Lösningar till Tentamensskrivnng

LGMA 50

Algebra och Talteori

Hörsalsvägen

Fredag den 18 mars, 2016

8.30 - 12.30

1 *[5] I dag är det fredagen den 18 mars 2016. Vilken veckodag var det för hundra år sedan och för två hundra år sedan?*

Ett år har som bekant 365 dagar, utom skottår då en extra dag införs mellan 28 februari och 1 mars. Enligt den Julianska kalendern är ett årtal X ett skottår om och endast om $X \equiv 0(4)$. Den Gregorianska kalendern infördes i Sverige på 1700-talet, och enligt denna skall ett skottår dessutom uppfylla villkoret $X \equiv 0(100)$ implicerar att $X \equiv 0(400)$

$365 = 1(7)$. Hundra år ger $100 \cdot 1 = 100 = 2(7)$. Under dessa hundra år har 25 skottår inträffat (det första 29 februari 1920, det sista 29 february 2016). Detta ger $2 + 25 = 27 = -1(7)$. Ur detta sluter vi att den 18 mars 2016 var en lördag. Går vi tillbaka ytterligare hundra år, har vi bara 24 skottdagar ty 1900 var inte ett skottår. Således $2 + 24 = 26 - 2(7)$ Så den 18 mars 1816 var en måndag.

2 *Låt* $n = 210 = 2 \cdot 3 \cdot 5 \cdot 7$

a) [2] Beräkna Eulerfunktionen $\phi(n)$

$\phi(n) = 210 \cdot (1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5})(1 - \frac{1}{7}) = 48$

b) [1] Ge en lista över alla primtal p *sådana att* $gcd(p, n) > 1$

$p = 2, 3, 5, 7$

c) [4] Ge en lista över alla tal m *sådana att* $1 \leq m < n$ *och* $gcd(m, n) = 1$ *men som inte är primtal*

Först och främst $m = 1$. Vidare $11^2, 13^2 < 210$ medan $17^2 > 210$ så minsta primtalsfaktorn blir $11, 13$. Vi har produkter av 11 och 13 mindre än 210, d.v.s. $11^2, 11 \cdot 13, 11 \cdot 17, 11 \cdot 19, 13^2$

d) [3] Utnyttja de föregående uppgifterna för att beräkna antalet primtal i intervallet $[0, 210]$

Vi får helt enkelt $48 + 4 - 6 = 46$ printal

3 *Betrakta följande tabell över resterna av* 2^i *med avseende på primtalet* 19

$i =$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$2^i =$	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1

Med hjälp av denna tabell (eller på annat sätt)

a) [2] Lös ekvationen $3x \equiv 7(19)$

$3 = 2^{13}, 7 = 2^6$ således $x = 2^{6-13} = 2^{-7} = (2^{18}2^{-7}) = 2^{11} = 15$

b) [3] Avgör vilka av talen $14, 3$, *och* 5 *som är kvadratiska residyer och finn de två kvadraträtterna i förekommande fall.* $14 = 2^7, 3 = 2^{13}, 5 = 2^{16}$ således bara 5 är en kvadrat. Vi får att $(2^8)^2 = 5$ och $2^8 = 9$ är en kvadratrot. Den andra är $19 - 9 = 10 (= 2^{17}, 2^{34} = 2^{16})$

c) [2] Vilka tal är kuber?

18 är delbart med 3, således $2^3 = 8, 2^6 = 7, 2^9 = 18, 2^{12} = 11, 2^{15} = 12, 2^{18} = 1$

d) [3] Finn samtliga lösningar till ekvationen $x^2 + x + 1 \equiv 0$

(Uppenbarligen söker vi lösningar modulo 19)

$x^3 = 1$ har tre lösningar, nämligen $1, 2^6 = 7, 2^{12} = 11$. Eftersom $x^3 - 1 = (x-1)(x^2 + x + 1)$ måste den andra faktorn ha rötterna $7, 11$

e) [5] I sekvensen ovan händer det att nästkommande tal antingen är större eller mindre än talet självt. Använd detta för att finna perioden av $\frac{1}{19}$ *i den binära utvecklingen d.v.s. i termer av* 2^{-n}

Exempel: $\frac{1}{3} = 0,010101\cdots = \frac{1}{2^2} + \frac{1}{2^4} + \frac{1}{2^6} + \ldots$ *med perioden* 01, *medan* $\frac{1}{7} = 0,001001001\cdots = \frac{1}{2^3} + \frac{1}{2^6} + \frac{1}{2^9} + \ldots$ *med perioden* 001

När vi utför den långa divisionen med 19 multiplicerar vi resten med 2 (inte 10 som i det vanliga decimalfallet). Om denna är större än 19 erhåller vi en etta, annars en nolla. I det första fallet blir resten mindre i det andra fallet större.

Således får vi

$0,000011010111100101...$ med period 000011010111100101

4 *[5] Visa att* $gcd(2^m - 1, 2^n - 1) = 2^{gcd(m,n)} - 1$

Om $d|m$ gäller att $2^d - 1$ delar $2^m - 1$. Därav ser vi att $2^{gcd(m,n)} - 1$ delar både $2^m - 1, 2^n - 1$. Omvänt om ett primtal p delar $2^m - 1, 2^n - 1$ gäller att $2^m = 1(p), 2^n = 1(p)$ och därmed att $2^{gcd(m,n)} = 1(p)$

Ett alternativt är följande: Antag att $m > n$ we kan då skriva $2^m - 1 = 2^{n-m}(2^m - 1) = 2^{m-n} - 1$, således gäller att $\gcd(2^m - 1, 2^n - 1) = \gcd(2^{m-n} - 1, 2^n - 1)$. Upprepar vi detta finner vi att s* länge $kn < m$ att $\gcd(2^m - 1, 2^n - 1) = \gcd(2^{m-kn} - 1, 2^n - 1)$. Sätter vi $m = kn + r_1$ finner vi således att $\gcd(2^m - 1, 2^n - 1) = \gcd(2^n - 1, 2^{r_1} - 1)$. Euklides algoritm för m, n löper således parallellt med algoritmen för $2^m - 1, 2^n - 1$ med de successiva resterna $2^{r_i} - 1$. Notera att $2^r - 1 = 0$ om och endast om $r = 0$.

5 *[5] Vilket är det minsta tal som kan skrivas som summan av två kvadrater på åtta olika sätt?*

Talet måste ha tre distinkta primtalsfaktorer av typ $1(4)$. De första tre sådana primtal är givna av $5, 13, 17$. Således $5 \cdot 13 \cdot 17 = 1105$

6 *a) [5] Hur många lösningar har ekvationen* $x^2 + a = y^2$ *modulo ett primtal* $p > 1$*?*

Ledning: Skriv ekvationen som $a = (y + x)(y - x)$ Vi kan skriva $a = t \cdot (a/t)$ för $t = 1, 2, \ldots p - 1$. Lös $y + x = t, y - x = a/t$ med lösningarna $y = \frac{1}{2}(t + a/t), x = \frac{1}{2}(t - a/t)$. D.v.s $p - 1$ lösningar.

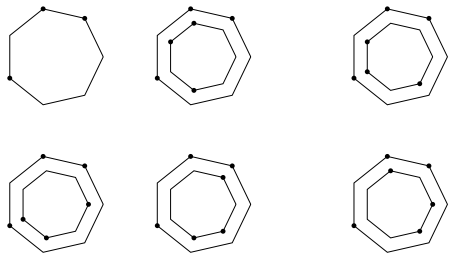
b) [10] Med hjälp av uppgiften ovan (eller på annat sätt) undersök hur många kvadratiska residyer förblir kvadratiska residyer efter en translation av ett tal $a \neq 0$*. Svaret beror på huruvida* $p = 1, 3(4)$

Lösningarna $\pm x, \pm y$ ger samma kvadrater x^2, y^2, men vi kan inte dividera med 4 ty vissa lösningar har $x = 0$ eller $y = 0$. Lösningen $(0, y)$ förekommer bara om a är en kvadratisk residy. Lösningen $(x, 0)$ förekommer bara om $-a$ är en kvadratisk residy.

Om $p = 3(4)$ är antingen a eller $-a$ en kvadratisk residy, och således förekommer endast två lösningar med $xy = 0$. Ta bort dessa och det återstår $p - 3$ lösningar, dividera dessa med 4 och vi får $\frac{p-3}{4}$ fall med $X + a = Y$ där $X, Y \neq 0$ är kvadratiska residyer.

Om $p = 1(4)$ och a är en kvadratisk residy kommer båda fallen $(x, 0), (0, y)$ att förekomma. Ta bort dessa fyra lösningar och dividera med 4 och vi får $\frac{p-1}{4} - 1$. Om a inte är en kvadratisk residy kommer ingen av fallen uppkomma och vi får $\frac{p-1}{4}$.

Detta problem har följande tolkning. Tag ett udda tal $N = 2n + 1$ och dela in cirkeln i detta antal lika delar och skapa en regelbunden polygon med N sidor. Markera n bland dessa N sidor (eller hörn) så att vid varje icke-trivial vridning av polygonen i sig själv ett fixt antal av de markerade sidorna (hörnen) överlappar. Detta är möjligt om $n = 2k + 1$ är udda och N är ett primtal och det fixa överlappande antalet är k genom att markera de kvadratiska residyerna skilda från noll. Nedan illustreras detta i fallet av heptagoner (d.v.s. $N = 7$). Notera alltid precis en överlappning.



Ulf Persson
12/3 2016
Telefonvakt: Carl Lundholm `tel: ankn 5325`