Integer multiplication in time $O(n \log n)$

David Harvey, **Joris van der Hoeven**

IHP, Paris

September 20, 2023

Motivation

$M(N)$: the complexity of multiplying two N-bit integers (Turing machine model)

Motivation

$M(N)$: the complexity of multiplying two N-bit integers (Turing machine model)

Why study the asymptotic behaviour of $M(N)$?

Motivation

$M(N)$: the complexity of multiplying two N-bit integers (Turing machine model)

Why study the asymptotic behaviour of $M(N)$?

Division. $O(M(N))$

Motivation

$M(N)$: the complexity of multiplying two N-bit integers (Turing machine model)

Why study the asymptotic behaviour of $M(N)$?

Division. $O(M(N))$

Gcd. $O(M(N)\log N)$

Motivation

$M(N)$: the complexity of multiplying two N-bit integers (Turing machine model)

Why study the asymptotic behaviour of $M(N)$?

Division. $O(M(N))$

Gcd. $O(M(N)\log N)$

Computing e, π. $O(M(N)\log N)$

Motivation

$M(N)$: the complexity of multiplying two N-bit integers (Turing machine model)

Why study the asymptotic behaviour of $M(N)$?

Division. $O(M(N))$

Gcd. $O(M(N)\log N)$

Computing e, π. $O(M(N)\log N)$

Base conversion. $O\left(M(N)\frac{\log N}{\log\log N}\right)$ (FFT-model)

Motivation

$\mathsf{M}(N)$: the complexity of multiplying two N-bit integers (Turing machine model)

Why study the asymptotic behaviour of $\mathsf{M}(N)$?

Division. $O(\mathsf{M}(N))$

Gcd. $O(\mathsf{M}(N)\log N)$

Computing e, π. $O(\mathsf{M}(N)\log N)$

Base conversion. $O\left(\mathsf{M}(N)\frac{\log N}{\log\log N}\right)$ (FFT-model)

FFT. $O(\mathsf{M}(np))$, length n, bit-precision $p \geqslant \log n$

Motivation

$M(N)$: the complexity of multiplying two N-bit integers (Turing machine model)

Why study the asymptotic behaviour of $M(N)$?

Division. $O(M(N))$

Gcd. $O(M(N)\log N)$

Computing e, π. $O(M(N)\log N)$

Base conversion. $O\left(M(N)\frac{\log N}{\log\log N}\right)$ (FFT-model)

FFT. $O(M(np))$, length n, bit-precision $p \geqslant \log n$

$M(N)$ = speed of basic arithmetic

Motivation

$\mathsf{M}(N)$: the complexity of multiplying two N-bit integers (Turing machine model)

Why study the asymptotic behaviour of $\mathsf{M}(N)$?

Division. $O(\mathsf{M}(N))$

Gcd. $O(\mathsf{M}(N)\log N)$

Computing e, π. $O(\mathsf{M}(N)\log N)$

Base conversion. $O\left(\mathsf{M}(N)\frac{\log N}{\log\log N}\right)$ (FFT-model)

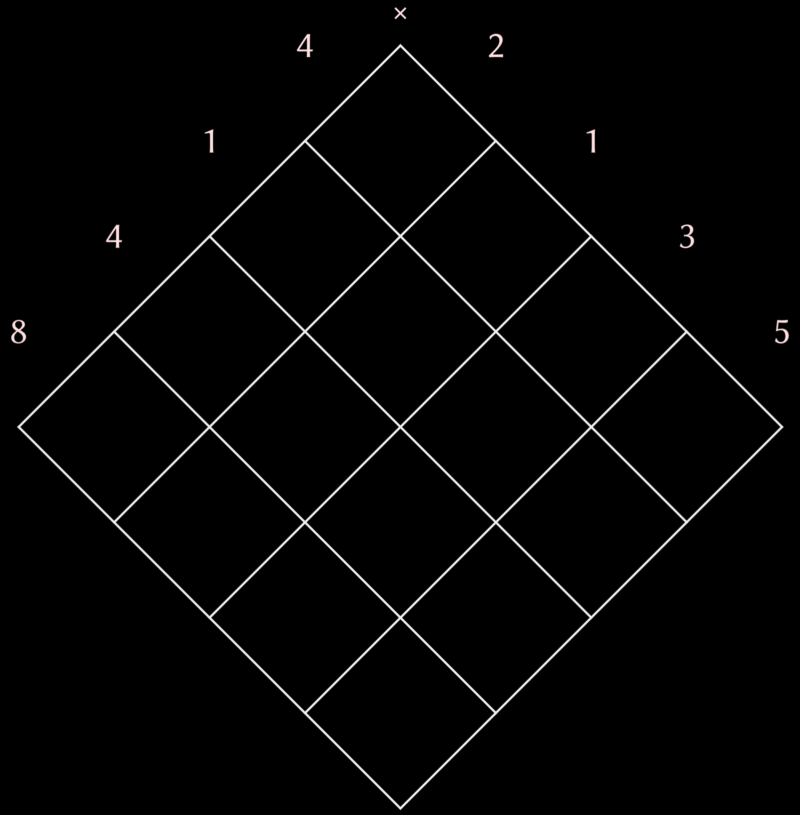
FFT. $O(\mathsf{M}(np))$, length n, bit-precision $p \geqslant \log n$

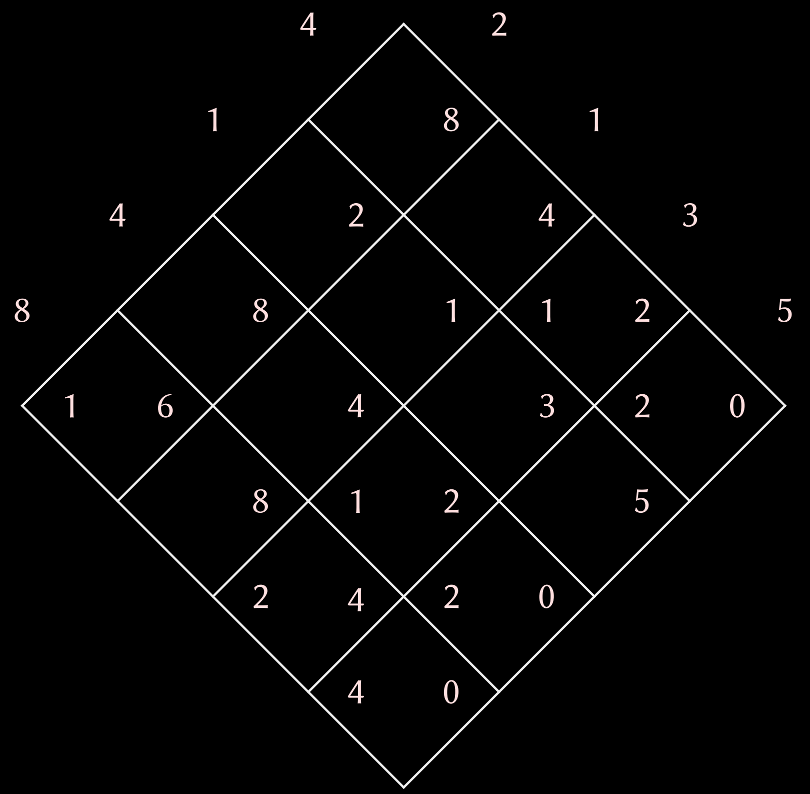
$\mathsf{M}(N)$ = speed of basic arithmetic

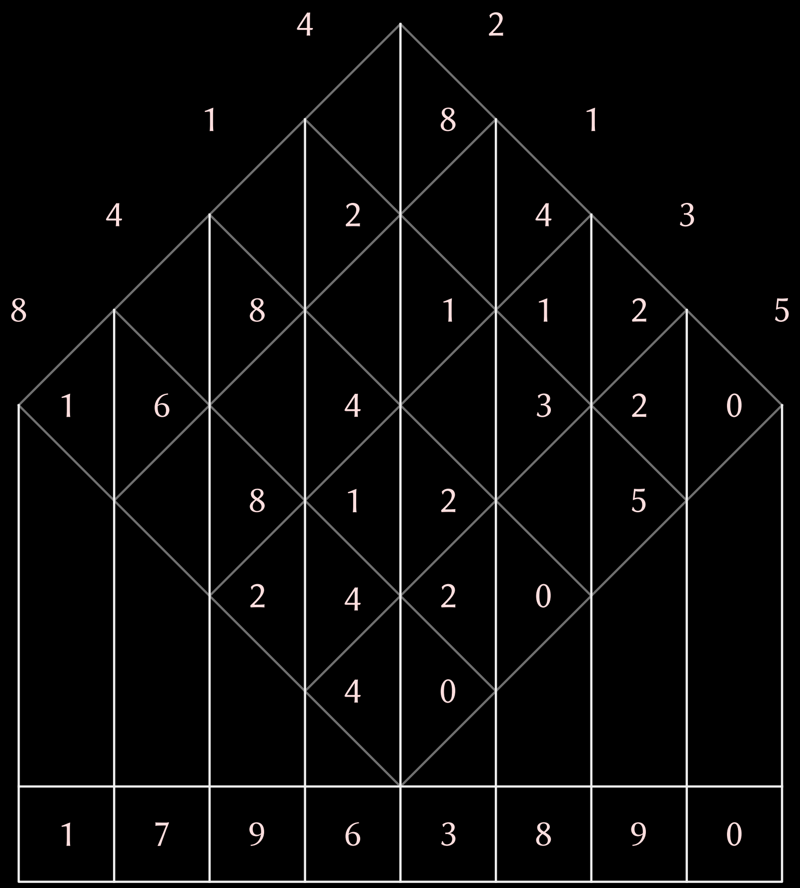
Also

- Better theoretical techniques $\xrightarrow{\text{often}}$ faster practical implementations
- Asymptotic complexity abstracts from concrete machines
- Mechanizing multiplication is a historically fascinating problem

8 4 1 4 × 2 1 3 5

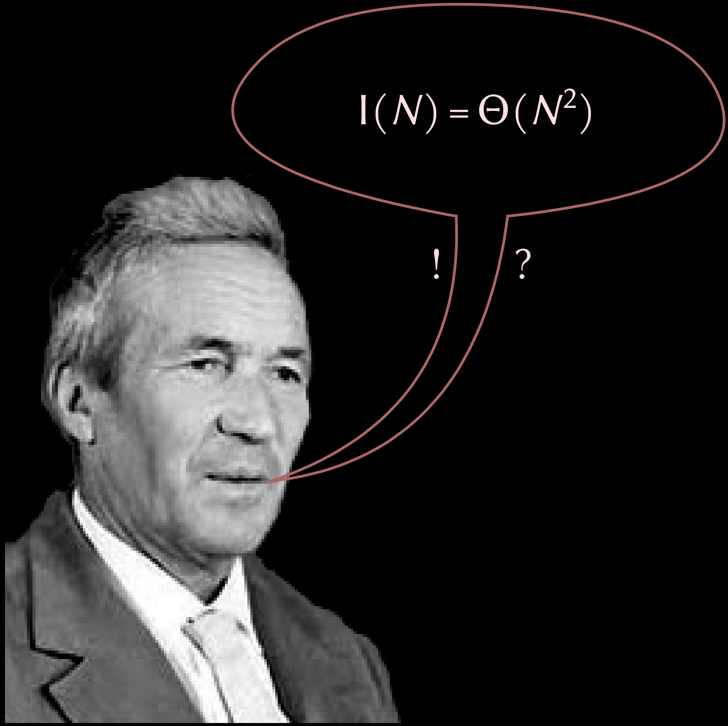

×
4
2
1
1
4
3
8
5


4 2
1 8 1
4 2 4 3
8 8 1 1 2 5
1 6 4 3 2 0
8 1 2 5
2 4 2 0
4 0


4 2
1 8 1
4 2 4 3
8 8 1 1 2 5
1 6 4 3 2 0
8 1 2 5
2 4 2 0
4 0
1 7 9 6 3 8 9 0

Can we do better?

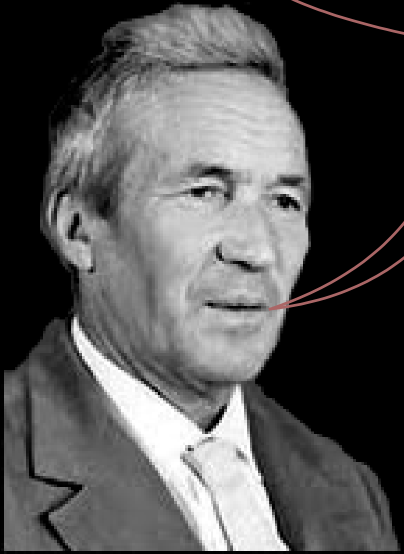
Can we do better?



Can we do better?

$$I(N) = \Theta(N^2)$$

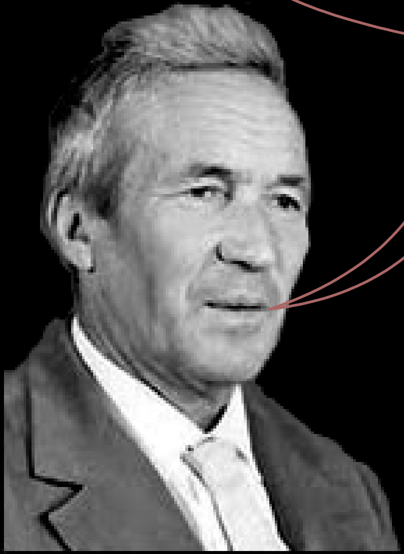
! ?



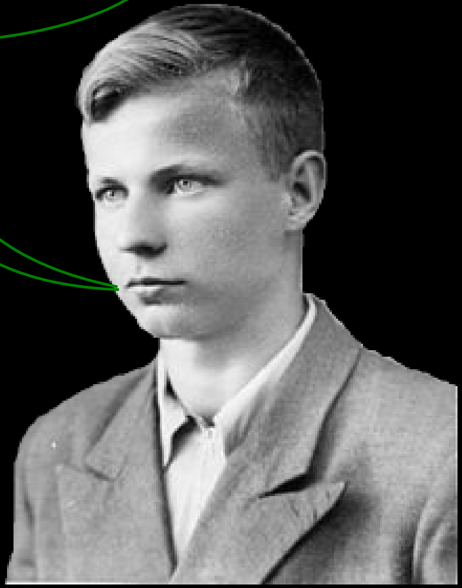
Can we do better?

$$\mathrm{I}(N) = \Theta(N^2)$$

! ?



$$\mathrm{I}(N) = O(N^{\log_2 3})$$



1962

Short history

1962	Karatsuba	$O(N^{\log 3/\log 2})$
1963	Toom	$O\left(N\,2^{5\sqrt{\log N/\log 2}}\right)$
1966	Schönhage	$O\left(N\,2^{\sqrt{2\log N/\log 2}}\,(\log N)^{3/2}\right)$
1969	Knuth	$O\left(N\,2^{\sqrt{2\log N/\log 2}}\log N\right)$
1971	Pollard	$O(N\log N\log\log N\log\log\log N\cdots)$
1971	Schönhage-Strassen	$O(N\log N\log\log N)$
2007	Fürer	$O(N\log N\,2^{O(\log^* N)})$
2014	Harvey-vdH-Lecerf	$O(N\log N\,8^{\log^* N})$
2017	Harvey	$O(N\log N\,6^{\log^* N})$
2017	Harvey-vdH	$O(N\log N\,(4\sqrt{2})^{\log^* N})$
2018	Harvey-vdH	$O(N\log N\,4^{\log^* N})$
2019	**Harvey-vdH**	$O(N\log N)$

Karatsuba multiplication

$$13022020 \quad \times \quad 31415926$$

Karatsuba multiplication

$$1302 \quad 2020 \quad \times \quad 3141 \quad 5926$$

Karatsuba multiplication

$$\underbrace{1302}_{a}\ \underbrace{2020}_{b} \times \underbrace{3141}_{c}\ \underbrace{5926}_{d}$$

Karatsuba multiplication

$$\underbrace{1302}_{a}\ \underbrace{2020}_{b} \times \underbrace{3141}_{c}\ \underbrace{5926}_{d}$$

$$(ax+b)\cdot(cx+d) \;=$$

Karatsuba multiplication

$$\underbrace{1302}_{a}\ \underbrace{2020}_{b} \times \underbrace{3141}_{c}\ \underbrace{5926}_{d}$$

$$(ax+b)\cdot(cx+d) = a\cdot c\,x^2 + (a\cdot d + b\cdot c)\,x + b\cdot d$$

Karatsuba multiplication

$$\underbrace{1302}_{a}\ \underbrace{2020}_{b} \times \underbrace{3141}_{c}\ \underbrace{5926}_{d}$$

$$(ax+b)\cdot(cx+d) = a\cdot c\,x^2 + (a\cdot d + b\cdot c)\,x + b\cdot d$$

$$a\cdot d + b\cdot c = (a+b)\cdot(c+d) - a\cdot c - b\cdot d$$

Karatsuba multiplication

$$\underbrace{1302}_{a}\ \underbrace{2020}_{b} \times \underbrace{3141}_{c}\ \underbrace{5926}_{d}$$

$$(ax+b)\cdot(cx+d) = a\cdot c\,x^2 + (a\cdot d + b\cdot c)\,x + b\cdot d$$

$$a\cdot d + b\cdot c = (a+b)\cdot(c+d) - a\cdot c - b\cdot d$$

Complexity

$$M(n) \leqslant 3M(n/2) + Cn$$

Karatsuba multiplication

$$\underbrace{1302}_{a}\ \underbrace{2020}_{b} \times \underbrace{3141}_{c}\ \underbrace{5926}_{d}$$

$$(ax+b)\cdot(cx+d) = a\cdot c\,x^2 + (a\cdot d + b\cdot c)\,x + b\cdot d$$

$$a\cdot d + b\cdot c = (a+b)\cdot(c+d) - a\cdot c - b\cdot d$$

Complexity

$$\begin{aligned} M(n) &\leqslant 3M(n/2) + Cn \\ &\leqslant 9M(n/4) + \tfrac{5}{2}Cn \end{aligned}$$

Karatsuba multiplication

$$\underbrace{1302}_{a}\ \underbrace{2020}_{b} \times \underbrace{3141}_{c}\ \underbrace{5926}_{d}$$

$$(ax+b)\cdot(cx+d) = a\cdot c\,x^2 + (a\cdot d + b\cdot c)\,x + b\cdot d$$

$$a\cdot d + b\cdot c = (a+b)\cdot(c+d) - a\cdot c - b\cdot d$$

Complexity

$$\begin{aligned} M(n) &\leqslant 3\,M(n/2) + C\,n \\ &\leqslant 9\,M(n/4) + \tfrac{5}{2}\,C\,n \\ &\leqslant 27\,M(n/8) + \tfrac{19}{4}\,C\,n \end{aligned}$$

Karatsuba multiplication

$$\underbrace{1302}_{a}\ \underbrace{2020}_{b} \times \underbrace{3141}_{c}\ \underbrace{5926}_{d}$$

$$(ax+b)\cdot(cx+d) = a\cdot c\,x^2 + (a\cdot d + b\cdot c)\,x + b\cdot d$$

$$a\cdot d + b\cdot c = (a+b)\cdot(c+d) - a\cdot c - b\cdot d$$

Complexity

$$\begin{aligned}
M(n) &\leqslant 3\,M(n/2) + C\,n \\
&\leqslant 9\,M(n/4) + \tfrac{5}{2}\,C\,n \\
&\leqslant 27\,M(n/8) + \tfrac{19}{4}\,C\,n \\
&\leqslant \cdots \\
&\leqslant O\left(n^{\frac{\log 3}{\log 2}}\right)
\end{aligned}$$

Kronecker segmentation

$$4627579679788114 \quad \times \quad 4519170871966234$$

$$\rightsquigarrow$$

$$(4627\,x^3 + 5796\,x^2 + 7978\,x + 8114) \quad \times \quad (4519\,x^3 + 1708\,x^2 + 7196\,x + 6234)$$

Integers versus polynomials

Kronecker segmentation

$$4627579679788114 \times 4519170871966234$$
$$\downarrow$$
$$(4627x^3 + 5796x^2 + 7978x + 8114) \times (4519x^3 + 1708x^2 + 7196x + 6234)$$

Kronecker substitution

$$(4627x^3 + 5796x^2 + 7978x + 8114) \times (4519x^3 + 1708x^2 + 7196x + 6234)$$
$$\downarrow$$
$$4627000005796000007978000008114 \times 4519000001708000007196000006234$$

Kronecker segmentation

$$4627579679788114 \times 4519170871966234$$

$$\downarrow$$

$$(4627x^3 + 5796x^2 + 7978x + 8114) \times (4519x^3 + 1708x^2 + 7196x + 6234)$$

Kronecker substitution

$$(4627x^3 + 5796x^2 + 7978x + 8114) \times (4519x^3 + 1708x^2 + 7196x + 6234)$$

$$\downarrow$$

$$4627000005796000007978000008114 \times 4519000001708000007196000006234$$

$$1004003 \times 2001005 = 2009015023015$$

Cyclic polynomials

$\mathbb{K}$: a field (or a suitable ring)

n : cycle length

$\mathbb{K}[x]/(x^n - 1)$: ring of cyclic polynomials of length n

Cyclic polynomials

$\mathbb{K}$: a field (or a suitable ring)

n : cycle length

$\mathbb{K}[x]/(x^n - 1)$: ring of cyclic polynomials of length n

$$P \in \mathbb{K}[x], \quad \deg P < n \quad \stackrel{\text{bijection}}{\longleftrightarrow} \quad \bar{P} \in \mathbb{K}[x]/(x^n - 1)$$

Cyclic polynomials

$\mathbb{K}$: a field (or a suitable ring)

n : cycle length

$\mathbb{K}[x]/(x^n - 1)$: ring of cyclic polynomials of length n

$$P \in \mathbb{K}[x], \quad \deg P < n \quad \stackrel{\text{bijection}}{\longleftrightarrow} \quad \bar{P} \in \mathbb{K}[x]/(x^n - 1)$$

$$P, Q \in \mathbb{K}[x], \quad \deg(PQ) < n, \qquad \text{Compute } PQ \iff \text{Compute } \bar{P}\bar{Q}$$

Cyclic polynomials

$\mathbb{K}$: a field (or a suitable ring)
n : cycle length
$\mathbb{K}[x]/(x^n - 1)$: ring of cyclic polynomials of length n

$$P \in \mathbb{K}[x], \quad \deg P < n \quad \overset{\text{bijection}}{\longleftrightarrow} \quad \bar{P} \in \mathbb{K}[x]/(x^n - 1)$$

$$P, Q \in \mathbb{K}[x], \quad \deg(PQ) < n, \qquad \text{Compute } PQ \iff \text{Compute } \bar{P}\bar{Q}$$

Summary so far

$$\mathbb{Z} \xrightarrow{\text{Kronecker}} \mathbb{K}[x] \xrightarrow{\text{Encode}} \mathbb{K}[x]/(x^n - 1)$$

The Discrete Fourier Transform

$\mathbb{K}$: a field (or a suitable ring)

n : cycle or transform length

ω : primitive n-th root of unity in $\mathbb{K}$, say $\omega = e^{\frac{2\pi i}{n}}$

The Discrete Fourier Transform

$\mathbb{K}$: a field (or a suitable ring)

n : cycle or transform length

ω : primitive n-th root of unity in $\mathbb{K}$, say $\omega = \mathrm{e}^{\frac{2\pi i}{n}}$

Chinese remainder theorem

$$(x^n - 1) = \prod_{0 \leqslant k < n} (x - \omega^k)$$

$\mathbb{K}$: a field (or a suitable ring)

n : cycle or transform length

ω : primitive n-th root of unity in $\mathbb{K}$, say $\omega = \mathrm{e}^{\frac{2\pi \mathrm{i}}{n}}$

Chinese remainder theorem

$$(x^n - 1) = \prod_{0 \leqslant k < n} (x - \omega^k)$$

$$\mathbb{K}[x]/(x^n - 1) \cong \bigoplus_{0 \leqslant k < n} \mathbb{K}[x]/(x - \omega^k)$$

$\mathbb{K}$: a field (or a suitable ring)

n : cycle or transform length

ω : primitive n-th root of unity in $\mathbb{K}$, say $\omega = \mathrm{e}^{\frac{2\pi\mathrm{i}}{n}}$

Chinese remainder theorem

$$(x^n - 1) = \prod_{0 \leqslant k < n} (x - \omega^k)$$

$$\mathbb{K}[x]/(x^n - 1) \cong \bigoplus_{0 \leqslant k < n} \mathbb{K}[x]/(x - \omega^k) \cong \mathbb{K}^n$$

The Discrete Fourier Transform

$\mathbb{K}$: a field (or a suitable ring)

n : cycle or transform length

ω : primitive n-th root of unity in $\mathbb{K}$, say $\omega = \mathrm{e}^{\frac{2\pi \mathrm{i}}{n}}$

Chinese remainder theorem

$$(x^n - 1) = \prod_{0 \leqslant k < n} (x - \omega^k)$$

$$\mathbb{K}[x]/(x^n - 1) \cong \bigoplus_{0 \leqslant k < n} \mathbb{K}[x]/(x - \omega^k) \cong \mathbb{K}^n$$

Discrete Fourier transform

$$\mathbb{K}[x]/(x^n - 1) \underset{\mathrm{DFT}_\omega^{-1}}{\overset{\mathrm{DFT}_\omega}{\rightleftarrows}} \bigoplus_{0 \leqslant k < n} \mathbb{K}[x]/(x - \omega^k)$$

The Discrete Fourier Transform

$\mathbb{K}$: a field (or a suitable ring)

n : cycle or transform length

ω : primitive n-th root of unity in $\mathbb{K}$, say $\omega = e^{\frac{2\pi i}{n}}$

Chinese remainder theorem

$$(x^n - 1) = \prod_{0 \leqslant k < n} (x - \omega^k)$$

$$\mathbb{K}[x]/(x^n - 1) \cong \bigoplus_{0 \leqslant k < n} \mathbb{K}[x]/(x - \omega^k) \cong \mathbb{K}^n$$

Discrete Fourier transform

$$\mathbb{K}[x]/(x^n - 1) \underset{\mathrm{DFT}_\omega^{-1}}{\overset{\mathrm{DFT}_\omega}{\rightleftarrows}} \bigoplus_{0 \leqslant k < n} \mathbb{K}[x]/(x - \omega^k)$$

$$\mathrm{DFT}_\omega^{-1} \quad \rightsquigarrow \quad \frac{1}{n} \mathrm{DFT}_{\omega^{-1}}$$

FFT multiplication

$$P \in \mathbb{K}[x]/(x^n - 1) \qquad\qquad Q \in \mathbb{K}[x]/(x^n - 1)$$

$$\downarrow \text{DFT} \qquad\qquad \downarrow \text{DFT}$$

$$\hat{P} \in \bigoplus_{0 \leqslant k < n} \mathbb{K}[x]/(x - \omega^k) \qquad\qquad \hat{Q} \in \bigoplus_{0 \leqslant k < n} \mathbb{K}[x]/(x - \omega^k)$$

$$\searrow \qquad\qquad \swarrow$$

$$\hat{P}\hat{Q} \in \bigoplus_{0 \leqslant k < n} \mathbb{K}[x]/(x - \omega^k)$$

$$\downarrow \text{DFT}^{-1}$$

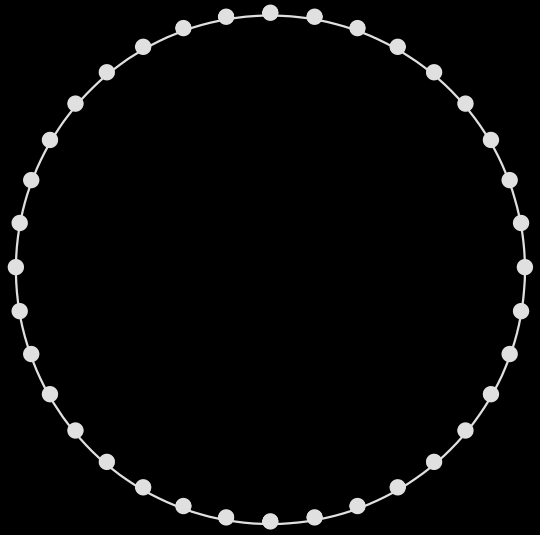
$$PQ \in \mathbb{K}[x]/(x^n - 1)$$

$$
\begin{array}{ccccc}
P \in \mathbb{K}[x]/(x^n-1) & & & & Q \in \mathbb{K}[x]/(x^n-1) \\
\downarrow \color{cyan}{\text{DFT}} & & & & \downarrow \color{cyan}{\text{DFT}} \\
\hat{P} \in \bigoplus_{0 \leqslant k < n} \mathbb{K}[x]/(x-\omega^k) & & & & \hat{Q} \in \bigoplus_{0 \leqslant k < n} \mathbb{K}[x]/(x-\omega^k) \\
& \searrow & & \swarrow & \\
& & \hat{P}\hat{Q} \in \bigoplus_{0 \leqslant k < n} \mathbb{K}[x]/(x-\omega^k) & & \\
& & \downarrow \color{cyan}{\text{DFT}^{-1}} & & \\
& & PQ \in \mathbb{K}[x]/(x^n-1) & &
\end{array}
$$

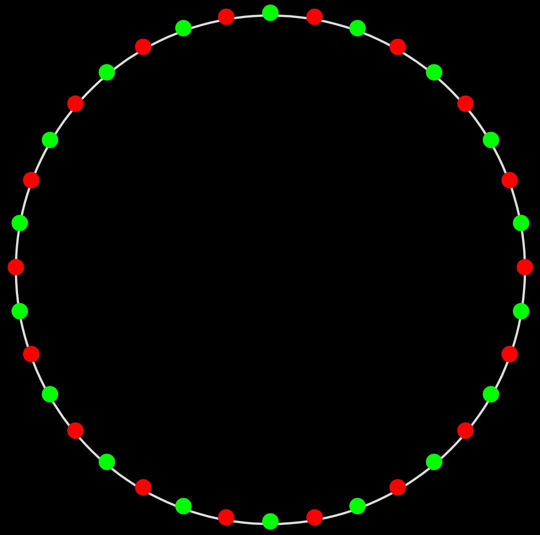
Summary so far

$$
\mathbb{Z} \xrightarrow{\text{Kronecker}} \mathbb{K}[x] \xrightarrow{\text{Embed}} \mathbb{K}[x]/(x^n-1) \xrightarrow{\text{DFT}} \mathbb{K}^n
$$

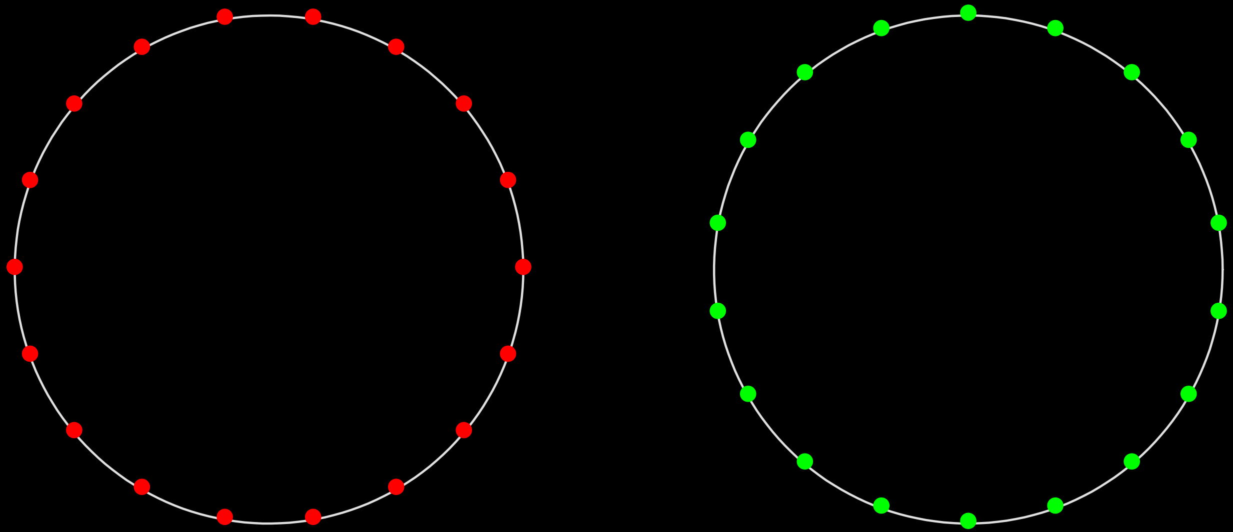
Making the FFT fast



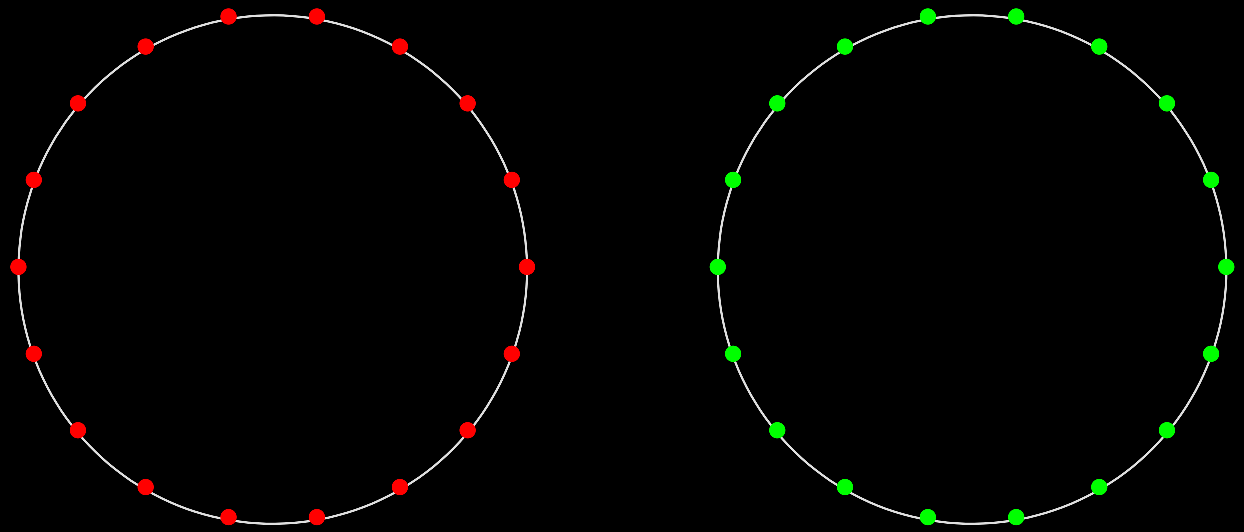
Making the FFT fast



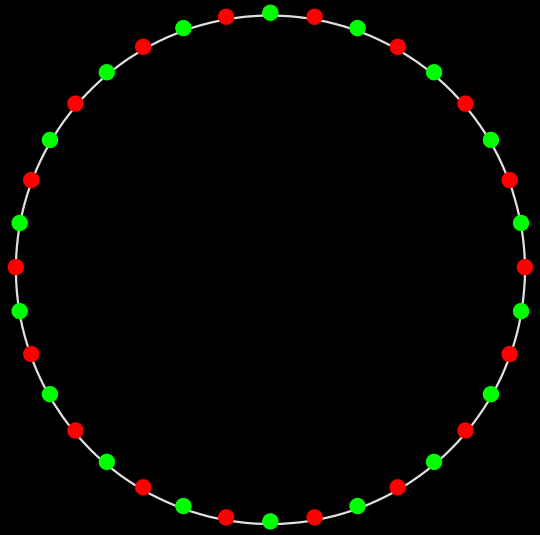
Making the FFT fast



Making the FFT fast

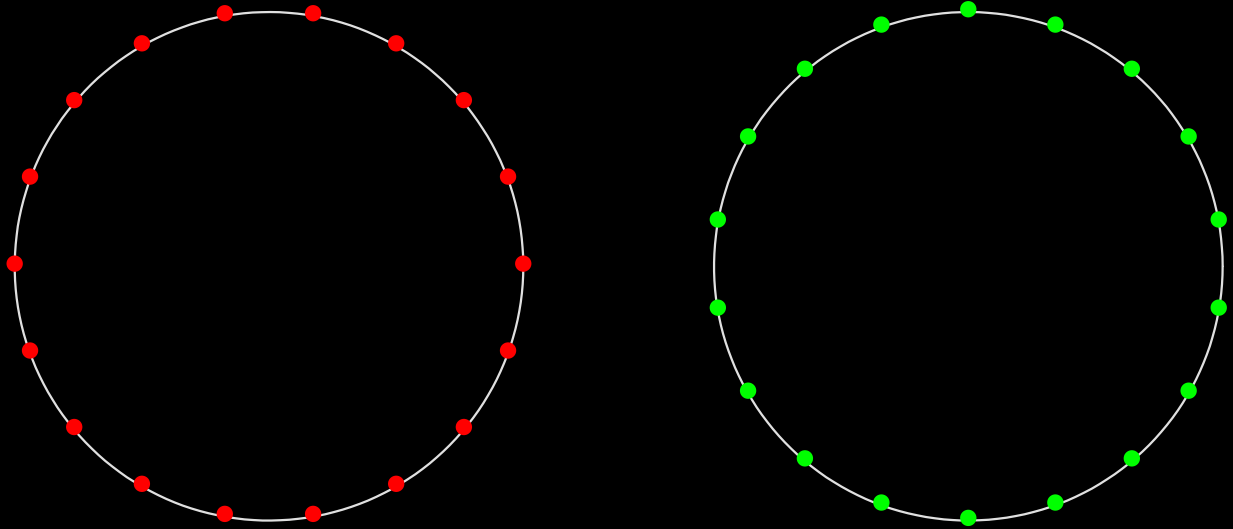


Making the FFT fast



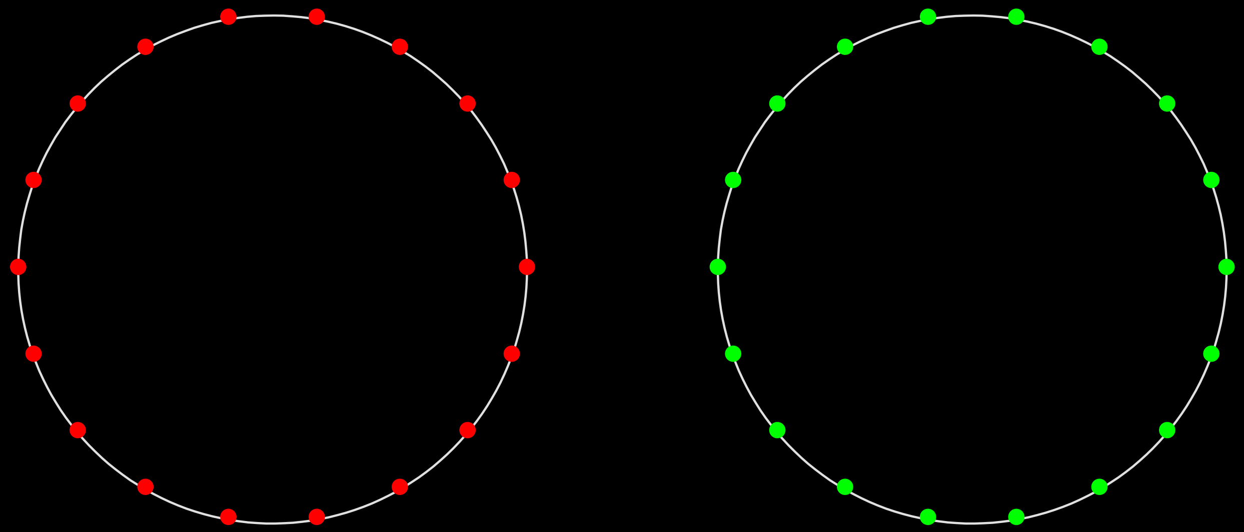
$$\mathbb{K}[x]/(x^{2n}-1)$$

Making the FFT fast



$$\mathbb{K}[x]/(x^{2n}-1) \cong \mathbb{K}[x]/(x^n-1) \oplus \mathbb{K}[x]/(x^n+1)$$

Making the FFT fast



$$\mathbb{K}[x]/(x^{2n}-1) \cong \mathbb{K}[x]/(x^n-1) \oplus \mathbb{K}[x]/(x^n+1)$$

$$\cong \mathbb{K}[x]/(x^n-1) \oplus \mathbb{K}[x]/(\tilde{x}^n-1)$$

$$\tilde{x} = \omega x$$

$$\omega^n = -1$$

Complexity analysis

$$\mathrm{F}_{\mathbb{K}}(2n) \leqslant 2\,\mathrm{F}_{\mathbb{K}}(n) + n\,\mathrm{add}_{\mathbb{K}} + n\,\mathrm{sub}_{\mathbb{K}} + n\,\mathrm{mul}_{\omega^{\mathbb{N}}}$$

Complexity analysis

$$\mathrm{F}_{\mathbb{K}}(2n) \leqslant 2\,\mathrm{F}_{\mathbb{K}}(n) + \underbrace{n\,\mathrm{add}_{\mathbb{K}} + n\,\mathrm{sub}_{\mathbb{K}}} + n\,\mathrm{mul}_{\omega^{\mathbb{N}}}$$

$$\mathbb{K}[x]/(x^{2n}-1)$$

$$\cong$$

$$\mathbb{K}[x]/(x^{n}-1) \oplus \mathbb{K}[x]/(x^{n}+1)$$

Complexity analysis

$$\mathrm{F}_{\mathbb{K}}(2n) \leqslant 2\,\mathrm{F}_{\mathbb{K}}(n) + \underbrace{n\,\mathrm{add}_{\mathbb{K}} + n\,\mathrm{sub}_{\mathbb{K}}} + \underbrace{n\,\mathrm{mul}_{\omega^{\mathbb{N}}}}$$

$$\mathbb{K}[x]/(x^{2n}-1) \cong \mathbb{K}[x]/(x^n-1) \oplus \mathbb{K}[x]/(x^n+1)$$

$$\mathbb{K}[x]/(x^n+1) \cong \mathbb{K}[x]/(\tilde{x}^n-1)$$

Complexity analysis

$$\mathrm{F}_{\mathbb{K}}(2n) \leqslant 2\,\mathrm{F}_{\mathbb{K}}(n) + \underbrace{n\,\mathrm{add}_{\mathbb{K}} + n\,\mathrm{sub}_{\mathbb{K}}} + \underbrace{n\,\mathrm{mul}_{\omega^{\mathbb{N}}}}$$

$$\mathbb{K}[x]/(x^{2n}-1) \cong \mathbb{K}[x]/(x^n-1) \oplus \mathbb{K}[x]/(x^n+1)$$

$$\mathbb{K}[x]/(x^n+1) \cong \mathbb{K}[x]/(\tilde{x}^n-1)$$

$$n = 2^{\lg n} \Longrightarrow \mathrm{F}_{\mathbb{K}}(n) \leqslant n \lg n \left(\mathrm{add}_{\mathbb{K}} + \tfrac{1}{2}\mathrm{mul}_{\omega^{\mathbb{N}}}\right)$$

Back to N-bit integer multiplication

How to choose $\mathbb{K}$?

Back to N-bit integer multiplication

How to choose $\mathbb{K}$?

I. $\mathbb{K} = \mathbb{C}_b$ with $b \asymp \log N$, $n \asymp \frac{N}{\log N}$, $\omega = e^{\frac{2\pi i}{n}}$

Back to N-bit integer multiplication

How to choose $\mathbb{K}$?

I. $\mathbb{K} = \mathbb{C}_b$ with $b \asymp \log N$, $n \asymp \frac{N}{\log N}$, $\omega = \mathrm{e}^{\frac{2\pi \mathrm{i}}{n}}$

II. $\mathbb{K} = \mathbb{F}_p$ with $p = s\,2^l + 1$, $\lg p \asymp \log N$, $n = 2^l \asymp \frac{N}{\log N}$, ω exists…

Back to N-bit integer multiplication

How to choose $\mathbb{K}$?

I. $\mathbb{K} = \mathbb{C}_b$ with $b \asymp \log N$, $n \asymp \frac{N}{\log N}$, $\omega = \mathrm{e}^{\frac{2\pi \mathrm{i}}{n}}$

II. $\mathbb{K} = \mathbb{F}_p$ with $p = s\,2^l + 1$, $\lg p \asymp \log N$, $n = 2^l \asymp \frac{N}{\log N}$, ω exists…

III. $\mathbb{K} = \mathbb{Z}/(2^m + 1)\,\mathbb{Z}$ with $m = 2^l \asymp \sqrt{N}$, $n \asymp \sqrt{N}$, $\omega = 2$

Back to N-bit integer multiplication

How to choose $\mathbb{K}$?

I. $\mathbb{K} = \mathbb{C}_b$ with $b \asymp \log N$, $n \asymp \frac{N}{\log N}$, $\omega = \mathrm{e}^{\frac{2\pi \mathrm{i}}{n}}$

II. $\mathbb{K} = \mathbb{F}_p$ with $p = s\,2^l + 1$, $\lg p \asymp \log N$, $n = 2^l \asymp \frac{N}{\log N}$, ω exists…

III. $\mathbb{K} = \mathbb{Z}/(2^m + 1)\,\mathbb{Z}$ with $m = 2^l \asymp \sqrt{N}$, $n \asymp \sqrt{N}$, $\omega = 2$

Complexity analysis

Back to N-bit integer multiplication

How to choose $\mathbb{K}$?

I. $\mathbb{K} = \mathbb{C}_b$ with $b \asymp \log N$, $n \asymp \frac{N}{\log N}$, $\omega = e^{\frac{2\pi i}{n}}$

II. $\mathbb{K} = \mathbb{F}_p$ with $p = s\,2^l + 1$, $\lg p \asymp \log N$, $n = 2^l \asymp \frac{N}{\log N}$, ω exists…

III. $\mathbb{K} = \mathbb{Z}/(2^m + 1)\,\mathbb{Z}$ with $m = 2^l \asymp \sqrt{N}$, $n \asymp \sqrt{N}$, $\omega = 2$

Complexity analysis

I. $M(N) = O(N\,M(\log N))$

$M(N) = O(N \log N \log\log N \cdots)$

Back to N-bit integer multiplication

How to choose $\mathbb{K}$?

I. $\mathbb{K} = \mathbb{C}_b$ with $b \asymp \log N$, $n \asymp \frac{N}{\log N}$, $\omega = \mathrm{e}^{\frac{2\pi \mathrm{i}}{n}}$

II. $\mathbb{K} = \mathbb{F}_p$ with $p = s\,2^l + 1$, $\lg p \asymp \log N$, $n = 2^l \asymp \frac{N}{\log N}$, ω exists…

III. $\mathbb{K} = \mathbb{Z}/(2^m + 1)\,\mathbb{Z}$ with $m = 2^l \asymp \sqrt{N}$, $n \asymp \sqrt{N}$, $\omega = 2$

Complexity analysis

I. $M(N) = O(N\,M(\log N))$ $\qquad M(N) = O(N \log N \log\log N \cdots)$

II. $M(N) = O(N\,M(\log N))$ $\qquad M(N) = O(N \log N \log\log N \cdots)$

Back to N-bit integer multiplication

How to choose $\mathbb{K}$?

I. $\mathbb{K} = \mathbb{C}_b$ with $b \asymp \log N$, $n \asymp \frac{N}{\log N}$, $\omega = \mathrm{e}^{\frac{2\pi \mathrm{i}}{n}}$

II. $\mathbb{K} = \mathbb{F}_p$ with $p = s\,2^l + 1$, $\lg p \asymp \log N$, $n = 2^l \asymp \frac{N}{\log N}$, ω exists…

III. $\mathbb{K} = \mathbb{Z}/(2^m + 1)\,\mathbb{Z}$ with $m = 2^l \asymp \sqrt{N}$, $n \asymp \sqrt{N}$, $\omega = 2$

Complexity analysis

I. $M(N) = O(N\,M(\log N))$ $\qquad M(N) = O(N \log N \log\log N \cdots)$

II. $M(N) = O(N\,M(\log N))$ $\qquad M(N) = O(N \log N \log\log N \cdots)$

III. $M^{\ominus}(N) \leqslant 2\sqrt{N}\,M^{\ominus}(\sqrt{N}) + O(N \log N)$ $\qquad M(N) = O(N \log N \log\log N)$

$M^{\ominus}(N)$: cost of multiplication in $\mathbb{Z}/(2^N + 1)\,\mathbb{Z}$

Note about Schönhage–Strassen multiplication

A careful construction yields

$$\mathsf{M}^{\ominus}(n) \leqslant C\, n \log n + 2\, n^{1/2}\, \mathsf{M}^{\ominus}(n^{1/2})$$

Note about Schönhage–Strassen multiplication

A careful construction yields

$$\begin{aligned} \mathrm{M}^{\ominus}(n) &\leqslant C\,n \log n + 2\,n^{1/2}\,\mathrm{M}^{\ominus}(n^{1/2}) \\ &\leqslant C\,n \log n + C\,n \log n + 4\,n^{3/4}\,\mathrm{M}^{\ominus}(n^{1/4}) \end{aligned}$$

Note about Schönhage–Strassen multiplication

A careful construction yields

$$
\begin{aligned}
\mathsf{M}^{\ominus}(n) &\leqslant C\,n\log n + 2\,n^{1/2}\,\mathsf{M}^{\ominus}(n^{1/2})\\
&\leqslant C\,n\log n + C\,n\log n + 4\,n^{3/4}\,\mathsf{M}^{\ominus}(n^{1/4})\\
&\leqslant C\,n\log n + C\,n\log n + C\,n\log n + 8\,n^{7/8}\,\mathsf{M}^{\ominus}(n^{1/8})
\end{aligned}
$$

Note about Schönhage–Strassen multiplication

A careful construction yields

$$\begin{aligned}
\mathsf{M}^{\ominus}(n) &\leqslant Cn\log n + 2n^{1/2}\,\mathsf{M}^{\ominus}(n^{1/2})\\
&\leqslant Cn\log n + Cn\log n + 4n^{3/4}\,\mathsf{M}^{\ominus}(n^{1/4})\\
&\leqslant Cn\log n + Cn\log n + Cn\log n + 8n^{7/8}\,\mathsf{M}^{\ominus}(n^{1/8})\\
&\ \ \vdots\\
&\leqslant Cn\log n + \overset{\log\log n\,\times}{\cdots} + Cn\log n + O(n\log n)
\end{aligned}$$

Note about Schönhage–Strassen multiplication

What if…

$$M^{\ominus}(n) \leqslant C\,n \log n + 1.98\, n^{1/2}\, M^{\ominus}(n^{1/2})$$

Note about Schönhage–Strassen multiplication

What if…

$$\begin{aligned} \mathrm{M}^{\ominus}(n) &\leqslant C\, n \log n + 1.98\, n^{1/2}\, \mathrm{M}^{\ominus}(n^{1/2}) \\ &\leqslant C\, n \log n + 0.99\, C\, n \log n + 1.98^2\, n^{3/4}\, \mathrm{M}^{\ominus}(n^{1/4}) \end{aligned}$$

Note about Schönhage–Strassen multiplication

What if…

$$\begin{aligned} M^{\ominus}(n) &\leqslant C n \log n + 1.98\, n^{1/2} M^{\ominus}(n^{1/2}) \\ &\leqslant C n \log n + 0.99 C n \log n + 1.98^2\, n^{3/4} M^{\ominus}(n^{1/4}) \\ &\leqslant C n \log n + 0.99\, C n \log n + 0.99^2\, C n \log n + 1.98^3\, n^{7/8} M^{\ominus}(n^{1/8}) \end{aligned}$$

Note about Schönhage–Strassen multiplication

What if…

$$
\begin{aligned}
\mathrm{M}^{\ominus}(n) &\leqslant C\,n\log n + 1.98\,n^{1/2}\,\mathrm{M}^{\ominus}(n^{1/2})\\
&\leqslant C\,n\log n + 0.99\,C\,n\log n + 1.98^2\,n^{3/4}\,\mathrm{M}^{\ominus}(n^{1/4})\\
&\leqslant C\,n\log n + 0.99\,C\,n\log n + 0.99^2\,C\,n\log n + 1.98^3\,n^{7/8}\,\mathrm{M}^{\ominus}(n^{1/8})\\
&\vdots\\
&\leqslant O(n\log n)
\end{aligned}
$$

Note about Schönhage–Strassen multiplication

What if…

$$\begin{aligned}
\mathsf{M}^{\ominus}(n) &\leqslant C\,n\log n + 1.98\,n^{1/2}\,\mathsf{M}^{\ominus}(n^{1/2}) \\
&\leqslant C\,n\log n + 0.99\,C\,n\log n + 1.98^2\,n^{3/4}\,\mathsf{M}^{\ominus}(n^{1/4}) \\
&\leqslant C\,n\log n + 0.99\,C\,n\log n + 0.99^2\,C\,n\log n + 1.98^3\,n^{7/8}\,\mathsf{M}^{\ominus}(n^{1/8}) \\
&\;\;\vdots \\
&\leqslant O(n\log n)
\end{aligned}$$

Next aim

$$\mathsf{M}(n) \leqslant C\,n\log n + (d-\epsilon)\,n^{1-1/d}\,\mathsf{M}(n^{1/d})$$

Note about Schönhage–Strassen multiplication

What if…

$$
\begin{aligned}
M^{\ominus}(n) &\leqslant C\,n\log n + 1.98\,n^{1/2}\,M^{\ominus}(n^{1/2})\\
&\leqslant C\,n\log n + 0.99\,C\,n\log n + 1.98^2\,n^{3/4}\,M^{\ominus}(n^{1/4})\\
&\leqslant C\,n\log n + 0.99\,C\,n\log n + 0.99^2\,C\,n\log n + 1.98^3\,n^{7/8}\,M^{\ominus}(n^{1/8})\\
&\ \ \vdots\\
&\leqslant O(n\log n)
\end{aligned}
$$

Next aim

$$M(n) \leqslant C\,n\log n + (d-\epsilon)\,n^{1-1/d}\,M(n^{1/d}) \quad \text{or}$$

$$M(n^d) \leqslant C\,d\,n^d\log n + (d-\epsilon)\,n^{d-1}\,M(n)$$

Nussbaumer Polynomial Transforms

$$\mathbb{L} := \mathbb{K}[u]/(u^n - 1)$$

$$\mathbb{L} := \mathbb{K}[u]/(u^n - 1)$$

Schönhage–Strassen

$$\mathbb{L}[x]/(x^n - 1) \overset{\text{DFT}}{\rightleftarrows} \mathbb{L}^n$$

$$\mathrm{mul}_{\mathbb{L}[x]/(x^n-1)} \leqslant n\,\mathrm{mul}_{\mathbb{L}} + O(n^2 \log n)$$

Nussbaumer Polynomial Transforms

$$\mathbb{L} := \mathbb{K}[u]/(u^n - 1)$$

Schönhage–Strassen

$$\mathbb{L}[x]/(x^n - 1) \underset{}{\overset{\text{DFT}}{\rightleftarrows}} \mathbb{L}^n$$

$$\text{mul}_{\mathbb{L}[x]/(x^n-1)} \leqslant n\,\text{mul}_{\mathbb{L}} + O(n^2 \log n)$$

Nussbaumer

$$\mathbb{L}[u_2, \ldots, u_d]/(u_2^n - 1, \ldots, u_d^n - 1) \overset{\text{DFT}}{\rightleftarrows} \mathbb{L}^{n^{d-1}}$$

$$\text{mul}_{\mathbb{L}[u_2,\ldots,u_d]/(u_2^n-1,\ldots,u_d^n-1)} \leqslant n^{d-1}\text{mul}_{\mathbb{L}} + O(d\,n^d \log n)$$

$$\mathbb{L} := \mathbb{K}[u]/(u^n - 1)$$

Schönhage–Strassen

$$\mathbb{L}[x]/(x^n - 1) \overset{\text{DFT}}{\rightleftarrows} \mathbb{L}^n$$

$$\mathrm{mul}_{\mathbb{L}[x]/(x^n-1)} \leqslant n\,\mathrm{mul}_{\mathbb{L}} + O(n^2 \log n)$$

Nussbaumer

$$\mathbb{L}[u_2, \ldots, u_d]/(u_2^n - 1, \ldots, u_d^n - 1) \overset{\text{DFT}}{\rightleftarrows} \mathbb{L}^{n^{d-1}}$$

$$\mathrm{mul}_{\mathbb{L}[u_2,\ldots,u_d]/(u_2^n-1,\ldots,u_d^n-1)} \leqslant n^{d-1}\,\mathrm{mul}_{\mathbb{L}} + O(d\,n^d \log n)$$

What if…

$$\mathbb{K}[x]/(x^{n^d} - 1) \overset{?}{\longrightarrow} \mathbb{K}[u_1, \ldots, u_d]/(u_1^n - 1, \ldots, u_d^n - 1)$$

Lifting the Chinese remainder theorem

$s_1, \ldots, s_d$ pairwise coprime

Lifting the Chinese remainder theorem

$s_1, \ldots, s_d$ pairwise coprime

$$\mathbb{Z}/(s_1 \cdots s_d \mathbb{Z}) \cong \mathbb{Z}/s_1\mathbb{Z} + \cdots + \mathbb{Z}/s_d\mathbb{Z}$$

Lifting the Chinese remainder theorem

$s_1, \ldots, s_d$ pairwise coprime

$$\mathbb{Z}/(s_1 \cdots s_d \mathbb{Z}) \cong \mathbb{Z}/s_1\mathbb{Z} + \cdots + \mathbb{Z}/s_d\mathbb{Z}$$

$$x^{\mathbb{Z}/(s_1 \cdots s_d \mathbb{Z})} \cong u_1^{\mathbb{Z}/s_1\mathbb{Z}} \times \cdots \times u_d^{\mathbb{Z}/s_d\mathbb{Z}}$$

Lifting the Chinese remainder theorem

$s_1, \ldots, s_d$ pairwise coprime

$$\mathbb{Z}/(s_1 \cdots s_d \mathbb{Z}) \cong \mathbb{Z}/s_1\mathbb{Z} + \cdots + \mathbb{Z}/s_d\mathbb{Z}$$

$$x^{\mathbb{Z}/(s_1 \cdots s_d \mathbb{Z})} \cong u_1^{\mathbb{Z}/s_1\mathbb{Z}} \times \cdots \times u_d^{\mathbb{Z}/s_d\mathbb{Z}}$$

$$\begin{aligned} \mathbb{K}[x]/(x^{s_1 \cdots s_d} - 1) &\cong \mathbb{K}[u_1]/(u_1^{s_1} - 1) \otimes \cdots \otimes \mathbb{K}[u_d]/(u_d^{s_d} - 1) \\ &\cong \mathbb{K}[u_1, \ldots, u_d]/(u_1^{s_1} - 1, \ldots, u_d^{s_d} - 1) \end{aligned}$$

Lifting the Chinese remainder theorem

$$s_1, \ldots, s_d \quad \text{pairwise coprime}$$

$$\mathbb{Z}/(s_1 \cdots s_d \mathbb{Z}) \cong \mathbb{Z}/s_1\mathbb{Z} + \cdots + \mathbb{Z}/s_d\mathbb{Z}$$

$$x^{\mathbb{Z}/(s_1 \cdots s_d \mathbb{Z})} \cong u_1^{\mathbb{Z}/s_1\mathbb{Z}} \times \cdots \times u_d^{\mathbb{Z}/s_d\mathbb{Z}}$$

$$\begin{aligned} \mathbb{K}[x]/(x^{s_1 \cdots s_d} - 1) &\cong \mathbb{K}[u_1]/(u_1^{s_1} - 1) \otimes \cdots \otimes \mathbb{K}[u_d]/(u_d^{s_d} - 1) \\ &\cong \mathbb{K}[u_1, \ldots, u_d]/(u_1^{s_1} - 1, \ldots, u_d^{s_d} - 1) \end{aligned}$$

Conclusion

$$\mathbb{K}[x]/(x^{s_1 \cdots s_d} - 1) \longrightarrow \mathbb{K}[u_1, \ldots, u_d]/(u_1^{s_1} - 1, \ldots, u_d^{s_d} - 1)$$

Achieved: $s_1, \ldots, s_d$ pairwise coprime

Required: $s_1 = \cdots = s_d = n$

Lifting the Chinese remainder theorem

$$s_1, \dots, s_d \quad \text{pairwise coprime}$$

$$\mathbb{Z}/(s_1 \cdots s_d \mathbb{Z}) \cong \mathbb{Z}/s_1\mathbb{Z} + \cdots + \mathbb{Z}/s_d\mathbb{Z}$$

$$x^{\mathbb{Z}/(s_1 \cdots s_d \mathbb{Z})} \cong u_1^{\mathbb{Z}/s_1\mathbb{Z}} \times \cdots \times u_d^{\mathbb{Z}/s_d\mathbb{Z}}$$

$$\begin{aligned} \mathbb{K}[x]/(x^{s_1 \cdots s_d} - 1) &\cong \mathbb{K}[u_1]/(u_1^{s_1} - 1) \otimes \cdots \otimes \mathbb{K}[u_d]/(u_d^{s_d} - 1) \\ &\cong \mathbb{K}[u_1, \dots, u_d]/(u_1^{s_1} - 1, \dots, u_d^{s_d} - 1) \end{aligned}$$

Conclusion

$$\mathbb{K}[x]/(x^{s_1 \cdots s_d} - 1) \longrightarrow \mathbb{K}[u_1, \dots, u_d]/(u_1^{s_1} - 1, \dots, u_d^{s_d} - 1)$$

Achieved: $s_1, \dots, s_d$ pairwise coprime

Required: $s_1 = \cdots = s_d = n$

What if… possible to slightly change $s_1, \dots, s_d$?

Rader reduction

DFT of length $p = 5$

$$\begin{pmatrix} A(1) \\ A(\omega^1) \\ A(\omega^2) \\ A(\omega^3) \\ A(\omega^4) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega^1 & \omega^2 & \omega^3 & \omega^4 \\ 1 & \omega^2 & \omega^4 & \omega^6 & \omega^8 \\ 1 & \omega^3 & \omega^6 & \omega^9 & \omega^{12} \\ 1 & \omega^4 & \omega^8 & \omega^{12} & \omega^{16} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix}$$

$$A(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 \in \mathbb{K}[x]/(x^5 - 1)$$

Rader reduction

DFT of length $p = 5$

$$\begin{pmatrix} A(1) \\ A(\omega^1) \\ A(\omega^2) \\ A(\omega^3) \\ A(\omega^4) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega^1 & \omega^2 & \omega^3 & \omega^4 \\ 1 & \omega^2 & \omega^4 & \omega^1 & \omega^3 \\ 1 & \omega^3 & \omega^1 & \omega^4 & \omega^2 \\ 1 & \omega^4 & \omega^3 & \omega^2 & \omega^1 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix}$$

$$A(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 \in \mathbb{K}[x]/(x^5 - 1)$$

Rader reduction

DFT of length $p = 5$

$$\begin{pmatrix} A(1) \\ A(\omega^{2^0}) \\ A(\omega^{2^1}) \\ A(\omega^{2^3}) \\ A(\omega^{2^2}) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega^{2^0} & \omega^{2^1} & \omega^{2^3} & \omega^{2^2} \\ 1 & \omega^{2^1} & \omega^{2^2} & \omega^{2^0} & \omega^{2^3} \\ 1 & \omega^{2^3} & \omega^{2^0} & \omega^{2^2} & \omega^{2^1} \\ 1 & \omega^{2^2} & \omega^{2^3} & \omega^{2^1} & \omega^{2^0} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix}$$

$$1 = 2^0, \quad 2 = 2^1, \quad 3 = 2^3, \quad 4 = 2^2 \pmod 5$$

Rader reduction

DFT of length $p = 5$

$$\begin{pmatrix} A(1) \\ A(\omega^{2^0}) \\ A(\omega^{2^1}) \\ A(\omega^{2^2}) \\ A(\omega^{2^3}) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega^{2^0} & \omega^{2^1} & \omega^{2^3} & \omega^{2^2} \\ 1 & \omega^{2^1} & \omega^{2^2} & \omega^{2^0} & \omega^{2^3} \\ 1 & \omega^{2^2} & \omega^{2^3} & \omega^{2^1} & \omega^{2^0} \\ 1 & \omega^{2^3} & \omega^{2^0} & \omega^{2^2} & \omega^{2^1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix}$$

$$1 = 2^0, \quad 2 = 2^1, \quad 3 = 2^3, \quad 4 = 2^2 \pmod 5$$

Rader reduction

DFT of length $p = 5$

$$\begin{pmatrix} A(1) \\ A(\omega^{2^0}) \\ A(\omega^{2^1}) \\ A(\omega^{2^2}) \\ A(\omega^{2^3}) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega^{2^0} & \omega^{2^1} & \omega^{2^2} & \omega^{2^3} \\ 1 & \omega^{2^1} & \omega^{2^2} & \omega^{2^3} & \omega^{2^0} \\ 1 & \omega^{2^2} & \omega^{2^3} & \omega^{2^0} & \omega^{2^1} \\ 1 & \omega^{2^3} & \omega^{2^0} & \omega^{2^1} & \omega^{2^2} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_4 \\ a_3 \end{pmatrix}$$

$$1 = 2^0, \quad 2 = 2^1, \quad 3 = 2^3, \quad 4 = 2^2 \pmod 5$$

Rader reduction

DFT of length $p = 5$

$$\begin{pmatrix} A(1) \\ A(\omega^1) \\ A(\omega^2) \\ A(\omega^4) \\ A(\omega^3) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega^1 & \omega^2 & \omega^4 & \omega^3 \\ 1 & \omega^2 & \omega^4 & \omega^3 & \omega^1 \\ 1 & \omega^4 & \omega^3 & \omega^1 & \omega^2 \\ 1 & \omega^3 & \omega^1 & \omega^2 & \omega^4 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_4 \\ a_3 \end{pmatrix}$$

DFT of length $p = 5$

$$\begin{pmatrix} v_0 \\ v_1 \\ v_2 \\ v_3 \end{pmatrix} = \begin{pmatrix} \omega^1 & \omega^2 & \omega^4 & \omega^3 \\ \omega^2 & \omega^4 & \omega^3 & \omega^1 \\ \omega^4 & \omega^3 & \omega^1 & \omega^2 \\ \omega^3 & \omega^1 & \omega^2 & \omega^4 \end{pmatrix} \begin{pmatrix} u_0 \\ u_1 \\ u_2 \\ u_3 \end{pmatrix}$$

$$\Updownarrow$$

$$v_0 + v_1 x + v_2 x^2 + v_3 x^3 = (\omega^1 + \omega^2 x + \omega^4 x^2 + \omega^3 x^3)(u_0 + u_1 x + u_2 x^2 + u_3 x^3)$$

$$\text{modulo } x^4 - 1$$

Rader reduction

DFT of length $p=5$

$$\begin{pmatrix} v_0 \\ v_1 \\ v_2 \\ v_3 \end{pmatrix} = \begin{pmatrix} \omega^1 & \omega^2 & \omega^4 & \omega^3 \\ \omega^2 & \omega^4 & \omega^3 & \omega^1 \\ \omega^4 & \omega^3 & \omega^1 & \omega^2 \\ \omega^3 & \omega^1 & \omega^2 & \omega^4 \end{pmatrix} \begin{pmatrix} u_0 \\ u_1 \\ u_2 \\ u_3 \end{pmatrix}$$

$$\Updownarrow$$

$$v_0 + v_1 x + v_2 x^2 + v_3 x^3 = (\omega^1 + \omega^2 x + \omega^4 x^2 + \omega^3 x^3)(u_0 + u_1 x + u_2 x^2 + u_3 x^3)$$

modulo $x^4 - 1$

$$\mathrm{F}(p) \leqslant \mathrm{M}^{\circ}_{\mathbb{K},\mathrm{fixed}}(p-1) + 2p \cdot \mathrm{add}_{\mathbb{K}}$$

$\mathrm{M}^{\circ}_{\mathbb{K}}(n)$: cost of one multiplication in $\mathbb{K}[x]/(x^n - 1)$

$\mathrm{M}^{\circ}_{\mathbb{K},\mathrm{fixed}}(n)$: when one argument is fixed

Rader reduction

DFT of length $p = 5$

$$\begin{pmatrix} v_0 \\ v_1 \\ v_2 \\ v_3 \end{pmatrix} = \begin{pmatrix} \omega^1 & \omega^2 & \omega^4 & \omega^3 \\ \omega^2 & \omega^4 & \omega^3 & \omega^1 \\ \omega^4 & \omega^3 & \omega^1 & \omega^2 \\ \omega^3 & \omega^1 & \omega^2 & \omega^4 \end{pmatrix} \begin{pmatrix} u_0 \\ u_1 \\ u_2 \\ u_3 \end{pmatrix}$$

$$\Updownarrow$$

$$v_0 + v_1 x + v_2 x^2 + v_3 x^3 = (\omega^1 + \omega^2 x + \omega^4 x^2 + \omega^3 x^3)(u_0 + u_1 x + u_2 x^2 + u_3 x^3)$$

modulo $x^4 - 1$

$$\begin{aligned} \mathrm{F}_{\mathbb{K}}(p) &\leqslant \mathrm{M}^{\circ}_{\mathbb{K},\mathrm{fixed}}(p-1) + 2p \cdot \mathrm{add}_{\mathbb{K}} \\ &\leqslant 2\,\mathrm{F}_{\mathbb{K}}(p-1) + 2p \cdot \mathrm{add}_{\mathbb{K}} \end{aligned}$$

$\mathrm{M}^{\circ}_{\mathbb{K}}(n)$: cost of one multiplication in $\mathbb{K}[x]/(x^n - 1)$

$\mathrm{M}^{\circ}_{\mathbb{K},\mathrm{fixed}}(n)$: when one argument is fixed

Multivariate Rader reduction

Univariate reduction

$$\text{FFT in } \mathbb{K}[x]/(x^p - 1) \longrightarrow \text{multiplication in } \mathbb{K} \oplus \mathbb{K}[x]/(x^{p-1} - 1)$$

Multivariate reduction

$$\text{FFT in } \bigotimes_{1 \leqslant i \leqslant d} \mathbb{K}[x_i]/(x^{p_i} - 1) \longrightarrow \text{multiplication in } \bigotimes_{1 \leqslant i \leqslant d} (\mathbb{K} \oplus \mathbb{K}[x_i]/(x_i^{p_i - 1} - 1))$$

Essentially

$$\mathbb{K}[x]/(x^{p_1 \cdots p_d} - 1) \longrightarrow \mathbb{K}[u_1, \ldots, u_d]/(u_1^{p_1 - 1} - 1, \ldots, u_d^{p_d - 1} - 1)$$

How to choose our primes

$$p_i \;=\; q_i 2^l + 1, \qquad q_i \;\ll\; 2^l, \qquad q_i \text{ odd prime}, \qquad i \;=\; 1, \ldots, d$$

How to choose our primes

$$p_i = q_i 2^l + 1, \qquad q_i \ll 2^l, \qquad q_i \text{ odd prime}, \qquad i = 1, \ldots, d$$

OK with “probability” l^{-1} for “random” prime with $q_i \ll 2^l$

How to choose our primes

$$p_i = q_i 2^l + 1, \qquad q_i \ll 2^l, \qquad q_i \text{ odd prime}, \qquad i = 1, \ldots, d$$

OK with “probability” l^{-1} for “random” prime with $q_i \ll 2^l$

Note: we assumed q_i prime for convenience, but this is not really essential

How to choose our primes

$$p_i = q_i 2^l + 1, \qquad q_i \ll 2^l, \qquad q_i \text{ odd prime}, \qquad i = 1, \ldots, d$$

OK with "probability" l^{-1} for "random" prime with $q_i \ll 2^l$

Note: we assumed q_i prime for convenience, but this is not really essential

$$
\begin{aligned}
l &= 8 & q &= 3, 13, 31, 37, 157, 163, 181, 193, \ldots \\
l &= 16 & q &= 37, 103, 307, 313, 397, 421, 487, 541, \ldots \\
l &= 32 & q &= 43, 73, 157, 181, 211, 433, 571, 601, \ldots \\
l &= 64 & q &= 163, 337, 487, 907, 1051, 1297, 1453, 1567, \ldots \\
l &= 128 & q &= 1171, 2551, 3607, 3907, 4021, 4483, 4567, 4603, \ldots \\
l &= 256 & q &= 607, 1567, 1783, 2683, 2797, 4993, 6577, 6871, \ldots \\
l &= 512 & q &= 223, 2083, 2803, 3853, 4783, 9403, 9781, 10303, \ldots \\
l &= 1024 & q &= 1987, 4447, 15031, 22807, 26713, 46153, 46507, 47653, \ldots
\end{aligned}
$$

How to choose our primes

$$p_i = q_i 2^l + 1, \qquad q_i \ll 2^l, \qquad q_i \text{ odd prime}, \qquad i = 1, \ldots, d$$

OK with "probability" l^{-1} for "random" prime with $q_i \ll 2^l$

Note: we assumed q_i prime for convenience, but this is not really essential

$$\begin{aligned} & \mathbb{K}[x_1, \ldots, x_d] / (x_1^{p_1 - 1} - 1, \ldots, x_d^{p_d - 1} - 1) \\ \cong\ & \mathbb{K}[u_1, \ldots, u_d, v_1, \ldots, v_d] / \left(u_1^{q_1} - 1, \ldots, u_d^{q_d} - 1, v_1^{2^l} - 1, \ldots, v_d^{2^l} - 1\right) \\ \cong\ & \mathbb{K}[y, v_2, \ldots, v_d] / \left(y^{q_1 \cdots q_d 2^l} - 1, v_2^{2^l} - 1, \ldots, v_d^{2^l} - 1\right) \end{aligned}$$

How to choose our primes

$$p_i = q_i 2^l + 1, \qquad q_i \ll 2^l, \qquad q_i \text{ odd prime}, \qquad i = 1, \ldots, d$$

OK with "probability" l^{-1} for "random" prime with $q_i \ll 2^l$

Note: we assumed q_i prime for convenience, but this is not really essential

$$\begin{aligned} & \mathbb{K}[x_1, \ldots, x_d] / (x_1^{p_1 - 1} - 1, \ldots, x_d^{p_d - 1} - 1) \\ \cong\ & \mathbb{K}[u_1, \ldots, u_d, v_1, \ldots, v_d] / \left(u_1^{q_1} - 1, \ldots, u_d^{q_d} - 1, v_1^{2^l} - 1, \ldots, v_d^{2^l} - 1\right) \\ \cong\ & \mathbb{K}[y, v_2, \ldots, v_d] / \left(y^{q_1 \cdots q_d 2^l} - 1, v_2^{2^l} - 1, \ldots, v_d^{2^l} - 1\right) \end{aligned}$$

Conclusion

$$\mathbb{K}[x] / (x^{p_1 \cdots p_d} - 1) \longrightarrow \mathbb{K}[y, v_2, \ldots, v_d] / \left(y^{q_1 \cdots q_d 2^l} - 1, v_2^{2^l} - 1, \ldots, v_d^{2^l} - 1\right)$$

$$\mathsf{M}_{\mathbb{K}}^{\circ}(\underbrace{p_1 \cdots p_d}_{\geqslant 2^{(d+\epsilon) l}}) \quad \leqslant \quad 2^{(d-1) l} \mathsf{M}_{\mathbb{K}}^{\circ}(\underbrace{q_1 \cdots q_d\, 2^l}_{2^{(1+\epsilon) l}}) + O(d\, 2^l \log 2^l \operatorname{add}_{\mathbb{K}})$$

Summary

$\mathbb{Z}$

→ Embed

$\mathbb{C}[x]/(x^{p_1 \cdots p_d} - 1)$

→ Chinese remaindering à la Good

$\mathbb{C}[u_1, \ldots, u_d]/(u_1^{p_1} - 1, \ldots, u_d^{p_d} - 1)$

→ FFT-multiplication

$\mathrm{DFT}(p_1, \ldots, p_d)$ over $\mathbb{C}$

→ Multivariate Rader transform

cheap $\mathrm{DFT}(2^l, \overset{(d-1)\times}{\ldots}, 2^l)$ over $\mathbb{C}[x]/(x^{q_1 \cdots q_d 2^l} - 1)$

$2^{(d-1)l}$ multiplications in $\mathbb{C}[x]/(x^{q_1 \cdots q_d 2^l} - 1)$

→ Reencode and recurse

Linnik constants

$$P(a,k) := \min\{ck+a : c \in \mathbb{N},\ ck+a \text{ is prime}\}$$

$$P(k) := \max\{P(a,k) : 0<a<k,\ a \wedge k = 1\}$$

$$L \text{ is a Linnik constant} :\Longleftrightarrow P(k) = O(k^L)$$

Conclusion

Linnik constants

$$P(a,k) := \min\{ck+a : c \in \mathbb{N},\ ck+a \text{ is prime}\}$$

$$P(k) := \max\{P(a,k) : 0<a<k,\ a \wedge k = 1\}$$

$$L \text{ is a Linnik constant } :\Longleftrightarrow P(k) = O(k^L)$$

Theorem

If there exists a Linnik constant $L < 1 + \frac{1}{303}$, *then*

$$\mathsf{I}(N) = O(N \log N).$$

Conclusion

Linnik constants

$$P(a,k) := \min\{ck+a : c \in \mathbb{N},\ ck+a \text{ is prime}\}$$

$$P(k) := \max\{P(a,k) : 0<a<k,\ a \wedge k = 1\}$$

$$L \text{ is a Linnik constant} :\Longleftrightarrow P(k) = O(k^L)$$

Theorem

If there exists a Linnik constant $L < 1 + \frac{1}{303}$, then

$$\mathsf{I}(N) = O(N \log N).$$

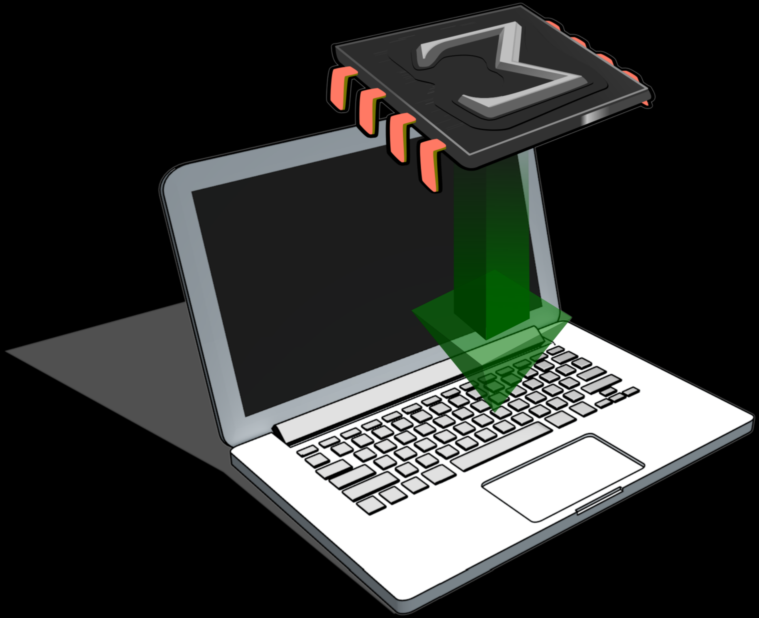
Theorem

If there exists a Linnik constant $L < 1 + 2^{-1162}$, then

$$\mathsf{M}_{\mathbb{F}_q}(n) = O(n \log q \log(n \log q)),$$

uniformly in q.

Thank you !



http://www.texmacs.org