FEMTE VECKOUTMANINGEN

DISKRET MATEMATIK

Denna veckas utmaning blandar den sista talteorin med kombinatorik.

Problem 1. Dela in er lilla grupp i tre team, vardera bestående av 1-2 personer, nämligen Team Alice, Team Bob och Team Caesar. Uppgiften är att Alice ska skicka ett hemligt tvåsiffrigt tal till Bob utan att Caesar får reda på det, genom att använda RSA-kryptering. Bob ska därför välja två olika, tresiffriga primtal, som han håller hemliga. Den öppna nyckeln ska göras känd för både Alice och Caesar. Medan Alice krypterar och skickar meddelandet till Bob, och Bob dektyrpterar, försöker Caesar att knäcka koden. Turas gärna om och välj olika meddelanden och primtal. Diskutera algoritmens säkerhet utifrån er erfarenhet! *OBS! Alla får använda miniräknare/dator med standardfunktioner, dvs de fyra räknesätten och liknande ting, men inte avancerade saker som primtalsfaktorisering och sådant. När Bob väljer sina primtal är det tillåtet att använda en primtalskontroll på datorn.*

Fermats lilla sats. Följande två uppgifter går ut på att, på två sätt, visa att om p är ett primtal och $a > 0$ ett godtyckligt heltal, så är $a^p \equiv a \pmod{p}$. Detta påstående kallas för Fermats lilla sats (FLS). Fundera först kort över varför FLS i princip följer ur Eulers sats, vilket vi dock inte ska använda nedan. (Alla kongruenser är modulo p.)

Problem 2. Låt p vara ett primtal.

(1) Visa att $p|\binom{p}{k}$ för varje $0 < k < p$.
(2) Visa därur att $(a+b)^p \equiv a^p + b^p$ för alla heltal a och b.
(3) Använd detta för att visa FLS med induktion över $a \in \mathbb{Z}_+$.

Problem 3. Ett *halsband med p hängen* är ett arrangemang av p bokstäver i en cirkel med hänsyn till inbördes ordning men utan hänsyn till förstabokstav (så att ABBA ger samma halsband som AABB, men inte som BABA). Vi kallar ett ord *socialt* om det ger samma halsband som åtminstone något annat ord. Vi ska nu räkna halsband med p hängen tagna ur ett alfabete med a bokstäver.

Antag först att alfabetet har $a = 2$ bokstäver. Hur många ord med $p = 5$ bokstäver finns det? Skriv dem i grupper så att orden i varje grupp ger samma halsband som varandra. Hur många grupper har bara ett ord? Vilka andra storlekar på grupper förekommer? Försök förstå varför det är så och hur $a^p - a$ kan uttryckas som ett visst antal ord. Härled därur FLS för $p = 5$ och $a = 2$.

Gör, om ni behöver, om detta med $p = 3$ och $a = 4$. Generalisera sedan ert resonemang till ett godtyckligt primtal p och heltal $a > 0$.

Problem 4. Ett företag med 10 anställda ska välja ett ombud bland 4 kandidater. Detta görs genom att varje anställd lägger sin röst på precis en valfri person bland kandidaterna. På hur många olika sätt kan valet falla ut? Hur skulle det se ut om det istället funnes n anställda och r kandidater?


A B C D E F
G H I J K L
M N O P Q R
S T U V W X
Y Z
&