

Tjugoförsta och sista föreläsningen

● REPETITIONSPROBLEM

1. Hur många ytor kan en reguljär, eulersk, enkel, plan graf med v hörn dela in planet i?
2. De 52 korten i en kortlek delas upp i 13 högar med 4 kort i varje. Visa att man kan dra ett kort slumpmässigt ur den första högen och komplettera med ett kort var ur de övriga högarna, så att man får kort med 13 olika valörer.
3. Minns att **fibonaccitalen** $\{F_n\}_{n \in \mathbb{N}}$ definieras rekursivt av $F_0 = 0$, $F_1 = 1$ och $F_{n+2} = F_{n+1} + F_n$ för $n \in \mathbb{N}$.
Visa att $\text{sgd}(F_m, F_n) = F_{\text{sgd}(m,n)}$ för alla $m, n \in \mathbb{N}$.
4. Definiera den binära operationen $\circ$ på $\mathbb{Z}$ enligt $m \circ n = m + n + 3$ för $m, n \in \mathbb{Z}$. Visa att $(\mathbb{Z}, \circ)$ är en grupp och att den är isomorf med $(\mathbb{Z}, +)$.
5. Låt H, K vara delgrupper till en ändlig grupp G .
Om $|H|$ och $|K|$ är relativt prima och $a, b \in G$, vilka värden är möjliga för $|aH \cap bK|$?
6. Visa att i en ring $(R, +, \cdot)$ där $x \cdot x = x$ för alla $x \in R$, är $x + x = 0$ för alla $x \in R$.
7. Låt p och q vara primtal sådana att $q \mid 2^p - 1$. Visa att $q > p$.
8. Hur många väsentligt olika färgningar med högst k färger av kanterna i en ikosaeder finns det?
- 9a. Faktorisera $f(x) = x^4 + 2x^2 + x + 2 \in \mathbb{Z}_3[x]$ i irreducibla faktorer.
b. I kroppen $F = \{b_1\alpha + b_0 \mid b_0, b_1 \in \mathbb{Z}_3\}$, med $g(\alpha) = 0$ för ett lämpligt andragradspolynom $g(x)$, är alla irreducibla faktorer till $f(x)$ (betraktat som ett element i $F[x]$) av första graden. Finn ett sådant $g(x)$ och en generator för F 's multiplikativa grupp $(F \setminus \{0\}, \cdot)$.
10. Finn en kontrollmatris H för en linjär binär kod $\mathcal{C}$ som rättar ett fel, med $|\mathcal{C}| = 16$ och $1011010, 1100010 \in \mathcal{C}$.
11. Finn det minsta talet $e \geq 100$ sådant att $(1189, e)$ kan användas som krypteringsnyckel i ett RSA-system. Finn också ett tal d , så att $(1189, d)$ är en motsvarande dekrypteringsnyckel.
[1189 = 29 · 41]