Lemmata und Sätze

1. Handschlaglemma: $\sum_{i=1}^{n} x_i = 2y$
2. Proposition Binomialkoeffizienten: $\binom{n}{k} = \frac{n!}{k!(n-k)!}$
   $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$
3. injektiv: $\forall a_1, a_2 \in A$ mit $f(a_1) = f(a_2)$ gilt, dass $a_1 = a_2 \Rightarrow$ injektiv
4. surjektiv: f[A]=B, $b \in B$, $a \in A \Rightarrow f(a) = b$
5. bijektiv: Kombination aus surjektiv und injektiv
6. Satz von Cantor-Schröder-Bernstein: $f : A \to B$
   $g : B \to A$
   Falls: f und g injektiv: Bijektion zwischen A und B
   falls $g : B \mapsto A$ surjektiv: f injektiv
7. Satz von Cantor: |A|<$|\mathcal{P}(A)|$
   Also: Potenzmenge der Menge A hat **immer** mehr Elemente als die Menge A selbst.
8. Permutationen: Es gibt n! Permutationen der Menge x={1,...,n} mit $n \in \mathbb{N}$
   Permutation ist eine Bijektion der Funktion $\pi(x \to x)$
   Jede Permutation der Menge x ist Komposition der Transposition (1,2)(2,3)...(n-1,n)
9. Stirling'sche Formel: n!$\approx \sqrt{2\pi n} * (\frac{n}{e})^n$
   Wenn $n \in \mathbb{N}$, f,g sind Funktionen $\mathbb{N} \to \mathbb{R}$
   f$\sim$g, wenn ϵ>0 existiert ein $n_0 \in \mathbb{N}$, sodass $\forall n \in \mathbb{N}$ mit n>n_0 gibt, dass |f(n)/g(n)-1|<ϵ
10. Definition: M^+:=M$\cup${M}
11. Addition: +: $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$
    induktiv: n+0:=0
    n$\cdot m^+ := n \cdot m + n$
12. Exponentation: $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$
    $n^0 := 1$
    $n^{m^+} := n^m \cdot n$
13. Definition(Primzahlen): Eine Zahl p$\in \mathbb{N}$ ist prim p>1 und wenn sie nur durch 1 und sich selbst teilbar ist.
    Primteiler einer Zahl n ist prim.

14. Primzahlsatz: $\pi(x) \approx \frac{x}{ln(x)}$

15. Fundamentalsatz der Arithmetik: $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k}$
    Jedes $n \in \mathbb{N}$ kann so dargestellt werden.
    p...prim; n>0; α>1

16. Euklidischer Algorithmus: a,b$\in \mathbb{Z}$, $b \neq 0$ existiert q,r$\in \mathbb{Z}$ mit a=q·b+r, 0≥r>|b|
    a,b$\in \mathbb{N}$ mit b>0 ggT(a,b)=ggT(b,q mod b)
    Algorithmus: Eingabe n,m$\in \mathbb{N}$ mit m≥n
    Ausgabe ggT(m,n)
    falls m|n, dann m ausgeben
    sonst Euklid: (n mod m,n) aus

17. Lemma von Bézout: wenn m,n$\in \mathbb{N}$, m und n **nicht beide** 0
    $\exists a, b \in \mathbb{Z}$ mit ggT(n,m)=am+bn

18. Erweiterter euklidischer Algorithmus: Eingabe: $n, m \in \mathbb{N}$ mit $m \leq n$
    Ausgabe: a,b$\in \mathbb{Z}$, sodass ggT(n,m)=am+bn
    falls m|n, dann gebe (1,0) aus, sonst sei (b'a') die Ausgabe von erw. Euklid(n mod m,m) Gebe (a'-b'[n/m],b')

19. Lemma von Euklid: Teilt eine Primzahl das Produkt zweier natürlicher Zahlen, so auch mindestens einen der Faktoren.

20. **MODULO:** Add.: $a +_{mod\ n} b := (a + b) mod\ n$
    Sub.: $a -_{mod\ n} b := (a - b) mod\ n$
    Mult.: $a \cdot_{mod\ n} b := (a \cdot b) mod\ n$

21. Homomorphieregel:
    (a+b)mod n=(a mod n+b mod n)
    (a-b)mod n=(a mod n-b mod n)
    (a·b)mod n=(a mod n·b mod n)
    a mod n=r a≡r (mod n)
    Beispiel: 333333· 444444· 56789≡ 33·44·89
    ≡33·11·4·89≡(330+33)·(320+36)
    ≡ 63·56 ≡ 3528
    ≡ 28 (mod 100)

22. Al-Kaschi: binäre Exponentation: Man kann bei jedem Rechenschritt modular vereinfachen (Homomorphieregel)
    Damit vermeidet man eine **EXPLOSION** der Zwischenergebnisse
    ⇒ Man kann mittels der Methode verdoppeln und quadrieren, die Berechnung in handhabbare Schritte zerlegen.

23. Chinesischer Restsatz:
    - m·n Felder (m-Höhe, n-Breite)
    - Felder durch nummerieren (start in 0. Zeile und 0. Spalte)
    - Standort zu Schritt x: k. Zeile und l. Spalte
    folgende Fälle: -k<m-1 und l<n-1. dann fahren wir mit dem Feld in der k+1. Zeile und l+1. Spalte fort.
    -k=m-1 und l<n-1. Fahre mit dem Feld in der 0. Zeile und l+1. Spalte fort
    -k<m-1 und l=n-1. Fahre mit dem Feld in der k+1. Zeile und 0. Spalte fort.
    - k=m-q und l=-1. Stopp

24. Satz: Es seien $n_1, ...n_r \in \mathbb{N}$ teilerfremd und $a_1, ..., a_r \in \mathbb{Z}$ dann gibt es genau eine natürliche Zahl $x \in \{0, ..., n_1 \cdot (...) \cdot n_r - 1\}$
    Mit x≡ $a_i (mod\ n_i)$ für alle i∈1,...,r

25. Definition Nullteiler: Man nennt a∈ $\mathbb{Z}_n \backslash \{0\}$ einen Nullteiler, wenn es ein b∈ $\mathbb{Z}_n \backslash \{0\}$ gibt mit a·$b = 0$

26. Definition Einheiten: Man nennt a∈ $\mathbb{Z}_n$ eine Einheit, wenn es eine Zahl b mit a· b=1 gibt.

27. Lemma Jährling Syndrom: Sei n∈ $\mathbb{Z}\backslash\{0\}$ dann sind äquivalent
    1. m ist Einheit in $\mathbb{Z}_n$
    2. m ist kein Nullteiler in $\mathbb{Z}_n$
    3. m und n sind teilerfremd.

28. Proposition: Hat $n \in \mathbb{N}$ die Primfaktorzerlegung: $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k}$, dann gilt
    ϕ(n)=$(p_1 - 1)p_1^{\alpha_1 - 1} \cdot ... \cdot (p_k - 1)p_k^{\alpha_k - 1}$
    $= n(1 - \frac{1}{p_1}) \cdot ... \cdot (1 - \frac{1}{p_k})$

29. Definition Gruppen: Eine Gruppe G heißt zyklisch falls sie von einem Element erzeugt wird, d.h. es gibt ein Gruppenmitglied g∈ G (den Erzeuger), sodass sich g schreiben lässt als G=$\{e, g, g^{-1}, g \circ g, (g \circ g)^{-1}, ...\}$
    =$\{g^m | m \in \mathbb{Z}\}$

30. Proposition: Die Anzahl der Erzeuger von $(\mathbb{Z}_n, +, -, 0)$ ist ϕ(n).

31. Satz von Gauß: Sei p prim, dann ist in $(\mathbb{Z}_p^*, \cdot, ^{-1}, 1)$ zyklisch.

32. Proposition: Die Anzahl der Erzeuger von $\mathbb{Z}_n^*$ ist $\phi(\phi(n))$.

33. Satz von Lagrange: Sei (G, $\circ$ $^{-1}$,e) eine Gruppe.
    Eine Untergruppe von G ist eine Teilmenge u von G, die das neutrale Element e enthält und die unter $^{-1}$ und $\circ$ abgeschlossen ist.
    Das soll heißen, dass mit jedem Element g∈U, g^{-1} ∈U, und das für alle g_1, g_2 ∈U

auch $g_1 \circ g_2 \in U$. Jede Untergruppe U ist ausgestattet mit den auf U eingeschränkten Operationen $\circ, ^{-1}$ und dem selben neutralen Element e, selbst wieder eine Gruppe. Um anzuzeigen, dass U ein Untergruppe von G ist, schreibt an U≤G

34. Definition Nebenklassen: Ist U eine Untergruppe der Gruppe G und g ein Element von G, dann nennt man g∘U:=$\{g \circ u | u \in U\}$ eine (links-) Nebenklasse von U und G.

35. Es sei U eine Untergruppe von G und $g_1, g_2 \in G$
Falls $g_1 \in g_2 \circ U$, dann gilt $g_1 \circ U = g_2 \circ U$.

36. Lemma Jährling-Pascal-Lukas: Je zwei Nebenklassen a∘ U und b∘ U sind entweder gleich oder disjunkt.

37. Definition Index: Es sei G eine Gruppe und U eine Untergruppe von G. Der Index von U in G ist die Anzahl der Nebenklassen von U und G und wird [G:U] geschrieben.

38. Satz von Lagrange: Ist U eine Untergruppe von einer endlichen Gruppe G, dann gilt [G:U]=|G|/|U|.

39. Lemma von Euler-Fermat: Ist p eine Primzahl, dann gilt für jede Zahl a∈ $\mathbb{Z}$, die nicht durch p teilbar ist:
$a^{p-1} \equiv 1 (mod\ p)$

40. Lemma Bob: Es seien q_1, q_2 teilerfremd. Dann gilt
a≡ $b (mod\ q_1)$ und a≡ $b (mod\ q_2)$, genau dann, wenn a≡b (mod q_1, q_2)

41. Definition Ansgar: Ein (schlichter, ungerichteter) Graph G ist ein Paar(V,E) bestehend aus einer Knotenmenge V und einer Kantenmenge E⊆ $\binom{V}{2}$. Die Knotenmenge von G wird auch mit V(G), und die Kantenmenge E(G) bezeichnet.

42. Definition Isomorphie: 2 Graphen G und H sind isomorph, wenn es eine Bijektion f:V(G)→V(H) gibt, sodass (u,v)∈E(G), genau dann, wenn (f(u),f(v)); intuitiv bedeutet das, dass man H aus G durch Umbenennen der Knoten von G erhält.

43. Definition Subgraph: Ein Graph H ist ein Subgraph von G, falls gilt V(H)⊆V(G) und E(H)⊆E(G). Ein induzierter Subgraph von G ist ein Graph H mit V(H)⊆V(G), und E(H)=E(G)∩$\binom{V(H)}{2}$.