Lec 14A Base conversion

March 4, 2021 1:42 PM

Chapter 6 Newton's iteration and the Hensel construction.

6.2 p-adic representations for $\mathbb{Z}$.

Theorem 1. Let $u \in \mathbb{Z}$, $p \in \mathbb{Z}$, $p > 1$. For $0 \le u < p^n$ there exist unique integers $u_0, u_1, \dots, u_{n-1}$ s.t. $u = u_0 + u_1 p + \cdots + u_{n-1} p^{n-1}$ where $0 \le u_i < p$

(unique: on the assignment.)

$u = u_0 + u_1 p + u_2 p^2 + \cdots$

$u_0 = u \bmod p$ where $0 \le u_0 < p$

$u \leftarrow (u - u_0)/p = u_1 + u_2 p + \cdots$

$u_1 = u \bmod p$

$u \leftarrow (u - u_1)/p = u_2 + u_3 p + \cdots$

$u_2 \leftarrow u \bmod p$.

etc

Example $u = 25$, $p = 3$, $25 < 3^3 \Rightarrow n = 3$.

$u = 25 = u_0 + u_1 \cdot 3 + u_2 \cdot 3^2 = 1 + 2\cdot 3 + 2\cdot 3^2$

$u_0 = 25 \bmod 3 = 1$

$u = (25-1)/3 = 8$

$u_1 = 8 \bmod 3 = 2$

$u = (8-2)/3 = 2$.

$u_2 = 2 \bmod 3 = 2$.

$u = (2-2)/3 = 0$.

Algorithm Base Conversion.

Input $p, u \in \mathbb{Z}$, $u \ge 0$, $p > 1$.

if $u = 0$ output 0.

$k \leftarrow 0$.

while $u \neq 0$ do

remainder $u_k \leftarrow u \bmod p$

quotient $u \leftarrow (u - u_k)/p$ } $u \div p$.

$k \leftarrow k+1$.

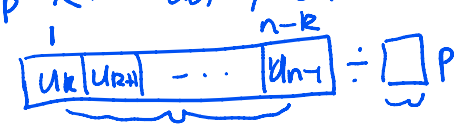
od

output $u_0, u_1, \dots, u_{k-1}$.

Cost

$u < p^n$ $u_0, u_1, \dots, u_{n-1}$

Step k. $u_0, \dots, u_{k-1}$



Case $p \le B$ a constant.

The cost of $u \div p \in O(n-k)$

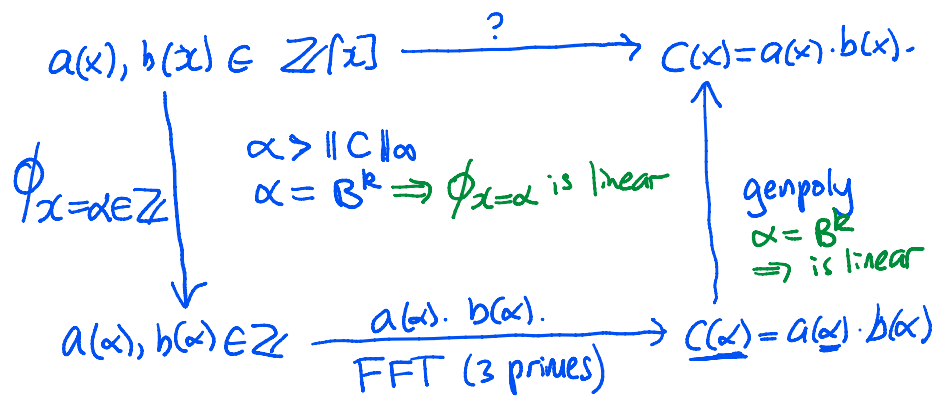
$$\text{Cost} = \sum_{k=0}^{n-1} O(n-k) \quad (>0) \quad = O\left(\sum_{k=0}^{n-1} n-k\right)$$

$$= O(n + n-1 + \cdots + 2 + 1)$$

$$= O\left(\frac{n(n+1)}{2} = \frac{n^2}{2} + \frac{n}{2}\right) = O(n^2).$$

Single point evaluation & interpolation.

Single point evaluation & interpolation.



Idea: reducing x in $\mathbb{Z}[x]$ to x in $\mathbb{Z}$ where an FFT based code is avaible.

$\|c\|_\infty = \|a\|_\infty \cdot \|b\|_\infty \cdot \min(\#\text{terms}, \#\text{terms})$.

$\|c\|_\infty = 3\cdot 3\cdot 3 = 27$

Example.

$a(x) = 3x^2 + 2x + 1$

$b(x) = 2x^2 + 2x + 3$

$c(x) = 6x^4 + 10x^3 + 15x^2 + 8x + 3$ ←

$B = 10$

$\alpha = 1000$

$a(1000) = 3002001$

$b(1000) = 2002003$

$c(1000) = 6|010|015|008|003$

Problem: -ve coefficients.

$(3x-3)(2x+1) = 6x^2 - 3x - 3$

$x = 1000$

$2997 \times 2001 = 5996997 = 6\cdot 1000^2 - 3\cdot 1000 - 3$.

$= 5\cdot 1000^2 + 996\cdot 1000 + 997$.

Theorem 2. Let $u, p \in \mathbb{Z}$, $p \geq 3$. If $-p^n/2 < u \leq \lfloor p^n/2 \rfloor$ there exist unique integers $u_0, u_1, \ldots, u_{n-1}$ s.t. $u = u_0 + u_1 p + \cdots + u_{n-1} p^{n-1}$ where $-p/2 < u_i \leq \lfloor p/2 \rfloor$

$p = 1000$.

$-499 \leq u_i \leq 500$.

Example $u = 5996997$, $p = 1000$ $\quad \frac{1000^2}{2} < u < \frac{1000^3}{2} \Rightarrow n = 3$.

$u = u_0 + u_1 \cdot p + u_2 p^2$

$u_0 = u \bmod p = -3$

$u \leftarrow (u - (-3))/1000 = 5997000/1000 = 5997$.

$u_1 = u \bmod p = -3$

$u = (5997 - (-3))/1000 = 6$

$u_2 = 6$

$u = (6-6)/1000 = 0$.

$u = -3 + -3\cdot 1000 + 6\cdot 1000^2$.