Konkrete Mathematik
Sommersemester 2018

Volker Diekert[1]

[1]Übungen: Jan Philipp Wächter

Diekerts Diskrete Mathematik

am Anfang

Vorkenntnisse?

Vorkenntnisse!

vor der Kenntnis der Vorlesung

und überhaupt

Konkrete Mathematik

nach Concrete Mathematics von Ronald L. Graham and Donald E. Knuth and Oren Patashnik

- konkret (engl: concrete)
- Beton (engl: concrete)
- „harter Beton“, aber auch „Fundament“
- kontinulierlich (engl: continous)
- diskret (engl: discrete)

Der Buchdeckel zeigt den griechischen Buchstaben Σ in Beton als Fundament gegossen.

Literatur

1. Diekert, Kufleitner, Rosenberger,
Elemente der Diskreten Mathematik, deGruyter 2013
2. Diekert, Kufleitner, Rosenberger,
Diskrete algebraische Methoden, deGruyter 2013
Discrete algebraic Methods, deGruyter 2015
3. Graham, Knuth, Patashnik,
Concrete Mathematics, Addison-Wesley, 1994
4. Flajolet, Sedgewick,
Analytic Combinatorics, Cambridge University Press, 2009

Einschub: $\mathcal{O}$–Notation

Häufig sind wir nicht an Funktionen selbst, sondern nur an ihrem Wachstumsverhalten interessiert. Hierfür haben sich die Landau-Symbole bewährt (Edmund Georg Hermann Landau, 1877–1938).

$$\begin{aligned}
\mathcal{O}(g) &= \{\, f : \mathbb{N} \to \mathbb{C} \;\mid\; \exists C > 0\, \forall n \geq n_0 \colon\; |f(n)| \leq C \cdot |g(n)| + C \,\} \\
\Omega(g) &= \{\, f : \mathbb{N} \to \mathbb{C} \;\mid\; g \in \mathcal{O}(f) \,\} \\
\Theta(g) &= \mathcal{O}(g) \cap \Omega(g)
\end{aligned}$$

Es gilt also $f \in \mathcal{O}(g)$, wenn f bis auf eine Konstante schließlich (ab einem n_0) nicht schneller wächst als g.

Konvention ist, dass durch $\mathcal{O}$ definierte Klassen stets nach unten abgeschlossen sind. Also

$$\binom{2n}{3} \in \Theta(n^3) \subsetneq \mathcal{O}(2^n) \subsetneq 2^{\mathcal{O}(n)}.$$

Asymptotische Gleichheit

Um *asymptotisch* gleiches Wachstum von Funktionen $f, g : \mathbb{N} \to \mathbb{C}$ auszudrücken, verwendet man die Bezeichnung $f \sim g$. In unserer etwas laxen Schreibweise, mit $f(n)$ je nach Kontext den Funktionswert bei n oder die Funktion $f : \mathbb{N} \to \mathbb{C}$ zu meinen, definieren wir $f \sim g$ durch die Äquivalenz

$$f(n) \sim g(n) \iff \lim_{n\to\infty} \frac{f(n)}{g(n)} = 1$$

Damit gilt zwar $\binom{n}{3} \in \Theta(n^3)$, aber $\binom{n}{3} \not\sim n^3$. Es gilt jedoch $\binom{n}{3} \sim \frac{n^3}{6}$. Allgemeiner können wir für $k \geq 0$ festhalten $\binom{n}{k} \sim \frac{n^k}{k!}$. Wir werden die Asymptotik nur auf Funktionen anwenden, die fast niemals den Wert Null annehmen und vermeiden die Diskussion, ob $0 \sim 0$ gilt.

Euklid von Alexandria, ca. 365–300 v.Chr.

Euklidischer Algorithmus

Es gilt:

- $\mathrm{ggT}(m, 0) = m$.

Für $m \geq n > 0$ schreibe $m = qn + r$ mit $0 \leq r < n$. Dann gilt:

- $\mathrm{ggT}(m, n) = \mathrm{ggT}(n, r)$.

Beispiel

Beispiel

Berechne $\mathrm{ggT}(21, 59)$.
Links der Rechenweg für die Rekursion; rechts eine kürzere Rechnung unter der Zuhilfenahme von negativen Zahlen.

$$59 = 2 \cdot 21 + 17 \qquad 59 = 3 \cdot 21 - 4$$
$$21 = 1 \cdot 17 + 4 \qquad 21 = 5 \cdot 4 + 1$$
$$17 = 4 \cdot 4 + 1$$

Damit ist $\mathrm{ggT}(21, 59) = 1$.

Laufzeit Euklid

Die Rekursion liefert auf Eingabe m, n eine Folge

$$(n_k, n_{k-1}, \ldots, n_1, n_0)$$

mit $n_0 = 0 = F_0$ und $n_1 = \mathrm{ggT}(m, n) \geq 1 = F_1$ sowie

$$n_{i+1} \geq n_i + n_{i-1}$$

Hieraus folgt sofort $n \geq F_{k-1} = (k-1)$-te Fibonacci-Zahl.
Umgekehrt:

$$\begin{aligned} \mathrm{ggT}(F_{n+1}, F_n) &= \mathrm{ggT}(F_n + F_{n-1}, F_n) \\ &= \mathrm{ggT}(F_n, F_{n-1}) \\ &\ldots \\ &= \mathrm{ggT}(F_1, F_0) = 1 \end{aligned}$$

Die Laufzeit des euklidischen Algorithmus ist also logarithmisch und benachbarte Fibonacci-Zahlen sind teilerfremd.

Leonardo da Pisa, genannt Fibonacci, ca. 1180–1241

Die Fibonacci-Zahlen sind definiert durch:

$$F_0 = 0, \quad F_1 = 1, \quad F_{n+1} = F_n + F_{n-1}$$

Die ersten Werte der Folge sind damit:

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584, \ldots$$

Die „Startwerte“ $F_0 = 0$ und $F_1 = 1$ liefern zusammen mit dem Bildungsgesetz $F_{n+1} = F_n + F_{n-1}$ eindeutige F_n für alle $n \in \mathbb{Z}$.

Wachstum

Die Fibonacci Zahlen wachsen schnell. Wegen $F_{n+2} = 2F_n + F_{n-1}$ gilt:

$$F_n \leq 2^n \leq F_{2n}$$

Betrachte $f_n = x^n$ für ein $x \in \mathbb{R}$ so, dass alle $n \in \mathbb{Z}$ gilt:

$$x^{n+1} = x^n + x^{n-1}$$

Dann kann x nicht Null sein, denn $0^2 \neq 0^1 + 0^0$. Für $x \neq 0$ können wir durch x^{n-1} dividieren, und die obige Gleichung ist äquivalent zu $x^2 = x + 1$. Diese quadratische Gleichung hat zwei Lösungen:

$$\Phi = \frac{1+\sqrt{5}}{2} \qquad \text{und} \qquad \widehat{\Phi} = \frac{1-\sqrt{5}}{2}$$

Wobei $\Phi = \frac{1+\sqrt{5}}{2}$ der *goldene Schnitt* ist.

Wachstum

$\Phi = \frac{1+\sqrt{5}}{2}$ ist das Seitenverhältnis b/a eines Rechtecks mit den Seitenlängen a und b, wenn $a/b = b/(a+b)$ gilt.

$$\Phi = 1{,}61803\ 39887\ 49894\ 84820\ 45868\ 34365\ \cdots$$

Aus $x^2 = x + 1$ folgt $x(x-1) = 1$, also ist $\Phi^{-1} = \Phi - 1 = -\widehat{\Phi}$. Die beiden Zahlen Φ und $\widehat{\Phi}$ genügen den Bildungsgesetzen $\Phi^{n+1} = \Phi^n + \Phi^{n-1}$ und $\widehat{\Phi}^{n+1} = \widehat{\Phi}^n + \widehat{\Phi}^{n-1}$, denn so wurden sie ja gerade bestimmt. Also gehorcht auch jede Linearkombination $F_n(a,b) = a\Phi^n + b\widehat{\Phi}^n$ dem Bildungsgesetz

$$F_{n+1}(a,b) = F_n(a,b) + F_{n-1}(a,b)$$

Um $F_n(a,b) = F_n$ zu finden, reicht es also, das folgende Gleichungssystem mit 2 Unbekannten zu lösen

$$a\Phi^0 + b\widehat{\Phi}^0 = F_0 = 0$$
$$a\Phi^1 + b\widehat{\Phi}^1 = F_1 = 1$$

Wachstum

Wir erhalten $b = -a$ und $a = \frac{1}{\sqrt{5}}$. Insgesamt ergibt sich

$$F_n = \frac{\Phi^n - \widehat{\Phi}^n}{\Phi - \widehat{\Phi}} = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right)$$

Nun ist $-0{,}7 < \frac{1-\sqrt{5}}{2} < -0{,}6$. Also fällt die Folge $\left(\frac{1-\sqrt{5}}{2}\right)^n$ (alternierend) exponentiell schnell gegen Null. Wir erhalten

$$F_n = \left[\frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^n \right]$$

Hierbei bezeichnet $[x]$ die nächste ganze Zahl mit kaufmännischem Runden, also gilt beispielsweise $[\pi] = 3 < [3{,}5] = 4$.

Fibonaccizahlen durch Exponentation einer Matrix

Setze

$$M_1 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} F_0 & F_1 \\ F_1 & F_2 \end{pmatrix}$$

Dann gilt:

$$M_1^n = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^n = \begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix}$$

Wir können also F_n (ohne Rundungsfehler mit exakter Arithmetik) in $\mathcal{O}(\log n)$ Schritten berechnen, indem wir $M_n = M_1^n \in \mathbb{Z}^{2\times 2}$ mittels schneller Exponentation bestimmen.

Selbsttest

- Was ist F_{33} mod 35?

F_{33} mod 5

$$M_3 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

$$\begin{aligned} M_5 &= \begin{pmatrix} 3 & 5 \\ 5 & 8 \end{pmatrix} \\ &\equiv \begin{pmatrix} -2 & 0 \\ 0 & -2 \end{pmatrix} \equiv -2 \bmod 5 \end{aligned}$$

$$M_{30} = (M_5)^6 \equiv (-2)^6 \equiv -1 \bmod 5$$

$$M_{33} = M_{30} \cdot M_3 \equiv \begin{pmatrix} -1 & -2 \\ -2 & -1 \end{pmatrix} \bmod 5$$

Also ist $F_{33} \equiv 3 \bmod 5$ und man sieht auch $F_{32} \equiv F_{34} \equiv 4 \bmod 5$.

F_{33} mod 7

$$M_1 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

$$M_1^8 = \begin{pmatrix} 13 & 21 \\ 21 & 34 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$M_1^{16} = M_1^{32} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Also ist $F_{33} \equiv 1 \bmod 7$ und wegen $F_{33} \equiv 3 \bmod 5$ folgt $F_{33} \equiv 8 \bmod 35$.

Eine überraschende Beziehung für Fibonacci-Zahlen mit einem bemerkenswert einfachem Beweis

Theorem

$$\mathrm{ggT}(F_m, F_n) = F_{\mathrm{ggT}(m,n)}$$

Teil 1. Beweis von $F_{\mathrm{ggT}(m,n)} \mid \mathrm{ggT}(F_m, F_n)$

Sei $g = \mathrm{ggT}(m, n)$. Es reicht, $F_g \mid F_n$ zu zeigen. Schreibe $n = gk$ und rechne modulo F_g:

$$\begin{aligned}
\begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix} &= \begin{pmatrix} F_{g-1} & F_g \\ F_g & F_{g+1} \end{pmatrix}^k \\
&\equiv \begin{pmatrix} F_{g-1} & 0 \\ 0 & F_{g+1} \end{pmatrix}^k \bmod F_g \\
&\equiv \begin{pmatrix} F_{g-1}^k & 0 \\ 0 & F_{g+1}^k \end{pmatrix} \bmod F_g
\end{aligned}$$

Hieraus folgt $F_g \mid F_n$, also die Behauptung von Teil 1.

Teil 2. Beweis von $\mathrm{ggT}(F_m, F_n) \mid F_{\mathrm{ggT}(m,n)}$

Ohne Einschränkung ist $0 < m < n$. Sei $g = \mathrm{ggT}(F_m, F_n)$. Schreibe $n = mk + r$ mit $0 \leq r < m < n$. Es reicht, $g \mid F_r$ zu zeigen. Denn dann gilt mit Induktion $g \mid F_{\mathrm{ggT}(r,m)} = F_{\mathrm{ggT}(m,n)}$

$$\begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix} = \begin{pmatrix} F_{m-1} & F_m \\ F_m & F_{m+1} \end{pmatrix}^k \cdot \begin{pmatrix} F_{r-1} & F_r \\ F_r & F_{r+1} \end{pmatrix}$$

$$\begin{pmatrix} F_{n-1} & 0 \\ 0 & F_{n+1} \end{pmatrix} \equiv \begin{pmatrix} F_{m-1} & 0 \\ 0 & F_{m+1} \end{pmatrix}^k \cdot \begin{pmatrix} F_{r-1} & F_r \\ F_r & F_{r+1} \end{pmatrix}$$

$$\equiv \begin{pmatrix} * & F_{m-1}^k \cdot F_r \\ * & * \end{pmatrix} \bmod g$$

Wir müssen also nur noch zeigen, dass F_{m-1} und F_m teilerfremd sind. Denn dann sind auch F_{m-1} und g teilerfremd, da $g \mid F_m$.

Teil 3. Beweis von $\mathrm{ggT}(F_m, F_{m-1}) = 1$

Es gilt $\det M_1 = \det \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = -1$, also ist

$$\begin{aligned} \det \begin{pmatrix} F_{m-1} & F_m \\ F_m & F_{m+1} \end{pmatrix} &\equiv \det \begin{pmatrix} F_{m-1} & 0 \\ 0 & F_{m+1} \end{pmatrix} \\ &\equiv F_{m-1}F_{m+1} \equiv (-1)^m \bmod F_m \end{aligned}$$

Insbesondere sind F_{m-1} und F_m teilerfremd. qed

Das Rechnen modulo n

Es sei n eine ganze Zahl, tatsächlich reicht für das Folgende die Annahme $n \in \mathbb{N}$. Für $a, b \in \mathbb{Z}$ schreiben wir

$$a \equiv b \bmod n$$

falls $a - b$ ein ganzzahliges Vielfaches von n ist, d. h. falls $a - b \in n\mathbb{Z}$ gilt.

Für $n = 0$ heißt dies $a = b$.

Für $n = 1$ gilt dies für alle $a, b \in \mathbb{Z}$.

Wir definieren (bei festem n) Klassen

$$[a] = \{\, b \in \mathbb{Z} \mid a \equiv b \bmod n \,\}.$$

$[a]$ heißt Restklasse (von a). Jedes $b \in [a]$ heißt Vertreter (oder Repräsentant) der Restklasse $[a]$.
Damit erhalten wir den „Restklassenring“ $\mathbb{Z}/n\mathbb{Z}$ wie folgt:

$$\mathbb{Z}/n\mathbb{Z} = \{\, [a] \mid a \in \mathbb{Z} \,\} = \{\, [0], \ldots, [n-1] \,\}.$$

Restklassen

Ohne Einschränkung sei $n \neq 0$. Mit $a \bmod n$ bezeichnen wir die eindeutig bestimmte Zahl $r \in \{0, \ldots |n| - 1\}$ mit $a \equiv r \mod n$ und nennen diese die *Restklasse* von a modulo n. Die Zahl r ist der Rest beim Teilen von a durch n. Für alle $k \in \mathbb{Z}$ gilt:

$$\mathbb{Z}/n\mathbb{Z} = \{ [a \bmod n] \mid a \in \mathbb{Z} \} = \{ [-k], \ldots, [n-1-k] \}.$$

Also für $n = 2^{32}$ kann man darstellen:

$$\mathbb{Z}/2^{32}\mathbb{Z} = \{ [-2^{31}], \ldots, [2^{31} - 1] \}$$

Das erste Bit sagt, ob die Zahl negativ ist.

Genauer:
Der Rechner stellt die Restklassen intern mit Hilfe des Vertretersystems $0, \ldots, 2^{32} - 1$ dar, interpretiert sie aber (z. B. bei der Ausgabe) gemäß des Vertretersystems $-2^{31}, \ldots, 2^{31} - 1$. Somit besagt das erste Bit der internen Darstellung, ob die Zahl negativ ist.

Ringeigenschaft der Menge $\mathbb{Z}/n\mathbb{Z}$

Die entscheidende Beobachtung der modularen Arithmetik besteht darin, dass man mit Restklassen addieren und multiplizieren kann wie mit ganzen Zahlen. Es gilt:

$$(k \bmod n) + (\ell \bmod n) \equiv k + \ell \mod n$$
$$(k \bmod n) \cdot (\ell \bmod n) \equiv k \cdot \ell \mod n$$

Damit ist $\mathbb{Z}/n\mathbb{Z}$ ein Ring.

- Für $n = 0$ heißt dies $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}$ (und $\mathbb{Z}/0\mathbb{Z}$ ist unendlich).
- Für $n = 1$ heißt dies $\mathbb{Z}/n\mathbb{Z} = \{\,[0]\,\}$ (also $0 \equiv 1$).
- Für $n > 1$ kann $\mathbb{Z}/n\mathbb{Z}$ mit der Menge $\{\,0, 1, \ldots, n-1\,\}$ identifiziert werden.

Ringe

Ein *Ring* R ist gegeben durch ein Tupel $(R, 0, 1, +, \cdot)$ mit:

1. $(R, +, 0)$ ist eine abelsche Gruppe, also $0 \in R$ und

$$\forall x \forall y \forall z \colon 0 + x = x,\ x + y = y + x,\ (x + y) + z = x + (y + z)$$
$$\forall x \exists! y : x + y = 0$$

d. h., es gibt genau ein y, nenne dieses $(-x)$

2. $(R, \cdot, 1)$ ist ein Monoid, also $1 \in R$ und

$$\forall x \forall y \forall z \colon 1 \cdot x = x \cdot 1 = x,\ (x \cdot y) \cdot z = x \cdot (y \cdot z)$$

3. Es gelten die Distributivgesetze:

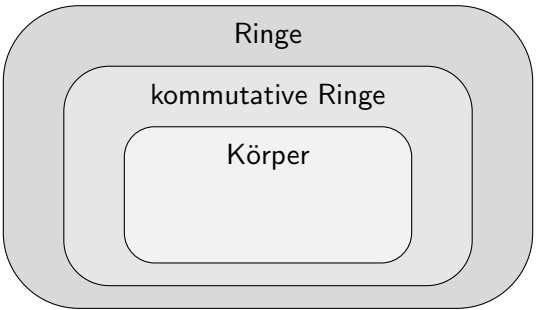
$$\begin{aligned} \forall x \forall y \forall z : (x + y) \cdot z &= x \cdot z + y \cdot z \\ z \cdot (x + y) &= z \cdot x + z \cdot y \end{aligned}$$

Kommutative Ringe und Körper

Ein Ring R heißt *kommutativ*, falls die Multiplikation kommutativ ist:

$$\forall x \forall y : x \cdot y = y \cdot x.$$

Einen kommutativen Ring, bei dem $(R \setminus \{0\}, \cdot, 1)$ eine Gruppe ist, nennen wir *Körper*. In diesem Fall nennt man $(R \setminus \{0\}, \cdot, 1)$ die *multiplikative Gruppe*. Insbesondere ist in Körpern $0 \neq 1$. Die Menge der multiplikativ invertierbaren Elemente ist die *Einheitengruppe* von R und wird mit R^* bezeichnet. In einem Körper R gilt $R^* = R \setminus \{0\}$.



Beispiele

Unsere Standardbeispiele sind:

1. $\mathbb{Z}$ = ganze Zahlen.
2. Körper: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ = rationale, reelle, komplexe Zahlen.
3. (Endliche) Restklassenringe $\mathbb{Z}/n\mathbb{Z}$.
4. Endliche Körper $\mathbb{Z}/p\mathbb{Z}$ für Primzahlen p.
5. Matrizenringe $R^{n\times n}$ über einem (kommutativen) Ring R.
6. Polynomringe $R[X]$ über einem (kommutativen) Ring R, wobei häufig R sogar ein Körper ist.
7. $\mathbb{N}$ ist kein Ring, nur ein „*Halbring*“.

Weitere Themen

1. **Erweiterter ggT.** Seien $m, n \in \mathbb{Z}$ und $g = \mathrm{ggT}(m, n)$. Dann lassen sich in $\mathcal{O}(\log n)$ Schritten Zahlen $a, b \in \mathbb{Z}$ bestimmen so, dass:

$$g = am + bn.$$

2. **Korollar:** Sei $\mathrm{ggT}(m, n) = 1$. Dann gibt es $a \in \mathbb{Z}$ mit $am \equiv 1 \bmod n$ (und $\mathrm{ggT}(a, n) = 1$), also

$$(\mathbb{Z}/n\mathbb{Z})^* = \{\, [a] \in \mathbb{Z}/n\mathbb{Z} \mid \mathrm{ggT}(a, n) = 1 \,\}.$$

3. **Korollar:** $\mathbb{Z}/n\mathbb{Z}$ ist genau dann ein Körper, wenn n eine Primzahl ist.
4. **Kleiner Satz von Fermat:** Sei p eine Primzahl, dann ist

$$a^{p-1} \equiv 1 \bmod p, \text{ falls } \mathrm{ggT}(a, p) = 1$$

Was ist 137^{-1} modulo 523?

Die Zahlen 523 und 137 sind Primzahlen, insbesondere gilt $\mathrm{ggT}(523, 137) = 1$.

	q	a	b	Kontrolle
		-11	42	$1 = -11 \cdot 523 + 42 \cdot 137$
$523 = 3 \cdot 137 + 112$	3	9	-11	$1 = 9 \cdot 137 - 11 \cdot 112$
$137 = 1 \cdot 112 + 25$	1	-2	9	$1 = -2 \cdot 112 + 9 \cdot 25$
$112 = 4 \cdot 25 + 12$	4	1	-2	$1 = 1 \cdot 25 - 2 \cdot 12$
$25 = 2 \cdot 12 + 1$	2	0	1	$1 = 0 \cdot 12 + 1 \cdot 1$

Chinesischer Restsatz

Seien $\mathrm{ggT}(p, q) = 1$ und $n = pq$. Dann gibt es einen Ringisomorphismus:

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} &\to \quad \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \\ m \bmod n &\mapsto (m \bmod p,\ m \bmod q) \end{aligned}$$

Beweis. Links und rechts stehen endliche Mengen mit jeweils n Elementen.
Euklid liefert ganze Zahlen a, b mit $1 = ap + bq$.
Zu $(r, s) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ betrachte $m = sap + rbq$.
Dann gilt

$$(m \bmod p,\ m \bmod q) = (r, s)$$

Also wird jedes Paar getroffen und der Ringhomomorphismus ist bijektiv. qed

Alice und Bob

Die RSA-Verschlüsselung nach Rivest, Shamir und Adleman:

1.) Alice wählt große Primzahlen p, q mit $p \neq q$.
Beispiel: $p = 5, q = 11$.

2.) Sie berechnet $n = pq$ und $\varphi(n) = (p-1)(q-1)$. Im Beispiel $\varphi(n) = 40$.

3.) Sie wählt $e > 1$ mit $\mathrm{ggT}(e, \varphi(n)) = 1$. Oft kann $e = 3$ eine gute Wahl sein. Im Beispiel gilt $\mathrm{ggT}(3, 40) = 1$.

4.) Sie berechnet s mit $es \equiv 1 \bmod \varphi(n)$. Im Beispiel $s = 27$.

5.) Sie veröffentlicht (n, e).

6.) Bob verschlüsselt eine Nachricht $0 \leq x \leq n-1$ durch

$$y = x^e \bmod n$$

7.) Alice entschlüsselt y durch $y^s \bmod n$. Dies ist korrekt, da
$x^{es} = x^{1+k\varphi(n)} \equiv x \bmod n$ für alle x gilt.

Alice is clever

Angenommen mit dem öffentlichen Paar $(n, e) = (55, 3)$ empfängt Alice den Wert $y = 18$ von Bob. Sie muss also

$$18^{27} \bmod 55$$

ausrechnen. Da sie clever ist, benutzt sie den chinesischen Restsatz. Sie rechnet zunächst modulo 5, dann modulo 11:

$$18^{27} \equiv 3^{3+24} \equiv 3^3 \equiv 27 \equiv 2 \bmod 5$$

$$18^{27} \equiv (-4)^{7+20} \equiv -4^7 \equiv -2^{4+10} \equiv -16 \equiv 6 \bmod 11$$

Wir wissen $1 = -2 \cdot 5 + 11$, also erhalten wir für $(r, s) = (2, 6)$ den Wert x durch:

$$m = -10 \cdot 6 + 11 \cdot 2 = -60 + 22 = -38 \equiv 17 \bmod 55$$

Alice kann also 18 durch die Zahl $x = 17$ entschlüsseln.

Wie sicher ist RSA?

Man weiß nicht viel, aber immerhin:

Satz

Für ein RSA-Paar (n, e) sind die folgenden Probleme sind in etwa gleich schwierig.

1. *Faktorisiere n in $n = p \cdot q$.*
2. *Finde $\varphi(n) = (p-1)(q-1)$.*
3. *Finde ein s mit $es \equiv 1 \bmod \varphi(n)$.*

Beweisskizze des Satzes

Die Lösung von 1) liefert 2), die von 2) liefert 3).
Sei jetzt s mit $es \equiv 1 \bmod \varphi(n)$ bekannt. Also $es - 1 = m(p-1)(q-1)$ für ein $m \in \mathbb{Z}$.
Schreibe $es - 1 = 2^k u$ mit u ungerade und $k \geq 2$.
Wähle $a \in \{1, \ldots, n-1\}$ zufällig.
Wir können $\mathrm{ggT}(a, n) = 1$ annehmen. Warum?
Setze

$$b \equiv a^u \bmod n.$$

Dann gibt es ein kleinstes $0 \leq t \leq k$ mit $b^{2^t} \equiv 1 \bmod n$. Warum?
Dieses finden wir nach höchstens $k \in \mathcal{O}(\log n)$ Schritten. Man weiß, dass für ein $r \in \{p, q\}$ die Wahrscheinlichkeit mindestens $1/2$ ist, dass $t > 1$ und $b^{2^s} \equiv 1 \bmod r$ für $s = t - 1$ gilt. Ohne Einschränkung sei $p = r$, also $b^{2^s} \equiv 1 \bmod p$.
Da t minimal ist, gilt $b^{2^s} \not\equiv 1 \bmod n$ und damit:

$$\mathrm{ggT}(b^{2^s} - 1,\ n) = p.$$

RSA-640 wurde am 2.11.2005 faktorisiert

RSA-640:

$$
\begin{aligned}
&310741824049004372135075003588856793003734602284272\\
&754572016194882320644051808150455634682967172328678\\
&243791627283803341547107310850191954852900733772482\\
&27835257423864540146917366024776523466 09\\
&=\\
&163473364580925384844313388386509085984178367003 30\\
&923121811108523893331001045081512121181675115 79\\
&\times\\
&190087128166482211312685157393541397547189678996851\\
&549366663853908802710380210449895719126146557 1
\end{aligned}
$$

RSA-768 wurde am 12.12.2009 faktorisiert

RSA-768:

$$
\begin{aligned}
&123018668453011775513049495838496272077285356959533\\
&479219732245215172640050726365751874520219978646938\\
&995647494277406384592519255732630345373154826850791\\
&702612214291346167042921431160222124047927473779408\\
&06653514195974598569021434 13\\
&=\\
&334780716989568987860441698482126908177047949837137\\
&685689124313889828837938780022876147116525317430877\\
&37814467999489\\
&\times\\
&367460436667995904282446337996279526322791581643430\\
&876426760322838157396665112792333734171433968102700
\end{aligned}
$$

Die Faktoren von RSA-1024 sind nicht öffentlich bekannt

RSA-1024:

135066410865995223349603216278805969938881475605667
027524485143851526510604859533833940287150571909441
798207282164471551373680419703964191743046496589274
256239341020864383202110372958725762358509643110564
073501508187510676594629205563685529475213500852879
416377328533906109750544334999811150056977236890927
563

Bekanntes von RSA

Bekannt seit 2009: RSA-768 wurde faktorisiert.

Bekannt: Die Methode des Zahlkörpersiebs.

Bestätigt wurde auch die Abschätzung des Aufwands, um eine Zahl n (also $\log_2 n$ Bits) zu faktorisieren:

$$e^{((64/9)^{1/3}+o(1))(\ln n)^{1/3}(\ln \ln n)^{2/3}}$$

Quelle: `http://eprint.iacr.org/2010/006.pdf` vom 07.01.2010
Aufwand: Allein die Stromkosten, um diese eine Zahl RSA-768 zu faktorieren, wurden (von uns) zwischen 50.000 und 200.000 Euro geschätzt. Wenn man den Aufwand, RSA-1024 1000 mal höher einschätzt, kommen wir also auf (mindestens) 50 Millionen Euro Stromkosten, um RSA-1024 zu faktorisieren.

Das Wachstum der Fakultätsfunktion

Die Folgen $n!$ und 2^n lassen sich induktiv definieren:

$$0! = 2^0 = 1, \quad (n+1)! = (n+1)n! \quad \text{und} \quad 2^{n+1} = 2 \cdot 2^n$$

Einige Anfangswerte finden sich in der folgenden Tabelle:

n	0	1	2	3	4 ...	10	...	20
2^n	1	2	4	8	16 ...	1024	...	1048576
$n!$	1	1	2	6	24 ...	3628800	...	2432902008176640000

Erste Schätzwerte

Grobe, aber häufig brauchbare Schätzwerte für 2^{10} und 2^{20} sind also 1000 und 1 Million, wobei der Fehler bei 1 Million bei etwa 5% liegt.
Für $n \geq 4$ gilt stets $n! > 2^n$.
Eine unmittelbare untere Schranke für $n!$ erhalten wir durch die Beobachtung, dass in dem Produkt $n!$ mindestens die Hälfte der Faktoren so groß sind wie $\frac{n}{2}$. Hieraus ergibt sich $(\frac{n}{2})^{\frac{n}{2}} \leq n!$; zusammen mit der oberen Schranke n^n ergibt sich:

$$\log n! \in \Theta(n \log n)$$

Wir wollen jetzt eine genauere Schranke für $n!$ herleiten.

Integralabschätzung

Offensichtlich ist für $n \geq 2$:

$$\ln n! = \ln 2 + \ln 3 + \cdots + \ln n$$

Ein (selbst zu zeichnendes) Schaubild zeigt:

$$\ln(n-1)! < \int_1^n \ln x \, dx < \ln n!$$

Die Stammfunktion von $\ln x$ ist $x \ln x - x + C$. Damit erhalten wir:

$$\ln(n-1)! < n \ln n - n + 1 < \ln n!$$

Es folgt:

$$(n-1)! < e \cdot \left(\frac{n}{e}\right)^n < n!$$

Es gilt für $n \geq 1$ (mit Gleichheit nur bei $n = 1$):

$$e \left(\frac{n}{e}\right)^n \leq n! \leq ne \left(\frac{n}{e}\right)^n$$

Stirlingsche Formel

Tatsächlich lassen sich durch eine genauere Untersuchung bessere Resultate erzielen. Insbesondere gilt die *Stirlingsche Formel*:

$$n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$$

Für $n = 20$ liefert die Stirlingsche Formel den Wert $2{,}42 \cdot 10^{18}$, was verglichen mit dem Tabelleneintrag für 20! von etwas mehr als $2{,}43 \cdot 10^{18}$ ziemlich gut ist. Unsere Integralabschätzung liefert $0{,}58 \cdot 10^{18} \leq 20! \leq 11{,}75 \cdot 10^{18}$.

Binomialkoeffizienten

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}, \qquad \text{für } 0 \le k \le n \in \mathbb{N}$$

Wir definieren hier allgemeiner $\binom{x}{k}$ als Polynom in x mit rationalen Koeffizienten für alle $k \in \mathbb{Z}$.
Für $k < 0$ sei $\binom{x}{k} = 0$ das Nullpolynom (vom Grad $-\infty$).
Für $k \ge 0$ sei die *fallende Faktorielle* das Polynom vom Grad k:

$$x^{\underline{k}} = x(x-1)\cdots(x-k+1)$$

und damit definieren wir den *Binomialkoeffizienten*:

$$\binom{x}{k} = \frac{x^{\underline{k}}}{k!} = \frac{x(x-1)\cdots(x-k+1)}{k!}$$

Für $k = 0$ ergibt sich das konstante Polynom $\binom{x}{0} = 1$ vom Grad Null.

Aufwärmübungen

Für $k \geq 0$ hat $\binom{x}{k}$ die Nullstellen $0, \ldots, k-1$.

Falls $x = n$ eine natürliche Zahl mit $n < k$ ist, so ist einer der Faktoren im Zähler 0, also auch $\binom{n}{k} = 0$.

Für $x < 0$ und $k \geq 0$ gilt stets $\binom{x}{k} \neq 0$.
Für $k \geq 0$ gilt:

$$\binom{-1}{k} = \frac{(-1) \cdot (-2) \cdots (-k)}{k!} = (-1)^k$$

$$\binom{1/2}{3} = \frac{(1/2) \cdot (-1/2) \cdot (-3/2)}{3!} = \frac{1}{16}$$

Sparen der Summationsgrenzen

Dadurch, dass Binomialkoeffizienten für alle $k \in \mathbb{Z}$ definiert sind, können wir uns oft Summationsgrenzen ersparen, was die Formeln übersichtlicher macht und Induktionsbeweise vereinfacht.

Addititionstheorem

Die folgende Identität ist nach Blaise Pascal (1623–1662) benannt:

Satz (Addititionstheorem)

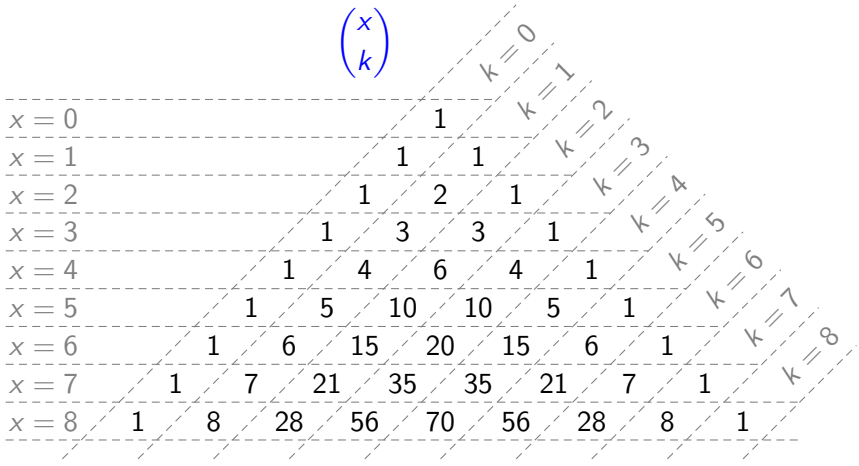
$$\binom{x}{k} = \binom{x-1}{k} + \binom{x-1}{k-1}$$

Beweis. Der Satz gilt für $k \leq 0$. Für $k > 0$ schreiben wir

$$\binom{x-1}{k} + \binom{x-1}{k-1} =$$
$$\frac{(x-1)\cdots(x-k+1)(x-k)}{k!} + \frac{(x-1)\cdots(x-k+1)\cdot k}{(k-1)!\cdot k} =$$
$$\frac{x(x-1)\cdots(x-k+1)}{k!} = \binom{x}{k}$$

qed

Pascalsches Dreieck



Ganzzahligkeit

Eine unmittelbare Konsequenz des Addititionstheorems ist die Ganzzahligkeit der Binomialkoeffizienten $\binom{n}{k}$ für $n \in \mathbb{N}$ (bzw. sogar $n \in \mathbb{Z}$), die dem Bruch $\frac{n \cdots (n-k+1)}{k!}$ nicht direkt anzusehen ist.

Korollar

Es gilt $\binom{n}{k} \in \mathbb{Z}$ für alle $n, k \in \mathbb{Z}$

Beweis. Dies folgt aus den folgenden Überlegungen:

1. Es ist $\binom{n}{k} \in \mathbb{Z}$ für $k < 0$.
2. Es ist $\binom{0}{k} \in \mathbb{Z}$ für $k \in \mathbb{Z}$.
3. Mit Induktion nach k folgt für alle $n \in \mathbb{Z}$:

$$\binom{n}{k} \in \mathbb{Z} \iff \binom{n-1}{k} \in \mathbb{Z}$$

qed

Binomialsatz

Satz

Es gilt:

$$(x+y)^n = \sum_k \binom{n}{k} x^k y^{n-k}$$

Beweis des Binomialsatzes

Der Satz gilt für $n = 0$. Für $n > 0$ verwenden wir Induktion und das Additionstheorem: $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$. Damit können wir schreiben

$$
\begin{aligned}
(x+y)^n &= (x+y)(x+y)^{n-1} \\
&= (x+y)\sum_k \binom{n-1}{k} x^k y^{n-1-k} \\
&= \left(\sum_k \binom{n-1}{k} x^{k+1} y^{n-1-k}\right) + \left(\sum_k \binom{n-1}{k} x^k y^{n-k}\right) \\
&= \left(\sum_k \binom{n-1}{k-1} x^k y^{n-k}\right) + \left(\sum_k \binom{n-1}{k} x^k y^{n-k}\right) \\
&= \sum_k \left(\binom{n-1}{k-1} + \binom{n-1}{k}\right) x^k y^{n-k} \\
&= \sum_k \binom{n}{k} x^k y^{n-k}
\end{aligned}
$$

Top 10: $k, m, n \in \mathbb{Z}$ und $r, x, y \in \mathbb{C}$

$\binom{n}{k} = \frac{n!}{k!(n-k)!}$	$n \geq k \geq 0$	factorial expansion
$\binom{n}{k} = \binom{n}{n-k}$	$n \geq 0$	symmetry
$\binom{x}{k} = \frac{x}{k}\binom{x-1}{k-1}$	$k \neq 0$	absorption/extraction
$\binom{x}{k} = \binom{x-1}{k} + \binom{x-1}{k-1}$		addition/induction
$\binom{x}{k} = (-1)^k \binom{k-x-1}{k}$		upper negation
$\binom{x}{m}\binom{m}{k} = \binom{x}{k}\binom{x-k}{m-k}$		trinomial revision
$\sum_k \binom{r}{k} x^k y^{r-k} = (x+y)^r$	$r \in \mathbb{N}$ or $\left\lvert\frac{x}{y}\right\rvert < 1$	binomial theorem
$\sum_{k \leq n} \binom{x+k}{k} = \binom{x+n+1}{n}$		parallel summation
$\sum_{0 \leq k \leq n} \binom{k}{m} = \binom{n+1}{m+1}$	$m, n \geq 0$	upper summation
$\sum_k \binom{x}{k}\binom{y}{n-k} = \binom{x+y}{n}$		Vandermonde convolution

Leitmotiv

Beweise und verstehe Identitäten mit Hilfe einer kombinatorischen Interpretation (sofern möglich) und versuche dann die Polynommethode.

Die Polynommethode besagt, dass zwei Polynome (mit Koeffizienten $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ oder $\mathbb{C}$) identisch sind, wenn sie an unendlich vielen Stellen übereinstimmen. Der Grund ist, dass ein Polynom vom Grad $d \geq 0$ in einem nullteilerfreien Ring nicht mehr als d Nullstellen haben kann.

Polynommethode und kombinatorische Interpretation

Beweise hiermit:

Additionstheorem:

$$\binom{x}{k} = \binom{x-1}{k} + \binom{x-1}{k-1}$$

Trinomial Revision:

$$\binom{x}{m}\binom{m}{k} = \binom{x}{k}\binom{x-k}{m-k}$$

Binomialsatz:

$$\sum_k \binom{r}{k} x^k y^{r-k} = (x+y)^r \quad r \in \mathbb{N} \vee \left|\frac{x}{y}\right| < 1$$

Für $r \in \mathbb{C}$ verwende Taylorreihen!

Elementares zu Binomialkoeffizienten

Der Binomialsatz und die kombinatorische Interpretation liefern sofort:

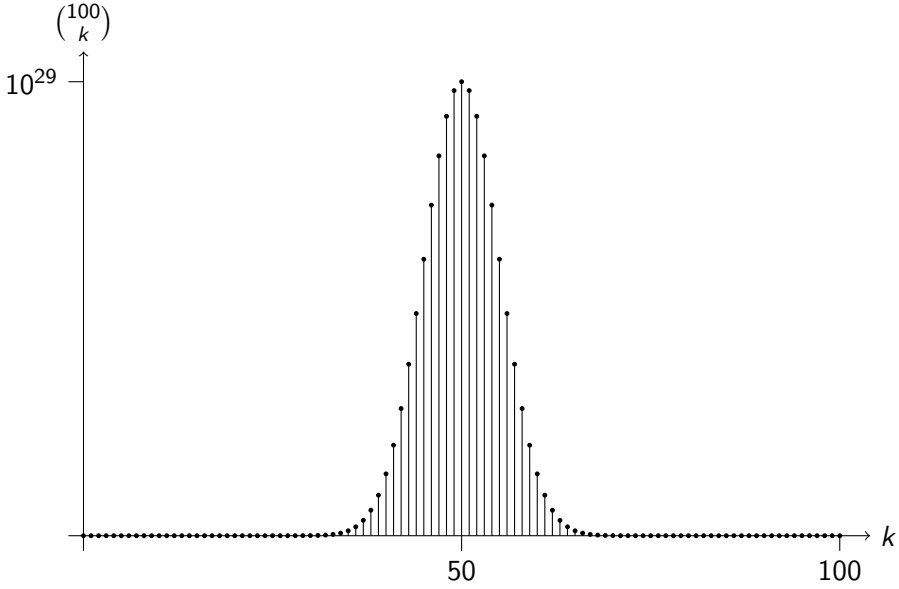
$$\sum_k \binom{n}{k} = 2^n = (1+1)^n$$

Klar ist auch:

$$1 = \binom{n}{0} < \binom{n}{1} < \cdots < \binom{n}{\lfloor \frac{n}{2} \rfloor} = \binom{n}{\lceil \frac{n}{2} \rceil} > \cdots > \binom{n}{n} = 1$$

Die Folge steigt bis zur Mitte hin an und fällt dann wieder.

Wachstum der Binomialkoeffizienten



Mehr über Binomialkoeffizienten

Für $n \geq 2$ ist $\binom{n}{\lfloor \frac{n}{2} \rfloor}$ also der größte Wert unter den n folgenden Werten $1+1$, $\binom{n}{1}$, …, $\binom{n}{n-1}$.
Damit muss $\binom{n}{\lfloor \frac{n}{2} \rfloor}$ mindestens so groß sein wie der Mittelwert. Wir erhalten für $n \geq 2$:

$$\frac{2^n}{n} \leq \binom{n}{\lfloor \frac{n}{2} \rfloor} = \binom{n}{\lceil \frac{n}{2} \rceil} < 2^n \tag{1}$$

Vermöge der Stirlingschen Formel erhält man die Asymptotik:

$$\binom{2n}{n} \sim \frac{\sqrt{4\pi n}\left(\frac{2n}{e}\right)^{2n}}{2\pi n\left(\frac{n}{e}\right)^{2n}} = \frac{4^n}{\sqrt{\pi n}}$$

Der Wert $\binom{20}{10}$ sollte also bei $\frac{2^{20}}{\sqrt{10\pi}}$ sein, was ungefähr 187000 liefert. Der tatsächliche Wert von $\binom{20}{10}$ ist 184756.

Summationen

Parallele Summation:

$$\sum_{k \le n} \binom{x+k}{k} = \binom{x+n+1}{n}$$

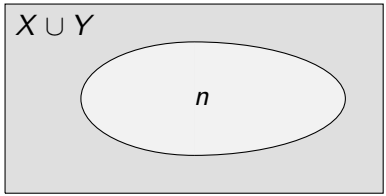
Obere Summation:

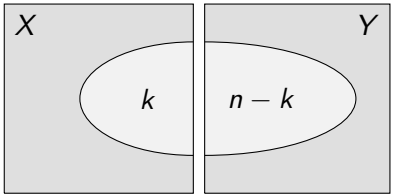
$$\sum_{0 \le k \le n} \binom{k}{m} = \binom{n+1}{m+1} \quad m, n \ge 0$$

Die folgende Gleichung ist nach dem französischen Mathematiker, Chemiker und Musiker Alexandre-Théophile Vandermonde (1735–1796) benannt:
Vandermonde Konvolution:

$$\sum_{k} \binom{x}{k} \binom{y}{n-k} = \binom{x+y}{n}$$

Beweis der Vandermondeschen Identität





Maximal t Objekte in ℓ Behältern

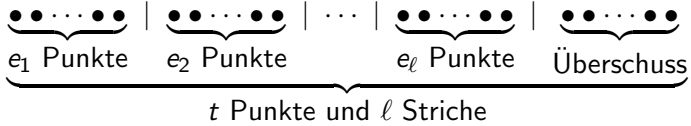
Angenommen, wir möchten bis zu t Objekte in ℓ Behälter aufteilen. Wie viele Möglichkeiten gibt es für die Behälterfüllungen? Die Antwort liefert der nächste Satz.

Satz

$$\left|\left\{ (e_1, \ldots, e_\ell) \in \mathbb{N}^\ell \;\middle|\; \sum_{1 \le k \le \ell} e_k \le t \right\}\right| = \binom{t+\ell}{\ell}$$

Maximal t Objekte in ℓ Behältern – Beweis

Beweis. Wir stellen uns $t + \ell$ Punkte vor, die in einer Reihe liegen. Wähle ℓ Punkte und ersetze diese durch Striche. Hierfür gibt es $\binom{t+\ell}{\ell}$ Möglichkeiten. Jede solche Auswahl entspricht genau einem ℓ-Tupel $(e_1, \ldots, e_\ell) \in \mathbb{N}^\ell$ mit $\sum_{k=1}^{\ell} e_k \leq t$.



Zunächst werden e_1 Punkte bis zum ersten Strich abgetragen. Nach dem ersten Strich werden e_2 Punkte abgetragen, usw. Nach dem ℓ-ten Strich kann noch ein Überschuss an Punkten folgen um insgesamt t Punkte zu erhalten. So lassen sich die Lösungen der Ungleichung und Auswahlen an Punkten und Strichen bijektiv aufeinander abbilden.
qed

Übung

Spezifikation: Ein Baum ist eine Wurzel gefolgt von einer Folge von Bäumen. Die Anzahl aller Bäume ist $\frac{1}{4n-2}\binom{2n}{n}$.
Man beweise zunächst:

$$\frac{-1}{2}\binom{\frac{1}{2}}{n}(-4)^n = \frac{1}{n}\binom{2n-2}{n-1} = \frac{1}{4n-2}\binom{2n}{n}.$$

Direktes Nachrechnen zeigt:

$$\frac{1}{n}\binom{2n-2}{n-1} = \frac{2n(2n-1)}{2n(2n-1)n}\binom{2n-2}{n-1} = \frac{1}{4n-2}\binom{2n}{n}.$$

Stirling Zahlen der 2. Art

Eine *Partition* einer Menge A ist eine Menge $P = \{ P_1, \ldots, P_k \}$ mit $\bigcup_{1 \leq i \leq k} P_i = A$, mit $P_i \neq \emptyset$ für alle $1 \leq i \leq k$ und mit $P_i \cap P_j = \emptyset$ für alle $1 \leq i < j \leq k$.

$$\left\{ n \atop k \right\} := |\{ P \mid P \text{ ist eine Partition von } \{1, \ldots, n\} \text{ in } k \text{ Klassen } \}|$$

In der kombinatorischen Interpretation bezeichnet $\left\{ n \atop k \right\}$ die obige Menge für $n \in \mathbb{N}$ und $k \in \mathbb{Z}$.

Beispiele

$$\left\{ n \atop n \right\} = 1 \quad \text{für } n \geq 0 \qquad \left\{ n \atop 0 \right\} = 0 \quad \text{für } n \geq 1$$

$$\left\{ n \atop k \right\} = 0 \quad \text{für } n < 0 \leq k \qquad \left\{ n \atop k \right\} = 0 \quad \text{für } 0 \leq n < k$$

$$\left\{ n \atop k \right\} > 1 \quad \text{für } n > k > 1 \qquad \left\{ n \atop 1 \right\} = 1 \quad \text{für } n \geq 1$$

$$\left\{ n \atop 2 \right\} = 2^{n-1} - 1 \quad \text{für } n \geq 1 \qquad \left\{ n \atop n-1 \right\} = \binom{n}{2} \quad \text{für } n \geq 1$$

Additionstheorem für Stirling-Zahlen zweiter Art

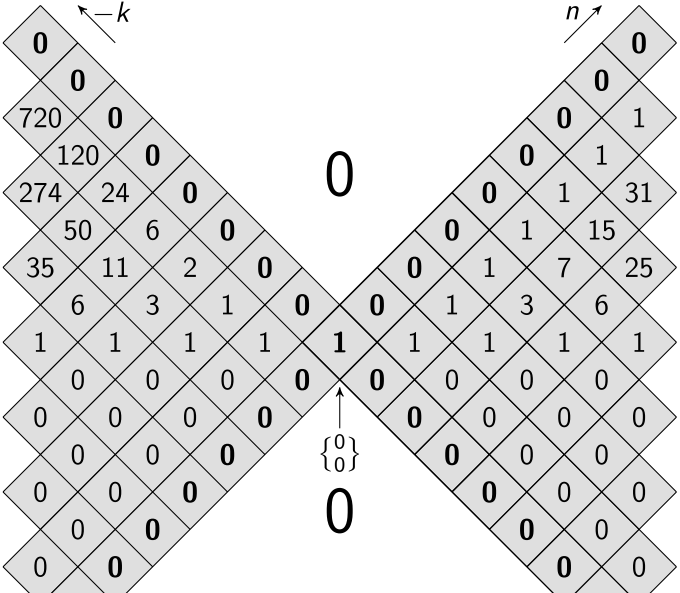
Theorem

$$\left\{ {n \atop k} \right\} = \left\{ {n-1 \atop k-1} \right\} + k \left\{ {n-1 \atop k} \right\}$$

Erweitere $\left\{ {n \atop k} \right\}$ durch $\left\{ {n \atop 0} \right\} = [n = 0]$ für alle $n \in \mathbb{Z}$ und dann mit dem Theorem für alle $n, k \in \mathbb{Z}$.
Dann können wir die Identität wie folgt umschreiben:

$$\left\{ {-k \atop -n} \right\} = \left\{ {-(k-1) \atop -(n-1)} \right\} + (n-1) \left\{ {-k \atop -(n-1)} \right\} \tag{2}$$

Stirling'scher Schmetterling



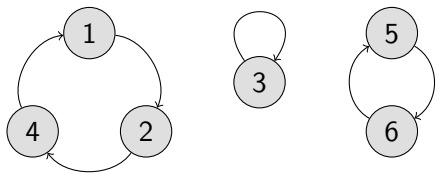
Zykelschreibweise für Permutationen

Beispiel

Sei $A = \{1, 2, 3, 4, 5, 6\}$. *Dann entspricht* $\pi = (1, 2, 4)(3)(5, 6)$*:*

i	1	2	3	4	5	6
$\pi(i)$	2	4	3	1	6	5

Diese Permutation besteht aus 3 *Zykeln. Weitere Schreibweisen sind z.B.* $(2, 4, 1)(5, 6)(3)$ *oder* $(3)(6, 5)(4, 1, 2)$. *Dies lässt sich graphisch folgendermaßen veranschaulichen:*



Die Stirling-Zahlen erster Art

Die Stirling-Zahlen $\begin{bmatrix} n \\ k \end{bmatrix}$ der ersten Art geben die Anzahl der Möglichkeiten an, n Objekte in k Zykel zu arrangieren. In der Sprache der Permutationen ist dies die Anzahl der Permutationen mit k Zykeln über n Elementen.
Für $n \geq 0$ und $k \in \mathbb{Z}$ definiere:

$$\begin{bmatrix} n \\ k \end{bmatrix} = |\{ \pi \mid \pi \text{ ist Permutation von } \{1, \ldots, n\} \text{ mit } k \text{ Zykeln } \}|$$

Satz

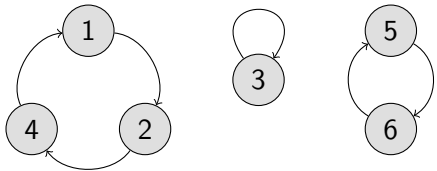
$$n! = \sum_k \begin{bmatrix} n \\ k \end{bmatrix}$$

Beispiel

Sei $A = \{1, 2, 3, 4, 5, 6\}$. Dann entspricht $\pi = (1, 2, 4)(3)(5, 6)$ folgender Permutation:

i	1	2	3	4	5	6
$\pi(i)$	2	4	3	1	6	5

Diese Permutation besteht aus drei Zykeln. Weitere Schreibweisen der selben Zykeldarstellungen sind z.B. $(2, 4, 1)(5, 6)(3)$ oder $(3)(6, 5)(4, 1, 2)$. Diese Darstellung lässt sich graphisch folgendermaßen veranschaulichen:



Einige Identitäten

$$\left\{ n \atop k \right\} \leq \left[n \atop k \right] \qquad \text{und daher} \qquad \sum_k \left\{ n \atop k \right\} \leq \sum_k \left[n \atop k \right] = n! \tag{3}$$

$$\left[0 \atop 0 \right] = 1 \qquad \left[n \atop 0 \right] = 0 \quad \text{für } n \geq 1$$

$$\left[n \atop n \right] = 1 \quad \text{für } n \geq 0 \qquad \left[n \atop k \right] = 0 \quad \text{für } 0 \leq n < k$$

$$\left[n \atop k \right] = 0 \quad \text{für } n < 0 \leq k \qquad \left[n \atop 1 \right] = (n-1)! \quad \text{für } n \geq 1$$

$$\left[n \atop k \right] > 1 \quad \text{für } n > k > 1 \qquad \left[n \atop n-1 \right] = \left\{ n \atop n-1 \right\} = \binom{n}{2} \quad \text{für } n \geq 1$$

$$\left[n \atop 2 \right] = (n-1)!\, H(n-1) \quad \text{für } n \geq 1$$

Additionstheorem

Theorem (Additionstheorem für Stirlingsche Zahlen der 1. Art)

$$\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} + (n-1) \begin{bmatrix} n-1 \\ k \end{bmatrix}$$

Beweis des Additionstheorems

Beweis. Wir zeigen das Additionstheorem für $n \geq 1$ und $k \in \mathbb{Z}$. Auf der linken Seite zählen wir alle Permutationen von $\{1, \ldots, n\}$ mit k Zykeln. Diese lassen sich in zwei Typen einteilen: Der erste Typ enthält (n) als Zykel und der zweite Typ nicht. Die Permutationen des ersten Typs entstehen, indem man den Zykel (n) zu einer Permutation von $\{1, \ldots, n-1\}$ mit $k-1$ Zykeln hinzunimmt. Hierfür gibt es $\left[\begin{smallmatrix} n-1 \\ k-1 \end{smallmatrix}\right]$ Möglichkeiten.

Die vom 2. Typ erhält man, indem man bei einer Permutation von $\{1, \ldots, n-1\}$ mit k Zykeln das Element n einfügt. Es gibt $\left[\begin{smallmatrix} n-1 \\ k \end{smallmatrix}\right]$ solche Permutationen, und bei jeder haben wir $n-1$ Möglichkeiten, das Element n direkt hinter einem der $n-1$ anderen Elemente in einen Zykel einzufügen. qed

Das Wachstum des kleinsten gemeinsamen Vielfachen

Der Abschnitt basiert auf einem Artikel von Mohan Nair von 1982.

$$
\begin{aligned}
\mathrm{kgV}(5) &= 2^2 \cdot 3 \cdot 5 &&= 60\\
\mathrm{kgV}(6) &= 2^2 \cdot 3 \cdot 5 &&= 60\\
\mathrm{kgV}(7) &= 2^2 \cdot 3 \cdot 5 \cdot 7 &&= 420\\
\mathrm{kgV}(8) &= 2^3 \cdot 3 \cdot 5 \cdot 7 &&= 840\\
\mathrm{kgV}(9) &= 2^3 \cdot 3^2 \cdot 5 \cdot 7 &&= 2\,520\\
\mathrm{kgV}(23) &= 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 &&= 140\,900\,760\\
\mathrm{kgV}(25) &= \mathrm{kgV}(23) \cdot 5 &&= 704\,503\,800\\
\mathrm{kgV}(26) &= \mathrm{kgV}(25)\\
\mathrm{kgV}(27) &= \mathrm{kgV}(25) \cdot 3 &&= 2\,113\,511\,400\\
\mathrm{kgV}(31) &= \mathrm{kgV}(27)
\end{aligned}
$$

Lemma: ein Primzahldichtesatz

Für alle $m, n \in \mathbb{N}$ mit $1 \leq m \leq n$ gilt

$$m\binom{n}{m} \mid \mathrm{kgV}(n)$$

Beweis 1. Teil

$$I = I(n,m) = \int_0^1 x^{m-1}(1-x)^{n-m}\,dx$$

Die Auswertung geschieht auf zweifache Weise.

$$x^{m-1}(1-x)^{n-m} = \sum_k (-1)^k \binom{n-m}{k} x^{m-1+k}$$

Die Auswertung des Integrals ergibt also:

$$\begin{aligned} I(n,m) &= \sum_k (-1)^k \binom{n-m}{k} \int_0^1 x^{m-1+k}\,dx \\ &= \sum_k (-1)^k \binom{n-m}{k} \frac{1}{m+k} \end{aligned}$$

Es folgt:

$$I(n,m) \cdot \mathrm{kgV}(n) \in \mathbb{N}$$

Beweis 2. Teil, Induktionsanfang

Induktiv nach $n - m$ zeigen wir als Nächstes

$$I(n, m) = \frac{1}{m\binom{n}{m}}$$

Für $m = n$ gilt:

$$I = \int_0^1 x^{m-1}(1-x)^{n-n}\,dx = \int_0^1 x^{m-1}\,dx = \left[\frac{1}{m}x^m\right]_0^1 = \frac{1}{m} = \frac{1}{m\binom{m}{m}}$$

Sei nun $1 \leq m < n$. Durch Verwendung partieller Integration

$$\int u' \cdot v = u \cdot v - \int u \cdot v' \qquad \text{mit}$$

$$u = \frac{1}{m} x^m \qquad v = (1-x)^{n-m}$$
$$u' = x^{m-1} \qquad v' = -(n-m)(1-x)^{n-m-1}$$

ergibt sich wegen $u(1) \cdot v(1) = u(0) \cdot v(0) = 0$ zunächst

$$I = \int_0^1 x^{m-1}(1-x)^{n-m}\,dx = \int_0^1 -u \cdot v'$$
$$= \frac{n-m}{m} \int_0^1 x^{(m+1)-1}(1-x)^{n-(m+1)}\,dx$$

Mit Induktion erhalten wir

$$I = \frac{n-m}{m} \cdot \frac{1}{(m+1)\binom{n}{m+1}} = \frac{1}{m\binom{n}{m}}.$$

Damit $m\binom{n}{m} \mid \mathrm{kgV}(n)$.

Für alle $n \geq 7$ gilt: $2^n < \mathrm{kgV}(n)$

$$(2n+1)\binom{2n}{n} = (n+1)\binom{2n+1}{n+1} \mid \mathrm{kgV}(2n+1)$$

$$n\binom{2n}{n} \mid \mathrm{kgV}(2n) \mid \mathrm{kgV}(2n+1)$$

Da n und $2n+1$ teilerfremd sind, folgt

$$n(2n+1)\binom{2n}{n} \mid \mathrm{kgV}(2n+1)$$

$$n \cdot 4^n < n\,(2n+1)\binom{2n}{n} \leq \mathrm{kgV}(2n+1) \tag{4}$$

Sei $n \geq 4$. Dann gilt

$$4 \cdot 2^{2n} = 2^{2n+2} \leq n \cdot 4^n < \mathrm{kgV}(2n+1) \leq \mathrm{kgV}(2n+2)$$

Es bleiben $n = 7,\ 8 : 2^8 = 256 < 420 = \mathrm{kgV}(7) < \mathrm{kgV}(8) = 840$.