Wer hat eigentlich die Multiplikation erfunden?

1 Multiplikation, was ist das?

Wenn man über Algorithmen spricht – und die Multiplikation von natürlichen Zahlen ist ein Musterbeispiel dafür – dann orientieren sich Informatiker gerne an einem Goethe-Zitat:

Das WAS bedenke, mehr bedenke WIE.
J.W. von Goethe, Faust II

WAS Multiplikation eigentlich ist, macht man sich am besten an einem aus dem Leben gegriffenen Beispiel klar: Man geht drei Mal in den Keller und holt jedes Mal vier Flaschen Wein (zwei in jeder Hand) rauf. Wie viele Flaschen sind das insgesamt? Jedes Mal, wenn man wieder mit vier Flaschen aus dem Keller kommt, addiert man diese zu den bereits vorhandenen: Multiplikation ist also nichts anderes, als eine Abkürzung für fortgesetzte Addition. Und weil Menschen zu allen Zeiten bemüht waren, nicht nur körperliche sondern auch geistige Arbeit zu minimieren, hat man auch seit jeher versucht, diese Abkürzung möglichst effizient zu gestalten. WIE man das aber am besten macht, ist gar keine so einfache Frage. Es wird bereits seit über 4000 Jahren daran gearbeitet.

Abbildung 1: Die Multiplikation als fortgesetzte Addition: $3 \cdot 4 = 4+4+4 = 12$

Wenn man nach den geschichtlichen Ursprüngen sucht, dann kann man der Binsenweisheit folgen „Lasst uns erst einmal betrachten, wie es die alten Griechen machten“. Tatsächlich findet man im siebten Buch der Elemente von Euklid (ca. 365 bis 300 v. Chr.) in Definition 15 eine Multiplikationsvorschrift [Euk]. Wörtlich übersetzt steht da:

"Man sagt, dass eine Zahl eine Zahl vervielfältige, wenn die zu vervielfältigende so oft zusammengesetzt wird, wie viel Einheiten jene enthält, und so eine Zahl entsteht!"

Soll beispielsweise die Zahl drei die Zahl vier vervielfältigen $(3 \cdot 4)$, so wird 4 so oft zusammengesetzt (addiert), wie die in 3 enthaltenen Einheiten angeben, also $4+4+4$. So entsteht eine Zahl, nämlich das Ergebnis 12.

Praktisch alle alten Kulturen kannten die Multiplikation [Tsc03]. Beispielsweise die Babylonier (mathematische Keilschrifttexte um 2000 v. Chr.), die Ägypter (Papyrus Rhind aus dem 19. Jahrhundert v. Chr.), natürlich die Griechen und die Römer, auch die Chinesen (Liu Hui, um 200) und Inder (Aryabhatiya, um 500), die Araber (al-Karagi, um 900) die Italiener (Leonardo von Pisa, 1170 bis 1240), die Deutschen (Adam Ries, 1492 bis 1559) und, und, und.

Kluge Leute haben also die Multiplikation an verschiedenen Stellen der Welt unabhängig voneinander immer wieder neu erfunden. Die eigentliche Frage lautet, ob das Problem der Multiplikation überhaupt schon abschließend gelöst werden konnte.

2 Die alten Römer hatten es nicht leicht

Im römischen Reich und weiten Teilen Europas hat man bis ins Mittelalter hinein das römische Ziffernsystem verwendet. Es basiert auf Zehnerpotenzen, die man zusätzlich mit 5 multiplizieren konnte. Die zugehörigen Zahlzeichen sind in Abb. 2 aufgelistet. Bei mehrstelligen Zahlen werden die erforderlichen Zahlzeichen mit von links nach rechts abfallenden Werten nebeneinander geschrieben. Der Zahlenwert der gesamten Zahl ergibt sich durch Aufaddieren der Zahlenwerte der einzelnen Zahlzeichen. Stellenabhängige Werte und die Null kennt das römische Ziffernsystem nicht. Als Besonderheit kommt hinzu, dass zur Reduktion der Zahlenlänge ein Zeichen **I**, **X** und **C** vom rechts daneben stehenden Zeichen abgezogen wird, wenn dieses um den Faktor 5 oder 10 größer ist. Für 9 schreibt man also nicht **VIIII** sondern kürzer **IX** und für 900 schreibt man **CM**. Aber **XM** für 990 ist nicht zulässig.

M	D	C	L	X	V	I

Abbildung 2: Die Grundziffern der römischen Zahlen: I=1, V=5, X=10, L=50, C=100, D=500 und M=1000. Noch größere Zahlen wurden durch Rahmen und Überstriche gekennzeichnet. Beispielsweise bedeutet $\overline{\text{M}}$ eine Million.

Für die praktische Ausführung von Multiplikationen hat man damals *Rechentücher* [Ger94] verwendet. Bei diesen waren in der obersten Zeile die Zahlsymbole eingetragen. Darunter gab es Felder, in die man Marken (*Rechenpfennige*) legen konnte, die angaben, wie oft das betreffende Symbol zu zählen war.

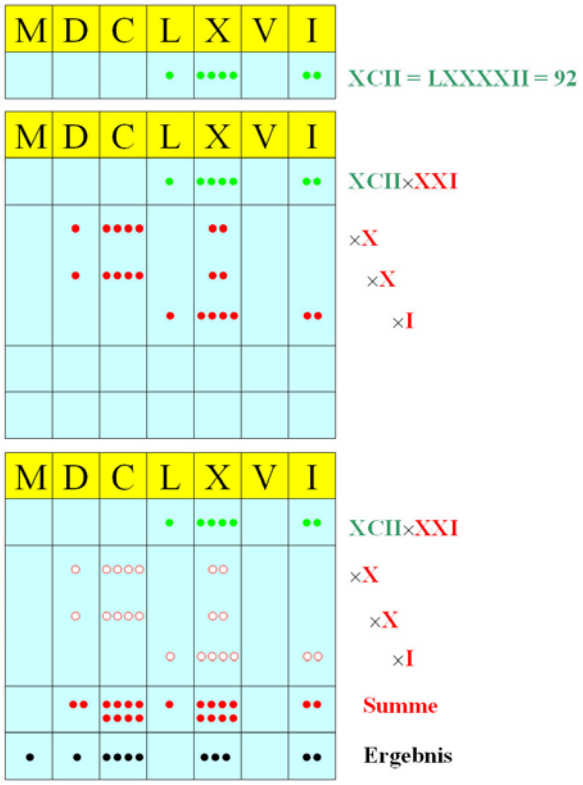

Abbildung 3: Multiplikation mit dem Rechentuch.

Abbildung 3 illustriert die Verwendung des Rechentuchs anhand des Beispiels 92·21= 1932. Zunächst wird der größere Faktor, also XCII=92 mit Marken in die erste Reihe gelegt. Die abkürzende Notation wird dabei aufgehoben, man legt also LXXXXII statt XCII. Nun werden diese Marken der Reihe nach mit den Zahlzeichen des zweiten Faktors XXI=21 multipliziert, also mit X, dann nochmals mit X und schließlich mit I. Man verwendet einfach das Distributivgesetz und rechnet: 92·(10 + 10 + 1). Die Zwischenergebnisse der Multiplikationen mit den einzelnen Stellen werden durch Auflegen von Marken in die jeweils folgenden Zeilen eingetragen. Die Multiplikation mit I ist trivial: Man kopiert einfach die Marken, die der zu multiplizierenden Zahl entsprechen. Eine Multiplikation mit X (C, M) entspricht der Verschiebung einer Marke um zwei (vier, sechs) Felder nach links. Bei der Multiplikation mit V sind zwei Fälle zu unterscheiden: Ist der Multiplikand eine Zehnerpotenz, so werden die Rechensteine um eine Stelle nach links verschoben. Ist der Multiplikand dagegen V, L oder D, so werden eine Marke in das betreffende Feld und zwei weitere in das links benachbarte Feld (also X, C oder M) kopiert. So wird aus V·V die Zahl XXV. Nach Verarbeitung sämtliche Stellen sammelt man spaltenweise alle Marken in der untersten Zeile auf. Das entspricht der Addition der Zwischenergebnisse. Sodann fasst man dann in jedem Feld so viele Marken zusammen, wie man für das nächsthöhere Zeichen benötigt. Im obigen Beispiel folgt so das Ergebnis, nämlich MDCCCCXXXII, bzw. verkürzt MCMXXXII = 1932.

3 Von Ägyptern, russischen Bauern und Pippi Langstrumpf

Die ägyptische Multiplikation

Die Ägypter kannten bereits vor Jahrtausenden eine Multiplikationsmethode, die in mancher Hinsicht nicht schlechter war als die heute verwendete [Ger94]. Hinweise darauf findet man auf dem berühmten Papyrus Rhind.

Die antike Methode funktioniert wie folgt: Zunächst schreibt man den größeren Faktor auf, im Beispiel $92 \cdot 21$ also die Zahl 92; daneben schreibt man eine 1. Nun verdoppelt man in den folgenden Zeilen jeweils die Zahlen der vorhergehenden Zeile. In der zweiten Zeile steht dann also $2 \cdot 92 = 184$ und daneben $2 \cdot 1 = 2$. So fährt man fort, bis die in der zweiten Spalte entstehende Zahl (offensichtlich eine Zweierpotenz) gerade noch kleiner ist als der kleinere der beiden Faktoren, hier also 21.

Die wesentlichen Vorteile des Verfahrens sind, dass das Verdoppeln eine sehr einfache Operation ist und dass es auch mit primitiven Ziffernsystemen wie dem römischen funktioniert, die keine Stellenwerte kennen, wie wir das vom Dezimalsystem gewöhnt sind. Das Verfahren sieht dann für $92 \cdot 21$ so aus:

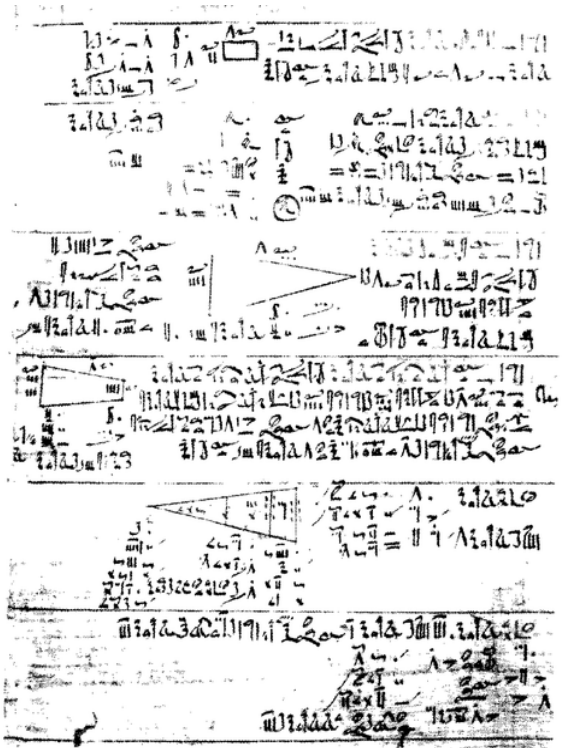

Abbildung 4: Ausschnitt aus dem fast 4000 Jahre alten ägyptischen Papyrus Rhind.

Mit arabischen Ziffern:				Mit römischen Zahlen:	
$1 \cdot 92$	**$= 92$**	**$1 = 2^0$**		**XCII**	**I**
$2 \cdot 92$	$= 184$	$2 = 2^1$		CLXXXIV	II
$4 \cdot 92$	**$= 368$**	**$4 = 2^2$**		**CCCLXVIII**	**IV**
$8 \cdot 92$	$= 736$	$8 = 2^3$		DCCXXXVI	VIII
$16 \cdot 92$	**$=1472$**	**$16 = 2^4$**	fertig, da 32>21	**MCDLXXII**	**XVI**

Die Prozedur endet in der fünften Zeile, weil da in der zweiten Spalte die Zahl 16 auftritt und die bei der nächsten Verdopplung entstehende Zahl 32 bereits größer als 21 wäre.

Im nächsten Schritt sucht man diejenigen Zahlen in der rechten Spalte auf, deren Summe gerade 21 ergibt und markiert die entsprechenden Zeilen – im obigen Beispiel durch blaue Farbe. Dies funktioniert immer auf eindeutige Weise. Schließlich addiert man die Zahlen in der ersten Spalte aller markierten Zeilen und erhält das korrekte Ergebnis 1932. Im Detail wurde folgendermaßen gerechnet:

$$92 \cdot 21 = 92 \cdot (1 + 4 + 16) = 1 \cdot 92 + 4 \cdot 92 + 16 \cdot 92 = 92 + 368 + 1472 = 1932 = \text{MCMXXXII}$$

Die wesentliche Idee der Methode ist, dass die Zahl 21 in eine Summe aus Zweierpotenzen zerlegt wurde: $21 = 1 + 4 + 16 = 2^0 + 2^2 + 2^4$ und dass außerdem immer nur verdoppelt wird. Man muss also im Zehnersystem das „kleine Einmaleins“ nicht beherrschen, um auf diese Weise multiplizieren zu können. Immerhin besteht das kleine Einmaleins aus einer Tabelle mit 50 größtenteils zweistelligen Zahlen, darunter so schlimme wie $7 \cdot 8 = 56$, die man mühsam auswendig lernen muss.

Auch mit den römischen Zahlen ist Verdoppeln unproblematisch, so dass intelligentere Römer, die mit der ägyptischen Multiplikation umgehen konnten, kein Rechentuch benötigten.

Die russische Bauernmultiplikation

Die russische Bauernmultiplikation ist mit der ägyptischen Multiplikation eng verwandt. In die erste Zeile wird wieder links der größere Faktor geschrieben, aber rechts jetzt nicht 1, sondern der kleinere der beiden Faktoren. Nun wird wieder zeilenweise vorgegangen. Dabei wird die linke Zahl immer verdoppelt, die rechte aber halbiert. Der bei Halbierung einer ungeraden Zahl auftretende „Rest 1“ wird dabei einfach weggelassen. Für $92 \cdot 21$ folgt damit:

92	**21**	
184	10	
368	**5**	
736	2	
1472	**1**	$92 + 368 + 1472 = 1932$

Man markiert jetzt alle Zeilen, in denen auf der rechten Seite eine ungerade Zahl steht (die Ausgangszahl zählt dabei auch mit) und addiert wie bei der ägyptischen Multiplikation die in den markierten Zeilen stehenden Zahlen in der linken Spalte.

Man könnte denken, dass die russischen Bauern diese Methode bevorzugt haben, weil nach russischem Geschmack Halbieren einfacher ist als Verdoppeln. Die Bauern waren aber tatsächlich schlauer als die Ägypter: Erstens muss man bei der russischen Methode nicht prüfen, ob bei der Verdopplung der Zahlen in der rechten Spalte das Ergebnis schon zu groß geworden ist, sondern das Verfahren endet einfach, sobald eine 1 erreicht ist. Zweitens ergeben sich die Markierungen der Zeilen sozusagen „von selbst“, wenn nämlich das Ergebnis der Halbierung ungerade ist. Bei der ägyptischen Multiplikation muss man dagegen alle Potenzen von 2 in der rechten Spalte probeweise addieren, um genau die zu finden, die in der Summe tatsächlich den zweiten Faktor ergeben.

Tatsächlich entspricht das fortgesetzte Halbieren der Umwandlung des Faktors 21 in eine Zahldarstellung im Zweier- oder *Binärsystem*. Man erkennt dies, wenn man die Basis des Binärsystems, also die Zahl 2, gemäß des *Horner'schen Schemas* ausklammert:

$$21 = 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = (((1 \cdot 2 + 0) \cdot 2 + 1) \cdot 2 + 0) \cdot 2 + 1$$

An den Koeffizienten 0 bzw. 1, mit denen die Zweierpotenzen multipliziert werden, liest man ab, wie die umgewandelte Zahl im Binärsystem lautet: $21_{\text{dez}} = 10101_{\text{bin}}$

Dividiert man den obigen Ausdruck für 21 fortgesetzt durch 2, so folgt:

$21 / 2 = 10$	Rest 1	oder explizit:	$[(((1 \cdot 2 + 0) \cdot 2 + 1) \cdot 2 + 0) \cdot 2 + 1] / 2$	$= ((1 \cdot 2 + 0) \cdot 2 + 1) \cdot 2$	Rest 1
$10 / 2 = 5$	Rest 0		$[((1 \cdot 2 + 0) \cdot 2 + 1) \cdot 2] / 2$	$= (1 \cdot 2 + 0) \cdot 2 + 1$	Rest 0
$5 / 2 = 2$	Rest 1		$[(1 \cdot 2 + 0) \cdot 2 + 1] / 2$	$= 1 \cdot 2$	Rest 1
$2 / 2 = 1$	Rest 0		$[1 \cdot 2] / 2$	$= 1$	Rest 0
$1 / 2 = 0$	Rest 1		$1 / 2$	$= 0$	Rest 1

Man erkennt, dass für ungerade Zahlen die Divisionsreste 1 sind und für gerade Zahlen 0. Diese Divisionsreste liefern, wie die explizite Rechnung durch Ausklammern der Basis 2 zeigt, die binären Stellen von 21 in aufsteigender Reihenfolge. Als ersten Divisionsrest erhält man demnach das niedrigstwertige Bit der Binärzahl und als letzten das höchstwertige.

Nach diesem Verfahren lernen Informatik-Studenten im ersten Semester, wie man Dezimalzahlen in Binärzahlen umwandelt. Die Methode ist nicht nur für das Dezimalsystem anwendbar, sondern für alle Umwandlungen aus beliebigen Zahlensystemen in jedes andere. Man muss einfach nur fortgesetzt durch die Basis des Zielsystems dividieren und die Divisionsreste als Ziffern im Zielsystem interpretieren.

Die russische Bauernmultiplikation entspricht damit weitgehend der Multiplikation von Binärzahlen, so wie sie auch in Computern ausgeführt wird.

Pippi Langstrumpf und die Plutimikation

Und wie kommt die passionierte Querdenkerin Pippi Langstrumpf ins Spiel? Als sie in der Schule das kleine Einmaleins auswendig lernen sollte, wollte sie das gar nicht einsehen. Unter Kennern wird vermutet, dass Sie während ihrer Reisen auf der Hoppetosse mitbekommen hatte, dass es mit der russischen Bauernmultiplikation auch einfacher geht. Daher beschloss sie „Plutimikation ist nicht mein Ding“, denn der Schulalgorithmus ist ja eigentlich viel zu schwierig.

Abbildung 5: Pippi Langstrumpf, Plutimikation war nicht ihr Ding.

4 Nach Adam Ries . . .

Vom Rechentuch zum Schulalgorithmus

Im Mittelalter begann sich, angetrieben durch den Handel mit der arabischen Welt, das *Zehnersystem* durchzusetzen, da man mit diesem viel effizienter rechnen, insbesondere multiplizieren konnte als mit den römischen Ziffern. Einer der Wegbereiter war *Leonardo von Pisa* (1170 bis 1240), besser bekannt unter dem Namen *Fibonacci*. Im 15. Jahrhundert hatten sich die arabischen Ziffern in Deutschland zwar schon längst durchgesetzt, man multiplizierte aber immer noch „auf der Linie“ mit diversen Varianten von Rechentüchern, Rechenbrettern und dem auf ähnlichen Prinzipien basierenden, um 1100 v. Chr. im Orient erfundenen *Abakus*. Auch Martin Luther hat das noch so gelernt. Mit Beginn des 16. Jahrhunderts wurde dann Adam Ries (nicht Riese) als „Churfürstlich Sächsischer Hofarithmetikus“ durch seine populären Rechenbücher zum sprichwörtlichen Rechenmeister der Deutschen [Rie]. Durch ihn wurde der auch heutzutage noch in der Grundschule gelehrte schriftliche Multiplikationsalgorithmus Allgemeingut.

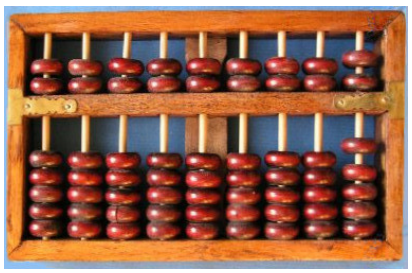

Abbildung 6: Ein mittelalterlicher Abakus. Die unteren Perlen repräsentieren Einer, die oberen Fünfer. Die senkrechten Spalten entsprechen den Stellen im Zehnersystem.

Ist beispielsweise die Multiplikationsaufgabe $92 \cdot 21$ auszuführen, so rechnet man nach Adam Ries:

$$92 \cdot 21 = 1932$$

$$\begin{array}{r} 184 \\ 92 \\ \hline 1932 \end{array}$$

Abbildung 7: Adam Ries und sein Rechenbuch aus dem Jahre 1522. Auf dem Buch ist ein damals verwendetes Rechenbrett abgebildet.

Wie schnell geht das eigentlich?

Zählt man die für die Multiplikation langer Zahlen erforderliche Anzahl der elementaren Multiplikationen einzelner Ziffern, so findet man rasch heraus, dass jede Ziffer des ersten Faktors mit jeder Ziffer des zweiten multipliziert werden muss. Haben beide Faktoren jeweils n Ziffern, so sind also n^2 Elementarmultiplikationen erforderlich. Dazu kommen noch einige Additionen, die aber sehr schnell ausführbar sind und daher bei der Abschätzung des Rechenaufwands vernachlässigt werden können. Natürlich können beide Faktoren unterschiedliche Stellenzahlen haben, der Einfachheit halber kann man aber annehmen, dass beide gleich lang sind, da sich dadurch an der Betrachtung des Rechenaufwands nichts Wesentliches ändert. Bei der Aufgabe $92 \cdot 21$ ist $n=2$, man benötigt also nur vier Elementarmultiplikationen. Für $n=10$ sind es aber schon 100 und für $n=100$ bereits $10\,000$. Wie man sieht, steigt der Arbeitsaufwand mit höheren Stellenzahlen sehr rasch an. Nun ist es aber so, dass Zahlen mit einigen hundert Stellen in der Praxis durchaus wichtig sind, beispielsweise für die effiziente Verschlüsselung von Nachrichten, so dass schnellere Multiplikationsverfahren sehr gefragt sind.

Der Aufwand für eine Multiplikation steigt also beim Standardverfahren quadratisch mit der Stellenzahl n der Faktoren an, nämlich proportional zu n^2. Man kann leicht zeigen, dass dies für die Ägyptische Methode und die russische Bauernmultiplikation auch nicht besser ist. Zwar muss man immer nur mit 2 multiplizieren, dafür sind aber die Stellenzahlen im Binärsystem um den Faktor $\mathrm{ld}(10) \approx 3.3219$ größer als im Zehnersystem. Dabei ist ld der Zweierlogarithmus mit der Basis 2.

5 Multiplikation auf Umwegen

Logarithmen

Manchmal ist der direkte Weg zur Lösung einer Aufgabe langwierig und/oder schwierig, so dass gelegentlich ein Umweg bequemer zum Ziel führt. Nach Einführung der *Logarithmen* in 1614 durch John Napier bot sich eine solche Gelegenheit für Multiplikationsverfahren. Die Logarithmusfunktion ist die Umkehrfunktion der Potenzfunktion: Aus $b^a = c$ folgt $\log_b c = a$. Betrachtet man beispielsweise die Beziehung $10^3 = 1000$, so liefert der *Zehnerlogarithmus* $\log(1000) = 3$ den Exponenten 3, mit dem man die Basis 10 potenzieren muss, damit man 1000 erhält. Wählt man anstelle der Basis $b=10$ die Basis $b=2$, so erhält man den auch im vorigen Kapitel schon verwendeten *Zweierlogarithmus*. Dieser liefert beispielsweise $\mathrm{ld}(256) = 8$, also den Exponenten 8, mit dem man die Basis 2 potenzieren muss, damit man 256 erhält.

Logarithmen haben die interessante Eigenschaft, dass $\log(a \cdot b) = \log(a) + \log(b)$ gilt. Angenommen, die Logarithmusfunktion wäre viel einfacher zu berechnen als die Multiplikation, dann liegt es nahe, wie in Abbildung 8 illustriert, zunächst die Logarithmen von a und b zu ermitteln (wie auch immer das geht) und diese zu addieren: $s = \log(a) + \log(b)$. Aus dem Zwischenergebnis s folgt das Resultat der Multiplikation durch „Delogarithmieren“ also durch Berechnen von 10^s.

Insgesamt hat man die folgende Identität ausgenützt: $a \cdot b = 10^{\log(a) + \log(b)}$

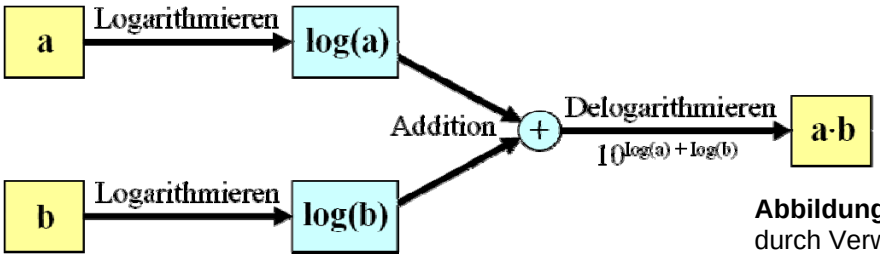

Abbildung 8: Prinzip des Multiplizierens durch Verwendung von Logarithmen.

Logarithmentafeln

Logarithmen oder Potenzen von 10 zu berechnen ist aber beileibe nicht einfacher als Multiplizieren, ganz im Gegenteil. Ein Vorteil ergibt sich aber dennoch, da man die benötigten Werte als Tabelleneinträge vorab berechnen und in einer *Logarithmentafel* auflisten kann. Das Logarithmieren und Delogarithmieren reduziert sich damit auf Nachschlagen in einer Logarithmentafel.

Möchte man beispielsweise $92 \cdot 21$ über den Umweg des Logarithmierens berechnen, so sucht man zunächst die Logarithmen von 92 und 21 in einer Logarithmentafel auf, bildet daraus die Summe s und berechnet schließlich das Ergebnis 10^s:

$\log(92) \approx 1.96379$

$\log(21) \approx 1.32222$

$s = 1.96379 + 1.32222 = 3.28601$

$92 \cdot 21 \approx 10^{3.28601} \approx 1932.01$

Zu beachten ist, dass man nur einen Näherungswert erhält; die Anzahl der korrekten Dezimalstellen hängt von der Stellenzahl der Logarithmentafel ab.


MIRIFICI
Logarithmorum
Canonis descriptio,
Ejusque usus, in utraque
Trigonometria, ut etiam in
omni Logistica Mathematica,
Authore ac Inventore,
IOANNE NEPERO,
EDINBVRGI,
Ex officinâ ANDREÆ HART

Abbildung 9: Die erste Logarithmentafel von John Napier aus 1624.

Rechenschieber

Schon wenige Jahre nach der Einführung von Logarithmentafeln wurde die Idee des Rechenschiebers geboren: Man verwendete zwei bewegliche Lineale mit logarithmischer Skalenteilung. Durch Aneinanderlegen der Skalen, entsprechend der Addition von Längen, konnte dann sehr viel schneller als durch Nachschlagen in Logarithmentafeln multipliziert werden. Als Erfinder des Rechenschiebers gilt *William Oughtred*, der 1622 das erste Modell mit beweglichen Skalen vorgestellt hatte.

Multiplikationen und Divisionen, aber auch Berechnungen mit Wurzeln und Winkelfunktionen sowie zahlreiche weitere Operationen können mithilfe zusätzlicher Skalen auf einem Rechenschieber mit etwas Übung sehr schnell ausgeführt werden, durchaus vergleichbar mit der Handhabung heutiger Taschenrechner. Allerdings liefern Rechenschieber wie auch Logarithmentafeln nur die Ziffernfolgen des Ergebnisses. Die Größenordnung muss man durch eine Überschlagsrechnung selbst ermitteln.

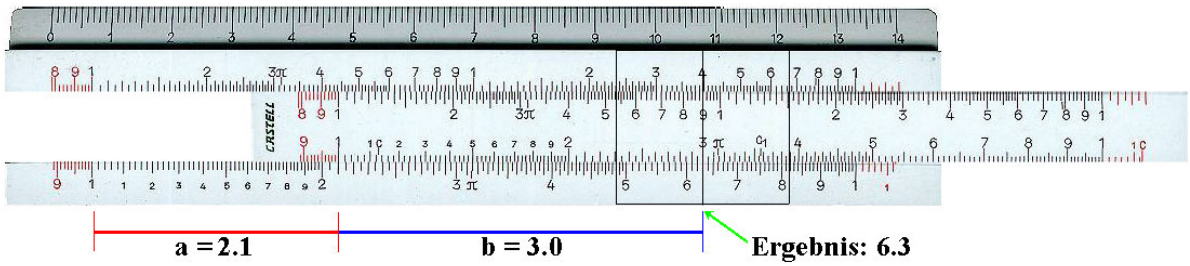

Abbildung 10: Beispiel für einen Schulrechenschieber. Zur Berechnung der Aufgabe $2.1 \cdot 3.0 = 6.3$ wird die Zahl 2.1 auf der feststehenden unteren Skala gesucht. Nun wird die bewegliche Zunge so nach rechts verschoben, dass deren 1 exakt über der Teilung 2.1 auf der unteren Skala steht. Anschließend verschiebt man den beweglichen Läufer so weit nach rechts, bis die darauf befindliche senkrechte Haarlinie exakt über dem Skalenstrich 3.0 der oberen Skala steht. Die Haarlinie des Läufers zeigt dann auf der unteren Skala das Ergebnis 6.3 an.

350 Jahre lang war der Rechenschieber weltweit in einer computerfreien Zeit das wichtigste Recheninstrument überhaupt. Ingenieuren diente er als unverzichtbares Werkzeug, so lange

drei exakte Stellen ausreichend waren. Auch das Münchner Olympiastadion wurde noch weitgehend computerfrei errichtet. Nach der Erfindung des Taschenrechners in 1969 dauerte es dann noch sechs Jahre, bis der Rechenschieber in deutschen Schulen offiziell durch den Taschenrechner abgelöst wurde.

6 Zwischenspiel: Multiplizieren und Quadrieren

Quadrieren statt Multiplizieren

Wenn Multiplizieren schon so schwierig ist, dann könnte man es ja mal mit Quadrieren versuchen. Tatsächlich ist es eine interessante Frage, ob das Quadrieren einer Zahl wesentlich schneller ausgeführt werden kann als die Multiplikation. Durch Abwandlungen der bekannten Algorithmen ist Quadrieren in der Tat fast doppelt so schnell möglich wie Multiplizieren, wie beispielsweise D. Zuras [Zur94] gezeigt hat. Allerdings sind hier prinzipielle Grenzen gesetzt, wie folgende einfache Überlegung zeigt. Die Multiplikation zweier Zahlen a und b lässt sich nämlich auch folgendermaßen durch zwei Quadrate darstellen, was sich durch Ausmultiplizieren der Klammern sofort nachvollziehen lässt:

$$a \cdot b = [(a + b)^2 - (a - b)^2]/4$$

Das Ersetzen der Multiplikation durch zwei Quadrate impliziert jedoch, dass Quadrier-Algorithmen prinzipiell nicht schneller als doppelt so schnell wie Multiplikations-Algorithmen sein können. Denn wenn es einen schnelleren Quadrieralgorithmus gäbe, so könnte man nach obiger Formel die Multiplikation eben durch diesen schnelleren Algorithmus ausdrücken. Bezeichnet man die Ausführungszeiten mit T, dann gilt folglich die Beziehung:

$$T_{\text{Multiplizieren}} \leq 2T_{\text{Quadrieren}}$$

Die Methode „Quadrieren statt Multiplizieren“ gemäß obiger Formel wird in *Analogrechnern* seit jeher praktiziert, da Quadrierer wesentlich einfacher als Hardware realisiert werden können als Multiplizierer. Man nützt dazu aus, dass man mit Netzwerken aus Dioden leicht elektronische Schaltungen mit parabelförmigen Kennlinien der Art $y=x^2$ entwickeln kann.

Multiplikation in Babylon

Erstaunlicherweise ist die Multiplikation mithilfe von *Quadratzahlen* nach der Formel $a \cdot b = [(a + b)^2 - (a - b)^2]/4$ die älteste bislang bekannt gewordene systematische Multiplikationsmethode. In sumerischen und babylonischen Keilschrifttafeln fand man Tabellen von Quadratzahlen [Con00] und etliche Berechnungsbeispiele, u.a. für die Konstruktion von Bewässerungskanälen. Zur Ausführung einer Multiplikation, etwa $32 \cdot 21$, berechnete man zunächst $32+21=53$ sowie $32-21=11$. Anschließend suchte man auf der tönernen Keilschrift-Tabelle (siehe Abbildung 11) die zugehörigen Quadratzahlen, also $53^2=2809$ sowie $11^2=121$. Subtraktion der beiden Quadratzahlen ergibt $2809-121=2688$. Division durch 4 oder, was einfacher ist, zweimaliges Halbieren liefert dann das Ergebnis 672. Die Babylonier arbeiteten übrigens mit einem Zahlensystem auf der Basis 60, da die 60 sehr viele Teiler besitzt, was die Division wesentlich erleichtert. Ein Relikt aus diesen antiken Tagen ist die Einteilung des Tages in 24 Stunden und das bei Kaufleuten früher gebräuchliche Rechnen im Zwölfersystem. Die Bezeichnung *Dutzend* für *Zwölf* erinnert heute noch daran.

Abbildung 11: Eine ca. 4000 Jahre Jahre alte babylonische Lehmtafel mit Quadratzahlen.

Geometrische Multiplikation mit Parabeln

Eine Weiterführung des Gedankens „Quadrieren statt Multiplizieren“ legt ein geometrisches Multiplikationsverfahren unter Verwendung einer um die Y-Achse symmetrischen Parabel $y = x^2$ nahe. Möchte man zwei Zahlen a und b miteinander multiplizieren, so setzt man zunächst b in die Parabelgleichung $y=x^2$ ein; dies ergibt den Punkt $P_1(b, b^2)$ auf dem rechten Ast der Parabel. Sodann setzt man $-a$ ein und erhält $P_2(-a, a^2)$ auf dem linken Ast. Das Multiplikationsergebnis $a \cdot b$ ist dann die Y-Komponente des Schnittpunkts der durch die beiden Punkte P_1 und P_2 verlaufenden Geraden mit der Y-Achse. Ein interessanter, aus Abbildung 12 ersichtlicher Nebeneffekt ist, dass sich dieses Verfahren als „Primzahlsieb“ erweist.

Eine durch zwei Punkte $P_1(x_1, y_1)$ und $P_2(x_2, y_2)$ verlaufende Gerade lautet allgemein:

$$\frac{y - y_1}{x - x_1} = \frac{y_2 - y_1}{x_2 - x_1} \qquad \text{und nach } y \text{ aufgelöst:} \quad y = (x - x_1)\frac{y_2 - y_1}{x_2 - x_1} + y_1$$

Setzt man $x_1=b$, $y_1=b^2$ sowie $x_2=-a$, $y_2=a^2$ ein und berücksichtigt noch, dass für den gesuchten Schnittpunkt mit der Y-Achse $x=0$ gilt, so folgt das in der Grafik verdeutlichte Ergebnis:

$$y = -b\frac{a^2 - b^2}{-a - b} + b^2 = b\frac{(a+b)(a-b)}{b+a} + b^2 = b(a-b) + b^2 = a \cdot b$$

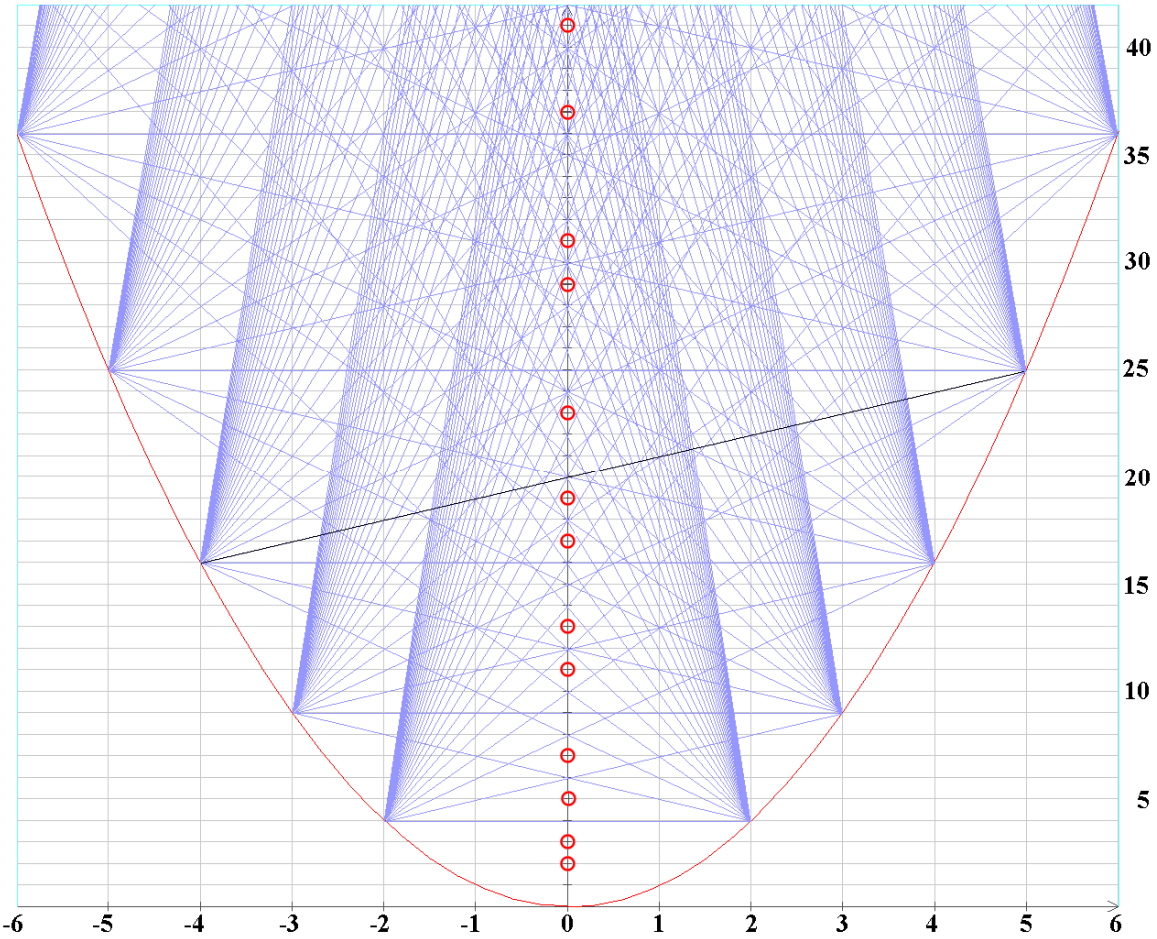

Abbildung 12: Geometrische Multiplikation mithilfe einer Parabel $y=x^2$. Verbindet man einen auf dem linken Ast der Parabel liegenden Punkt mit einem auf dem rechten Ast liegenden Punkt durch eine Gerade, so ergibt der Schnittpunkt der Verbindungsgeraden mit der Y-Achse das Produkt der zu den beiden Punkten gehörenden X-Koordinaten. Alle Geraden, die Produkten von natürlichen Zahlen zwischen 2 und 6 entsprechen, sind blau eingezeichnet. Die schwarze Gerade hebt als Beispiel den Fall $4 \cdot 5 = 20$ hervor. Die auf der Y-Achse liegenden Primzahlen sind dadurch erkennbar, dass sie durch keine Gerade geschnitten werden. Dies ist durch die roten Kreise markiert.

7 Divide et Impera!

Eine Anleihe bei Cäsar

Abbildung 13: Alexeij Karatsuba

Auf eine wesentliche Verbesserung der bekannten Methoden zur Multiplikation natürlicher Zahlen musste man nach Erscheinen des Rechenbuchs von Adam Ries noch ca. 450 Jahre lang warten. Das lag vor allem an mangelnder Motivation der Mathematiker. Denn erst mit der Verfügbarkeit von Computern konnte man so große Zahlen multiplizieren, dass der quadratische Anstieg des Aufwands überhaupt eine Rolle spielte. Gleichzeitig reichte für viele technische Anwendungen die Genauigkeit von Rechenschiebern und Logarithmentafeln nicht mehr aus. 1962 gaben die russischen Mathematiker Alexeij Karatsuba und Yu Ofman [Kar62, Knu81] einen als *Karatsuba-Verfahren* bekannten Multiplikationsalgorithmus an, der – frei nach Cäsar – das Prinzip *Divide et Impera*, also *Teile und Herrsche*, ausnutzte. Die Grundidee ist, dass man ein großes Problem häufig effizienter lösen kann, wenn man es in viele kleinere Teilprobleme zerlegt, diese dann einzeln löst und die Teillösungen schließlich zur Gesamtlösung kombiniert.

Der Karatsuba-Algorithmus

Die Multiplikation von zwei n-stelligen natürlichen Zahlen A und B lässt sich folgendermaßen in drei Multiplikationen von Zahlen mit nur der halben Stellenzahl $n/2$ umformulieren:

$$A \cdot B = a_1 b_1 10^n + a_2 b_2 + [(a_1 + a_2)(b_1 + b_2) - a_1 b_1 - a_2 b_2] 10^{n/2}$$

Dabei werden die n-stelligen Zahlen A und B durch die beiden $n/2$-stelligen Hälften a_1 und a_2 bzw. b_1 und b_2 ersetzt. Es ist also:

$$A = a_1 10^{n/2} + a_2 \quad \text{und} \quad B = b_1 10^{n/2} + b_2$$

Ohne Beschränkung der Allgemeinheit kann angenommen werden, dass die Stellenzahl n für A und B identisch ist und dass n eine Zweierpotenz ist. Durch Voranstellen von 0en am Anfang der Zahlen lässt sich dies immer erzwingen.

Offenbar kann mit diesem Verfahren eine n-stellige Multiplikation durch drei $n/2$-stellige Multiplikationen ersetzt werden. Allerdings kommen noch 8 einfache und schnell ausführbare Operationen hinzu, nämlich 4 Additionen, 2 Subtraktionen und 2 Verschiebungen (d.h. Multiplikation mit Zehnerpotenzen).

Die halbe ursprüngliche Stellenzahl $n/2$ kann natürlich immer noch eine große Zahl sein, daher wendet man denselben Algorithmus auf die drei resultierenden $n/2$-stelligen Zahlen nochmals an und so weiter, bis schließlich im letzten Schritt nur noch elementare, einstellige Multiplikationen auszuführen sind. Diese fortwährende Halbierung ist auch der Grund für die Annahme, dass n eine Zweierpotenz ist. Es handelt sich also um ein *rekursives* Verfahren, das $\mathrm{ld}(n)$ mal aufgerufen wird, bis schließlich die Stellenzahl 1 erreicht wird. Da n eine Zweierpotenz ist, liefert $\mathrm{ld}(n)$ eine natürliche Zahl als Ergebnis.

Ein Multiplikationsbeispiel

Am besten macht man sich die Wirkungsweise des Karatsuba-Algorithmus anhand eines Beispiels klar. Es soll das Produkt $2142 \cdot 3312$ aus zwei vierstelligen Zahlen berechnet werden. Der Standardalgorithmus liefert in $n^2=16$ einstelligen Multiplikationen das Ergebnis 7094304.

Bei Verwendung des Karatsuba-Algorithmus werden zunächst die Faktoren $A = 2142$ und $B = 3312$ wie folgt zerlegt:

$$A = a_1 10^{n/2} + a_2 = 21 \cdot 10^2 + 42 \quad \text{und} \quad B = b_1 10^{n/2} + b_2 = 33 \cdot 10^2 + 12$$

Nun rechnet man:

$$\begin{aligned} 2142 \cdot 3312 &= a_1 b_1 10^n + a_2 b_2 + [(a_1 + a_2)(b_1 + b_2) - a_1 b_1 - a_2 b_2] 10^{n/2} \\ &= 21 \cdot 33 \cdot 10^4 + 42 \cdot 12 + [(21 + 42)(33 + 12) - 21 \cdot 33 - 42 \cdot 12] \cdot 10^2 \\ &= 21 \cdot 33 \cdot 10^4 + 42 \cdot 12 + [63 \cdot 45 - 21 \cdot 33 - 42 \cdot 12] \cdot 10^2 \end{aligned}$$

Auf die drei Produkte $p_1 = 21 \cdot 33$, $p_2 = 42 \cdot 12$ und $p_3 = 63 \cdot 45$ wird derselbe Algorithmus nochmals angewendet:

$$p_1 = 21 \cdot 33 = 2 \cdot 3 \cdot 10^2 + 1 \cdot 3 + (3 \cdot 6 - 2 \cdot 3 - 1 \cdot 3) \cdot 10$$

$$p_2 = 42 \cdot 12 = 4 \cdot 1 \cdot 10^2 + 2 \cdot 2 + (6 \cdot 3 - 4 \cdot 1 - 2 \cdot 2) \cdot 10$$

$$p_3 = 63 \cdot 45 = 6 \cdot 4 \cdot 10^2 + 3 \cdot 5 + (9 \cdot 9 - 6 \cdot 4 - 3 \cdot 5) \cdot 10$$

Setzt man diese Zwischenergebnisse ein, so erhält man das gesuchte Produkt in einer Form, die nur noch 9 verschiedene (blau hervorgehobene) einstellige Multiplikationen enthält:

$$\begin{aligned} 2142 \cdot 3312 &= p_1 \cdot 10^4 + p_2 + [p_3 - p_1 - p_2] \cdot 10^2 \\ &= [\mathbf{2 \cdot 3} \cdot 10^2 + \mathbf{1 \cdot 3} + (\mathbf{3 \cdot 6} - 2 \cdot 3 - 1 \cdot 3) \cdot 10] \cdot 10^4 \\ &+ \mathbf{4 \cdot 1} \cdot 10^2 + \mathbf{2 \cdot 2} + (\mathbf{6 \cdot 3} - 4 \cdot 1 - 2 \cdot 2) 10 \\ &+ [(\mathbf{6 \cdot 4} \cdot 10^2 + \mathbf{3 \cdot 5} + (\mathbf{9 \cdot 9} - 6 \cdot 4 - 3 \cdot 5) \cdot 10 \\ &- (2 \cdot 3 \cdot 10^2 + 1 \cdot 3 + (3 \cdot 6 - 2 \cdot 3 - 1 \cdot 3) \cdot 10 \\ &- (4 \cdot 1 \cdot 10^2 + 2 \cdot 2 + (6 \cdot 3 - 4 \cdot 1 - 2 \cdot 3) \cdot 10] \cdot 10^2 \\ &= 693 \cdot 10^4 + 504 + (2835 - 693 - 504) \cdot 10^2 = 7094304 \end{aligned}$$

Der Ablauf dieses Multiplikationsverfahrens ist in der folgenden Abbildung nochmals skizziert.

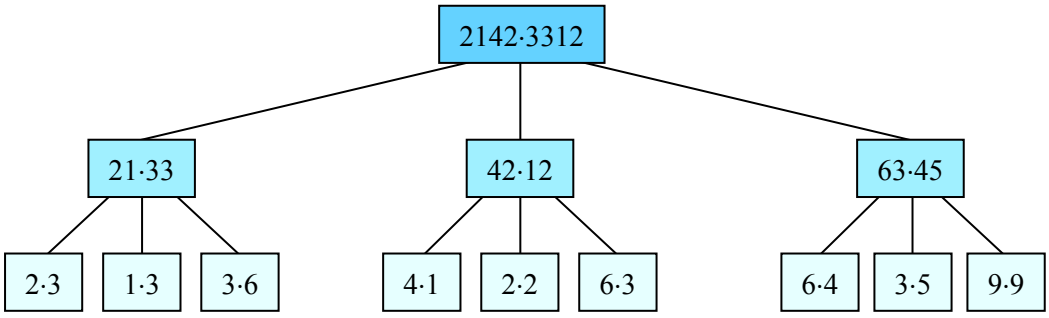

Abbildung 14: Baumstruktur zur Erläuterung des Karatsuba-Algorithmus anhand des Beispiels $2142 \cdot 3312$. Die letzte Zeile zeigt die für dieses Beispiel erforderlichen 9 elementaren Multiplikationen.

Ist Karatsuba wirklich schneller?

Das obige Beispiel deutet darauf hin, dass der Karatsuba-Algorithmus deutlich schneller ist als der Standardalgorithmus, denn es waren zur Multiplikation von zwei vierstelligen Zahlen anstelle von 16 nur 9 elementare Multiplikationen erforderlich. Dazu kamen allerdings noch 24 Additionen und 12 Multiplikation von Zehnerpotenzen, die aber nur Verschiebungen entsprechen. Ob die Erkenntnis aus diesem einen Beispiel verallgemeinert werden kann, ist allerdings noch zu zeigen.

Ist der Zeitbedarf einer n-stelligen Multiplikation $T(n)$, so lässt sich dieser auch durch den Zeitbedarf $T(n/2)$ für eine $n/2$-stellige Multiplikation ausdrücken:

$$T(n) = 3 \cdot T(n/2) + t(n)$$

Dabei trägt der Term $t(n)$ den für die Kombination der $n/2$-stelligen Multiplikationen zum Gesamtergebnis zusätzlich erforderlichen Operationen Rechnung.

Diese für Problemlösungen nach dem Prinzip „Teile und Herrsche“ typische Beziehung lässt sich für die Zerlegung eines Problems der Größe n in r Teilprobleme der Größe n/s verallgemeinern:

$T(n) = r \cdot T(n/s) + t(n)$ für $n>1$
$T(1) = 1$ für $n=1$

Für den Grenzfall $n=1$ wird eine vorgegebene, maschinenabhängige Konstante verwendet, für die man den Zahlenwert 1 annehmen kann, da eine Skalierung hier nicht von Interesse ist.

Man bezeichnet eine derartige Beziehung als eine *rekursive Relation*. Nimmt man an, dass n eine Potenz von 2 ist, so gilt $n=s^k$ und damit $k=\log_s n$. Für diesen Fall lautet die allgemeine Lösung der rekursiven Relation:

$$T(n)=r^k+\sum_{i=0}^{k-1} r^i t(s^{k-i})$$

Der Beweis dieses Ergebnisses lässt sich ohne große Mühe durch vollständige Induktion führen und auch auf Zahlen n erweitern, die keine Potenzen von 2 sind.

Meist überwiegt der erste Term r^k, so dass für Aufwandsbetrachtungen die Summe vernachlässigt werden kann. Man findet dann für $T(n)$ die Näherungslösung:

$$T(n) \approx r^{\log_s n} = n^{\log_s r}$$

Für das oben genannte Beispiel der Multiplikation ergibt sich mit $r=3$ und $s=2$:

$$T(n) \approx n^{\log_2 3} = n^{ld3} \approx n^{1.585}$$

Im Vergleich mit dem üblichen Multiplikations-Algorithmus, dessen Aufwand wie $T(n) \approx n^2$ wächst, bedeutet dies einen signifikanten Fortschritt, denn $n^{1.585}$ steigt mit wachsendem n wesentlich langsamer an als n^2, wie aus Abbildung 19 ersichtlich ist.

Für $n=4$ benötigt der Standardalgorithmus $4^2 = 16$ elementare Multiplikationen, der Karatsuba-Algorithmus aber nur $4^{1.585} \approx 9.0$, in guter Übereinstimmung mit dem obigen Zahlenbeispiel $2142 \cdot 3312$. Die Überlegenheit des Karatsuba-Algorithmus nimmt mit wachsendem n dramatisch zu, für $n = 250$ ist er bereits um den Faktor 10 schneller als das Standardverfahren.

Toom-Cook-Algorithmen

Man kann die Methode „Teile und Herrsche“ zur Verbesserung des Karatsuba-Algorithmus noch weiter treiben, indem man die beiden Faktoren nicht nur in zwei, sondern in drei oder sogar noch mehr Teile zerlegt. Diese als *Toom-Cook-Algorithmen* bezeichneten Verfahren wurden zuerst von A. L. Toom [Too63] vorgeschlagen und dann von S. A. Cook in seiner Doktorarbeit [Coo66] verfeinert und detailliert beschrieben. Auch danach gelangen noch Detailverbesserungen [Zur94]. Einige Ergebnisse sind:

Zerteilung in 3 Teile mit 5 Multiplikationen: $T(n) = n^{\log 5/\log 3} \approx n^{1.465}$
Zerteilung in 4 Teile mit 7 Multiplikationen: $T(n) = n^{\log 7/\log 4} \approx n^{1.404}$
Zerteilung in 5 Teile mit 9 Multiplikationen: $T(n) = n^{\log 9/\log 5} \approx n^{1.365}$

8 Die Weltmeister

Falten statt Multiplizieren

Natürliche Zahlen lassen sich immer als Summe von Potenzen einer Basis darstellen, d.h. als *Polynom*. Bei der Ägyptischen Multiplikation wurde die Basis 2 verwendet, geläufiger ist natürlich das Zehnersystem mit der Basis 10. So kann man beispielsweise für $c=a\cdot b$ mit $a=2142$ und $b=3312$ schreiben:

$$c = a\cdot b = 2142\cdot 3312 = (2\cdot 10^3 + 1\cdot 10^2 + 4\cdot 10^1 + 2\cdot 10^0)\cdot(3\cdot 10^3 + 3\cdot 10^2 + 1\cdot 10^1 + 2\cdot 10^0) =$$
$$= 2\cdot 3\cdot 10^6 + (1\cdot 3 + 2\cdot 3)\cdot 10^5 + (4\cdot 3 + 1\cdot 3 + 2\cdot 1)\cdot 10^4 + (2\cdot 3 + 4\cdot 3 + 1\cdot 1 + 2\cdot 2)\cdot 10^3$$
$$+ (2\cdot 3 + 4\cdot 1 + 1\cdot 2)\cdot 10^2 + (2\cdot 1 + 4\cdot 2)\cdot 10^1 + 2\cdot 2 =$$
$$= 6\cdot 10^6 + 9\cdot 10^5 + 17\cdot 10^4 + 23\cdot 10^3 + 12\cdot 10^2 + 10\cdot 10^1 + 4 =$$
$$= 7\cdot 10^6 + 0\cdot 10^5 + 9\cdot 10^4 + 4\cdot 10^3 + 3\cdot 10^2 + 0\cdot 10^1 + 4 = 7094304$$

Eigentlich ist die obige Rechnung nichts anderes, als eine ausführlichere Schreibweise des Standard-Multiplikationsalgorithmus mit der einzigen Änderung, dass die Überträge erst in der letzten Zeile berücksichtigt werden. Man beginnt dazu in der letzten Stelle ganz rechts und reicht ggf. den Übertrag jeweils um eine Stelle nach links weiter.

Allgemein lässt sich die Multiplikation zweier Zahlen mit $n=4$ Stellen so schreiben:

$$a = a_3\cdot 10^3 + a_2\cdot 10^2 + a_1\cdot 10^1 + a_0, \quad b = b_3\cdot 10^3 + b_2\cdot 10^2 + b_1\cdot 10^1 + b_0$$
$$c = a\cdot b = a_3\cdot b_3\cdot 10^6 + (a_2\cdot b_3 + a_3\cdot b_2)\cdot 10^5 + (a_1\cdot b_3 + a_2\cdot b_2 + a_3\cdot b_1)\cdot 10^4 + (a_0\cdot b_3 + a_1\cdot b_2 + a_2\cdot b_1 + a_3\cdot b_0)\cdot 10^3$$
$$+ (a_0\cdot b_2 + a_1\cdot b_1 + a_2\cdot b_0)\cdot 10^2 + (a_0\cdot b_1 + a_1\cdot b_0)\cdot 10^1 + a_0\cdot b_0$$

Haben die Zahlen a und b jeweils vier Stellen mit Indizes von 0 bis 3, so hat das Ergebnis c mindestens $2\cdot n-1=7$ Stellen mit Indizes 0 bis 6. Eine weitere Stelle kann eventuell hinzu kommen, wenn sich die Überträge bis über die höchste Stelle hinaus fortsetzen.

Die Stellenwerte c_i des Produkts, also die Koeffizienten des Polynoms c, lassen sich unter Verwendung des Summenzeichens kürzer und allgemeiner für beliebige Stellenzahl n folgendermaßen schreiben:

$$c_s = \sum_{k=0}^{n-1} a_{s-k}\, b_k \qquad \text{mit } s = 0 \text{ bis } 2n\text{-}2$$

Die Koeffizienten von a und b sind eigentlich nur für Indizes von 0 bis $n\text{-}1$ definiert, in der obigen Summe kommen aber für a_{s-k} auch Indizes vor, die negativ sind oder größer als $n\text{-}1$. In diesen Fällen wird für die nicht definierten Koeffizienten in die Summe einfach der Wert 0 eingesetzt.

Eine solche Summe über das Produkt von Koeffizienten wird ganz allgemein ohne Bezug auf die Multiplikation als *diskrete Faltung* bezeichnet. Diese ist ein Spezialfall des für kontinuierliche Funktionen definierten *Faltungsintegrals*, wenn man nur endlich viele (diskrete) Werte verwendet. Aus dem Integral wird dann die oben angegebene einfache Summe. Die Multiplikation ist also eigentlich im Wesentlichen (bis auf die Überträge) eine Faltung.

Die Faltung ist ein wichtiges mathematisches Konzept, das in vielen praktischen Anwendungen eine immense Rolle spielt, insbesondere in der Nachrichtentechnik und der Signalverarbeitung. Die Faltung lässt sich sehr schön geometrisch veranschaulichen, wie die folgende Abbildung verdeutlicht. Man stellt dazu die Koeffizienten von a und b als Histogramme dar. Sodann wird das a-Histogramm gespiegelt (wegen des Index $-k$ in der Summe) und schrittweise von links nach rechts über das b-Histogramm geschoben. Die Koeffizienten des Faltungsergebnisses c sind dann gerade die im Überlappungsbereich von a und b miteinander multiplizierten und summierten Werte. Zur Vereinfachung ist in dem in Abbildung 15 dargestellten Beispiel $a=b$ angenommen.

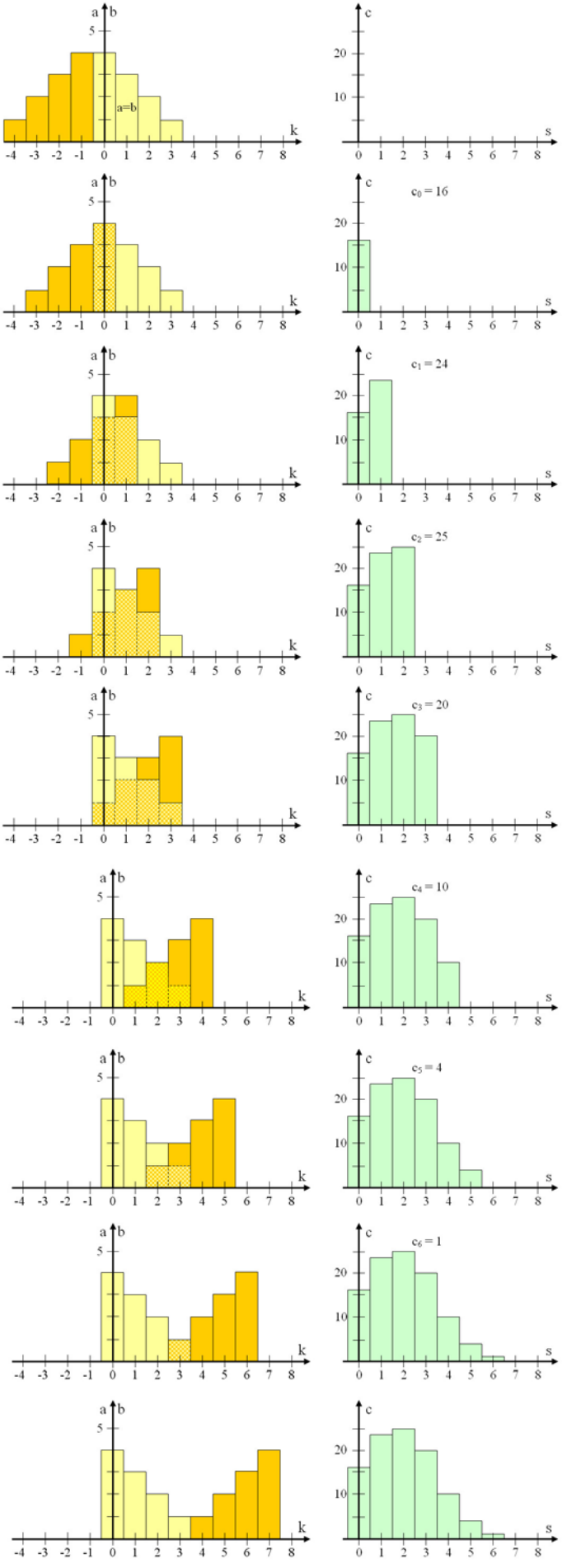

Abbildung 15: Beispiel für eine Faltung.

Gegeben seien die beiden identischen Zahlen a=b=1234. Die Stellenzahl ist also n=4 und die Koeffizienten lauten $a_0=b_0=1$, $a_1=b_1=2$, $a_2=b_2=3$ und $a_3=b_3=4$. Nun wird die Faltung durch Einsetzen von a und b in die Summe $c_s = \sum_{k=0}^{3} a_{s-k} b_k$ berechnet.

Mit s=0 bis 6 erhält man die Ergebnisse $c_0=16$, $c_1=24$, $c_2=25$, $c_3=20$, $c_4=10$, $c_5=4$, und $c_6=1$. Durch Weiterreichen des Übertrags von der niedrigsten Stelle c_0 bis zur höchstwertigen Stelle c_6 folgt dann das Multiplikationsergebnis $a \cdot b = 1234 \cdot 1234 = 1 \cdot 10^6 + 4 \cdot 10^5 + 10 \cdot 10^4 + 20 \cdot 10^3 + 25 \cdot 10^2 + 24 \cdot 10 + 16 = 1522756$.

Die nebenstehende Figur illustriert diesen Faltungsvorgang. Die Koeffizienten von b sind gelb aufgetragen, die von a in umgekehrter Reihenfolge (wegen des Index -k in der Summe) etwas dunkler links daneben. In den darunter stehenden Teilbildern werden die Koeffizienten von a schrittweise mit den Verschiebungen s=0 bis s=6 nach rechts bewegt. Die markierten Überlappungsbereiche liefern dann jeweils die rechts in Grün dargestellten Beiträge c_0 bis c_6 zur Faltung.

Schnelle Faltung über Umwege

Durch Einführung der Faltung ist die Multiplikation allerdings noch nicht schneller geworden, da es sich nur um eine andere Schreibweise für den Standardalgorithmus handelt. Die Faltung hat jedoch eine äußerst interessante, durch das *Faltungstheorem* beschriebene mathematische Eigenschaft, die man zur Beschleunigung der Multiplikation ausnützen kann. Das Faltungstheorem besagt, dass man die Faltung zweier Funktionen a und b auch dadurch berechnen kann, dass man zunächst die zugehörigen *Fourier-Transformierten* A von a und B von b ermittelt, diese dann komponentenweise multipliziert und das Ergebnis wieder zurück transformiert [Mey02]. Dieses Schema ist in Abbildung 16 skizziert. Der Vorteil ist, dass bei direkter Ausführung der Faltung n^2 elementare Multiplikationen von Koeffizienten a_j und b_k erforderlich sind, beim Umweg über die Fourier-Transformation aber nur n Multiplikationen der transformierten Koeffizienten A_j und B_k, da die Fourier-Transformation bewirkt, dass jetzt nur eine komponentenweise Multiplikation mit $j=k$ auszuführen ist. Das ist natürlich eine erhebliche Zeitersparnis; es ist aber zu bedenken, dass der Aufwand für die beiden Fourier-Transformationen sowie die Fourier-Rücktransformation noch hinzu kommt. Tatsächlich kann die Fourier-Transformation mittels der diskreten schnellen Fourier-Transformation (Discrete Fast Fourier Transformation, *DFFT*) extrem schnell ausgeführt werden, der erforderliche Zeitaufwand steigt nur proportional zu $n \cdot \log(n)$ an, also viel langsamer als für die Multiplikation nach dem Standard-Algorithmus.

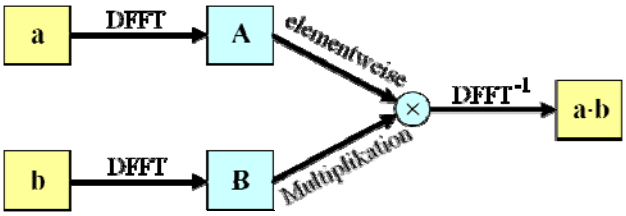

Abbildung 16: Die Multiplikation zweier Zahlen a und b kann als Faltung der Koeffizienten aufgefasst werden. Durch Anwendung des Faltungstheorems mithilfe der DFFT lässt sich dann die Multiplikation erheblich beschleunigen.

Die Abbildung 16 erinnert stark an Abbildung 8, in der die Multiplikation mithilfe von Logarithmen ausgeführt wird. An die Stelle der Logarithmusfunktion tritt hier die DFFT. Der Nachteil der Logarithmen-Methode ist, dass diese nur mit vorab berechneten Tabellen schnell ist. Die erzielbare Genauigkeit ist daher vor allem für Zahlen mit hoher Stellenzahl ungenügend. Die DFFT kann dagegen auf Computern für beliebig große Zahlen implementiert werden.

Schneller als Multiplizieren: Die Fourier-Transformation

Eine Frage wurde noch nicht beantwortet: Wie funktioniert eigentlich die DFFT und warum ist sie so schnell ausführbar? Die Fourier-Transformation ist eigentlich ein komplexes Integral und als solches der Schrecken vieler Studierender. Für diskrete Werte, wie im Falle der Multiplikation, wird daraus jedoch nur eine gar nicht mehr so schreckliche Summe. Man erhält folgende Formeln für die diskrete Fourier-Transformation:

$$F_j = \sum_{k=0}^{n-1} f_k w^{jk}$$ Fourier-Transformation f nach F

$$f_k = \frac{1}{n} \sum_{j=0}^{n-1} F_j w^{-jk}$$ Fourier-Rücktransformation von F nach f

Dabei ist w wie folgt durch die *Exponentialfunktion* mit der *imaginären Einheit* i definiert:

$$w = e^{i2\pi/n} = \cos(2\pi/n) + i \cdot \sin(2\pi/n)$$

Auf den ersten Blick scheint auch dies keine Verbesserung zu bringen, da ja n Koeffizienten transformiert werden müssen und für jeden Koeffizienten in der Summe n Elementarmultiplikationen erforderlich sind, zusammen also wieder n^2. Der Clou ist aber, dass die Exponentialfunktion wegen des Zusammenhangs mit den Winkelfunktionen Sinus und Kosinus in der *komplexen Zahlenebene* ein zyklisches Verhalten zeigt. Dies hat zur Folge, dass die in den

Summen auftretenden Potenzen von w, wie in Abbildung 17 ersichtlich, alle symmetrisch auf dem *Einheitskreis* in der komplexen Zahlenebene liegen. Daher wiederholen sie sich mit wachsendem Exponenten immer, so dass nur n verschiedene Werte auftreten. Es gilt also $w^n=w^0$, $w^{n+1}=w^1$, $w^{n+2}=w^2$ usw. und allgemein $w^{nk+m}=w^m$.

Diese wiederholt auftretenden Faktoren kann man bei der Berechnung ausklammern. Einzig und allein dieses Ausklammern führt dazu, dass jetzt der Aufwand für die Ausführung der schnellen diskreten Fourier-Transformation so dramatisch sinkt.

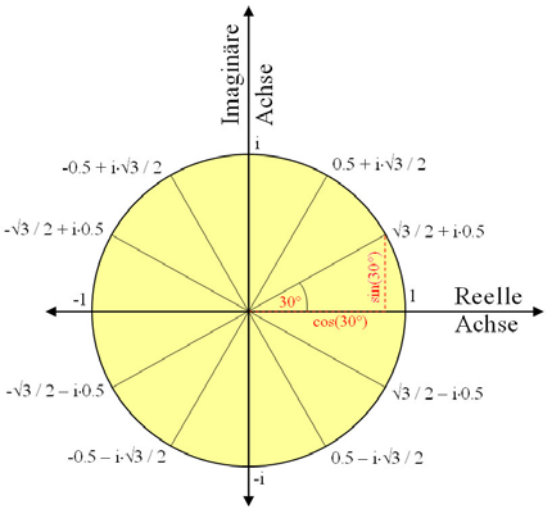

Abbildung 17: Der Einheitskreis in der komplexen Zahlenebene. Die Werte für $w = e^{i2\pi/n} = \cos(2\pi/n) + i \cdot \sin(2\pi/n)$ für $n=12$ sind eingezeichnet. Es sind dies gerade die Koordinaten der Ecken eines regelmäßigen Zwölfecks.

Ein Multiplikationsbeispiel

Als Beispiel soll die Multiplikationsaufgabe $a \cdot a = 123 \cdot 123$ mittels Faltung und DFFT berechnet werden. Die Zahl $a=123$ hat $n=3$ Stellen, das Ergebnis wird daher $2n-1=5$ Stellen haben. Dies wird bei der Fourier-Transformation durch Ergänzen der fehlenden Stellen mit Nullen berücksichtigt. Diese müssen also mit $n=5$ in die obige Summe eingesetzt werden. Es folgt:

$$A_k = \sum_{j=0}^{4} a_j w^{jk}$$

oder ausgeschrieben mit Einsetzen von $a_0=1$, $a_1=2$, $a_2=3$, $a_3=0$ und $a_4=0$:

$$\begin{aligned}
A_0 &= 1\cdot w^0 + 2\cdot w^0 + 3\cdot w^0 + 0\cdot w^0 + 0\cdot w^0 &&= 1 + 2 + 3 &&= 6\\
A_1 &= 1\cdot w^0 + 2\cdot w^1 + 3\cdot w^2 + 0\cdot w^3 + 0\cdot w^4 &&= 1 + 2\cdot w^1 + 3\cdot w^2 &&= -0.809017 + i\cdot 3.66547\\
A_2 &= 1\cdot w^0 + 2\cdot w^2 + 3\cdot w^4 + 0\cdot w^6 + 0\cdot w^8 &&= 1 + 2\cdot w^2 + 3\cdot w^4 &&= 0.309017 - i\cdot 1.67760\\
A_3 &= 1\cdot w^0 + 2\cdot w^3 + 3\cdot w^6 + 0\cdot w^9 + 0\cdot w^{12} &&= 1 + 2\cdot w^3 + 3\cdot w^1 &&= 0.309017 + i\cdot 1.67760\\
A_4 &= 1\cdot w^0 + 2\cdot w^4 + 3\cdot w^8 + 0\cdot w^{12} + 0\cdot w^{16} &&= 1 + 2\cdot w^4 + 3\cdot w^3 &&= -0.809017 - i\cdot 3.66547
\end{aligned}$$

Nach dem zweiten Gleichheitszeichen wurde $w^0=1$ gesetzt, da eine Potenzierung mit dem Exponenten 0 immer 1 ergibt. Außerdem wurde wegen des zyklischen Verhaltens der Exponentialfunktion $w^5=w^0=1$, $w^6=w^1$ und $w^8=w^3$ gesetzt. Natürlich müssen noch die Potenzen von w ermittelt werden. Da aber wegen der Kreissymmetrie nicht n^2, sondern nur n verschiedene Potenzen auftreten und da diese zudem auch für die Rücktransformation verwendet werden können, ist dies ein vernachlässigbarer Aufwand. Für den vorliegenden Fall berechnet man:

$$\begin{aligned}
w^0 &= 1\\
w^1 &= 0.309017 + i\cdot 0.951057\\
w^2 &= -0.809017 + i\cdot 0.587785\\
w^3 &= -0.809017 - i\cdot 0.587785\\
w^4 &= 0.309012 - i\cdot 0.951057
\end{aligned}$$

Damit ergeben sich die Resultate nach dem dritten Gleichheitszeichen in der obigen Berechnung, womit die DFFT für $a=123$ komplett ist.

Im nächsten Schritt werden nun die Koeffizienten elementweise miteinander multipliziert, wobei für die imaginäre Einheit $i\cdot i=-1$ zu beachten ist. Man erhält: $C_i = A_i \cdot A_i$ für $i=0$ bis 4, also:

$$\begin{aligned}
C_0 &= 36\\
C_1 &= -12.78120 - i\cdot 5.93058\\
C_2 &= -2.71885 - i\cdot 1.03681\\
C_3 &= -2.71885 + i\cdot 1.03681\\
C_4 &= -12.78120 + i\cdot 5.93058
\end{aligned}$$

Einsetzen in $c_k = \frac{1}{5}\sum_{j=0}^{4} C_j w^{-jk}$ liefert schließlich das Ergebnis der Faltung:

$c_0 = 1,\ c_1 = 4,\ c_2 = 10,\ c_3 = 12,\ c_4 = 9$

Nun müssen nur noch die Überträge in der Koeffizientenfolge $1,4,10,12,9$ beachtet werden und man hat das Multiplikationsergebnis $123 \cdot 123 = 15129$.

Noch eine Zutat aus China

Das Ergebnis hat allerdings noch einige Schönheitsfehler. Zum einen treten komplexe Zahlen mit der imaginären Einheit i auf. Diese heben sich zwar bei der Fourier-Rücktransformation wieder weg, sie erhöhen aber bis dahin den Aufwand im schlimmsten Fall um den Faktor zwei. Ein weiteres Problem ist, dass man mit Brüchen rechnen muss. Dies lässt sich durch Multiplikation aller Zahlen mit einer entsprechend hohen Potenz von 2 beheben, so dass man doch wieder mit natürlichen Zahlen auskommt. Man muss dazu jedoch für die Koeffizienten A_k deutlich mehr Bits reservieren als für die Koeffizienten a_k. Ein weiteres Problem ist, dass nicht nur elementare Multiplikationen auftreten, sondern auch solche mit w^{jk}, die deutlich mehr signifikante Stellen aufweisen. Doch auch für diese „mittelgroßen" Zahlen gibt es eine schnelle Multiplikationsmethode, die auf dem *chinesischen Restsatz* basiert, aber hier nicht weiter erläutert werden soll. Man nutzt dabei die algebraische Struktur von *Ringen* aus, bei der die durch *Modulo-Division* der Faktoren entstehenden Reste eindeutig das Multiplikationsergebnis charakterisieren. Da dies aber auf den Zahlenbereich des Rings beschränkt ist, handelt es um keine allgemein einsetzbare Multiplikationsmethode, die aber gleichwohl für diese Spezialanwendung sehr nützlich ist.

Der Schönhage-Strassen-Algorithmus

Dieses hier skizzierte Grobschema für eine schnelle Multiplikation ist die Grundlage für den 1971 von Arnold Schönhage und Volker Strassen vorgestellten *Schönhage-Strassen-Algorithmus*. Mit den erwähnten Verfeinerungen, nämlich einer auf die spezielle Anwendung zugeschnittenen „superschnellen" DFFT-Variante auf Basis von Zweierpotenzen sowie einer geschickten Nutzung der Restklassenarithmetik in endlichen Zahlenringen entstand daraus die bislang effizienteste Multiplikationsmethode.

Die Anzahl der Elementarmultiplikationen steigt beim Schönhage-Strassen-Algorithmus unter Berücksichtigung aller Details proportional zu $n \cdot \log(n) \cdot \log(\log(n))$. Für $n=200$ ist dies eine Beschleunigung um den Faktor 40 im Vergleich zum Standard-Multiplikationsalgorithmus und immerhin um den Faktor 3 verglichen mit dem Karatsuba-Algorithmus. Der Toom-Cook-Algorithmus wird aber erst bei Stellenzahlen über 1000 geschlagen. In Abbildung 19 wird dieses Zeitverhalten mit den anderen hier besprochenen Algorithmen verglichen.

Abbildung 18: Arnold Schönhage und Volker Strassen.

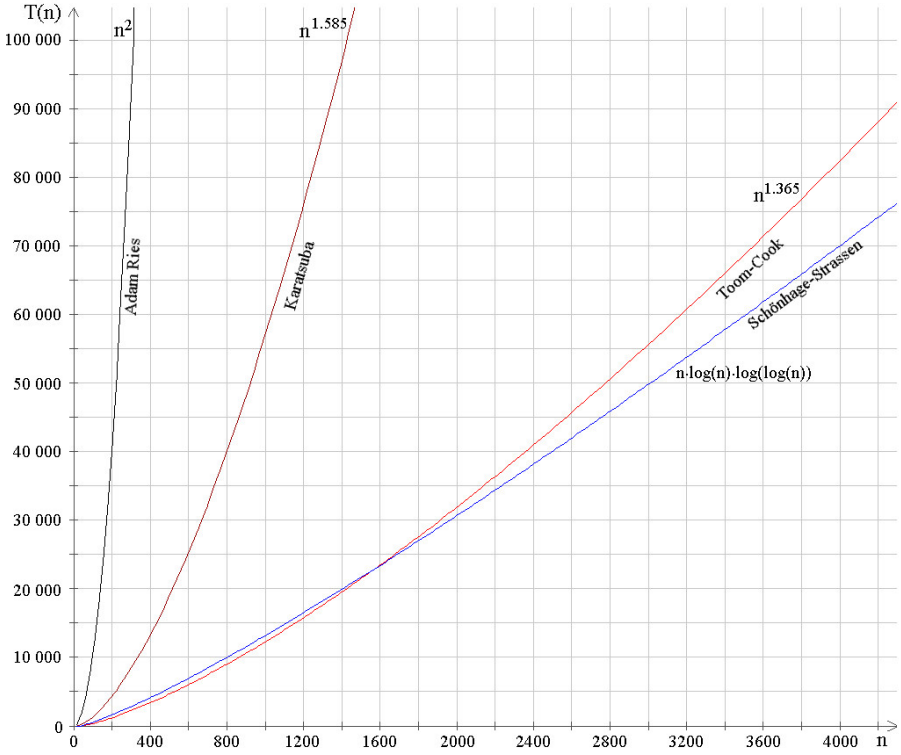

Abbildung 19: Zusammenstellung des Zeitverhaltens der diversen Multiplikationsalgorithmen.

Ausblick

Man kennt heute zwar Multiplikationsalgorithmen, die sehr viel schneller sind als alle naiven Varianten. Andererseits wird aber auch deutlich, dass Vieles noch verborgen ist. Der in Abbildung 20 zitierte Vierzeiler von Wilhelm Busch trifft daher in vollem Umfang auch auf das Problem der Multiplikation zu.

Sokrates, der alte Greis,
sagte oft in tiefen Sorgen:
„Ach wie viel ist doch verborgen,
was man immer noch nicht weiß.“

Wilhelm Busch

Wissenschaftsjahr 2008
Mathematik
Alles, was zählt

Abbildung 20: Auch beim Problem der Multiplikation ist vieles noch verborgen. Das Jahr der Mathematik motiviert aber dazu, mathematische Probleme allgemeinverständlich darzustellen.

Die Multiplikation ist ferner ein gutes Beispiel für eine Entwicklung, die in allen kulturellen Bereichen zu verzeichnen ist – keineswegs nur in der Mathematik: Vieles wird im Sinne höherer Effizienz optimiert, aber bei allem ästhetischem Reiz eleganter Algorithmen werden die Erfolge doch durch eine exponentiell zunehmende Kompliziertheit bezahlt. Wissen wird dadurch immer elitärer. Dies leistet einer kulturellen Zersplitterung und Ausgrenzung Vorschub, was zahlreiche Menschen auf der Suche nach Einfachheit in die Arme fragwürdiger Pseudowissenschaften treibt. Es ist dies ein Trend, dem man entgegenwirken sollte, gerade an praxisorientierten Hochschulen für angewandte Wissenschaften. 2008 ist das Wissenschaftsjahr der Mathematik, für den Autor Motivation genug für den Versuch, die Entwicklung der Multiplikation in einen geschichtlichen Rahmen zu stellen und möglichst allgemeinverständlich auszuloten, wo wir heute stehen.

Als ultimative theoretische Grenze für die Anzahl der Elementarmultiplikationen bei der Multiplikation großer Zahlen gilt erstaunlicherweise wie für die Addition die Stellenzahl n. Ob diese Grenze in der Praxis tatsächlich erreicht werden kann, ist immer noch offen. Bis heute konnte jedenfalls noch kein schnelleres Verfahren gefunden werden als der Schönhage-Strassen-Algorithmus. Arnold Schönhage und Volker Strassen sind daher unbestritten die Weltmeister im Multiplizieren.

Literatur

[Coo66] Cook, S. A.: *On the minimum computation time of functions*. Thesis, University of Harvard (1966)

[Euk] Euklid: *Die Elemente*. Übersetzung von C. von Thaer Harri Deutsch (2003), Originalausgabe um (330 v. Chr.)

[Fri52] Fricke, H.W: *Der Rechenschieber*. Fachbuchverlag Leipzig (1952)

[Ger94] Gericke, H.: *Mathematik in Antike und Orient, Band 1 und 2*. Fourier (1994)

[Kar62] Karatsuba, A. and Y. Ofman: *Multiplication of Many-Digital Numbers by Automatic Computers*. Doklady Akad. Nauk SSSR, Vol. 145, pp 293–294 (1962) Translation in Physics-Doklady, 7, pp. 595–596 (1963)

[Knu81] Knuth, D. E.: *The Art of Computer Programming*. Vol. 2, second edition, pp 278-301, Addison-Wesley (1981)

[Lin45] Lindgren, A.: *Pippi Langstrumpf*. Gesamtausgabe in einem Band. Oettinger Verlag (1987). Originalausgabe (1945)

[Mey02] Meyer, M. und O. Mildenberger: *Grundlagen der Informationstechnik: Signale, Systeme, Filter*. Vieweg (2002)

[Sch71] Schönhage, A. und V. Strassen: *Schnelle Multiplikation großer Zahlen.* Computing, Vol. 7, pp 281-292 (1971)

[Ries] Ries, Adam: *Rechnung auff der Linihen*. Erstausgabe (1522).

[Tsc03] Tschacher, K.: www.mathematik.uni-erlangen.de/~tschach/vortraege/Malnehmen.pdf (2003)

[Too63] Toom, A. L.: *The complexity of a scheme of functional elements realizing the multiplication of integers*. Soviet Math., Vol. 3, pp 714-716 (1963)

[Zur94] Zuras, D.: *More on squaring and multiplying large integers*. IEEE Transaction on Computers, Vol. 43, no. 8, pp 899-908 (1994)

[Con00] O'Connor, J. J. and E. F. Robertson: http://www-groups.dcs.st-and.ac.uk/~history /HistTopics/Babylonian_mathematics.html (2000)