1 and p are not zerodivisors

Körper: abelsche Gruppe in ⊕ und ⊙, kommutativer unitärer Ring. Assoziativ, Kommu, neutrales Elem und Inverse in ⊕ und ⊙. Ausserdem $a\cdot(b+c)=ab+ac$ und $(b+c)\cdot a=ab+ac$

unit: Invertible elem of a Ring => not zerodivisor

R^* is multiplicative Group of units of R

Körper ⊆ → keine Nullteiler

<u>Integral Domain</u>: Commutative Ring without zerodivisors e.g. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$

$\mathbb{Z}_m$ is an integral Domain iff m is prime. Else $ab=m$ => a, b are zerodivisor

if $a|b$, then c s.t. $ac=b$ is unique

Körper <u>Field</u>: Commutative Ring where every nonzero Elem is a unit.

$\mathbb{Z}_p$ is a Field iff p is prime. Then $\mathbb{Z}_p = GF(p)$

$x^p+y^p=(x+y)^p$ falls p charakteristik vom Feld

associativity, commutativity, distributivity, identity and inverses for addition and multiplication

Untergruppen bestimmen

Lagrange: Nullteiler der # Elem von G betrachten. ord(1) → {e}, ord(6) → G, ord(2): Inverse ist immer enthalten, also e, a wobei a ist selbstinvers → {e, a}, ord(4)

Generatoren von grossen Gruppen nicht rechnen. E.g. $D_4 = \{e, r, rr, rrr, s, sr, srr, srrr\}$ → Untergruppe mit ord(4) = {e, rr, s, srr}

$\mathbb{Z}_n^*$ = alle Teilerfremden < n

$\mathbb{Z}_n$ = alle < n

not Fields unless $\mathbb{Z}_{prime}$

<u>Gallois Field</u> = finite Field, GF(a) contains a Elements

$\mathbb{Z}_{prime} = GF(prime)$ GF contains no zerodivisors

$GF(p^a)$ = Field over the polynomials in GF(p) with degree < a irreduzibel in GF(2)

$GF(8) = GF(2)[x]_{x^3+x+1}$

↑ betrifft Koeffizienten

0	$0x^0$
1	$1x^0$
2	$x + 0$
3	$x + x^0$
4	x^2
5	$x^2 + x^0$
6	$x^2 + x$
7	$x^2 + x + 1$

Irreducible in GF(2): x, $x+1$, x^2+x+1, x^3+x+1, x^3+x^2+1, x^4+x+1, $x^4+x^3+x^2+x+1$, x^4+x^3+1, x^5+x^2+1 ...

<u>Berechnen</u>: Entweder nach Rechnung Polynomdivision anwenden und Rest behalten

Oder zuerst die Potenzen in mod x^3+x+1 ausdrücken

$x^1 = x^1, \ldots, x^3 = -x-1 = x+1, x^4 = -x^2 - \cancel{x} = x^2 + \cancel{x}$

Und dann normal rechnen und diese Potenzen einfach ersetzen:

$(x^2+x+1)(x^2+1) = x^4+x^3+x^2+x^2+x+1 = x^2+\cancel{x}+x+1+2x^2+x+1$

$= 3x^2+3x+2 = x^2+x+0$ //mod x^3+x+1

Euler φ: $\varphi(n)$ = # teilerfremde Zahlen < n, d.h. $ggT(m,n)=1$

$\varphi(prim) = p-1$

$\varphi(mn) = \varphi(m)\varphi(n)$ falls m, n teilerfremd

$\varphi(n) = \prod((p-1)p^{(k-1)})$, p = Primfaktor

The Ring $F[x]_{m(x)}$ is a Field iff m is irreducible. ("monisch")

Any two finite Fields of the same order are Isomorphic

<u>Fermat</u> zur φ-Funktion von Euler: für $m \geq 2$, $gcd(a,m)=1$ gilt $a^{\varphi(m)} \equiv_m 1$

für prime p, a not divisible by p: $a^{p-1} \equiv_p 1$

<u>Euklid</u> for given $a, b > 0$, $a \geq b$, compute $d = gcd(a,b)$ and u, v satisfying $ua+vb=gcd(a,b)$

1. Divide larger by smaller
2. replace the pair of ints by the smaller and the Remainder of (1)
3. repeat until remainder is 0
4. gcd = last non-zero remainder

Works also with polynomials where size is defined as degree

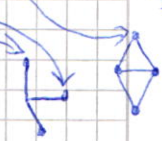
Note "$q := s_1$ div s_2" means that q is the largest integer multiple of s_2 contained in s_1

```
s1 := a; s2 := b;
u1 := 1; u2 := 0;
v1 := 0; v2 := 1;
while s2 > 0 {
  q := s1 div s2;
  r := s1 - q s2;
  s1 := s2; s2 := r;
  t := u2; u2 := u1 - q u2; u1 := t;
  t := v2; v2 := v1 - q v2; v1 := t;
}
d := s1; u := u1; v := v1;
```

<u>Hasse</u>

grösstes / kleinstes Elem eindeutig falls existiert

Maximales Elem nicht eindeutig



<u>Grosser Satz von Fermat</u>

$a^n + b^n = c^n$ besitzt für $n > 2$ keine Lsg mit positiven $a, b, c \in \mathbb{N}$

<u>Fermats' last</u>: $\neg(\exists xyzn\,(n \geq 3 \land x^n + y^n = z^n))$

CNF = (v) ∧ (v)   verneinung where Truthtable = 0
DNF = (∧) v (∧)   where Truth table = 1

Prenex: Pull ∃ and ∀ out, rename vars

Prädikatenlogik

$\forall x\, (P(x) \land Q(x)) \Leftrightarrow \forall x\, P(x) \land \forall x\, Q(x)$
$\exists x\, (P(x) \land Q(x)) \Rightarrow \exists x\, P(x) \land \exists x\, Q(x)$

$\neg \forall x\, P(x) \Leftrightarrow \exists x\, \neg P(x)$
$\neg \exists x\, P(x) \Leftrightarrow \forall x\, \neg P(x)$

$\exists y\, \forall x\, P(x,y) \Rightarrow \forall x\, \exists y\, P(x,y)$

De Morgan

$\neg(P \lor Q) = \neg P \land \neg Q$

$\neg(P \land Q) = \neg P \lor \neg Q$

$A \to B \Leftrightarrow \neg A \lor B$

$\neg(F \Leftrightarrow G) \Leftrightarrow (F \Leftrightarrow \neg G)$

Mengenlogik

Es gilt immer: Idempotence: $A \cup A = A = A \cap A$

Commutativity: $A \cap B = B \cap A$, $A \cup B = B \cup A$

Associativity: $A \cap (B \cap C) = (A \cap B) \cap C$, $A \cup (B \cup C) = (A \cup B) \cup C$

$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$ "Inclusion-Exclusion"

Absorption: $A \cap (A \cup B) = A = A \cup (A \cap B)$

Complementarity: $A \cap \bar{A} = \emptyset$, $A \cup \bar{A} = U$

Distributivity: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Consistency: $A \cup B = B \Leftrightarrow A \subseteq B \Leftrightarrow A \cap B = A$

sort: $A \subseteq B \Leftrightarrow \bar{A} \subseteq \bar{B}$

Poset: all Subsets, S itself and $\{\} = P(S)$
$P(\{1\}) = \{\{\}, \{1\}\}$

Subset rules:
$\{1,2\} \subseteq \{1, \{1,2\}\}$
$\{1,2\} \not\in \{1, \{1,2\}\}$

$|A \times B| = |A| \cdot |B|$

Cartesian Product:
$\{1,2,3\} \times \{4,5,6\} = \{(1,4), (1,5), (1,6), (2,4), (2,5), (2,6), (3,4), (3,5), (3,6)\}$

Eulersche φ-Funktion

weist einer Zahl n # aller kleineren teilerfremden Zahlen zu, d.h. $ggt(n,a) = 1$

$\varphi(Prim) = 1$
$\varphi(mn) = \varphi(m)\varphi(n)$ falls $ggt(m,n) = 1$

$\varphi(n) = \prod ((p-1)p^{(k-1)})$
p = Primfaktor
k = wie oft p in PFZ ist

Algebra

An operation on a Set S $f: S^n \mapsto S$ has "arity" n. Eg. unary, binary, ...

Algebra $\langle S, \Omega \rangle$
Set, Set of operations

$e * a = a = a * e$
leftneutral, rightneutral

Semigroup

Is an Algebrastere $\langle M; *; e \rangle$
* associative
and e is the neutral element
=> Monoid

Group $\langle G, *, \hat{}, e \rangle$

* associative
∃ neutral element e
$\forall a\, \exists \hat{a}$ ← Inverse on both sides

Generator: falls g^n mit beliebigem n die Gruppe aufbaut ist g Generator der Gruppe $\langle g \rangle$

A Group is "abelian" / "commutative" if $a * b = b * a$ for all
cyclic implies abelian

Subgroup

A fully closed Group within a group
trivial ones: $\{e\}$, G

Inverse

Is an Element of S s.t. $\hat{a} \circ a = e$ and $a \circ \hat{a} = e$

Ideal by (a,b) generated $= \{ua + vb; u,v \in \mathbb{Z}\}$
by (a) $= \{ua, u \in \mathbb{Z}\}$
if $i \in$ Ideal then $a \circ i \in$ Ideal
$I \subseteq$ Ring abgeschl. bezgl. ⊕ in I, ⊙ mit Ring
bsp: gerade Zahlen ist ein Ideal

=> For a Group, we have
$\hat{\hat{a}} = a$
$\widehat{a * b} = \hat{b} * \hat{a} \xrightarrow{\text{falls kommutativ}} \hat{a} * \hat{b}$

$a * b = a * c \Rightarrow b = c$
$a * b = c * b \Rightarrow a = c$
$a * x = b$ and $x * a = b$ have unique solutions for x

associative => folgt dass das Inverse eindeutig ist, falls existent

Lemma: $a^m \cdot a^n = a^{m+n}$
$a^{mn} = (a^m)^n$

Group elem Order

$ord(a) = m$ s.t. $a^m = e$
or ∞

$ord(a) = 2 \Rightarrow a \circ \hat{a} = e$

Direct product of n Groups

Is the Algebra $\langle G_1 \times G_2 \times \dots; * \rangle$ where * is componentwise
$(a_1, a_2, \dots, a_n) * (b_1, \dots, b_n) = (a_1 *_1 b_1, a_2 *_2 b_2, \dots, a_n *_n b_n)$

=> e and Inverse are also component-wise

Group Homomorphism

$\varphi: G \to H$

$\varphi(a * b) = \varphi(a) ♥ \varphi(b)$
* in H

if bijective => isomorphism

Lemma: $\varphi(e) = e'$
$\varphi(\hat{a}) = \widehat{\varphi(a)}$

Cyclic groups

are isomorphic to $\langle \mathbb{Z}_n, \oplus \rangle$ and hence abelian

Every Group of prime order is cyclic and everything except neutral elem is a Generator

Ring

is an Algebra
$\langle R; +, -, 0, \cdot, 1 \rangle$ is commutative Group
$\langle R; \cdot, 1 \rangle$ is monoid

$a(b+c) = ab + ac$
$(a+b)c = ac + ab$

"commutative" if $ab = ba$ multiplication

$\Rightarrow (-a)b = -ab$
$(-a)(-b) = ab$
$1 \neq 0$ if more than 1 elem

commutative => $a|b$ & $b|c \to a|c$
$a|b \to a|bc$
$a|b$ & $a|c \to a|(b+c)$

characteristic: order of 1 in ⊕, if infinite, it is 0

Diedergruppe: rotationen & Spiegelungen des n-Ecks

Selection:

Ordered with indistinguable repetition $t, r, s, \ldots$: $\frac{n!}{r! \cdot s! \cdots t!}$

Ordered, with repetition	n^k
Ordered, without rep.	$\frac{n!}{(n-k)!} = \binom{n}{k} k! = {}_nP_k$
Unordered, without rep.	$\frac{n^{\underline{k}}}{k!} = \binom{n}{k} = \frac{n!}{k!(n-k)!}$
Unordered, with rep.	$\binom{k+n-1}{k} = \frac{(k+n-1)!}{n-1!}$

(Urnen-Modell)

Binomialcoefficients

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

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n$$

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$$

For any real or complex $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$

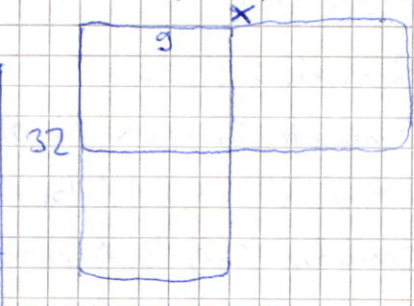
$$n^{\underline{k}} = n(n-1)\cdots(n-k+1)$$

Double-Counting Principle

For a Set $A \times B$, we can either count all b that fit to a or all a that fit to b
$|A \times B| = \sum m_a = \sum m_b$, m_a, m_b are Amount of ones in the Matrixrow

Example: 32 airlines, each flies to 9 airports. 16 airlines per airport.

$$\Rightarrow 32 \cdot 9 = 16 \cdot x$$



Trick: Einheit $\text{airport}^{-1} \cdot \text{airline}^{-1}$ gleich links & rechts

Pigeonhole Principle

If a set is divided into $k < n$ partitions, at least one of these Subsets contains $\lceil \frac{n}{k} \rceil$ elements

Vandermonde

$$\binom{m+n}{k} = \sum_{i=0}^{k} \binom{m}{i} \binom{n}{k-i}$$

$$\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}^2$$

Mauer Anmalen

d) Unbekannte Anzahl blaue, müssen aber nebeneinander sein
$\Rightarrow$ mit Segmenten rechnen. Grenzen ununterscheidbar
damit nicht Anfang Ende überholt, dann für Wand mit 7 Feldern
$1 + \binom{8}{2}$

e) Keine zwei rote dürfen Benachbart sein. Rekursiver Ansatz: $C_k = \underbrace{C_{k-1}}_{\text{"last blue" case}} + \underbrace{C_{k-2}}_{\text{"last piece red" case}}$ Möglichkeiten
$C_1 = 2 \quad C_2 = 3 \Rightarrow C_7 = 34$

Würfel bemalen

2 Seiten fix färben oder am Schluss durch mögliche Rotationen dividieren

Binomialsatz

$$(a+p)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k = a^p + b^p + \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k} b^k$$

Wahl des Inselrats. AP 2 Kandidaten
BP 7, PP 5
niemand mehr als 3 im Rat
$\Rightarrow$ Fallunterscheidung, kleinste (AP) zuerst entscheiden

Wenn auch Enthaltung möglich, erstelle einen Kandidaten "Enthaltung"

Urnenmodell: # Kandidaten + 1 = # Wände. Links & Rechts sind fix $\Rightarrow$ Es bleiben noch
$n-2+1 \Rightarrow n-1+k$ Plätze, wo die Restlichen $n-1$ Trennwände sein können.

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

Grosses Aufzählen von Fällen $\Rightarrow$ Evt ist (Alles minus was zu viel ist) schneller?!

a) Bäckerregal: ohne zwei nebeneinanderliegende auszuwählen k auszuwählen. Vorgehen mit Urnenmodell.
k gewählte Bäcker $\hat{=}$ Trennwände. Die können zu max 1 gleichzeitig jeweils zwischen den übrigen $(n-k)$ Bäckern sein $\Rightarrow \binom{n-k+1}{k}$ // sie können auch am Rand sein!

b) Arthus: Ritter im Kreis wählen, nie 2 nebeneinander. Vorgehen: Fix one.
Case 1: He is chosen. Those next to him are not. Remaining $(n-3)$ knights.
Same case as in a) but $n_1 = n-3$, $k_1 = k-1$ because one's already chosen

Case 2: He isn't chosen. Those next to him may be. $\Rightarrow$ case like in a) with $n_2 = n-1$ and $k_2 = k$

$$\Rightarrow \text{both added together} = \binom{n-3-k+1+1}{k-1} + \binom{n-1+1-k}{k}$$

Powerset$(\{a,\{b\}\}) = \{\{\}, \{a\}, \{b\}, \{a,\{b\}\}\}$

Proofs

Direct: prove $F \to G$ by assuming F and deriving G
Indirect: prove $F \to G$ by proving $\neg G \to \neg F$
Modus Ponens: Prove a precondition and prove that precondition implies G
Case distinction: prove all cases
Contradiction: prove F by proving $\neg F$ wrong
Existence: show an x or use a non-constructive proof
Counterexample
Induction: 1. Prove $P(0)$ 2. Prove $P(n) \to P(n+1)$

To prove finite, an injection $A \to N$ suffices

Relations

is on a set if from = to

Matrix representation ρ: from $\{a,b\}$ to $\{u,v\}$

$$\begin{array}{c|cc} & u & v \\ \hline a & 1 & 0 \\ b & 1 & 1 \end{array} \quad \rho = \{(a,u),(b,u),(b,v)\}$$

Inverse relation $\neq$ Inverse Matrix

$\widehat{a}\widehat{b} = \widehat{ab}$

$A \prec B \overset{\text{def}}{\Longleftrightarrow} |A| < |B|$ "B dominates a"

$\rho^2 = \rho \circ \rho$

// $A \preccurlyeq B \Longleftrightarrow \exists$ bijection $A \to B$

Reflexiv: $a\rho a$
Symmetric: $a\rho b \Longleftrightarrow b\rho a$
antisymmetric: $a\rho b \wedge b\rho a \Rightarrow a=b$
transitiv: $a\rho b \wedge b\rho c \Rightarrow a\rho c$

Compositions

if $a\rho b$ and $b\sigma c$ then $a\rho\sigma c$
"$\exists b$ s.t. $(a\rho b \wedge b\sigma c)$"
Compositioning is associative
ie. $\alpha(\rho\sigma) = (\alpha\rho)\sigma$

Transitive Closure ρ^*

contains everything accessible by repeatedly applying ρ
$a\rho^k b \Longleftrightarrow b$ is reachable from a in k times

Equivalence Relations

symmetric, transitive, reflexive

e.g. $\equiv_3$ is an equivalence relation

Equivalence Class: Set of all elements equivalent to a
denoted: $[a]_\rho = \{b \in A \mid b\rho a\}$

Composition $\rho\theta$ of 2 EqRels is again an Eqrel

Partitions are mutually disjunct subsets of A
$\Rightarrow$ EqClasses are Partitions

Quotient set

set of representants of all EqClasses mod a quotient
e.g. $\{0,1,2\}$ under mod 3

Partial order Relations

order Relation $\Rightarrow$ zusätzlich total für

anti-symmetric, transitive, reflexive

e.g $\leq$ is a partial order Relation

comparable: $a\rho b$ XOR $b\rho a$
else the two are uncomparable

"totally ordered" if all elems are mutually comparable

glb and lub

greatest lower bound of x and y
is $z \leq x \leq y$
similarly for lowest upper bound.

$glb(\{a,b\}) = meet(a,b)$
$lub(\{a,b\}) = joint(a,b)$

if a Poset has both, its called a Lattice.

[Ablesen in Hassediagramm]

well-ordered

if it is totally ordered and every non-empty subset has a least element. Every totally ordered finite Poset is well-ordered.
Any subset of a well-ordered is too, by the same relation.

Hassediagramm

Only draw direct ways.
higher Numbers higher
e.g. $\{1,2,3\}$ with $\leq$ relation
$\Rightarrow$

3
|
2
|
1

Function

Function $A \to B$ from Domain to Codomain is basically a well-defined, totally defined relation. i.e. $\forall a \in A\ \exists b \in B\ afb$
$\forall a \in A\ \forall b,b' \in B\ afb \wedge afb' \Rightarrow b=b'$

The set of all Functions $A \to B$ is denoted B^A

partial function: blue part not necessary

$f_1 \cong f_2$ if $A_1 = A_2$, $B_1 = B_2$, $P_1 = P_2$
equivalent

injective: no collisions from A to B
surjective: for each B at least one A

Chinese Remainder

m_i are relatively prime integers. for any $a_i < m_i$
the system $x \equiv_{m_1} a_1$ has a unique solution for x
$\cdots$
$x \equiv_{m_r} a_r$ satisfying $0 \leq x <$ Product of all m_i

$x = R_M \left(\sum_{i=1}^{r} a_i M_i N_i \right)$ r = max i

"N_i exists unique"

N_i = mult. inverse mod m_i of M_i

$M_i = \frac{M}{m_i}$ M = Product of all m_i

Example: $2^{1000} \bmod 35 = ?$

$2^4 \equiv_5 1 \Rightarrow 2^{1000} \bmod 5 = 1$

$2^3 \equiv_7 1 \Rightarrow 2^{1000} \equiv_7 2$

=> find integer that fulfills both ≤ 34

=> $x = 16$

Example: $k \equiv_8 1$, $k \equiv_7 2$, $k \equiv_5 3$

$R_{280}(1 \cdot 35 \cdot 3 + 2 \cdot 40 \cdot 3 + 3 \cdot 56 \cdot 1) = 233$

Binomialsatz $(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k = a^p + b^p + \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k} b^k$

Kombination ohne Zurücklegen $\binom{n}{k} = \frac{n!}{k!(n-k)!}$

Kombination mit Zurücklegen $\frac{(n+k-1)!}{(n-1)!\,k!} = \binom{n+k-1}{k} = \binom{n+k-1}{n-1}$

Reihenfolge ohne Zurücklegen
Anordnungsmöglichkeiten: $n!$

Möglichkeiten eine Reihenfolge von k von n Elementen auszuwählen: $nPr\binom{n}{k} = \frac{n!}{(n-k)!} = \binom{n}{k} k!$

Reihenfolge mit Zurücklegen
Für alle: $\frac{n!}{r! \cdot s! \cdot t!}$ mit r, s, t = # nicht unterscheidbare Elemente

Für einige: n^k

RSA: nach diffie-Hellman

Alice select x_A, x_B at random Bob

$y_A = R_p(g^{x_A})$ $y_B = R_p(g^{x_B})$

$k_{AB} = R_p(y_B^{x_A})$ $k_{BA} = R_p(y_A^{x_B})$

$k_{AB} \equiv_p g^{x_B x_A} \equiv_p g^{x_A x_B} \equiv_p k_{BA}$

Where p and g are predefined, y_A is efficiently computable
Thanks to chinese Remainder theorem.

Composite? (Not Prime)
If $a^{n-1} \equiv_n 1$
for a chosen base a
is violated => not Prime
else retry

Irreducible?
test all irreducibles of one rank smaller as divisors

A code can correct t Errors iff $d \geq 2t+1$
minimum distance

RSA: Generate Primes a and b => $n = a \cdot b$
$p = (a-1)(b-1)$

select $e \Rightarrow d \equiv_p e^{-1}$

send n, e to Bob as public key. Bob has Plaintext m
cyphertext(m) = $y = R_n(m^e) \longrightarrow$ Alice $m = R_n(y^d)$

Error-Correcting Codes (k, n) code over the Alphabet A with $|A| = q$ is a subset of A^n with cardinality q^k
e.g. $|\{0,1\}| = 2$

"Hamming distance": number of Positions at which two codewords differ

"minimum distance": smallest Hamming distance

nicht complete

kann nicht $A \models A \vee B$ weil dafür maste aus $\{\{A\}\} \rightarrow \{A, B\}$ abgeleitet werden

Proof System

Statement S is true or false
Proof P is maybe complete and sound
truth value T(S) says 1 if S is true
φ verification function: says 1 if proof is correct

φ efficiently computable
S, P strings

Resolution
CNF given
clause is true if at least one Element is true
if 2 clauses contain ¬A and A, merge without A.
prove unsatisfiability.

Logical consequence: $M \cup \neg F$ unsat then $M \models F$

$\Pi = (S, P, T, \varphi)$ is sound if no false statement has a proof
is complete if every true statement has a proof

Logic The Syntax: Defines an Alphabet and specifies which strings are syntactically correct

An Interpretation is suitable if all Variables are defined
A suitable interpretation is a model $A \models F$
Formula satisfiable if there exists a model, else unsatisfiable ⊥
Tautology iff ¬F is unsatisfiable
G is logical consequence if every for both suitable Interpretation yields F = G values
$F \models G$ $F \equiv G \Leftrightarrow F \models G \wedge G \models F$
If F is Tautology, write $\models F$

A Theorem is a formula to be proven

$A \models F$ is not a formula

$\{0,1\}^*$ is finite, $\mathbb{N}^2$ is countable, $\mathbb{Q}$ is countable, $\mathbb{R}$ uncountable

set A^n (tuples over A) are countable, Union of countable is countable, $\{0,1\}^\infty$ is not countable

Graph

$\deg(V)$ = #Edges from it

$\overline{P}$ = Complement of P

$\Gamma(V)$ = Neighbourhood of V = All vertices adjacent

Sum of all degrees in undirected Graph = $|E|$
in directed Graph = $2|E|$

K_4: Kompletter Graph mit 4 Knoten

Mesh / "Gittergraph": coord (i,j) is connected to $(i,j+1)$ or $(i+1,j)$ => square/cube..

Note: enumerate from 1, not from 0

Adjacency Matrix
1 if (v_i, v_j) connected
0 otherwise
diag. usually 0

diag von A^2 $= 2|E|$

A directed Graph corresponds to a relation => an undirected is like directed in both sides => irreflexive, symmetric

Anzahl Pfade von i nach j mit k Kanten drin = Eintrag (i,j) von A^k

$K_{3,4}$: Kompletter bipartiter Graph mit 3 Punkten in A und 4 in B, jedes A mit jedem B verbunden

Hypercube denoted $Q_{n,m}$; Path P_n consists of n edges (may reuse edges, may contain circles)
Cycle C_n contains n edges; A walk is a path, a tour is a path without reuse; a circuit is a tour with A=B.

Isomorphism (denoted $\cong$) = bijection; Subgraph $\preccurlyeq$

A Graph is regular if all Vertices have the same degree. k-regulär mit deg k

If planar $\boxed{E \leq 3V-6}$ für $|V| \geq 3$? connected?

Grap is "connected" if all Vertices are

Hamiltonian Cycle
visits all vertices $|V|$
A Graph with $|V| \geq 3$ and $\deg(u)+\deg(v) \geq |V|$ for ~~every~~ non-adjacent u,v is Hamiltonian. In particular, If $\deg(v) \geq |V|/2$

Tree is k-ary if each Vertex has at most k children.

Tree $\iff$ V−1 Edges and connected $\iff$ V−1 Edges and no circles

A planar connected Graph divides the plane into $|E|-|V|+2$
The sum of (how many edges touched by region) is $2|E|$

If G is bipartite, then $|E| \leq 2|V|-4$

K_n is planar iff $n \leq 4$
$K_{3,3}$ is not planar

Beweisen
Dass ein k-regulärer Graph zusammenhängt. Mit Voraussetzung $k \geq \frac{|V|-1}{2}$
$|\text{Nachbarn}(u) \cap \text{Nachbarn}(v)| = |N(u)|+|N(v)| - |N(u) \cup N(v)| = 2k - [x \leq n-2]$
$\geq 2k-n+2 \geq (n-1)-n+2 \geq 1$ □

Dass nicht planar: Allowed operations: deletion of edges; merging neighboring Vertices into one, keeping all connections; deletions of singleton vertices
Aim: Show that the simpler graph is non-planar

Polyhedra
regular if each vertex meets m faces and each face is a regular n-gon.
There are exactly 5 regular Polyhedra: $(3,3),(3,4),(4,3),(3,5),(5,3)$

Modulo

$R_m(a+b) = R_m(R_m(a)+R_m(b))$

$R_m(ab) = R_m(R_m(a)R_m(b))$

$R_a((a+b)^a) = b$

$R_m(a+mb) = R_m(R_m(a)+R_m(mb)) = R_m(R_m(a)+0) = R_m(a)$

$R_{a+1}(a^n) = R_{a+1}((-1)^n)$

$R_a(b^n) = R_a(R_a(b)^n)$

$R_m(x^{ab}) = R_m(R_m(x^a)^b)$

$a \equiv_m b \iff R_m(a) = R_m(b)$

mod 9: Quersumme mod 9. repeat bis 1 Ziffer übrig

mod 11: Ziffern von rechts her abwechselnd addieren und subtrahieren