NTNU

Kunnskap for en bedre verden

Institutt for matematiske fag

Eksamensoppgave i **MA1301/MA6301 Tallteori**

Faglig kontakt under eksamen: Kristian Seip

Tlf: 911 29 136

Eksamensdato: 8. august 2022

Eksamenstid (fra–til): 09:00–13:00

Hjelpemiddelkode/Tillatte hjelpemidler: A: Alle trykte og håndskrevne hjelpemidler tillatt. Alle kalkulatorer tillatt.

Annen informasjon:
Denne prøven består av 10 delpunkt som alle teller like mye. Alle svar må begrunnes.

Målform/språk: bokmål

Antall sider: 3

Antall sider vedlegg: 0

Kontrollert av:

Dato Sign

Oppgave 1 Primtallene som deler 70! er alle primtall som er mindre enn eller lik 70, det vil si $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67$.

Oppgave 2 Den diofantiske ligningen $78x - 144y = 36$ kan etter forkorting skrives enklere som $13x - 24y = 6$. Vi finner først løsningen av $13x - 24y = 1$ ved Euklids algoritme:

$$\begin{aligned} -24 &= -2 \cdot 13 + 2 \\ 13 &= 6 \cdot 2 + 1 \end{aligned}$$

Om vi nå starter fra den siste linjen i ovenstående iterasjon og reverserer Euklids algoritme, får vi:

$$\begin{aligned} 1 &= 13 - 6 \cdot 2 \\ &= 13 - 6 \cdot (-24 + 2 \cdot 13) = -11 \cdot 13 + 6 \cdot 24, \end{aligned}$$

som gir oss den spesielle løsningen $x = -11$ og $y = -6$. Den generelle løsningen av ligningen $13x - 24y = 6$ blir dermed $x = -66 + 24t$ og $y = -36 + 13t$, hvor t er et vilkårlig heltall.

Oppgave 3 Vi kan vise at $\gcd(7t + 2, 4t + 1) = 1$ for alle heltall t ved å vise at den diofantiske ligningen

$$(7t + 2)x + (4t + 1)y = 1$$

har løsning for alle t. Vi ser ved inspeksjon at $x = 4$ og $y = -7$ løser ligningen. (Alternativt kan vi bruke Euklids algoritme.)

Oppgave 4 Vi observerer først at det er nok å vise at

$$13^{81} \equiv 13 \pmod{123} \tag{1}$$

fordi vi da får at

$$13^{81^n} \equiv 13 \pmod{123}$$

holder for alle n ved induksjon. Vi ser at (1) vil følge hvis vi kan vise at

$$13^{80} \equiv 1 \pmod{123}.$$

Vi primtallsfaktoriserer $123 = 41 \cdot 3$, hvilket medfører at $\phi(123) = 2 \cdot 40 = 80$. Siden $\gcd(13, 123) = 1$, følger resultatet ved Eulers teorem.

Oppgave 5

a) Siden 97 er et primtall, gir Wilsons teorem at

$$95! \equiv 1 \pmod{97}$$

og dermed

$$11 \cdot 94 \cdot 95 \cdot 93! \equiv 6 \cdot 11 \cdot 93! \equiv 11 \pmod{97}.$$

som betyr at vi må løse kongruensen

$$6x \equiv 11 \pmod{97}.$$

Om vi ganger begge sider med 16 og bruker at $96 \equiv -1 \pmod{97}$, får vi

$$x \equiv -176 \equiv 18 \pmod{97}.$$

Resten blir dermed 18.

b) Vi må løse følgende systemet av lineære kongruenser:

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{5} \\ x &\equiv 4 \pmod{8}. \end{aligned}$$

Vi ser at vi kan bruke det kinesiske restteoremet siden $3, 5, 8$ er parvis relativt primiske. Alternativt kan vi løse problemet ved å se at kombinasjonen av den andre og den tredje kongruensen gir at siste siffer i x må være 8, og det minste aktuelle tallene er derfor $28, 68, \ldots$. Vi ser at 68 løser alle kongruensene, og generell løsning er derfor $68+120t$ hvor t er et vilkårlig heltall. Minste positive løsning er 68.

Oppgave 6 Relasjonen $\phi(pq) = 32256$ gir ligningen $(p-1)(q-1) = 32256$. Om vi setter inn at $pq = 32689$, gir dette $p + q = 434$ eller $q = 434 - p$. Om vi setter dette inn i ligningen $pq = 32689$, får vi annengradsligningen

$$p^2 - 434p + 32689 = 0$$

som har løsningene 337 og 97. Vi finner altså at $p = 337$ og $q = 97$.

Oppgave 7 Legendre-symbolet er fullstendig multiplikativt, så vi får at

$$\left(\frac{(p-1)!}{p}\right) = \prod_{j=1}^{p-1}\left(\frac{j}{p}\right).$$

Vi vet at nøyaktig halvparten av tallene $1, \ldots, p-1$ er kvadratiske rester modulo p, og dermed har nøyaktig halvparten av disse tallene Legendre-symbol lik -1. Vi får derfor

$$\left(\frac{(p-1)!}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

Oppgave 8 Vi vet at alle tallene $r_1, \ldots r_{\phi(n)}$ deler $\phi(n)$. Det betyr at

$$\operatorname{lcm}(r_1, \ldots, r_{\phi(n)}) | \phi(n),$$

noe som i dette tilfellet betyr det at $(n-1)|\phi(n)$. Men siden vi også har $\phi(n) \leq n-1$, impliserer dette at $\phi(n) = n-1$. Dette kan bare inntreffe dersom n er et primtall.

Oppgave 9 Teorem 1.2 i Notat 2 om RSA sier at

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

holder for alle heltall a hvis og bare hvis n er kvadratfritt. Ved induksjon gir dette at

$$a^{k\phi(n)+1} \equiv a \pmod{n}$$

for alle positive heltall k. I vårt tilfelle er $n = 2022 = 2 \cdot 3 \cdot 337$, og dette teoremet kan derfor brukes. Vi finner at

$$\phi(2022) = 2 \cdot 336 = 2^4 \cdot 3 \cdot 7$$

som er relativt primisk til 5 (men ingen andre heltall i intervallet $[2, 10]$). Kongruensen

$$5e \equiv 1 \pmod{\phi(2022)}$$

har derfor en entydig løsning $\bmod \phi(2022)$. (Vi trenger ikke å løse denne kongruensen.) Den gitte kongruensen løses da ved at vi setter $x = a^e$. Denne løsningen er entydig $\bmod n$ siden vi nettopp får

$$x \equiv a^e \pmod{n}$$

om vi opphøyer hver side av den gitte kongruensen i e.