Inlämningsuppifter B

A

1. (a) Ta reda på exakt hur många primtal det finns som är mindre än var dera av följande tal: $10, 10^2, 10^3, 10^4$ och 10^5. Använd gärna t ex Matlab eller sök på nätet.
   (b) Gauss och Legendre gav runt 1800 en approximativ formel för antalet primtal mindre än ett givet värde. Vad ger den för de ovanstående värdena. Hur stora är felen?
   (c) Ungefär hur stor andel av alla tal mindre än 2^{32} är primtal.
   (d) Ungefär hur stor andel utgör primtalen av de nästakommande 2^{32} tal, dvs av talen mellan 2^{32} och $2 \cdot 2^{32}$ (4)

2. Ge två primtal p_i sådana att talen $2^{p_i} - 1$ är sammansatta tal och ge primtalsfaktoriseringarna av dessa. (2)

3. (a) Vilket är det största primtal som har hittats utan hjälp av datorer. Vem gjorde det och när?
   (b) Vilket är det största kända primtalet idag.
   (c) Hur skulle du göra för att hitta primtal mellan 10 000 och 10 050 och kontrollera att det verkligen är ett primtal? Du behöver inte genomföra det utan bara berätta noggrannt hur du skulle göra. (3)

4. Lös ekvationen $x^{10001} \equiv 203 \pmod{1039}$. (5)

5. (a) I uppgift 10.3 i boken visade du att 561 är ett Carmichael tal. Visa att även 1105 är det.
   (b) Ett tal a kallas ett *vittne* för m om $a^{m-1} \neq 1 \pmod{m}$. Visa att 2 är ett vittne för 18 genom att använda succesiv kvadrering.
   (c) Ge din tolkning till varför det kallas vittne, d v s förklara vad a är vittne till? (7)

6. Låt oss för naturligta tal x definiera funktionen
$$\sigma(x) = \sum_{d|x} d.$$
   Visa att $\sigma(n \cdot m) = \sigma(n)\sigma(m)$ om SGD(n, m)=1. (6)

7. Låt oss göra ett RSA krypto med de offentliga nycklarna $m = 7303$ och $k = 5$. Låt vidare bokstäverna i alfabetet översättas till siffrorna 11 och uppåt i tur och ordning.
   (a) Välj ett eget ord och visa hur du krypterar det.
   (b) Kan du knäcka kryptot och dekryptera ordet 5427, 7110, 2165, 1 (8)