NTNU

Kunnskap for en bedre verden

Institutt for matematiske fag

Eksamensoppgave i **MA1301 Tallteori—Løsning**

Faglig kontakt under eksamen: Kristian Seip

Tlf: 911 29 136

Eksamensdato: 25. november 2020

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. I og med at alle hjelpemidler er tillatt, er det viktig at svarene på oppgavene er godt begrunnet.

Målform/språk: bokmål

Antall sider: 3

Antall sider vedlegg: 0

Kontrollert av:

Dato Sign

Oppgave 1 Ved Euklids algoritme får vi

$$\begin{aligned} 567 &= 1 \cdot 417 + 150 \\ 417 &= 2 \cdot 150 + 117 \\ 150 &= 1 \cdot 117 + 33 \\ 117 &= 3 \cdot 33 + 18 \\ 33 &= 1 \cdot 18 + 15 \\ 18 &= 1 \cdot 15 + 3 \\ 15 &= 5 \cdot 3, \end{aligned}$$

hvorav vi slutter at $\gcd(567, 417) = 3$. Om vi nå starter fra den nestsiste linjen i ovenstående iterasjon og reverserer Euklids algoritme, får vi:

$$\begin{aligned} 3 &= 18 - 1 \cdot 15 \\ &= 18 - 1 \cdot (33 - 1 \cdot 18) = -1 \cdot 33 + 2 \cdot 18 \\ &= -1 \cdot 33 + 2 \cdot (117 - 3 \cdot 33) = 2 \cdot 117 - 7 \cdot 33 \\ &= 2 \cdot 117 - 7 \cdot (150 - 1 \cdot 117) = -7 \cdot 150 + 9 \cdot 117 \\ &= -7 \cdot 150 + 9 \cdot (417 - 2 \cdot 150) = 9 \cdot 417 - 25 \cdot 150 \\ &= 9 \cdot 417 - 25 \cdot (567 - 1 \cdot 417) = -25 \cdot 567 + 34 \cdot 417, \end{aligned}$$

som gir oss løsning $x = -25$ og $y = 34$ av den diofantiske ligningen $567x+417y = 3$. Den generelle løsningen blir dermed $x = -19 + 139t$ og $y = 28 - 189t$, hvor t er et vilkårlig heltall.

Oppgave 2

a) Vi antar at p er et odde primtall. Hvis $p \neq 5$, har vi $\gcd(p, 10) = 1$. Siden $\phi(10) = \phi(5) \cdot \phi(2) = 4$, får vi derfor ved Eulers teorem

$$p^{2020} \equiv p^{4 \cdot 505} \equiv 1 \pmod{10}.$$

I det spesielle tilfellet $p = 5$ har vi $5^2 \equiv 5 \pmod{10}$ og dermed $5^m \equiv 5 \pmod{10}$ for alle positive heltall m ved induksjon. Svaret er altså at det siste sifferet i p^{2020} er 1 hvis $p \neq 5$ og 5 hvis $p = 5$.

b) Vi vet at $\phi(7^2 \cdot 13) = (7^2 - 7) \cdot 12 = 42 \cdot 12 = 504$. Siden $\gcd(7^2 \cdot 13, 5) = 1$, gir Eulers teorem

$$5^{2016} \equiv 5^{504 \cdot 4} \equiv 1 \pmod{7^2 \cdot 13}.$$

Det holder derfor å regne ut $5^4 = 625$ modulo $7^2 \cdot 13 = 637$. Resten blir dermed 625 når vi deler 5^{2020} på $7^2 \cdot 13$.

c) Siden 79 er et primtall, gir Wilsons teorem at $77! \equiv 1 \pmod{79}$. Vi har dermed

$$7 \equiv 7 \cdot 77! \equiv -2 \cdot 7 \cdot 76! \pmod{79}.$$

Siden $-2 \cdot 39 \equiv -78 \equiv 1 \pmod{79}$, får vi derfor

$$7 \cdot 76! \equiv 7 \cdot 39 \equiv 36 \pmod{79}.$$

Vi får dermed rest 36 når vi deler $7 \cdot (76!)$ på 79.

Oppgave 3 Vi har at $143 = 11 \cdot 13$ og dermed $\phi(143) = 10 \cdot 12 = 120$. I følge RSA-algoritmen finner vi den hemmelige dekrypteringsnøkkelen $\{143, d\}$ ved å løse kongruensen

$$de \equiv 1 \pmod{120},$$

hvor $e = 11$. Siden $11^2 = 121$, har denne kongruensen løsning $d = 11$. Den hemmelige dekrypteringsnøkkelen er derfor $\{n, d\} = \{143, 11\}$. Dekrypteringen av den krypterte meldingen 5 finner vi ved følgende beregning:

$$5^{11} \equiv 5 \cdot 3125^2 \equiv 5 \cdot (-21)^2 \equiv 2205 \equiv 60 \pmod{143}.$$

Den dekrypterte meldingen er dermed 60.

Oppgave 4

a) 67 er et primtall, og vi har derfor $\phi(67) = 66$. Siden $22|66$ og $\phi(22) = \phi(2)\phi(11) = 10$, har 10 tall mellom 1 og 66 orden 22 modulo 67.

b) Hvis r er en primitiv rot til p, får vi alle primitive røtter til p ved å beregne r^k modulo p for alle k, $1 \leq k \leq p-1$, slik at $\gcd(k, p-1) = 1$. Siden $\gcd(5, 18) = 1$ og $2^5 \equiv 32 \equiv 13 \pmod{19}$, kan vi slutte at 13 er en primitiv rot til 19 når vi vet at 2 er en primitiv rot til 19.

Oppgave 5 Hvis $p = 3$, er $p^2 + 20 = 29$ som er et primtall. Alle andre primtall[1] kan skrives som $p = 3k + 1$ eller $p = 3k + 2$. Hvis $p = 3k + 1$, får vi $p^2 + 20 = 9k^2 + 6k + 21$ som er delelig med 3. Hvis $p = 3k + 2$, får vi $p^2 + 20 = 9k^2 + 12k + 24$ som også er delelig med 3. Dermed er 3 det eneste primtallet slik at også $p^2 + 20$ er et primtall.

[1]Du kan uttrykke dette mer kompakt ved hjelp av kongruensregning: Alle andre primtall er enten $p \equiv 1 \pmod{3}$ eller $p \equiv 2 \pmod{3}$ og dermed måtte vi eventuelt ha $p^2 + 20 \equiv 0 \pmod{3}$.

Oppgave 6 Ved definisjonen av Legendre-symbolet har den kvadratiske kongruensen

$$x^2 \equiv p \pmod{q}$$

en løsning hvis og bare hvis $(p/q) = 1$. Siden p og q er antatt å være odde, gjelder den kvadratiske resiprositetsloven:

$$(p/q) \cdot (q/p) = (-1)^{\frac{(p-1)}{2} \cdot \frac{(q-1)}{2}}.$$

Vår antagelse er at $(p/q) = 1$. For at vi også skal ha $(q/p) = 1$, det vil si at den kvadratiske kongruensen

$$x^2 \equiv q \pmod{p}$$

også har en løsning, må vi derfor ha at $\frac{(p-1)}{2} \cdot \frac{(q-1)}{2}$ er et partall. Betingelsen blir dermed at minst ett av de to primtallene p og q er kongruent til 1 modulo 4.

Oppgave 7 Primtallsfaktoriseringen til 2020 er $2 \cdot 2 \cdot 5 \cdot 101$. Siden τ er en multiplikativ funksjon som kun tar positive heltallsverdier, betyr det at høyst 4 primtall kan dele n. Vi noterer oss at $\tau(p^k) = k + 1$ for ethvert primtall p, noe som spesielt betyr at $\tau(p^k)$ kun avhenger av k og ikke av p. Vi kan dermed anta at ingen primtall > 7 deler n, siden vi i motsatt fall kunne erstatte et av primtallene i n med et mindre primtall og på den måten finne $m < n$ slik at $\tau(m) = \tau(n)$. Vi kan derfor anta at $n = 2^{k_1} \cdot 3^{k_2} \cdot 5^{k_3} \cdot 7^{k_4}$, hvor

$$(k_1 + 1)(k_2 + 1)(k_3 + 1)(k_4 + 1) = 2020$$

og $k_1 \geq k_2 \geq k_3 \geq k_4 \geq 0$. Det er klart at $k_1 = 100$ siden vi ellers ville ha $k_1 \geq 201$ og dermed at $n \geq 2^{201} > 2^{100} \cdot 3^{19}$ og $\tau(2^{100} \cdot 3^{19}) = 2020$. Tilsvarende må vi ha $k_2 = 4$ siden $3^9 > 3^4 \cdot 5 \cdot 7$, og videre at $k_3 = k_4 = 1$ siden $5^3 > 5 \cdot 7$. Konklusjonen blir derfor at det minste tallet n slik at $\tau(n) = 2020$ er $n = 2^{100} \cdot 3^4 \cdot 5 \cdot 7$.