Räkneuppgifter vecka 8 och 9

Tyvärr finns det två versioner av bokens fjärde upplaga. Uppgifterna jag hänsvisar till är till den vanliga inbundna boken, men i den billigare "International edition" har vissa kapitel tagits bort och flyttats. Detta börjar runt kapitel 20. Därför översätter jag här de uppgifter som är rekommenderade till vecka 8 och 9. Jag tog mig lite friheter vid översättningen, men det spelar ingen roll om man gör bokens uppgifter eller dessa.

1 Vecka 8

Redovisningsuppgifter till torsdag v8 är: **21.1, 21.3, 22.2, 22.7** nedan.

20.1 Gör två listor med alla kvadratiska rester (KR), och alla kvadratiska icke-rester (IR) modulo 19.

21.1 Ta reda på vilka av följande ekvationer som har lösningar! Alla modulus är primtal.
a) $x^2 \equiv -1 \mod 5987$
b) $x^2 \equiv 6780 \mod 6781$
d) $x^2 - 64x + 943 \equiv 0 \mod 3011$
Tips på d: kvadratkomplettera vänsterledet!

21.3 För vilka primtal p är 3 en kvadratisk rest? Med andra ord, när är $\left(\frac{3}{p}\right) = 1$?
Testar man så ser man att 3 är en kvadratisk rest för primtalen:

$$11, 13, 23, 37, 47, 59, 61, 71, 73, 83, 97, 107, 109, \cdots$$

och 3 är en icke-rest för primtalen

$$5, 7, 17, 19, 29, 31, 41, 43, 53, 67, 79, 89, 101, 103, 113, 127, \cdots$$

Prova reducera dessa listor modulo olika tal och försök hitta en regel för när 3 är en KR. Formulera en förmodan och försök sedan bevisa den!

22.1 Använd kvadratisk reciprocitet för att beräkna följande Legendre-symboler.

$$\mathbf{a}) \quad \left(\frac{85}{101}\right) \qquad \mathbf{b}) \quad \left(\frac{29}{541}\right) \qquad \mathbf{c}) \quad \left(\frac{101}{1987}\right) \qquad \mathbf{d}) \quad \left(\frac{31706}{43789}\right)$$

22.2 Har ekvationen $x^2 - 3x - 1 \equiv 0 \mod 31957$ någon lösning? Tips: Du behöver inte hitta en lösning! Kvadratkomplettera, eller använd formeln för vanliga andragradsekvationer. I formeln ingår talet $\frac{1}{2}$ vilken inte är ett heltal. Går 2 kanske att invertera modulo 31957?

22.7 Låt p vara ett primtal som uppfyller $p \equiv 3 \mod 4$. Antag att a är en kvadratisk rest (KR) modulo p.
a) Visa att $x = a^{\frac{p+1}{4}}$ är en lösning till $x^2 \equiv a \mod p$. Detta ger ett explicit sätt att hitta kvadraträtter modulo primtal som kongruenta med 3 mod 4.
b) Lös ekvationen $x^2 \equiv 7 \mod 787$. Dina svar ska ligga mellan 0 och 787.

Vecka 9

Rekommenderade uppgifter:
Uppgifterna nedan är från J. Silverman's bok. Uppgifter från algebra-kompendiet ingår också till vecka 9, se kursplaneringen på kurshemsidan.

24.3 Skriv primtalet $p = 12049$ som en summa av två kvadrater, $p = a^2 + b^2$ genom att utgå från likheten

$$557^2 + 55^2 = 26 \cdot 12049$$

och använda "Fermats nedgångsprocedur" två gånger.

25.1 Skriv följande tal som en summa av två kvadrater, eller förklara varför detta inte är möjligt. Inga av talen är primtal.

(a) 4370

(b) 1885

(c) 1189

(d) 3185