NÁSOBENÍ A DĚLENÍ

NÁSOBENÍ > 10× DELŠÍ NEŽ SČÍTÁNÍ

μproc > 3× (PARALELIZACE HW)

ZÁŽITKOVĚ ~1 (PIPELINING)

V μproc je DĚLENÍ 10× DELŠÍ NEŽ NÁSOB

2 HLEDISKA MULTIPLE-PRECISION ARITHM.

DĚLENÍ >> NÁSOBENÍ >> SČÍTÁNÍ

HLAVNÍ CÍL: VYHNOUT SE DĚLENÍ (INVERZI)

DĚLENÍ OBECNĚ?

RYZE TEOR. (PROJ. SOUŘADNICE)

HW ZÁVISLÉ

DĚL. 2, 4, 8, . . . 2^w

REALIZOVAT EF.

$W = 32, 64, 128$

SLOVO POČ.

ZÁS. PROBLÉM

SČÍTÁNÍ ✓

2. NÁS.

POČÍTÁNÍ MOD p

$0 \dots p-1$ $a, b \in \mathbb{Z}_p$ pokud bychom chtěli najít c

že $ab = pq + c$

BĚŽNÉ NÁS.

NAIVNÍ DĚLENÍ SE ZBYTKEM

JAK C NAJÍT

b

10

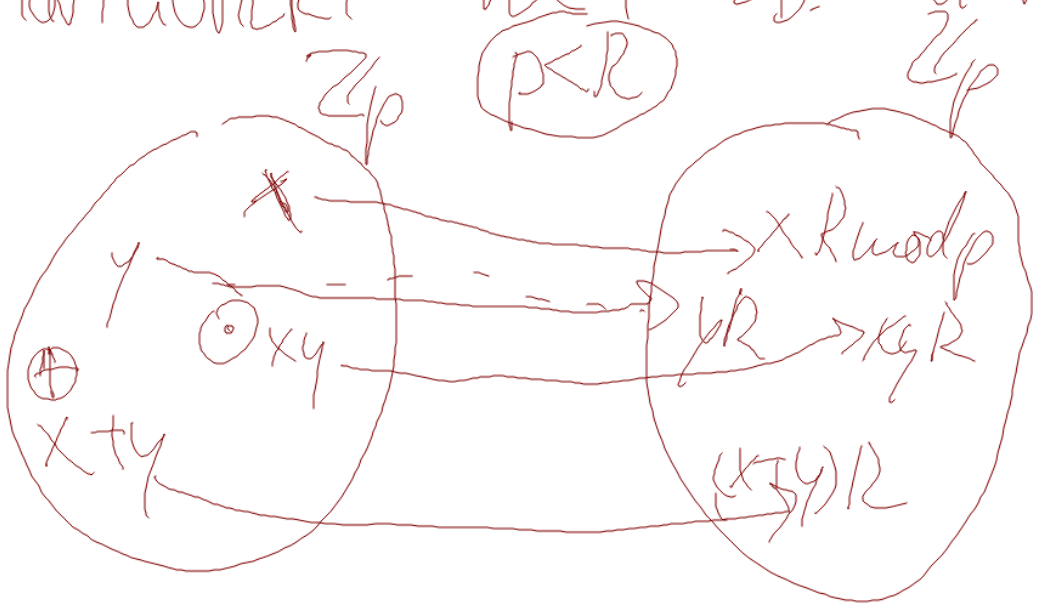
OBECNĚ $1/p$

SPECIÁLNÍ p

$xyR^2 \to xyR \bmod p$

$a \to aR^{-1} \bmod p$

MONTGOMERY VĚC 1 2D. KOMPLIKUJE



$R = b^t > p > b^{t-1}$

t počet slov kam se vejde p

SČÍTÁNÍ NEVÍ PROD.

$xR + yR \equiv (x+y)R \bmod p$

STAČÍ SEČÍST ZAPSAT MOD P

CO SI PŘEDS

JAK REAL V PAMĚTI POČ

Mohou vyhovovat dvojčíslo $xR \cdot yR = xyR^2 = a$

$0 \le a < p^2 < R^2$ Pokud z a UMím odvodit $b \in \mathbb{Z}_p$, $\exists b$ $bR = a \bmod p$

TAK b JE ZÁPIS $(xy) \bmod p$

A BUDE ZÁPIS $(x+y)$

CHCEME: z a, $0 \leq a < p^2$ ODVODIT p
$0 \leq b < p$, že $bR \equiv a \bmod p$

ZMĚNA ZNAČENÍ $(a,b) \rightsquigarrow (x,y)$

$0 \leq x < p^2$ HLEDÁME $y \equiv xR^{-1} \bmod p$ $R = b^c > p$

TENTO PROCES
MONTGOMERYHO REDUKCE

PŘEDPOČÍTANÁ HODNOTA Σ, $0 \leq \Sigma < p$

$\boxed{\Sigma p \equiv -1 \bmod R}$ (pokračujeme nejprve
p inverzní modulo R)

MYŠLENKA

$[x]_p = [x + xp\varsigma]_p$ $\quad x < p^2 \quad p < R$

$p\varsigma \equiv -1 \bmod R \implies R \mid x + xp\varsigma$ $\quad \frac{x+pu}{R} \cdot R \equiv x \bmod p$

VÝPOČETNĚ NEPOHODLNÉ $\quad p \sim b^t \quad \varsigma \sim b^t$

$x \sim b^{2t} \quad xp\varsigma \sim b^{4t}$ ŘÁD

CHCEME ZŮSTAT $< b^{2t}$ ŘÁD

SPOČÍTEJME NEJPRVE

UKR $\quad u = x\varsigma \pmod R$ ← LACINÉ

$R \mid x + pu$ $\quad (x+pu)/R$ odečíst

↑ ↑ dělení zdarma

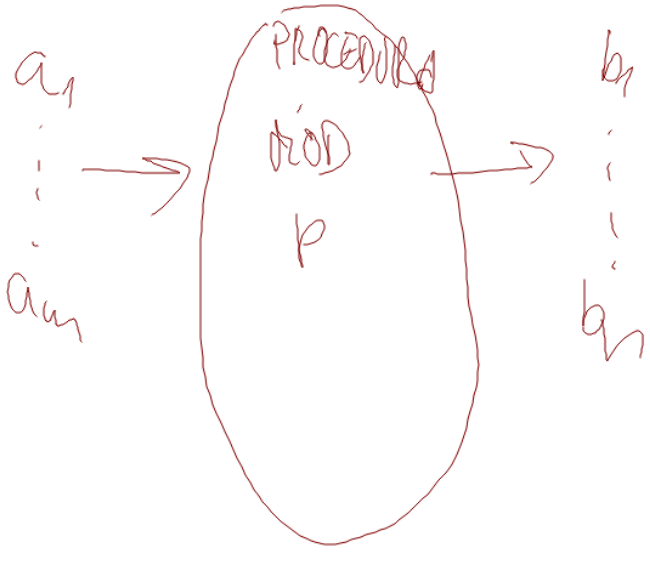
$\geq 0 \quad \geq 0$ $\quad 0 \leq \frac{x+pu}{R} < 2p$ $\quad$ Ať $z = \frac{x+pu}{R}$ $\quad$ VÝSTUP VINT RED.

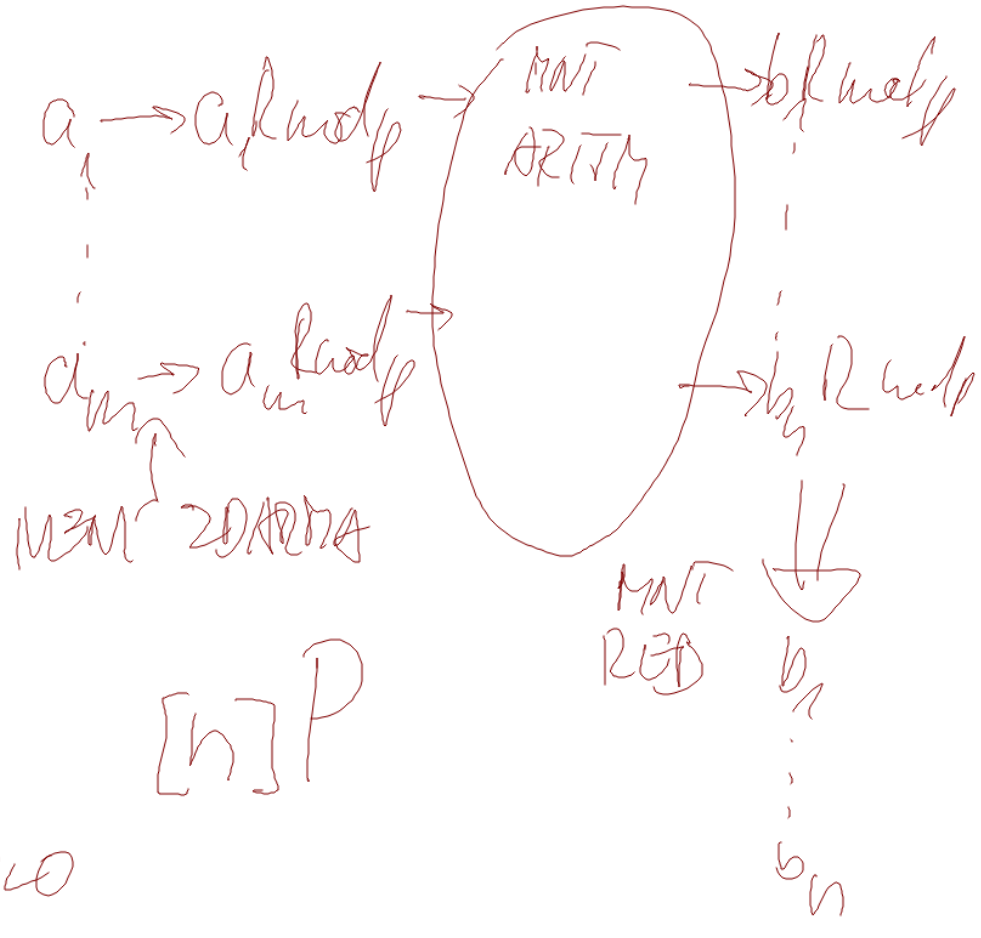
ODHAD $\frac{x+pu}{R}$ ODVODÍM Z ODHADU $\quad$ IF $z < p$ $\quad y = z$

$0 \leq x + pu < p^2 + pR < 2pR$ $\quad$ ELSE $\quad y = z - p$

$yR \equiv x \bmod p$

MNT ARITH





PROCEDURA NAD BYT
DOSTATEČNĚ RYCHLÁ,
ABY SE TO VYPLATILO

[n] P

PŘÍMOČARÁ REDUKCE

$u = x \sum \mod R$ $\quad l = b^t$

x ROZSAH $\quad b^{2t} \times b^t \quad (b^t \times b^t)$

up $\mod R \quad b^t \times b^t$

PROCEDURU LLE ZEFEKTIVNIT

NATRÁZENÍ $b^t \times b^t$ lineární vzdálenost

$b^t \times b$

NAVÍC STAČÍ ZNÁT POUZE $g^1, g^{p\Sigma^1} \equiv -1 \mod b$

(mělo by R)

$p\xi' \equiv -1 \mod b$

$x = \sum x_i \cdot b^i \quad 0 \le i \le 2t-1$

PŘEDSTAVME SI, ŽE $x_0 = \dots = x_{r-1} = 0$

$b^r \mid x$

$u < b$, $p < b^t$

POLOŽME $u = x_r \xi' \pmod b$

$x' = x + u p b^r$

$x \bmod b^{r+1}$ $\quad x' \equiv x_r b^r + p\xi' x_r b^r \equiv 0 \mod b^{r+1}$

($p\xi' \equiv -1 \mod b$)

$x' - x = p b^r u$, $u < b$

$b^r \mid x \rightarrow b^{r+1} \mid x'$

TOTO SPUSTÍME ITERATIVNĚ A POSTUPNĚ BUDEME NULOVAT POZICE 0, 1, ...

$x' - x$ je $p b^r \cdot$ kmalé

Po t krocích se x změní na $x + vp$, kde $0 \le v < b^k$

Po t krocích $R = b^t$ dělí $x + vp$

$b^k \mid x + vp$

```
i=0
while (i<t) do:
    u = x_i Σ' (mod b);
    X = X + pub^i;
    i = i+1;
y = X/R;
if (y>p) THEN y=y-p;
RETURN y;
```

b^{i+1} divisx

$R = b^t$

Z JAK SPOČÍTAT EFEKTIVNĚ

Σ

Σ' = ...

LZE ZKOMBINOVAT NÁSOBENÍ

$X = xR$ s $Y = yR$ a PRNT RED. DO 1 ALG.

$XY \to XY/R \bmod p$

? $p^{-1} \bmod 2^w$?

? $x^{-1} \bmod 2^w$? kde x liché

```
y = 1; i = 1;
while (i < w) do
    j = i + 1;
    u = x*y mod 2^j   (= 2^(i+1))
    if (2^j < u)  y = y + 2^i;
    i = j;
return y;
```

OZNAČME y_i hodnotou
na konci i-té iterace

$y_0 = 1$ VÝSTUPNÍ $y_{w-1} = y$

$y_i < 2^{i+1}$

OVĚŘIT TŘEBA $xy_i \equiv 1 \bmod 2^{i+1}$

IND. PŘEDP. $xy_{i-1} \equiv 1 \bmod 2^i$ $u = xy_{i-1} \bmod 2^{i+1}$

mod 2 možné hodnoty $1 \bmod 2^{i+1}$

$u \equiv 1 \bmod 2^i$ ① $u = 1 + 2^i \bmod 2^{i+1}$

① $y_i = y_{i-1}$ $xy_i \equiv 1 \bmod 2^i$

② $xy_i \equiv 1 + 2^i \times (y_{i-1} + 2^i) \equiv 1 + 2^i + 2^i \equiv 1 \bmod 2^{i+1}$

$y_{i-1} \to y_{i-1} + 2^i$

KOMENTÁŘ K NÁSOBENÍ, KTERÉ PROKLÁDANÉ REDUKCÍ (INTERLEAVING)

$X = \sum_{0 \le j < t} x_j \cdot b^j$ $\quad Y = \sum_{0 \le j < t} y_j \cdot b^j$

NA VSTUPU $\sum z_j \cdot b^j$

$(\sum z_j \cdot b^j) R \equiv (\sum x_j b^j)(\sum y_j \cdot b^j) \pmod p$

Počítáme v každém kroku $i = 1, 2, \ldots$

$(\sum z_j \cdot b^j) b^i \equiv (\sum_{j=1}^{i} x_j \cdot b^j)(\sum y_j \cdot b^j) \pmod p$

z_i $\quad x_i$ $\quad y$

x_i

ST. POSTUP PAK ZJISTÍ, ŽE

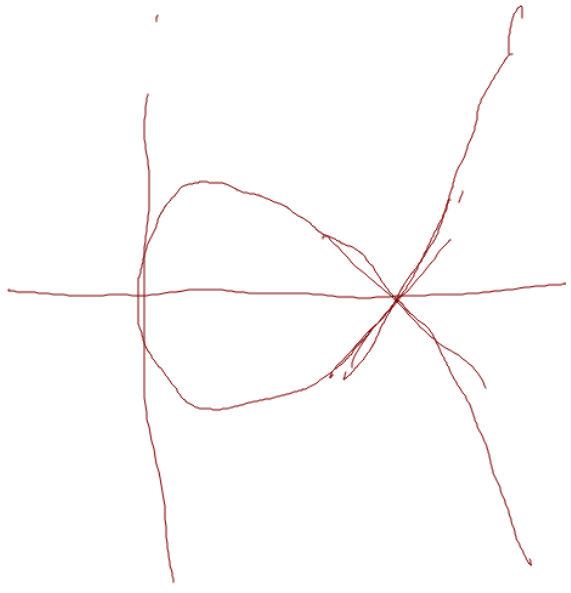
$\sum_i b^i - \overline{x_i y} = p v_i \quad 0 \le v_i < b^i$

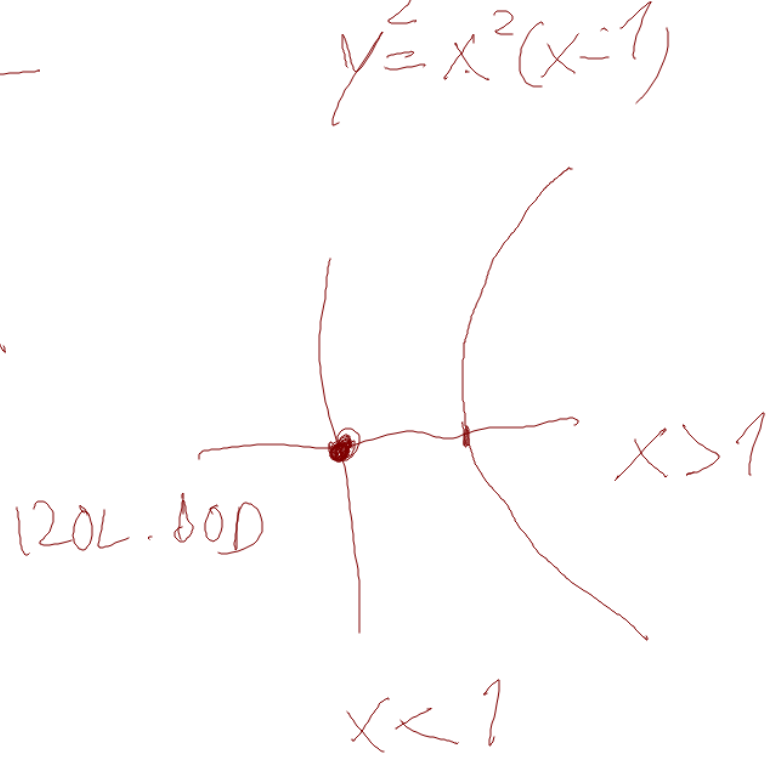
NA KONCI $2b^t - xy \le pb^t \quad b^t = l$

$2R \le xy + pR < 2pR$

DĚLENÍ PROBÍHÁ PROBÍRÁNÍ (V KAŽDÉM KROKU SE DĚLÍ HODNOTOU b)


$y^2=x^3$
HROT


$y^2=x(x-1)^2$


$y^2=x^2(x-1)$
$x>1$
120L.80D
$x<1$