Färbbarkeit: chromatische Zahl $\chi(G)$

bipartiten Graphen G: $\chi(G) \le 2$

2 - färbbar $\Leftrightarrow$ G enthält keinen Kreis ungerade Länge.

Unterteilung:

Satz von Kuratowski: G ist planar $\Leftrightarrow$ G enthält weder eine Unterteilung von K_5 noch von $K_{3,3}$

$K_{1,n}$, $K_{2,n}$ ist planar $K_{m,n}$ für $m,n \ge 3$ ist nicht planar.

Eulersche Polyederformel

- G zsh. und planar
- F die Menge der Gebiete

$\Rightarrow |F| = |E| - |V| + 2$

$\Rightarrow$ Für jeden planaren Graphen G mit $|V| \ge 3$ gilt:

$$|E| \le 3 \cdot |V| - 6$$

$\Rightarrow$ Ist G planar, so existiert $v \in V$ mit $d(v) \le 5$

k regulärer Graph: 每个点有k边

$2|E| = \sum_{v \in V} d(v)$

- Jeder planare Graph ist 4, 6 färbbar

Kleiner Satz von Fermat

Für alle $n \in \mathbb{N}$ mit $n \ge 2$ gilt: n ist eine Primzahl gdw.

$a^{n-1} \equiv 1 \pmod n$ für alle $a \in \mathbb{Z}_n \setminus \{0\}$

Eulersche φ-Funktion   1213见下大

Sei $n \ge 2$. Dann ist $\varphi(n) = |\{a \in \mathbb{Z}_n \setminus \{0\} \mid ggT(a,n) = 1\}|$

Primzahl p : $\varphi(p) = p - 1$

Primzahlpotenzen p^e: $\varphi(p^e) = p^e - p^{e-1} = (p-1)p^{e-1}$

PFZ: $n = \prod_{i=1}^{k} p_i^{e_i}$: $\varphi(n) = \prod_{i=1}^{k} (p_i - 1) p^{e_i - 1}$

Lemma von Euklid: $ggT(a,b) = 1$ und $a \mid b \cdot c \Rightarrow a \mid c$

Satz von Euler: f.a. $n \in \mathbb{N}$, $n \ge 2$, alle a mit $ggT(a,n) = 1$:

$a^{\varphi(n)} \equiv 1 \pmod n$

Legendre's formula

$10! = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7$

$\lfloor \frac{10}{2} \rfloor = 5$ $\lfloor \frac{10}{4} \rfloor = 2$ $\lfloor \frac{10}{8} \rfloor = 1$ $5+2+1 = 8$

$\lfloor \frac{10}{3} \rfloor = 3$ $\lfloor \frac{10}{9} \rfloor = 1$ $3+1 = 4$

$\lfloor \frac{10}{5} \rfloor = 2$ $\lfloor \frac{10}{7} \rfloor = 1$

Das Produkt von n aufeinanderfolgenden natürlichen Zahlen ist durch n! teilbar

erweiterten euklidischen Algo:

$201 - 1 \cdot 111 = 90$ $\Rightarrow 21 = 111 - (201 - 111) = 2 \cdot 111 - 201$

$111 - 90 = 21$ $6 = (201 - 111) - 4 \cdot (2 \cdot 111 - 201)$

$90 - 4 \cdot 21 = 6$ $= 5 \cdot 201 - 9 \cdot 111$

$21 - 3 \cdot 6 = 3$ $3 = 29 \cdot 111 - 16 \cdot 201$

$6 - 2 \cdot 3 = 0$ $\overset{\shortparallel}{ggT(201, 111)}$

Für $a, b, m \in \mathbb{Z}$ und $m \ge 2$ gilt

1) $(a+b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$

2) $(a \cdot b) \bmod m = ((a \bmod m) \cdot (b \bmod m)) \bmod m$

$a \equiv b \pmod m$ und $c \equiv d \pmod m$

$\Rightarrow (a+c) \equiv (b+d) \pmod m$

$\Rightarrow (a \cdot c) \equiv (b \cdot d) \pmod m$

n gerade $\Leftrightarrow$ n^2 gerade

n ungerade $\Leftrightarrow$ n^2 ungerade

Jedes $n \in \mathbb{N}_{\ge 2}$ hat eine eindeutige Primfaktorzerlegung.

z.z. $n^5 - n \equiv 0 \pmod{30}$ PFZ: $30 = 2 \cdot 3 \cdot 5$

$n^5 - n = n(n-1)(n+1)(n^2+1)$

n-1, n, n+1 sind Faktoren und 3 aufeinanderfolgende Zahlen.

$\Rightarrow 2 \mid (n^5 - n)$ $3 \mid (n^5 - n)$

Nun betrachten wir ob $n^5 - n$ durch 5 teilbar ist.

$n^5 - n = n(n-1)(n+1)(n^2+1)$

1) $n \equiv 0 \pmod 5$ $\Rightarrow$ n ist durch 5 teilbar, somit $n^5 - n$

2) $n \equiv 1 \pmod 5$ $\Rightarrow$ (n-1) durch 5 teilbar

3) $n \equiv 2 \pmod 5$ $\Rightarrow n^2 \equiv 4 \pmod 5 \Rightarrow n^2 + 1 \equiv 5$

$\Rightarrow n^2 + 1$ durch 5 teilbar

4) $n \equiv 3 \pmod 5$ $\Rightarrow n^2 + 1 \equiv 10 \pmod 5$

5) $n \equiv 4 \pmod 5$ $\Rightarrow$ (n+1) durch 5 teilbar

Chinesische Restsatz (finden 最小的x, welche folgende Kongruenzen erfüllt:

$x \equiv 4 \pmod 7$

$x \equiv 2 \pmod 8$

$x \equiv 2 \pmod 5$

① $M = 7 \cdot 8 \cdot 5 = 280$

$M_1 = 8 \cdot 5 = 40$ $M_2 = 5 \cdot 7 = 35$ $M_3 = 7 \cdot 8 = 56$

② Modulare Inverse: Gesucht: w_1 mit $40 \cdot w_1 \bmod 7 = 1$

Erw-Euklid(40,7):

$40 - 5 \cdot 7 = 5$ $2 = 7 - (40 - 5 \cdot 7) = 6 \cdot 7 - 40$

$7 - 5 = 2$ $\Rightarrow 1 = 3 \cdot 40 - 17 \cdot 7$ $\Rightarrow w_1 = 3$

$5 - 2 \cdot 2 = 1$ Das modular inverse von 40 bezüglich 7 ist 3

Erw-Euklid(35, 8): $w_2 = 3$

Erw-Euklid(56, 5): $w_3 = 1$

③ Berechne T_i und $x \in \{0, \dots, M-1\}$

$T_1 = M_1 \cdot W_1 \cdot b_1 = 40 \cdot 3 \cdot 4 = 480$ $T_2 = M_2 W_2 b_2 = 210$ $T_3 = 112$

$\Rightarrow x = (T_1 + T_2 + T_3) \bmod M = 802 \bmod 280 = 242$

eulersche φ-Function

$\varphi(2^1 \cdot 3^2 \cdot 5^3) = (2-1) 2^0 \cdot (3-1) \cdot 3^1 \cdot (5-1) 5^2$

$\varphi(5!) = \varphi(2^3 \cdot 3 \cdot 5) = 2^2 \cdot 2 \cdot 3^0 \cdot 4 \cdot 5^0$

RSA: Primzahlen p, q, $n = p \cdot q$

berechen $\varphi(n) = (p-1)(q-1)$

berechen k und ℓ mit $ggT(k, \varphi(n)) = 1$

und $k \cdot \ell \equiv 1 \pmod{\varphi(n)}$

öffentlicher Schlüssel n, k   Geheimer Schlüssel ℓ

Nachricht: $M \in \{0, \dots, n-1\}$

Verschlüss: $S := M^k \bmod n$

Gesendete Nachricht: S

Entschlüsseln:

$M' := S^{\ell} \bmod n$

$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ wobei $p_1 < p_2 < \cdots < p_k$ Primzahl

$e_1, e_2, \ldots, e_k \in \mathbb{N}$.

ggT und kgV

$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ $b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$

(wobei $a_i, b_i = 0$ ist erlaubt)

$ggT(a,b) = p_1^{\min\{a_1,b_1\}} \cdot \ldots \cdot p_n^{\min(a_n,b_n)}$

$kgV(a,b) = p_1^{\max\{a_1,b_1\}} \cdots p_n^{\max(a_n,b_n)}$

$a \cdot b = ggT(a,b) \cdot kgV(a,b)$

reflexiv: $\forall a \in A, (a,a) \in R$

irreflexiv: $\forall a \in A, (a,a) \notin R$

symmetrisch: $\forall a,b \in A$, Wenn $(a,b) \in R$, dann auch $(b,a) \in R$

antisymmetrisch: $\forall a \neq b \in M$, Wenn $(a,b) \in R$, dann $(b,a) \notin R$

transitiv: $\forall a,b,c \in M$, Wenn $(a,b) \in R, (b,c) \in R$, dann $(a,c) \in R$

Äquivalenzrelation: reflexiv, symmetrisch, transitiv

Quotientenstruktur:

M Menge, $E \subseteq M^2$ Relation $R \subseteq M^2$ Äquivalenzrelation

$M_{/R} := \{[u]_R : u \in M\}$

$E_{/R} := \{([u]_R, [v]_R) : (u,v) \in E\}$

Quotient $(M_{/R}, E_{/R})$ von (M, E) bzgl R

strikte (partielle Ordnung): $- (a,a) \notin R$ irreflexive

antisym $-$ Wenn $(a,b) \in R, (b,a) \in R$, dann $a=b$

transitive $-$ wenn $(a,b) \in R, (b,c) \in R$, dann $(a,c) \in R$

partielle Ordnung: reflexiv, antisymmetrisch, transitiv

linear: f.a. $u \neq v \in M$, $(u,v) \in R$ oder $(v,u) \in R$

Verband: eine partiell geordnete Menge $(M, \sqsubseteq)$, Wenn es f.a $x, y \in M$ sowohl ein Supremum als ein Infimum gilt

$(P(M), \subseteq)$: Teilmengenverband

Satz von Dilworth: Sei $(M, \sqsubseteq)$ ein poset wobei M endlich ist. Die max. Länge r einer Antikette in $(M, \sqsubseteq)$ ist gleich der min. Größe k einer Überdeckung von $(M, \sqsubseteq)$ durch Ketten.

a: obere Schranke für x,y, falls $x \leq a$ und $y \leq a$

untere Schranke für x,y, falls $a \leq x$ und $a \leq y$

totale Ordnung: partielle Ordnung und $\forall a,b$ mit $a \neq b$ gilt $a \leq b$ oder $b \leq a$

Supreme 最小上界 Infimum 最大下界

$(M, *)$ heißt Algebra falls gilt:

- $M \neq \emptyset$
- $* : M^n \to M$ ist eine „innere Verknüpfung"

Monoid: - $*$ assoziativ: $\forall a,b,c \in M$, $(a*b)*c = a*(b*c)$

- es gibt ein neutrales Element

$\exists e \in M, \forall a \in M. \; e*a = a*e = a$

Gruppe: - $*$ assoziativ

- es gibt ein neutrales Element
- jedes Element $a \in M$ besitzt ein Inverses Element

↳ $\forall a \in M \; \exists x \in M: x*a = a*x = e$

inverse Element bsp.

$a \in A_m^+$. Dann ist $0 \equiv m \bmod m$ $= [a + (m-a)] \bmod m$

$= a +_m \underbrace{(m-a)}_{\in A_m} \Rightarrow a^{-1} = m-a$

Ist dagegen $a = 0$

Gesucht $f: (\mathbb{Z}, +) \to (\mathbb{Q}, +)$ mit $f(x+y) = f(x) + f(y)$ f.a. $x, y \in \mathbb{Z}$

I. $f(0) = f(0+0) = f(0) + f(0) \Rightarrow 0 = f(0)$

II. $0 = f(0) = f(x + (-x)) = f(x) + f(-x)$

$\Rightarrow f(-x) = -f(x) \quad \forall x$

III. es gilt $f(2) = f(1+1) = f(1) + f(1) = 2f(1)$

induktion: $f(n) = nf(1)$

IV. Aus II. III folgt für $z \in \mathbb{Z} \setminus \mathbb{N}$, dass $-z \in \mathbb{N}$ und

$f(z) = f(-(-z)) = -f(-z) \overset{III}{=} -(-z f(1)) = z \cdot f(1)$

$\Rightarrow$ gilt $f(z) = z f(1)$ f.a. $z \in \mathbb{Z}$

$\Rightarrow F \{f_x : z \mapsto z \cdot x \mid x \in \mathbb{Q}\}$ ist gesuchte Menge

$10000 < x < 10000$, gilt $x \equiv 3 \pmod 7$ und $x \equiv 4 \pmod{11}$

$x = 7k + 3 \equiv 4 \pmod{11}$

$7k \equiv 1 \pmod{11}$

Module Inverse: $11 - 7 = 4$ $\quad 3 = 2 \cdot 7 - 11$

$7 - 4 = 3$ $\quad 1 = 2 \cdot 11 - \underline{3} \cdot 7$

$4 - 3 = 1$

$k = 3 + 11m$

$x = 7k + 3 = 21 + 77m + 3 > 10000 \Rightarrow m = 130 \quad x = 10061$