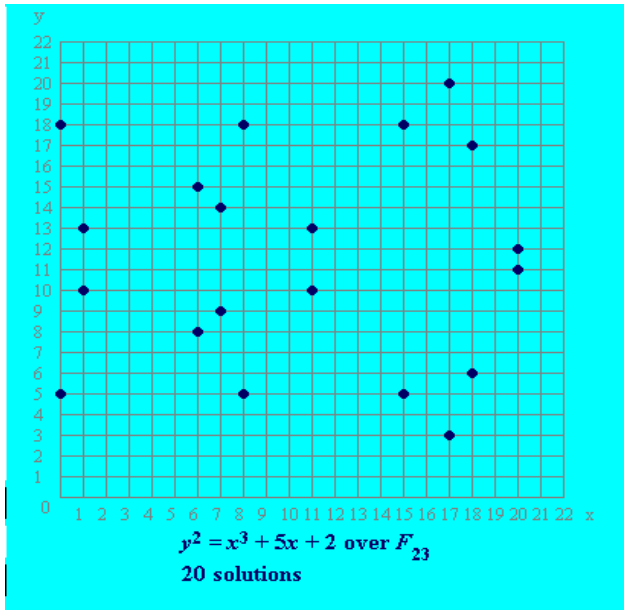
$$s = (3x_P^2 + a)(2y_P)^{-1} \bmod p,$$

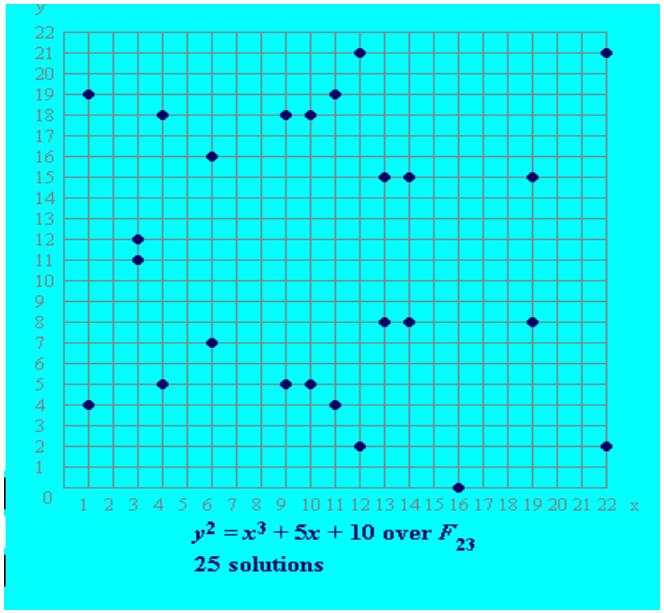
**gdzie $s$ jest nachyleniem stycznej do krzywej w punkcie $P$;**

$$x_R = s^2 - 2x_P \bmod p;$$

$$y_R = -y_P + s(x_P - x_R) \bmod p.$$

**Przykłady krzywych eliptycznych nad $F_{23}$**

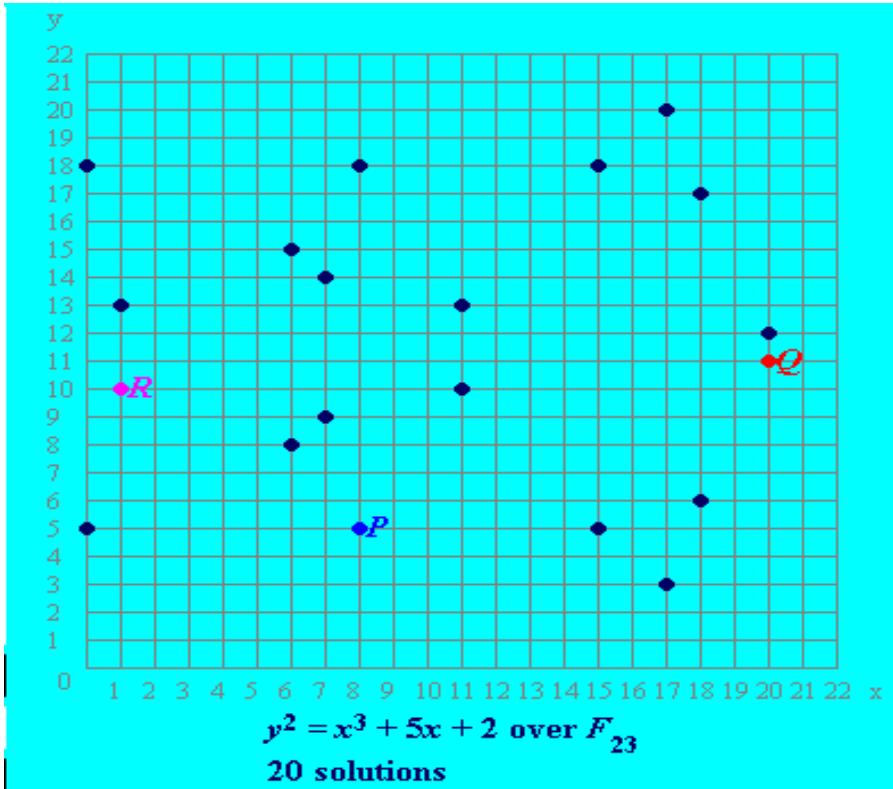



Źródło: http://www.certicom.com/index.php/ecc-tutorial

# GRUPY PUNKTÓW NA KRZYWYCH ELIPTYCZNYCH NAD $F_p$ (3/4)

## Przykład dodawania punktów krzywej eliptycznej nad $F_{23}$




$P$ (8, 5)
$Q$ (20, 11)
$R$ (1, 10)

$l = (y_P - y_Q) * (x_P - x_Q)^{-1} \bmod p$
$= -6 * (-12)^{-1} \bmod 23$
$= 17 * 11^{-1} \bmod 23$
$= 17 * 21 \bmod 23$
$= 12$

$x_R = l^2 - x_P - x_Q \bmod p$
$= 144 - 8 - 20 \bmod 23$
$= 1$

$y_R = -y_P + l * (x_P - x_R) \bmod p$
$= -5 + 12 * (8 - 1) \bmod 23$
$= 18 + 12 * 7 \bmod 23$
$= 18 + 15 \bmod 23$
$= 10$

$P + Q = R = (1, 10)$.

Źródło: http://www.certicom.com/index.php/ecc-tutorial

# GRUPY PUNKTÓW NA KRZYWYCH ELIPTYCZNYCH NAD $F_p$ (4/4)

## Przykładowe praktycznie zalecane wartości parametrów dla krzywych eliptycznych nad $F_p$ (FIPS 186-2)

P-224: $p = 2^{224} - 2^{96} + 1$, $a = -3$, $h = 1$

```
S = 0x BD713447 99D5C7FC DC45B59F A3B9AB8F 6A948BC5
r = 0x 5B056C7E 11DD68F4 0469EE7F 3C7A7D74 F7D12111 6506D031 218291FB
b = 0x B4050A85 0C04B3AB F5413256 5044B0B7 D7BFD8BA 270B3943 2355FFB4
n = 0x FFFFFFFF FFFFFFFF FFFFFFFF FFFF16A2 E0B8F03E 13DD2945 5C5C2A3D
x = 0x B70E0CBD 6BB4BF7F 321390B9 4A03C1D3 56C21122 343280D6 115C1D21
y = 0x BD376388 B5F723FB 4C22DFE6 CD4375A0 5A074764 44D58199 85007E34
```

P-256: $p = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$, $a = -3$, $h = 1$

```
S = 0x C49D3608 86E70493 6A6678E1 139D26B7 819F7E90
r = 0x 7EFBA166 2985BE94 03CB055C 75D4F7E0 CE8D84A9 C5114ABC AF317768 0104FA0D
b = 0x 5AC635D8 AA3A93E7 B3EBBD55 769886BC 651D06B0 CC53B0F6 3BCE3C3E 27D2604B
n = 0x FFFFFFFF 00000000 FFFFFFFF FFFFFFFF BCE6FAAD A7179E84 F3B9CAC2 FC632551
x = 0x 6B17D1F2 E12C4247 F8BCE6E5 63A440F2 77037D81 2DEB33A0 F4A13945 D898C296
y = 0x 4FE342E2 FE1A7F9B 8EE7EB4A 7C0F9E16 2BCE3357 6B315ECE CBB64068 37BF51F5
```

P-384: $p = 2^{384} - 2^{128} - 2^{96} + 2^{32} - 1$, $a = -3$, $h = 1$

```
S = 0x A335926A A319A27A 1D00896A 6773A482 7ACDAC73
r = 0x 79D1E655 F868F02F FF48DCDE E14151DD B80643C1 406D0CA1 0DFE6FC5 2009540A
      495E8042 EA5F744F 6E184667 CC722483
b = 0x B3312FA7 E23EE7E4 988E056B E3F82D19 181D9C6E FE814112 0314088F 5013875A
      C656398D 8A2ED19D 2A85C8ED D3EC2AEF
n = 0x FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF C7634D81 F4372DDF
      581A0DB2 48B0A77A ECEC196A CCC52973
x = 0x AA87CA22 BE8B0537 8EB1C71E F320AD74 6E1D3B62 8BA79B98 59F741E0 82542A38
      5502F25D BF55296C 3A545E38 72760AB7
y = 0x 3617DE4A 96262C6F 5D9E98BF 9292DC29 F8F41DBD 289A147C E9DA3113 B5F0B8C0
      0A60B1CE 1D7E819D 7A431D7C 90EA0E5F
```

- ***p* - liczba pierwsza określająca ciało $F_p$;**
- ***S* – losowe „ziarno” wykorzystywane do generowania współczynników krzywej eliptycznej (zgodnie z algorytmem przedstawionym w ANSI X9.62);**
- ***r* – „wyjście” *SHA-1* (zgodnie z tym samym algorytmem, co powyżej);**
- ***a*,*b* – współczynniki krzywej eliptycznej $y^2 = x^3+ax+b$, przy czym $rb^2 \equiv a^3 (\mathrm{mod}\ p)$;**
- ***n* – rząd (liczba pierwsza) punktu bazowego *P*;**
- ***h* - kofaktor;**
- ***x*, *y* – współrzędne punktu *P*.**

# GRUPY PUNKTÓW NA KRZYWYCH ELIPTYCZNYCH NAD $F_2^m$ (1/3)

Grupy te, to zbiory punktów $P = (x, y)$ spełniających równanie:

$$y^2 + xy = x^3 + ax^2 + b \qquad (x, y, a, b \in F_2^m, b \neq 0),$$

oraz punkt $O$ „w nieskończoności”.

Istnieją dwie formy reprezentacji punktów na takich krzywych: wielomianowa i za pomocą optymalnej bazy normalnej.

Punktem „przeciwnym” do punktu $P = (x, y)$ jest punkt $(x, x + y)$.

Współrzędne punktu $R = P + Q$, gdzie $P \neq Q$ i $P \neq -Q$, a ponadto oba punkty są różne od punktu $O$, określane są następująco:

$$s = (y_P - y_Q)(x_P + x_Q)^{-1},$$

gdzie $s$ jest nachyleniem prostej łączącej punkty $P$ i $Q$;

$$x_R = s^2 + s + x_P + x_Q + a;$$
$$y_R = s(x_P + x_R) + x_R + y_P.$$

# GRUPY PUNKTÓW NA KRZYWYCH ELIPTYCZNYCH NAD $F_2^m$ (2/3)

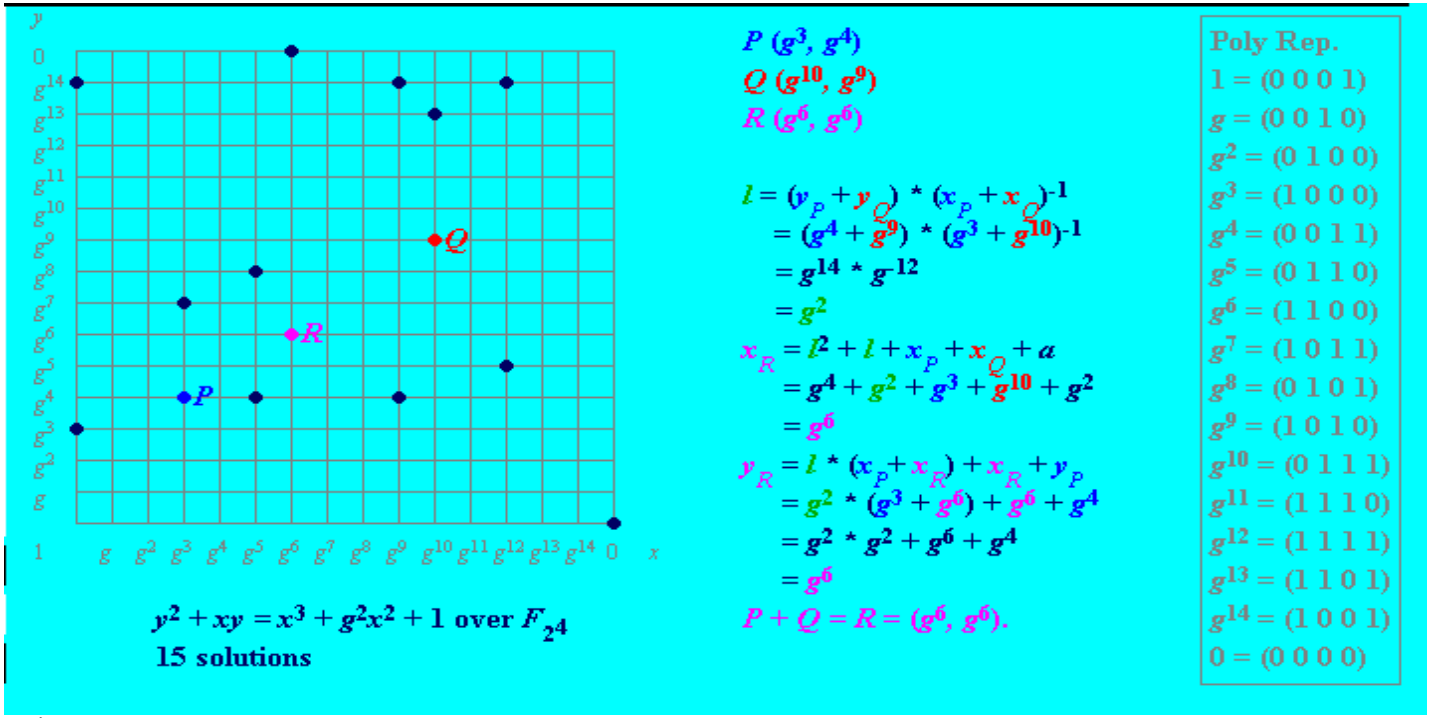
**Współrzędne punktu $R = 2P$, gdy $P \neq O$, określane są następująco:**

$$s = x_P + y_P(x_P)^{-1},$$

**gdzie $s$ jest nachyleniem stycznej do krzywej w punkcie $P$;**

$$x_R = s^2 + s + a;$$

$$y_R = x_P^2 + (s + 1)\, x_R.$$




**Przykład krzywej eliptycznej nad $F_2^4$**

***UWAGA: osie „wyskalowane” w potęgach generatora grupy multiplikatywnej ciała $F_2^4$***

Źródło: http://www.certicom.com/index.php/ecc-tutorial

# GRUPY PUNKTÓW NA KRZYWYCH ELIPTYCZNYCH NAD $F_2^m$ (3/3)

## Przykładowe praktycznie zalecane wartości parametrów dla krzywych eliptycznych nad $F_2^m$ (FIPS 186-2)

B-163: $m = 163$, $f(z) = z^{163} + z^7 + z^6 + z^3 + 1$, $a = 1$, $h = 2$

```
S = 0x 85E25BFE 5C86226C DB12016F 7553F9D0 E693A268
b = 0x 00000002 0A601907 B8C953CA 1481EB10 512F7874 4A3205FD
n = 0x 00000004 00000000 00000000 000292FE 77E70C12 A4234C33
x = 0x 00000003 F0EBA162 86A2D57E A0991168 D4994637 E8343E36
y = 0x 00000000 D51FBC6C 71A0094F A2CDD545 B11C5C0C 797324F1
```

B-233: $m = 233$, $f(z) = z^{233} + z^{74} + 1$, $a = 1$, $h = 2$

```
S = 0x 74D59FF0 7F6B413D 0EA14B34 4B20A2DB 049B50C3
b = 0x 00000066 647EDE6C 332C7F8C 0923BB58 213B333B 20E9CE42 81FE115F 7D8F90AD
n = 0x 00000100 00000000 00000000 00000000 0013E974 E72F8A69 22031D26 03CFE0D7
x = 0x 000000FA C9DFCBAC 8313BB21 39F1BB75 5FEF65BC 391F8B36 F8F8EB73 71FD558B
y = 0x 00000100 6A08A419 03350678 E58528BE BF8A0BEF F867A7CA 36716F7E 01F81052
```

B-283: $m = 283$, $f(z) = z^{283} + z^{12} + z^7 + z^5 + 1$, $a = 1$, $h = 2$

```
S = 0x 77E2B073 70EB0F83 2A6DD5B6 2DFC88CD 06BB84BE
b = 0x 027B680A C8B8596D A5A4AF8A 19A0303F CA97FD76 45309FA2 A581485A F6263E31
       3B79A2F5
n = 0x 03FFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFEF90 399660FC 938A9016 5B042A7C
       EFADB307
x = 0x 05F93925 8DB7DD90 E1934F8C 70B0DFEC 2EED25B8 557EAC9C 80E2E198 F8CDBECD
       86B12053
y = 0x 03676854 FE24141C B98FE6D4 B20D02B4 516FF702 350EDDB0 826779C8 13F0DF45
       BE8112F4
```

B-409: $m = 409$, $f(z) = z^{409} + z^{87} + 1$, $a = 1$, $h = 2$

```
S = 0x 4099B5A4 57F9D69F 79213D09 4C4BCD4D 4262210B
b = 0x 0021A5C2 C8EE9FEB 5C4B9A75 3B7B476B 7FD6422E F1F3DD67 4761FA99 D6AC27C8
       A9A197B2 72822F6C D57A55AA 4F50AE31 7B13545F
n = 0x 01000000 00000000 00000000 00000000 00000000 00000000 000001E2 AAD6A612
       F33307BE 5FA47C3C 9E052F83 8164CD37 D9A21173
x = 0x 015D4860 D088DDB3 496B0C60 64756260 441CDE4A F1771D4D B01FFE5B 34E59703
       DC255A86 8A118051 5603AEAB 60794E54 BB7996A7
y = 0x 0061B1CF AB6BE5F3 2BBFA783 24ED106A 7636B9C5 A7BD198D 0158AA4F 5488D08F
       38514F1F DF4B4F40 D2181B36 81C364BA 0273C706
```

- *m – stopień „rozszerzenia” ciała $F_2^m$;*
- *f (z) – wielomian „redukujący” stopnia m ;*
- *a,b – współczynniki krzywej eliptycznej $y^2 + xy = x^3 + ax^2 + b$;*
- *n – rząd (liczba pierwsza) punktu bazowego P;*
- *h - kofaktor;*
- *x, y – współrzędne punktu P.*

# ALGORYTMY PODPISU DSA I ECDSA (1/2)

## *Digital Signature Standard - DSS*
## *(National Institute of Standards and Technology - NIST - 1991 r.)*

*Generowanie kluczy:*

Podmiot *A* wybiera :

- liczbę pierwszą *q* , mającą ok. *160 bitów* (tak, jak wartości funkcji *SHA-1*);
- liczbę pierwszą $p \equiv 1 \pmod 4$ , o długości od *512* do*1024 bitów;*
  (obecnie sugerowana jest długość ok. *1024 bitów* oraz „dłuższe" funkcje skrótu: *SHA-256, SHA-384, SHA-512*, również *q* musi być wtedy odpowiednio większa)
- generator *g* rzędu *q* jedynej podgrupy cyklicznej grupy $\mathbb{Z}^*_p$ taki, że:

$$g^{(p-1)/q} \bmod p \neq 1;$$

(wynika to ze znanych ataków na system podpisu ElGamala)

- losową liczbę $x$ $(0 < x < q)$, która będzie jego *kluczem prywatnym*, *kluczem publicznym* jest wtedy liczba $y \equiv g^x \pmod p$ oraz *g*, *q* i *p*.

## *Elliptic Curve Digital Signature Algorithm - EC-DSA*

*Generowanie kluczy:*

Podmiot *A* wybiera :

- krzywą eliptyczną *E* zdefiniowaną nad $\mathbb{Z}_p$, gdzie *p* jest liczbą pierwszą; liczba punktów $E(\mathbb{Z}_p)$ powinna być podzielna przez dużą liczbę pierwszą *n;*
- punkt *P* rzędu *n* należący do *E;*
- unikalną i „nieprzewidywalną" losową liczbę *d* należącą do $\mathbb{Z}^*_p$;
- oblicza punkt $Q=dP$; *kluczem prywatnym* jest liczba *d* ; *kluczem publicznym* są *E*, *P*, *Q* i *n*.

# ALGORYTMY PODPISU DSA I ECDSA (2/2)

*Podpisywanie :*

- przekształca się wiadomość jawną *m* przez funkcję skrótu (*SHA-x*), uzyskując :

$$0 < h = f(m) < q;$$

- wybiera się pewną liczbę losową $k$ ( $0 < k < q$) i oblicza:

$$r = [g^{k} \bmod p\,] \bmod q;$$

- wyznacza się liczbę:

$$s = [k^{-1}( h + x\,r)] \bmod q;$$

Podpisem jest para $(r, s)$, a odbiorcy wysyła się $(m, h, r, s)$.

*Weryfikacja podpisu:*

- oblicza się dwie wielkości :

$$u_1 = s^{-1}\, h \bmod q \quad \text{i} \quad u_2 = s^{-1}\, r \bmod q;$$

- jeżeli $[g^{u_1} y^{u_2} \bmod p \equiv r\,] \bmod q$ to uznaje się autentyczność podpisu.

*Podpisywanie:*

- przekształca się wiadomość jawną *m* przez funkcję skrótu, uzyskując :

$$h = SHA\text{-}x(m);$$

- wybiera się unikalną i „nieprzewidywalną" losową liczbę losową $k$ ( $0 < k < n - 1$) i oblicza punkt $kP = (x1, y1)$ oraz liczbę:

$$r = x1 \bmod n \quad (r \neq 0);$$

- wyznacza się liczbę $s = [k^{-1}( h + d\,r)] \bmod n \quad (s \neq 0)$;

Podpisem jest para $(r, s)$, a odbiorcy wysyła się $(m, h, r, s)$.

*Weryfikacja podpisu:*

- oblicza się dwie wielkości : $u_1 = s^{-1}\, h \bmod q$ i $u_2 = s^{-1}\, r \bmod q$;
- wyznacza punkt $u_1P + u_2Q = (x0, y0)$ oraz liczbę $v = x0 \bmod n$; jeżeli $r = v$ , to uznaje się autentyczność podpisu.

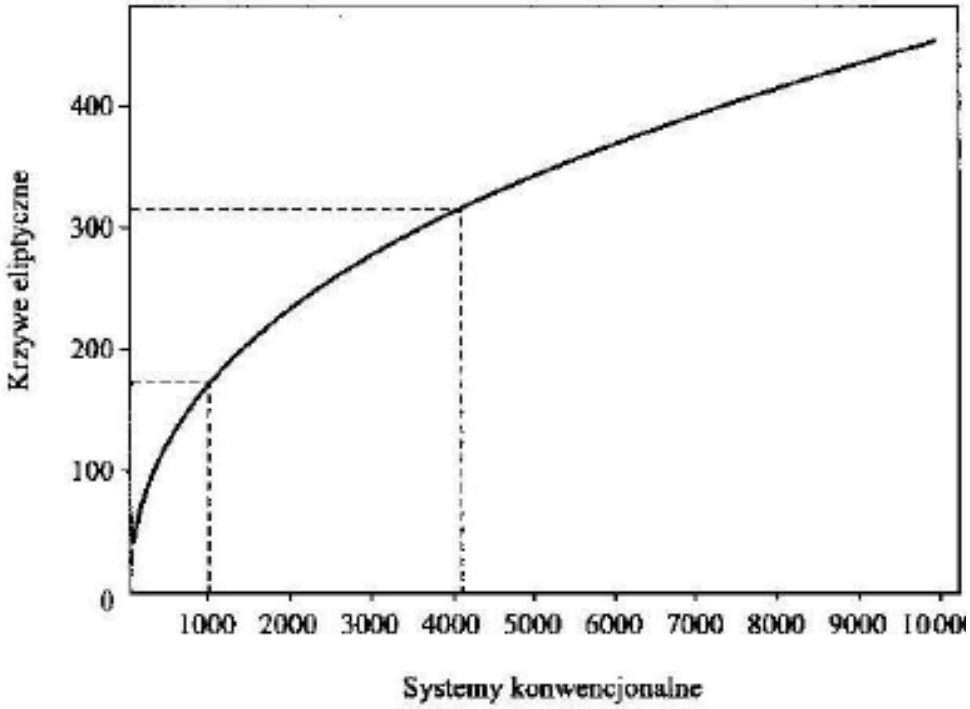
# Porównanie siły algorytmów w zależności od parametrów (1/2)

*(Darrel Hankerson, Alfred Menezes, Scott Vanstone - Guide to Elliptic Curve Cryptography)*

| | Poziom bezpieczeństwa (bity) | | | | |
|---|---|---|---|---|---|
| | 80 (SKIPJACK) | 112 (3DES) | 128 (AES-128) | 192 (AES-192) | 256 (AES-256) |
| Parametr *q* DL | 160 | 224 | 256 | 384 | 512 |
| Parametr *n* EC | 160 | 224 | 256 | 384 | 512 |
| Moduł *n* RSA | 1024 | 2048 | 3072 | 8192 | 15360 |
| Moduł *p* DL | 1024 | 2048 | 3072 | 8192 | 15360 |

# Porównanie siły algorytmów w zależności od parametrów (2/2)

*(Ian Blake, Gadiel Seroussi, Nigel Smart - Krzywe eliptyczne w kryptografii)*




**1024 bity „konwencjonalne" – 173 bity „eliptyczne"**

**4096 bitów „konwencjonalnych" – 313 bitów „eliptycznych"**

# „BEZPIECZNE” KRZYWE ELIPTYCZNE

**W wielu różnych normach *de facto* i *de jure* zaleca się zestaw krzywych eliptycznych „godnych zastosowania” w ECC, np.:**

- ANSI X9.62 (1999)
- IEEE P1363 (2000)
- SEC 2 (2000)
- NIST FIPS 186-2 (2000)
- ANSI X9.63 (2001)
- Brainpool – RFC 5639 (2005)
- NSA Suite B (2005)
- ANSSI FRP256V1 (2011)

**Głównym celem „selekcjonerów” było zapewnienie, że na wskazanych krzywych problem wyznaczania logarytmu dyskretnego (ECDLP) jest trudnym problemem obliczeniowym.**

Użyteczny link: https://safecurves.cr.yp.to

# „BEZPIECZNE” KRZYWE ELIPTYCZNE (cd.)

**Istnieje jednak „subtelna” różnica między trudnością ECDLP a bezpieczeństwem ECC.**

**Istnieje wiele ataków, które łamią realnie implementowane ECC bez rozwiązywania ECDLP. Podstawowym problemem jest to, że implementując zalecane w tych normach krzywe nie uwzględnia się faktu, że implementacja może:**

- **nieprawidłowo realizować obliczenia dla niektórych punktów na krzywych eliptycznych;**
- **powodować „wyciek” tajnych danych, gdy dane wejściowe nie są punktami krzywej;**
- **być podatna na „side-channels-attacks” (timing attacks, SPA, DPA, fault introduction/induction attacks, itp.);**
- **powodować „wyciek” tajnych danych z pamięci podręcznej (cache).**

# „BEZPIECZNE” KRZYWE ELIPTYCZNE (cd.)

| | | Parameters: | | | ECDLP security: | | | | ECC security: | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Curve | Safe? | field | equation | base | rho | transfer | disc | rigid | ladder | twist | complete | ind |
| Anomalous | False | True✓ | True✓ | True✓ | True✓ | False | False | True✓ | False | False | False | False |
| M-221 | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ |
| E-222 | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ |
| NIST P-224 | False | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | False | False | False | False | False |
| Curve1174 | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ |
| Curve25519 | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ |
| BN(2,254) | False | True✓ | True✓ | True✓ | True✓ | False | False | True✓ | False | False | False | False |
| brainpoolP256t1 | False | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | False | False | False | False |
| ANSSI FRP256v1 | False | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | False | False | False | False | False |
| NIST P-256 | False | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | False | False | True✓ | False | False |
| secp256k1 | False | True✓ | True✓ | True✓ | True✓ | True✓ | False | True✓ | False | True✓ | False | False |
| E-382 | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ |
| M-383 | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ |
| Curve383187 | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ |

Źródło: https://safecurves.cr.yp.to

# ODWZOROWANIA DWULINIOWE - PAIRINGS (1/8)

**Niech n będzie liczbą pierwszą, $G_1$ i $G_2$ addytywnymi grupami przemiennymi rzędu n, zaś $G_3$ multiplikatywną grupą cykliczną rzędu n.**
**Odwzorowanie dwuliniowe/biliniowe (*pairing*):**

$$e: G_1 \times G_2 \rightarrow G_3$$

**jest odwzorowaniem o niżej wymienionych własnościach.**

## Dwuliniowość (*Bilinearity*):

$$e(P+P',Q) = e(P,Q)e(P',Q) \qquad \forall \; P,P' \in G_1, Q \in G_2$$

$$e(P,Q+Q') = e(P,Q)e(P,Q') \qquad \forall \; P \in G_1, \; Q,Q' \in G_2$$

## Niezdegenerowanie (*Non-Degeneracy*):

$$\forall \quad P \neq O \quad \wedge \quad P \in G_1, \qquad \exists \; Q \in G_2 \; : \qquad e(P,Q) \neq 1.$$

$$\forall \quad Q \neq O \quad \wedge \quad Q \in G_2, \qquad \exists \; P \in G_1 \; : \qquad e(P,Q) \neq 1.$$

Based on: Dustin Moody (NIST) - An Introduction to Pairing Based Cryptography (PBC)

# ODWZOROWANIA DWULINIOWE - PAIRINGS (2/8)

1) $e(P,0) = e(0,Q) = 1$

2) $e(-P,Q) = e(P,Q)^{-1} = e(P,-Q)$

3) $e([a]P,Q) = e(P,Q)^{a} = e(P,[a]Q) \qquad \forall \quad a \in \mathbf{Z}$

4) $e([a]P,[b]Q) = e(P,Q)^{ab} \qquad \forall \quad a,b \in \mathbf{Z}$

**$Z$ – zbiór liczb całkowitych**

**$[x]P$ – ($x$-1)-krotne „dodawanie do siebie" elementu $P$**

**$R^{y}$ - ($y$-1)-krotne „mnożenie przez siebie" elementu $R$**

Based on: Dustin Moody (NIST) - An Introduction to Pairing Based Cryptography (PBC)

# ODWZOROWANIA DWULINIOWE - PAIRINGS (3/8)

## Wykorzystanie addytywnych grup punktów na krzywych eliptycznych do konstrukcji odwzorowań dwuliniowych

Niech ***E*** będzie krzywą eliptyczną nad $F_q$.

Niech ***P*** będzie ustalonym punktem rzędu ***n*** na tej krzywej, (***n*** jest liczbą pierwszą).

Niech ***k*** będzie rzędem ***q*** mod ***n***.

Wtedy ***k*** jest także najmniejszą liczbą całkowitą spełniającą warunek $n \mid (q^k - 1)$.

***k*** jest nazywane stopniem osadzenia (*embedding degree*).

Odwzorowanie dwuliniowe będzie miało postać:

$$e : \langle P \rangle \times \langle P \rangle \rightarrow \mu_n \subseteq F_{q^k}^*$$

Ponadto wymaga się, by $e(P,P) \neq 1$.

Based on: Dustin Moody (NIST) - An Introduction to Pairing Based Cryptography (PBC)

# ODWZOROWANIA DWULINIOWE - PAIRINGS (4/8)

## Wykorzystanie addytywnych grup punktów na krzywych eliptycznych do konstrukcji odwzorowań dwuliniowych (cd.)

**Przykładami odwzorowań dwuliniowych na krzywych eliptycznych są np. iloczyn Weil'a i iloczyn Tate'a.**

**Przy założeniu, że stopień osadzenia $k$ jest mały, oba odwzorowania są łatwo obliczalne.**

**Dla losowych krzywych eliptycznych wykorzystywanych w „klasycznej" kryptografii stopień osadzenia $k \approx n$, czyli stanowczo zbyt duży.**

**Twierdzenie: Jeżeli $E$ jest supersingularną krzywą eliptyczną, to stopień osadzenia $k \leq 6$.**

Based on: Dustin Moody (NIST) - An Introduction to Pairing Based Cryptography (PBC)

# ODWZOROWANIA DWULINIOWE - PAIRINGS (5/8)

## Wykorzystanie addytywnych grup punktów na krzywych eliptycznych do konstrukcji odwzorowań dwuliniowych (cd.)

### „Kamienie milowe”

**1988**

**Burt Kaliski w swojej pracy doktorskiej zastosował iloczyn Weila’a do konstrukcji generatora pseudolosowych ciągów binarnych.**

**1993**

**Alfred Menezes, Tatsuaki Okamoto i Scott Vanstone zastosowali iloczyn Weil’a sprowadzając atak na logarytm dyskretny na krzywych eliptycznych do ataku na logarytm dyskretny w grupie multiplikatywnej ciała GF($p^k$).**

**Najlepsze algorytmy dla krzywych eliptycznych- O($\sqrt{n}$ ).**

**Najlepsze dla GF() – subwykładnicze (index calculus).**

Based on: Dustin Moody (NIST) - An Introduction to Pairing Based Cryptography (PBC)

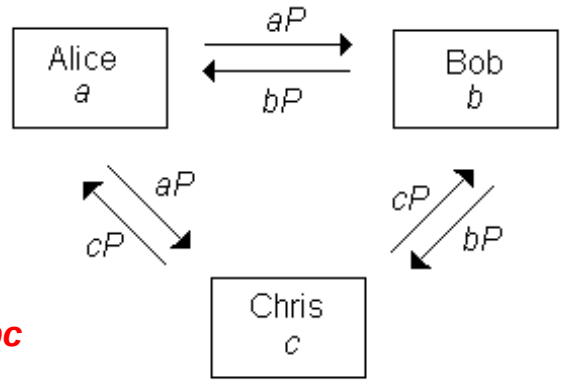
# ODWZOROWANIA DWULINIOWE - PAIRINGS (6/8)

## Wykorzystanie addytywnych grup punktów na krzywych eliptycznych do konstrukcji odwzorowań dwuliniowych (cd.)

### „Kamienie milowe”

**2000**

**Antoine Joux przedstawił trójstronny jednoprzebiegowy protokół uzgadniania sekretu.**




1) Alice wysyła $[a]P$ do Boba i Chrisa
2) Bob wysyła $[b]P$ do Alice i Chrisa
3) Chris wysyła $[c]P$ do Alice i Boba
4) Wszyscy mogą obliczyć klucz $e(P,P)^{abc}$

   (Na przykład: Alice oblicza $e([b]P,[c]P)^{a}$)

Based on: Dustin Moody (NIST) - An Introduction to Pairing Based Cryptography (PBC)

# ODWZOROWANIA DWULINIOWE - PAIRINGS (7/8)

## Wykorzystanie addytywnych grup punktów na krzywych eliptycznych do konstrukcji odwzorowań dwuliniowych (cd.)

### „Kamienie milowe”

**2001**

**Dan Boneh, Ben Lynn i Hovav Schacham przedstawiają schemat krótkich podpisów cyfrowych.**

**Parametry: *E*,*e*,*P* oraz funkcja skrótu** $H_1 : \{0,1\}^m \to \langle P \rangle$ .

**„Setup”: Kluczem prywatnym jest liczba całkowita *r*.**

**Kluczem publicznym jest *R* = [*r*]*P*.**

**Podpisywanie wiadomości M: *S* =[*r*]$H_1$(M).**

**Weryfikacja podpisu: sprawdzenie, czy *e*(*P*, *S*) = *e*(*R*,$H_1$(M)).**

**Uzasadnienie poprawności weryfikacji:**

***e*(*P*, *S*) = *e*(*P*, [*r*]$H_1$(M)) = *e*([*r*]*P*,$H_1$(M)) = *e*(*R*,$H_1$(M)).**

Based on: Dustin Moody (NIST) - An Introduction to Pairing Based Cryptography (PBC)

# ODWZOROWANIA DWULINIOWE - PAIRINGS (8/8)

## Wykorzystanie addytywnych grup punktów na krzywych eliptycznych do konstrukcji odwzorowań dwuliniowych (cd.)

### „Kamienie milowe”

**2001**

**Dan Boneh i Franklin przedstawiają schemat szyfrowania oparty na tożsamości (IBE – Identity Based Encryption).**

**Parametry: *E*, *P*, *e* i dwie funkcje skrótu:** $H_1 : \{0,1\}^m \rightarrow < P >$

$H_2 : \mathrm{F}_{q^k} \rightarrow \{0,1\}^m$

**„Setup”: Klucz publiczny Alice $K_A = H_1(ID_A)$.**

**TA (Trusted Authority) ma klucz prywatny *s* i klucz publiczny $S=[s]P$.**

**TA przekazuje Alice jej tajny klucz deszyfrujący $D_A = [s]K_A$.**

**Szyfrowanie: W celu zaszyfrowania wiadomości M Bob wybiera losową wartość *r* i oblicza $R = [r]P$ oraz $c = M \oplus H_2(e(K_A, S)^r)$. Wysyła Alice $(R, c)$.**

**Deszyfrowanie: Alice wykorzystując swój klucz prywatny $D_A$ oblicza**

$$c \oplus H_2(e(D_A,R)) = c \oplus H_2(e([s]K_A, [r]P)) = c \oplus H_2(e(K_A, S)^r) = M.$$

Based on: Dustin Moody (NIST) - An Introduction to Pairing Based Cryptography (PBC)

# Koniec części 6