Elementär talteori, våren 2013
Förslag till lösningar för övning 6

1. Hur många primitiva rötter finns det modulo 13? Beräkna primitiva rötterna modulo 13.

2. Presentera ett reducerat restsystem modulo 13 med hjälp av någon primitiv rot.

Lösningar. Vi bestämmer först ordningen för talet två, dvs. $\mathrm{ord}_{13}\,2$. Ordningen delar talet $13-1=12$ enligt Lemma 34, och därmed är ordningen något av talen 1, 2, 3, 4, 6 och 12. Vi vet att $\mathrm{ord}_{13}2 \neq 1$, och eftersom det dessutom gäller att

$$2^2 \equiv 4 \not\equiv 1, \quad 2^3 \equiv 8 \not\equiv 1, \quad 2^4 \equiv 16 \equiv 3 \not\equiv 1, \quad \text{och} \quad 2^6 \equiv 64 \equiv 12 \not\equiv 1 \pmod{13},$$

måste $\mathrm{ord}_{13}2 = 12$, alltså är 2 en primitiv rot modulo 13.

Nu kan vi skriva alla restklasser olika noll som en potens av 2: Vi beräknar först de potenser som saknas, dvs. potenserna

$$2^5 \equiv 32 \equiv 6, \quad 2^7 \equiv 2^{5+2} \equiv 24 \equiv 11, \quad 2^8 \equiv 2^{7+1} \equiv 22 \equiv 9,$$
$$2^9 \equiv 2^{8+1} \equiv 18 \equiv 5, \quad 2^{10} \equiv 2^{9+1} \equiv 10, \quad 2^{11} \equiv 2^{10+1} \equiv 20 \equiv 7.$$

Då är de efterfrågade presentationerna

$1 \equiv 2^{12}$	$5 \equiv 2^9$	$9 \equiv 2^8$
$2 \equiv 2^1$	$6 \equiv 2^5$	$10 \equiv 2^{10}$
$3 \equiv 2^4$	$7 \equiv 2^{11}$	$11 \equiv 2^7$
$4 \equiv 2^2$	$8 \equiv 2^3$	$12 \equiv 2^6$

Eftersom det för varje $\alpha \in \{1, 2, \ldots, 12\}$ gäller att ordningen för potensen 2^α är

$$\mathrm{ord}_{13}2^\alpha = \frac{\mathrm{ord}_{13}2}{(\alpha, \mathrm{ord}_{13}2)} = \frac{12}{(\alpha, 12)},$$

så är primitiva rötterna modulo 13 de potenser för vilka $(\alpha, 12) = 1$, dvs.

$$2^1 \equiv 2, \quad 2^5 \equiv 6, \quad 2^7 \equiv 11 \quad \text{och} \quad 2^{11} \equiv 7.$$

3. Lös ekvationen $x^2 \equiv 12 \pmod{13}$. (Tips: skriv talet 12 med hjälp av en primitiv rot, berätta värför du kan använda kvadratrot i ekvationen och använd sedan Lagranges sats.)

Lösning. Från förra uppgiften vet vi att $12 \equiv 2^6 \pmod{13}$. Eftersom $(\pm 2^3)^2 = 2^6 \equiv 12 \pmod{13}$, finns det två olika lösningar $x \equiv \pm 2^3 \equiv \pm 8 \pmod{13}$, alltså lösningarna $x \equiv 5$ och $x \equiv 8 \pmod{13}$. Enligt Lagranges sats finns det högst två lösningar, alltså har vi hittat alla lösningar.

4. Låt $n = 47 \cdot 53$. Välj något tal e som du kan använda i den offentliga nyckeln i RSA (inte talet 1, eftersom metoden inte då krypterar), och bestäm de andra talen som behövs för att använda RSA. Slutligen, demonstrera metoden genom att kryptera och sedan dekryptera något tal du valt.

Lösning. Vi beräknar först

$$\varphi(n) = \varphi(47 \cdot 53) = 46 \cdot 52 = 2 \cdot 23 \cdot 2 \cdot 2 \cdot 13 = 2^3 \cdot 13 \cdot 23 = 2392.$$

Talet e får inte ha några gemensamma delare med talet 2392. Ur primtalsfaktoriseringen för talet 2392 ser vi att t.ex. talet $e = 11$ duger. Nu kan vi lösa talet d ur kongruensekvationen

$$de \equiv 1 \pmod{\varphi(n)},$$

eller ur Diofantiska ekvationen

$$11d - 2392x = 1.$$

Vi löser d med Euklides algoritm: För det första gäller

$$2392 = 217 \cdot 11 + 5, \quad \text{och} \quad 11 = 2 \cdot 5 + 1,$$

alltså

$$1 = 11 - 2 \cdot 5 = 11 - 2\,(2392 - 217 \cdot 11) = 435 \cdot 11 - 2 \cdot 2392,$$

dvs. uppfyller talet $d = 435$ kraven.

Nu är alltså den offentliga nyckeln $(n, e) = (47 \cdot 53, 11) = (2491, 11)$, och den hemliga nyckeln är $(p, q, \varphi(n), d) = (47, 53, 2392, 435)$.

Vi demonstrerar metoden genom att kryptera talet $w = 28$:

$$\begin{aligned} w' \equiv w^e \equiv 28^{11} \equiv 28^{1+2+8} &\equiv 28 \cdot 784 \cdot 2027 \\ &\equiv 21952 \cdot 2027 \equiv 44496704 \equiv 2462 \pmod{2491} \end{aligned}$$

Vi kan dekryptera w' genom att utföra följande beräkning:

$$\begin{aligned} w'^d \equiv 2462^{435} \equiv -29^{1+2+16+32+128+256} &\equiv -29 \cdot 841 \cdot 2217 \cdot 346 \cdot 1976 \cdot 1179 \\ \equiv -24389 \cdot 767082 \cdot 2329704 &\equiv -1970 \cdot 2345 \cdot 619 \equiv -4619650 \cdot 619 \\ &\equiv -1336 \cdot 619 \equiv -826984 \equiv -2463 \equiv 28 \pmod{2491}. \end{aligned}$$

5. Låt $n = 16637$. Bestäm dess primtalsfaktorer p och q.

Lösning. Vi hoppas att kraven i Sats 42 gäller, och utför beräkningarna

$$t = \lceil \sqrt{n} \rceil = \lceil \sqrt{16637} \rceil = 129,$$

och

$$r = \sqrt{t^2 - n} = \sqrt{129^2 - 16637} = \sqrt{4} = 2.$$

Nu märker vi att

$$n = t^2 - \left(t^2 - n\right) = t^2 - r^2 = (t + r)\,(t - r) = (129 + 2)\,(129 - 2) = 131 \cdot 127.$$

Eftersom både 127 och 131 är primtal, har vi hittat primtalsfaktorerna p och q.

6. Låt $(n, e) = (16637, 11)$ vara en offentlig nyckel i RSA-systemet. Hitta den hemliga nyckeln.

Lösning. Från den förra uppgiften vet vi att primtalsfaktoriseringen för talet n är $131 \cdot 127$. Vi kan alltså beräkna

$$\varphi(n) = 130 \cdot 126 = 16380,$$

och då får vi exponenten d genom att lösa den Diofantiska ekvationen

$$11d - 16380x = 1.$$

Vi kan igen använda Euklides algoritm: Vi beräknar

$$16380 = 1489 \cdot 11 + 1,$$

och av detta följer det att

$$\begin{aligned} 1 = 16380 + (-1489) \cdot 11 = 16380 \cdot (-10) + (16380 - 1489) \cdot 11 \\ = 16380 \cdot (-10) + 14891 \cdot 11. \end{aligned}$$

Nu märker vi att talet $d = 4891$ duger.