THI 3

Fib,ϕ	4	$F(n) = \frac{\phi^n - \hat{\phi}^n}{\sqrt{5}};\ \phi, \hat{\phi} = \frac{1 \pm \sqrt{5}}{2};\ \phi^2 = \phi + 1$
(K-)SAT	16-18	$T_n \sim a^n$
Landau-Notation	22,23	
Summen	24	$n! \in \Theta((\frac{n}{e})^n \sqrt{2\pi n});\ \sum_{i=0}^{n} q^i = \frac{q^{n+1}-1}{q-1}$
Catalan-Zahlen	25,26	$c_n = \frac{\binom{2n}{n}}{n+1} \sim \frac{4^n}{(n+1)\sqrt{\pi n}} = B_{i(t)=n} = T_n$
Lexikografischer Vergleich	29	$\overline{V_n} = \frac{1}{k-1}(k - \frac{1}{k^{n-1}})$
Maxfind, lrm	30,31	$E(lrm_n) = H_n \sim \ln n + \gamma; \gamma = 0.5772...$
Permutationen, Inversionen	35-37	$\#inv_{wc} = \binom{n}{2};\ E(inv) = \frac{1}{2}\binom{n}{2}$
Insertionsort	42,43	
Mergesort	45-47	$\overline{V_{n,rek}} = n \log n - 2^{\log n};\ \overline{V_{n,it}} = n \log n + 4n$
Quicksort	59,60	$\overline{V_n} = 2 \ln 2 n \log n + O(n);\ \overline{\#split_n} \sim \frac{2}{n}$
Binäre Bäume	64-68,75	$\log e(t) \leq h(t);\ w_e(t) = w_i(t) + 2i(t);\ \bar{h}(t) = \frac{w_e(t)}{e(t)} \sim 2 \ln n$
geordnete Bäume	74,75	
untere Sortierschranke	73	$\lceil \log n! \rceil$
Entropie, Shannon	82,85	$H(\underline{p}) = -\sum_k p_k \log p_k;\ maxH(\underline{p}) = \log n \leftrightarrow p_i = \frac{1}{n}$
Huffman	92	$H(\underline{p}) \leq \bar{h}(t) < H(\underline{p}) + 1$
Karatsuba, Strassen	93-95	$T_{Kara} \in O(n^{\log 3});\ T_{Strassen} \in O(n^{log7})$
erzeugende Funktion	97	$a(z) = \sum_{n \geq 0} a_n z^n$
Newton's Binomialformel	98,103	$a(z) = \frac{P(z)}{(1-\gamma z)^k} \wedge grad(P) < k \leftrightarrow a_n = R(n)\gamma^n \wedge grad(R) < k$
Code-Rate, $\#l_n(Typ3)$	99-101,107	$\lim_{n \to \infty} \frac{\log_{\lvert\Sigma\rvert} \#l_n}{n}$
C-Rekursion	104-107	$a(z) = \frac{P(z)}{Q(z)}, grad(P) < grad(Q);\ Q(z) = 1 - q_1 X - q_2 X^2 - ...$
Transfermatrix $\rightarrow$ erz. Funktion	110	
Master-Theorem	121	
ggT, Primzahl, kgV	129,130	$kgV \cdot ggT = a \cdot b$
euklidischer Algorithmus	130,131	Lamé: $\#Div(ggT(a,b)) \leq 2 \log \max(a,b) + 1$
erweiterter eukl. Algorithmus	132,133	
lin. Gleichungen in $\mathbf{Z}$, Bézout	134	$\exists s, t \in \mathbf{Z} : as + bt = c \leftrightarrow ggT(a,b) \vert c$
binärer eukl. Algorithmus	138	$\#Bitoperationen \in O(\log^2(a+b))$
Inverse in $\mathbf{Z}_n$, Gleichungen	140,141	
Eulers φ-Funktion	141,142	$ggT(a,b) = 1 \rightarrow \varphi(ab) = \varphi(a)\varphi(b);\ n = \sum_{d \vert n} \varphi(d)$
		$\varphi(p^e) = p^{e-1}(p-1);\ \varphi(n) = n \cdot \prod_{p \vert n}(1 - \frac{1}{p})$
Satz von Lagrange	146	$ord_G(a) \vert \#G;\ a^k = a^{k \mod ord_G(a)}$

Satz von Euler	147	$ggT(a,n) = 1 \rightarrow a^{\varphi(n)} \equiv 1 \mod n$
Satz von Fermat	147	$a^{p-1} \equiv 1 \mod p$
Primzahlen	150-153	$\pi(n) \sim \frac{n}{\ln n}$
Primzahlkriterium, Zertifikate	154,157	n prim $\leftrightarrow \exists a \in \mathbf{Z}_n^* \begin{cases} a^{n-1} \equiv 1 \mod n \\ \forall p_{p\|(n-1)} a^{(n-1)/p} \not\equiv 1 \mod n \end{cases}$
schnelle Exponentiation	158,159	$M(n) = l(n) + \#1(n)_2 - 2$
Chinesischer Restesatz	168,169	$x \equiv c_i \mod m_i \leftrightarrow \begin{cases} x = \sum c_i \cdot \frac{M}{m_i} \cdot v_i \\ m_i \cdot u_i + \frac{M}{m_i} \cdot v_i = 1 \end{cases}$; m_i teilerfremd
Modulare Arithmetik	170	
Partialbruchdarstellung	174	$\frac{a}{M} = \alpha_0 + \sum_i \frac{\alpha_i}{m_i}$; $M = \prod m_i$; $ggT(m_i, m_j) = 1$
nicht teilerfremde Moduln	175	lösbar $\leftrightarrow ggT(m_i, m_j) \| a_i - a_j$
Primzahltests, Miller-Rabin	176+,181,183	p prim $\rightarrow \begin{cases} a^u \equiv 1 \mod p,\ p - 1 = 2^t + u \\ a^{u \cdot 2^i} \equiv -1,\ 0 \leq i < t \end{cases}$
Verschl. durch Exponentiat.	185	$ggT(e, \varphi(p)) = 1$; $d \cdot e \equiv 1 \mod \varphi(p)$; $M^e \mod p$; $C^d \mod p$
RSA	186,189	$n = p \cdot q$; $ggT(d, \varphi(n)) = 1$; $d \cdot e \equiv 1 \mod \varphi(n)$
Carmichael-Zahlen	190	$\forall a : E(a) \rightarrow F(a)$