SIGMA
CENTRUM MODELOWANIA MATEMATYCZNEGO

Szybka transformata Fouriera w kryptografii klucza publicznego

Andrzej Chmielowiec

3 września 2008

Streszczenie

Artykuł poświęcony jest wykorzystaniu szybkiej transformaty Fouriera (FFT) do realizacji operacji arytmetycznych. Potencjalnym miejscem zastosowania szybkich algorytmów jest kryptografia klucza publicznego, która intensywnie korzysta z operacji na długich liczbach. Przyspieszenie wykonywania operacji arytmetycznych bardzo zyskało na znaczeniu w ciągu ostatnich lat. Wiąże się to z koniecznością zwiększenia długości kluczy i jednoczesnego zachowania dotychczasowej wydajności systemów kryptograficznych.

Słowa kluczowe: Fast Fourier Transform (FFT), szybka transformata Fouriera, szybkie mnożenie, szybka arytmetyka, mnożenie liczb, mnożenie wielomianów

1 Wprowadzenie

Przekształcenie RSA wymaga wykonywania obliczeń na relatywnie długich liczbach. Postęp, który dokonał się na przestrzeni ostatnich lat w kryptografii wskazuje na to, że wykorzystywanie kluczy o długości 3072 lub 4096 bitów jest koniecznością. Może to prowadzić do drastycznego spadku wydajności obliczeń w przypadku urządzeń peryferyjnych dysponujących niewielkimi mocami obliczeniowymi. W takich przypadkach może być opłacalne zastosowanie szybkiej transformaty Fouriera do mnożenia długich liczb. W artykule przedstawię szybką transformatę Fouriera zarówno od strony teoretycznej, jak i praktycznej. Zaprezentowane zostaną między innymi dwa algorytmy służące do mnożenia liczb całkowitych oraz ich zastosowanie w arytmetyce modularnej. Przedstawię w jaki sposób można zastąpić zespolone pierwiastki z jedności odpowiednimi pierwiastkami ciał skończonych podczas realizacji szybkiego mnożenia liczb całkowitych. Takie podejście eliminuje konieczność wykonywania operacji zmiennoprzecinkowych i dbania o ich odpowiednią precyzję. Pokażę również w jaki sposób można wykorzystać szybkie

przekształcenie Fouriera do realizacji asymptotycznie szybkiej arytmetyki w pierścieniu formalnych szeregów potęgowych (mnożenie i dzielenie szeregów). Implementacja takich operacji jest bowiem niezbędna jeśli chcemy relatywnie szybko zliczać punkty na krzywej eliptycznej zadanej nad ciałem skończonym. Zagadnienie to jest bardzo istotne dla nowej generacji systemów kryptograficznych, których bezpieczeństwo opiera się na problemie logarytmu dyskretnego w grupie punktów krzywej.

2 Wielomiany i pierwiastki z jedności

Wielomianem zmiennej X nad ciałem K nazywamy funkcję $A(X)$, która ma postać

$$A(X) = \sum_{j=0}^{n} a_j X^j.$$

Stopniem wielomianu nazywamy największą liczbę całkowitą $d \leq n$, dla której $a_d \neq 0$. W przypadku, gdy wszystkie współczynniki a_j są zerowe, wielomian nazywamy zerowym i przyjmujemy, że jego stopień wynosi -1. Zbiór wszystkich wielomianów tworzy pierścień, który oznaczamy przez $K[X]$. Jeżeli wielomiany $A, B \in K[X]$ mają postać

$$A(X) = \sum_{j=0}^{n} a_j X^j, \quad B(X) = \sum_{j=0}^{n} b_j X^j,$$

to ich sumę, różnicę i iloczyn definiujemy następująco

$$A(X) + B(X) = \sum_{j=0}^{n} (a_j + b_j) X^j,$$

$$A(X) - B(X) = \sum_{j=0}^{n} (a_j - b_j) X^j,$$

$$A(X) \cdot B(X) = \sum_{j=0}^{2n} \left(\sum_{k=0}^{j} a_k b_{j-k} \right) X^j.$$

Z przytoczonych formuł wynika, że do wykonania dodawania lub odejmowania wielomianów konieczne jest wyznaczenie n sum lub różnic odpowiednich współczynników. Natomiast do wykonania mnożenia potrzebujemy wyznaczyć aż n^2 iloczynów odpowiednich współczynników. Taka liczba mnożeń nie stanowi większego problemu w przypadku, gdy wielomiany mają nieduże stopnie. Metoda ta jest jednak bardzo czasochłonna jeżeli wielomiany mają po kilka milionów niezerowych współczynników (takie wielomiany są wykorzystywane między innymi w algorytmach zliczania punktów krzywej eliptycznej nad prostym ciałem skończonym).

2.1 Reprezentacja wielomianów

Przedstawiona powyżej reprezentacja wielomianu nosi nazwę współczynnikowej i pozwala traktować wszystkie wielomiany o ograniczeniu stopnia n jako wektory współczynników $(a_0, \ldots, a_n) \in K^n$. Jest ona bardzo wygodna w przypadku, gdy chcemy określić wartość wielomianu w danym punkcie lub szukamy jego pierwiastków. Wyznaczanie wartości wielomianu w danym punkcie x nosi nazwę ewaluacji i może być efektywnie wykonane przy użyciu schematu Hornera

$$A(x) = a_0 + x(a_1 + x(a_2 + \cdots + x(a_{n-1} + x(a_n)) \ldots)).$$

Operacja ta jest szybka i wymaga wykonania jedynie n mnożeń i dodawań. Poza tym schemat Hornera ma bardzo dobre własności numeryczne, które determinują jego wykorzystanie podczas obliczeń zmiennoprzecinkowych. Niestety wykonanie mnożenia dwóch wielomianów reprezentowanych przez ich współczynniki jest, jak zauważyliśmy już wcześniej, operacją czasochłonną. Tej wady nie ma reprezentacja poprzez wartości w punktach. Okazuje się bowiem, że jeśli mamy dany zbiór par

$$\{(x_0, y_0), (x_1, y_1), \ldots, (x_n, y_n)\}$$

takich, że $x_j \neq x_k$, to istnieje dokładnie jeden wielomian $A(X) \in K[X]$ o stopniu ograniczonym przez n, dla którego mamy

$$A(x_j) = y_j.$$

Wykonanie mnożenia wielomianów sprowadza się w tym przypadku do wymnożenia odpowiednich wartości i wymaga jedynie n operacji w ciele K. Należy w tym miejscu zwrócić szczególną uwagę na to, aby suma stopni czynników nie przekraczała liczby n. W przeciwnym przypadku wynik otrzymany tą metodą będzie niepoprawny.

Dotychczasowe rozważania pokazują, że mnożenie może być wykonane bardzo szybko, jeśli tylko zastosujemy inną reprezentację wielomianu (reprezentację przez wartości w punktach). W dalszej części artykułu pokażemy w jaki sposób szybko zmieniać reprezentację wielomianu i jak można zastosować otrzymane rezultaty w arytmetyce liczb całkowitych.

2.2 Pierwiastki z jedności

Jeżeli dla danego wielomianu $A(X) \in K[X]$ istnieje taki element $x \in K$ dla którego $A(x) = 0$, to x nazywamy pierwiastkiem wielomianu A. W szczególności, gdy

$$A(X) = X^n - 1,$$

to x nazywamy pierwiastkiem n-tego stopnia z jedności. Jeżeli ponadto x nie jest pierwiastkiem żadnego wielomianu $X^d - 1$ dla $d < n$, to nazywamy go pierwiastkiem pierwotnym n-tego stopnia z jedności. Warto w tym miejscu zauważyć, że zbiór H_n pierwiastków n-tego stopnia

z jedności tworzy podgrupę zawartą w grupie $K^\times$. Aby uzasadnić ten fakt wystarczy zauważyć, że jeśli $x, y \in H_n \subset K^\times$ spełniają równanie $X^n - 1 = 0$, to

$$\left(xy^{-1}\right)^n = 1.$$

W związku $xy^{-1} \in H_n$, co oznacza, że H_n jest grupą.

Przykład 1 Niech $K = \mathbb{C}$ będzie ciałem liczb zespolonych. Wielomian $X^8 - 1$ ma w tym ciele 8 pierwiastków, którymi są kolejne potęgi liczby $\omega_8 = e^{2\pi i\ /8}$. W związku z tym wielomian $X^8 - 1$ rozkłada na czynniki liniowe.

$$\begin{array}{lllll}
 & & & (X-1) & = (X-\omega_8^0) \\
 & & (X^2-1) & & \\
 & & & (X+1) & = (X-\omega_8^4) \\
 & (X^4-1) & & & \\
 & & & (X-\omega_8^2) & = (X-\omega_8^2) \\
 & & (X^2+1) & & \\
 & & & (X+\omega_8^2) & = (X-\omega_8^6) \\
(X^8-1) & & & & \\
 & & & (X-\omega_8) & = (X-\omega_8^1) \\
 & & (X^2-\omega_8^2) & & \\
 & & & (X+\omega_8) & = (X-\omega_8^5) \\
 & (X^4+1) & & & \\
 & & & (X-\omega_8^3) & = (X-\omega_8^3) \\
 & & (X^2+\omega_8^2) & & \\
 & & & (X+\omega_8^3) & = (X-\omega_8^7)
\end{array}$$

Kolejność czynników na powyższym diagramie nie została dobrana przypadkowo. Okazuje się, że dla każdego wielomianu postaci $X^{2^n} - 1$ można tak je uporządkować, aby iloczyn kolejnych dwóch był dwumianem. Ta własność, jak się później okaże, jest bardzo istotna z punktu widzenia implementacji szybkiej transformaty Fouriera. □

W dalszej części uwagę skupimy na tych pierwiastkach z jedności, których stopień jest potęgą liczby 2. Te bowiem najlepiej nadają się do wykorzystania podczas realizacji szybkiej transformaty Fouriera. Przyjmijmy zatem, że $n = 2^m$, a wielomian $X^m - 1$ ma w ciele K dokładnie n pierwiastków $\omega^0, \omega^1, \ldots, \omega^{n-1}$.

Lemat 1 Jeżeli $\Phi_{0,k} = X - \omega^{l_k}$, gdzie $l_k = \sum_{j=0}^{m-1} \left(\left\lfloor \frac{k}{2^j} \right\rfloor \mod 2\right) \cdot 2^{m-1-j}$, to wszystkie wyrażenia

$$\Phi_{j,k} = \Phi_{j-1,2k}\Phi_{j-1,2k+1}$$

są dwumianami o niezerowym wyrazie wolnym i stopniu równym 2^j.

Zanim przejdziemy do dowodu tego lematu wyjaśnimy jaki jest faktyczny związek pomiędzy potęgą pierwiastka z jedności, a pozycją na której powinien być ustawiony. Zawarty w treści lematu wzór $l_k = \sum_{j=0}^{m-1} \left(\left\lfloor \frac{k}{2^j} \right\rfloor \mod 2 \right) \cdot 2^{m-1-j}$, choć mało czytelny, wyraża bardzo prostą zależność. Jeżeli bowiem przedstawimy liczbę k w jej m-bitowej reprezentacji $\sum_{j=0}^{m-1} b_j 2^j$, to liczba l_k jest niczym innym jak $\sum_{j=0}^{m-1} b_{m-1-j} 2^j$. Oznacza to, że liczba l_k powstaje z liczby k poprzez odwrócenie kolejności bitów reprezentacji.

Dowód: Rozwijając wzór rekurencyjny na wyrażenie $\Phi_{j,k}$ otrzymujemy związek

$$\Phi_{j,k} = \prod_{i=2^j k}^{2^j(k+1)-1} \Phi_{0,i} = \prod_{i=2^j k}^{2^j(k+1)-1} \left(X - \omega^{l_i} \right).$$

Na mocy uwagi poczynionej przed dowodem lematu możemy stwierdzić, że skoro i przebiega wszystkie liczby ze zbioru $\{2^j k + r : 0 \leq r < 2^j\}$ to wykładniki l_i przebiegają wszystkie liczby ze zbioru $\{2^{m-j} r + k' : 0 \leq r < 2^j\}$. Liczba k' powstaje z liczby k poprzez zamianę kolejności bitów i co do wartości jest równa $l_{2^j k}$. Możemy zatem zapisać, że

$$\Phi_{j,k} = \prod_{r=0}^{2^j-1} \left(X - \omega^{2^{m-j} r + k'} \right).$$

Przyjmując $\alpha = \omega^{k'}$ i $\beta = \omega^{2^{m-j}}$ upraszczamy powyższe wyrażenie do postaci

$$\Phi_{j,k} = \prod_{r=0}^{2^j-1} (X - \alpha\beta^r) = \alpha^{2^j} \prod_{r=0}^{2^j-1} \left(\frac{X}{\alpha} - \beta^r \right).$$

Ale potęgi elementu β generują wszystkie pierwiastki stopnia 2^j z jedności. Oznacza to, że ostatni iloczyn w powyższej formule reprezentuje wielomian $(X/\alpha)^{2^j} - 1$ i ostatecznie wzór na $\Phi_{j,k}$ upraszcza się do postaci

$$\Phi_{j,k} = X^{2^j} - \alpha^{2^j} = X^{2^j} - \omega^{2^j k'},$$

co kończy dowód lematu. ■

Przykład 2 Zobaczmy jak działa wprowadzony lemat w praktyce. Niech $K = \mathbb{C}$, a naszymi pierwiastkami z jedności niech będą kolejne potęgi liczby $\omega = e^{2\pi i/8}$.

$$\begin{array}{ll}
k = 0 = (0,0,0)_2 & l_0 = (0,0,0)_2 = 0 \\
k = 1 = (0,0,1)_2 & l_1 = (1,0,0)_2 = 4 \\
k = 2 = (0,1,0)_2 & l_2 = (0,1,0)_2 = 2 \\
k = 3 = (0,1,1)_2 & l_3 = (1,1,0)_2 = 6 \\
k = 4 = (1,0,0)_2 & l_4 = (0,0,1)_2 = 1 \\
k = 5 = (1,0,1)_2 & l_5 = (1,0,1)_2 = 5 \\
k = 6 = (1,1,0)_2 & l_6 = (0,1,1)_2 = 3 \\
k = 7 = (1,1,1)_2 & l_7 = (1,1,1)_2 = 7
\end{array}$$

Jak można było przypuszczać, otrzymana kolejność pierwiastków jest taka sama, jak w poprzednim przykładzie. □

3 Szybka transformata Fouriera i mnożenie wielomianów

Głównym celem tego artykułu jest pokazanie w jaki sposób transformata Fouriera może być wykorzystana podczas mnożenia wielomianów, liczb i szeregów potęgowych. Dlatego też nasze wysiłki skupimy na wyjaśnieniu w jaki sposób można przy jej pomocy zmieniać reprezentację wielomianu, co bezpośrednio prowadzi do efektywnych algorytmów mnożenia.

3.1 Dyskretna transformata Fouriera

Zajmiemy się teraz znalezieniem szybkiej metody przejścia od reprezentacji wielomianu za pomocą współczynników do jego reprezentacji za pomocą wartości w punktach. Podczas naszych rozważań będziemy zakładali, że stopień rozpatrywanego wielomianu jest mniejszy od $n = 2^m$, a jego współczynniki pochodzą z ciała K w którym $\Phi_n(X) = X^n - 1$ rozkłada się na czynniki liniowe. Oznaczmy przez $\omega^0, \omega^1, \ldots, \omega^{n-1} \in K$ kolejne pierwiastki wielomianu Φ_n. To właśnie wartości w tych punktach będą wyznaczane podczas zmiany reprezentacji. Poniższy lemat przedstawia dwie proste własności wielomianów, które będą nam potrzebne w dalszej części artykułu.

Lemat 2 Niech x będzie dowolnym elementem ciała K, a wielomiany $A, B, C, R \in K[X]$ spełniają warunki $A \mod B = R$ i $B \mod C = 0$. Wtedy prawdziwe są następujące równości

$$A(x) = A \mod (X - x) \qquad \text{i} \qquad A \mod C = R \mod C.$$

Dowód: Dla dowodu pierwszej tożsamości przyjmijmy, że $A(X) = \sum_{j=0}^{n-1} a_j X^j$. Poniższa tożsamość

$$X^k = (X^{k-1} + xX^{k-2} + \cdots + x^{k-2}X + x^{k-1})(X - x) + x^k,$$

pokazuje, że $X^k \mod (X - x) = x^k$. Wykorzystując teraz fakt, że operacja $\mod$ jest homomorfizmem naturalnym pierścienia $K[X]$ otrzymujemy zależność

$$\begin{aligned} A \mod (X - x) &= \left(\sum_{j=0}^{n-1} a_j X^j\right) \mod (X - x) \\ &= \sum_{j=0}^{n-1} a_j \left(X^j \mod (X - x)\right) \\ &= \sum_{j=0}^{n-1} a_j x^j = A(x), \end{aligned}$$

co kończy dowód pierwszej części lematu. Dla dowodu drugiej części zauważmy, że skoro $A \mod B = R$, to istnieje taki wielomian $D \in K[X]$, który spełnia tożsamość $A = D \cdot B + R$.

Uwzględniając warunek $B \mod C = 0$ otrzymujemy ostatecznie

$$\begin{aligned} A \mod C &= (D \cdot B + R) \mod C \\ &= (D \mod C)(B \mod C) + (R \mod C) \\ &= R \mod C, \end{aligned}$$

co kończy dowód lematu. ■

Lematy 1 i 2 dają nam możliwość szybkiego wyznaczenia wartości wielomianu w punktach będących pierwiastkami z jedności.

Twierdzenie 1 (Dyskretna transformata Fouriera) Niech $A \in K[X]$ będzie wielomianem stopnia mniejszego od $n = 2^m$, którego wartości w pierwiastkach z jedności mają być obliczone. Przyjmijmy, tak jak w lemacie 1, że $\Phi_{0,k} = X - \omega^{l_k}$ dla $l_k = \sum_{j=0}^{m-1} \left(\left\lfloor \frac{k}{2^j} \right\rfloor \mod 2\right) \cdot 2^{m-1-j}$ oraz

$$\Phi_{j,k} = \Phi_{j-1,2k}\Phi_{j-1,2k+1}.$$

Jeżeli ciąg $A_{j,k}$ zdefiniowany jest jako

$$A_{j,k} = A_{j+1,\lfloor k/2 \rfloor} \mod \Phi_{j,k} \qquad \text{i} \qquad A_{m,0} = A,$$

to wszystkie jego wyrazy można wyznaczyć wykonując $m \cdot n$ mnożeń w ciele K i $A_{0,k} = A(\omega^{l_k})$.

Dowód: Najpierw wykażemy, że $A_{0,k} = A(\omega^{l_k})$. W tym celu przeanalizujemy ciąg operacji, które prowadzą do wyznaczenia wyrazu $A_{0,k}$.

$$\begin{aligned} A_{0,k} &= \left(A_{1,\lfloor k/2 \rfloor} \mod \Phi_{0,k}\right) \\ &= \left(A_{2,\lfloor k/2^2 \rfloor} \mod \Phi_{1,\lfloor k/2 \rfloor}\right) \mod \Phi_{0,k} \\ &\vdots \\ &= \left(\left(\ldots\left(A_{m,\lfloor k/2^m \rfloor} \mod \Phi_{m,\lfloor k/2^{m-1} \rfloor}\right)\ldots\right) \mod \Phi_{1,\lfloor k/2 \rfloor}\right) \mod \Phi_{0,k} \end{aligned}$$

Biorąc pod uwagę, że $k < n = 2^m$ i $A_{m,0} = A$ otrzymujemy związek

$$A_{0,k} = \left(\left(\ldots\left(A \mod \Phi_{m,\lfloor k/2^{m-1} \rfloor}\right)\ldots\right) \mod \Phi_{1,\lfloor k/2 \rfloor}\right) \mod \Phi_{0,k}.$$

Teraz zauważmy, że z rekurencyjnej definicji $\Phi_{j,k}$ wynika zależność $\Phi_{j,k} \mid \Phi_{j+1,\lfloor k/2 \rfloor}$, która prowadzi do podzielności $\Phi_{0,k} \mid \Phi_{1,\lfloor k/2 \rfloor} \mid \cdots \mid \Phi_{m,\lfloor k/2^{m-1} \rfloor}$. Stosując lemat 2 otrzymujemy zatem

$$A_{0,k} = A \mod \Phi_{0,k} = A(\omega^{l_k}).$$

W celu oszacowania liczby niezbędnych mnożeń w ciele K wykorzystamy wyniki z lematu 1. Zauważmy, że wielomian $A_{j,k}$ powstaje przez redukcję wielomianu $A_{j+1,\lfloor k/2 \rfloor}$ o najwyżej 2^{j+1}

współczynnikach modulo dwumian $\Phi_{j,k} = X^{2^j} - \alpha^{2^j}$. Taka redukcja jest bardzo łatwa do przeprowadzenia i wymaga wykonania 2^j mnożeń

$$\begin{aligned} A_{j+1,\lfloor k/2 \rfloor} \mod \Phi_{j,k} &= \left(\sum_{i=0}^{2^{j+1}-1} a_i X^i \right) \mod \left(X^{2^j} - \alpha^{2^j} \right) \\ &= \sum_{i=0}^{2^j-1} a_i X^i + \alpha^{2^j} \sum_{i=0}^{2^j-1} a_{2^j+i} X^i \\ &= \sum_{i=0}^{2^j-1} \left(a_i + \alpha^{2^j} \cdot a_{2^j+i} \right) X^i. \end{aligned}$$

W związku z tym do wyznaczenia pojedynczego wielomianu $A_{j,k}$ konieczne jest wykonanie co najwyżej tylu mnożeń w ciele K, jaki jest stopień $\Phi_{j,k}$. Zauważmy, że na każdym poziomie rekurencji zachodzi równość $\prod_k \Phi_{j,k} = \Phi_n = X^n - 1$. Ponieważ mamy m poziomów rekurencji, to maksymalna liczba mnożeń jakie należy wykonać wynosi $m \cdot n$. ■

Ponieważ nadmiar indeksów nie służy zrozumieniu istoty zagadnienia, zobaczmy jak faktycznie działa dyskretna transformata Fouriera na przykładzie.

Przykład 3 Tym razem nasze rozważania będziemy prowadzili w ciele skończonym $K = \mathbb{F}_{17}$. Wszystkie niezerowe elementy tego ciała są pierwiastkami stopnia 16 z jedności. Do naszego przykładu wykorzystamy jedynie pierwiastki stopnia 4, którymi są $\omega^0 = 1, \omega^1 = 13, \omega^2 = 16, \omega^3 = 4$. Z przykładów 1 i 2 wynika następująca hierarchia wielomianów $\Phi_{j,k}$.

$$\begin{array}{ccc} & & \Phi_{0,0} = X - 1 \\ & \Phi_{1,0} = X^2 - 1 & \\ & & \Phi_{0,1} = X - 16 \\ \Phi_{2,0} = X^4 - 1 & & \\ & & \Phi_{0,2} = X - 13 \\ & \Phi_{1,1} = X^2 - 16 & \\ & & \Phi_{0,3} = X - 4 \end{array}$$

Powiedzmy, że chcemy znaleźć wartości wielomianu $A(X) = X^3 + 2X^2 + 3X + 4$ w punktach $\omega^0, \ldots, \omega^3$. Postępując zgodnie z procedurą opisaną w twierdzeniu 1 otrzymujemy następujący

ciąg wielomianów $A_{j,k}$.

$$\begin{aligned}
A_{2,0} &= X^3 + 2X^2 + 3X + 4 \\
\\
A_{1,0} &= A_{2,0} \mod \Phi_{1,0} = (X^3 + 2X^2 + 3X + 4) \mod (X^2 - 1) \\
&= 4X + 6 \\
A_{1,1} &= A_{2,0} \mod \Phi_{1,1} = (X^3 + 2X^2 + 3X + 4) \mod (X^2 - 16) \\
&= 2X + 2 \\
\\
A_{0,0} &= A_{1,0} \mod \Phi_{0,0} = (4X + 6) \mod (X - 1) \\
&= 10 = A(1) \\
A_{0,1} &= A_{1,0} \mod \Phi_{0,1} = (4X + 6) \mod (X - 16) \\
&= 2 = A(16) \\
A_{0,2} &= A_{1,1} \mod \Phi_{0,2} = (2X + 2) \mod (X - 13) \\
&= 11 = A(13) \\
A_{0,3} &= A_{1,1} \mod \Phi_{0,2} = (2X + 2) \mod (X - 4) \\
&= 10 = A(4)
\end{aligned}$$

□

3.2 Odwrotna dyskretna transformata Fouriera

Wyznaczanie wartości wielomianu w punktach przy użyciu transformaty Fouriera pozwala na zamianę reprezentacji tylko w jedną stronę. Aby nasze rozważania były kompletne musimy jeszcze wyjaśnić w jaki sposób można realizować przekształcenie odwrotne, które pozwala na powrót do reprezentacji współczynnikowej wielomianu.

Twierdzenie 2 (Odwrotna dyskretna transformata Fouriera) Przyjmijmy, tak jak w lemacie 1, że $\Phi_{0,k} = X - \omega^{l_k}$ dla $l_k = \sum_{j=0}^{m-1} \left(\left\lfloor \frac{k}{2^j} \right\rfloor \mod 2 \right) \cdot 2^{m-1-j}$ oraz

$$\Phi_{j,k} = \Phi_{j-1,2k} \Phi_{j-1,2k+1}.$$

Niech $A \in K[X]$ będzie wielomianem stopnia mniejszego od $n = 2^m$, którego wartości w pierwiastkach z jedności $\omega^0, \omega^1, \ldots, \omega^{n-1}$ są znane. Jeżeli ciąg $A_{j,k}$ zdefiniowany jest jako

$$A_{j,k} = A_{j+1,\lfloor k/2 \rfloor} \mod \Phi_{j,k} \qquad \text{i} \qquad A_{0,k} = A(\omega^{l_k}),$$

to wszystkie jego wyrazy można wyznaczyć wykonując $2 \cdot m \cdot n$ mnożeń w ciele K i $A_{m,0} = A$.

Dowód: Z lematu 1 wynika, że dwumiany $\Phi_{j,k}$ mają postać $X^{2^j} - \alpha^{2^j}$, gdzie element α jest zadany dla każdego z tych dwumianów osobno. Ponieważ $\Phi_{j,k} = \Phi_{j-1,2k} \Phi_{j-1,2k+1}$ jest

iloczynem dwumianów o tym samym stopniu, to mamy

$$\Phi_{j-1,2k} = X^{2^{j-1}} - \alpha^{2^{j-1}} \qquad \text{i} \qquad \Phi_{j-1,2k+1} = X^{2^{j-1}} + \alpha^{2^{j-1}}.$$

Wyznaczenie wyrazów ciągu $A_{j,k}$ przy pomocy formuły podanej w treści twierdzenia jest niewykonalne, ponieważ dysponujemy jedynie wyrazami $A_{0,k}$. Potrzebujemy zatem warunku, który byłby równoważny i pozwalał na odtwarzanie ciągu w kierunku przeciwnym. Sprawdzimy teraz, że takim warunkiem jest

$$A_{j,k} = \frac{1}{2}\left(A_{j-1,2k} + A_{j-1,2k+1}\right) + \frac{X^{2^{j-1}}}{2\alpha^{2^{j-1}}}\left(A_{j-1,2k} - A_{j-1,2k+1}\right).$$

Dla dowodu słuszności powyższej formuły wystarczy wykazać, że $A_{j-1,2k} = A_{j,k} \mod \Phi_{j-1,2k}$ i $A_{j-1,2k+1} = A_{j,k} \mod \Phi_{j-1,2k+1}$. Ale to jest oczywiste, gdyż biorąc pod uwagę postać dwumianów $\Phi_{j-1,2k}$ i $\Phi_{j-1,2k+1}$ mamy

$$A_{j,k} \mod \Phi_{j-1,2k} =$$

$$\left(\frac{1}{2}\left(A_{j-1,2k} + A_{j-1,2k+1}\right) + \frac{X^{2^{j-1}}}{2\alpha^{2^{j-1}}}\left(A_{j-1,2k} - A_{j-1,2k+1}\right)\right) \mod \left(X^{2^{j-1}} - \alpha^{2^{j-1}}\right) =$$

$$\frac{1}{2}\left(A_{j-1,2k} + A_{j-1,2k+1}\right) + \frac{1}{2}\left(A_{j-1,2k} - A_{j-1,2k+1}\right) = A_{j-1,2k}$$

$$A_{j,k} \mod \Phi_{j-1,2k+1} =$$

$$\left(\frac{1}{2}\left(A_{j-1,2k} + A_{j-1,2k+1}\right) + \frac{X^{2^{j-1}}}{2\alpha^{2^{j-1}}}\left(A_{j-1,2k} - A_{j-1,2k+1}\right)\right) \mod \left(X^{2^{j-1}} + \alpha^{2^{j-1}}\right) =$$

$$\frac{1}{2}\left(A_{j-1,2k} + A_{j-1,2k+1}\right) - \frac{1}{2}\left(A_{j-1,2k} - A_{j-1,2k+1}\right) = A_{j-1,2k+1}.$$

Teraz wystarczy zauważyć, że w celu wyznaczenia każdego z wielomianów $A_{j,k}$ wykonujemy dwa razy więcej mnożeń niż w przypadku schematu podanego w twierdzeniu 1. Dlatego należy wykonać $2 \cdot m \cdot n$ mnożeń w ciele K. To kończy dowód. ■

Dysponując szybkim przekształceniem do zmiany reprezentacji wielomianów możemy wykorzystać je do realizacji asymptotycznie szybkiego algorytmu mnożenia. Zasada działania takiego algorytmu jest bardzo prosta.

1. Transformujemy wielomiany $A, B \in K[X]$ reprezentowane przez współczynniki do ich reprezentacji przez wartości w punktach.
2. Mnożymy wielomiany poprzez wymnożenie wartości w odpowiadających sobie punktach.
3. Używamy transformaty odwrotnej, aby ponownie zamienić reprezentację na współczynnikową.

4 Zastosowanie szybkiej transformaty Fouriera do realizacji arytmetyki modularnej

Do tej pory zobaczyliśmy jedynie w jaki sposób można zastosować transformatę Fouriera do szybkiego mnożenia wielomianów. Aby zastosować nasze dotychczasowe wyniki, musimy w jakiś sposób powiązać liczby całkowite i wielomiany. Załóżmy zatem, że reprezentujemy liczby całkowite w systemie o podstawie R. W związku z tym każda dodatnia liczba całkowita a jest reprezentowana w sposób jednoznaczny poprzez swoje cyfry

$$a = \sum_{j=0}^{n-1} a_j R^j.$$

Patrząc na przedstawioną powyżej liczbę, wydaje się, że najbardziej naturalnym pomysłem jest utożsamienie jej z wielomianem postaci

$$A = \sum_{j=0}^{n-1} a_j X^j.$$

Należy jednak pamiętać, że wykonanie mnożenia z wykorzystaniem transformaty Fouriera wiąże się z koniecznością interpretowania liczb a_j jako elementów pewnego ciała. Nasuwają się tutaj dwie możliwości.

1. Możemy potraktować liczby a_j jako elementy ciała liczb zespolonych.
2. Możemy potraktować liczby a_j jako elementy pewnego ciała skończonego $\mathbb{F}_p$.

Tak naprawdę żadna z powyższych opcji nie jest doskonała. W pierwszym przypadku jesteśmy bowiem zmuszeni do kontroli błędów zaokrągleń. Drugie podejście usuwa ten problem, ale konieczne jest zapewnienie, że wynik nie zostanie zredukowany modulo p. To jednak jest dość łatwe do osiągnięcia. Jeżeli bowiem chcemy wymnożyć dwie liczby n bitowe, to wystarczy spełnić warunek $R^2 \cdot \lfloor \log_2 n + 1 \rfloor < p$. Takie ograniczenie powoduje, że żaden ze współczynników iloczynu wielomianów nie zostanie zredukowany modulo p i na tej podstawie będzie można uzyskać informację na temat iloczynu liczb całkowitych.

4.1 Szybkie mnożenie liczb całkowitych

Załóżmy, że chcemy wymnożyć dwie n bitowe dodatnie liczby całkowite a i b. Liczby te reprezentowane są w systemie o podstawie R i mają postać

$$a = \sum_{j=0}^{n-1} a_j R^j, \qquad b = \sum_{j=1}^{n-1} b_j R^j.$$

Zamieniamy te liczby na wielomiany

$$A = \sum_{j=0}^{n-1} a_j X^j, \qquad B = \sum_{j=1}^{n-1} b_j X^j.$$

Teraz musimy znaleźć taką liczbę pierwszą p, która spełnia warunki

1. $R^2 \cdot \lfloor \log_2 n + 1 \rfloor < p$ - odpowiada za brak redukcji modulo p podczas obliczeń.
2. $p = 2^{m+1}r+1$ dla pewnego $2^{m+1} \geq 2n$ - odpowiada za wystarczającą liczbę pierwiastków z jedności.

Z twierdzenia Dirichleta wynika, że liczb pierwszych postaci $2^{m+1}r+1$ jest nieskończenie wiele i można je szybko znaleźć poprzez systematyczne przeszukiwanie zbioru liczb tej postaci. Należy w tym miejscu zwrócić uwagę na fakt, że wyznaczenie pierwiastków stopnia 2^m w ciele $\mathbb{F}_p$ wymaga znajomości rozkładu liczby $p-1$ na czynniki pierwsze. Możemy zatem wybierać jedynie te liczby $p = 2^{m+1}r + 1$, dla których znamy rozkład liczby r na czynniki pierwsze.

Taki dobór liczby p zapewnia, że wynik mnożenia wielomianów A i B przy użyciu transformaty Fouriera będzie identyczny z tym, który uzyskalibyśmy traktując te wielomiany jako elementy pierścienia $\mathbb{Z}[X]$ i mnożąc je w sposób tradycyjny. Przyjmijmy, że $C = A \cdot B$ jest dany z pomocą wyrażenia

$$C = \sum_{j=0}^{2n-1} c_j X^j.$$

Niestety otrzymane podczas obliczeń współczynniki c_j nie mogą być traktowane jako cyfry liczby $c = a \ \cdot b$, gdyż na ogół są one większe od liczby R. Wynika to z faktu, że mnożenie wielomianów nie uwzględnia przeniesienia. Przyjmijmy zatem, że s jest najmniejszą liczbą całkowitą, dla której $p \leq R^s$. Wtedy wielomian C i jego współczynniki możemy zapisać w postaci

$$C = \sum_{j=0}^{2n-1} \left(\sum_{k=0}^{s-1} c_{j,k} R^k \right) X^j,$$

gdzie $c_{j,k} < R$. Zamieniając kolejność sumowania otrzymujemy

$$C = \sum_{k=0}^{s-1} \left(R^k \sum_{j=0}^{2n-1} c_{j,k} X^j \right) = \sum_{k=0}^{s-1} C_k R^k,$$

gdzie współczynniki wielomianów C_k można już traktować jako cyfry odpowiadających im liczb. Przyjmując, że $\overline{c}_k$ odpowiada liczbie reprezentowanej przez C_k mamy

$$c = \overline{c}_0 + \overline{c}_1 R + \cdots + \overline{c}_{s-1} R^{s-1}.$$

Konieczność zsumowania liczb $\overline{c}_k$ nie ma istotnego wpływu na złożoność algorytmu, gdyż w praktycznych implementacjach liczba s przyjmuje najczęściej wartość 3 lub 4. To już jednak zależy od architektury sprzętu, na który projektowany jest algorytm. Mając na przykład do dyspozycji maszynę 32 bitową możemy przyjąć $R = 2^{32}$ i wybrać liczbę $p = 2^{32}r + 1$, która ma 96 bitów. Pozwala to na efektywne mnożenie liczb nie przekraczających $2^{2^{31}}$ i związane jest z koniecznością zsumowania jedynie trzech liczb $\overline{c}_k$.

W zależności od możliwości sprzętu, który ma wykonywać obliczenia, można rozważać jeszcze inne podejście do szybkiego mnożenia liczb w oparciu o ciała skończone. Polega ono na wykonaniu obliczeń w kilku mniejszych ciałach $\mathbb{F}_{p_i}$ i zastosowaniu twierdzenia chińskiego o resztach w celu wyłuskania właściwego wyniku. W tym celu należy znaleźć liczby pierwsze p_i, które spełniają następujące warunki.

1. $R^2 \cdot \lfloor \log_2 n + 1 \rfloor < \prod p_i$ - odpowiada za brak redukcji modulo $\prod p_i$.
2. $p_i = 2^{m+1}r_i + 1$ dla pewnego $2^{m+1} \geq 2n$ - odpowiada za wystarczającą liczbę pierwiastków z jedności.

Zaletą tego podejścia jest możliwość operowania na liczbach pojedynczej precyzji (takich, które mieszczą się w rejestrze maszyny). Niestety pewne ograniczenie w zastosowaniu tej metody stanowi warunek 2. W istotny bowiem sposób utrudnia on implementację tej metody dla długich liczb na maszynach mających niewielkie rejestry (na przykład 8 bitowe).

4.2 Szybka realizacja arytmetyki w pierścieniu reszt

Teraz pokażemy w jaki sposób można efektywnie realizować arytmetykę modulo pewna liczba M przy założeniu, że $(M, R) = 1$. Założenie to jest na ogół spełnione podczas realizacji obliczeń kryptograficznych. W takich bowiem algorytmach jak RSA, DSA i DH moduły są bądź dużymi liczbami pierwszymi (DSA i DH), bądź ich iloczynami (RSA). Natomiast za podstawę systemu reprezentacji liczb przyjmuje się na ogół potęgę liczby 2.

Lemat 3 Załóżmy, że liczby $(M, R) = 1$, $a, b < M < R^n$, $q = -M^{-1} \mod R^n$ i

$$\begin{aligned} t_1 &= a \cdot b \\ t_2 &= t_1 \mod R^n \\ t_3 &= t_2 \cdot q \\ t_4 &= t_3 \mod R^n \\ t_5 &= t_4 \cdot M \\ t &= (t_1 + t_5)/R^n. \end{aligned}$$

Wtedy spełniony jest jeden z poniższych warunków

$$abR^{-n} \mod M = t \qquad \text{lub} \qquad abR^{-n} \mod M = t - M.$$

Dowód: Dla dowodu lematu wystarczy wykazać, że $t \equiv abR^{-n} \mod M$ i $t < 2M$. Ze wzorów przedstawionych w treści wynika równość $t_4 = -abM^{-1} \mod R^n$. W związku z tym liczba t_5 spełnia następujące warunki

$$\begin{aligned} t_5 &\equiv -ab \mod R^n \\ t_5 &\equiv 0 \mod M. \end{aligned}$$

To oznacza, że $t_1 + t_5 \equiv 0 \mod R^n$ i dzielenie przez R^n wymaga jedynie usunięcia najmłodszych n cyfr, które są zerami. Z drugiej strony mamy natomiast $t_1 + t_5 \equiv t_1 \mod M$, co bezpośrednio prowadzi do związku $t = (t_1 + t_5)/R^n \equiv abR^{-n} \mod M$. Aby wykazać, że $t < 2M$ zauważmy, że $t_4 < R^n$ gdyż jest wynikiem redukcji modulo R^n. W związku z tym $t_5 = t_4 M < R^n M$. Ponadto wiemy, że $t_1 < M^2$, gdyż $a, b < M$. Ostatecznie otrzymujemy więc warunek

$$t = \frac{t_1 + t_5}{R^n} < \frac{M^2 + R^n M}{R^n} < \frac{2R^n M}{R^n} = 2M,$$

co kończy dowód. ■

Poniższe twierdzenie pokazuje w jaki sposób działanie wprowadzone w lemacie 3 wiąże się z operacjami wykonywanymi w sposób tradycyjny.

Twierdzenie 3 Jeżeli $(M, R) = 1$, a działania w pierścieniach $R_1 = \langle \mathbb{Z}_M, 0, 1, +, -, \cdot \rangle$ i $R_2 = \langle \mathbb{Z}_M, 0, R^n, +, -, \odot \rangle$ określone są następująco

$$\begin{aligned} a \pm b &= a \pm b \mod M \\ a \cdot b &= ab \mod M \\ a \odot b &= abR^{-n} \mod M, \end{aligned}$$

to pierścienie te są izomorficzne.

Dowód: Definiujemy przekształcenie $h : R_1 \to R_2$ jako

$$h(x) = xR^n \mod M.$$

Jest ono różnowartościowe i na, gdyż liczby M i R są względnie pierwsze. Aby dokończyć dowód wystarczy zatem pokazać, że zachowuje działania

1. $h(0) = 0$, $h(1) = R^n$,
2. $h(a \pm b) = (a \pm b)R^n \mod M = (aR^n \pm bR^n) \mod M = h(a) + h(b)$,
3. $h(a \cdot b) = abR^n \mod M = (aR^n bR^n)R^{-n} \mod M = h(a) \odot h(b)$.

To kończy dowód. ■

5 Asymptotycznie szybka arytmetyka w pierścieniu formalnych szeregów potęgowych

W tej części będziemy rozważali zagadnienie mnożenia i dzielenia formalnych szeregów potęgowych o współczynnikach całkowitych. W naszych rozważaniach będziemy przyjmowali, że interesuje nas jedynie n współczynników reprezentacji takiego szeregu. Jeżeli chodzi o mnożenie takiej skończonej reprezentacji szeregu potęgowego, to nie różni się ona od mnożenia wielomianów. Trzeba jedynie dobrać ciało $\mathbb{F}_p$ w którym będą przeprowadzane obliczenia. Jeżeli przez R oznaczymy ograniczenie górne na wartość bezwzględną współczynników reprezentacji, to liczba pierwsza definiująca ciało $\mathbb{F}_p$ powinna spełniać poniższe warunki.

1. $4R^2 \cdot \lfloor \log_2 n + 1 \rfloor < p$ - odpowiada za brak redukcji modulo p podczas obliczeń.
2. $p = 2^{m+1}r+1$ dla pewnego $2^{m+1} \geq 2n$ - odpowiada za wystarczającą liczbę pierwiastków z jedności.

Podobnie, jak w przypadku algorytmu mnożenia liczb całkowitych można zastąpić obliczenia w ciele $\mathbb{F}_p$ serią obliczeń w mniejszych ciałach $\mathbb{F}_{p_i}$. Wtedy liczby p_i muszą spełniać następujące warunki.

1. $4R^2 \cdot \lfloor \log_2 n + 1 \rfloor < \prod p_i$ - odpowiada za brak redukcji w wyniku obliczeń.
2. $p_i = 2^{m+1}r_i+1$ dla pewnego $2^{m+1} \geq 2n$ - odpowiada za wystarczającą liczbę pierwiastków z jedności.

Jeżeli ograniczenie na wartość bezwzględną współczynników R jest dość duże, to bardziej opłacalne jest stosowanie drugiej metody mnożenia. Przy czym liczby p_i warto, jeżeli jest to możliwe, dobierać w taki sposób, aby mieściły się rejestrze procesora.

Jeżeli chodzi o dzielenie szeregów potęgowych, to istnieje bardzo prosta metoda pozwalająca wyznaczać szereg odwrotny. Jest to metoda iteracyjna Newtona podczas której wykonywane są jedynie operacje odejmowania i mnożenia szeregów. Dużą jej zaletą jest szybka zbieżność, która nie zależy od danych wejściowych. Podczas każdej iteracji precyzja wyniku zwiększa się dwukrotnie. Oznacza to konieczność wykonania jedynie około $\log n$ iteracji, aby wyznaczyć szereg odwrotny z dokładnością do n współczynników. Jeżeli mamy dany szereg

$$A = \sum_{j=0}^{n-1} a_j X^j,$$

którego pierwszy wyraz jest odwracalny, to zaprezentowana poniżej procedura pozwala na wyznaczenie szeregu odwrotnego.

1. $m \leftarrow 0$;
2. $B \leftarrow \frac{1}{a_0}$;
3. **while** $2^m < n$ **do**
3.1. $\quad B \leftarrow 2B - B^2 \sum_{j=0}^{2^m} a_j X^j$;
3.2. $\quad m \leftarrow m + 1$;
4. **return** B;

6 Podsumowanie

W artykule przedstawiono dokładny opis zastosowania dyskretnej transformaty Fouriera do szybkiego mnożenia wielomianów. Zaprezentowana metoda została później adoptowana do realizacji asymptotycznie szybkiego mnożenia w pierścieniu liczb całkowitych. Pokazano również w jaki sposób można realizować szybkie mnożenie w szerokiej klasie pierścieni reszt modulo. W ostatniej części połączono szybkie przekształcenie Fouriera z własnościami pierścieni p-adycznych w celu realizacji szybkiego algorytmu znajdowania odwrotności formalnego szeregu potęgowego.