$[k]P$

kP $(G,+)$ $P \in G$ $P \oplus \cdots \oplus P$ (k volků)

$k = \sum_{i=0}^{t} k_i 2^i$

```
Q = 0; i = 0;
while (i < t) do
    if (k_i = 1) Q = Q + P;
    P = 2P;
    i++;
return Q
```

$\Leftarrow$ P_j (původní P) $\cdot 2^{i+1}$

$[k]P$

kP $(G,+)$ $P \in G$ $P \oplus \cdots \oplus P$ (k krát)

$k = \sum_{i=0}^{t} k_i 2^i$

```
Q = 0; i = 0;
while (i < t) do
    if (k_i = 1) Q = Q + P;
    P = 2P;
    i++;
return Q
```

$\Leftarrow P_j$ ("původní P") $\cdot 2^{j+1}$

ZNĚNÍM VÝŠE UVEDENÝM $k = \sum k_i 2^i$ TAK, ŽE PŘIPUSTÍME $k_i \in \{-1, 1\}$

$k = \sum k_i 2^i$ NESOUSEDNÉ VYJÁDŘENÍ (NON-ADJACENT)

$k_i \in \{-1, 0, 1\}$ $\forall i$ $0 \in \{k_i, k_{i+1}\}$

NEMÁME VEDLE SEBE NENULOVÉ HODNOTY

<u>LEMMA</u> $\forall k \in \mathbb{Z}$ $\exists!$ NAF (F = form)

D: $\exists$ STAČÍ PRO $n \geq 0$ $-n$ dodám $k_i \to -k_i$

POSTUPUJI INDUKCÍ

$n = 2m$ [m] 0

$n = 4m+1$ [m] 01

$n = 4m-1$ [m] 0-1

DÁLE SE POSTUPUJE PODOBNĚ JAKO V ČÁSTI $\exists$

0	0
1	1
2	10
3	10-1
4	100
5	101
6	10-10
7	100-1

JEDNOZNAČNOST.

n MÁ 2 RŮZNÁ VYJ.

INDUKCÍ $n = 0$

AŤ 0 $k_r \dots k_0$ z nejmenší kostí

$k_0 = 0$. $k_r \dots k_1$ kratší zápis

$k_0 \neq 0 \implies 0$ je liché číslo Σ

DÁ SE UKÁZAT, ŽE V PRŮMĚRU JE V NAF 1/3 ZÁPISU NENULY

—|— ŽE JE TO OPTIMÁLNÍ ZÁPIS V 0,1,-1 CO DO VÁHY

Váha zápisu je počet pozic $\neq 0$

Máme-li zápis k, který není v NAF, tak jeho váha $\geq$ váze v NAF

NAPŘ. 11   10-1

OBA ZÁPISY VÁHU 4

```
Q=0; i=0;
while (i<t) do:
   if(k_i=1) Q=Q+P;
   if(k_i=-1) Q=Q-P;
   P=2P;
   i++;
return Q
```

POVODNÍ ALGORITMUS

if $k_i = 1$

$Q = Q + P$;

$P = 2P$

P
2P
4P
8P

$k_{t-1} = 1$

$Q = P$;

$i = t-1$;

while $(i > 0)$ do;

$i = i - 1$;

$Q = 2Q$;

if $(k_i = 1)$ $Q = Q + P$;

Return Q;

ZLEVA DOPRAVA (OD VYSOKÝCH BITŮ)

ZPRAVA DOLEVA (OD NÍZKÝCH BITŮ)

$$k = \sum_{i=0}^{t-1} k_i 2^i < 2^t$$

(kdyby nebylo, tak si ho najdeme)

ZLEVA DOPRAVA SE LÉPE HODÍ PRO POSUVNÉ OKNO (SLIDING WINDOW)

SL. W.

MÁM PŘEDPOČÍTÁNO j^P $\quad 0 \leq j < b$

$\uparrow$ nejaká malá mocnina 2

$k = \sum k_i b^i \quad 0 \leq k_i < b$

```
Q = P;
i = t-1;
while (i >= 0) do
    i = i-1;
    Q = bQ;   (pokud b=2^r, tak v krát provedu 2Q)
    Q = PRE[k_i] + Q ;
RETURN Q;
```

1

LZE KOMBINOVAT S PŘESKAKOVÁNÍM NUL

$k = \sum_{i=0}^{t-1} k_i 2^i$

$k_i = 0$ $Q \to 2Q$

$k_i \neq 0$ DYNAMICKY SPOČÍTÁT

$s = k_i 2^{v-1} + k_{i+1} 2^{v-2} + \dots + k_{i+v-1} 2^0$

$Q \to 2^v Q + PRE[s]$

NAF SE DÁ POČÍTAT I ZEZDA DOPRAVA

$Q = P$ $i = t-1$

while

$i--$

$Q = 2Q$

if $k_i = 1$ $Q = Q + P$

$k_i = -1$ $Q = Q - P$

KOMBINACE NAF

A SLIDING WINDOW S PŘESK. NUL

V ČASE SLIBNÉ

NAF se dají počítat i pro větší základ než 2

Ať základ mocnina 2 ; $b = 2^v$

zapíšu k jako $\sum k_i 2^i$, kde $k_i \in \{-b+1, \dots, 0, \dots, b-1\}$

TAK ABY PLATILO 0000 MUSÍ BÝT
$\geq v$ nul MEZI NENULOVÝMI HODNOTAMI

∃ NAF PŘI ZÁKLADU $b = 2^v$
SE SPOČÍTÁ JENOM MODIFIKACÍ
POSTUPU PRO $b = 2$

$k = 2^v k'$ → VYUŽIJI ZÁPIS k'

2.2.4 (DOPLNÍTE)

$k = 2^{2v} k' + w$ $\quad w < 2^w$

w cifer