Fibonacci-Zahlen

Benannt nach Sohn des Bonacci: *Filius Bonacci* (um 1200 n.Chr.)

$$F_0 = 0 \qquad F_1 = 1 \qquad F_{n+2} = F_{n+1} + F_n$$

Die ersten Folgenglieder:

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

Rekursive Berechnung (Funktion Fib mit Inputparameter n):

IF $n < 2$ RETURN n ELSE RETURN $Fib(n-1) + Fib(n-2)$;

Iterative Berechnung ist geschickter:

Pseudocode bitte selbst entwerfen...

Fibonacci-Zahlen: Interpretation

Es gibt viele Möglichkeiten, Interpretationen für diese Zahlen zu konstruieren oder in Flora und Fauna zu finden.

Die Dominostein-Interpretation:

Es stehen beliebig viele Dominosteine von zwei Sorten zur Verfügung, nämlich solche der Länge 1 und solche der Länge 2.

Wieviele Möglichkeiten gibt es, damit eine Sequenz der Länge n zu legen?

Länge 1: eine Möglichk., Länge 2: zwei Mögl., Länge 3: drei Mögl.

Für Längen größer als 3: F_{n+1} Möglichkeiten.

Der Beweis durch vollständige Induktion bleibt den Teilnehmern überlassen.

Fibonacci-Zahlen: Abschätzungen

Wir behaupten, dass für alle $n \geq 3$ gilt:

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

Induktionsanfang für $n = 3$ und $n = 4$: $F_3 \leq 2^3 \leq F_6$ ist korrekt, da $F_3 = 2$, $2^3 = 8$ und $F_6 = 8$ gilt. Ebenso gilt $F_4 \leq 2^4 \leq F_8$, denn $F_4 = 3$, $2^4 = 16$ und $F_8 = 21$.

Induktionsschritt:

Es sei $n \geq 3$ und die Formel gelte für n und $n+1$. Dann:

$$F_{n+2} = F_{n+1} + F_n \leq 2^{n+1} + 2^n < 2 \cdot 2^{n+1} = 2^{n+2}$$

und

$$2^{n+2} = 2 \cdot 2^{n+1} < 2F_{2n+2} + F_{2n+1} = F_{2n+2} + F_{2n+3} = F_{2n+4}$$

Anders ausgedrückt: $2^n \leq F_{2n} \leq 2^{2n}$ bzw. $(\sqrt{2})^n \leq F_n \leq 2^n$

Fibonacci-Zahlen und goldener Schnitt

Suche eine Darstellung der Form $F_n = x^n$ für reelle Zahl $x > 0$.

Aus der definierenden Gleichung folgt sofort $x^2 = x + 1$.

Dann liefert die p-q-Formel: $x_{1,2} = \frac{1}{2} \pm \sqrt{\frac{1}{4} + 1}$
bzw. $x_{1,2} = \frac{1}{2}(1 \pm \sqrt{5})$

Setzen wir $\Phi = \frac{1}{2}(1 + \sqrt{5})$ und $\hat{\Phi} = \frac{1}{2}(1 - \sqrt{5})$
und betrachten für Zahlen a und b die Kombination
$F_n(a, b) = a \cdot \Phi^n + b \cdot \hat{\Phi}^n$.

Für jede solche Kombination gilt

$$F_{n+2}(a, b) = F_{n+1}(a, b) + F_n(a, b).$$

Fibonacci-Zahlen und goldener Schnitt (2)

Wie müssen wir a und b wählen?

So, dass $F_0(a,b) = 0$ und $F_1(a,b) = 1$ gilt!

Alle anderen Werte der Fibonacci-Reihe ergeben sich dann von selbst...

Es muss also $a + b = 0$ gelten und $a \cdot \Phi + b \cdot \hat{\Phi} = 1$.

Daraus folgt: $a = \frac{1}{\sqrt{5}}$ und $b = -\frac{1}{\sqrt{5}}$, und wir erhalten

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

Hieraus kann man leicht ableiten, dass F_n die nächstgelegene natürliche Zahl bei

$$\frac{1}{\sqrt{5}} \cdot \left(\frac{1+\sqrt{5}}{2}\right)^n$$

ist.

Fibonacci-Zahlen und ggT

Der folgende Satz wirkt auf den ersten Blick erstaunlich.

Wir geben ihn hier ohne Beweis an:

Satz:

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

Als Beispiel betrachten wir $m = 8$ und $n = 12$.

Der Satz besagt dann (weil $\mathrm{ggT}(8, 12) = 4$):

$$\mathrm{ggT}(F_8, F_{12}) = F_4 = 3$$

Das ist korrekt, denn es gilt $F_8 = 21$ und $F_{12} = 144$, sowie $\mathrm{ggT}(21, 144) = 3$.

ggT mit Euklid

Satz: Um $\mathrm{ggT}(k, l)$ mit dem Euklidischen Algorithmus zu berechnen, braucht man höchstens $\lceil \log_\Phi k \rceil < \frac{3}{2} \log_2 k$ rekursive Aufrufe.

Das heißt, um den ggT von zwei 1000-Bit-Zahlen zu ermitteln, kommt man mit Rekursionstiefe ca. 1500 aus.

Wir verzichten hier auf den Beweis des Satzes, machen uns aber klar, dass schon ein naives Argument zeigt, dass Rekursionstiefe $2 \log_2 k$ in jedem Fall ausreicht.

Denn man sieht leicht, dass in der Sequenz $r_n, r_{n-1}, r_{n-2}, \ldots$ für jedes i gilt:

$$r_i + r_{i-1} \geq 2(r_{i-2} + r_{i-3}).$$

Aufgabe 1.4

Seien a und b teilerfremde natürliche Zahlen.
Zeige:

$$\mathrm{ggT}(a+b, a-b) \in \{1, 2\}$$

Lösung:

Der ggT sei g. Dann ist g Teiler von $(a+b)+(a-b) = 2a$ und von $(a+b)-(a-b) = 2b$, also von $\mathrm{ggT}(2a, 2b)$.

Allgemein gilt: $\mathrm{ggT}(ca, cb) = c \cdot \mathrm{ggT}(a, b)$.

Da hier a und b teilerfremd sind, folgt $\mathrm{ggT}(2a, 2b) = 2$.

Also erhalten wir: g teilt 2, und damit $g \in \{1, 2\}$.

Aufgabe 1.5

a) Zeige: $n \in \mathbb{N}$ ist durch 3 teilbar gdw. die Quersumme von n in der Dezimaldarstellung durch 3 teilbar ist.

Lösung: Modulo 3 gilt:

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_2 \cdot 10^2 + a1 \cdot 10 + a_0 \equiv$$
$$a_k \cdot 1^k + a_{k-1} \cdot 1^{k-1} + \cdots + a_2 \cdot 1^2 + a1 \cdot 1 + a_0$$

und die Summe der letzten Zeile ist genau die Quersumme von n.

---

b) Wann ist n durch 11 teilbar?

Lösung: Wir haben $10 \equiv -1 \bmod 11$. Daher gilt modulo 11:

$$n = a_k \cdot (-1)^k + a_{k-1} \cdot (-1)^{k-1} + \cdots + a_2 \cdot (-1)^2 + a1 \cdot (-1) + a_0$$

Also ist n durch 11 teilbar gdw. die alternierende Quersumme von n durch 11 teilbar.

Aufgabe 1.6: Satz von Wilson

Zu beweisen ist der folgende Satz (von Wilson):

Für alle natürlichen Zahlen $n \geq 2$ gilt:

$$(n-1)! \equiv -1 \bmod n \iff n \text{ ist Primzahl}$$

Zuerst sei n keine Primzahl, d.h. es existiert ein Teiler a mit $2 \leq a < n$. Also ist a ein Teiler von $(n-1)!$. Wäre $(n-1)! \equiv -1 \bmod n$, dann wäre n Teiler von $(n-1)!+1$, und folglich auch a Teiler von $(n-1)!+1$, also wäre $a = 1$, im Widerspruch zu $2 \leq a$.

Jetzt nehmen wir an, dass n eine Primzahl ist, dann ist $(n-1)!$ gerade das Produkt aller Elemente aus $(\mathbb{Z}/n\mathbb{Z})^*$. Wir betrachten zu jedem a in der Gruppe immer auch gleich das entsprechende a^{-1} – diese Paare tragen also zum Produkt mit dem Wert 1 bei. Nur 1 und -1 sind ihre eigenen Inversen. Diese beiden tragen mit $1 \cdot (-1)$ zum Produkt bei, welches sich also zu -1 ergibt.

Aufgabe 1.11

Zeige für alle $n \in \mathbb{N}$:

a) $n^5 \equiv n \mod 30$

b) $3^{n^4+n^2+2n+4} \equiv 21 \mod 60$

c) $7^{n+2} + 8^{2n+1} \equiv 0 \mod 57$

Zu a): n ist gerade gdw. n^5 gerade ist, d.h. die Gleichung gilt modulo 2.
n ist durch 3 teilbar gdw. n^5 durch 3 teilbar, und falls n nicht durch 3 teilbar ist, gilt $n^2 \equiv 1 \mod 3$, da $\varphi(3) = 2$ ist.
n ist durch 5 teilbar gdw. n^5 durch 5 teilbar, und falls n nicht durch 5 teilbar ist, gilt $n^4 \equiv 1 \mod 5$, da $\varphi(5) = 4$ ist.
Es gilt also $n^5 \equiv n \mod 2$, mod 3 und mod 5, also auch mod $2 \cdot 3 \cdot 5 = 30$.

Zu b): Wir müssen die Aussage modulo 3, 4 und 5 prüfen. (Teilweise an der Tafel)
Modulo 3 klar (0=0). Modulo 4 steht rechts 1 und links eine Potenz von -1. Zeige also, dass Exponent gerade ist. Modulo 5 nutzen wir, dass $3^4 \equiv 1$ gilt.

Zu c): Benutze, dass $8^2 \equiv 7 \mod 57$ gilt. Damit folgt:

$$7^{n+2} + 8^{2n+1} \equiv 49 \cdot 7^n + 8 \cdot 7^n \equiv 57 \cdot 7^n \equiv 0 \mod 57$$

Begriffe und Methoden

Im ersten Teil über Diskrete Strukturen verwendete Begriffe:

Induktion, Primzahl, $\mathbb{N}, \mathbb{Z}, \mathbb{R}, \mathbb{Q}, \mathbb{C}$, assoziativ, neutrales Element, invers, invertierbar, kommutativ, abelsch, distributiv, Halbgruppe, Monoid, Gruppe, Ring, Körper, Einheit, Unterstruktur, Homomorphismus, Isomorphismus, Teiler, ggT, Primfaktorzerlegung, Restklasse, modulo n, Eulersche φ-Funktion, zyklische Gruppe, Ordnung einer Gruppe, Ordnung eines Elements, Fibonacci-Zahlen, goldener Schnitt,...

Methoden und Resultate:

Euklidischer Algorithmus, Lemma von Bézout, eindeutige Primfaktorzerlegung, $k \in (\mathbb{Z}/n\mathbb{Z})^* \iff \gcd(k,n) = 1 \iff x \mapsto kx$ auf $\mathbb{Z}/n\mathbb{Z}$ bijektiv, Berechnung des Inversen mod n, $\mathbb{Z}/n\mathbb{Z}$ ist Körper $\iff$ n ist Primzahl, Chinesischer Restsatz, Lösung simultaner Kongruenzen, Existenz unendl. vieler Primzahlen, Kleiner Satz von Fermat, Fermat-Test, schnelle Exponentiation, RSA-Verfahren, Berechnung des Werts $\varphi(n)$, Satz von Euler, $\sum_{t \mid n} \varphi(t) = n$, Satz von Lagrange, Primzahlzertifikat, Interpretation der Fibonacci-Zahlen, Formel mit goldenem Schnitt, $\mathrm{ggT}(F_m, F_n) = F_{ggT(m,n)}$, logarithmische Rekursionstiefe beim Euklidischen Algorithmus.

Wachstum von $n!$

Wie schnell wächst die Fakultätsfunktion?

Man kann leicht zeigen: $\log(n!) \in \Theta(n \log n)$

denn für alle $n \geq 2$ gilt: $\left(\frac{n}{2}\right)^{\frac{n}{2}} < n! < n^n$

und daraus folgt die obige Behauptung.

Es gilt aber auch: $e \cdot (\frac{n}{e})^n \leq n! \leq n \cdot e \cdot (\frac{n}{e})^n$

(Der Beweis folgt gleich...)

Und sogar: $n! \sim \sqrt{2\pi n} \cdot (\frac{n}{e})^n$

(*Stirling-Formel* - hier ohne Beweis)

Beweis der Formel

Zu zeigen ist:

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

Es gilt $\ln(n!) = \ln(2) + \ln(3) + \cdots + \ln(n)$, also kann das Integral $\int_1^n \ln(x)dx$ nach oben durch $\ln(n!)$ und nach unten durch $\ln((n-1)!)$ abgeschätzt werden.

Die Stammfunktion von $\ln(x)$ ist $x\ln(x) - x + c$, damit erhalten wir für das Integral den Wert

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

und daher: $(n-1)! < e^{n\ln(n)-n+1} < n!$

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

woraus man direkt die Behauptung ableiten kann.

Wachstum der Binomialkoeffizienten

Wir interessieren uns hauptsächlich für Koeffizienten der Form $\binom{2n}{n}$ bzw. für $\binom{n}{\lfloor \frac{n}{2} \rfloor}$ oder $\binom{n}{\lceil \frac{n}{2} \rceil}$.

Beachte hierbei: $\sum_k \binom{n}{k} = 2^n$ Warum ist das so?

Damit können wir schließen, dass diese Binomialkoeffizienten im „Durchschnitt“ von der Größenordnung $\frac{2^n}{n}$ sind.

Das ergibt den folgenden Satz:

Satz: Für $n \geq 3$ gilt:

$$\binom{n}{\lfloor \frac{n}{2} \rfloor} = \binom{n}{\lceil \frac{n}{2} \rceil} > \frac{2^n}{n}$$