Eine verständliche Beschreibung des Schönhage-Strassen-Algorithmus

Malte Leip

9. April 2009

1 Einleitung

1.1 Wieso gibt es diesen Text?

Im Internet findet man kaum Beschreibungen des Schönhage-Strassen-Algorithmus. Die verfügbaren Beschreibungen sind für die meisten Menschen schwer verständlich und beinhalten keine Beispiele. Dies möchte ich mit meiner Beschreibung ändern. Ich hoffe sie ist einfacher als die anderen Beschreibungen und hilft, den Schönhage-Strassen-Algorithmus zu verstehen. Ich beschreibe beide Varianten des Schönhage-Strassen-Algorithmus, die komplexe Variante und die modulare Variante.

1.2 Was ist hier anders?

Ich versuche in meinem Text auch Schritte zu erklären, die für jemanden mit guten mathematischen Vorkenntnissen "offensichtlich" sind. Diese werden in anderen Informationsquellen oft übersprungen. Zusätzlich gibt es zu den meisten Schritten ein Beispiel, damit das Vorgehen klarer wird. Schlussendlich gibt es dann auch noch ein komplettes Beispiel zum Multiplizieren mit beiden Varianten des Schönhage-Strassen-Algorithmus.

1.3 Wie ist dieser Text aufgebaut?

Der Text ist in zwei Hälften geteilt. Die linke Seite beinhaltet die theoretische Beschreibung und einige kleine Beispiele. Die wichtigsten Abschnitte und Gleichungen sind fett gedruckt. Wenn man nur die fetten Stellen liest, erhält man einen "Kurzüberblick" über den Schönhage-Strassen-Algorithmus. Dies ist z. B. bei erneutem Lesen hilfreich, da man so die Herleitungen usw. überspringen kann. Die rechte Seite beinhaltet ein vollständiges Beispiel des Schönhage-Strassen-Algorithmus, mit allen Schritten. Dieses Beispiel ist zur besseren Unterscheidung auch in einer anderen Schriftart geschrieben. Ich empfehle zunächst einmal nur das theoretische zu lesen und danach noch einmal beides gemeinsam, wobei man versucht, das Beispiel nachzuvollziehen.

1.4 Zwei Varianten

Die Grundidee des Schönhage-Strassen-Algorithmus ist das Aufspalten der Zahlen in Stücke geeigneter Länge, der Fourier-Transformation, Multiplikation der einzelnen Elemente und Rücktransformation. Dies kann man entweder mit komplexen Zahlen oder in einem Restklassenring durchführen. Ich werde sowohl die komplexe als auch die modulare Variante beschreiben. Bei der komplexen Variante hat man Zahlen, die nicht mit unendlicher Genauigkeit berechnet werden können. Deshalb muss mit einer genügend hoher Genauigkeit gerechnet werden, damit der Fehler hinterher rausfällt. Die modulare Variante benötigt so etwas nicht. Sie ist meist schneller, weshalb sie auch bevorzugt eingesetzt wird.

...

2 Der Schönhage-Strassen-Algorithmus mit komplexen Zahlen

2.1 Das Faltungsprodukt

Multipliziert man zwei n-stellige Zahlen miteinander ohne den Übertrag zu beachten, so ist die so erhaltene Folge das Faltungsprodukt der zwei Eingabefolgen (der zwei zu multiplizierenden Zahlen). Ein Beispiel:

1	2	3	4	*	2	3	4	1
					1	2	3	4
				4	8	12	16	
			3	6	9	12		
		2	4	6	8			
		2	7	16	26	26	19	4

Die Folge $(2, 7, 16, 26, 26, 19, 4)$ ist das Faltungsprodukt der Folgen $(1, 2, 3, 4)$ und $(2, 3, 4, 1)$ Macht man jetzt noch die Überträge, so erhält man das Produkt, 2888794.

Aus was besteht dieses Faltungsprodukt? Das Element ganz rechts ist das Produkt der beiden ganz rechten Elemente, also $1 * 4$, das Element eins weiter links ist die Summe der Produkte des jeweils ganz rechten und das zweitrechteste Element, also $(1 * 3) + (4 * 4)$.

Allgemein, haben wir die Folgen $(..., a_2, a_1, a_0)$ und $(..., b_2, b_1, b_0)$ und das Faltungsprodukt $(...c_2, c_1, c_0)$, so ist c_r definiert als:

$$c_r = \sum_{i+j=r} a_i b_j \tag{1}$$

Dies ist sehr interessant in Verbindung mit der Fourier Transformation. Man hat zwei Zahlen a und b mit n Ziffern. Man wählt eine natürliche Zahl K aus, die die Bedingung $K \geq 2n$ erfüllt (bei den Zahlen oben ist $n = 4$, also gilt $K \geq 8$ und man wählt K z. B. $K = 8$). Hat man die Folgen $(a_{K-1}, ..., a_1, a_0)$, von der Zahl a (welche noch immer eigentlich aus n Ziffern besteht, die Anzahl an Elementen wird nur bis K Ziffern mit Nullen aufgefüllt), also z. B. $(0, 0, 0, 0, 1, 2, 3, 4)$, und $(b_{K-1}, ..., b_1, b_0)$, also z. B. $(0, 0, 0, 0, 2, 3, 4, 1)$, so erhält man durch die Fourier Transformation die Folgen $(\hat{a}_{K-1}, ..., \hat{a}_1, \hat{a}_0)$ und $(\hat{b}_{K-1}, ..., \hat{b}_1, \hat{b}_0)$. Multipliziert man die einzelnen Elemente miteinander, so dass man die Folge $(\hat{a}_{K-1}\hat{b}_{K-1}, ..., \hat{a}_1\hat{b}_1, \hat{a}_0\hat{b}_0)$ erhält, so ist diese Folge die Fouriertransformierte einer Folge $(c_{K-1}, ..., c_1, c_0)$, wobei gilt

$$c_r = \sum_{i+j \equiv r(mod K)} a_i b_j \tag{2}$$

$i + j \equiv r(modK)$ bedeutet, dass, wenn man $i + j$ durch K teilt, der selbe Rest bleibt, wie wenn man r durch K teilt ($i + j$ und r sind kongruent modulo K).

Man kann natürlich auch mehr als eine Ziffer in jedes Element der Folge packen, d.h. man kann die Zahl auch in Stücke zu je l Ziffern teilen. Hat man immer nur eine Ziffer, so ist eben $l = 1$.

Somit ist die Folge $(c_0, c_1, ..., c_{K-1})$, welche man durch die inverse diskrete Fourier Transformation bekommt, das Faltungsprodukt, womit man dann das Endergebnis der Multiplikation errechnen kann.[8] Dies nennt sich das Faltungstheorem und ist die Grundidee hinter dem Schönhage-Strassen-Algorithmus.

Hier wird auch klar, warum $K \geq 2n$ sein muss. Wenn man zwei Zahlen mit n Ziffern multipliziert, so erhält man eine Zahl mit maximal $2n$ Ziffern.

...

Um dann noch das Produkt zu erhalten, muss man nur noch die Überträge machen, d.h. Wir addieren die einzelnen Elemente. Allerdings hat c_{K-2} einen höheren Stellenwert als c_{K-1}. Deswegen "verschieben" wir die Zahlen bevor wir sie addieren:

$$c = \sum_{h=0}^{K-1} c_h 10^{hl} \tag{3}$$

Das benutzte Element bei $h = 1$ muss um l Stellen verschoben werden, d.h. wir multiplizieren mit 10^l, da wir im Dezimalsystem sind. Wären wir im Dualsystem, so würden wir mit 2^l multiplizieren. Das Element bei $h = 2$ muss um $2l$ verschoben werden etc. Deswegen multiplizieren wir mit 10^{hl}.

...

2.2 Durchführung der Multiplikation

Nun kommen wir zu dem eigentlichen Ziel: zwei ganze Zahlen zu multiplizieren. Die Durchführung der einzelnen Schritte wird dann in den jeweiligen Unterkapiteln erklärt (die Fourier-Transformation, etc.). Einiges hier wird erst nach der Lektüre der unteren Abschnitte voll verständlich sein.

Die Zahlen liegen in Binärschreibweise vor und haben **je n Ziffern** (ist eine kürzer als die andere, werden entsprechend viele Nullen vorne angefügt). Die beiden Zahlen werden **a bzw. b genannt** . Diese könnten z. B. 9876_{10} und 1234_{10} sein, also in der geforderten Binärschreibweise $a = 10011010010100_2$ und $b = 10011010010_2$. n, also die Anzahl an Ziffern, ist bei a 14 und bei b 11. Wir erweitern b also zu $b = 00010011010010_2$. Somit ist n nun bei beiden gleich 14. Da wir für die Fourier Transformation schließlich eine Folge brauchen, ist der nächste Schritt das **Aufspalten der beiden Zahlen in K Stücke zu je l Bits** . Dabei muss **K eine Zweierpotenz sein, also $K = 2^k$** . Außerdem definieren wir **$L = 2^l$** . Für das Aufspalten in Teilstücke gilt die Beschränkung **$2n \leq 2^k l < 4n$** (warum größer $2n$ siehe das Kapitel Faltungsprodukt). Das heißt in unserem Beispiel $28 \leq 2^k l < 56$. Wählen wir für $l = 4$. Dann haben wir $28 \leq 2^k * 4 < 56$, dividieren wir nun durch 4, so ergibt sich $7 \leq 2^k < 14$. Um k herauszufinden logarithmieren wir zur Basis 2: $log_2(7) \leq k < log_2(14)$. Setzt man nun die Werte der Logarithmen ein, so erhält man $2,81... \leq 2^k < 3,81....$ Die einzige ganze Zahl, die für k in Frage kommt ist somit $k = 3$. Wir haben nun die Folgen $(0000, 0000, 0000, 0000, 0010, 0110, 1001, 0100)_2$ und $(0000, 0000, 0000, 0000, 0000, 0100, 1101, 0010)_2$. Wir können für a und b schreiben $a = (a_{K-1}...a_1a_0)_L$ und entsprechend für b. D.h. $a_0 = 0100, a_1 = 1001, a_2 = 0110, a_3 = 0010, a_4 = 0000, ..., a_7 = 0000$ und $b_0 = 0010, b_1 = 1101, b_2 = 0100, b_3 = 0000, ..., b_7 = 0000$.

Bevor die Fourier Transformation der Folgen gemacht wird, empfiehlt Knuth[1], **die einzelnen Elemente durch 2^{k+l} zu teilen** , damit der Fehler, der durch fehlende Genauigkeit auftritt, besser abschätzbar wird (die Absolutwerte wären dann kleiner 1). Nachdem c_j zurück transformiert wurde, wird jedes c_j mit $2^{2(k+l)}$ multipliziert. Im Beispiel wird dies nicht berücksichtigt, da bei solch kleinen Zahlen der Fehler sowieso zu klein ist um etwas zu bewirken, aber ohne die Division etc. ist das ganze übersichtlicher (die Zahlen sind dann nicht so klein).

Man **berechnet also die diskrete Fourier Transformation der beiden Folgen**, und erhält somit **$(\hat{a}_{K-1}, ..., \hat{a}_1, \hat{a}_0)$ und $(\hat{b}_{K-1}, ..., \hat{b}_1, \hat{b}_0)$** . Nun multipliziert man die Elemente miteinander, sodass **$\hat{c}_s = \hat{a}_s\hat{b}_s$ für $0 \leq s < K$** . Danach wird die **doppelte Transformation, also $\hat{\hat{c}}_s$** ausgerechnet und **damit dann auch c_s** (wie das Ganze funktioniert wird in den entsprechenden Unterkapiteln beschrieben). Somit erhält man die Folge **$(c_{K-1}, ..., c_1, c_0)$** . Daraus lässt sich das Produkt folgendermaßen ausrechnen:

$$ab = \sum_{h=0}^{K-1} c_h L^h = c_0 + c_1 L + ... + c_{K-2} L^{K-2} + c_{K-1} L^{K-1} \tag{4}$$

Dies ist einfach wieder das Zusammensetzten einer Zahl aus der Ergebnisfolge. Diese Ergebnisfolge war das Faltungsprodukt, somit ist auch klar, wieso mit L multipliziert wird.

Machen wir ein Beispiel der Multiplikation mit dem komplexen Schönhage-Strassen-Algorithmus: Wir möchten die beiden Zahlen $a = 9876$ und $a = 5678$ miteinander multiplizieren. In Binärschreibweise sind diese $a = 10011010010100_2$ und $b = 01011000101110_2$. Wir teilen diese Zahlen in Stücke zu je 4 Bits, also $l = 4$. Durch $2n \leq 2^k l < 4n$, also $2n \leq 4 * 2^k < 4n$ bekommen wir $\frac{1}{2}n \leq 2^k < n$. n ist hier 14, somit haben wir $7 \leq 2^k < 14$. Logarithmieren wir nun wieder, so erhalten wir $log_2(7) \leq k < log_2(14)$, und schließlich $2,807... \leq k < 3.807$. k ist somit 3. Berechnen wir nun gleich $K = 2^k = 2^3 = 8$. Nun stückeln wir die beiden Zahlen und erhalten somit

s	a_s		b_s	
0	0100_2	4_{10}	1110_2	14_{10}
1	1001_2	9_{10}	0010_2	2_{10}
2	0110_2	6_{10}	0110_2	6_{10}
3	0010_2	2_{10}	0001_2	1_{10}
4	0000_2	0_{10}	0000_2	0_{10}
5	0000_2	0_{10}	0000_2	0_{10}
6	0000_2	0_{10}	0000_2	0_{10}
7	0000_2	0_{10}	0000_2	0_{10}

2.3 Berechnung von ω

Bei der Fouriertransformation werden wir bald oft die primitive Einheitswurzel ω und die Potenzen davon benötigen. Dabei ist $\omega = e^{\frac{2\pi i}{K}}$. Anstatt diese jedes Mal neu zu berechnen, ist es sinnvoller, die Werte vorzuberechnen. Ein Problem ist auch die Genauigkeit, die komplexe Zahl ω kann nicht auf unendliche Genauigkeit berechnet werden. Mit der Genauigkeit beschäftigt sich ein Kapitel weiter unten. Um die Potenzen von ω vorzuberechnen geht man folgendermaßen vor[1][3]: Zuerst wird definiert:

$$\omega_r = e^{\frac{2\pi i}{2^r}} \tag{5}$$

Außerdem schreiben wir

$$\boldsymbol{\omega_r = x_r + iy_r} \tag{6}$$

Um den jeweils nächsten reellen bzw. komplexen Teil zu berechnen kann man folgende Formeln verwenden:

$$\boldsymbol{x_{r+1} = \sqrt{\frac{1 + x_r}{2}}} \tag{7}$$

und

$$\boldsymbol{y_{r+1} = \frac{y_r}{2x_{r+1}}} \tag{8}$$

für $r > 1$ (die Werte für $r = 0$ und $r = 1$ werden eingespeichert). Hat man dann diese Werte ausgerechnet, so können die Potenzen von ω folgendermaßen berechnet werden:

$$\boldsymbol{\omega^j = \omega_1^{j_{k-1}} ... \omega_{k-1}^{j_1} \omega_k^{j_0}} \tag{9}$$

Zu k siehe oben, j ist hier der Exponent und $\boldsymbol{j = (j_{k-1} ... j_1, j_0)_2}$.

Wie kommen diese Formeln zustande? Betrachten wir zunächst die ω auf dem Einheitskreis der komplexen Ebene.

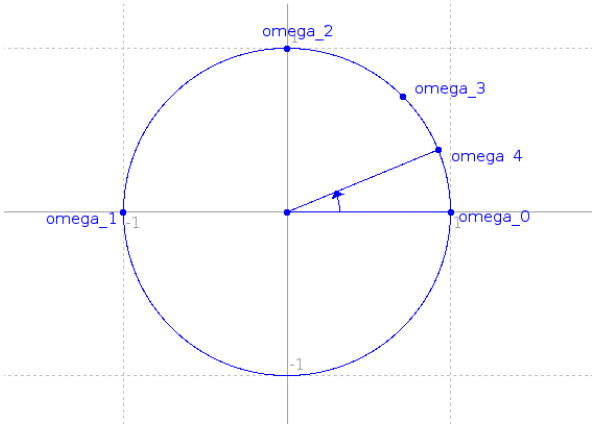

Abbildung 1: Skizze zur den Omega auf dem Einheitskreis der komplexen Ebene

Hier kann man auch anschaulich sehen, dass sich der Winkel von ω_r auf ω_{r+1} halbiert. Was bringt uns das? Wenn wir $\omega_r = x_r + iy_r$ haben, so möchten wir nun den Punkt auf dem Einheitskreis herausfinden, der durch den halben Winkel charakterisiert ist (für ω_r mit $r \geq 2$).

Bevor wir mit der Fourier Transformation weitermachen, erstellen wir zunächst eine Liste von Werten für ω, wofür wir allerdings zunächst die Werte von x_r und y_r benötigen: **Anmerkung: In allen folgenden Tabellen/Listen sind die Werte auf 3 Nachkommastellen gerundet!**

- $x_1 = -1$
- $x_2 = 0$
- $x_3 = \sqrt{\frac{1+0}{2}} = \sqrt{0,5} = 0,707$

und für y:

- $y_1 = 0$
- $y_2 = 1$
- $y_3 = \frac{1}{2*0,707} = \frac{1}{1,414} = 0,707$

Zusammengesetzt ergeben sich die Werte von ω:

- $\omega_1 = -1$
- $\omega_2 = i$
- $\omega_3 = 0,707 + 0,707i$

Hieraus können wir nun die Werte der Potenzen von ω, welches hier den Wert von ω_3 hat, errechnen:

- $\omega^0 = (-1)^0 * (i)^0 * (0,707 + 0,707i)^0 = 1$
- $\omega^1 = (-1)^0 * (i)^0 * (0,707 + 0,707i)^1 = 0,707 + 0,707i$
- $\omega^2 = (-1)^0 * (i)^1 * (0,707 + 0,707i)^0 = i$
- $\omega^3 = (-1)^0 * (i)^1 * (0,707 + 0,707i)^1 = -0,707 + 0,707i$
- $\omega^4 = (-1)^1 * (i)^0 * (0,707 + 0,707i)^0 = -1$
- $\omega^5 = (-1)^1 * (i)^0 * (0,707 + 0,707i)^1 = -0,707 - 0,707i$
- $\omega^6 = (-1)^1 * (i)^1 * (0,707 + 0,707i)^0 = -i$
- $\omega^7 = (-1)^1 * (i)^1 * (0,707 + 0,707i)^1 = 0,707 - 0,707i$

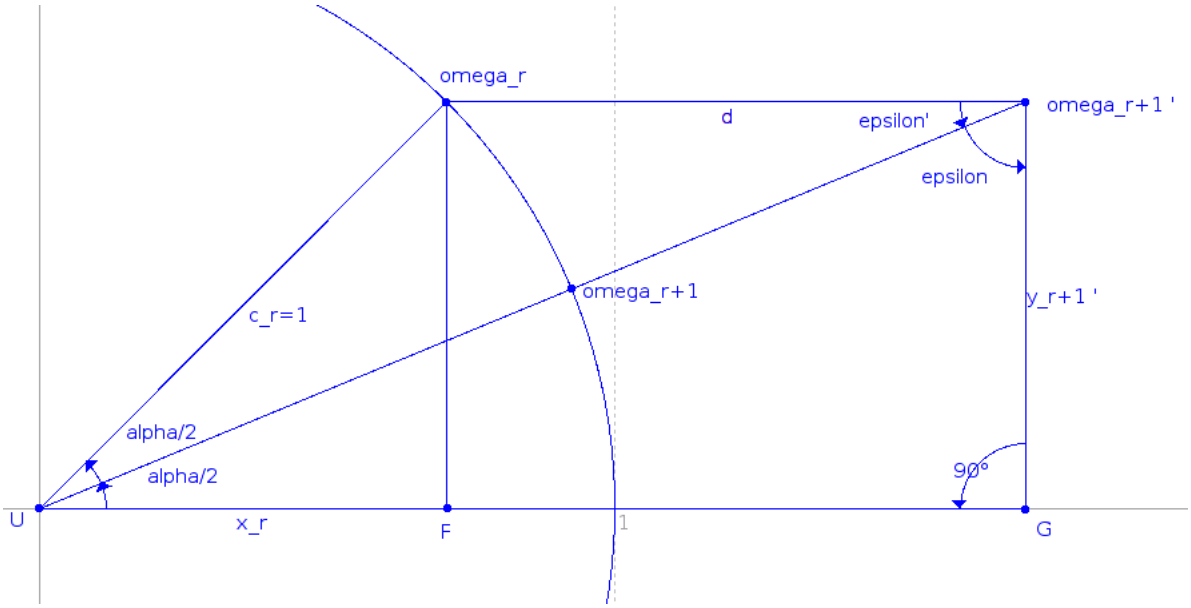

Abbildung 2: Skizze zur Konstruktion des nächsten Omegas

Wir haben das Dreieck mit den Seiten x_r, y_r und der Seite $c = 1$. Betrachten wir nun das Dreieck, welches den halben Winkel hat und $y'_{r+1} = y_r$. Hier sind $c' \neq c$ und $x_{r+1} \neq x_r$:

Das die Winkel $\angle GU\omega_{r+1}{}'$ und $\angle\omega_{r+1}{}'U\omega_r$ jeweils den Wert $\alpha/2$ haben ist klar, denn hiervon gehen wir aus.

Da die Winkelsumme in einem Dreieck 180 ist, folgt, dass der Winkel $\epsilon = 180-(90+\frac{\alpha}{2}) = 90-\frac{\alpha}{2}$. Da ϵ und ϵ' zusammen 90 ergeben, folgt, dass $\epsilon' = 90 - \epsilon = 90 - (90 - \frac{\alpha}{2}) = \frac{\alpha}{2}$. Somit hat das Dreieck $\omega_{r+1}{}'U\omega_r$ zwei gleiche Winkel und folglich auch zwei gleiche Seiten, d.h. $d = c_r = 1$

Um den Punkt $\omega_{r+1}{}'$ zu finden, gehen wir von ω einfach eins nach rechts. Hier ist natürlich $c_{r+1}{}' \neq 1$, wir brauchen allerdings ω_{r+1} mit $c_{r+1} = 1$. Wir teilen also alle Seiten unseres "neuen" Dreiecks $GU\omega_{r+1}{}'$ durch die Länge von $c_{r+1}{}'$. Was ist diese Länge? Durch den Satz des Pythagoras erhalten wir: $c_{r+1}{}' = \sqrt{(x_r+1)^2 + y_r^2} = \sqrt{x_r^2 + 2x_r + 1 + y_r^2} = \sqrt{2x_r + 1 + x_r^2 + y_r^2}$. Wir wissen aus dem anderen Dreieck, dass $x_r^2 + y_r^2 = c_r^2 = 1$, d.h. wir haben: $c_{r+1}{}' = \sqrt{2x_r + 1 + 1^2} = \sqrt{2x_r + 2} = \sqrt{2(x_r + 1)}$.

Wir müssen nun also $x_r + 1$ durch $\sqrt{2(x_r + 1)}$ teilen, um x_{r+1} zu erhalten. Wir bekommen somit $x_{r+1} = \frac{x_r+1}{\sqrt{2(x_r+1)}} = \frac{\sqrt{(x_r+1)^2}}{\sqrt{2(x_r+1)}} = \sqrt{\frac{(x_r+1)^2}{2(x_r+1)}} = \sqrt{\frac{(x_r+1)}{2}}$.

Somit haben wir die erste Formel schon geklärt. Betrachten wir nun y_{r+1}. Hier teilen wir nur y_r durch $\sqrt{2(x_r + 1)}$, somit erhalten wir: $y_{r+1} = \frac{y_r}{\sqrt{2(x_r+1)}} = \frac{y_r}{\sqrt{\frac{4(x_r+1)}{2}}} = \frac{y_r}{2\sqrt{\frac{(x_r+1)}{2}}}$ Hier können wir x_{r+1} einsetzen. Wir erhalten $y_{r+1} = \frac{y_r}{2x_{r+1}}$.

...

2.4 Die Diskrete Fourier Transformation

Die normale Diskrete Fourier Transformation der Folge $(a_0, a_1, ..., a_{K-1})$ ist gegeben durch

$$\hat{a}_s = \sum_{t=0}^{K-1} \omega^{st} a_t \tag{10}$$

bei $0 \leq s < K$ [4] . Hierbei ist ω eine primitive K-te Einheitswurzel, wobei

$$\omega = e^{\frac{2\pi i}{K}} \tag{11}$$

genommen wird.[5] [1]

Ein Beispiel zur DFT: Hat man die Folge $(12, 3, 5) = (a_2, a_1, a_0)$, so ist $n = 3$. Da $K \geq 2n - 1$ nimmt man $k = 3$ und $K = 2^k = 2^3 = 8$. Deshalb erweitert man die Folge zu $(0, 0, 0, 0, 0, 12, 3, 5) = (a_7, a_6, ..., a_1, a_0)$. Man möchte nun z. B. $\hat{a}_3$ herausfinden:

$$\hat{a}_3 = \sum_{t=0}^{7} \omega^{3t} a_t = a_0 + \omega^3 a_1 + \omega^6 a_2 + \omega^9 a_3 + \omega^{12} a_4 + \omega^{15} a_5 + \omega^{18} a_6 + \omega^{21} a_7 \tag{12}$$

Der Wert für ω wird folgendermaßen berechnet:

$$\omega = e^{\frac{2\pi i}{K}} = \omega = e^{\frac{2\pi i}{8}} = 0,707106781... + 0,707106781...i \tag{13}$$

Wir bekommen nun folgende Werte:

- Bei $t = 0$ bekommen wir $\omega^{3*0} a_0 = 1 * 5 = 5$
- Bei $t = 1$ bekommen wir $\omega^{3*1} a_1 = \omega^3 * 3 = -2,12132034 + 2,12132034i$
- Bei $t = 2$ bekommen wir $\omega^{3*2} a_2 = \omega^6 * 12 = -12i$
- Bei $t = 3$ bekommen wir $\omega^{3*3} a_3 = \omega^9 * 0 = 0$
- Bei $t = 4$ bekommen wir $\omega^{3*4} a_4 = \omega^{12} * 0 = 0$
- Bei $t = 5$ bekommen wir $\omega^{3*5} a_5 = \omega^{15} * 0 = 0$
- Bei $t = 6$ bekommen wir $\omega^{3*6} a_6 = \omega^{18} * 0 = 0$
- Bei $t = 7$ bekommen wir $\omega^{3*7} a_0 = \omega^{21} * 0 = 0$

Zusammenaddiert ergibt sich $\hat{a}_3 = 5 - 2,12132034 + 2,12132034i - 12i = 2,87867966 - 9,87867966i$ - dies ist das dritte Element der Fourier Transformierten der Reihe $(a_7, a_6, a_5, a_4, a_3, a_2, a_1, a_0)$.

...

2.5 Die Fast Fourier Transformation

Ist K eine Zweierpotenz, und zwar $K = 2^k$ so kann die Diskrete Fourier Transformation schneller berechnet werden (deswegen wurde K oben eingeführt).

Wir definieren zunächst einmal:

$A^{[j+1]}(s_{k-1}, ..., s_{k-j-1}, t_{k-j-2}, ..., t_0) \leftarrow$
$A^{[j]}(s_{k-1}, ..., s_{k-j}, 0, t_{k-j-2}, ..., t_0) + A^{[j]}(s_{k-1}, ..., s_{k-j}, 1, t_{k-j-2}, ..., t_0) * \omega^{2^{k-j-1}(s_{k-j-1}...s_{k-1})_2}$

und:

$A^{[0]}_{(t_{k-1},...,t_0)} = a_t$

wobei $t = (t_{k-1}...t_0)_2$.

Anmerkung: der Pfeil $\leftarrow$ ist der Substitutionsoperator, $a \leftarrow b$ bedeutet, dass der Wert von a durch den aktuellen Wert von b ersetzt werden soll.

Wir erhalten:

$A^{[k]}_{(s_{k-1}...s_0)} = \hat{a_s}$

wobei $s = (s_0 s_1 ... s_{k-1})$

Wie können wir das beweisen?

Nehmen wir an, wir haben bewiesen, dass:

$$A^{[j]}_{(s_{k-1},...,s_{k-j},t_{k-j-1},...,t_0)} = \sum_{0 \le t_{k-1},...,t_{k-j} \le 1} \omega^{2^{k-j}(s_{k-j}...s_{k-1})_2 (t_{k-1}...t_{k-j})_2} a_t \tag{14}$$

Dies lässt sich für z.B. $j = 1$ schnell überprüfen.

Dann können wir nach der Formel oben einsetzen und erhalten somit:

$A^{[j+1]}(s_{k-1}, ..., s_{k-j-1}, t_{k-j-2}, ..., t_0) =$
$\sum_{0 \le t_{k-1},...,t_{k-j} \le 1} \omega^{2^{k-j}(s_{k-j}...s_{k-1})_2 (t_{k-1}...t_{k-j})_2} a_{t_0} + \sum_{0 \le t_{k-1},...,t_{k-j} \le 1} \omega^{2^{k-j}(s_{k-j}...s_{k-1})_2 (t_{k-1}...t_{k-j})_2} a_{t_1} *$
$\omega^{2^{k-j-1}(s_{k-j-1}...s_{k-1})_2}$

Hierbei ist gemeint $t = (t_{k-1}...t_{k-j-1}...t_0)_2$, wobei bei t_0, eben $t_{k-j-1} = 0$ und bei t_1 ist $t_{k-j-1} = 1$.

Versuchen wir nun, diese Formel so umzuformen, dass wir nur , die dasselbe ist, allerdings mit einer Summenformel.

Die beiden Summen an sich kann man zusammenfassen, indem man noch t_{k-j-1} hinzufügt:

$\sum_{0 \le t_{k-1},...,t_{k-j-1} \le 1} \omega^{2^{k-j}(s_{k-j}...s_{k-1})_2 (t_{k-1}...t_{k-j})_2} a_t$

Das hier ist jetzt allerdings nicht gleich der Formel oben, da noch die Multiplikation mit der Potenz von ω fehlt, wenn $t_{k-j-1} = 1$.

Formen wir zunächst die gerade erhaltene Formel um. Wir machen bei den ts einen Shift um eine Stelle, d.h. wir multiplizieren mit 2. Dafür ziehen wir vom Exponenten von 2 noch 1 ab, damit der Wert sich nicht verändert.

$\sum_{0 \le t_{k-1},...,t_{k-j-1} \le 1} \omega^{2^{k-j-1}(s_{k-j}...s_{k-1})_2 (t_{k-1}...t_{k-j}0)_2} a_t$

Nun können wir bei den s auch noch s_{k-j-1} einsetzen, da der Wert, der zusätzlich entstehen würde, wenn $s_{k-j-1} = 1$ wäre, ist $\omega^{2^{k-j-1} * (s_{k-j-1} * 2^j) * 2} = \omega^{2^k * s_{k-j-1}}$ (die Multiplikation mit 2, da der Wert der ts mindestens 2 ist). Wegen der primitiven Einheitswurzel ist dies gleich 1:

$\sum_{0 \le t_{k-1},...,t_{k-j-1} \le 1} \omega^{2^{k-j-1}(s_{k-j-1}...s_{k-1})_2 (t_{k-1}...t_{k-j}0)_2} a_t$

Wenn wir nun 0 mit t_{k-j-1} ersetzen, dann wird, wenn $t_{k-j-1} = 1$, mit $\omega^{2^{k-j-1}(s_{k-j-1}...s_{k-1})_2}$ zusätzlich multipliziert, genau das, was oben noch fehlte!

Somit erhalten wir nun, dass:

$$A^{[j+1]}(s_{k-1}, ..., s_{k-j-1}, t_{k-j-2}, ..., t_0) = \sum_{0 \le t_{k-1},...,t_{k-j-1} \le 1} \omega^{2^{k-j-1}(s_{k-j-1}...s_{k-1})_2 (t_{k-1}...t_{k-j-1})_2} a_t \tag{15}$$

Das ist wieder die Form, von der wir oben ausgegangen sind, nur mit $j+1$ anstatt von j (14).

Im nächsten Schritt errechnen wir zuerst die Fourier Transformation von a über die schnelle Fourier Transformation (FFT), wozu wir zunächst eine Tabelle für die A's errechnen. Die erste Spalte (für $A^{[0]}$) ist simpel, wir setzen einfach die a's ein.

$(u,v,w) =$	$(0,0,0)$	$(0,0,1)$	$(0,1,0)$	$(0,1,1)$	$(1,0,0)$	$(1,0,1)$	$(1,1,0)$	$(1,1,1)$
$A^{[0]}(u,v,w) =$	4	9	6	2	0	0	0	0

Nun müssen wir die $A^{[1]}(u,v,w)$ entsprechend substituieren und dann ausrechnen. Machen wir uns also folgende Liste (2^{k-1} wird hierbei gleich durch 4 ersetzt.):

- $A^{[1]}(0,0,0) \leftarrow A^{[0]}(0,0,0) + \omega^{4*0} A^{[0]}(1,0,0)$
- $A^{[1]}(0,0,1) \leftarrow A^{[0]}(0,0,1) + \omega^{4*0} A^{[0]}(1,0,1)$
- $A^{[1]}(0,1,0) \leftarrow A^{[0]}(0,1,0) + \omega^{4*0} A^{[0]}(1,1,0)$
- $A^{[1]}(0,1,1) \leftarrow A^{[0]}(0,1,1) + \omega^{4*0} A^{[0]}(1,1,1)$
- $A^{[1]}(1,0,0) \leftarrow A^{[0]}(0,0,0) + \omega^{4*1} A^{[0]}(1,0,0)$
- $A^{[1]}(1,0,1) \leftarrow A^{[0]}(0,0,1) + \omega^{4*1} A^{[0]}(1,0,1)$
- $A^{[1]}(1,1,0) \leftarrow A^{[0]}(0,1,0) + \omega^{4*1} A^{[0]}(1,1,0)$
- $A^{[1]}(1,1,1) \leftarrow A^{[0]}(0,1,1) + \omega^{4*1} A^{[0]}(1,1,1)$

Setzen wir nun unsere schon erhaltenen Werte ein und rechnen aus, so können wir unsere Tabelle folgendermaßen ergänzen:

$(u,v,w) =$	$(0,0,0)$	$(0,0,1)$	$(0,1,0)$	$(0,1,1)$	$(1,0,0)$	$(1,0,1)$	$(1,1,0)$	$(1,1,1)$
$A^{[0]}(u,v,w) =$	4	9	6	2	0	0	0	0
$A^{[1]}(u,v,w) =$	4	9	6	2	4	9	6	2

Fertigen wir wieder eine Liste zu $A^{[2]}$ an (2^{k-2} ist hierbei schon durch 2 ersetzt).

- $A^{[2]}(0,0,0) \leftarrow A^{[1]}(0,0,0) + \omega^{2*0} A^{[1]}(0,1,0)$
- $A^{[2]}(0,0,1) \leftarrow A^{[1]}(0,0,1) + \omega^{2*0} A^{[1]}(0,1,1)$
- $A^{[2]}(0,1,0) \leftarrow A^{[1]}(0,0,0) + \omega^{2*2} A^{[1]}(0,1,0)$
- $A^{[2]}(0,1,1) \leftarrow A^{[1]}(0,0,1) + \omega^{2*2} A^{[1]}(0,1,1)$
- $A^{[2]}(1,0,0) \leftarrow A^{[1]}(1,0,0) + \omega^{2*1} A^{[1]}(1,1,0)$
- $A^{[2]}(1,0,1) \leftarrow A^{[1]}(1,0,1) + \omega^{2*1} A^{[1]}(1,1,1)$
- $A^{[2]}(1,1,0) \leftarrow A^{[1]}(1,0,0) + \omega^{2*3} A^{[1]}(1,1,0)$
- $A^{[2]}(1,1,1) \leftarrow A^{[1]}(1,0,1) + \omega^{2*3} A^{[1]}(1,1,1)$

Hier sieht man auch sehr schön, wir das s immer mehr Ziffern umfasst. Bei $A^{[1]}$ war es nur die Ziffern in der Klammer ganz links, hier sind es zwei Ziffern, außerdem waren oben die linken Spalten immer 0 oder 1, hier sind es die mittleren Spalten.

Wenn wir nun für $j = k$ einsetzen, dann erhalten wir:
$A^{[k]}_{(s_{k-1},\ldots,s_{k-k},t_{k-k-1},\ldots,t_0)} = \sum_{0\leq t_{k-1},\ldots,t_{k-k}\leq 1} \omega^{2^{k-k}(s_{k-k}\ldots s_{k-1})_2(t_{k-1}\ldots t_{k-k})_2} a_t$
und somit:
$A^{[k]}_{(s_{k-1},\ldots,s_0)} = \sum_{0\leq t_{k-1},\ldots,t_0\leq 1} \omega^{(s_0\ldots s_{k-1})_2(t_{k-1}\ldots t_0)_2} a_t$
Wenn wir jetzt s und t einsetzen (siehe oben), erhalten wir:
$A^{[k]}_{(s_{k-1},\ldots,s_0)} = \sum_{t=0}^{K-1} \omega^{st} a_t$
Dies ist genau die Definition der diskreten Fourier Transformation!

Berechnen wir nun nochmals $\hat{a}_3$. Wir brauchen dafür $A^{[3]}(1,1,0)$ (da 3 im Dualsystem 011_2 ist, und dies umgedreht 110 entspricht). Schritt für Schritt (Wir ersetzen einfach immer weiter und fassen zusammen):

- $A^{[3]}(1,1,0)$
- $A^{[2]}(1,1,0) + \omega^3 A^{[2]}(1,1,1)$
- $(A^{[1]}(1,0,0) + \omega^6 A^{[1]}(1,1,0)) + \omega^3(A^{[1]}(1,0,1) + \omega^6 A^{[1]}(1,1,1))$
- $[(A^{[0]}(0,0,0)+\omega^4 A^{[0]}(1,0,0))+\omega^6(A^{[}0](0,1,0)+\omega^4 A^{[}0](1,1,0))]+\omega^3[(A^{[0]}(0,0,1)+\omega^4 A^{[0]}(1,0,1))+ \omega^6(A^{[0]}(0,1,1) + \omega^4 A^{[0]}(1,1,1))]$
- $[(a_0 + \omega^4 a_4) + \omega^6(a_2 + \omega^4 a_6)] + \omega^3[(a_1 + \omega^4 a_5) + \omega^6(a_3 + \omega^4 a_7)]$
- $[(5 + \omega^4 * 0) + \omega^6(12 + \omega^4 * 0)] + \omega^3[(3 + \omega^4 * 0) + \omega^6(0 + \omega^4 * 0)]$
- $[5 + \omega^6 * 12] + \omega^3 * 3$
- $[5 - 12i] - 2,12132034 + 2,12132034i$
- $2,87867966 - 9,87867966i$

Diese Berechnungen der Fourier-Transformation werden durch das Beispiel klarer.

Setzten wir nun wieder die Werte ein und berechnen somit die nächste Spalte unserer Tabelle:

$(u,v,w) =$	$(0,0,0)$	$(0,0,1)$	$(0,1,0)$	$(0,1,1)$	$(1,0,0)$	$(1,0,1)$	$(1,1,0)$	$(1,1,1)$
$A^{[0]}(u,v,w) =$	4	9	6	2	0	0	0	0
$A^{[1]}(u,v,w) =$	4	9	6	2	4	9	6	2
$A^{[2]}(u,v,w) =$	10	11	-2	7	$4+6i$	$9+2i$	$4-6i$	$9-2i$

Und schlussendlich das ganze noch einmal für $A^{[3]}$...

- $A^{[3]}(0,0,0) \leftarrow A^{[2]}(0,0,0) + \omega^0 A^{[2]}(0,0,1)$
- $A^{[3]}(0,0,1) \leftarrow A^{[2]}(0,0,0) + \omega^4 A^{[2]}(0,0,1)$
- $A^{[3]}(0,1,0) \leftarrow A^{[2]}(0,1,0) + \omega^2 A^{[2]}(0,1,1)$
- $A^{[3]}(0,1,1) \leftarrow A^{[2]}(0,1,0) + \omega^6 A^{[2]}(0,1,1)$
- $A^{[3]}(1,0,0) \leftarrow A^{[2]}(1,0,0) + \omega^1 A^{[2]}(1,0,1)$
- $A^{[3]}(1,0,1) \leftarrow A^{[2]}(1,0,0) + \omega^5 A^{[2]}(1,0,1)$
- $A^{[3]}(1,1,0) \leftarrow A^{[2]}(1,1,0) + \omega^3 A^{[2]}(1,1,1)$
- $A^{[3]}(1,1,1) \leftarrow A^{[2]}(1,1,0) + \omega^7 A^{[2]}(1,1,1)$

...und ergänzen wieder die Tabelle:

$(u,v,w) =$	$(0,0,0)$	$(0,0,1)$	$(0,1,0)$	$(0,1,1)$	$(1,0,0)$		$(1,0,1)$		$(1,1,0)$		$(1,1,1)$
$A^{[0]}(u,v,w) =$	4	9	6	2	0		0		0		0
$A^{[1]}(u,v,w) =$	4	9	6	2	4		9		6		2
$A^{[2]}(u,v,w) =$	10	11	-2	7	$4+6i$		$9+2i$		$4-6i$		$9-2i$
$A^{[3]}(u,v,w) =$	21	-1	$-2+7i$	$-2-7i$	$8,950-13,778i$	$+$	$-0,950-1,778i$	$-$	$-0,950-1,778i$	$+$	$8,950-13,778i$

Wenn wir für b genauso vorgehen, bekommen wir für b folgende Tabelle:

$(u,v,w) =$	$(0,0,0)$	$(0,0,1)$	$(0,1,0)$	$(0,1,1)$	$(1,0,0)$		$(1,0,1)$		$(1,1,0)$		$(1,1,1)$
$A^{[0]}(u,v,w) =$	14	2	6	1	0		0		0		0
$A^{[1]}(u,v,w) =$	14	2	6	1	14		2		6		1
$A^{[2]}(u,v,w) =$	20	3	8	1	$14+6i$		$2+i$		$14-6i$		$2-i$
$A^{[3]}(u,v,w) =$	23	17	$8+i$	$8-i$	$14,707-8,121i$	$+$	$13,293-3,879i$	$+$	$13,293-3,879i$	$-$	$14,707-8,121i$

...

Nun haben wir alle Daten, um die Fourier-Transformation zu berechnen, wir benötigen: $\hat{a}_s = A^{[k]}(s_{k-1}, ..., s_1, s_0)$ wobei $s = (s_0 s_1 ... s_{k-1})_2$, d.h. hierbei muss man beachten, die Ziffern in der Klammer die *umgedrehte* Binärdarstellung des Indexes sind, Somit berechnen sich die Fouriertransformierten so:

- $\hat{a}_0 = A^{[3]}(0,0,0)$
- $\hat{a}_1 = A^{[3]}(1,0,0)$
- $\hat{a}_2 = A^{[3]}(0,1,0)$
- $\hat{a}_3 = A^{[3]}(1,1,0)$
- $\hat{a}_4 = A^{[3]}(0,0,1)$
- $\hat{a}_5 = A^{[3]}(1,0,1)$
- $\hat{a}_6 = A^{[3]}(0,1,1)$
- $\hat{a}_7 = A^{[3]}(1,1,1)$

Dasselbe gilt natürlich auch für $\hat{b}$.

Somit erhalten wir folgende Werte, wobei wir für die unterste Zeile einfach mit den beiden darüber multiplizieren:

$s =$	0	1	2	3	4	5	6	7
$\hat{a}_s =$	21	$8,950 + 13,778i$	$-2+7i$	$-0,950 + 1,778i$	-1	$-0,950 - 1,778i$	$-2-7i$	$8,950-13,778i$
$\hat{b}_s =$	23	$14,707 + 8,121i$	$8+i$	$13,293 - 3,879i$	17	$13,293 + 3,879i$	$8-i$	$14,707-8,121i$
$\hat{c}_s =$	483	$19,737 + 275,316i$	$-23+54i$	$-5,731 + 27,320i$	-17	$-5,731 - 27,320i$	$-23-54i$	$19,737-275,316i$

2.6 Die Rücktransformation

Um c von $\hat{c}$ zu erhalten muss die Inverse Fast Fourier Transformation (iFFT) angewandt werden. Um $\hat{c}$ zurück zu transformieren muss **zuerst die doppelte Transformation ausgerechnet werden**, d.h. $\hat{\hat{c}}$ wird von $\hat{c}$ mit der oben besprochenen Methode berechnet. **Um von $\hat{\hat{c}}$ dann zu c zu kommen** wird folgende Beziehung verwendet:

$$\hat{\hat{c}}_r = K c_{(-r) mod K} \tag{16}$$

Ein Beispiel: $\hat{\hat{c}}_3 = 456$, $K = 8$. Nun haben wir also $456 = 8c_{(-3)mod8}$, woraus folgt $456 = 8c_5$ nun wird durch 8 geteilt, so dass herauskommt $c_5 = 456/8 = 57$

Um nun die doppelte Transformation von $\hat{c}$ auszurechnen, berechnen wir wie üblich ersteinmal die Tabelle:

$(u,v,w) =$	$(0,0,0)$	$(0,0,1)$	$(0,1,0)$	$(0,1,1)$	$(1,0,0)$	$(1,0,1)$	$(1,1,0)$	$(1,1,1)$
$A^{[0]}(u,v,w) =$	483	$19,737+$ $275,316i$	-23 $+$ $54i$	$-5,731+$ $27,320i$	-17	$-5,731-$ $27,320i$	-23 $-$ $54i$	$19,737-$ $275,316i$
$A^{[1]}(u,v,w) =$	466	$14,006+$ $247,996i$	-46	$14,006-$ $247,996i$	500	$25,468+$ $302,636i$	$108i$	$-25,468+$ $302,636i$
$A^{[2]}(u,v,w) =$	420	$28,012$	512	$495,992i$	392	$-277,168+$ $277,168i$	608	$328,104+$ $328,104i$
$A^{[3]}(u,v,w) =$	$448,012$	$391,988$	$16,008$	$1007,992$	$0,025$	$783,975$	$143,991$	$1072,009$

Somit erhalten wir dann (hier muss man wieder aufpassen, dass die Ziffern in der Klammer der *umgedrehten* Binärdarstellung des Indexes entsprechen):

$\hat{\hat{c}}_0 = 448$
$\hat{\hat{c}}_1 = 0$
$\hat{\hat{c}}_2 = 16$
$\hat{\hat{c}}_3 = 144$
$\hat{\hat{c}}_4 = 392$
$\hat{\hat{c}}_5 = 784$
$\hat{\hat{c}}_6 = 1008$
$\hat{\hat{c}}_7 = 1072$

Nun müssen wir aus der doppelten Transformation die Rücktransformation erhalten, dafür wissen wir, dass $\hat{\hat{c}}_r = Kc_{(-r)modK}$

Zur Verdeutlichung fertigen wir folgende Liste an:

$448 = 8c_{(-0)mod8} = 8c_0$
$0 = 8c_{(-1)mod8} = 8c_7$
$16 = 8c_{(-2)mod8} = 8c_6$
$144 = 8c_{(-3)mod8} = 8c_5$
$392 = 8c_{(-4)mod8} = 8c_4$
$784 = 8c_{(-5)mod8} = 8c_3$
$1008 = 8c_{(-6)mod8} = 8c_2$
$1072 = 8c_{(-7)mod8} = 8c_1$

Somit haben wir nun folgende Liste:

- $c_0 = 448/8 = 56 = 111000_2$
- $c_1 = 1072/8 = 134 = 10000110_2$
- $c_2 = 1008/8 = 126 = 1111110_2$
- $c_3 = 784/8 = 98 = 1100010_2$
- $c_4 = 392/8 = 49 = 110001_2$
- $c_5 = 144/8 = 18 = 10010_2$
- $c_6 = 16/8 = 2 = 10_2$
- $c_7 = 0/8 = 0 = 0_2$

...

Das Produkt berechnet sich dann schlussendlich durch diese Formel: $ab = c_{K-2}L^{K-2}+...+c_1L+c_0$. Fertigen wir also wiederum eine Liste an, in der die Shifts vollzogen wurden (zur besseren Darstellung wurden noch Nullen vorne eingefügt):

- $c_0 = 000000000000000000000111000_2$
- $c_1 = 000000000000001000011000000_2$
- $c_2 = 000000000001111110000000000_2$
- $c_3 = 000000011000100000000000000_2$
- $c_4 = 000011000100000000000000000_2$
- $c_5 = 010010000000000000000000000_2$
- $c_6 = 100000000000000000000000000_2$
- $c_7 = 000000000000000000000000000_2$

  ———————————————————————————

- $ab = 110101011110100110100110000_2$

Wandeln wir nun ab wieder in die dezimale Schreibweise um, so erhalten wir: $ab = 110101011110100110100110000_2 = 560759281_0 = 5678_{10} * 9876_{10}$. Somit haben wir soeben mithilfe des Schönhage-Strassen-Algorithmus das richtige Ergebnis der Multiplikation errechnet.

2.7 Wie genau muss gerechnet werden?

Die Zwischenwerte können nicht auf unendliche Genauigkeit berechnet werden. Es ist also wichtig zu wissen, wie viele Stellen man berechnen muss, damit der daraus resultierende Fehler klein genug ist, dass man immer noch das richtige Ergebnis erhält.

Damit am Ende das richtige Ergebnis ab herauskommt, ist es notwendig, dass die c_s am Ende korrekt sind. Damit diese auf den richtigen Wert gerundet werden (es müssen ja ganze Zahlen herauskommen (das Faltungsprodukt zweier ganzer Zahlen enthält nur ganze Zahlen), bei einer Zahl, die durch den Fehler nicht ganzzahlig ist, wird gerundet), muss der Fehler bei diesen Werten folglich kleiner als $\frac{1}{2}$ sein.

Werte werden durch Näherungswerte ersetzt. Damit es nicht passieren kann, dass $|(\omega^j)'| \leq 1$ nicht gilt ("′" bezeichnet hierbei den Näherungswert) werden, anstatt zu runden, einfach in Richtung 0 die Ziffern nach der benötigten Genauigkeit "abgeschnitten"(truncation). $|(\omega^j)|$ ist eigentlich immer gleich 1, da primitive Einheitswurzeln immer auf dem Einheitskreis der komplexen Ebene liegen. Bei der Berechnung der Schnellen Fourier Transformation gibt es die Berechnung(en)

$$a \leftarrow b + \omega^j c \tag{17}$$

Stattdessen haben wir nun

$$a' \leftarrow b' + (\omega^j)' c' \tag{18}$$

Die anderen Werte werden natürlich ebenfalls durch einen Näherungswert ersetzt und ebenfalls "abgeschnitten", deswegen das "′". Nun schauen wir uns den Fehler, der dabei entsteht, genauer an. Wir benennen die (absoluten) Fehler mit dem Buchstaben δ. Wir schreiben, der Fehler der durch das Ersetzen von b mit einem Näherungswert entsteht (also $|b' - b|$) ist kleiner gleich δ_1, also anders gesagt (bzw. geschrieben):

$$|b' - b| \leq \delta_1 \tag{19}$$

Genauso machen wir das auch für die anderen Teile des Terms, also

$$|(\omega^j)' - \omega^j| \leq \delta_2 \tag{20}$$

und

$$|c' - c| \leq \delta_3 \tag{21}$$

Hätten wir nun

$$a \leftarrow b' + (\omega^j)' c' \tag{22}$$

so wäre der Fehler hier

$$\leq \delta_1 + \delta_2 + \delta_3 \tag{23}$$

Das kann man folgendermaßen berechnen: Bei Multiplikation zweier Näherungswerte $(\omega^j)'$ und c', also $(\omega^j + \delta_2) * (c + \delta_3)$ ergibt sich:

$$\omega^j c + \omega^j \delta_3 + c\delta_2 + \delta_2\delta_3 \tag{24}$$

Das richtige Ergebnis ist $\omega^j c$; der Fehler, der bei der Multiplikation entsteht, ist also

$$\omega^j \delta_3 + c\delta_2 + \delta_2\delta_3 \tag{25}$$

Hierbei fällt $\delta_2\delta_3$ weg, da die Fehler sich in den hinteren Ziffern abspielen. Nach einer Multiplikation ist der Betrag des Produktes kleiner als die Genauigkeit, die wir benutzen, somit fällt dieser Fehlerteil weg. Nun bleibt noch

$$\omega^j \delta_3 + c\delta_2 \tag{26}$$

...

Da ω^j und c beide kleiner gleich 1 sind, gilt:

$$\omega^j \delta_3 + c\delta_2 \leq \delta_2 + \delta_3 \tag{27}$$

Dann wird dieser Näherungswert mit dem Fehler $\delta_2 + \delta_3$ zu einem Näherungswert mit dem Fehler δ_1 addiert, der Fehler addiert sich logischerweise zu

$$\delta_1 + \delta_2 + \delta_3 \tag{28}$$

Da a auch durch die Stellenzahl limitiert ist, fügt sich ein weiterer Fehler hinzu. Diesen nennen wir δ. **Die Anzahl an Stellen (binär), die wir berechnen, nennen wir m.** Der Maximalwert von δ ist dann 2^{-m} für eine reelle Zahl, da a allerdings noch einen komplexen Teil besitzt, wird der Fehler zu $\delta = |2^{-m} + 2^{-m}i|$ Mittels der komplexen Betragsfunktion[9] ergibt sich

$$\delta = 2^{\frac{1}{2}-m} \tag{29}$$

Nun haben wir also

$$|a' - a| < \delta + \delta_1 + \delta_2 + \delta_3 \tag{30}$$

Betrachten wir nun den Näherungswert $(\omega^j)'$ genauer. $(\omega^j)'$ wird mithilfe der im Kapitel **Berechnung von** ω beschriebenen $(\omega_r)'$ berechnet. Diese werden in einer genügend hohen Genauigkeit berechnet, sodass nur der Fehler durch die limitierte Stellenanzahl auftritt, anders gesagt:

$$|(\omega_r)' - \omega_r| < \delta \tag{31}$$

Was bedeutet das nun für den Fehler δ_2? Der Wert von $(\omega^j)'$ wir durch k Multiplikationen von Näherungswerten mit dem Fehler δ gebildet. Dabei entsteht also der Fehler $k\delta$. Allerdings müssen die Ergebnisse der Multiplikationen selbst noch "abgeschnitten" werden, somit wird der Fehler zu $(2k-1)\delta$

Da $\delta_1 = \delta_3$ (b und c werden ja an der gleichen Stelle abgeschnitten), definieren wir

$$\epsilon = \delta_1 = \delta_3 \tag{32}$$

Nach einem Schritt der Schnellen Fourier Transformation war der Fehler $\delta + \delta_1 + \delta_2 + \delta_3$, wir können nun stattdessen schreiben

$$\delta + \delta_1 + \delta_2 + \delta_3 = 2\epsilon + 2k\delta \tag{33}$$

Setzen wir diesen Wert in ϵ des nächsten Schrittes ein, so erhalten wir folgende Liste mit Fehlerfortpflanzung (Bei Schritt 0 gibt es logischerweise keinen Fehler, deswegen ist dort $\epsilon = 0$):

- $2k\delta$
- $6k\delta$
- $14k\delta$
- $30k\delta$
- etc.

Es ist hier schon leicht erkennbar, dass man den Fehler an Schritt j mit $(2^j - 1)2k\delta$ berechnen kann.

...

Da für die Fourier Transformation k Schritte benötigt werden ist der Fehler

$$|(\hat{a}_s)' - \hat{a}_s| < (2^k - 1)2k\delta \tag{34}$$

Dasselbe gilt für $(\hat{b}_s)'$. Nun werden diese beiden Näherungswerte miteinander multipliziert, zusätzlich kommt natürlich noch die Ungenauigkeit des Ergebnisses dazu, also

$$|(\hat{c}_s)' - \hat{c}_s| < 2(2^k - 1)2k\delta + \delta \tag{35}$$

Um bei der doppelten Transformation den Fehler besser berechnen zu können benutzen wir den Fehler $(4k2^k - 2k)\delta$ welcher nur etwas größer ist. Setzt man dies für ϵ ein, so erhält man

$$|(\hat{\hat{c}}_r)' - \hat{\hat{c}}_r| < 2^k(4k2^k - 2k)\delta + (2^k - 1)2k\delta \tag{36}$$

Aus der doppelten Transformierten wird dann noch c'_s errechnet, wobei durch 2^k dividiert wird. Der Fehler ist also bei

$$|c'_r - c_r| < 4k2^k\delta \tag{37}$$

Nun kehren wir zurück zur anfänglichen Idee, und zwar muss $2^{2k+2l}c'_r$ zur richtigen ganzen Zahl runden (hier wird multipliziert, da wir ja am Anfang die Eingangselemente durch 2^{k+l} teilten). So kommen wir darauf, dass

$$\boldsymbol{2^{2k+2l}4k2^k2^{\frac{1}{2}-m} < \frac{1}{2}} \tag{38}$$

Nach Knuth [1] ist dies gegeben, sofern

$$\boldsymbol{k \geq 7} \tag{39}$$

und

$$\boldsymbol{m \geq 4k + 2l} \tag{40}$$

...

3 Der modulare Schönhage-Strassen-Algorithmus

3.1 Rechnen modulo einer Fermat-Zahl

Wie oben schon geschrieben, wird im modularen Schönhage-Strassen-Algorithmus anstatt komplexer Zahlen ein Restklassenring $\mathbb{Z}_{F_n}$ verwendet, mit der Fermatzahl

$$F_n = 2^{2^n} + 1 \tag{41}$$

Ist n z. B. 2, so ist $F_n = 2^{2^2} + 1 = 2^4 + 1 = 16 + 1 = 17$ Die Zahlen in diesem Ring werden als binäre Zahlen mit $\mathbf{2^{n+1}}$ **Ziffern** dargestellt. Wenn wir unser Beispiel fortführen, so wären das dann $2^{n+1} = 2^{2+1} = 2^3 = 8$ Ziffern.

Diese Darstellung ist durch einige Eigenschaften vorteilhaft. Es ist offensichtlich, dass

$$2^{2^n} \equiv -1 \pmod{F_n} \tag{42}$$

(da ja $2^{2^n} + 1 = F_n$). Daraus ergibt sich, dass

$$2^{2^{n+1}} \equiv 1 \pmod{F_n} \tag{43}$$

(hier wurden einfach beide Seiten quadriert).

Schauen wir uns nun an, was das für Konsequenzen für verschiedene Rechenoperationen in dieser Darstellung hat. **Bei einem Überlauf bei der Addition**, d.h. sollte sich ein Übertrag ergeben, der auf die $2^{n+1} + 1$-te Ziffer gehört, so **wird einfach 1 an der ersten Stelle addiert**, da diese Ziffer ja den Wert $2^{2^{n+1}}$ hat und $2^{2^{n+1}} \equiv 1 \pmod{F_n}$. Ein Beispiel: Addieren wir $10101111_2 = 175_{10}$ mit $01100100_2 = 100_{10}$:

$$\begin{array}{rl} & 10101111_2 \\ + & 01100100_2 \\ \hline & \mathbf{1}00010011_2 \end{array}$$

Hier hat nun ein Übertrag statt gefunden, auf die (theoretisch) 9. Ziffer. Wir addieren also einfach 1 dazu, die "9. Stelle" fällt weg:

$$\begin{array}{rl} & 1_2 \\ + & \not{1}00010011_2 \\ \hline & 00010100_2 \end{array}$$

$00010100_2 = 20_{10}$

Überprüfen wir nun die Richtigkeit des Ergebnisses. $175_{10} + 100_{10} = 275_{10}$. $275 \equiv 20 \pmod{F_n}$, denn $20 + 15 * 17 = 275$.

...

Durch die Kongruenz

$$2^{2^n} \equiv -1 \pmod{F_n} \tag{44}$$

kann man bei einer **Subtraktion den Subtrahenden einfach zyklisch um 2^n Stellen verschieben und dann addieren**. Ein Beispiel: Man möchte die im oberen Beispiel schon genutzten Zahlen subtrahieren. Man verschiebt nun den Subtrahenden: Aus 01100100_2 wird $01000110_2 = 70_{10}$. Addiert man die beiden Zahlen, so ergibt sich $175 + 70 = 245$. Überprüfen wir nun das Ergebnis: $175 - 100 = 75$ und $75 \equiv 245 \pmod{F_n}$.

Um **von einer Zahl x dieser Darstellung (d.h. mit 2^{n+1} Ziffern) zum minimalen nicht negativen Rest ξ** zu kommen (d.h. das $\xi \equiv x \pmod{F_n}$ und $0 \leq \xi < F_n$), rechnet man wie folgt: **Man zerlegt die Zahl x** zunächst in unserer Darstellung **in zwei gleich große Stücke u und v** , sodass dann gilt

$$x = u + v * 2^{2^n} \tag{45}$$

Überlegen wir nun, wie sich das machen lässt. Nehmen wir an, $v \leq u$. Wir erinnern uns,

$$2^{2^n} \equiv -1 \pmod{F_n} \tag{46}$$

v ist in der Darstellung von x genau ein vielfaches von 2^{2^n}, somit ist

$$v * 2^{2^n} \equiv v * (-1) \pmod{F_n} \tag{47}$$

u an sich ist ja schon reduziert, da es kleiner als 2^{2^n} sein muss. Folglich können wir schreiben

$$\boldsymbol{\xi = u - v} \tag{48}$$

(wenn $v \leq u$).

Was passiert, wenn $v > u$? Dann hätten wir nach der Berechnung $u - v$ eine negative Zahl! Wir suchen allerdings den kleinsten *nicht* negativen Rest. Also addieren wir einfach noch einmal $F_n = 2^{2^n} + 1$ hinzu (dies können wir machen, da selbstverständlich gilt $F_n \equiv 0 \pmod{F_n}$). Somit ist

$$\boldsymbol{\xi = (u - v) + (2^{2^n} + 1)} \tag{49}$$

(wenn $v > u$).

Hier kann ein Beispiel hilfreich sein: Nehmen wir die obige Zahl $245_{10} = 11110101_2$. Hier haben wir $u = 0101_2 = 5_{10}$ und $v = 1111_2 = 15_{10}$. Hier ist also $v > u$. Somit ist $\xi = (5 - 15) + (2^{2^2} + 1) = -10 + 17 = 7$. Dies ist wirklich der kleinste nicht-negative Rest, denn $7 \equiv 245 \pmod{F_n}$, da $7 + 17 * 14 = 245$, und $7 < F_n$.

...

3.2 Durchführung

Wir haben nun **die zu multiplizierenden Zahlen a und b in Binärdarstellung** vorliegen und möchten das Ergebnis $\boldsymbol{c = ab}$ berechnen. Diese beiden Zahlen haben **je M Ziffern** (in Binärdarstellung - war eine der beiden Zahlen kleiner als die andere, so wird mit Nullen aufgefüllt). Das Produkt ab hat maximal $2M$ Ziffern. Somit kann anstatt in den ganzen Zahlen $\mathbb{Z}$ im Restklassenring $\mathbb{Z}_{F_m}$ gerechnet werden, wenn m groß genug ist. Wie groß muss m also sein? Die grösste Zahl, die mit $2M$ Ziffern erreicht werden kann ist $2^{2M}-1$. Somit muss $F_m = 2^{2^m}+1$ größer sein. Dies ist sicher gegeben, wenn $2^{2^m} > 2^{2M}$. Logarithmieren wir mit dem Duallogarithmus, so erhalten wir, dass $2^m > 2M$. Wenn wir noch einmal Logarithmieren, so **wählen wir $\boldsymbol{m}$ die kleinste ganze Zahl**

$$\boldsymbol{m > log_2(2M)} \tag{50}$$

Machen wir an dieser Stelle ein Beispiel: Wir nehmen zwei Zahlen mit je 3 Ziffern, und zwar $a = 010_2$ und $b = 110_2$. Somit ist $M = 3$. Berechnen wir nun m: $m > log_2(2M)$ und $m > log_2(2*3)$, somit ist $m > log_2(6)$ und $m > 2,585...$, somit wählen wir $m = 3$.

Bei dem modularen Schönhage-Strassen-Algorithmus gibt es einen **Unterschied in der Durchführung zwischen geraden und ungeraden m. Wir werden zunächst den ungeraden Fall behandeln.** Wir wählen ein n, sodass $m = 2n - 1$. Somit errechnet sich n durch

$$\boldsymbol{n = (m + 1)/2} \tag{51}$$

. In unserem Beispiel ist das $n = (m + 1)/2 = (3 + 1)/2 = 4/2 = 2$.

Im geraden Fall haben wir $m = 2n - 2$. Dort ist die Anzahl der Stücke (wir werden a und b im nächsten Absatz zerlegen) anders, was sich dann auf die Fourier-Transformation etc. auswirkt. Die Unterschiede werden unten in einem eigenen Unterkapitel erläutert

Wie oben haben wir die **Zahlen a und b als 2^{m+1} stellige binäre Zahlen** vorliegen. Wir **teilen sie in Abschnitte mit jeweils 2^{n-1} Ziffern** (das sind dann 2^{n+1} Abschnitte). a_0 enthält dann die Ziffern 0 bis $(2^{n-1} - 1)$. Somit ist dann

$$a = \sum_{i=0}^{2^{n+1}-1} a_i 2^{i2^{n-1}} \tag{52}$$

(wobei dann gilt: $0 \leq a_i < 2^{2^{n-1}}$) und entsprechend für b. Hier wird mit $2^{i2^{n-1}}$ multipliziert, da a_i ja um i "a"s verschoben werden muss, welche jeweils 2^{n-1} Bits besitzen, um das originale a wieder zusammenzusetzen.

Führen wir nun unser Beispiel von oben fort: Wir teilen $a = 010_2$ und $b = 110_2$ (die wir als $2^{m+1} = 16$-Stellige Dualzahlen darstellen, also $a = 0...010_2$ und $b = 0...110_2$) in $2^{n+1} = 2^3 = 8$ Abschnitte mit jeweils $2^{n-1} = 2^1 = 2$ Ziffern, somit haben wir:

r	a_r	b_r
0	10_2	10_2
1	00_2	01_2
2	00_2	00_2
3	00_2	00_2
4	00_2	00_2
5	00_2	00_2
6	00_2	00_2
7	00_2	00_2

Machen wir ein Beispiel zu Multiplikation mithilfe des modularen Schönhage-Strassen-Algorithmus. Wir möchten die Zahlen $a = 11830_{10} = 10111000110110_2$ und $b = 8955_{10} = 10001011111011_2$ multiplizieren. Beide Zahlen haben 14 Ziffern, somit ist $M = 14$. Nun müssen wir m herausfinden. $m > log_2(2M)$, also $m > log_2(28)$ und somit $m > 4,81...$ Die kleinste ganze Zahl m auf die dies zutrifft ist $m = 5$.

Wir multiplizieren also in $\mathbb{Z}_{F_m}$, wobei $F_m = 2^{2^m} + 1 = 2^{2^5} + 1 = 2^{32} + 1 = 4294967297_{10}$. $m = 5$, also ungerade. $n = (m + 1)/2 = (5 + 1)/2 = 6/2 = 3$. Wir verlängern nun die Darstellung der Zahlen a und b auf $2^{m+1} = 2^{5+1} = 2^6 = 64$ Ziffern und teilen sie in Abschnitte zu $2^{n-1} = 2^{3-1} = 2^2 = 4$ Ziffern (das sind dann $2^{n+1} = 2^{3+1} = 2^4 = 16$ Stücke):
$a = ...|0000|0010|1110|0011|0110_2$
$b = ...|0000|0010|0010|1111|1011_2$
Somit haben wir:

- $a_0 = 0110_2$
- $a_1 = 0011_2$
- $a_2 = 1110_2$
- $a_3 = 0010_2$
- $a_4 = 0000_2$
- ...
- $a_{15} = 0000_2$

und:

- $b_0 = 1011_2$
- $b_1 = 1111_2$
- $b_2 = 0010_2$
- $b_3 = 0010_2$
- $b_4 = 0000_2$
- ...
- $b_{15} = 0000_2$

Durch das Faltungstheorem wissen wir, dass wir, wenn wir

$$c_r = \sum_{i+j \equiv r (mod 2^{n+1})} a_i b_j \tag{53}$$

haben (wobei $0 \leq i, j < 2^{n+1}$), auch das Produkt $c = ab$ ausrechnen können:

$$c \equiv \sum_{r=0}^{2^{n+1}-1} c_r 2^{r 2^{n-1}} \pmod{F_m} \tag{54}$$

Siehe dazu das Kapitel über das Faltungsprodukt.

Allerdings ist $2^{2^n 2^{n-1}} = 2^{2^{2n-1}}$. Wir hatten auch oben definiert: $m = 2n - 1$. Somit ist

$$2^{2^{2n-1}} = 2^{2^m} \tag{55}$$

und

$$2^{2^m} \equiv -1 \pmod{F_m} \tag{56}$$

Haben wir $2^{(2^n+x)2^{n-1}}$, so wird daraus

$$2^{(2^n+x)2^{n-1}} = 2^{2^{2n-1}+x2^{n-1}} = 2^{2^m} 2^{x2^{n-1}} \tag{57}$$

Wenden wir die obige Erkenntnis an, so erhalten wir

$$2^{2^m} 2^{x2^{n-1}} \equiv -2^{x2^{n-1}} \pmod{F_m} \tag{58}$$

Indem wir dies ausnutzen, können wir die Summenformel umschreiben:

$$c \equiv \sum_{r=0}^{2^n-1} (c_r - c_{r+2^n}) 2^{r 2^{n-1}} \pmod{F_m} \tag{59}$$

Was haben wir hier gemacht? Sobald $r \geq 2^n$, können wir schreiben $r = 2^n + x$. Somit haben wir dann als Produkt:

$$c_r 2^{(2^n+x)2^{n-1}} \tag{60}$$

Das kommt uns bekannt vor. Wir können also schreiben:

$$c_r 2^{(2^n+x)2^{n-1}} \equiv c_r (-1) 2^{x2^{n-1}} \pmod{F_m} \tag{61}$$

Dies haben wir benutzt und konnten so immer zwei Summanden zusammenfassen, wobei der, bei dem Index $\geq 2^n$, einfach negativ wird. Auf den ersten Blick scheint dies keinen Sinn zu machen, allerdings werden wir später sehen, dass diese Umschreibung uns einen Schritt spart.

Um diese Formel etwas übersichtlicher zu gestalten, führen wir z ein, welches definiert ist durch:

$$z_j = c_j - c_{j+2^n} \tag{62}$$

für $0 \leq j < 2^n$

...

...und schreiben dann:

$$\boldsymbol{c \equiv \sum_{r=0}^{2^{n+1}-1} z_r 2^{r 2^{n-1}} \pmod{F_m}} \tag{63}$$

Nun brauchen wir noch ein anderes Hilfsmittel. Später wird uns von Nutzen sein,wenn wir **mit vorgegebenen Zahlen ξ und η, die Zahl x berechnen können, sodass**

$$\boldsymbol{x \equiv \xi \pmod{F_n}, 0 \leq \xi < 2^{2^n} + 1} \tag{64}$$

$$\boldsymbol{x \equiv \eta \pmod{2^{n+2}}, 0 \leq \eta < 2^{n+2}} \tag{65}$$

wobei $0 \leq x < 2^{n+2} F_n$

Dies wird uns dann bei der Berechnung der z_j nutzen. Wichtig ist hier, dass 2^{n+2} und F_n teilerfremd sind. So kann man x folgendermaßen berechnen: Zuerst berechnet man

$$\boldsymbol{\delta \equiv \eta - \xi \pmod{2^{n+2}}} \tag{66}$$

(mit $0 \leq \delta < 2^{n+2}$) , woraufhin dann x berechnet werden kann:

$$\boldsymbol{x = \xi + \delta(F_n)} \tag{67}$$

.

Überlegen wir uns nun, woher diese Formel kommt. Sie basiert auf dem Chinesischen Restsatz (siehe Glossar), welcher hier nicht beschrieben werden kann. Ich beschreibe allerdings für Interessierte, wie man vom Chinesischen Restsatz auf diese Formel kommt.

Ausgehend von der obigen simultanen Kongruenz, hat man beim Chinesischen Restsatz:

$$N_1 = (F_n * 2^{n+2})/F_n = 2^{n+2} \tag{68}$$

und

$$N_1 = (F_n * 2^{n+2})/2^{n+2} = F_n \tag{69}$$

Man braucht die Lösungen x_1 und x_2 der folgenden Kongruenzen:

$$N_1 x_1 \equiv 1 \pmod{F_n} \tag{70}$$

$$N_2 x_2 \equiv 1 \pmod{2^{n+2}} \tag{71}$$

Setzen wir N_1 und N_2 ein, so erhalten wir:

$$2^{n+2} x_1 \equiv 1 \pmod{F_n} \tag{72}$$

$$F_n x_2 \equiv 1 \pmod{2^{n+2}} \tag{73}$$

2^{2^n} ist bei $n \geq 2$ immer ein Vielfaches von 2^{n+2}, also:

$$2^{n+2} x_1 \equiv 1 \pmod{F_n} \tag{74}$$

$$F_n * 1 \equiv 1 \pmod{2^{n+2}} \tag{75}$$

Somit ist $x_2 = 1$.

Wählen wir $x_1 = -\frac{2^{2^n}}{2^{n+2}}$, so ist auch die erste Kongruenz erfüllt, da $\cancel{2^{n+2}} * (-\frac{2^{2^n}}{\cancel{2^{n+2}}}) = -2^{2^n} \equiv 1 \pmod{F_n}$

...

Somit haben wir also

$$x_1 = -\frac{2^{2^n}}{2^{n+2}} \tag{76}$$

und

$$x_2 = 1 \tag{77}$$

Somit berechnen wir nach dem Chinesischen Restsatz:

$$x = \xi N_1 x_1 + \eta N_2 x_2 \tag{78}$$

Setzten wir die entsprechenden Werte ein, so erhalten wir:

$$x = \xi \cancel{2^{n+2}}(-\frac{2^{2^n}}{\cancel{2^{n+2}}}) + \eta F_n 1 \tag{79}$$

Somit erhält man:

$$x = -2^{2^n}\xi + F_n\eta \tag{80}$$

Dies ist dann:

$$x = (2^{2^n} + 1)\eta - 2^{2^n}\xi \tag{81}$$

Formen wir etwas um (es wir einfach ein ξ zuviel abgezogen und dafür hinterher wieder hinzugefügt):

$$x = (2^{2^n} + 1)\eta - (2^{2^n} + 1)\xi + \xi \tag{82}$$

Klammern wir nun $F_n = 2^{2^n} + 1$ aus:

$$x = F_n(\eta - \xi) + \xi \tag{83}$$

Den Ausdruck in Klammern kann man auch vorher schon $\mod 2^{n+2}$ reduziert werden, da der Ausdruck ja mit F_n multipliziert wird.

Hier kann ein Beispiel hilfreich sein. Wir haben $n = 2$ (somit ist $F_n = 2^{2^n} + 1 = 2^4 + 1 = 17$ und $2^{n+2} = 2^4 = 16$) und es sei $\xi = 3$ und $\eta = 13$. Also berechnen wir $\delta \equiv 13 - 3 \pmod{2^{n+2}}$. Wir haben also $\delta = 10$ und berechnen somit $x = \xi + \delta(F_n) = 3 + 10F_n = 3 + 10 * 17 = 3 + 170 = 173$. Überprüfen wir nun das Ergebnis: $173 \equiv 3 \pmod{17}$, da $173 - 17 * 10 = 3$ und $173 \equiv 13 \pmod{16}$, da $173 - 16 * 10 = 13$.

Wenn wir uns dies zunutze machen, müssen wir die z_j nicht direkt $\mod F_m$ *berechnen, sondern berechnen zunächst einfach*

$$z_j \mod 2^{n+2} \tag{84}$$

und

$$z_j \mod F_n \tag{85}$$

Die z_j berechnen wir dann wie eben beschrieben.

...

3.3 Berechnung der $z_j \mod 2^{n+2}$

Zunächst **reduzieren** wir die **a's und b's** , sodass

$$\boldsymbol{\alpha_i \equiv a_i \pmod{2^{n+2}}} \tag{86}$$

und

$$\boldsymbol{\beta_i \equiv b_i \pmod{2^{n+2}}} \tag{87}$$

Dazu **schneiden wir von ihnen einfach die rechten $n+2$ Ziffern ab** , sie sind das reduzierte a bzw. b. Alle anderen Ziffern sind nur Vielfache von 2^{n+2} und es gilt natürlich:

$$x2^{n+2} \equiv 0 \pmod{2^{n+2}} \tag{88}$$

für alle ganzen x und natürlichen n. Dann **setzen wir** aus diesen Werten **die Zahlen u und v zusammen** , und zwar so, dass **jedes α (bzw. β) $3n+5$ Ziffern bekommt** (So werden sich die einzelnen Teilstücke beim Produkt uv sicher nicht überlappen) **:**

$$u = \sum_{l=0}^{2^{n+1}-1} \alpha_l 2^{l(3n+5)} \tag{89}$$

$$v = \sum_{l=0}^{2^{n+1}-1} \beta_l 2^{l(3n+5)} \tag{90}$$

Warum genau $3n+5$ Ziffern? Die einzelnen Elemente haben ursprünglich $n+2$ Ziffern, und wir haben davon 2^{n+1} Stück. Jedes "Element" des Produktes ist also maximal eine Summe aus 2^{n+1} Produkten von zwei Zahlen zu je $n+2$ Ziffern. Diese Produkte habem maximal $2*(n+2) = 2n+4$ Ziffern. Wir addieren 2^{n+1} mal solche Zahlen. Die maximale Anzahl an Überträgen ist im Binärsystem dann $log_2(2^{n+1}) = n+1$. Somit ist die maximale Anzahl an Ziffern hier $(n+1)+(2n+4) = 3n+5$.

Das Produkt **uv teilen wir dann wieder in Stücke zu je $3n+5$ Ziffern** und **nennen diese Stücke γ_r.** Man kann erkennen, dass durch die Multiplikation folgendes gilt (siehe dazu auch den Abschnitt zum Faltungsprodukt):

$$\gamma_r = \sum_{i+j=r} \alpha_i \beta_j \tag{91}$$

Wir erinnern uns an die Definition oben:

$$c_r = \sum_{i+j \equiv r (mod 2^{n+1})} a_i b_j \tag{92}$$

Also haben wir hier

$$c_r \equiv \gamma_r + \gamma_{r+2^{n+1}} \pmod{2^{n+2}} \tag{93}$$

Die γ_r und $\gamma_{r+2^{n+1}}$ decken alle Kombinationen von α_j und β_j nach der obigen Definition von c_r ab. Nun haben wir also die

$$c_r \mod 2^{n+2} \tag{94}$$

berechnet. Wir brauchen allerdings die z_j, welche definiert waren durch:

$$z_j = c_j - c_{j+2^n} \tag{95}$$

Nun brauchen wir die z_j, und zwar $\mod 2^{n+2}$ und $\mod F_n$. Beginnen wir mit $\mod 2^{n+2}$: Wir reduzieren zunächst die a_j und b_j $\mod 2^{n+2} = 2^{3+2} = 2^5 = 32$ um die α_j und β_j zu bekommen. Allerdings sind hier die a_j und b_j schon reduziert, da sie als Maximalwert $2^{2^{n-1}} - 1 = 15$ haben. Ansonsten würden wir, wie oben beschrieben, die entsprechenden Ziffern einfach abschneiden. Jetzt setzen wir die Zahlen u und v zusammen, jedes Stück bekommt $3n + 5 = 3 * 3 + 5 = 9 + 5 = 14$ Ziffern, also:
$u = ...|00000000000010|00000000001110|00000000000011|00000000000110$
$v = ...|00000000000010|00000000000010|00000000001111|00000000001011$
Wir berechnen das Produkt, es ist:
$uv = 100|00000000100000|00000001000000|00000011111010$
$|\quad 00000011010011|00000001111011|00000001000010$

Wir haben also:

$\gamma_0 = 00000001000010_2 = 66_{10}$
$\gamma_1 = 00000001111011_2 = 123_{10}$
$\gamma_2 = 00000011010011_2 = 211_{10}$
$\gamma_3 = 00000011111010_2 = 250_{10}$
...

$\gamma_4 = 00000001000000_2 = 64_{10}$
$\gamma_5 = 00000000100000_2 = 32_{10}$
$\gamma_6 = 00000000000100_2 = 4_{10}$
$\gamma_7 = 00000000000000_2 = 0_{10}$

Wir können somit definieren: $z_j \equiv c_j - c_{j+2^n} \pmod{2^{n+2}}$ und durch Einsetzen:

$$z_j \equiv \gamma_j + \gamma_{j+2^{n+1}} - (\gamma_{j+2^n} + \gamma_{j+2^n+2^{n+1}}) \pmod{2^{n+2}} \tag{96}$$

durch Umformen erhalten wir:

$$\boldsymbol{z_j \equiv \gamma_j + \gamma_{j+2*2^n} - \gamma_{j+2^n} - \gamma_{j+3*2^n} \pmod{2^{n+2}}} \tag{97}$$

Dies muss dann noch reduziert werden, wobei wir wie oben vorgehen (einfach die Ziffern abschneiden). Somit brauchen wir nur noch die $z_j \mod F_n$.

Rechnen wir nun die z_j für $0 \leq j < 2^n$ aus ($2^n = 2^3 = 8$):

$z_0 \equiv \gamma_0 + \gamma_{16} - \gamma_8 - \gamma_{24} = 66 + 0 - 0 - 0 = 66 \pmod{2^{n+2}}$
$z_1 \equiv \gamma_1 + \gamma_{17} - \gamma_9 - \gamma_{25} = 123 + 0 - 0 - 0 = 123 \pmod{2^{n+2}}$
$z_2 \equiv \gamma_2 + \gamma_{18} - \gamma_{10} - \gamma_{26} = 211 + 0 - 0 - 0 = 211 \pmod{2^{n+2}}$
$z_3 \equiv \gamma_3 + \gamma_{19} - \gamma_{11} - \gamma_{27} = 250 + 0 - 0 - 0 = 250 \pmod{2^{n+2}}$
$z_4 \equiv \gamma_4 + \gamma_{20} - \gamma_{12} - \gamma_{28} = 64 + 0 - 0 - 0 = 64 \pmod{2^{n+2}}$
$z_5 \equiv \gamma_5 + \gamma_{21} - \gamma_{13} - \gamma_{29} = 32 + 0 - 0 - 0 = 32 \pmod{2^{n+2}}$
$z_6 \equiv \gamma_6 + \gamma_{22} - \gamma_{14} - \gamma_{30} = 4 + 0 - 0 - 0 = 4 \pmod{2^{n+2}}$
$z_7 \equiv \gamma_7 + \gamma_{23} - \gamma_{15} - \gamma_{31} = 0 + 0 - 0 - 0 = 0 \pmod{2^{n+2}}$

Diese z_j müssen noch um $\mod 2^{n+2} = 2^5 = 32$ reduziert werden (d.h. die rechten 5 Ziffern abschneiden und alle anderen Ziffern verwerfen). So erhalten wir:
$z_0 \equiv 66 = \cancel{0000000}1000010_2 \equiv 00010_2 = 2 \pmod{2^{n+2}}$
$z_1 \equiv 123 = \cancel{0000000}1111011_2 \equiv 11011_2 = 27 \pmod{2^{n+2}}$
$z_2 \equiv 211 = \cancel{0000000}1110011_2 \equiv 10011_2 = 19 \pmod{2^{n+2}}$
$z_3 \equiv 250 = \cancel{0000000}1111010_2 \equiv 11010_2 = 26 \pmod{2^{n+2}}$
$z_4 \equiv 64 = \cancel{0000000}1000000_2 \equiv 00000_2 = 0 \pmod{2^{n+2}}$
$z_5 \equiv 32 = \cancel{0000000}1000000_2 \equiv 00000_2 = 0 \pmod{2^{n+2}}$
$z_6 \equiv 4 = \cancel{0000000}0000100_2 \equiv 00100_2 = 4 \pmod{2^{n+2}}$
$z_7 \equiv 0 = \cancel{0000000}0000000_2 \equiv 00000_2 = 0 \pmod{2^{n+2}}$

3.4 Berechnung der $z_j \mod F_n$

Hier benutzen wir nun die Fouriertransformation, wobei wir **im Restklassenring $\mathbb{Z}_{F_n}$ rechnen** werden (siehe dazu die Bemerkungen zur Addition, Subtraktion etc. oben). Zunächst berechnen wir mithilfe der schnellen Fourier Transformation **$\hat{a}_k$ und $\hat{b}_k$** , sodass wir dann

$$\hat{c}_k \equiv \hat{a}_k \hat{b}_k \pmod{F_n} \tag{98}$$

errechnen können. Bei diesen Fourier-Transformationen benutzen wir als **$\omega = 2$** . Die Zahl 2 besitzt hier alle benötigten Eigenschaften,

$$2^{2^{(n+1)}} \equiv 1 \pmod{F_n} \tag{99}$$

und

$$2^{2^{(n+1)-1}} \equiv -1 \pmod{F_n} \tag{100}$$

Anstatt mit $\omega^x = 2^x$ zu multiplizieren, können wir einfach einen zyklischen Shift um x Stellen nach links ausführen. Um $z_j \mod F_n$ zu bekommen, brauchen wir

$$c_j - c_{j+2^n} \mod F_n \tag{101}$$

Das $A^{[1]}(1, ...)$ liefert allerdings schon ein

$$c_j - c_{j+2^n} \tag{102}$$

Warum dies so ist werden wir unten im entsprechenden Kapitel sehen Somit müssen wir nicht bis $A^{[0]}$ zurückrechnen. Nachdem wir nun also die

$$\hat{c}_k \mod F_n \tag{103}$$

errechnet haben (nur für ungerade k, siehe oben) , machen wir die **inverse Fourier Transformation zurück bis $A^{[1]}$ (nur für $A^{[v](1,...)}$** , dies alles wird dann unten deutlich - bei der Fourier Transformation zu $\hat{a}_k$ natürlich auch nur für $A^{[v](1,...)}$). **Die Ergebnisse reduzieren wir $\mod F_n$ - und haben unser $z \mod F_n$**

Nun können wir die **z_j aus**

$$z_j \mod 2^{n+2} \tag{104}$$

und

$$z_j \mod F_n \tag{105}$$

berechnen, und mit diesen dann auch das Produkt $c = ab$.

...

3.5 Die Schnelle Fourier Transformation

Wir hatten die schnelle Fourier Transformation schon beim komplexen Schönhage-Strassen-Algorithmus angesprochen. Da wir 2^{n+1} Abschnitte (a_j) haben und somit bis $A^{[n+1]}$ rechnen müssen, benutzen wir hier $(n+1)$ anstatt k.
Wir gehen aus von

$$A^{[0]}(t_0, ..t_{(n+1)-1}) \leftarrow a_t \tag{106}$$

wobei $t = (t_0...t_{(n+1)-1})_2$
Wir benutzen hier etwas umgeformte Formeln:

$A^{[v+1]}(..., s_{v-1}, s_v, t_{v+1}, ...) \leftarrow$
$A^{[v]}(..., s_{v-1}, 0, t_{v+1}, ...) + A^{[v]}(..., s_{v-1}, 1, t_{v+1}, ...) * \omega^{2^{(n+1)-1-v}(s_v 2^v s_{(v-1)} 2^{v-1} ... s_0 2^0)}$

Wir fordern, dass

$$\omega^{2^{(n+1)-1}} \equiv -1 \pmod{F_n} \tag{107}$$

und

$$\omega^{2^{(n+1)}} \equiv 1 \pmod{F_n} \tag{108}$$

Da allerdings, wenn $s_v = 1$, auch:

$$2^{(n+1)-1-v} * 2^v = 2^{(n+1)-1-v+v} = 2^{n-1} \tag{109}$$

Hier haben wir die erste Potenz im Exponenten von ω mit dem ersten Teil der Klammer, also $s_v 2^v$ multipliziert.

Nimmt man dies als Exponenten von ω, so haben wir:

$$2^{2^{(n+1)-1}} \equiv -1 \pmod{F_n} \tag{110}$$

Somit können wir schreiben (hierbei fällt bei $s_v = 1$ eben s_v heraus und dafür wird das zweite $A^{[v]}$ negativ):
$A^{[v+1]}(..., s_{v-1}, 0, t_{v+1}, ...) \leftarrow$
$A^{[v]}(..., s_{v-1}, 0, t_{v+1}, ...) + A^{[v]}(..., s_{v-1}, 1, t_{v+1}, ...) * \omega^{2^{(n+1)-1-v}(s_{(v-1)} 2^{v-1} ... s_0 2^0)}$
$A^{[v+1]}(..., s_{v-1}, 1, t_{v+1}, ...) \leftarrow$
$A^{[v]}(..., s_{v-1}, 0, t_{v+1}, ...) - A^{[v]}(..., s_{v-1}, 1, t_{v+1}, ...) * \omega^{2^{(n+1)-1-v}(s_{(v-1)} 2^{v)-1} ... s_0 2^0)}$
um das ganze übersichtlicher zu gestalten, definieren wir
$\boldsymbol{x = 2^{(n+1)-1-v}(s_{(v-1)} 2^{v-1} ... s_0 2^0)}$ **sodass**
$\boldsymbol{A^{[v+1]}(..., s_{v-1}, 0, t_{v+1}, ...) \leftarrow A^{[v]}(..., s_{v-1}, 0, t_{v+1}, ...) + A^{[v]}(..., s_{v-1}, 1, t_{v+1}, ...)\omega^x}$
$\boldsymbol{A^{[v+1]}(..., s_{v-1}, 1, t_{v+1}, ...) \leftarrow A^{[v]}(..., s_{v-1}, 0, t_{v+1}, ...) - A^{[v]}(..., s_{v-1}, 1, t_{v+1}, ...)\omega^x}$
und wir haben dann

$$\boldsymbol{\hat{a}_s = A^{[(n+1)]}(s_0, s_1, ..., s_{(n+1)-1})} \tag{111}$$

wobei $\boldsymbol{s = (s_{(n+1)-1} ... s_1 s_0)_2}$

Später werden wir sehen, dass wir nur die $\hat{a}_j$ mit ungeradem j benötigen. Um diese zu erhalten werden nur die $A^{[k]}(1, ...)$ bei $k \geq 1$ gebraucht.

Nun benötigen wir noch die $z_j \mod F_n$. Dafür benötigen wir die Fourier-Transformierte, wobei wir allerdings nur $A^{[v]}(1,...)$ brauchen.

Stellen wir zunächst die a_j und b_j mit $2^{n+1} = 2^{3+1} = 2^4 = 16$ Ziffern dar, damit wir dann wie oben beschrieben rechnen können. Wir haben also:

$a_0 = 0000000000000110_2$ $\quad$ $b_0 = 0000000000001011_2$
$a_1 = 0000000000000011_2$ $\quad$ $b_1 = 0000000000001111_2$
$a_2 = 0000000000001110_2$ $\quad$ $b_2 = 0000000000000010_2$
$a_3 = 0000000000000010_2$ $\quad$ $b_3 = 0000000000000010_2$
$a_4 = 0000000000000000_2$ $\quad$ $b_4 = 0000000000000000_2$
... $\quad$ ...
$a_{15} = 0000000000000000_2$ $\quad$ $b_{15} = 0000000000000000_2$

Da m ungerade ist, benutzen wir $\omega = 2$. Beginnen wir zunächst mit der Fourier-Transformation für a_j:

Der erste Schritt ist einfach:

$A^{[0]}(0,0,0,0) = a_0 = 0000000000000110_2$ $\quad$ $A^{[0]}(1,0,0,0) = a_8 = 0000000000000000_2$
$A^{[0]}(0,0,0,1) = a_1 = 0000000000000011_2$ $\quad$ $A^{[0]}(1,0,0,1) = a_9 = 0000000000000000_2$
$A^{[0]}(0,0,1,0) = a_2 = 0000000000001110_2$ $\quad$ $A^{[0]}(1,0,1,0) = a_10 = 0000000000000000_2$
$A^{[0]}(0,0,1,1) = a_3 = 0000000000000010_2$ $\quad$ $A^{[0]}(1,0,1,1) = a_11 = 0000000000000000_2$
$A^{[0]}(0,1,0,0) = a_4 = 0000000000000000_2$ $\quad$ $A^{[0]}(1,1,0,0) = a_12 = 0000000000000000_2$
$A^{[0]}(0,1,0,1) = a_5 = 0000000000000000_2$ $\quad$ $A^{[0]}(1,1,0,1) = a_13 = 0000000000000000_2$
$A^{[0]}(0,1,1,0) = a_6 = 0000000000000000_2$ $\quad$ $A^{[0]}(1,1,1,0) = a_14 = 0000000000000000_2$
$A^{[0]}(0,1,1,1) = a_7 = 0000000000000000_2$ $\quad$ $A^{[0]}(1,1,1,1) = a_15 = 0000000000000000_2$

Beginnen wir mit dem zweiten Schritt (da wir hier bei $A^{[1]}$ sind, brauchen wir nur die Werte für $A^{[1]}(1,...)$):

$A^{[1]}(1,0,0,0) \leftarrow A^{[0]}(0,0,0,0) - A^{[0]}(1,0,0,0)\omega^x$
$A^{[1]}(1,1,0,0) \leftarrow A^{[0]}(0,1,0,0) - A^{[0]}(1,1,0,0)\omega^x$
$A^{[1]}(1,0,0,1) \leftarrow A^{[0]}(0,0,0,1) - A^{[0]}(1,0,0,1)\omega^x$
$A^{[1]}(1,1,0,1) \leftarrow A^{[0]}(0,1,0,1) - A^{[0]}(1,1,0,1)\omega^x$
$A^{[1]}(1,0,1,0) \leftarrow A^{[0]}(0,0,1,0) - A^{[0]}(1,0,1,0)\omega^x$
$A^{[1]}(1,1,1,0) \leftarrow A^{[0]}(0,1,1,0) - A^{[0]}(1,1,1,0)\omega^x$
$A^{[1]}(1,0,1,1) \leftarrow A^{[0]}(0,0,1,1) - A^{[0]}(1,0,1,1)\omega^x$
$A^{[1]}(1,1,1,1) \leftarrow A^{[0]}(0,1,1,1) - A^{[0]}(1,1,1,1)\omega^x$

Da wir hier $v = 0$ haben, ist hier $x = 2^{(n+1)-1-v}(s_{(n+1)-1}2^{(n+1)-1} + ... + s_0) = 2^{4-1-0}(s_3 2^3 + s_2 2^2 + s_1 2 + s_0) = 2^3(s_3 2^3 + s_2 2^2 + s_1 2 + s_0) = 8(s_3 + 2^3 s_2 2^2 + s_1 2 + s_0)$. Allerdings haben wir in den Klammern nur t und keine s (das größte s wäre s_{-1} was natürlich Unsinn ist - siehe zu den s und t auch links die Beschreibung). Somit bleibt $x = 0$

Nun führen wir den zweiten Schritt fort:

$A^{[1]}(1,0,0,0) \leftarrow 0000000000000110_2 - 0000000000000000_2\omega^0$
$A^{[1]}(1,0,0,1) \leftarrow 0000000000000011_2 - 0000000000000000_2\omega^0$
$A^{[1]}(1,0,1,0) \leftarrow 0000000000001110_2 - 0000000000000000_2\omega^0$
$A^{[1]}(1,0,1,1) \leftarrow 0000000000000010_2 - 0000000000000000_2\omega^0$
$A^{[1]}(1,1,0,0) \leftarrow 0000000000000000_2 - 0000000000000000_2\omega^0$
$A^{[1]}(1,1,0,1) \leftarrow 0000000000000000_2 - 0000000000000000_2\omega^0$
$A^{[1]}(1,1,1,0) \leftarrow 0000000000000000_2 - 0000000000000000_2\omega^0$
$A^{[1]}(1,1,1,1) \leftarrow 0000000000000000_2 - 0000000000000000_2\omega^0$

Nun können wir die Werte berechnen:

$A^{[1]}(1,0,0,0) \leftarrow 0000000000000110_2$ $\quad$ $A^{[1]}(1,1,0,0) \leftarrow 0000000000000000_2$
$A^{[1]}(1,0,0,1) \leftarrow 0000000000000011_2$ $\quad$ $A^{[1]}(1,1,0,1) \leftarrow 0000000000000000_2$
$A^{[1]}(1,0,1,0) \leftarrow 0000000000001110_2$ $\quad$ $A^{[1]}(1,1,1,0) \leftarrow 0000000000000000_2$
$A^{[1]}(1,0,1,1) \leftarrow 0000000000000010_2$ $\quad$ $A^{[1]}(1,1,1,1) \leftarrow 0000000000000000_2$

...

Machen wir nun den dritten Schritt:

$$
\begin{aligned}
A^{[2]}(1,0,0,0) &\leftarrow A^{[1]}(1,0,0,0) + A^{[1]}(1,1,0,0)\omega^x \\
A^{[2]}(1,0,0,1) &\leftarrow A^{[1]}(1,0,0,1) + A^{[1]}(1,1,0,1)\omega^x \\
A^{[2]}(1,0,1,0) &\leftarrow A^{[1]}(1,0,1,0) + A^{[1]}(1,1,1,0)\omega^x \\
A^{[2]}(1,0,1,1) &\leftarrow A^{[1]}(1,0,1,1) + A^{[1]}(1,1,1,1)\omega^x \\
A^{[2]}(1,1,0,0) &\leftarrow A^{[1]}(1,0,0,0) - A^{[1]}(1,1,0,0)\omega^x \\
A^{[2]}(1,1,0,1) &\leftarrow A^{[1]}(1,0,0,1) - A^{[1]}(1,1,0,1)\omega^x \\
A^{[2]}(1,1,1,0) &\leftarrow A^{[1]}(1,0,1,0) - A^{[1]}(1,1,1,0)\omega^x \\
A^{[2]}(1,1,1,1) &\leftarrow A^{[1]}(1,0,1,1) - A^{[1]}(1,1,1,1)\omega^x
\end{aligned}
$$

Hier ist $v = 1$, und so haben wir ein x, nämlich $x = 2^{(n+1)-1-v}(s_{(n+1)-1}2^{(n+1)-1}...s_0) = 2^{4-1-1}(s_3 2^3 + s_2 2^2 + s_1 2 + s_0) = 2^2(...) = 4(s_3 2^3 + s_2 2^2 + s_1 2 + s_0)$. Wir haben ein s_0, und so ist $x = 4(s_0)$. s_0 ist immer 1, da wir andere Werte nicht berechnen müssen (s_0 ist ja die Ziffer ganz links - siehe dazu auch oben), und so ist $x = 4$, d.h. wir machen einen zyklischen Shift um vier Stellen nach links. Da die fraglichen Zahlen allerdings alle 0 sind, verändert der Shift hier nichts.

Wir haben dann:

$$
\begin{aligned}
A^{[2]}(1,0,0,0) &\leftarrow 0000000000000110_2 + 0000000000000000_2\omega^4 \\
A^{[2]}(1,0,0,1) &\leftarrow 0000000000000011_2 + 0000000000000000_2\omega^4 \\
A^{[2]}(1,0,1,0) &\leftarrow 0000000000001110_2 + 0000000000000000_2\omega^4 \\
A^{[2]}(1,0,1,1) &\leftarrow 0000000000000010_2 + 0000000000000000_2\omega^4 \\
A^{[2]}(1,1,0,0) &\leftarrow 0000000000000110_2 - 0000000000000000_2\omega^4 \\
A^{[2]}(1,1,0,1) &\leftarrow 0000000000000011_2 - 0000000000000000_2\omega^4 \\
A^{[2]}(1,1,1,0) &\leftarrow 0000000000001110_2 - 0000000000000000_2\omega^4 \\
A^{[2]}(1,1,1,1) &\leftarrow 0000000000000010_2 - 0000000000000000_2\omega^4
\end{aligned}
$$

Und wir erhalten:

$$
\begin{aligned}
A^{[2]}(1,0,0,0) &\leftarrow 0000000000000110_2 & A^{[2]}(1,1,0,0) &\leftarrow 0000000000000110_2 \\
A^{[2]}(1,0,0,1) &\leftarrow 0000000000000011_2 & A^{[2]}(1,1,0,1) &\leftarrow 0000000000000011_2 \\
A^{[2]}(1,0,1,0) &\leftarrow 0000000000001110_2 & A^{[2]}(1,1,1,0) &\leftarrow 0000000000001110_2 \\
A^{[2]}(1,0,1,1) &\leftarrow 0000000000000010_2 & A^{[2]}(1,1,1,1) &\leftarrow 0000000000000010_2
\end{aligned}
$$

Nun der nächste Schritt:

$$
\begin{aligned}
A^{[3]}(1,0,0,0) &\leftarrow A^{[2]}(1,0,0,0) + A^{[2]}(1,0,1,0)\omega^x \\
A^{[3]}(1,0,0,1) &\leftarrow A^{[2]}(1,0,0,1) + A^{[2]}(1,0,1,1)\omega^x \\
A^{[3]}(1,0,1,0) &\leftarrow A^{[2]}(1,0,0,0) - A^{[2]}(1,0,1,0)\omega^x \\
A^{[3]}(1,0,1,1) &\leftarrow A^{[2]}(1,0,0,1) - A^{[2]}(1,0,1,1)\omega^x \\
A^{[3]}(1,1,0,0) &\leftarrow A^{[2]}(1,1,0,0) + A^{[2]}(1,1,1,0)\omega^x \\
A^{[3]}(1,1,0,1) &\leftarrow A^{[2]}(1,1,0,1) + A^{[2]}(1,1,1,1)\omega^x \\
A^{[3]}(1,1,1,0) &\leftarrow A^{[2]}(1,1,0,0) - A^{[2]}(1,1,1,0)\omega^x \\
A^{[3]}(1,1,1,1) &\leftarrow A^{[2]}(1,1,0,1) - A^{[2]}(1,1,1,1)\omega^x
\end{aligned}
$$

Für den Exponenten von ω, also x, muss man hier die beiden linken Ziffern in der Klammer betrachten, sie umdrehen und die dann als binäre Zahlen mit zwei multiplizieren. Hier sieht man auch schön, wie sich das Vorzeichen ändert, wenn sich die dritte Ziffer in der Klammer ändert.

$$
\begin{aligned}
A^{[3]}(1,0,0,0) &\leftarrow 0000000000000110_2 + 0000000000001110_2\omega^2 \\
A^{[3]}(1,0,0,1) &\leftarrow 0000000000000011_2 + 0000000000000010_2\omega^2 \\
A^{[3]}(1,0,1,0) &\leftarrow 0000000000000110_2 - 0000000000001110_2\omega^2 \\
A^{[3]}(1,0,1,1) &\leftarrow 0000000000000011_2 - 0000000000000010_2\omega^2 \\
A^{[3]}(1,1,0,0) &\leftarrow 0000000000000110_2 + 0000000000001110_2\omega^6 \\
A^{[3]}(1,1,0,1) &\leftarrow 0000000000000011_2 + 0000000000000010_2\omega^6 \\
A^{[3]}(1,1,1,0) &\leftarrow 0000000000000110_2 - 0000000000001110_2\omega^6 \\
A^{[3]}(1,1,1,1) &\leftarrow 0000000000000011_2 - 0000000000000010_2\omega^6
\end{aligned}
$$

...

Nun machen wir die zyklischen Shifts wegen der Multiplikation mit ω:

$A^{[3]}(1,0,0,0) \leftarrow 0000000000000110_2 + 0000000000111000_2$
$A^{[3]}(1,0,0,1) \leftarrow 0000000000000011_2 + 0000000000001000_2$
$A^{[3]}(1,0,1,0) \leftarrow 0000000000000110_2 - 0000000000111000_2$
$A^{[3]}(1,0,1,1) \leftarrow 0000000000000011_2 - 0000000000001000_2$
$A^{[3]}(1,1,0,0) \leftarrow 0000000000000110_2 + 0000001110000000_2$
$A^{[3]}(1,1,0,1) \leftarrow 0000000000000011_2 + 0000000010000000_2$
$A^{[3]}(1,1,1,0) \leftarrow 0000000000000110_2 - 0000001110000000_2$
$A^{[3]}(1,1,1,1) \leftarrow 0000000000000011_2 - 0000000010000000_2$

...und den zyklischen Shift um $2^n = 8$ Stellen dort wo subtrahiert wird:

$A^{[3]}(1,0,0,0) \leftarrow 0000000000000110_2 + 0000000000111000_2$
$A^{[3]}(1,0,0,1) \leftarrow 0000000000000011_2 + 0000000000001000_2$
$A^{[3]}(1,0,1,0) \leftarrow 0000000000000110_2 + 0011100000000000_2$
$A^{[3]}(1,0,1,1) \leftarrow 0000000000000011_2 + 0000100000000000_2$
$A^{[3]}(1,1,0,0) \leftarrow 0000000000000110_2 + 0000001110000000_2$
$A^{[3]}(1,1,0,1) \leftarrow 0000000000000011_2 + 0000000010000000_2$
$A^{[3]}(1,1,1,0) \leftarrow 0000000000000110_2 + 1000000000000011_2$
$A^{[3]}(1,1,1,1) \leftarrow 0000000000000011_2 + 1000000000000000_2$

Es ergibt sich:

$A^{[3]}(1,0,0,0) \leftarrow 0000000000111110_2$
$A^{[3]}(1,0,0,1) \leftarrow 0000000000001011_2$
$A^{[3]}(1,0,1,0) \leftarrow 0011100000000110_2$
$A^{[3]}(1,0,1,1) \leftarrow 0000100000000011_2$
$A^{[3]}(1,1,0,0) \leftarrow 0000001110000110_2$
$A^{[3]}(1,1,0,1) \leftarrow 0000000010000011_2$
$A^{[3]}(1,1,1,0) \leftarrow 1000000000001001_2$
$A^{[3]}(1,1,1,1) \leftarrow 1000000000000011_2$

Analog hierzu wird dann noch der letzte Schritt ausgeführt, auf die Einzelschritte verzichten wir hier:

$\hat{a}_1 = A^{[4]}(1,0,0,0) \leftarrow 0000000001010100_2$
$\hat{a}_9 = A^{[4]}(1,0,0,1) \leftarrow 0001011000111110_2$
$\hat{a}_5 = A^{[4]}(1,0,1,0) \leftarrow 0011100001100111_2$
$\hat{a}_{13} = A^{[4]}(1,0,1,1) \leftarrow 1001100100000110_2$
$\hat{a}_3 = A^{[4]}(1,1,0,0) \leftarrow 0000011110011110_2$
$\hat{a}_{11} = A^{[4]}(1,1,0,1) \leftarrow 0001101110001010_2$
$\hat{a}_7 = A^{[4]}(1,1,1,0) \leftarrow 1000000111001001_2$
$\hat{a}_{15} = A^{[4]}(1,1,1,1) \leftarrow 0100000000001011_2$

Nun machen wir die Transformation für b_j (diese wird nicht mehr so ausführlich gemacht wie bei a_j, da diese als Beispiel schon genügen, allerdings geben wir die Werte an, so dass man diese beim Nachrechnen überprüfen kann)

$b_0 = 0000000000001011_2$
$b_1 = 0000000000001111_2$
$b_2 = 0000000000000010_2$
$b_3 = 0000000000000010_2$
$b_4 = 0000000000000000_2$
$b_5 = 0000000000000000_2$
...
$b_{15} = 0000000000000000_2$

Der erste Schritt:

$A^{[0]}(0,0,0,0) = b_0 = 0000000000001011_2$
$A^{[0]}(0,0,0,1) = b_1 = 0000000000001111_2$
$A^{[0]}(0,0,1,0) = b_2 = 0000000000000010_2$
$A^{[0]}(0,0,1,1) = b_3 = 0000000000000010_2$
$A^{[0]}(0,1,0,0) = b_4 = 0000000000000000_2$
$A^{[0]}(0,1,0,1) = b_5 = 0000000000000000_2$
$A^{[0]}(0,1,1,0) = b_6 = 0000000000000000_2$
$A^{[0]}(0,1,1,1) = b_7 = 0000000000000000_2$
$A^{[0]}(1,0,0,0) = b_8 = 0000000000000000_2$
$A^{[0]}(1,0,0,1) = b_9 = 0000000000000000_2$
$A^{[0]}(1,0,1,0) = b_{10} = 0000000000000000_2$
$A^{[0]}(1,0,1,1) = b_{11} = 0000000000000000_2$
$A^{[0]}(1,1,0,0) = b_{12} = 0000000000000000_2$
$A^{[0]}(1,1,0,1) = b_{13} = 0000000000000000_2$
$A^{[0]}(1,1,1,0) = b_{14} = 0000000000000000_2$
$A^{[0]}(1,1,1,1) = b_{15} = 0000000000000000_2$

...

Machen wir nun den zweiten Schritt:

$A^{[1]}(1,0,0,0) \leftarrow 0000000000001011_2$ $A^{[1]}(1,1,0,0) \leftarrow 0000000000000000_2$
$A^{[1]}(1,0,0,1) \leftarrow 0000000000001111_2$ $A^{[1]}(1,1,0,1) \leftarrow 0000000000000000_2$
$A^{[1]}(1,0,1,0) \leftarrow 0000000000000010_2$ $A^{[1]}(1,1,1,0) \leftarrow 0000000000000000_2$
$A^{[1]}(1,0,1,1) \leftarrow 0000000000000010_2$ $A^{[1]}(1,1,1,1) \leftarrow 0000000000000000_2$

Der dritte Schritt:

$A^{[2]}(1,0,0,0) \leftarrow 0000000000001011_2$ $A^{[2]}(1,1,0,0) \leftarrow 0000000000001011_2$
$A^{[2]}(1,0,0,1) \leftarrow 0000000000001111_2$ $A^{[2]}(1,1,0,1) \leftarrow 0000000000001111_2$
$A^{[2]}(1,0,1,0) \leftarrow 0000000000000010_2$ $A^{[2]}(1,1,1,0) \leftarrow 0000000000000010_2$
$A^{[2]}(1,0,1,1) \leftarrow 0000000000000010_2$ $A^{[2]}(1,1,1,1) \leftarrow 0000000000000010_2$

Der vierte Schritt:

$A^{[3]}(1,0,0,0) \leftarrow 0000000000010011_2$ $A^{[3]}(1,1,0,0) \leftarrow 0000000010001011_2$
$A^{[3]}(1,0,0,1) \leftarrow 0000000000010111_2$ $A^{[3]}(1,1,0,1) \leftarrow 0000000010001111_2$
$A^{[3]}(1,0,1,0) \leftarrow 0000100000001011_2$ $A^{[3]}(1,1,1,0) \leftarrow 1000000000001011_2$
$A^{[3]}(1,0,1,1) \leftarrow 0000100000001111_2$ $A^{[3]}(1,1,1,1) \leftarrow 1000000000001111_2$

Und nun der letzte Schritt:

$\hat{b}_1 = A^{[4]}(1,0,0,0) \leftarrow 0000000001000001_2$ $\hat{b}_3 = A^{[4]}(1,1,0,0) \leftarrow 0000010100000011_2$
$\hat{b}_9 = A^{[4]}(1,0,0,1) \leftarrow 0010111000010011_2$ $\hat{b}_{11} = A^{[4]}(1,1,0,1) \leftarrow 0111100010001111_2$
$\hat{b}_5 = A^{[4]}(1,0,1,0) \leftarrow 0000100111101100_2$ $\hat{b}_7 = A^{[4]}(1,1,1,0) \leftarrow 1000011111001011_2$
$\hat{b}_{13} = A^{[4]}(1,0,1,1) \leftarrow 1110100100001100_2$ $\hat{b}_{15} = A^{[4]}(1,1,1,1) \leftarrow 0100000000010011_2$

Zusammenfassend haben wir erhalten:

$\hat{a}_1 = 0000000001010100_2$ $\hat{b}_1 = 0000000001000001_2$
$\hat{a}_3 = 0000011110011110_2$ $\hat{b}_3 = 0000010100000011_2$
$\hat{a}_5 = 0011100001100111_2$ $\hat{b}_5 = 0000100111101100_2$
$\hat{a}_7 = 1000000111001001_2$ $\hat{b}_7 = 1000011111001011_2$
$\hat{a}_9 = 0001011000111110_2$ $\hat{b}_9 = 0010111000010011_2$
$\hat{a}_{11} = 0001101110001010_2$ $\hat{b}_{11} = 0111100010001111_2$
$\hat{a}_{13} = 1001100100000110_2$ $\hat{b}_{13} = 1110100100001100_2$
$\hat{a}_{15} = 0100000000001011_2$ $\hat{b}_{15} = 0100000000010011_2$

Nun multiplizieren wir die $\hat{a}_j$ und $\hat{b}_j$ um dann $\hat{c}_j$ zu erhalten. Damit das Ergebnis in $2^{(n+1)}$ Ziffern passt, reduzieren wir zunächst. Reduzieren wir als Beispiel $\hat{a}_1 = 0000000001010100_2$. Hier ist $u = 01010100_2$ und $v = 00000000_2$. Es ist klar, dass $u > v$, und somit ist $\xi = (u - v) = u - 0 = 01010100_2 = 84_{10}$. Als zweites Beispiel reduzieren wir $\hat{a}_{13} = 1001100100000110_2$. Hier ist $u = 00000110_2$ und $v = 10011001_2$. Hier ist $v > u$. Wir rechnen also $\xi = (u - v) + (2^{2^n} + 1) = u + (2^{2^n} + 1) - v = 100000111_2 - 10011001_2 = 1101110_2 = 110_{10}$

Wir bekommen nun nur die a_j für ungerade j, da wir nur diese brauchen und deswegen nur $A^{[v]}(1,...)$ berechnet haben.

Wir haben nun also (dies sind jetzt die reduzierten Werte - d.h sie unterscheiden sich von den a_j oben um ein Vielfaches von F_n):

$\hat{a}_1 \equiv 0000000001010100_2 = 84 \pmod{F_n}$ $\hat{b}_1 \equiv 0000000001000001_2 = 65 \pmod{F_n}$
$\hat{a}_3 \equiv 0000000010010111_2 = 151 \pmod{F_n}$ $\hat{b}_3 \equiv 0000000011111111_2 = 255 \pmod{F_n}$
$\hat{a}_5 \equiv 0000000000101111_2 = 47 \pmod{F_n}$ $\hat{b}_5 \equiv 0000000011100011_2 = 227 \pmod{F_n}$
$\hat{a}_7 \equiv 0000000001001000_2 = 72 \pmod{F_n}$ $\hat{b}_7 \equiv 0000000001000100_2 = 68 \pmod{F_n}$
$\hat{a}_9 \equiv 0000000000101000_2 = 40 \pmod{F_n}$ $\hat{b}_9 \equiv 0000000011100110_2 = 230 \pmod{F_n}$
$\hat{a}_{11} \equiv 0000000001101111_2 = 111 \pmod{F_n}$ $\hat{b}_{11} \equiv 0000000000010111_2 = 23 \pmod{F_n}$
$\hat{a}_{13} \equiv 0000000001101110_2 = 110 \pmod{F_n}$ $\hat{b}_{13} \equiv 0000000000100100_2 = 36 \pmod{F_n}$
$\hat{a}_{15} \equiv 0000000011001100_2 = 204 \pmod{F_n}$ $\hat{b}_{15} \equiv 0000000011010100_2 = 212 \pmod{F_n}$

...

Wir haben dann (in Wirklichkeit würde man natürlich nicht in das Dezimalsystem wechseln - wir tun dies nur zur besseren Übersicht):

$$\hat{c}_1 = \hat{a}_1\hat{b}_1 \equiv 84_{10} * 65_{10} = 5460_{10} = 0001010101010100_2 \pmod{F_n}$$
$$\hat{c}_3 = \hat{a}_3\hat{b}_3 \equiv 151_{10} * 255_{10} = 38505_{10} = 1001011001101001_2 \pmod{F_n}$$
$$\hat{c}_5 = \hat{a}_5\hat{b}_5 \equiv 47_{10} * 227_{10} = 10669_{10} = 0010100110101101_2 \pmod{F_n}$$
$$\hat{c}_7 = \hat{a}_7\hat{b}_7 \equiv 72_{10} * 68_{10} = 4896_{10} = 0001001100100000_2 \pmod{F_n}$$
$$\hat{c}_9 = \hat{a}_9\hat{b}_9 \equiv 40_{10} * 230_{10} = 9200_{10} = 0010001111110000_2 \pmod{F_n}$$
$$\hat{c}_{11} = \hat{a}_{11}\hat{b}_{11} \equiv 111_{10} * 23_{10} = 2553_{10} = 0000100111111001_2 \pmod{F_n}$$
$$\hat{c}_{13} = \hat{a}_{13}\hat{b}_{13} \equiv 110_{10} * 36_{10} = 3960_{10} = 0000111101111000_2 \pmod{F_n}$$
$$\hat{c}_{15} = \hat{a}_{15}\hat{b}_{15} \equiv 204_{10} * 212_{10} = 43248_{10} = 1010100011110000_2 \pmod{F_n}$$

3.6 Die inverse Fourier Transformation

Die inverse Fourier Transformation ist ähnlich definiert:
$\boldsymbol{A^{[v]}(..., s_{v-1}, 0, t_{v+1}, ...) \leftarrow 2^{-1}(A^{[v+1]}(..., s_{v-1}, 0, t_{v+1}, ...)+A^{[v+1]}(..., s_{v-1}, 1, t_{v+1}, ...))}$
$\boldsymbol{A^{[v]}(..., s_{v-1}, 1, t_{v+1}, ...) \leftarrow \omega^{-x}2^{-1}(A^{[v+1]}(..., s_{v-1}, 0, t_{v+1}, ...)-A^{[v+1]}(..., s_{v-1}, 1, t_{v+1}, ...))}$
x ist hier genauso definiert wie oben.

Man bemerkt hier, dass:
$\boldsymbol{A^{[1]}(1, t_1, ..., t_{(n+1)-1}) = A^{[0]}(0, t_1, ..., t_{(n+1)-1})-A^{[0]}(1, t_1, ..., t_{(n+1)-1}) = a_t-a_{t+2^{(n+1)-1}}}$

Warum ist das so? Nach der obigen Formel haben wir:
$A^{[0]}(0, ...) \leftarrow 2^{-1}(A^{[1]}(0, ...) + A^{[1]}(1, ...))$
$A^{[0]}(1, ...) \leftarrow \omega^{-x}2^{-1}(A^{[1]}(0, ...) - A^{[1]}(1, ...))$

Nehmen wir die Differenz dieser beiden Terme, so haben wir (hier ist $x = 0$, deshalb fällt es dann weg):

$A^{[0]}(0, ...) - A^{[0]}(1, ...)$
$= (2^{-1}(A^{[1]}(0, ...) + A^{[1]}(1, ...))) - (2^{-1}(A^{[1]}(0, ...) - A^{[1]}(1, ...)))$
$= (2^{-1}A^{[1]}(0, ...) + 2^{-1}A^{[1]}(1, ...)) - (2^{-1}A^{[1]}(0, ...) - 2^{-1}A^{[1]}(1, ...))$
$= 2^{-1}A^{[1]}(0, ...) + 2^{-1}A^{[1]}(1, ...) - 2^{-1}A^{[1]}(0, ...) + 2^{-1}A^{[1]}(1, ...)$
$= 2^{-1}A^{[1]}(1, ...) + 2^{-1}A^{[1]}(1, ...)$
$= 2 * (2^{-1}A^{[1]}(1, ...))$
$= A^{[1]}(1, ...)$

Das ganze kann man dann natürlich auch rückwärts lesen.

Um zu diesen $A^{[1]}(1, ...)$ zu kommen, **werden nur die $\hat{a}_j$ mit ungeradem j gebraucht** . Um diese zu erhalten muss man ebenfalls **nur alle $A^{[v]}(1, ...)$ für $v \geq 1$ berechnen.**

Nun machen wir die Inverse Fourier Transformation. Wir haben

$A^{[4]}(1,0,0,0) = 0001010101010100_2$ $A^{[4]}(1,1,0,0) = 1001011001101001_2$
$A^{[4]}(1,0,0,1) = 0010001111110000_2$ $A^{[4]}(1,1,0,1) = 0000100111111001_2$
$A^{[4]}(1,0,1,0) = 0010100110101101_2$ $A^{[4]}(1,1,1,0) = 0001001100100000_2$
$A^{[4]}(1,0,1,1) = 0000111101111000_2$ $A^{[4]}(1,1,1,1) = 1010100011110000_2$

Jetzt müssen wir einen Schritt zurückgehen:

$A^{[3]}(1,0,0,0) \leftarrow 2^{-1}(A^{[4]}(1,0,0,0) + A^{[4]}(1,0,0,1))$
$A^{[3]}(1,0,0,1) \leftarrow 2^{-1}\omega^{-x}(A^{[4]}(1,0,0,0) - A^{[4]}(1,0,0,1))$
$A^{[3]}(1,0,1,0) \leftarrow 2^{-1}(A^{[4]}(1,0,1,0) + A^{[4]}(1,0,1,1))$
$A^{[3]}(1,0,1,1) \leftarrow 2^{-1}\omega^{-x}(A^{[4]}(1,0,1,0) - A^{[4]}(1,0,1,1))$
$A^{[3]}(1,1,0,0) \leftarrow 2^{-1}(A^{[4]}(1,1,0,0) + A^{[4]}(1,1,0,1))$
$A^{[3]}(1,1,0,1) \leftarrow 2^{-1}\omega^{-x}(A^{[4]}(1,1,0,0) - A^{[4]}(1,1,0,1))$
$A^{[3]}(1,1,1,0) \leftarrow 2^{-1}(A^{[4]}(1,1,1,0) + A^{[4]}(1,1,1,1))$
$A^{[3]}(1,1,1,1) \leftarrow 2^{-1}\omega^{-x}(A^{[4]}(1,1,1,0) - A^{[4]}(1,1,1,1))$

Bei der Multiplikation mit 2^{-1} machen wir einen zyklischen Shift um eine Stelle nach rechts, bei ω^{-x} machen wir einen zyklischen Shift um x Stellen nach rechts.

$A^{[3]}(1,0,0,0) \leftarrow 2^{-1}(0001010101010100_2 + 0010001111110000_2)$
$A^{[3]}(1,0,0,1) \leftarrow 2^{-1}\omega^{-1}(0001010101010100_2 - 0010001111110000_2)$
$A^{[3]}(1,0,1,0) \leftarrow 2^{-1}(0010100110101101_2 + 0000111101111000_2)$
$A^{[3]}(1,0,1,1) \leftarrow 2^{-1}\omega^{-5}(0010100110101101_2 - 0000111101111000_2)$
$A^{[3]}(1,1,0,0) \leftarrow 2^{-1}(1001011001101001_2 + 0000100111111001_2)$
$A^{[3]}(1,1,0,1) \leftarrow 2^{-1}\omega^{-3}(1001011001101001_2 - 0000100111111001_2)$
$A^{[3]}(1,1,1,0) \leftarrow 2^{-1}(0001001100100000_2 + 1010100011110000_2)$
$A^{[3]}(1,1,1,1) \leftarrow 2^{-1}\omega^{-7}(0001001100100000_2 - 1010100011110000_2)$

Nun rechnen wir den Term in Klammer aus: bei den Subtraktionen müssen wir vor dem Addieren noch wie gewohnt den zyklischen Shift ausführen:

$A^{[3]}(1,0,0,0) \leftarrow 2^{-1}(0011100101000100_2)$
$A^{[3]}(1,0,0,1) \leftarrow 2^{-1}\omega^{-1}(0000010101111000_2)$
$A^{[3]}(1,0,1,0) \leftarrow 2^{-1}(0011100100100101_2)$
$A^{[3]}(1,0,1,1) \leftarrow 2^{-1}\omega^{-5}(1010000110111100_2)$
$A^{[3]}(1,1,0,0) \leftarrow 2^{-1}(1010000001100010_2)$
$A^{[3]}(1,1,0,1) \leftarrow 2^{-1}\omega^{-3}(1000111101110011_2)$
$A^{[3]}(1,1,1,0) \leftarrow 2^{-1}(1011110000010000_2)$
$A^{[3]}(1,1,1,1) \leftarrow 2^{-1}\omega^{-7}(0000001111001001_2)$

Wir führen nun den Shift aus:

$A^{[3]}(1,0,0,0) \leftarrow 0001110010100010_2$
$A^{[3]}(1,0,0,1) \leftarrow 0000000101011110_2$
$A^{[3]}(1,0,1,0) \leftarrow 1001110010010010_2$
$A^{[3]}(1,0,1,1) \leftarrow 1111001010000110_2$
$A^{[3]}(1,1,0,0) \leftarrow 0101000000110001_2$
$A^{[3]}(1,1,0,1) \leftarrow 0011100011110111_2$
$A^{[3]}(1,1,1,0) \leftarrow 0101111000001000_2$
$A^{[3]}(1,1,1,1) \leftarrow 1100100100000011_2$

...

Machen wir den nächsten Schritt

$$
\begin{aligned}
A^{[2]}(1,0,0,0) &\leftarrow 2^{-1}(A^{[3]}(1,0,0,0) + A^{[3]}(1,0,1,0))\\
A^{[2]}(1,0,0,1) &\leftarrow 2^{-1}(A^{[3]}(1,0,0,1) + A^{[3]}(1,0,1,1))\\
A^{[2]}(1,0,1,0) &\leftarrow 2^{-1}\omega^{-x}(A^{[3]}(1,0,0,0) - A^{[3]}(1,0,1,0))\\
A^{[2]}(1,0,1,1) &\leftarrow 2^{-1}\omega^{-x}(A^{[3]}(1,0,0,1) - A^{[3]}(1,0,1,1))\\
A^{[2]}(1,1,0,0) &\leftarrow 2^{-1}(A^{[3]}(1,1,0,0) + A^{[3]}(1,1,1,0))\\
A^{[2]}(1,1,0,1) &\leftarrow 2^{-1}(A^{[3]}(1,1,0,1) + A^{[3]}(1,1,1,1))\\
A^{[2]}(1,1,1,0) &\leftarrow 2^{-1}\omega^{-x}(A^{[3]}(1,1,0,0) - A^{[3]}(1,1,1,0))\\
A^{[2]}(1,1,1,1) &\leftarrow 2^{-1}\omega^{-x}(A^{[3]}(1,1,0,1) - A^{[3]}(1,1,1,1))
\end{aligned}
$$

Setzten wir wieder ein:

$$
\begin{aligned}
A^{[2]}(1,0,0,0) &\leftarrow 2^{-1}(0001110010100010_2 + 1001110010010010_2)\\
A^{[2]}(1,0,0,1) &\leftarrow 2^{-1}(0000000101011110_2 + 1111001010000110_2)\\
A^{[2]}(1,0,1,0) &\leftarrow 2^{-1}\omega^{-x}(0001110010100010_2 - 1001110010010010_2)\\
A^{[2]}(1,0,1,1) &\leftarrow 2^{-1}\omega^{-x}(0000000101011110_2 - 1111001010000110_2)\\
A^{[2]}(1,1,0,0) &\leftarrow 2^{-1}(0101000000110001_2 + 0101111000001000_2)\\
A^{[2]}(1,1,0,1) &\leftarrow 2^{-1}(0011100011110111_2 + 1100100100000011_2)\\
A^{[2]}(1,1,1,0) &\leftarrow 2^{-1}\omega^{-x}(0101000000110001_2 - 0101111000001000_2)\\
A^{[2]}(1,1,1,1) &\leftarrow 2^{-1}\omega^{-x}(0011100011110111_2 - 1100100100000011_2)
\end{aligned}
$$

Nach dem Berechnen der Klammern ergibt sich:

$$
\begin{aligned}
A^{[2]}(1,0,0,0) &\leftarrow 2^{-1}(1011100100110100_2)\\
A^{[2]}(1,0,0,1) &\leftarrow 2^{-1}(1111001111100100_2)\\
A^{[2]}(1,0,1,0) &\leftarrow 2^{-1}\omega^{-2}(1010111100111110_2)\\
A^{[2]}(1,0,1,1) &\leftarrow 2^{-1}\omega^{-2}(1000100001010000_2)\\
A^{[2]}(1,1,0,0) &\leftarrow 2^{-1}(1010111000111001_2)\\
A^{[2]}(1,1,0,1) &\leftarrow 2^{-1}(0000000111111011_2)\\
A^{[2]}(1,1,1,0) &\leftarrow 2^{-1}\omega^{-6}(0101100010001111_2)\\
A^{[2]}(1,1,1,1) &\leftarrow 2^{-1}\omega^{-6}(0011110011000000_2)
\end{aligned}
$$

Führen wir wiederum den Shift aus:

$$
\begin{aligned}
A^{[2]}(1,0,0,0) &\leftarrow 0101110010011010_2\\
A^{[2]}(1,0,0,1) &\leftarrow 0111100111110010_2\\
A^{[2]}(1,0,1,0) &\leftarrow 1101010111100111_2\\
A^{[2]}(1,0,1,1) &\leftarrow 0001000100001010_2\\
A^{[2]}(1,1,0,0) &\leftarrow 1101011100011100_2\\
A^{[2]}(1,1,0,1) &\leftarrow 1000000011111101_2\\
A^{[2]}(1,1,1,0) &\leftarrow 0001111010110001_2\\
A^{[2]}(1,1,1,1) &\leftarrow 1000000001111001_2
\end{aligned}
$$

Nun brauchen wir nur noch einen einzigen Schritt:

$$
\begin{aligned}
A^{[1]}(1,0,0,0) &\leftarrow 2^{-1}(A^{[2]}(1,0,0,0) + A^{[2]}(1,1,0,0))\\
A^{[1]}(1,0,0,1) &\leftarrow 2^{-1}(A^{[2]}(1,0,0,1) + A^{[2]}(1,1,0,1))\\
A^{[1]}(1,0,1,0) &\leftarrow 2^{-1}(A^{[2]}(1,0,1,0) + A^{[2]}(1,1,1,0))\\
A^{[1]}(1,0,1,1) &\leftarrow 2^{-1}(A^{[2]}(1,0,1,1) + A^{[2]}(1,1,1,1))\\
A^{[1]}(1,1,0,0) &\leftarrow 2^{-1}\omega^{-x}(A^{[2]}(1,0,0,0) - A^{[2]}(1,1,0,0))\\
A^{[1]}(1,1,0,1) &\leftarrow 2^{-1}\omega^{-x}(A^{[2]}(1,0,0,1) - A^{[2]}(1,1,0,1))\\
A^{[1]}(1,1,1,0) &\leftarrow 2^{-1}\omega^{-x}(A^{[2]}(1,0,1,0) - A^{[2]}(1,1,1,0))\\
A^{[1]}(1,1,1,1) &\leftarrow 2^{-1}\omega^{-x}(A^{[2]}(1,0,1,1) - A^{[2]}(1,1,1,1))
\end{aligned}
$$

...

Wir setzen ein und rechnen gleich aus:

$$A^{[1]}(1,0,0,0) \leftarrow 2^{-1}(0011001110110111_2)$$
$$A^{[1]}(1,0,0,1) \leftarrow 2^{-1}(1111101011101111_2)$$
$$A^{[1]}(1,0,1,0) \leftarrow 2^{-1}(1111010010011000_2)$$
$$A^{[1]}(1,0,1,1) \leftarrow 2^{-1}(1001000110000011_2)$$
$$A^{[1]}(1,1,0,0) \leftarrow 2^{-1}\omega^{-4}(0111100101110001_2)$$
$$A^{[1]}(1,1,0,1) \leftarrow 2^{-1}\omega^{-4}(0111011101110011_2)$$
$$A^{[1]}(1,1,1,0) \leftarrow 2^{-1}\omega^{-4}(1000011100000110_2)$$
$$A^{[1]}(1,1,1,1) \leftarrow 2^{-1}\omega^{-4}(1000101010001010_2)$$

Jetzt noch die Shifts:

$$A^{[1]}(1,0,0,0) \leftarrow 1001100111011011_2$$
$$A^{[1]}(1,0,0,1) \leftarrow 1111110101110111_2$$
$$A^{[1]}(1,0,1,0) \leftarrow 0111101001001100_2$$
$$A^{[1]}(1,0,1,1) \leftarrow 1100100011000001_2$$
$$A^{[1]}(1,1,0,0) \leftarrow 1000101111001011_2$$
$$A^{[1]}(1,1,0,1) \leftarrow 1001101110111011_2$$
$$A^{[1]}(1,1,1,0) \leftarrow 0011010000111000_2$$
$$A^{[1]}(1,1,1,1) \leftarrow 0101010001010100_2$$

Wir haben jetzt:

$$c_0 - c_8 = A^{[1]}(1,0,0,0) = 1001100111011011_2$$
$$c_1 - c_9 = A^{[1]}(1,0,0,1) = 1111110101110111_2$$
$$c_2 - c_{10} = A^{[1]}(1,0,1,0) = 0111101001001100_2$$
$$c_3 - c_{11} = A^{[1]}(1,0,1,1) = 1100100011000001_2$$
$$c_4 - c_{12} = A^{[1]}(1,1,0,0) = 1000101111001011_2$$
$$c_5 - c_{13} = A^{[1]}(1,1,0,1) = 1001101110111011_2$$
$$c_6 - c_{14} = A^{[1]}(1,1,1,0) = 0011010000111000_2$$
$$c_7 - c_{15} = A^{[1]}(1,1,1,1) = 0101010001010100_2$$

Nun müssen wir diese Zahlen zunächst wieder reduzieren (dies wird jetzt nicht ausführlich gemacht, da dies oben schon geschehen ist).

$$c_0 - c_8 = 01000010_2 = 66$$
$$c_1 - c_9 = 01111011_2 = 123$$
$$c_2 - c_{10} = 11010011_2 = 211$$
$$c_3 - c_{11} = 11111010_2 = 250$$
$$c_4 - c_{12} = 01000000_2 = 64$$
$$c_5 - c_{13} = 00100000_2 = 32$$
$$c_6 - c_{14} = 00000100_2 = 4$$
$$c_7 - c_{15} = 00000000_2 = 0$$

Wir haben jetzt also die $z_j \mod 2^{n+2}$ und $\mod F_n$ berechnet, hier sind noch einmal die Werte:

$$z_0 \equiv 2 \pmod{2^{n+2}}$$
$$z_1 \equiv 27 \pmod{2^{n+2}}$$
$$z_2 \equiv 19 \pmod{2^{n+2}}$$
$$z_3 \equiv 26 \pmod{2^{n+2}}$$
$$z_4 \equiv 0 \pmod{2^{n+2}}$$
$$z_5 \equiv 0 \pmod{2^{n+2}}$$
$$z_6 \equiv 4 \pmod{2^{n+2}}$$
$$z_7 \equiv 0 \pmod{2^{n+2}}$$

und:

$$z_0 \equiv 66 \pmod{F_n}$$
$$z_1 \equiv 123 \pmod{F_n}$$
$$z_2 \equiv 211 \pmod{F_n}$$
$$z_3 \equiv 250 \pmod{F_n}$$
$$z_4 \equiv 64 \pmod{F_n}$$
$$z_5 \equiv 32 \pmod{F_n}$$
$$z_6 \equiv 4 \pmod{F_n}$$
$$z_7 \equiv 0 \pmod{F_n}$$

..

Nun berechnen wir die $z_j \mod F_m$ daraus. Wir haben $z_0 \equiv 2 \pmod{2^{n+2}}$ und $z_0 \equiv 66 \pmod{F_n}$. Also haben wir $\delta \equiv \eta - \xi = 2 - 66 = -64 \equiv 0 \pmod{2^{n+2}}$ (Im letzten Schritt haben wir $2 * 2^{n+2}$ dazu addiert, damit $0 \leq \delta < 2^{n+2}$). Machen wir uns so eine Liste der δ :

$\delta_0 = 0$
$\delta_1 = 0$
$\delta_2 = 0$
$\delta_3 = 0$
$\delta_4 = 0$
$\delta_5 = 0$
$\delta_6 = 0$
$\delta_7 = 0$

Durch besondere Umstände in diesem Beispiel erhalten wir überall 0.

Errechnen wir nun damit die $z_j \mod F_m$: Bei z_0 haben wir $z_0 = \eta + \delta F_n = 66 + 0F_n = 66$. Machen wir wieder eine Liste:

$z_0 \equiv 66 \pmod{F_m}$
$z_1 \equiv 123 \pmod{F_m}$
$z_2 \equiv 211 \pmod{F_m}$
$z_3 \equiv 250 \pmod{F_m}$
$z_4 \equiv 64 \pmod{F_m}$
$z_5 \equiv 32 \pmod{F_m}$
$z_6 \equiv 4 \pmod{F_m}$
$z_7 \equiv 0 \pmod{F_m}$

Nun haben wir also die benötigten z_j errechnet. Die z_j für $2^n \leq j < 2^{n+1}$ sind alle $2^{2^n+1+n} = 2^{8+1+3} = 2^{12}$. Eine Multiplikation mit ihnen entspricht einem Shift um 12 Stellen nach links. Diese multipliziert mit $2^{r2^{n-1}}$ sind immer kongruent $0 \mod F_m$

Wir hatten die Formel: $c \equiv \sum_{r=0}^{2^{n+1}-1} z_r 2^{r2^{n-1}} \pmod{F_m}$

Schlüsseln wir diese Summe auf: c ist die Summe folgender Werte **(Anmerkung: bei den Shifts würde man zyklische Shifts bei $2^{m+1} = 64$ Stellen machen. Dies ist hier allerdings zu umständlich darzustellen, deswegen rechnen wir einfach im Dezimalsystem und reduzieren hinterher.)**:

$z_0 2^{0*2^{n-1}} = z_0 = 66 * 1 = 66$
$z_1 2^{1*2^{n-1}} = z_1 2^4 = 123 * 2^4 = 1968$
$z_2 2^{2*2^{n-1}} = z_2 2^8 = 211 * 2^8 = 54016$
$z_3 2^{3*2^{n-1}} = z_3 2^{12} = 250 * 2^{12} = 1024000$
$z_4 2^{4*2^{n-1}} = z_4 2^{16} = 64 * 2^{16} = 4194304$
$z_5 2^{5*2^{n-1}} = z_5 2^{20} = 32 * 2^{20} = 33554432$
$z_6 2^{6*2^{n-1}} = z_6 2^{24} = 4 * 2^{24} = 67108864$
$z_7 2^{7*2^{n-1}} = z_7 2^{28} = 0 * 2^{28} = 0$

Zusammenaddiert ergibt sich: 105937650. Um $\mod 2^{2^m} + 1 = 4294967297$ reduziert bleibt sie unverändert, da sie kleiner ist als $2^{2^m} + 1$. Dies ist also unser Produkt. Machen wir die Kontrolle: Am Anfang hatten wir die Zahlen $a = 11830$ und $b = 8955$. Deren Produkt $c = ab = 11830 * 8955 = 105937650$.

3.7 Unterschiede wenn m gerade ist

Ist m gerade, so haben wir $m = 2n - 2$. Wir teilen die Zahlen diesmal wieder in Stücke zu 2^{n-1} Ziffern, was diesmal dann nur 2^n Stück sind. Bei der Fourier-Transformation haben wir dann folglich (n) anstatt $(n+1)$ und machen so auch einen Schritt weniger. Als ω verwenden wir $\omega = 4$. Dies ist möglich, da:

$$4^{2^{(n)}} \equiv 1 \pmod{F_n} \tag{112}$$

und

$$4^{2^{(n)-1}} \equiv -1 \pmod{F_n} \tag{113}$$

Hier fehlt, da wir n anstatt $n + 1$ haben, eine Eins im Exponenten. Deswegen "ziehen" wir diese in die Basis und haben somit als Basis $2^2 = 4$.

...

A Glossar

A.1 modulo

Der Modulo ist der Rest bei einer Division, d.h. $a \mod b$ ist der Rest, der bei der Division von a durch b entsteht. Ist z. B. $a = 19$ und $b = 4$ so ist $a \mod b = 3$, da $19/4 = 4\ rest\ 3$.

A.2 Ring

Ein Ring kann man sich (vereinfacht dargestellt) als eine Art "Menge" vorstellen, welche die Operationen "Addition" und "Multiplikation" haben muss, wobei das Ergebnis dann wieder ein Element des "Rings" sein muss. Damit diese "Menge" ein Ring ist, müssen auch noch bestimmte andere Eigenschaften vorhanden sein, so muss z. B. für die Addition das Kommutativgesetz gelten etc. Die ganzen Zahlen und die rationalen Zahlen sind Beispiele für Ringe.

A.3 Restklassenring

In einem Restklassenring $\mathbb{Z}_x$ sind grob gesagt alle Zahlen $\mod x$ reduziert. Genauer gesagt befinden sich alle Zahlen, die sich um ein Vielfaches von x unterscheiden in der selben Restklasse. Um zwei Restklassen z. B. zu multiplizieren, nimmt man einfach ein beliebiges Element beider Restklassen. Meist ist es allerdings von Vorteil, das kleinste Element größer 0 zu nehmen, da die Multiplikation somit weniger Zeit in Anspruch nimmt.

A.4 Kongruenz

$a \equiv b \pmod{c}$ bedeutet, dass a und b kongruent modulo c sind, was heißt, dass sie beide denselben Rest beim Teilen durch c liefern, oder in anderen Worten, dass sie sich genau um ein Vielfaches von c unterscheiden.

A.5 Der Chinesische Restsatz

Eine Zahl x kann simultan zu mehreren anderen Zahlen a_i kongruent $\mod n_i$ sein. Wenn die n_i teilerfremd sind, so erhält man durch den Chinesischen Restsatz eine Lösung für x.

A.6 Die Fourier-Transformation

Die Fourier-Transformation weist einer Funktion eine andere Funktion zu. Die Fourier-Transformation hat zahlreiche Anwendungsgebiete in der Physik, Mathematik, Signalverarbeitung, Kryptographie, Wirtschaftswissenschaften etc. In der Physik kann man z. B. durch die Fourier-Transformation von der zeitlichen Darstellung einer Schwingung (z. B. Schall- oder Lichtwellen) in die Domain der Frequenz-Darstellung wechseln. Es gibt verschiedene Varianten der Fourier-Transformation, so z. B. die Diskrete Fourier-Transformation, die kontinuierliche Fourier-Transformation und die Fourier-Reihe.

A.7 Die Diskrete Fourier-Transformation

Die Diskrete Fourier-Transformation führt die Fourier-Transformation an diskreten Wertepunkten aus, d.h. sie weist einer Folge eine andere Folge zu. Sie wird sonst häufig in der Physik, Signalverarbeitung, etc. verwendet, ein bekanntes Beispiel ist z. B. das mp3-Format, bei dem für Menschen nicht hörbare Frequenzen durch die Diskrete Fourier-Transformation herausgefiltert werden. Durch die inverse Diskrete Fourier-Transformation kann man von der diskreten Fourier-Transformation einer Folge wieder zur Ausgangsfolge zurückgelangen.

A.8 Die Fast Fourier-Transform

Die Fast Fourier-Transform (FFT) berechnet die Werte der Diskreten Fourier-Transformation. Wie der Name schon sagt, ist diese Methode nur schneller. Dies wird durch eine geschickte Umformung erreicht, die es erlaubt, einige Werte nicht neu berechnen zu müssen, da sie schon berechnet wurden. Somit werden Rechenschritte eingespart.

A.9 Einheitswurzel

x ist eine n-te Einheitswurzel (wobei $n \in \mathbb{N}$), wenn $x^n = 1$. Normalerweise liegen diese Zahlen alle auf dem Einheitskreis der komplexen Ebene. 1 ist immer eine n-te Einheitswurzel.

A.10 primitive Einheitswurzel

Eine Einheitswurzel wie oben ist primitiv, wenn sie keine k-te Einheitswurzel ist für alle $k < n$. D.h. $x^k \neq 1$ für alle $k < n$ und $k \in \mathbb{N}$. Man kann eine solche primitive Einheitswurzel immer durch die Formel $x = e^{\frac{2\pi i}{n}}$ berechnen. Warum? x ist zumindest schon einmal eine n-te Einheitswurzel, da $(e^{\frac{2\pi i}{n}})^n = e^{2\pi i}$ und dies ergibt 1. Um zu erkennen, warum diese Einheitswurzel auch primitiv ist, brauchen wir noch eine Eigenschaft des komplexen Einheitskreises. Hat man einen Punkt P auf diesem Einheitskreis, der durch den Winkel α zur x-Achse festgelegt ist, so ergibt P^2 einen Punkt, der durch den Winkel 2α festgelegt ist, P^3 ergibt einen Punkt, der durch 3α festgelegt ist. Allgemein gilt, dass P^n durch den Winkel $n\alpha$ festgelegt ist. Der Punkt, den man durch $(e^{\frac{2\pi i}{n}})$ erhält, ist durch den Winkel $\frac{360^\circ}{n}$ festgelegt. Somit kann bei einer Multiplikation mit Zahlen kleiner n der Winkel 360° nie erreicht werden. Somit haben wir mit der obigen Formel eine primitive Einheitswurzel erhalten.

A.11 Fermat-Zahl

Eine Fermat-Zahl ist eine Zahl $F_n = 2^{2^n} + 1$, wobei $n \in \mathbb{N}$

A.12 Faltungsprodukt

Das Faltungsprodukt entspricht grob gesagt einer Multiplikation ohne Übertrag, auf eine Folge übertragen. Das Faltungsprodukt ist für den Schönhage-Strassen-Algorithmus sehr wichtig und wird deshalb ausführlich oben in einem eigenen Kapitel erklärt.

A.13 Faltungstheorem

Das Faltungstheorem macht den Schönhage-Strassen-Algorithmus überhaupt erst möglich. Das Faltungstheorem besagt, dass man das Faltungsprodukt zweier Folgen erhält, indem man die Diskrete Fourier-Transformation der beiden Folgen macht, die einzelnen Elemente multipliziert und dann die Rücktransformation macht. Siehe dazu das Kapitel oben.

Literatur

[1] Donald E. Knuth, *The Art of Computer Programming, Volume 2 Seminumerical Algorithms, Third Edition*, Addison Wesley, 22. Ausgabe, 1998

[2] A. Schönhage, V. Strassen, *Schnelle Multiplikation großer Zahlen, Computing 7, 281-292*, Springer-Verlag, 1971

[3] Steve R. Tate, *Stable Computation of the Complex Roots of Unity*, IEEE Transactions on Signal Processing, Vol. 43, No. 7, 1995, S. 1709–1711

[4] Wikipedia, *Diskrete Fourier-Transformation*, 8. Juli 2008

[5] Englische Wikipedia, *Root of unity*, 1. April 2008

[6] Englische Wikipedia, *Schönhage-Strassen algorithm*, 31. Dezember 2008

[7] Deutsche Wikipedia, *Schnhage-Strassen-Algorithmus*, 17. September 2008

[8] Englische Wikipedia, *Convolution theorem*, 11. August 2008

[9] Wikipedia, *Betragsfunktion*, 11. Juli 2008