SKRYPT
SYSTEMY KRYPTOGRAFICZNE

Wykonali:
Jakub Paluch
Tomasz Zalewski

Spis Treści:

1. Podstawowe pojęcia algebraiczne

Z – zbiór liczb całkowitych
Z^* - zbiór liczb całkowitych dodatnich (bez zera)
Z_0^* – zbiór liczb całkowitych dodatnich z zerem
Q – zbiór liczb wymiernych

1.1 Grupa

Jest to pewna struktura algebraiczna (zbiór z wyszczególnionym działaniem i elementem neutralnym)

$$(G,*,e) = (G,\bullet,1)$$

Gdzie:
G – zbiór
* - działanie
E – element neutralny, zazwyczaj oznaczamy przez 1

Aksjomaty, które spełnia Grupa:
1) łączność, np. a*(b*c)=(a*b)*c
2) a*1 = 1*a = a
3) $\forall_{a \in G} \exists_{a' \in G} \longrightarrow (a * a' = 1)$
4) Grupa jest abelowa (przemienna) jeśli a * b = b * a dla każdego a i b $\in$ G.

Grupą multiplikatywną nazywamy grupę G z działaniem mnożenia ($\bullet$) i elementem neutralnym 1.

Grupą addytywną nazywamy grupę G z działaniem (+) i elementem neutralnym 0.

Przykłady:

$$G=(Z,+,0)$$
$$G=(Z \setminus \{0\},\bullet,1)$$

1.2 Pierścień

P=(P,+, $\bullet$;0,1)
Klasy aksjomatów spełniane przez pierścień:
1) P z działaniem + i elementem 0 to grupa abelowa (warunki 1-4)
2) P z działaniem * i elementem 1 spełnia warunki 1,2 i 4
3) Rozdzielność dodawania względem mnożenia

$$\forall_{a,b,c\in P} a*(b+c) = a*b + a*c$$

Strukturę spełniającą te trzy klasy warunków nazywana jest **Pierścieniem przemiennym z jedynką**.

Neutralny element grupy multiplikatywnej nazywamy jedynką pierścienia.
Neutralny element grupy addytywnej nazywamy zerem pierścienia.

Przykład:
(pierścień wielomianów naz Z):

P=(Z [x],+,*,0,1)

1.3 Ciało

Jest to pierścień spełniający dodatkowy warunek:
Dla każdego niezerowego elementu a z ciała K istnieje element a' również należący do K, taki, że a * a'=1 tzn. każdy niezerowy element tego ciała posiada element odwrotny.

Przykład:

K = (Q,+,*,0,1)

Def.
Pierścień P nazywamy Dziedziną Całkowitości wtedy i tylko wtedy gdy zachodzi warunek

$$\forall_{a,b\in P} a*b = 0 \Rightarrow a = 0 \vee b = 0$$

(tzn. nie zawiera nietrywialnych dzielników zera).

1.4 Relacja podzielności (|) w dziedzinie całkowitości.

$$a \mid b \Rightarrow \exists_{c\in P} a*c = b \quad \text{(a dzieli b)}$$

Własności relacji podzielności:
1) zwrotność i przechodniość
2) $a \mid b \Rightarrow \forall_c a*c \vee b*c$
3) $a \mid b \wedge a \mid c \Rightarrow a \mid b*u + c*v \forall_{c,v\in P}$

4) Jeśli a dzieli 1 to element a jest odwracalny
5) Jeśli 0 dzieli a to ten element musi być równy 0

Def.

Elementy niezerowe a oraz b, należące do pierścienia P nazywamy **stowarzyszonymi** wtedy i tylko wtedy gdy a dzieli b oraz b dzieli a.

Wniosek:

Elementy są stowarzyszone wtedy i tylko wtedy gdy różnią się o element odwracalnym tzn.

$$\exists_{u \in P} a = u * b$$

Dowód:

$$a \mid b \wedge b \mid a \Rightarrow \exists_{c_1, c_2 \in P} a * c1 = b \wedge b * c2 = a \Rightarrow a * c1 * c2 = a$$

$$a * (c_1 * c_2 - 1) = 0$$

$$(c_1 * c_2 - 1) = 0$$

Zatem $c_1 * c_2 = 1$ z czego wynika, że c_1 oraz c_2 są elementami odwracalnymi.

Stowarzyszonym z 0 jest tylko 0, natomiast z 1 wszystkie elementy odwracalne pierścienia P.

Def.

Element a należący do pierścienia P, który nie jest stowarzyszony ani z 0 ani z 1 nazywamy nierozkładalnym wtedy i tylko wtedy gdy każdy dzielnik jest stowarzyszony z 1 lub nim samym.

Def.

Element a należący do pierścienia P nazywamy pierwszym wtedy i tylko wtedy gdy:

$$\forall_{a,b} a \mid b * c \Rightarrow a \mid b \vee a \mid c$$

I element a nie jest stowarzyszony z 0 ani 1.

Wniosek:

W dowolnej dziedzinie całkowitości P, każdy element pierwszy jest nierozkładalny.

Dowód:

Gdyby p$\in$ P był rozkładem to p = ab | ab skąd ab | a lub ab | b i dalej b | 1 lub a | 1 co jest niemożliwe.

Def.

Dziedzinę całkowitości P nazywamy **Dziedziną z Jednoznacznością** Rozkładu (DJR) wtedy i tylko wtedy gdy:

1) każdy element rozkładalny jest iloczynem pewnej liczby elementów pierwszych
2) przedstawienie elementu rozkładalnego w postaci iloczynu elementów pierwszych jest jednoznaczne z dokładnością do porządku i stowarzyszenia.

Przykład:

(Z,+,• ,1,0)

6 = 2*3 = 3*2
6 = (-2)*(-3) ale -1 jest stowarzyszone z 1.

Tw.

Jeśli P jest Dziedziną z Jednoznacznością Rozkładu to P[x] też jest Dziedziną z jednoznacznością Rozkładu.

Wniosek:

Każdy wielomian unormowany o współczynnikach całkowitych można przedstawić w postaci iloczynu unormowanych wielomianów nierozkładalnych nad Z.

Def.

Największym Wspólnym Dzielnikiem elementów a oraz b należących do pierścienia P jest taki element d należący do P że:

1) $d \mid a \wedge d \mid b$
2) $\forall_c c \mid a \wedge c \mid b \Rightarrow c \mid d$

Def.

Najmniejszą Wspólną Wielokrotnością elementów a oraz b należących do pierścienia P jest taki element m należący do P że:

1) $a \mid m \wedge b \mid m$
2) $\forall_c a \mid c \wedge b \mid c \Rightarrow m \mid c$

1.5 Relacja prostopadłości ($\perp$) w DJR

Niech P – dziedzina z jednoznacznością rozkładu, f,g $\in$ P.

Def.

Powiemy, że f jest prostopadłe do g (f$\perp$ g) wtedy i tylko wtedy gdy NWD (f,g) = 1

Własność 1:

h$\perp$ f * g $\Leftrightarrow$ h$\perp$ f$\wedge$ h$\perp$ g

Dowód:

Implikacja „$\Rightarrow$ ” jest oczywista. Dla dowodu „$\Leftarrow$ ” załóżmy, że l$\neq$ h’=NWD(h, f * g)
Wtedy $h' \mid ih' \mid f * g$. Niech p będzie elementem pierwszym dzielących h’. Wtedy p | f lub p | g i w konsekwencji p | NWD(h,f) lub p | NWD(h,g) przeczy założeniu i tym samym kończy dowód.

Własność 2:

H | f * g $\wedge$ h $\perp$ f $\Rightarrow$ h | g

Dowód:

Niech $h = p_1^{\alpha_1} * \ldots * p_r^{\alpha_r}$ będzie rozkładem h na iloczyn elementów pierwszych.
Ponieważ h $\perp$ f więc $p_i^{\alpha_i} \mid g, i = 1,\ldots,r$ i w konsekwencji NWW

$$p_i^{\alpha_i} = \prod_i p_1^{\alpha_1} \mid g$$

Wprost z definicji wynikają następujące własności relacji podzielności i

prostopadłości:
- relacja podzielności jest relacją zwrotną, antysymetryczną i przechodnią, oraz spełnia następujący warunek:
Jeśli $(a,b) \in R$ i $a-k*b \neq 0$ to $(a,a-k*b \in R)$ dla dowolnego $k \in Z^+$
- relacja prostopadłości spełnia warunki dualne tzn. jest anty zwrotna, symetryczna, nieprzechodnia oraz spełnia warunek:
Jeśli $a < b$ i $(a,b) \in R$ to $(a,b \pm a) \in R$

Odwrotnie można powiedzieć, że powyższe warunki charakteryzują relacje podzielności („|”) i prostopadłości (jeśli R zawiera nietrywialną parę prostopadłą)

2. Pierścienie Euklidesa i struktura ilorazowa

2.1 Pierścień Euklidesa

Pierścieniem Euklidesowym nazywamy dziedzinie całkowitości R, w której zadane jest dzielenie z resztą (a przez $b \neq 0$) oraz norma $N:R \rightarrow N_0$ spełniająca warunki:

1) Dla każdego elementu $a \in R$ i $b \in R$ $(b \neq 0)$ istnieją elementy $q, r \in R$ takie, że $a = bq + r$, gdzie $N(r) < N(b)$ i norma spełnia warunki poniższe:
2) $N(a)=0 \Leftrightarrow a = 0$
3) $N(ab) = N(a)N(b)$

q – iloraz z dzielenia a przez b
r- reszta z dzielenia a przez b

Przykład:

$R = Z$ (klasyczny algorytm dzielenia z resztą)

Twierdzenie:

W pierścieniu euklidesowym R zachodzi równoważność

$$f \perp g \Leftrightarrow \exists_{a,b \in P} af + bg = 1$$

Dowód:

1) „$\Leftarrow$”
Wystarczy pokazać, że gdyby $f \not\perp g$ to nie zachodzi warunek
$af + bg = 1$

Zatem NWD(f,g)=h, gdzie h nie jest elementem odwracalnym.

Wtedy:
f = hf' i g = hg'
1 = af + bg = ahf' + bhg' = h(af' + bg')
Stąd h jest odwracalny a to przeczy założeniu.

3) „⇒ ”
NWD(f,g) = 1
$f = qg + r_1$ gdzie $N(r) < N(g)$
$g = g_1r_1 + r_2$
$r_1 = g_2r_2 + r_3$
…
$r_{k-1}=q_kr_k + r_{k+1}$
Skoro ciąg jest malejący to dojdzie do 0 i gdzieś się skończy
($r_k=0$, $N(r_{k-1})=0$)

Czytając od dołu:
$r_k = r_{k-2}-q_{k-1}r_{k-1}=r_{k-2}-q_{k-1}(r_{k-3}-q_{k-3}r_{k-2}) = r_{k-2}(1 - q_{k-1}q_{k-2}) + r_{k-3}(-q_{k-1})$

$NWD(r_i,r_{i+1})$ jest niezmiennicze
$NWD(f,g) = 1= \ldots = NWD(r_k,r_{k-1}) = NWD(r_k,q_kr_k) = r_k = 1$

Co więcej $r_k = \alpha\ r_{k-2} + \beta\ r_{k-1} = \alpha\ 'r_{k-3} + \beta\ 'r_{k-2} = \ldots = \alpha\ ''f + \beta\ ''g$

C.K.D.

Przykład:

R = Z N(a)=|a|
f=5,g=2
$\exists a,b \in Z : 5 * a + 2 * b = 1$
$5 = 2 * 2 + 1$
$1 = 5 * 2 * 2 = 5 * 1 + 2 * (-2) = 1 * f + (-2) * g^2$

Def.

Ideałem pierścienia R nazywamy grupę addytywną (R,+,0) spełniającą warunek:
Jeśli $a \in I$ to $ab \in I \forall\ b \in R$

Lemat:

W pierścieniu euklidesowym każdy ideał jest główny tzn. jest postaci:

I = (f) = { bf, b ∈ R }

Dowód:

Niech I ≠ 0 oraz g = I będzie elementem o minimalnej normie. Pokażemy , że I = (g).
Niech f ∈ I. Wystarczy zauważyć, że f=b*g dla pewnego b ∈ R, bo gdyby nie to f = g*q + r Nr < Ng to by przeczyło założeniu minimalności normy g.
C.K.D.

Def.

Idea I ⊂ R nazywamy maksymalnym wtedy i tylko wtedy, gdy zachodzi implikacja $\forall J(I \subset J \subset R \Rightarrow J = I \text{ lub } J = R$

Def.

I ⊂ R nazywamy głównym wtedy i tylko wtedy, gdy I = (x), dla pewnego x ∈ R. Pierścień w którym ideał jest główny nazywamy pierścieniem ideałów głównych (PIG)

Twierdzenie:

W pierścieniu euklidesowym każdy ideał pierwszy jest maksymalny.

Dowód:

R i PIG zatem I = (f) i f jest elementem pierwszym. Pokażemy, że (f) jest ideałem maksymalnym:
Niech (f) ⊂ J ⊂ R i niech g ∈ J : J = (g) zatem f = gq dla pewnego q ∈ R
Ponieważ f jest pierwszy, więc zachodzi implikacja:
f | gq ⇒ f | g lub f | q
f | g —→ (f) = (g) —→ (g) = J = (f)
f | q —→ (f) = (q) —→ (g) = R
C.K.D.

2.2 Grupa Jedności pierścienia (elementów odwracalnych pierścienia R)

Uwaga
Zbiór elementów odwracalnych pierścienia R ma strukturę grupy multiplikatywnej i

jest oznaczany R^*. nazywamy go grupą jedności pierścienia R.

2.3 Struktury ilorazowe

Def.
Odwzorowanie $\varphi : R_1 \to R_2$ nazywamy homomorfizmem pierścieni R_1 i R_2 wtedy i tylko wtedy gdy φ zachowuje działanie tj.

$$\varphi(a * b) = \varphi(a) * \varphi(b)$$

$$\forall_{a,b \in R_1} \varphi(a + b) = \varphi(a) + \varphi(b)$$

Jeśli φ jest wzajemnie jednoznaczne to φ nazywamy izomorfizmem pierścieni R_1 i R_2.
Jądrem homomorfizmu $\varphi : R_1 \to R_2$ nazywamy zbiór:
$\ker\varphi = \{a \in R_1 : \varphi(a) = 0\}$

Wniosek:

Jądro homomorfizmu $\varphi : R_1 \to R_2$ jest ideałem pierścienia R_1.

2.4 Pierścień ilorazowy

Niech I będzie ideałem pierścienia R. Definiujemy relację (równoważności) „~” na zbiorze R x R.
$a \sim b \Leftrightarrow a - b \in I$
Na klasach abstrakcji $[a]=[a]_\sim$ mamy dobrze określone działania:

$[a]_\sim + [b]_\sim := [a+b]_\sim$
$[a]_\sim * [b]_\sim := [a*b]_\sim$

Wtedy zbiór klas abstrakcji tako kreślonymi działaniami jest pierścieniem ilorazowym, który oznaczamy R/I

Twierdzenie 1 (o izomorfizmie):

Niech $\varphi : R_1 \to R_2$ będzie homomorfizmem pierścieni takim, że
$\varphi(R_1) = R_2$ .Wtedy pierścień ilorazowy $R_1/\ker\varphi$ jest izomorficzny z R_2

Def.

Niech R_1,R_2 – dowolne pierścienie przemienne z 1. Na produkcie kartezjańskim R

x R można zadać strukturę pierścienia w ten sposób, że działanie wykonujemy „po współrzędnych”

$$(a_1,b_2) + (a_2,b_2) = (a_1 + a_2, b_1 + b_2)$$
$$(a_1,b_2) * (a_2,b_2) = (a_1 * a_2, b_1 * b_2)$$

Z elementem neutralnym (0,0) i jednością (1,1). Taki pierścień oznaczać będziemy $R_1 \oplus R_2$.

2.5 Twierdzenie Chińskie

(R, +, •) – pierścień

Twierdzenie:

Jeśli $f \perp g$ to $\frac{R}{f * g} = \frac{R}{f} \oplus \frac{R}{g}$

Dowód:

Dla dowodu rozważymy homomorfizm pierścieni

$$\varphi : R \longrightarrow \frac{R}{f} \oplus \frac{R}{g}$$
$$\varphi\,(a(\mathrm{mod}\, f * g) : a(\mathrm{mod}\, f), a(\mathrm{mod}\, g))$$

Pokażemy, że ten homomorfizm jest izomorfizmem, tzn. że jądro $\ker\varphi$ jest trywialne ($\ker\varphi = 0$). Mamy:

$$\ker\varphi = \{a(\mathrm{mod}\, f * g) : a(\mathrm{mod}\, f) = 0 \wedge a(\mathrm{mod}\, g) = 0\} = \{a(\mathrm{mod}\, f * g) : f \mid a \wedge g \mid a\} =$$
$$= a(\mathrm{mod}\, f * g) : f * g \mid a = 0$$

Twierdzenie:

Jeśli $f \perp g$ to $(R|fg)^* = (R|f)^* \oplus (R|g)^*$

Dowód:

Dla dowodu rozważmy homomorfizm $\Phi^* : R^{\perp}_{fg} \longrightarrow R^{\perp}_{f} \oplus R^{\perp}_{g}$

$\Phi^*(a(\mathrm{mod}\, fg)) = (a(\mathrm{mod}\, f), a(\mathrm{mod}\, g))$

Ponieważ $h \perp fg \Leftrightarrow h \perp f$ i $h \perp g$ więc homomorfizm Φ^* jest dobrze określony i

jest izomorfizmem.

Fakt:

R – dziedzina całkowitości
I – element pierwszy
Wtedy R/I jest ciałem

Twierdzenie:

R – pierścień euklidesowy
P – element pierwszy
$(R|p)^*$ jest podgrupą grupy $(R|p^a)^*$

Dowód:

Ponieważ R|p jest ciałem więc grupa jedności $(R|p)^*$ jest generowana przez pewien element $a \in (R|p)^*$. Rozważamy homomorficzny naturalnie $R \to R|p$ i $R \to R|p^a$. Na mocy twierdzenia o izomorfizmie istnieje homomorfizm $h:R|p^a \to R|p$
I niech h* będzie jego obcięciem do odpowiednich grup jedności.

Niech $\bar{a}$ będzie przeciwobrazem a przy działaniu h należącym do $R|p^a$.

Wtedy rząd $\bar{a}$ jest wielokrotnością rzędu a. Zatem rząd $\bar{a}=k^*|(R|p)^*|$ w takim przypadku element $(\bar{a})^k$ generuje podgrup izomorficzną z grupą

$(R|p)^*$.

3. Pierścień funkcji wielomianowych na krzywej algebraicznej

W tym rozdziale przypomnimy definicje dziedziny całkowitości; dziedziny z jednoznacznością rozkładu, a następnie zdefiniujemy pojęcia ciała ułamków pierścienia oraz pierścienia lokalnego. W drugiej części pokażemy przykłady związane z krzywymi algebraicznymi.

R – pierścień przemienny z jedynką

Definicja:

R jest dziedziną całkowitości: wtt. gdy nie istnieją w nim właściwe dzielniki

zera. To znaczy , jeśli $a*b=0$ to $a=0$ lub $b=0$.

Wniosek:

Jeśli $a*b=a*c$ to $a=0$ lub $b=c$.

Definicja:

$a|b$ wtt. gdy $\underset{c\in R}{\exists} a*c=b$

W dalszym ciągu R^* będziemy oznaczać grupę elementów odwracalnych (grupa jedności) pierścienia R; tzn.

$R^*=\{a\in R: \underset{b\in R}{\exists} a*b=1\}$

Wniosek:

$d\in R^*$ wtt. gdy $a|1$

Definicja:

Element a in R nazywamy pierwszym wtt. gdy zachodzi implikacja $a|b*c\Rightarrow a|b\ lub\ a|c$

Definicja:

Element $a\in R\setminus R^*\cup 0$ nazywamy nierozkładalnym wtt. gdy zachodzi implikacja $a=b*c\Rightarrow b\in R^*\ lub\ c\in R^*$.

Definicja:

Pierścień R nazywamy dziedziną z jednoznacznością rozkładu (DJR) wtt. każdy element $a\in R\setminus(R^*\cup\{0\})$ można przedstawić jednoznacznie z dokładnością do porządku i odwracalności w postaci iloczynu elementów nierozkładalnych.

Twierdzenie 1:

Jeśli R – dziedzina całkowitości to każdy element pierwszy jest nierozkładalny. Jeśli co więcej R jest DJR to zachodzi również odwrotna

implikacja, tzn. każdy element nierozkładalny jest pierwszy.

Przykład:

Pierścień wielomianów K[X, Y] nad ciałem K jest DJR

Twierdzenie 2:

Niech R – pierścień (przemienny z jedynka), wtedy zachodzi implikacja:

Jeśli a – pierwszy to pierścień ilorazowy R/(a) jest ciałem.
Jeśli a – nierozkładalny to pierścień ilorazowy R/(a) jest D.C.

Niech R – D.C.
Definiujemy relację (równoważności)

$$\forall r, s, r', s' \in R$$
$$(r, s) \sim (r', s') \Leftrightarrow r * s' - s * r' = 0$$

Klasy abstrakcji tej relacji nazywamy ułamkami w R i oznaczamy:
$\frac{r}{s}; \frac{r'}{s'}$ odpowiednio. Zbiór ułamków z działaniami

$$\frac{r}{s} * \frac{r'}{s'} = \frac{r * r'}{s * s'}$$

$$\frac{r}{s} + \frac{r'}{s'} = \frac{r * s' + s * r'}{s * r'}$$

ma strukturę ciała. Nazywamy go ciałem ułamków pierścienia R.

Ideał I pierścienia nazywamy maksymalnym wtt. gdy zachodzi implikacja

$$I \subset J \subset R \Rightarrow J = I \; lub \; J = R$$

Definicja:

Pierścień R nazywamy lokalnym wtt. gdy posiada dokładnie jeden ideał maksymalny.

Twierdzenie 3:

Następujące warunki są równoważne:

1. R jest pierścieniem lokalnym.

2. Zbiór wszystkich elementów nieodwracalnych jest ideałem pierścienia R.

Dowód Tw 3:

"⇐" tzn. że z (2) wynika (1)
Niech S – zbiór wszystkich elementów nieodwracalnych R. Wiemy, że S jest ideałem. Pokażemy, że S jest jedynym ideałem maksymalnym pierścienia R. W tym celu wystarczy zauważyć, że ideał generowany przez S i dowolny element a ∉ S jest całym pierścieniem R a to wynika stąd, że taki element a musi być odwracalny w R.

"⇒" tzn. że z (1) wynika (2)
Niech I – ideał maksymalny pierścienia R. Wystarczy pokazać, że suma elementów nieodwracalnych w R jest elementem nieodwracalnym w R. W tym celu rozważmy dwa ideały: $(a)\subset R,(b)\subset R$. Na mocy założenia $(a)\subset I,(b)\subset I$ gdzie I jest jedynym ideałem maksymalnym pierścienia R. Ponieważ I jest grupą addytywna to $a+b\in I$, zatem $a+b$ jest elementem nieodwracalnym w R. CKD

Definicja

K nazywamy ciałem algebraicznie domkniętym wtt. gdy każdy wielomian o współczynnikach w tym ciele posiada w nim także pierwiastki.

Lemat:

Jeśli K - ciało algebraiczne domknięte to
$|K|=\infty$

Dowód:

Wystarczy rozważyć wielomiany x^p-1 gdzie p – przebiega liczby pierwsze i zauważyć, że jeśli $x^{p_1}=1$ oraz $x^{p_2}=1$ to
$x^{NWD(p_1,p_2)}=x^1=1$.

Definicja:

$A^2(K)$ – przestrzeń afiniczna dwuwymiarowa $(A^2(K)=K\times K)$

Niech C – krzywa algebraiczna płaska, tj. zbiór rozwiązań równania
$C(X,Y)=0$
gdzie $C\in K[X,Y]$

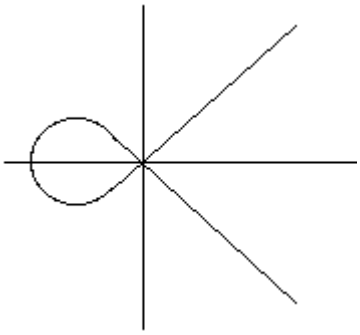
tzn. $C=\{(x,y)\in A^2(K): C(x,y)=0\}$

Przykład:

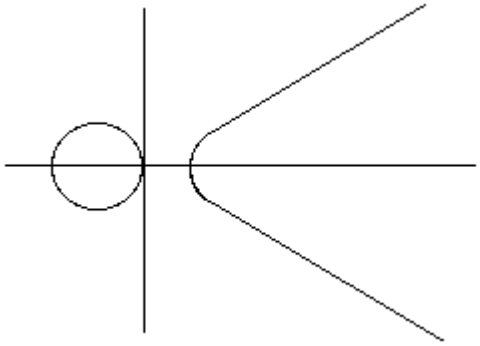
$K=\mathbb{R}$

$D=Y^2-(X^3+X^2)$

$E=Y^2-(X^3-X)$



D



E

Wniosek 2:

Jeśli K – ciało algebraicznie domknięte, to krzywa algebraiczna płaska $C\in K[X,Y]$ zawiera nieskończenie wiele punktów.

Dowód:

$\forall_{x\in K} C(X,Y)=0$ ma rozwiązanie Y = y na mocy algebraicznej domkniętości K.

$|\{(x,y): C(x,y)=0\}|\geq \sum_{x\in K} 1 = \infty$ na mocy wniosku 1.

Definicja:

$C\subset A^2(K)$, $P=(x,y)$ punkt leżący na krzywej $C, (P\in C)$ powiemy, że P jest punktem osobliwym wtt gdy

$$\frac{\partial C}{\partial x}(P)=\frac{\partial C}{\partial Y}(P)=0$$

Krzywa C jest osobliwa wtt gdy posiada co najmniej jeden punkt osobliwy.

Przykład:

$$\frac{\partial D}{\partial x}(0,0) = -(3x^2 + 2x) = 0$$

$$\frac{\partial D}{\partial y}(0,0) = 2y = 0$$

$$\frac{\partial E}{\partial x}(0,0) = -(3x^2 - 1) = 1$$

$$\frac{\partial E}{\partial y}(0,0) = 2y = 0$$

Zatem punkt P = (0, 0) jest punktem osobliwym krzywej D ale nie jest punktem osobliwym krzywej E.

3.1 Funkcje wielomianowe i wymierne na krzywej C

Definicja:

Pierścieniem współrzędnych krzywej C nazywamy pierścień ilorazowy K[C] = K[X, Y] / (C), w dalszym ciągu będziemy zakładać, że C[X, Y] jest wielomianem nierozkładalnym nad ciałem K.

Wniosek:

Na mocy twierdzeń 1 i 2 mamy, że:
K[C] jest dziedziną całkowitości

Uwaga:

Elementy pierścienia współrzędnych K[C] są klasami abstrakcji relacji równoważności określonej następująco:
[f] = f + (C), gdzie (C) oznacza ideał generowany przez wielomian C(X, Y)

Definicja:

Ciałem funkcji wymiernych na krzywej C nazywamy ciało ułamków pierścienia K[C], i oznaczamy je przez K(C).

Wniosek:

Elementy ciała funkcji wymiernych są postaci $r = \frac{f}{g}$ gdzie $f, g \in K[C]$

3.2 Pierścień lokalny

Niech $P \in C$ – krzywa eliptyczna płaska
K(C) - ciało funkcji wymiernych

Definicja:

$r \in K(C)$ jest regularna w punkcie P jeśli istnieje reprezentacja :

$r = \frac{f}{g}, f, g \in k[C]$ oraz $g(P) \neq 0$

Definicja:

Pierścień funkcji wymiernych regularnych w punkcie P nazywamy pierścieniem lokalnym krzywej C i oznaczamy $O_P(C)$

4. Krzywe eliptyczne afiniczne

Definicja

Równaniem Weierstrassa nad ciałem *K* nazywamy równanie:
$E: Y^2 + a_1 XY + a_3 Y = X^3 + a_2 X^2 + a_4 X + a_6$
$gdzie\ a \in K, i = 1, 2 \ldots 6$

Równanie to nazywamy osobliwym wtt. gdy układ
$\frac{\partial E}{\partial X} = \frac{\partial E}{\partial Y} = 0$ nie ma rozwiązań dla żadnego *P = (x, y)* należącego do *E*

Definicja

Krzywą ***E*** zadaną przez powyższe równanie Weierstrassa, która jest nieosobliwą nazywamy krzywą eliptyczną afiniczna

Uwaga

W dalszym ciągu będziemy identyfikować krzywą ***E*** z jej równaniem

Weiestrassa a także wielomianem $E(X,Y)\in K[X,Y]$

$$E(X,Y)=Y^2+a_1XY+a_3Y-(X^3+a_2X^2+a_4X+a_6)$$

Definicja

Stopniem funkcji wymiernej $r=\frac{f}{g}$ $r\in K(X)$, nazywamy liczbę $st(r)=st(f)-st(g)$

Zachodzą równości:

$st(rs)=st(r)+st(s)$

$st(\frac{1}{r})=-st(r)$

$st(r+s)\leqslant min(st(r),st(s))$

Równość zachodzi wtt. gdy $st(r)\neq st(s)$

Twierdzenie 1

Niech R – dziedzina z jednoznacznością rozkładu, L – ciało ułamków pierścienia R i niech $a\in R[Y]$ będzie elementem nierozkładalnym w *R[Y]*. Wtedy $a\in R$ lub a jest nierozkładalny w $L[Y]$.

Dowód

Załóżmy nie wprost, że a in R[Y] niestały i że a ma rozkład w L[Y].

Wtedy $a=\frac{f_1}{g_1}*\frac{f_2}{g_2}$ gdzie $f_i,g_i\in R[Y]$

Gdyby istotnie p-element pierwszy dzielił g_1g_2, wtedy $p|f_1f_2\Rightarrow p|f_1$ lub $p|f_2$ a to niemożliwe bo $f_1f_2\perp g_1g_2$ zatem g_1g_2 jest elementem odwracalnym w $R[Y]$ i wtedy $a=f_1f_2$ gdzie $f_{1,}f_2\in R[Y]$ co przeczy nierozkładalności a w $R[Y]$.

Twierdzenie 2

Wielomian $E(X,Y)$ występujący w równaniu Weierstrassa jest nierozkładalny w $K[X,Y]$.

Dowód

Niech $R=K[X]$ – dziedzina z jednoznacznością rozkładu.

Gdyby E był rozkładalny w $K[X,Y]$ to także nie mamy powyższego twierdzenia w $K(x)[Y]=L[K]$ wtedy $E=(Y+r)(Y+s)$ gdzie

$$r, s \subset K(x)$$

Porównując współczynniki dostajemy:

$$r+s=a_1X+a_3$$
$$rs=-(X^3+a_2X^2+a_4+a_6)$$
$$st(r+s)\leqslant 1$$
$$1\geqslant st(r+s)=max(str, sts)\geqslant\frac{3}{2}$$ - sprzeczność

Dla dowolnego $f \in K[E] oraz (x, y)=P\in E$ definiujemy wartość $f(P)=f(X,Y)(x,y)=f(x,y)$ która nie zależy od wyboru reprezentacji wielomianu f gdyż biorąc $g=f+cE$ otrzymujemy $g(P)=f(P)+cE(P)=f(P)+c*0=f(P)$

Uwaga

Ciało K(E) jest rozszerzeniem stopnia dwa ciała K(X). Automorfizm ciała K(E) na K(X) jest zadany przez odwzorowanie:
$\tau: Y\to\bar{Y}=-Y-a_1X-a_3$
Dla dowolnego $f\in K(E)$ definiujemy:
$\bar{f}(X,Y)=f(X,\bar{Y})$
gdzie $\bar{Y}$ jak wyżej

Podobnie jeśli $P=(x,y)\in E$ to $(\bar{P})=(x,\bar{y})$ tez należy do E gdzie $\bar{y}=-y-a_1X-a_3$
Wynika to z podstawienia $y\to\bar{y}$ w równaniu Weiestrassa
$Y+a_1XY+a_3Y=Y(+a_1X+a_3)=(-Y-a_1X-a_3)(-Y)=Y(Y+a_1X+a_3)$

Definiujemy funkcję normy i śladu:
$N: K(E)\to K(X)$
$Tr: K(E)\to K(X)$
$N(f): f\to f\bar{f}$
$Tr(f): f+\bar{f}$
Norma jest pożytecznym narzędziem przy redukcji wielomianów dwu zmiennych do jednej zmiennej. W szczególności pozwala udowodnić, że:

Stwierdzenie

K[E] jest pierścieniem funkcji wielomianowych na E tzn. zachodzi równoważność $\forall P\in E \quad f(P)=0$ wtt. gdy $f=0\, w\, K[E]$

4.1 Izomorfizm krzywych eliptycznych

Krzywa E i E' zadane równaniami Weierstrassa

$E: Y^2 a_1 XY + a_3 Y = X^3 a_2 X^2 + a_4 X + a_6$

$E': Y^2 + a'_1 XY + a'_3 Y = X^3 + a'_2 X^2 + a'_4 X + a'_6$

nazywamy izomorficznymi wtt. gdy istnieje zamiana zmiennych

$$\psi: \begin{pmatrix} x \\ y \end{pmatrix} \to \begin{pmatrix} u^2 & 0 \\ u^2 s & u^3 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} r \\ t \end{pmatrix}$$

gdzie $u \neq 0$, r, s, t dowolne elementy ciała K

Przekształcenie ψ nazywamy dopuszczalną zamianą zmiennych lub izomorfizmem.

Przykład

$$\psi: (X, Y) \to (X, \bar{Y}) = (X, -Y - a_1 X - a_3)$$

Wniosek

Relacje izomorfizmu są relacją równoważności
Przekształcenie odwrotne do ψ zadane jest wzorem

$$\psi^{-1}: \begin{pmatrix} x \\ y \end{pmatrix} \to \begin{pmatrix} u^{-2} & 0 \\ -u^{-2} s & u^{-3} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \to \begin{pmatrix} u^{-2} r \\ u^{-3}(t - rs) \end{pmatrix}$$

Wniosek

Ściślej mówiąc przekształcenie ψ zamienia układ współrzednych (X, Y) w którym zadana jest krzywa E = E(X, Y) na układ (X', Y') w którym krzywa E ma postać E' tj. $\begin{pmatrix} X \\ Y \end{pmatrix} = \psi \begin{pmatrix} X' \\ Y' \end{pmatrix}$
i macierz ψ jest dana powyżej. Zatem $E' = E \circ \psi$ i $E'(P') = E(P)$, gdzie $P' = \phi(P) \in E'$ i ϕ jest równe ψ^{-1}. Naturalnym rozszerzeniem ψ jest:

$\psi: K(E) \to K(E')$

$\psi(f) = f \circ \psi$

Wniosek

Izomorfizm krzywych E i E' jest jedynym w klasie transformacji afinicznych postaci:

$$\begin{pmatrix} X \\ Y \end{pmatrix} \to \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} + \begin{pmatrix} r \\ t \end{pmatrix}$$

4.2 Postacie normalnie krzywych eliptycznych

Niech K - dowolne ciało. Jeśli istnieje p>0 takie że $\overbrace{1+1+,\ldots,+1}^{p\ razy} = 0$ to ciało ma charakterystykę dodatnią.
Najmniejsza taka liczba p jest nazywana charakterystyką ciała i oznaczana przez char(K).
W przeciwnym przypadku ciało K ma charakterystykę zero i piszemy char(K)=0

Przykład

$char(Z_2) = 2 \quad , char(Z_3) = 3$
Niech ψ - dopuszczalna zamiana zmiennych $\psi : (X', Y') \to (X, Y)$.

Wtedy:

$\psi : K(E) \to K(E')$ takie, że
$\psi(f) = f \circ \psi$ (złożenie zadaje izomorfizm odpowiednich ciał)
Wtedy odbicie (ψ do pierścienia lokalnego) $O_P(E)$ indukuje odpowiednie przekształcenie $\tilde{\psi} | O_P(E) : O_P(E) \to O_{P'}(E')$

Uwaga

Operacje sprzężenia „-„ zadaje izomorfizm krzywej E w krzywą E'=E (automorfizm krzywej E), gdyż $\tau : E \to E \quad P \in E \to P' \in E$, a macierz τ wygląda następująco: $\tau : \begin{pmatrix} X \\ Y \end{pmatrix} \to \begin{pmatrix} X \\ -Y - a_1 X - a_3 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -a_1 & -1 \end{pmatrix} \begin{pmatrix} Y \\ Y \end{pmatrix} + \begin{pmatrix} 0 \\ -a_3 \end{pmatrix}$

Automorfizm τ jest stały na ciele funkcji wymiernych $K(X)$, Ponieważ $\psi^{-1} K(E') \to K(E)$ wiec $\psi \circ \tau \circ \psi^{-1} : K(E') \to K(E')$ jest to automorfizm stałym na $K(X)$. Zatem $\psi \circ \tau \circ \psi^{-1}$ musi być sprzężeniem na ciele $K(E')$ oznaczanym symbolem τ'.

Wniosek 1

Izomorfizm ψ komutuje a automorfizmem sprzężenia tzn. $\tau \circ \psi = \psi \circ \tau'$

Wniosek 2

Dla dowolnej funkcji wymiernej zachodzi równość $r \in K(E)$
$\psi(\bar{r}) = (\psi \circ \tau)(r) = (\tau \circ \psi)(r) = \psi(r) = \overline{\psi(r)}$

Wniosek 3

ψ komutuje z operatorami normy N i ślady Tr tzn. $\psi \circ N = N \circ \psi$,
$\psi \circ Tr = Tr \circ \psi$

Dowód

Dla normy:

$$N(\psi(f)) = (f \circ \psi)\overline{(f \circ \psi)}$$

$$\psi \circ N(f) = \psi(Nf) = \psi(f\bar{f}) = f\bar{f} \circ (\psi) = (f \circ \psi)(\bar{f} \circ \psi) = (f \circ \psi)\overline{(f \circ \psi)}$$

Dla śladu:
$Tr \circ \psi(f) = Tr(\psi f) = Tr(f \circ \psi) = (f \circ \psi) + \overline{(f \circ \psi)}$
$\psi \circ Tr(f) = \psi(Trf) = \psi \circ (f + \bar{f}) = (f + \bar{f}) \circ \psi = f \circ \psi + \bar{f} \circ \psi = (f \circ \psi) + \overline{(f \circ \psi)}$
Ostatnie przekształcenie zachodzi na mocy wniosku 2.

Postacie normalne

Dopuszczalna zamiana zmiennych ψ przeprowadza krzywą E na krzywą E’
$E: Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$
$E': Y^2 + a'_1 XY + a'_3 Y = X^3 + a'_2 X^2 + a'_4 X + a_6$
gdzie :
$a_i, a'_i \in K, i = 1,\ldots,6$ są powiązane równościami

$$a'_1 = u^{-1}(a_1 + 2s)$$
$$a'_3 = u^{-3}(a_3 + ra_1 + 2t)$$
$$a'_2 = u^{-2}(a_2 + sa_1 + 3r - s^2)$$
$$a'_4 = u^{-4}(a_4 + 2ra_2 - (rs + t)a_1 - sa_3 + 3r^2 - 2st)$$
$$a'_6 = u^{-6}(a_6 + r^2a_2 + ra_2 - rta_1 - ta_3 + r^3 - t^2)$$
$$b'_2 = u^{-2}(b_1 + 12r)$$
$$b'_4 = u^{-4}(b_4 + rb_2 + 6r^2)$$
$$b'_6 = u^{-6}(b_6 + 2rb_4 + r^2b_2 + 4r^3)$$
$$b'_8 = u^{-8}(b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4)$$
$$c'_4 = u^{-4}c_4$$
$$\Delta' = u^{-12}\Delta$$
$$j' = j$$

Wniosek

Krzywe izomorficzne mają ten sam j - niezmiennik. Ponieważ $u \neq 0$ więc krzywe izomorficzne mają jednocześnie wyróżnik niezerowy lub zerowy. Klasyfikacja postaci normalnej wyróżnia dwa przypadki:

Przypadek 1

Podstawiając $(X,Y) \to \left(X, Y - \frac{1}{2}(a_1X + a_3)\right)$ przeprowadzamy krzywą E na $E': Y^2 = X^3 + a'_2X^2 + a'_4X + a'_6$

Dalej jeśli dodatkowo $char(K) \neq 3$ to podstawiając $(X,Y) \to \left(X - \frac{1}{3}a'_2, Y\right)$ przeprowadzamy krzywą E' na $E'': Y^2 = X^3 + a''_4X + a''_6$

Jeżeli $char(K) = 3$ to

1) Jeżeli $a'_2 = 0 \left(tj.\ j' = \frac{a'^6_2}{\Delta}\right)$ to E ma żądaną postać : $Y^2 = X^3 + a''_4X + a''_6$

2) W przeciwnym przypadku podstawienie $(X,Y) \to \left(X + \frac{a'_4}{a'_2}, Y\right)$ przeprowadza krzywą E' na $E'': Y^2 = X^3 + a''_2X^2 + a''_6$

Przypadek 2 (char(K) = 2)

1. Jeżeli $a_1 = 0 \left(tj.\ j' = \frac{a_1^{12}}{\Delta}, \Delta \neq 0\right)$ to podstawienie $(X,Y) \to (X + a_2, Y)$

przeprowadza E na postać : $E': Y^2 + a'_3 Y = X^2 + a'_4 X + a'_6$

2) Jeżeli $a_1 \neq 0$ to podstawienie $(X,Y) \to \left(a_1^2 X + \frac{a_3}{a_1}, Y + \frac{a_1^2 a_4 + a_3^2}{a_1^3} \right)$

przeprowadza krzywą E na $E': Y^2 + XY = X^3 + a'_2 X^2 + a'_6$

5.Waluacje dyskretne

Kryterium nieosobliwości krzywej afinicznej $C \in K[X,Y]$

Twierdzenie

Krzywa zadana równaniem Weierstrassa jest osobliwa tedy i tylko wtedy gdy $\Delta = 0$

Dowód

Izomorfizm φ (dopuszczalna zmiana zmiennych zachowuje niezerowość wyróżnika Δ), więc wystarczy rozważać postać normalną krzywej.

Załóżmy, że $char(K) \neq 2 \; i \; char(K) \neq 3$, wtedy:
$E: Y^2 = X^3 + a_4 X + a_0, \quad \Delta = -16\left(4a_4^3 + 27a_6^2\right)$
Z drugiej strony na mocy wzorów CARDANO mamy, że wielomian $X^3 + a_4 X + a_6$ ma pierwiastki wielokrotne wtedy i tylko wtedy, gdy :
$\left(\frac{a_6}{2}\right)^2 + \left(\frac{a_4}{3}\right)^3 = 0 \quad tj. \; gdy \; \Delta = 0$
Zatem istnieje równanie układu
$\frac{\delta E}{\delta Y} = 2Y = 0$
$\frac{\delta E}{\delta X} = \frac{\delta}{\delta X}(x - x_1)^2 (x - x_2)(-1) = -\left[2(x - x_1)(x - x_2) + (x - x_1)^2\right]$
Zatem punkt $(x_1, 0)$ jest punktem osobliwym krzywej E. Odwrotnie jeśli punkt p jest punktem osobliwym krzywej E to $\Delta = 0$.

Niech:
R- dowolny (przemienny z 1)
R* - oznacza grupą jedności pierścienia R

Definicja

Waluacje dyskretną pierścienia R nazywany funkcję addytywną $v : R \to (0,\infty]$ spełniającą następujący warunek „trójkąta” tzn.

$$\forall_{a,b \in R} \; v(a+b) \geqslant min(v(a) \supset v(b))$$

Wniosek

Waluacje v spełnia następujące warunki:

a) $v(0) = \infty$

b) $a \in R^* \to v(a) = 0$

Dowód

1)Z addytywności:

Gdyby $v(0) < \infty$ to $v(0) = v(0 \cdot a) = v(a) \cdot v(0) \Rightarrow 0 = v(a)$ dla dowolnego $a \in R$,co jest niemożliwe. Zatem $v(0) = \infty$ cbdo.

2)Mamy $v(a) = 0(a \cdot 1) = v(a) + v(1) \Rightarrow v(1) = 0$. Dalej jeżeli $a \in R$ oraz istnieje $b \in R$ takie, że $ab = 1$, to wtedy

$0 = v(1) = v(a \cdot b) = v(a) + v(b) \Rightarrow v(a) = v(b) = 0$ cbdo.

Definicja

Jeżeli w pierścieniu istnieje element nieodwracalny $n \in R \setminus \{R^* \cup \{0\}\}$ taki że dowolny $s \in R \setminus \{0\}$ można przedstawić w postaci $s = n^d t$, $d \in N_0$, $t \in R^*$, to n nazywamy parametrem lokalnym.

Wniosek

Wartość *d* jest określona jednoznacznie.

Dowód

$s = n^{d_1} \cdot t_1 = n^{d_1} \cdot t_2$ wtedy $1 = u^{d_1 d_2} t_1 t_2^{-1} \Rightarrow u^{d_1 d_2} = t_2 t_1^{-1}$ co jest niemożliwe, gdyż lewa strona równania jest elementem nieodwracalnym w R a prawa strona równania jest elementem odwracalnym. Otrzymana sprzeczność dowodzi że $d_1 = d_2$.

Uwaga

W pierścieniu lokalnym $O_p(E)$ dowolna prosta afiniczna, która nie jest „styczna” do krzywej E w punkcie P jest parametrem lokalnym.

Definicja

Punkt $P \in E, P=(x,y)$ jest punktem rzędu 2 wtedy i tylko wtedy, gdy $P=\bar{P}$ (sprzężone) tj. $y = \bar{y} = -y - a_1 x - a_3$.

Twierdzenie

Każdy element $r \in O_P$ można przedstawić w postaci $s = n^d \cdot t, d \in N_0, t \in R^*$, gdzie $n \in m_P(E)$.
Gdzie:

$m_P(E)$ - ideał maksymalny pierścienia lokalnego $O_P(E)$

Jeśli $f(P) \neq 0$ to f jest jednością pierścienia i (1) zachodzi dla $d=0$.
Załóżmy więc, że f nie jest jednością tj. f(P) = 0
Pokażemy,że $u = X - x$ jest parametrem lokalnym w pierś $O_P(E)$ cieniu
Każdy $f \in K[E]$ można przedstawić w postaci:

$$0 \neq f = u(x) + Y \cdot W(x)$$
$$f \in K[X,Y]$$

Niech $f = (X-x)^{d_1}(X_1 + Y_{w_1}) = (X-x)^{d_1} f_g$
gdzie $(X-x)^{d_1}$ jest maksymalną potęga dzielącą zarówno $u(x)$ jak i $w(x)$ Ponieważ $f \neq 0$, więc v_1 lub $w_1 \neq 0$.

Jeśli $f_1(P) \neq 0$ to f_1 – jedność to (1) zachodzi dla $d = d_1$
Jeśli $\bar{f}_1(P) \neq 0$ to $\bar{f}_1$ – jedność oraz mamy:

$$f_1 = N(f_1)(\bar{f}_1)^{-1}$$

gdzie $N(f_1) \in K[X]$

Zatem niech

$$N(f_1) = (X-x)^{d_2} f_2$$

gdzie f_2 – jedność, wtedy (1) zachodzi dla $d = d_1 + d_2$

Pozostały przypadek to $f_1(P) = \bar{f}_1(P) = 0$ (*)
Pokażemy, że tak się nie może zdarzyć, w tym celu rozważmy układ równań postaci:

$$\begin{pmatrix} 1 & Y(P) \\ 1 & \bar{Y}(P) \end{pmatrix} \begin{pmatrix} v_1 \\ w_1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

który ma rozwiązanie niezerowe (v_1, w_1) na mocy (*)
Ale wyznacznik macierzy wynosi $\bar{Y}(P) - Y(P) \neq 0$ (gdyż P nie jest punktem rzędu 2) co przeczy założeniu, że powyższy układ ma rozwiązanie niezerowe i tym samym kończy dowód twierdzenia.

Wniosek

Dla dowolnego $P \in E$ i $f \in K[E]$ wartość $d = d(f)$ o której mowa w twierdzeniu, nazywamy rzędem funkcji f w punkcie P. Oznaczamy $ord_p f$. Pojęcie rzędu rozszerzamy na dowolną funkcję wymierną $r = \frac{f}{g}$ jak poniżej:

$$ord_p 0 = \infty$$
$$ord_p \frac{f}{g} = ord_p f - ord_p g$$

W dalszym ciągu będziemy rozważać rozszerzenie pojęcia waluacji dyskretnej $\nu : R \to (-\infty, +\infty]$ spełniające warunek addytywności i trójkąta.

Stwierdzenie

Dla dowolnego $P \in E$ $ord_P : K(E) \to \mathbb{Z} \cup \{\infty\}$ jest waluacja dyskretną.

Dowód

Warunek addytywności jest rzeczywisty.
Załóżmy teraz, że:

$$s = \frac{f_1}{f_2} = \frac{u^{d_1} t_1}{u^{d_2} t_2}$$
$$s' = \frac{f'_1}{f'_2} = \frac{u^{d'_1} t'_1}{u^{d'_2} t'_2}$$

Wtedy:

$$s + s' = u^{d_1 - d_2}(t_1 t_2^{-1}) + u^{d'_1 - d'_2}(t'_1 (t'_2)^{-1}) = u^6 (t\, u^{d_1 - d_2 - \delta} + t')$$

gdzie $\delta = min(d_1 - d_2, d'_1 - d'_2)$ i $d_1 - d_2 \geq d'_1 - d'_2$, $t\, i\, t'$ są jednościami.
Zatem $ord_p(s + s') \geq \delta = min(ord_p s, ord_p s')$ C.N.D.

6. Krzywe eliptyczne rzutowe

6.1 Płaszczyzna rzutowa

Niech k-ciało algebraiczne domknięte
W zbiorze $K^3 \setminus\{0\}$ określającą relację równoważności, zadaje jak następuje
$(x_1, y_1, z_1)(x_2, y_2, z_2)$ wtt.
$exist\, \lambda \in K^*(x_2, y_2, z_2) = (\lambda x_1, \lambda y_1, \lambda z_1)$

Zbiór klas abstrakcji: $K^3 \setminus\{0\}$ nazywamy płaszczyzny rzutowe i oznaczamy $P^2(K)$

Przykład

Przestrzeń rzutowa $P^1(R)$ można identyfikować dowolnym punktem na prostej y=1 lub prostej y=0

W zbiorze $P^2(K)$ możemy wyodrębnić podzbiór "punktów skończonych" płaszczyzny rzutowej odpowiadająca cyklicznym kierunkom równoległych do płaszczyzny z=0

Odwrotnie jeśli $Q=(x, y, z) \in P^2(K)$ to jego "odjednorodnienie" definiujemy.

W ten sposób każdemu punktowi afinicznemu można przyporządkować jego ujednorodnienie $Q^* \in P^2(K)$ a każdemu punktowi $Q \in P^2(K)$ jego odjednorodnienie $Q_* \in A^2(K)$.

Operację (*) nazywamy ujednorodnieniem i odjednorodnieniem odpowiednio.

Niech :
$\phi : A^2(K) \to P^2(K)$
$Q \to Q^*$
$\psi : P^2(K) \to A^2(K)$
$Q \to Q_*$
Wtedy mamy:
$\psi \circ \phi = Id_{A^2(K)}$
$\phi \circ \psi = Id_U$
Gdzie $U \in P^2(K)$ jest zbiorem punktów skończonych płaszczyzny rzutowej

$P^2(K)$ (ze względu na ustalona współrzędną)
Ujednorodnienie i odjednorodnienie wielomianów

Operacje "*" p rzutuje się w sposób naturalny na wielomiany
$f \subset K[X,Y]$
$\phi : K[X,Y] \to K[X,Y,Z]_{nom}$
$\phi : f \to F$
$F(X,Y,Z) = f(\frac{X}{Z}, \frac{Y}{Z}) * Z^{st\,f}$
gdzie $K[X\,Y\,Z]_{nom}$ jest zbiorem wielomianów jednorodnch tzn spełniających warunek $F(\lambda X, \lambda Y, \lambda Z) = \lambda^{st\,F} F(X,Y,Z)$

Podobnie definiujemy :
$\psi : K[X,Y,Z]_{hom} \to K[X,Y]$
$F \to f$
$f(X,Y) = F(X,Y,Z)$
mamy równość:
$\phi \circ \psi = Id$
$\psi \circ \phi = Id$
na odpowiednich dziedzinach zachodzi następująco:

Lemat

Mamy dla $f \in K[X,Y],\ F \in K[X,Y,Z]_{hom}$
1) $(fg)* = f*g*$
2) $(FG)* = F*G*$
3) $(f*)* = f$
4) Jeśli $Z*F$ to $(F_*)* = F$

6.2 Krzywe rzutowe

Niech C -krzywa algebraiczna płaska. Zatem $C[X,Y]$ jest wielomianem nieoznakowanym $K[X,Y]$.

Krzywe rzutowe $C*$ definiujemy jako krzywe zadane przez ujednorodnienie $C*[X,Y,Z]$ wielomianami $C[X,Y]$. Zauważmy, że $C*[X,Y,Z]$ jest rozkładem wtedy i tylko wtedy gdy $C[X,Y]$

Pierścień ilorazowy

$K[X,Y,Z]/C^*$ nazywamy pierścieniem współrzędnych dla krzywej rzutowanej C^* oznaczamy go $K[C^*]$.

Aby funkcja wymierna $r=\frac{F}{G}$ była dobrze określona na $P^2(K)$ F i G muszą być wielomianami tego samego stopnia st(F)=st(G) .

Zatem $K(C^*)=r=\frac{F}{G};G,F\in K[Z,Y,Z]\,hom/C^*, st\,F=st\,G$.

Lokalizując $K(C^*)$ w punkcie $P^*\in C^*$ otrzymujemy pierścień lokalny $O_P{}^*(C^*)$, dokładniej $O_P{}^*(C^*)=\{r=\frac{F}{G}\in K(C^*);G(P)=0\}$.

Analogicznie mamy $\Phi: K(C^*)\to K(C)$ $\frac{F}{G}\to\frac{F^*}{G^*}=\frac{F(X,Y,Z)}{G(X,Y,Z)}$

aby $\Phi(r)$ było dobrze zdefiniowane położymy

$$\Phi(r)=FI(\frac{F}{G})=Z^{st\,F=st\,G}\frac{Z^{st\,F}F(\frac{X}{Z},\frac{Y}{Z})}{Z^{st\,G}G(\frac{X}{Z},\frac{Y}{Z})}=\frac{F(\frac{X}{Z},\frac{Y}{Z})}{G(\frac{X}{Z},\frac{Y}{Z})}$$,wtedy

$$\Phi(r)(\lambda x,\lambda y,\lambda z)=\frac{F(\frac{\lambda X}{\lambda Z},\frac{\lambda Y}{\lambda Z})}{G(\frac{\lambda X}{\lambda Z},\frac{\lambda Y}{\lambda Z})}=\frac{F(\frac{X}{Z},\frac{Y}{Z})}{G(\frac{X}{Z},\frac{Y}{Z})}=\Phi(r)(X,Y,Z)$$ więc

$\Phi(r)$ nie zależy od reprezentanta klasy abstrakcji relacji “r”

Wiosek

Mamy równość:

$\psi\,\phi=Id_{K(C)}$

$\phi\,\psi=Id_{K(C^*)}$

Dowód

$$\psi\,\phi(r)(x,y)\cdot\psi(\frac{F(\frac{X}{Z},\frac{Y}{Z})}{G(\frac{X}{Z},\frac{Y}{Z})})=r(x,y)$$ więc $\psi\,\phi(r)=r$

$$\psi\,\phi(R)(x,y,z)=\phi(R(x,y,1))=R(\frac{x}{y},\frac{y}{z},1)=(\frac{F(\frac{X}{Z},\frac{Y}{Z},1)}{G(\frac{X}{Z},\frac{Y}{Z},1)})=$$

$$=\frac{Z^{-st\,F}F(X,Y,Z)}{Z^{-st\,G}G(X,Y,Z)}=R(X,Y,Z)$$ wiec $\phi\circ\psi(R)=R$

Uwaga

Ponieważ operacja (*) jest homomorfizmem więc x,y

$$\phi(r,s)(x,y)=\phi(\frac{F}{G},\frac{F'}{G'})=\phi(\frac{FF'}{\mathrm{GG'}})=\frac{F(\frac{X}{Z},\frac{Y}{Z})}{G(\frac{X}{Z},\frac{Y}{Z})}\cdot\frac{F'(\frac{X}{Z},\frac{Y}{Z})}{G'(\frac{X}{Z},\frac{Y}{Z})}=\phi(r)\cdot\phi(s)$$

i podobnie

$$\phi(R,S)(X,Y,Z)=\psi\phi(\frac{FF'}{\mathrm{GG'}})(X,Y,Z)=\frac{F(X,Y,Z)F'(X,Y,Z)}{G(X,Y,Z)G'(X,Y,Z)}=\psi(R)\cdot\psi(S)$$

Definicja

Rzutowanym równaniem weiestrassa nazywamy równanie postaci : $E^*: X^{2Z}+a_1XYZ+a_3XZ^3=x^3+a_2X^2Z+a_4XZ^2+a_6Z^3$ a krzywą E* zadaną tym

równaniem rzutowieniem krzywej afinicznej E (lub domknięciem rzutowym E)

Powiedzmy, że dwie krzywe E, E' zadane odpowiednim równaniem Weiestrassa są izomorficzne wtedy i tylko tedy gdy istnieje dopuszczalna zamiana zmiennych przeprowadzająca jedną krzywą w drugą

$\begin{pmatrix}x\\y\\z\end{pmatrix}\to\begin{pmatrix}u^2X+r^2\\u^3Y+u^2sX+2\\z\end{pmatrix}$ gdzie $u,r,s,t\in K,\ u\neq 0$ z uwzględnieniem dzielenia obu stron równania przez u^6 . Krzywą rzutową nazywamy nieosobliwą, jeżeli wyróżnik Δ jest różny od 0 co jest zgodne z oryginalna definicja nieosobliwości (przez pochodne cząstkowe)

Definicja

E* - nazywamy krzywą eliptyczną rzutową wtedy i tylko wtedy gdy jest nieosobliwa to jest gdy $\Delta\neq 0$

Wniosek

Krzywa Eliptyczna rzutowa E* składa się z punktów skończonych (które uzyskujemy przez odjednorodnienie E*) oraz punktu w nieskończoności $\Theta=(0,1,1)$.

Dowód

Odjednorodniając wielomian opisujący krzywą E* ze względu na $z\neq 0$

otrzymujemy krzywą eliptyczną E (punkty skończone). Jeśli natomiast $z=0$ to równanie E* wynika, że $X=0$, otrzymujemy punkt (0,Y,0)=(0,1,0)

Twierdzenie

Niech $P^* \in E^*$ (E* - krzywa eliptyczna rzutowa), wtedy $O_{P^*}(E^*)$ jest pierścieniem z waluacją dyskretną.

Dowód

Jeżeli P* - skończony to było to już udowodnione, jeśli $P^*=\Theta$ to pokażemy, że parametrem lokalnym ze względu na zmienne Y jest $u=\frac{X}{Y}$

Dla dowolnej rozważmy odjednorodnienie E krzywe E* ze względu Y.
$E: Z+a_1 ZX+a_3 Z^3=X^3+a_2 X^2 Z+a_4 XZ^2+a_6 Z^3$ Wystarczy pokazać, że u=X jest parametrem lokalnym krzywej E w punkcie (0,0) gdyż
$(0,1,0)=(\frac{0}{1},\frac{0}{1})$

Zauważmy że X jest dzielnikiem Z w pierścieniu $O_{(0,0)}(E)$, gdyż
$Z=\frac{Zx^3}{x^3}=\frac{Zx^3}{Z+...-a_6 Z^3}=x^3\frac{1}{1+a_1 x+...+a_6 x^2}(1)$
zatem
$x^3|Z$ więc $x|Z$.

Niech teraz $f\in K[E]$ będzie zapisany w postaci
$f=r(Z)+s(Z)X+t(Z)X^2$.

Wyciągniemy najwyższą potęgę Z w każdym wielomianie r, s, t i napiszemy $f-r_1(Z)Z^i+s_1(Z)Z^j X+t_1(Z)Z^k X^2$, gdzie ZXr_1 lub ZXs_1 lub ZXt_1 lub $r_1=0$ lub $s_1=0$ lub $t_1=0$.

Zastępując Z przez postać (1) dostaniemy, że:
$f=r_1(\frac{x^3}{1}+...)+s_1(\frac{x^3}{1}+...)X+t_1(\frac{x^3}{1}+...)=r_2 X^3+s_2 X^{3j+1}+t_2 X^{3k+2}$ gdzie r_2 , s_2 , $t_2\in K(E)$, każdy z nich jest albo regularny w punkcie (0, 0) albo tożsamościowo równy zero w $K(E)$.

Niech d będzie minimum z tych $3i, 3j+1, 3k+2$ dla których odpowiednie r_2 , s_2 , $t_2 \neq 0$. Wtedy $f = x^d f'$ gdzie f' jest funkcją regularną w punkcie (0, 0) c.k.d.

Przykład

$\frac{Z}{Y}$ ma zero rzędu 3 w punkcie $\Theta^* na E^*$, Z ma zero rzędu 3 na E gdyż $Z = x^3 r, r(0,0) \neq 0$.

Zatem $\frac{Y}{Z}$ i $\frac{1}{Z}$ maja bieguny rzędu 3 w (0, 0) ponieważ $ord_p(\frac{X}{Y}) = 1$ więc $\frac{x - xZ}{Z} = \frac{\frac{X - xZ}{Y} * y}{Z}$ ma biegun rzędu 2 w punkcie $0^* \in E^*$.

Wcześniej pokazaliśmy jakie zera (i rzędy zer) ma funkcja liniowa $X - x$. Teraz w przestrzeni rzutowej ujednorodnienie funkcji $X - x$ to $\frac{X}{Z} - x = \frac{X - xZ}{Z}$. W tym przypadku widać, że suma rzędów zer i biegunów jet równy 0.

6.3 Grupa dywizorów

Dla kontrolowania rzędów zer i biegunów funkcji wymiernych wygodnie jest haszować je jako współczynniki grupy abelowej wolnej generowanych przez punkty krzywej E .

Przykład

Niech $P = (x, y) \in E$ E - krzywa afiniczna

mamy przypadki:
1) Jeśli $p = (x, y)$ nie jest punktem rzędu 2 (tzn $y \neq \bar{y}$) to funkcja $X - x$ jest parametrem lokalnym i ma zera w punktach $p = (x, y)$, $\bar{P} = (x, \bar{y})$ oraz 0 rzędu zero w dowolnym innym punkcie krzywej E .

2) char $\neq$ 2 i P jest punktem rzędu 2 na E i załóżmy, że E jest w postaci normalnej $Y^2 = (X - x_1)(X - x_2)(X - x_3)$ gdzie x_1, x_2, x_3 - różne.

Ponieważ Y jest parametrem lokalnym to $X - x_1$ ma zero rzędu 2 w punkcie $P_1 = (x_1, y_1)$ i zera rzędu zero we wszystkich pozostałych punktach krzywej. Podobnie $x = x_2 i x = x_3$

3) char $K=2$, p jest punktem rzędu 2 na E wtedy sprowadzając E do postaci normalnej mamy $E: Y^2+xY=X^3+a_2X^2+a_6$ i parametrem lokalnym jest $Y+\sqrt{a_6}$ gdyż $X=(Y+\sqrt{a_6})^2\frac{1}{X^2+a_2X+Y}$

Zatem funkcja X ma zero podwójne w punkcie $p=(0,\sqrt{a_6})$ i zerem rzędu zero we wszystkich pozostałych punktach.

Definicja

Grupę abelową generowana przez punkty krzywej E nazywamy grupą dywizorów krzywej E .

$\mathrm{Div}(E)=\sum_{P\in E} m_P(P)$ gdzie $m_P=0$ dla prawie wszystkich punktów $P\in E$.

Działanie dodawania dywizorów wygląda następująco:
$\Delta_1=\sum m_P(P)\Delta_2=\sum m_P'(P)$
$\Delta_1+\Delta_2=\sum (m_P+m_P')(P)$

Definicja

Stopień dywizora $\Delta\in Div(E)$ tożsamość $deg\,\Delta=\sum_{P\in E} m_P$
Podgrupę dywizorów stopnia 0 nazywamy $Div^0(E)$

Definicja

Dywizorem głównym nazywamy (dywizor funkcji r) dywizor postaci
$Div\,r=\sum ord_P\, r(P)$ gdzie $r\in K(E)$
W dalszym ciągu udowodnimy że dywizory główne stanowią podgrupę grupy $Div(E)$

Pokazaliśmy, że funkcja wymierna $r=\frac{X-x^2}{Z}$ ma dwa zera (licząc w krotnościach) i jeden biegun rzędu 2 w nieskończoności na krzywej rzutowej E^* . To oznacza, że $P=(x,y,1)\in E^*$ jest reprezentantem klasy $[X,Y,Z]$, natomiast $\bar{P}=(x_{3,}-y-a_1x-a_3)$.

Izomorfizm krzywych $\psi: E\to E^*$ indukuje odpowiedni izomorfizm ciała funkcji wymiernych $\psi: K(E)\to K(E^*)$ $r\to\psi(r):=r\circ\psi$.

W szczególności więc izomorfizm odpowiednich pierścieni lokalnych

$\psi : \theta_P(E) \to \theta_{\phi(P)}(E')$ a zatem i grup dywizonów $\psi : Prin(E) \to Prin(E')$ zadanych wzorem $\mathrm{div}(\psi(r)) = \mathrm{div}(r \circ \psi) = \psi(\mathrm{div}\, r) = \sum ord_{\phi(P)}(r \circ \psi)(\psi(P))$

Odwzorowanie $\mathrm{div} : K(E)^* \to \mathrm{DIV}(E)$ zadana wzorem $\mathrm{div}(r) = \sum orp_P(r)\,(P)$ jest homorfizmem grupy gdyż $ord_P(r_1, r_2) = ord_P(r) + ord_P(r_2)$. Szczególnym izomorfizmem jest sprzężenia który jest inwolucja, a więc $(\psi = \phi)$. Stąd mamy, że $\mathrm{div}(\psi(r)) = \mathrm{div}(r \circ \psi) = \mathrm{div}(\bar{r})$ oraz $\phi(\mathrm{dir}(r)) = \psi(\mathrm{dir}(r)) = \mathrm{dir}(r)$ tj. $\mathrm{dir}(\bar{r}) = \mathrm{dir}(r)$.

Uwaga

Korzystając z faktu,że dowolna funkcja wielomianowa $f \in K[E]$ ma stopień $N(f)$ zer (licząc z krotnościami), dowodzi się że f*ma biegun rzędu $max(2\,st.v, 2\,st.w+3)$ w punkcie skończonym gdzie $f = v(x) + Yw(X)$.

Wniosek

Jeśli $f = v(X) + Yw(x) \in K[E]$ to $st.N(f) = max(2\ st.v, 2\ st.w)$

Dowód

$N(f) = v^2 + N(Y)w^2 + Tr(Y)w \cdot v$ gdzie $st.\, Tr(Y)w \le 1 + st.w < + 2st.w$
$st.\, N(T) = st(Y \cdot \bar{Y}) = st.(x^3 + a_4 X^2 + a_6) = 3$ c.k.d

Ponieważ powyższe maximum jest co najmniej równe 2 otrzymujemy

Wniosek 1

Każde niestałe funkcje $f \in K(E)$ ma co najmniej 2 zera (liczone z krotnościami)

Wniosek 2

Funkcja wymierna $r \in K(E^*)$ ma tyle zer co biegunów.

Wiemy, że ujednorodnienie wielomianu $f \in K[E]$ może mieć biegun w punkcie nieskończonym ale nie w punkcie skończonym . Odwrotnie zachodzi.

Lemat

Jeśli $r \in K(E)$ nie ma biegunów w punktach skończonych to r_* jest wielomianem.

Z powyższych uwag wynika stwierdzenie :

Funkcja wymierna należąca do $K(E)$ zadająca dywizor główny jest wyznaczona jednoznacznie z dokładnością do stałej $\neq 0$.

6.4 Grupa Picarda

Definicja

Grupą Picarda krzywej eliptycznej E nazywamy grupę ilorazową

$Pic(E) = \frac{\mathrm{Div}(E)}{Prin(E)}$ (mierzymy odstępstwo grupy dywizionów od grupy dywizjonów głównych).

Część zerowa grupy Picarda to grupa ilorazowa

$Pic^0(E) = \frac{\mathrm{Div}(E)}{Prin(E)}$

która jest izomorficzna z grupą punktów wymiernych na krzywej eliptycznej $E/K \simeq Div^0(E)/Prin(E)$. Zatem, każdy punkt P na krzywej E będziemy identyfikować z dywizorem (P) > (Q) stopnia 0 z dokładnością do dywizorów głównych. Co więcej $A = \sum a_P(P)$ jest dywizorem głównym, wtedy i tylko tedy gdy :

$$\begin{cases} \sum a_P = 0 \ oraz \\ \sum a_P P = \theta \end{cases}$$

w sensie struktury grupowej na *E*. Dywizor główny nazywamy często - dywizorem funkcji i oznaczamy $(f) = \sum ord_P f(P)$

Dywizory funkcji liniowych

Niech l: ax + by + c = 0 i niech P, Q, R będą punktami przecięcia krzywej *E* z prostą *l*, wtedy $Div(l) = (P) + (Q) + (\overline{P+Q}) - 3(\theta)$

Jeśli $b=0$ to $l: x+c=0$ wtedy dywizor $Div(l^*)=(P)+(\bar{P})-2(\theta)$

Definicja

Jeśli f jest funkcja na krzywej E oraz $A=\sum a_P(P)$ jest dywizorem to
$f(A)=\prod_{P\in A} f(P)^{a_P}$

Przykład:

$f(x,y)=x-x_R$
$A=(P)-(Q)$
$f(A)=(x_P-x_R)^1\cdot(x_Q-x_R)^{-1}=\frac{x_P-x_R}{x_Q-x_R}$

$$f((P)-(Q))=f(P)\cdot f(Q)^{-1}=\frac{f(P)}{f(Q)}$$

Definicja

Dwa dywizjony Δ_1, Δ_2 nazywamy liniowo niezależnymi wtedy i tylko wtedy gdy ich warstwy modulo Prin(E) są identyczne tzn. :
$\Delta_1 \sim \Delta_2 \Leftrightarrow \Delta_1 - \Delta_2 \in Prin(E)$

Badanie dywizorów sprowadza się do badania dywizorów funkcji liniowych tj. funkcji postaci :
$l=\alpha X+\beta Y+\gamma$ gdzie $\alpha lub \beta \neq 0$.

Jeżeli $\beta \neq 0$ to zachodzi :

Lemat

Niech $l=Y-(mX+b)$ $P=(x,y,1)\in E^*\cap C^*$ wtedy $ord_P l^*$ jest krotnością x jako zero wielomianu $E(X, mX+b)$

Dowód

Wystarczy przedstawić $E(X,T)$ w postaci
$T^2-Tr(Y)T-N(Y)=(Y-T)(\bar{Y}-T)$ oraz wykorzystać reprezentację
$E(X,mx+b)=-(X-x_1)(X-x_2)(X-x_3)=(l^*)(\tau^*)$
gdyż
$(l^*)(\tau^*)^*=(y-(mx+b))(\bar{Y}-mx+b)=(Y-T)(\bar{Y}-T)$, gdzie $T=mx+b$
Z powyższego lematu można otrzymać wzory na dodanie punktów na krzywej eliptycznej.

Działania na krzywej E(K)

Niech $y=\alpha x+\beta$ będzie sieczną przechodzącą przez punkty $(x_1, y_1),(x_2, y_2)$ krzywej E wtedy $(\alpha x+\beta)^2=x_1^3+Ax_1+B$.
gdzie

$$\alpha=\frac{y_2-y_1}{x_2-x_1} \quad (x_2\neq x_1) \; ; \quad \beta=y_2-\alpha x_2=y_2-\frac{y_2-y_1}{x_2-x_1}*x_2$$

Ze wzorów Viete'a
$x_1+x_2+x_3=\alpha^2$

skąd

$$(\#) \quad \begin{cases} x_3=-x_1-x_2+\left(\dfrac{y_2-y_1}{x_2-x_1}\right)^2 \\ y_3=\alpha x_3+\beta \end{cases}$$

Jeśli $x_1=x_2$ (sieczna jest styczną) to jej równanie ma postać $y=\alpha x+\beta$ gdzie
$\alpha=\dfrac{dy}{dx}$
Ponieważ:

$$dE=\frac{\partial E}{\partial x}dx+\frac{\partial E}{\partial y}dy=0 \qquad \text{więc} \quad \frac{dy}{dx}=\frac{\partial E/dx}{\partial E/\partial y}$$

$$\alpha=\frac{dy}{dx}=-\frac{\partial E/dx}{\partial E/\partial y}=-\frac{3x^2+A}{2y}$$

układ (#) zachodzi z odpowiednimi wartościami α i β to mamy:

$$x_3=-2x_1+\left(\frac{3x_1^2+A}{2y_1}\right)^2=\frac{x_1^4+2Ax_1^2-8x_1B+A^2}{4(x_1^3+Ax_1+B)}=\frac{x_1^4+2Ax_1^2-8x_1B+A^2}{f(x_1)}$$

Zatem jeśli $y_1=0$ to $x_3=\infty$ (styczna jest pionowa) to jest $(x_3, y_3)=O$. W ten sposób określiliśmy działanie na krzywej E(R). Te same wzory zadają działanie na krzywej nad dowolnym ciałem charakterystyki $\neq 2,3$ (bo wtedy

E zadaje się równaniem Weierstrassa). $y^2 = f(x)$)

Wniosek

(E(K), +) jest grupą abelową. Przypuszczenie Poincare (1900 r.) mówi, że dla ciał liczbowych K ,$(E(K),+)$ jest skończenie generowaną grupą abelową i zostało udowodnione przez Mordella w 1928 r.. Natomiast w pełnej ogólności (dla rozmaitości abelowych) przez Weila.

Mamy: E(K) = Z' □ E
(Mazur (1977 r.) udowodnił, że dla K=Q , E(Q) = Z_m , m = 0, 1 ..., m
Lub E(Q) = Z_m □ Z_2 i wyznaczył dopuszczalne wartości m .

7. Zastosowania Struktur Dwuliniowych

7.1 Grupowe struktury dwuliniowe

G_1, G_2 - grupy skończone cykliczne o rzędzie będącym zadanym liczbą pierwszą

Działanie dwuliniowe (iloczyn dwuliniowy)
$e: G_1 \times G_2 \to G_2$ spełniający warunki: $G_1 = (G_{1,}+)$ $G_2 = (G_{2,}*)$
1)dwuliniowość $e(aP, bP) = e(P, Q)^{ab}$ $a, b \in \mathbb{Z}$ $P, Q \in G_1$
2)nietrywialność (niezdegenerowalność) to oznacza, że $e(G_1 \times G_1) \neq (\mathbf{1}_{G_2})$, gdzie $\mathbf{1}$ oznacza element neutralny grupy multiplikatywnej.
3)obliczalność

$\forall P, Q \in G_1$ istnieje efektywny obliczeniowo algorytm pozwalający obliczyć $e(P, Q)$

Wniosek 1

Jeśli P jest generatorem G_1 to element $e(P, P)$ jest generatorem G_2

Dowód

Każdy element G_1 jest postaci aP . Zatem niech Q, R takie punkty G_2 , że $e(Q, R) \neq (\mathbf{1}_{G_2})$, $e(P, P)^{ab} \neq (\mathbf{1}_{G_2}) \Rightarrow e(P, P) \neq (\mathbf{1}_{G_2})$. Zatem $e(P, P)$ -

generuje nietrywialną podgrupę w G_2 rzędu dzielącego liczbę pierwszą P. Zatem jest całą grupą G_2 .

Trójkę (G_1, G_2, e) nazywamy strukturą z działaniem dwuliniowym

Protokół Difiego-Helmana w strukturze dwuliniowej

$P, Q \in G_1$ punkty znane publicznie

A → B
aP - publ. bP – publ.
aQ – prywatne bQ – prywante
a,b – losowe

Każda strona wyznacza wspólny klucz wymiany obliczając
$e(bP, aQ) = e(aP, bQ)$
$e(P, Q)^{ba} = e(P, Q)^{ab} = k_{AB}$ - klucz wymiany

Analiza złożoności protokołu

Niech T – operacja transmisji, O – operacja obliczeniowa
Złożoność protokołu D-H dla struktury dwuliniowej wynosi 2T + 6O
Teraz możemy wykorzystać klucz $k_{AB} = e(P, Q)^{a,b}$ do szyfrowania i deszyfrowania wiadomości "m" co daje łącznie 3T +8O operacji

7.2 System "szyfrowanie ze wskazówką" (odpowiada kryptosystemowi ElGamala)

A "m" → B
rP - publ. bP – publ.
rQ – prywatne bQ – prywante
(2O+1T)
r – losowe

1. $[e(bP, rQ) \cdot m, rP]$ – otrzymuje dzieląc pierwszą współrzędną przekazu przez $e(rP, bQ)$ - koszt 4O+1T + 2O
B – oblicza $e(rP, bQ)$
Łączny koszt to 8O +2T

7.3 Podpis cyfrowy w strukturze dwuliniowej

A → B
aP - publ. rP – publ.
aQ – prywatne rQ – prywante
r – losowe

Podpis $\sigma_{a,r}(m)=[(mr+a),rP]$
$[m,\sigma_{a,r}(m)]\rightarrow B$

Weryfikacja

Strona B sprawdza czy : $e((mr+a)Q,P)=e(mQ,rP)\cdot e(Q,aP)$
Poprawność wynika z własności iloczynu

Uzasadnienie

Iloczyn ma własność $e(P+Q,R)=e(P,R)e(Q,R)$ bo
$e(mrQ,P)\cdot e(aQ,P)=e(Q,P)^{mr}\cdot e(Q,P)^{a}=e(mQ,rP)\cdot e(Q,aP)$ ckd

7.3.1 Podpis Schnorra w strukturze dwuliniowej

A “m” **B**
składa podpis → weryfikuje podpis

Podpisywanie wiadomości “m” (wybieramy losowe *r* i obliczamy)
$\sigma_{r,a}(m)=[r+ah,rP]$ gdzie $h=h(m,rP)$ jest publicznie znaną funkcją haszującą.

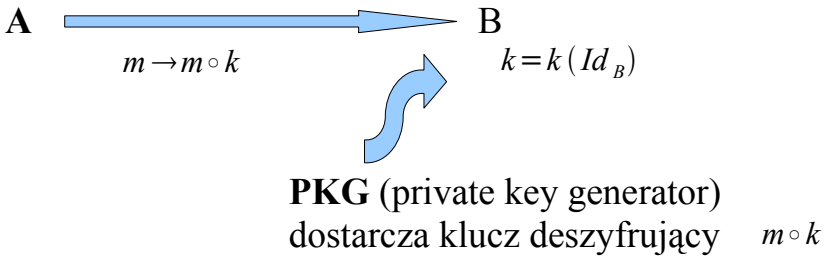
Weryfikacja polega na sprawdzeniu czy zachodzi równość:
(*) $e((r+ah)Q,P)=e(Q,rP)\,e(Q,r\,aP)^{h}$

Poprawność: jeśli podpis przebiega prawidłowo to weryfikacja powiedzie się.

Sprawdzamy (*)
Na mocy własności dzielenia (dwuliniowości) mamy:
$lewa=\langle(r+ah)Q,P\rangle=\langle rQ,P\rangle\langle ahQ,P\rangle=\langle a,rP\rangle\langle Q,P\rangle^{ah}=\langle Q,rP\rangle\langle Q,aP\rangle^{h}=prawa$

Bezpieczeństwo podpisu $\sigma_{r,a}(m)$ sprowadza się odpowiednio do trudności obliczenia wartości $a \, lub \, r$, mając dane punkty $aP \, lub \, rP$ na krzywej eliptycznej – jest to problem logarytmu dyskretnego w grupie punktów wymiernych na krzywej eliptycznej $E(K)$, gdzie K – ciało skończone.

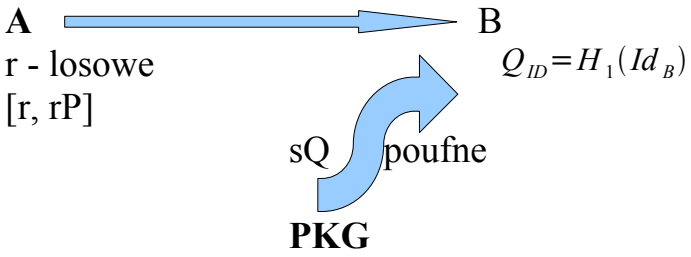
7.4 System szyfrowania oparty na identyfikacji



E – publicznie znana krzywa

P, Q – zadane punkty na E

H_1, H_2 – publicznie znane funkcje haszujące



sQ – klucz deszyfrujący dla *B*

sP – klucz publiczny dla *B*

s – master key

Szyfrogram wiadomości "m" generowany przez *A* jest parą:

$c = [rP, m \oplus H_2(g_{ID}^r)]$ gdzie $g_{ID} = \langle Q_{ID}, sP \rangle$; □ - dodawanie mod 2

c = [X, Y]

Odbiorca używający kluczy sQ oraz $c = [X, Y]$, najpierw oblicza $H_2(g_{ID}^r)$ potem dodaje $H_2(t)Y = m \oplus H_2 \oplus H_2 = m$.

Wystarczy pokazać, że *R* może obliczyć g_{ID}, mianowicie

$g_{ID}^r = \langle Q_{ID}, sP \rangle^r = \langle sQ_{ID}, rP \rangle$ co kończy wnioskowanie.

7.5 Problemy obliczeniowe w strukturze dwuliniowej

7.5.1 Problem Diffie-Hellmana

Struktura (grupowa) dwuliniowa (G_1, G_2, e) , $e: G_1 \times G_1 \to G_2$,
$ord\, G_1 = ord\, G_2 = q$, q – liczba pierwsza.
Problemy:
1) Problem logarytmu dyskretnego DLG (ang. Discrete Logarithm Problem)
2) Problem obliczeniowy Diffie-Hellmana CDH (ang. Computational Diffie-Hellman Problem)
3) Problem decyzyjny Diffie-Hellmana DDH (ang. Decisional Diffie-Hellman Problem)

Założenia
1) Problem DDL w G_2 jest trudny
2) Problem CDH w G_1 jest trudny

Problemy CDH w G_1 :
Dane $[P, aP, bP]$, obliczyć Q = abP
Problemy CDH w G_2 :
Dane $[g, g^a, g^b]$, obliczyć g^{ab}
Problem DDH w G_2 :
Czy czwórka $[g, g^a, g^b, g^c]$ jest czwórka Diffiego – Hellmana
tzn. taką, że $g^c = g^{ab}$
Problem DDH w G_1 :
Czy czwórka $[P, aP, bP, cP]$ jest czwórką Diffiego – Hellmana
tzn. taką, że $abP = cP$

7.5.2 Redukcje MOV

Twierdzenie

Redukcja MOV (Menezes, Okamoto, Vanstone)
Niech (G_1, G_2, e) - struktura dwuliniowa. Wtedy problem DLG w G_1 nie jest trudniejszy niż problem DLG w G_2

Dowód

Niech $P,Q\in G_1$. Szukamy $a: aP=Q$.
Niech $g=e(P,P)$, $h=e(P,Q)$. P,a – generatory G_2 . Pokażemy, że rozwiązując problem DLG w G_2 , rozwiązujemy DLG w G_1 .
Dane :
$g,h\in G_2$
Znajdź :
$\alpha: g^{\alpha}=h$
Niech α będzie rozwiązaniem tego problemu w G_2 tzn. $g^{\alpha}=h$.
Zauważmy, że $a=\alpha$ jest rozwiązaniem problemu DLG w G_1 , bo jeśli $Q=\alpha P$ to $h=e(P,\alpha P)=e(P,P)^{\alpha}=g^{\alpha}$, cnd.

7.5.3 Problem jednokierunkowości

Twierdzenie 2

Odwzorowania $\psi_Q: G_1\to G_2$ zadane wzorem:

$\psi_Q(P)=e(P,Q)$ jest homomorfizmem jednokierunkowym o ile problem DDH w G_2 jest trudny.

Dowód

Załóżmy, że "odwróciliśmy" $\psi_Q(P)$ tzn. Mając dany iloczyn e(P, Q) możemy wyznaczyć P. Pokażemy, że wtedy DDH w G_2 jest łatwy. Zauważmy, że DDH w G_1 jest łatwy bo dla stwierdzenia czy czwórka $[P,aP,bP,cP]$ jest właściwą czwórką D-H wystarczy sprawdzić czy $e(P,cP)=e(aP,bP)=e(P,P)^c=e(P,P)^{ab}$.

Niech (g,g^a,g^b,g^c) będzie dane. Mamy stwierdzić czy jest to czwórka D-H w G_2 wiadomo, że jeśli g-generator G_1 to $e(P,bP)=g^c=e(P,cP)$. Korzystając z założenia można obliczyć aP,bP,cP . Jeśli $[P,aP,bP,cP]$ jest czwórką D-H w G_1 to stwierdzić można, że $[g,g^a,g^b,g^c]$ jest właściwą czwórką D-H w G_2 .
A zatem rozwiązanie problemu DDH w G_2 jest niemożliwe bo założyliśmy, że jest on trudny. A zatem ψ jest jednokierunkowe c.k.d.

Problem BDH (dwuliniowy Diffie-Hellman)
Niech P – generator w G_1 rzędu q

Dane: $[P, aP, bP, cP]\ gdzie\ a, b, c \in \boldsymbol{Z}_q$
Obliczyć: $e(P, P)^{abc}$

Algorytm *A* ma przewagę □ w rozwiązaniu problemu BDH jeśli $Pr[A(P, aP, bP, cP) = e(P, P)^{abc}]$ □ □ gdzie prawdopodobieństwo jest wyznaczane po "losowych" wyborach $a, b, c \in \boldsymbol{Z}_q$ i losowych bitach algorytmu *A*.

Generatorem parametrów (IG) dla struktury $(G_{1,}\ G_{2,}\ e)$ nazywamy algorytm zrandomizowany spełniający warunki:
1. Na wyjściu dane $k \in N$
2. (IG) działa w czasie $O(k^c)$
3. (IG) daje na wyjściu strukturę $(G_{1,} G_{2,} e)$ taką, że $|G_i| = q$ dla i = 1, 2. oznacza ze generator parametrów ma na wyjściu parametr bezpieczeństwa złożony z k jedynek. $IG(1^k)$

Definicja

(IG) spełnia założenia BDH jeśli dowolny zrandomizowany i działający w czasie wielomianowym (od k) algorytm *A* rozwiązuje problem BDH z

przewagą co najwyżej 1/f(k) dla dowolnego wielomianu f.

7.6 Iloczyn WEILA

7.6.1 Wprowadzenie

W tym rozdziale zdefiniujemy działanie dwuliniowe spełniające warunki: nietrywialności i obliczalności.

Definicja 1

Niech $E = E/\bar{K}$ ($\bar{K}$ – algebraicznie domknięte ciało)
Wtedy $E[n] = \{P \in E : nP = \theta\}$ nazywamy grupą punktów n-torsyjnych na krzywej $E/\bar{K}$ (θ punkt neutralny w grupie).
Dalej zakładamy, że $e: E[n] \times E[n] \to (\bar{K})^*$

Definicja 2

Iloczynem Weila nazywamy działanie dwuliniowe trywialne na przekątnej tzn. spełniające warunek : $e(P, P) = 1$ dla dowolnego $P \in E(n)$.

Twierdzenie 1

Niech $e: H \times H \to G$ będzie nietrywialnym działaniem dwuliniowym takim, że $e(P,P)=1$ dla dowolnego $P \in H$ oraz niech $\phi: H \times H \to G$ – homomorfizm taki, że grupa $<P, \phi(P)>$ generowana przez P i $\phi(P)$ jest równa H. Wtedy odwzorowanie $\hat{e}=H \times H \to G$ określone następująco: $\hat{e}(P,Q)=e(P,\phi(Q))$ jest działaniem dwuliniowym nietrywialnym na przekątnej.

Dowód

Niech $Q \in H$ takie, że $(P,Q) \neq 1$ Ponieważ $<P, \Phi(P)>=H$ to $Q=aP+b\phi(P)$. Zatem $1 \neq e(P,Q)=e(P,aP+b\phi(P))=e(P,P)^a e(P,\phi(P))^b$ $=e(P,\phi(P))^b$ c.k.d.

7.6.2 Grupa klas dywizorów krzywej eliptycznej

Przypomnienie

Niech $E/K \simeq Div^0(E)/Prin(E)$. Zatem, każdy punkt P na krzywej E będziemy identyfikować z dywizorem (P) - (Q) stopnia 0 z dokładnością do dywizorów głównych. Co więcej $A= \sum a_P(P)$ jest dywizorem głównym, wtedy i tylko tedy gdy :

$$\begin{cases} \sum a_P = 0 \ oraz \\ \sum a_P P = \theta \end{cases}$$

w sensie struktury grupowej na *E*. Dywizor główny nazywamy często - dywizorem funkcji i oznaczamy $(f)=\sum ord_P f(P)$

Dywizory funkcji liniowych

Niech l: ax + by + c = 0 i niech P, Q, R będą punktami przecięcia krzywej *E* z prostą *l*, wtedy $Div(l)=(P)+(Q)+(\overline{P+Q})-3(\theta)$
Jeśli $b=0$ to $l: x+c=0$ wtedy dywizor $Div(l^*)=(P)+(\bar{P})-2(\theta)$

Definicja

Jeśli f jest funkcja na krzywej E oraz $A=\sum a_P(P)$ jest dywizorem to $f(A)=\prod_{P\in A} f(P)^{a_P}$

Przykład:

$$f(x,y)=x-x_R$$
$$A=(P)-(Q)$$
$$f(A)=(x_P-x_R)^1\cdot(x_Q-x_R)^{-1}=\frac{x_P-x_R}{x_Q-x_R}$$
$$f((P)-(Q))=f(P)\cdot f(Q)^{-1}=\frac{f(P)}{f(Q)}$$

7.6.3 Określenie iloczynu Weila

Definicja

Iloczynem Weila $e:E[n]\times E[n]\to(\bar{K})^*$ nazywamy przekształcenie zadane wzorem:

$e_n=(P,Q)=\frac{f_p{}^n(A_Q)}{f_Q{}^n(A_Q)}$, gdzie $(f_p^n)\sim n(P)-n(\theta)$ $A_Q\sim(Q)-(\theta)$

$(f_Q^n)\sim n(Q)-n(\theta)$ $A_P\sim(P)-(\theta)$

Wnioski

Wartość $e_n(P,Q)$ nie zależy od wyboru reprezentantów klas dywizorów modulo dywizory główne.

Dowód

Niech $\tilde{A}_P$ będzie dywizorem równoważnym A_P *tzn.* $\tilde{A}_P=A_P+(g)$

g – funkcja wymierna na krzywej E oraz $\tilde{f_P}^n=f_P{}^n\cdot g^n$ bo

$\operatorname{div}(f_P{}^n\cdot g^n)=\operatorname{div} f_P{}^n+n(\operatorname{div})g$ oraz $\tilde{A}_P\sim(P)-(\theta)+(g)$ (bo $(\tilde{f_P}^n)\sim n\tilde{A}_P\sim n[(P)-(\theta)+g]=n(P)-n(\theta)+n(g)=(f_P{}^n)+(g^n)$).

Zatem mamy :

$$e_n(P,Q)=\frac{f_P{}^n(\tilde{A}_Q)}{f_Q{}^n(\tilde{A}_P)}=\frac{f_P(A_Q)g(A_Q)^n}{f_Q(A_P)f_Q(g)}=\frac{f_P(A_Q)}{f_Q(A_P)}\cdot\frac{g(nA_Q)}{f_Q(g)}=\frac{f_P(A_Q)}{f_Q(A_P)}\cdot\frac{g(f_Q{}^n)}{f_Q(g)}=\frac{f_P(A_Q)}{f_Q(A_P)}$$

ostatnia równość zachodzi na mocy wzoru wzajemności $f((g))=g((f))$

Lemat

Istnieje efektywny algorytm D , który dla danych wejściowych $f_b(A_Q), f_c(A_q)$ oraz $bP, cP, (b+c)P \ (b,c\in N)$ oblicza wartość $f_{b+c}(A_Q)$ gdzie $f_a \quad a\in\{b,c,b+c\}$ jest funkcją wymierną której dywizor jest równoważny dywizorowi.

$A_Q=a(P+R_1)-a(R_1)-(aP)+(\Theta)$

Dowód

Zdefiniujemy dwie funkcje liniowe g_1, g_2 na krzywej E

$g_1:(g_1)=(bP)+(cP)+(\overline{(b+c)P})-3(\Theta)$
$g_2:(g_2)=((b+c)P+\overline{(b+c)P})-2(\Theta)$

Zatem g_1 jest prostą przechodzącą przez punkty $bP, cP.$ Jeżli $b=c$ to g_1 jest styczną do krzywej E w punkcie bP. Niech $g_1(x,y)=a_1x+b_1y+c_1$. Dalej g_2 jest prostą pionować przechodzącą przez punkt $(b+c)P$. Niech $g_2(x,y)=x+c_2$.

Z definicji mamy, że

$A_b=b(P+R_1)-b(R_1)-(bP)+(\Theta)$
$A_c=c(P+R_1)-c(R_1)-(cP)+(\Theta)$
$A_{c+b}=(b+c)(P+R_1)-(b+c)(P+R_1)-[(b+c)(P+R_1)]+(\Theta)$

Zatem otrzymujemy, że $A_{c+b}=A_b+A_c+g_1-g_2$ skąd

$f_{b+c}(A_Q)=f_b(A_Q)+f_c(A_Q)+g_1-g_2$

Wniosek

Jeśli p jest punktem n-torsyjnym , to dywizory funkcji $f_n \ i \ f_P{}^n$ są równoważne.

Dowód

$(f_p{}^n)\sim nA_P\sim n(P)-n(\Theta)$. Z definicji A_n wiemy, że (f_n) jest dywizorem

równoważnym $A_n \sim n(P+R_1)-n(P_1)-(nP)+\Theta$, który jest równoważny dywizorowi $n(P)-n(\Theta)$.

Wniosek 2

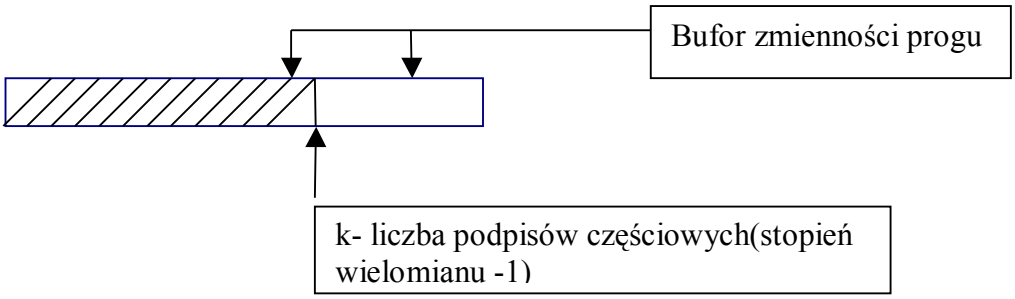
Dla rekurencyjnego obliczenia f_{b+c} rozpoczniemy do obliczenia f_1 takiego,że $(f_1)=(P+R_1)-(R_1)-(P)+\Theta$; taka funkcja jest ilorazem funkcji $g_2`(x,y)/g_1`(x,y)$ gdzie $g_2`(x,y)$ jest prostą pionową przechodzącą przez $(P+R_1)$ natomiast $g_1`(x,y)$ jest prostą przechodzącą przez punkty $P \; i \; R_1$.

Wniosek 3

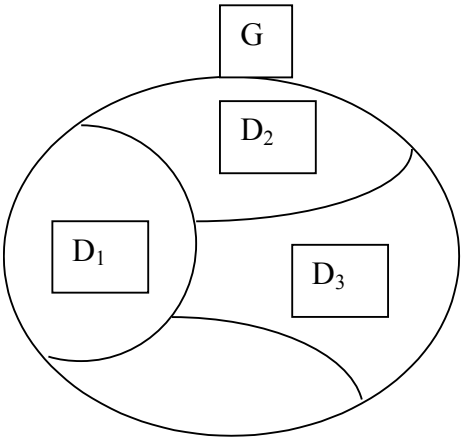
Obliczanie iloczynu Weila $e_n(P,Q)$ wykonuje się w czasie $O(\log^c n)$ gdzie *c* jest pewną stałą dodatnią.

7.6.4 Schematy hierarchiczne w grupie Diffie-Hellmana z LUKĄ

Bardziej elastyczna wersja podpisów grupowych (np. zmiana progu)

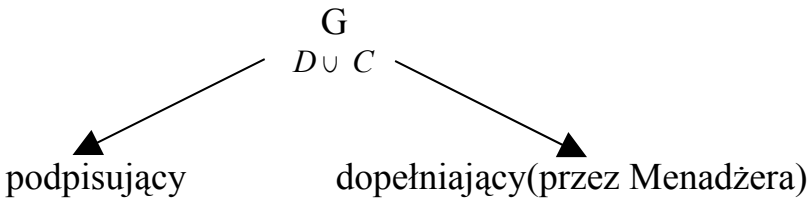


D_i -różne działy



M- zarządza(menadżer kontroluje uzupełnienie podpisów częściowych)

Próg ustalony przez stopień wielomianu, przy zmianie progu wielomian się nie zmienia,ale trzeba go „dopełniać".



Def.

G nazywamy grupą Diffie-Hellmana z luką, gdy:

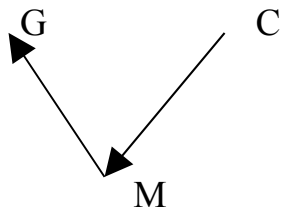
1)Problem obliczeniowy jest trudny w grupie CDH
2)problem decyzyjny D-H jest łatwy w grupie DDH

ad. 1)Dla danych (P, aP, bP) oblicz abp
ad. 2)Dla danej (P, aP, Bp, cP) rozstrzygnij czy c= ab(mod |G|)

Przykład:

Przykładem takiej grupy jest struktura dwuliniowa (G_1, G_2, E_1P), e: $G_1 \rightarrow G_2$ jest iloczynem Weil'a
Wystarczy zauważyć ,że jeśli e(P, cP)=e(aP, bP) to (P, aP, Bp, cP) jest czwórką Diffie-Hellmana

Model komunikacyjny



2 kanały połączeń: poufny i rozgłaszania

Zakładamy, że przeciwnik może „korumpować" t- członków grupy Ct- poziom korupcji

Protokół podpisu(ze zmiennym progiem)

1) generacja kluczy i dzielenie sekretu
2) decyzja Menadżera
3) Podpisywanie:
   a)Członkowie G obliczają podpisy
   b)Delegowany członek G 'skleja' podpisy
4)Weryfikacja

7.7 Ślepe podpisy cyfrowe w grupie GDH Diffe - Hallmana z luką

G_i – grupa DH z luką
$H – \{0,1\}^* \rightarrow G_1$
(G_1,G_2,e) – struktura dwuliniowa
x – klucz prywatny podpisującego
$y = g^x$ – klucz publiczny, gdzie g to generator grupy

(zakładamy dla uproszczenia, że G_1 jest grupą multiplikatywną)

Schemat:

1 Faza

Zaciemnienie wiadomości m. Podmiot A przygotowuje wiadomość. Oblicza jej zaciemnienie czynnikiem losowym g^r i przekazuje do podpisu wartość $H(m)g^r$.

2 Faza

Podpisywanie:

Podmiot B wykonuje ślepy podpis $\sigma = (H(m)g^r)^{x^i}$ i przekazuje stronie A.

3 Faza

Obliczanie właściwego podpisu. Podmiot A zdejmuje czynnik zaciemniający obliczając:

$$\frac{\sigma}{g^r} = \frac{(H(m)g^r)^x}{g^{x_r}} = H(m)^x$$

7.8 Podpis skumulowany

Mamy grupę podpisujących różne wiadomości.

Cel:
Wykonanie podpisu pod wszystkimi wiadomościami takiego, żeby weryfikacja była w jednym kroku.

x_i – klucze prywatne
$y_i = g^{xi}$ – klucze publiczne podpisujących (członków grupy)
m_i – wiadomość podpisywana przez i-tego członka

1. Podpisywanie

Każdy z członków oblicza podpis częściowy $\sigma_i H(m_i)^{x_i}$, który jest walidowany (sprawdzany) dzięki obliczaniu odpowiednich iloczynów Weila. Podpis całkowity ma postać:

$$\sigma = \prod \sigma_i$$

2. Weryfikacja podpisu

Podpis σ jest akceptowany wtedy i tylko wtedy gdy: $e(g,\sigma) = \prod_i e(y_i, H(m_i))$

Wniosek:
Poprawność podpisu wynika z dwuliniowości iloczynu Weila, gdyż:

$$e(g,\sigma) = \prod_i e(g,\sigma_i) = \prod_i e(g, H(m_i)^{x_i}) =$$

$$\prod e(g, H(m_i))^{x_i} = \prod_i e(y_i, H(m))$$

7.9 Podpis pierścieniowy

Ten rodzaj podpisu pozwala na ukrycie tożsamości podpisującego. Wiadomo jedynie, że jest on członkiem danej grupy podpisujących (użytkowników w liczbie

k).

1. Podpisywanie wiadomości m.
   Dowolny użytkownik używa swojego klucza prywatnego x_i i kluczy publicznych y_{ij} gdzie $i \neq j$ wszystkich pozostałych użytkowników do obliczenia podpisu pod wiadomością m.

   Pozostali użytkownicy nie biorą udziału w tym podpisywaniu. Podpisujący w przeciwieństwie do podpisów grupowych jest niewytrapialny.
   Użytkownik i-ty oblicza podpis generując najpierw losowe r_j dla wszystkich $j \neq i$. Podpis ma postać:

$$\sigma(m) = (\sigma_1(m),...,\sigma_k(m)), \text{ gdzie } \sigma_j = g^{r_j},(i \neq j), \sigma_i = \left(\frac{H(m)}{\prod_{i \neq j} y_j^{r_j}}\right)^{\frac{1}{x_i}}$$

2. Weryfikacja
   Podpis $\sigma_1,\sigma_2,...,\sigma_k$ jest zaakceptowany wtedy i tylko wtedy gdy

$$e(g,H(m)) = \prod_{s=1}^{k} e(y_i,\sigma_i)$$

   Wniosek:
   Poprawność wynika z własności iloczynu Weila, a mianowicie:

$$\prod_{s=1}^{k} e(y_s,\sigma_s) = \prod_{s \neq i} e(g^{x_s},g^{r_s}) e(g^{x_i},\left(\frac{H(m)}{\prod_{j \neq i} y_j^{r_j}}\right)^{\frac{1}{x_i}}) =$$

$$\prod_{s \neq i} e(g,g^{x_s r_s}) e(g,\frac{H(m)}{\prod_{j \neq i} y_j^{r_j}}) = \prod_{s \neq i} e(g,y_s^{r_s} \cdot \frac{H(m)}{\prod_{j \neq i} y_j^{r_j}}) =$$

$$e(g,\prod_{s \neq i} (\frac{y_s^{r_s}}{\prod_{j \neq i} y_j^{r_j}}) H(m) = e(g,1 * H(m))$$

c.n.d

8 Metody uwierzytelniania:

podmiot(strona) uwierzytelniany
podmiot (strona) uwierzytelniający

8.1 Hasła

A dostaje od zaufanej strony certyfikat: Cert=($Id_{A,f}$, f(wD)), gdzie f jest zadaną funkcją jednokierunkową a ‘w’- hasło

Uwierzytelnianie:

A „wpisuje” w, system oblicza f(w) i przekazuje do B

8.2 Protokół wyzwanie- odpowiedz

Zakładamy, że A i B

I) B generuje losowe wyzwanie r

II) A odpowiada i przekazuje do B wartość f(s,r), gdzie f jest zadaną funkcją jednokierunkową

III)B wykonuje to samo obliczenie i uwierzytelnia A jak wyniki zgadzają się

8.3 Uwierzytelnianie w systemie z kluczem publicznym

s-sekret strony A, S=Φ(s) wartość przekazana dla B

Wtedy powyższy protokół można identyfikować z „podpisem” strony A pod wiadomością „r”.

8.4 Protokół LAMPORTA

A generuje losowe w i oblicza ciąg wartości funkcji haszującej

$h(w), h(h(w))=h^2(w),\ldots\ldots,h^k(w)=h(h^{k-1}(w))$

Niech $Cert=(Id_A, h, h^k(w))$ będzie certyfikatem strony A

<u>Uwierzytelnianie</u>:

Strona A przekazuje $h^{k-1}(w)$ i Cert dla B

Strona B oblicza $h(h^{k-1}(w))$ i sprawdza zgodność z wartością w certyfikacie

W kolejnych uwierzytelnieniach strona A przekazuje do B wartość h^{k-1} a strona B sprawdza czy $h(h^{k-1}(w))=h^{k-1}$

8.5 Protokół FIATA-SHAMIRA

Jest to protokół o wiedzy zerowej, w którym strona uwierzytelniana dowodzi, że zna pewną tajemnice a strona B z prawdopodobieństwem bliskim jedności przekonuje się o wiarygodności A. W czasie protokołu B nie uzyskuje, żadnej wiedzy na temat tajemnicy strony A

5) A losuje s i oblicza $y=s^2(\text{mod } n)$, które przekazuje do B wraz z certyfikatem
6) B generuje losowe r ($1<r<n$) oraz b $\epsilon\{0,1\}$ i przesyła do A
7) A oblicza i wysyła do B wartość $t^b * r(\text{mod } n)$
8) B sprawdza czy $(t^b * r)^2=x^b * r^2(\text{mod } n)$

(II,III,IV)-tzw. Runda

Tę rundę powtarzamy k- razy wtedy prawdopodobieństwo „fałszywego” uwierzytelniania nie przekracza 2^{-k}

Bezpieczeństwo tego protokołu Fiata- Shamira wynika stąd, że pierwiastkowanie(kwadratowe) modulo liczba złożona jest protokołem obliczeniowo trudnym. O ile nie znamy rozkładu na czynniki pierwsze.

Agitacja:

Powiedzmy, że znany jest wydajny algorytm C, który znajduje dla losowego

$y \in (Z_n^*)^Z$ wartości któregokolwiek losowego z 4 pierwiastków z

$\sqrt{y}(\mathrm{mod}\, n)$

Wykorzystując te wartość dwukrotnie otrzymamy, że jeśli $\sqrt{y} = x_1$ i $\sqrt{y} = x_2$

to $(x_1 * x_2^{-1})^2 = y * y^{-1} = 1 (\mathrm{mod}\ n)$

Zatem algorytm C pozwala efektywnie znaleźć każdy pierwiastek kwadratowy z 1(modulo n) to oznacza, że znajduje losową wartość x, spełniającą równanie $x^2 = 1 (\mathrm{mod}\ n)$.

Zatem obliczając NWD(x-1, n) z prawdopodobieństwa ≥ 0,5(jedna druga) znajdziemy nietrywialny dzielnik pierwszej liczby n.

To wynika z faktu, że jeśli x=1(mod p) i x=-1(mod q)

lub x=-1(mod p) i x=1(mod q)

to NWD (x-1, n)=p

lub NWD(x-1,n)=q

9. Kryptoanaliza systemu Rivesta – Shamira – Allemana (RSA)

Oznaczenia:

N =p*q (p, q – duże liczby pierwsze)
e – wykładnik szyfrujący
d – wykładnik deszyfrujący (prywatny) e*d=1 mod (p-1)(q-1)
E: $Z_n \rightarrow Z_n$ – funkcja szyfrująca $E(m)=m^e(\mathrm{mod}\ n)$
D: $Z_n \rightarrow Z_n$ – funkcja deszyfrująca $D(m) = m^d(\mathrm{mod}\ n)$
S: $Z_n \rightarrow Z_n$ – funkcja podpisu $S(m)=m^d(\mathrm{mod}\ n)$
V: $Z_n \rightarrow Z_n$ – funkcja weryfikacji podpisu $V(m)=m^e(\mathrm{mod}\ n)$

Funkcja nadmiarowości:

Dla bezpieczeństwa systemu RSA wprowadzamy funkcję nadmiarowości h: $Z_n \rightarrow Z_n$, która powoduje dołączenie dodatkowych bitów do wiadomości. Powody tego są następujące:

3. Arytmetyczny charakter funkcji RSA (pozwala bo w szczególności na podpisanie dowolnej wiadomości zależnej multiplikatywnie od już podpisanych wiadomości bez znajomości klucza prywatnego) np. m_1 i m_2
   $S(m_1)=m_1^d(\text{mod } n)=S(m_2)=m_2^d(\text{mod } n)$
   $S(m_1,m_2)=(m_1m_2)^d=S(m_1)*S(m_2)(\text{mod } n)$

4. Bezpieczeństwo semantyczne – szyfrogram może mieć pewne informacje na temat wiadomości np. funkcja RSA zachowuje symbol JACOBIEGO $\left(\frac{m}{N}\right)$ tzn. $\left(\frac{m}{N}\right)=\left(\frac{RSA[m]}{N}\right)$. Załóżmy, że $\left(\frac{m}{N}\right)=1$ i wtedy $RSA(m)=m^d$ więc $\left(\frac{RSA(m)}{N}\right)=\left(\frac{m^d}{N}\right)=\left(\frac{m}{N}\right)^d=1=\left(\frac{m}{N}\right)$ na mocy multiplikatywności symbolu JACOBIEGO oraz faktu, że wartości J są z {-1,0,1} oraz d jest nieparzyste.

5. Determinizm – jeśli szyfrogram jest funkcją zależną jedynie od oryginalnej wiadomości to podsłuchujący może łatwo ustalić, czy dwa kryptogramy pochodzą od tej samej wiadomości. Dla uniknięcia takiej sytuacji stosujemy zrandomizowaną funkcję nadmiarowości (lub znacznik czasowy)

System RSA zmodyfikowany funkcją nadmiarowości:
$E(m)=h(m)^e(\text{mod } n)$ $D(m)=h^{-1}(m^d) \text{ mod } n$ $h(m)=m||b_1||\_||b_k$ $b_i \in \{0,1\}$
$S(m)=h(m)^d(\text{mod } n)$ $V(m)= h^{-1}(m^e) \text{ mod } n$

Rodzaje ataków:

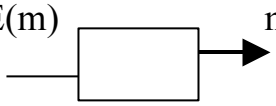
3. Klasyfikacja według "siły" ataku
   d. Tajność złamana – poznanie klucza prywatnego
   e. Całkowita dedukcja – szyfrogram zdeszyfrowany bez znajomości klucza prywatnego
   f. Częściowa dedukcja – jw. ale tylko dla pewnego podzbioru wiadomości (uprzednio nieznanych)
   g. Częściowa informacja – możliwość uzyskania nietrywialnej informacji na temat wiadomości z jej kryptogramu

4. Klasyfikacja ze względu na założenia (typ ataku)

e. Atak pasywny – znany jest jedynie kryptogram wiadomości
f. Atak ze znanym tekstem jawnym – dysponujemy pewnym zbiorem kryptogramów i odpowiadającym im wiadomości.
g. Nieadaptywny atak z wybranym szyfrogramem – dysponujemy dostępem do „wyroczni" deszyfrującej, co pozwala na zdeszyfrowanie wybranych przez nas kryptogramów
h. Adaptywny atak z wybranym szyfrogramem – mamy dostęp do „wyroczni" w chwili przeprowadzania ataku, deszyfrujemy p[pewien kryptogram o który pytaliśmy wyroczni.

Uwaga: Analogicznie identyfikacja typów siły ataku mamy dla podpisu cyfrowego.

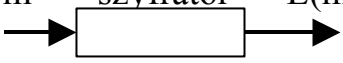
Przykład: nieadaptatywnego ataku z wybranym szyfrogramem

4) E(m)  m

szyfrujemy kluczem publicznym właściciela karty

5) dostęp do urządzenia szyfrującego np. niezabezpieczonego komputera

m szyfrator E(m)



Ataki na RSA:

4) Atak CoperSwitha – przy małym kluczu RSA i małych wiadomościach
5) Atak Hastada – stosowany np. gdy wiadomość jest wysyłana do różnych adresatów (lub jej kopia)
6) Ataki wykorzystujące powiązane wiadomości – 2 podobne wiadomości z podpisami

Ad 1.
$m^e \pmod n$ dla e=3 (np.)
wtedy deszyfrogram jest pierwiastkowany w Z (ale nie w Z_n) i stosujemy algorytm przeszukiwania binarnego

Ad 2.
Zakładamy, że k>e k-liczba adresatów. Ten sam klucz publiczny dla różnych modułów RSA na mocy chińskiego twierdzenia o resztach obliczamy $m^e \pmod{N_1,...,N_k}$ i pierwiastkujemy w Z

Ad 3.
$m_1=f(m_2)$ f-wielomian małego stopnia

Znajdujemy $e_1=m_1^e$ i m_2^e (mod n)
m_2 jest wspólnym pierwiastkiem wielomianu $g_2(x)=x^e-c_2$(mod n)
$g_1(x)=f(x)^e-c_1$(mod n)

zatem obliczając NWD($g_1(x)$, $g_2(x)$) znajdujemy czynnik liniowy x-c i wtedy m_2-c=0(mod n) => m_2=c(mod n) czyli poznajemy wiadomość m_2

10. Bezpieczeństwo semantyczne schematu szyfrowania

Def.

Funkcja f: N -> R nazywamy zaniedbywalną, jeżeli $\forall_{E} > 0$, $\exists_{K=KC}$ i $\forall_{k>kc}$
$|f(k)| < k^{-c}$

Def.

Powiemy, że funkcja F: N->e jest wielomianem ograniczonym, jeśli istnieje wielomian p: N ->R o współczynnikach rzeczywistych, taka że $\forall_{i \in N}$
$|f(i)| \leq |p(i)|$

Def.

Funkcja f: NxR->R nazywamy rozszerzoną funkcją zaniedbywalną jeśli dla każdej wielomianowo ograniczonej funkcji n zaniedbywalną jest funkcja g:N->R określona następująco: g(x)=f(x,n(x))

A(wejście)=wyjście

W dalszym ciągu będziemy zakładać, że A jest pewnym wielomianowym algorytmem probabilistycznym. Dla zdarzenia Z, pr(Z) oznacza jego prawdopodobieństwo. Podobnie jeśli x to zmienna losowa, to prawdopodobieństwo, że x przyjmuje wartość d ozn. Pr[x=d].

Schemat szyfrowania:

Szyfr asymetryczny to trójka probabilistycznych algorytmów E=(Ekg,E,D) działających w czasie wielomianowym od parametru bezpieczeństwa k, takim że :

6. Ekg(1^k) = (e,d) = Ke x Kd; e,d to odpowiedni klucz publiczny i prywatny. Zbiór K = {(e',d') : $\exists_K : pr[EKg(1^k) = (e',d') > 0]$ nazywamy przestrzenią

kluczy.

7. E Ke x M -> C Algorytm E nazywamy algorytmem szyfrującym, M i C to przestrzeń wiadomości i kryptogramów.
8. D Kd x C ->M Algorytm D nazywamy algorytmem deszyfującym.
9. Dla dowolnej pary (e,d) $\in K$ zachodzi równość

$\forall_{m \in M} pr[D(d, E(e,m)) = m] = 1 - E(k)$ dla pewnej funkcji zaniedbywalnej E.

Własności schematy szyfrującego:

A – przeciwnik

Eksperyment $Exp_{E,A}^{(k)}$

5. $Ekg(1^k) \rightarrow (p_k, s_k)$
   $A(p_k) \rightarrow (m_0, m_1, state)$
   $A(E_{pk}(m_b), state) \rightarrow d \quad d=\{0,1\}$

Wynikiem eksperymentu jest 1, gdy d=b.
Niech $Exp_{E,A}^{(k)}$ oznacza eksperyment, w którym w pierwszym kroku losujemy wartość b={0,1} z rozkładem jednostajnym. Wtedy prawdopodobieństwo sukcesu wynosi

$pr[Exp_{E,A}^{(k)}=1] =$
$= \sum_{x,y \in \{01\}} pr[\mathrm{Exp}_{E,A}(k) = 1, b = x, d = y] = \sum_{z \in \{0,1\}} pr[b = z, d = z] = \sum_{z \in \{0,1\}} 1/4 = 1/4 = 1/2$

Def.
Przewagą przeciwnika w eksperymencie $Exp_{E,A}^{(k)}$ jest wartość
$Adv_{E,A}(k) = |pr[Exp_{E,A} = 1] - pr[Exp_{E,A} = 1]|$

Def.

Schemat szyfrowania jest semantycznie bezpieczny (ma własność nieodróżnialności) jeśli dla wszystkich algorytmów probabilistycznych A o złożoności wielomianowej $Adv_{E,A}(k)$ jest funkcją zaniedbywalną.

11. Hierarchie dostępu

11.1 Motywy dostępu:

- wspólne użytkowanie systemów informatycznych

- współdzielenie zasobów

- administrowanie zasobem

- kontrola dostępu

- praktyczność struktur hierarchicznych

Def.

(V, ≤) nazywamy porządkiem częściowym na V jeśli ≤ jest relacja dwuczynnikową na która jest zawarta przechodniość antysmetryczność tj. V ≤ V

$\forall\, v \in V$

$V_1 \leq V_2 \_ i \_ V_2 = V_3 \Rightarrow V_1 = V_3$

$V_1 \leq V_2 \_ i \_ V_2 \leq V_1 \Rightarrow V_1 = V_2$

Polityka przepływu interakcji wg. modelu BELL-LA-PADULA. W takim modelu x ≤ y oznacza, że informacja może przepływać od x d y (w górę hierarchii)

Def.

Polityka bezpieczeństwa to piątka (V_1, ≤, P, O, λ): V- zbiór klas bezpieczeństwa V={v_1,v_2,v_3,…,v_n} P- zbiór podmiotów (użytkowników) O- zbiór obiektów

$\lambda : O \cup P \rightarrow V$ - *funkcje _ kontroli _ bezpieczenstwa*

Operacja (przykładowa):

- czytanie informacji zawartych w obiekcie
- zapis do obiektu
- dopisywanie do obiektu
- wykonywanie programu

Ustalając operacje powiemy, że jest ona dowolnie dla pary (P, O) wtedy i tylko wtedy, gdy $\lambda(p) \geq \lambda(o)$

Każdemu obiektowi przypisany jest jeden klucz bezpieczeństwa $\lambda(a)$

Każdemu podmiotowi przypisane są dwa podmioty (elementy zb. Klas bezpieczeństwa) $\lambda(p) = \lambda_{bież}(p)$ oraz
$\lambda(p) = \lambda_{dow}(p)$

Jeżeli n jest zadanym wprowadzeniem to trójka (p, o, n) opisuje uprawnienie podmiotu p do obiektu o w danym momencie tzn. przy uprawnieniu do obiektu
$O \Leftrightarrow \lambda(p) \geq \lambda(a)$

W danym ciągu politykę bezpieczeństwa dostępu do danych $(V_1, \leq, P, O, \lambda)$ będziemy ograniczać do pary (V,E).

Przykład:

$V=(v_1,v_2,v_3,v_4)$

v_1- poziom jawny

v_2- informacje poufne

v_3- informacje tajne

v_4- informacje ściśle tajne

11.2 Grafy skierowane

W dalszym ciągu będziemy patrzeć na reprezentacje wyjściowego porządku (V,≤) jako zadane przez graf (acykliczny i skierowany) G=(V, E)

Polityka bezpieczeństwa realizuje się przez przypisanie każdej klasie $v \in V$ klucza k od V, który ma strzec „dostępu" do obiektu w klasie v tj. takich, że $\lambda(o)=v$

Oznaczenia:

$G^-(v)=\{w \in V$; istnieje ścieżka w do V$\}$

$G^+(v)=\{w \in V$; istnieje ścieżka v do w$\}$

D(v)- zbiór bezpośrednich potomków w (dzieci)

R(v)- zbiór bezpośrednich przodków (rodziców)

Def.

Schematem przedziału kluczy nazywamy parę dwóch algorytmów wielomianowych (sat, Derive) określonych jak następuje
Set(1^l,G) jest randomizowanym algorytmem, który na wejściu dostaje parametr bezpieczeństwa 1^l a na wyjściu dwa odwzorowania:

- publiczne Pub: $V \cup E \rightarrow \{0,1\}^*$,który przypisuje wierzchołkom w grafie pewne parametry publiczne oraz krawędzie (v_i, v_j) pewne etykiety publiczne.

- tajny sec: $V \rightarrow \{0,1\}^* * \{0,1\}^l$, który przypisuje każdemu wierzchołkowi pewna prywatna informacje z funkcją s= s(v) oraz klucz k= k(v), v ϵ V

-Derive (G, Pub, v_i, v_j, s_i) jest deterministycznym algorytmem, który na wyjściu pobiera publiczna (graf G) informację. Pub wygenerowane przez algorytm set wierzchołek barwiony v_i dowolny, vj którego klucz chcemy obliczyć oraz tajna informacje s_i wierzchołka w_i. Algorytm zwraca klucz k_j $=k_i(v_j)$ dla wierzchołka v_j o ile $v_j \in G_r^+(V_i)$ lub specjalny symbol $\perp$ w przeciwnych przypadkach

Dla poprawności, algorytmy: Set i Derive musza spełniać następujący warunek poprawności dla każdego

$$\forall v \in V \_\_\_ \forall v_j \in G_v^+(V_i) \_\_\_ \Pr\left[\begin{matrix} k_j = Derive(G, Pub, v_i, v_j, s_i) \_\_ (PUB, set) = set(1^l, G) \\ (s_i, k_i) = Sec(v_i) \qquad\qquad (s_j, k_j) = Sec(v_j) \end{matrix}\right]$$

Przy losowych wyborach algorytmu set

G=(V,E) – graf skierowany
P,Q,R – parami rozłącznie zbiory liczb pierwszych (nieskończone), oraz takie że:

$P \cap Q = \emptyset$, $P \cap R = \emptyset$, $Q \cap R = \emptyset$

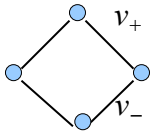
P - aspekt – odpowiedzialny zasadniczo za bezpieczne usuwanie wierzchołków grafu

Q – aspekt – zasadniczo odpowiedzialny za dodawanie nowych wierzchołków do grafu

Załóżmy dla uproszczenia, że *V* jest grafem takim że:

$v_- \leqslant v \leqslant v_+$

Na rysunku można to przedstawić w następujący sposób:

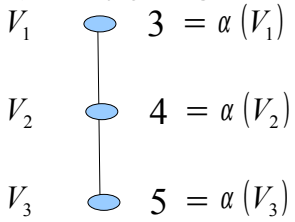


P – aspekt

$\forall p \in P$ rozważmy funkcje $\alpha_p : V \to N_0$ (N_0 - zbiór liczb całkowitych nieujemnych), która spełnia następujące warunki:
1) $v_1 \leq v_2 \Rightarrow \alpha_p(v_1) \geqslant \alpha_p(v_2)$
2) min $\alpha_p(v) > \alpha_p(v_-) - \alpha_p(v_+)$, przy założeniu że $v_- \leqslant v \leqslant v_+$

Przykład

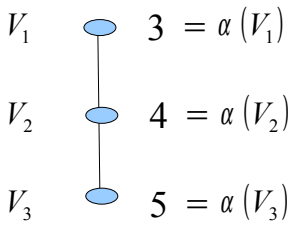
1) Dany jest graf *G(V, E)*, należy sprawdzić czy spełnione są warunki 1) i 2)



Pierwszy warunek jest spełniony (1 < 2 < 3) natomiast 2) już nie gdyż 1 < 3 – 1 = 2.

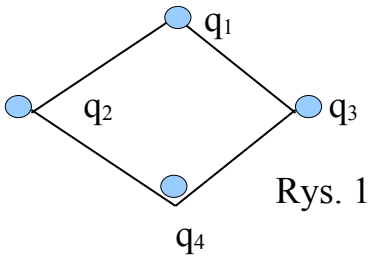
2) Dany jest graf *G(E,V)*, należy sprawdzić czy spełnione są warunki arytmetyki modularnej.

3)

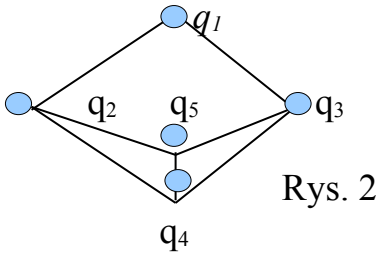


W tym grafie pierwszy warunek jest spełniony (3 < 4 < 5), jak i również warunek drugi (4 > 5 – 3 = 2)

11.3 Q – aspekt (odpowiedzialny za dodawanie wierzchołków)



Rys. 1



Rys. 2

Rysunek nr 1 to hierarchia przed dodaniem nowego wierzchołka:

$Q_1 = q_1\ q_2\ q_3\ q_4$

$Q_2 = q_2\ q_4$

$Q_3 = q_3\ q_4$

$Q_4 = q_4$

Następnie dodajemy nowy wierzchołek:

$q_5 \in Q \setminus \{ q_1, q_2, q_3, q_4 \}$

Rysunek 2 przedstawia hierarchię z nowym wierzchołkiem:

$Q_1 = q_1\ q_2\ q_3\ q_4\ q_5$

$Q_2 = q_2\ q_4\ q_5$

$Q_3 = q_3\ q_4\ q_5$

$Q_4 = q_4$

$Q_5 = q_5\ q_4$

11.4 Dodawanie nowych wierzchołków – dzielenie funkcji dostępu

Załóżmy, że dodajemy nowy wierzchołek $v_0 \in V$, wtedy przypisujemy mu

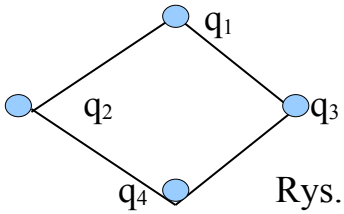
liczbę pierwszą $q_0 \in V$ i definiujemy rozszerzenie :

$$\tilde{f} : V \cup v_0 \Rightarrow Q$$

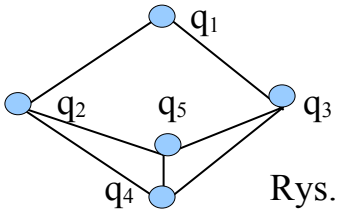
$$\tilde{Q}(v) = \begin{cases} Q(x) \; jeśli \; v \geq v_0 \\ q_0 Q(v) \; jeśli \; v \leq v_0 \end{cases}$$

$$\tilde{a}(x) = \frac{P(v)}{\tilde{Q}(v)} \quad mod\ m$$

Przykład:



Rys. 1



Rys. 2

$Q(v_1) = q_1\, q_2\, q_3\, q_4$

$Q(v_2) = q_2\, q_4$

$Q(v_3) = q_3\, q_4$

$Q(v_4) = q_4$

$\tilde{Q}(v_5) = q_4 q_5$

$\tilde{Q}(v_4) = q_4$

$\tilde{Q}(v_3) = q_3 q_4 q_5$

$\tilde{Q}(v_2) = q_2 q_4 q_5$

$\tilde{Q}(v_1) = q_1 q_2 q_3 q_4 q_5$

11.5 Usuwanie wierzchołków i określenie k(v)

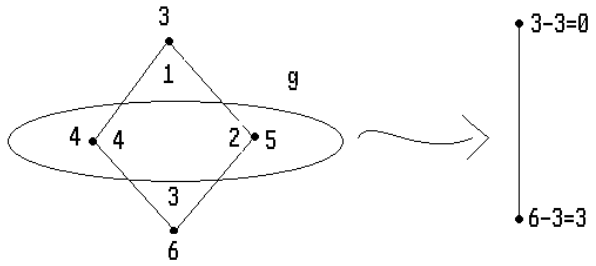
Niech . $V(G) = \{w : v_- \leq w : v_+\}, S = \{v_1, v_2, \ldots, v_r\} \subset V$ Mamy $\alpha = \alpha_p \; (p \in P)$ i definiujemy $\delta = \delta(S) = \alpha_p(v_-) - \min_{v \in S} \alpha_p(v_+) + 1$

Nowe funkcje :

$$\tilde{\alpha}_p : V \setminus S \rightarrow \mathbb{N}_0$$

$$\tilde{\alpha}_p = \alpha_p - \delta$$

Przykład:



Definicja Klucz w hierarchii:

Wartość klucza dla wierzchołka *v* wynosi $k(v) = \gamma^{a(v)} \pmod m$ gdzie $m = \lambda(n)$, natomiast γ jest elementem rzędu $\lambda(n)$ w grupie Z_n^* .

$$a(v) = \frac{P(v)}{Q(v)} \pmod m$$

11.6 P –aspekt (odpowiedzialny za usuwanie wierzchołków)

Budujemy funkcję $\alpha_p : V \to N_0$ ($p \in P$), taką że

6. $v \geqslant w \Rightarrow \alpha(v) \leqslant \alpha(w)$
7. Dla dowolnego pod-grafu $G' \subset G$, $V' \subset V$,
   takiego że $V' = \{w : v_- \leqslant w \leqslant v_+\}$ zachodzi warunek $2\alpha(v_-) > \alpha(v_+)$

W praktyce warunek 2) będziemy zastępować warunkiem 2')

2') $min\ \alpha_p(v) > \alpha_p(v_-) - \alpha_p(v_+)$

Jeżeli ścieżka ma długość *N* to możemy definiować:

$\alpha(v_+) = N + 1$

$\alpha(v_-) = 2N$

$2\alpha(v_+) = 2N + 2 > 2N$

Funkcje dostępu wyglądają następująco:

$k(v) = q^{a(v)} \pmod n$

$a(v) = P(v) / Q(v)$

$P(v) = P^{\alpha p(v)}$

teraz:

$a(v_1) = P(v_1) / Q(v_1) = P^3 / q_1q_2q_3q_4$
$a(v_2) = P^4 / q_2q_4$
$a(v_3) = P^5 / q_3q_4$
$a(v_4) = P(v_4) / Q(v_4) = P^6 / q_4$
$k(v_2) = (k(v_1))^{pq_1q_3}$

Przykład

Wyrazić przez potęgowanie klucz k_4 za pomocą kluczy k_1, k_2, k_3.

Rozwiązanie:

$$k(v_4)=(k(v_3))^{pq_3}$$
$$k(v_4)=(k(v_2))^{p^2q_2}$$
$$k(v_4)=(k(v_1))^{p^3q_1q_2q_3}$$

Przykład

$n = p*q \quad p-1 = 2q' \qquad (p,q,p',q' - \text{liczby pierwsze} \in R)$
$n = \lambda(n) = NWW(p-1,q-1) = NWW(2p',2q') = 2p'q' = \frac{\varphi(n)}{2}$
γ - element rzędu $\frac{\varphi(n)}{2}$,
$k(v)=\gamma^v \pmod n$

Obliczanie funkcji Eulera

$\phi(p)=p-1$
$\tilde{\phi}(p)=p^{\alpha-1}(p-1)$
$\phi(p,q^0)=p^{\alpha-1}(p+1)q^{\beta-1}(q-1)=\phi(p^\alpha)\phi(q^\beta)$
$\phi(p^\alpha,q^\beta)=p^{\alpha-1}(p-1)+q^{\beta-1}(q-1)=\phi(p^\alpha)\phi(q^\beta)$

Przykład

N=pq=3*11
p-1=2=2*1=2p`

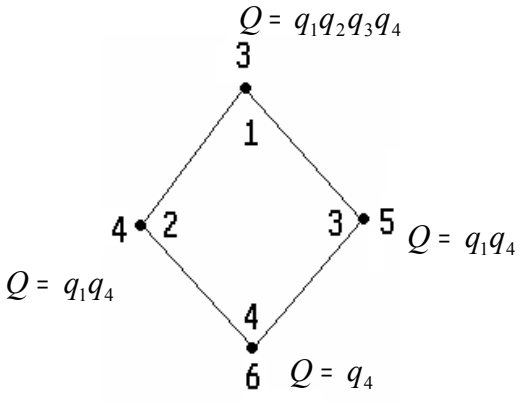
q-1=11=11-1=10=2*5=2q`

$$\varphi(n) = \varphi(pq) = \varphi(p)\cdot\varphi(q) = (p-1)(q-1) = 20$$

$$m = \lambda(n) = \frac{\phi(n)}{2} = \frac{20}{2} = 10$$

γ jest elementem rzędu 10 w grupie Z_{33}^{*}

Przykład: Obliczanie kluczy w hierarchii



$$P(v) = p^{\alpha_p(v)} \qquad (p=7)$$

$$k(v) = \gamma^{\frac{P(v)}{Q(v)}} = \gamma^{\frac{p^{\alpha_p(v)}}{Q(v)}}$$

$$k(v_1) = \gamma^{\frac{P(v)}{Q(v)}} = \gamma^{\frac{7^3}{q_1 q_2 q_3 q_4}}$$

$$k(v_2) = \gamma^{\frac{7^4}{q_2 q_4}}$$

$$k(v_3) = \gamma^{\frac{7^5}{q_3 q_4}}$$

$$k(v_4) = \gamma^{\frac{7^6}{q_4}}$$

11.7 Hierarchia potęgowa

Problem I (logarytmu dyskretnego dla G)

Dana jest multiplikatywna grupa G i generator g ∈ G oraz
A ∈ G. Znaleźć (o ile istnieje) wartość $\log_g(A)=x : g^x=A(w\,grupie\,G)$.

Problem II

Niech $s=\{k_1, k_2, ..., k_r\}\setminus\{k_j\}, j\in r \quad x=x_1\,x_2\,...\,x_r$
Dane: $g^{x/x_j}, j=1,2,...r(w\,grupie\,G)$
Szukamy: g^x

Problem obliczenia g^x na podstawie g^{x/x_j} jest obliczeniem trudnym – decyzyjny problem D-H (Diffie-Hellmana).

Przykład:

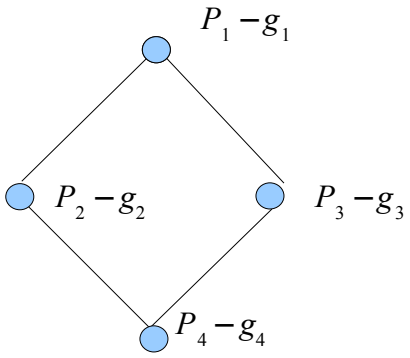
$r=2,\ x=x_1\,x_2,\ x_i\in N, G=Z_p^*$
Dane: $g^{x/x_1}=g^{x_2}\ oraz\ g^{x/x_2}=g^{x_1}(mod\ p)$
problem D-H to obliczenie $g^x=g^{x_1 x_2}(mod\ p)$
$[(g^{x_1})^{x_2}=(g^{x_2})^{x_1}]$ czyli trzeba obliczyć $\log x_1\ lub \log x_2$

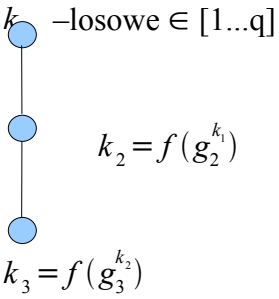
11.7.1 Diagram Hasse

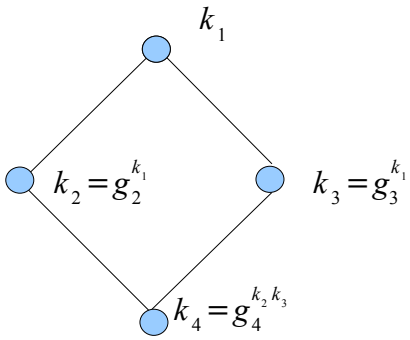
Funkcja pomocnicza: $f : G\to\{1,2,..,q\}$
G – podgrupa Z_p^* rzędu q $(q=\frac{p-1}{2})$

$$f(x)=\begin{cases} x\ jeśli\ 1\leqslant x\leqslant q \\ p-x\ jeśli\ x>q \end{cases}$$

Parametry systemu g_i – dowolny generator grupy G (odpowiadający graczowi P_i).







$K_4 = [g_4^{k_2}, g_4^{k_3}]$ P_2 *oblicza* $k_4 : (g_4^{k_3})^{k_2} = g_4^{k_2 k_3} = k_4$

11.7.2 Faza generacji kluczy

Algorytm

1. P_i losuje g_i – generator G
2. Jeśli P_i nie ma rodzica to k_i – losowe z przedziału {1, 2, ..., q}
3. Jeśli ma dokładnie jednego rodzica P_j , to
   $k_i = f(g_i^{k_j})$
4. Jeśli $P_{j1} \dots P_{jn}$ są rodzicami P_i to:
   $k_i = f(g_i^{k_{j1} k_{j2} \dots k_{jr}}) - klucz\ prywatny$
   $K_i = [h_{ij1}, h_{ij2}, \dots, h_{ijr}] - klucz\ publiczny$

11.7.3 Faza obliczania kluczy

Jeśli P_i ma dokładnie jednego rodzica P_j to $f(g_i^{k_j})$
w przeciwnym wypadku wybieramy jako P_j dowolnego rodzica i :

$$k_i = f(h_{ij}^{k_j})$$

11.7.4 Złożoność obliczeniowa

Potęgowanie modularne
$(a, b) \to a^b \bmod n \qquad a, b \leqslant n$
zapisujemy *b* dwójkowo

$$c = c_0 * 2^0 + c_1 * 2^1 + ... + c_k * 2^k$$

$$k \leqslant \log_2 n$$

$$a^b = (a^{2^0})^{c_0} * (a^{2^1})^{c_1} * ... * (a^{2^k})^{c_k} (mod\ n)$$

$(a^{2^k}) = (a^{2^{k-1}})^2$ – *więc obliczenie* a^b *sprowadza się do co najwyżej k podnoszeń do kwadratu*

Jeśli przez M oznaczymy operację mnożenia, a P podniesienie do kwadratu modulo n, to ostatecznie mamy:
koszt $a^b (mod\ n) \leqslant kM + kP \leqslant (\log_2 n) M + (\log_2 n) P$

12. Systemy dowodzenia

Def.
System dowodzenia nazywamy parę (P,V): P – strona, V – strona weryfikująca gdzie P przekazuje V, że zna pewien sekret (np. rozwiązania pewnego problemu). P i V są wyposażone w algorytmy probabilistyczne, gdzie V jest algorytmem wielomianowym.

Def.
Interaktywny system dowodzenia nazwiemy parę (P,V), gdzie P i V są połączone kanałem komunikacyjnym i każda ze stron może być w jednym z trzech nietrywialnych stanów (otrzymanie wiadomości, wysyłanie wiadomości, obliczanie)

Def.
System dowodzenia z wiedzą zerową nazywamy taki system (P,V), w którym V nie "dowiaduje" się niczego na temat sekretu strony dowodzącej.

Przykład 1
Dowód i wiedzy zerowej znajomości izomorfizmu dla grafów G_1 i G_2. Jest to przykład dowodzenia, gdy dany jest pewien (trudny) problem decyzyjny M i P dowodzi, że pewna instancja tego problemu jest instancją z odpowiedzią TAK.

Takie dowody powinny posiadać dwie własności:

1. Kompletność – jeśli X jest instancją z odpowiedzią TAK dla problemu M to weryfikujący zawsze zaakceptuje dowód P
2. Poprawność – jeśli X jest instancją z odpowiedzią NIE problemu M to prawdopodobieństwo, że V zaakceptowanie dowodu jest "małe"

Dane $G_1=(V_1,E_1)$, $G_2=(V_2,E_2)$
Pytanie Czy grafy są izomorficzne, czyli czy istnieje bijekcja $\Pi:V_1->V_2$, taka że (u,v) należy do E_1 wtedy i tylko wtedy gdy (Π (u), Π (v)) należy do E_2

W dowodzie izomorfizm G_1,G_2, P "generuje" graf H (otrzymany z G_1, przez permutację jego wierzchołków i w zależności od zapytania verifier'a pokazuje izomorfizm pomiędzy H i G_1 lub H i G_2

1. P H <- G_1 <- G_2
2. V {0,1}
3. P jest o to podaje Π a jak 1 to podaje $\Pi o^\circ \delta$

Kolejny przykład opiera się na trudności znajdowania logarytmów dyskretnych w pewnych grupach skończonych.

<u>Protokół I</u>
(dowód, że dwie pary (a,b) zawierają się w G^2, (c,d) zawierają się w G^2 mają ten sam znany P logarytm dyskretny $s=\log_a b=\log_c d$ czyli P zna wartość s)

1) V generuje losowe r i przekazuje P wartość $A=(ac)^r$
2) P oblicza A^s
3) V sprawdza czy $A^s=(bd)^r$

Kompletność wynika stąd, że $A^s=((ac)^r)^s=(a^s c^s)^r=(bd)^r$

<u>Protokół II</u>

(dowód znajomości logarytmu dyskretnego w grupie rzędu N)
P chce przekazać V, że zna x: $b^x=y$ w grupie G

1) P losuje e i oblicza $b'=b^e$ i przekazuje do V
2) V wybiera bit {0,1} i przekazuje bo P
3) P odpowiada wartością e gdy r=0 lub x+e(mod N) gdy r=1
4) V sprawdza czy $b^e=b'$, gdy r=0 lub $b^{x+e}=yb'$, gdy r=1
5) Kroki 1-4 powtarzane k – razy

Zastosowania praktyczne:
- podpisy grupowe

- identyfikacja – dowodzenie tożsamości