Elementär talteori, våren 2013
Förslag till lösningar för övning 4

Kom ihåg att anmäla er till tenten! Deadline är på måndagen 18.2.

1. Hitta ett reducerat restsystem modulo 30.

Lösning. Enligt kompendiet räcker det att välja något fullständigt restsystem modulo 30, t.ex. 0, 1, 2, 3, ..., 29, och från det ta bort de tal som har en gemensam delare med talet 30. Eftersom $30 = 2 \cdot 3 \cdot 5$, måste vi alltså ta bort tal delbara med 2, 3 och 5. Kvar blir då talen

$$1,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23 \text{ och } 29.$$

2. Hitta alla primitiva rötter modulo 11 och ordningen hos alla tal i det reducerade restsystemet modulo 11.

Lösning. Vi undersöker först ordningen för talet 2 modulo 11. Enligt Lemma 34 gäller $\operatorname{ord}_{11}2 \mid (11-1) = 10$, alltså är $\operatorname{ord}_{11}2$ något av talen 1, 2, 5 och 10. Klart gäller att $\operatorname{ord}_{11}2 \neq 1$, och eftersom det dessutom gäller att

$$2^2 \equiv 4 \not\equiv 1 \pmod{11} \quad \text{och} \quad 2^5 \equiv 32 \equiv 10 \not\equiv 1 \pmod{11},$$

måste $\operatorname{ord}_{11}2 = 10$. Därmed är 2 en primitiv rot modulo 11.

Eftersom 2 är en primitiv rot, bildar potenserna $2, 2^2, 2^3, \ldots, 2^{10}$ ett reducerat restsystem modulo 11 enligt Sats 28, och enligt Lemma 36 är potensens 2^α (var $\alpha \in \mathbb{Z}_+$) ordning $\frac{10}{(\alpha,10)}$. Genom att räkna potenserna för talet 2 får vi ett reducerat restsystem modulo 11, som innehåller talen

$$\begin{aligned} 2, \quad 2^2 \equiv 4, \quad 2^3 \equiv 8, \quad 2^4 \equiv 5, \quad 2^5 \equiv 10, \\ 2^6 \equiv 9, \quad 2^7 \equiv 7, \quad 2^8 \equiv 3, \quad 2^9 \equiv 6, \quad 2^{10} \equiv 1, \end{aligned}$$

och deras ordning är enligt Lemma 36

$$\begin{aligned} 10, \quad \tfrac{10}{2} = 5, \quad 10, \quad \tfrac{10}{2} = 5, \quad \tfrac{10}{5} = 2, \\ \tfrac{10}{2} = 5, \quad 10, \quad \tfrac{10}{2} = 5, \quad 10, \quad 1. \end{aligned}$$

Samma sak i en tabell:

n	1	2	3	4	5	6	7	8	9	10
$\operatorname{ord}_{11}n$	1	10	5	5	5	10	10	10	5	2

Från tabellen ser vi att primitiva rötterna modulo 11 är 2, 6, 7 och 8.

3. Hitta rötterna för polynomet $x^2 - x$ modulo 5. Hitta även rötterna för polynomet modulo 6, och förklara värför detta inte kontradikterar Lagranges sats.

Lösning. Talet fem är ett primtal, och eftersom polynomet i fråga är av graden två kan det enligt Lagranges sats ha högst två rötter modulo 5. Eftersom $0^0 - 0 \equiv 0$ och $1^1 - 1 \equiv 0 \pmod{5}$, är 0 och 1 de enda rötterna för polynomet modulo 5.

Vi hittar rötterna modulo 6 genom att räkna ut värdet för polynomet med alla tal i ett fullständigt restsystem:

$$0^0 - 0 \equiv 0, \quad 1^1 - 1 \equiv 0, \quad 2^2 - 2 \equiv 2, \quad 3^2 - 3 \equiv 0, \quad 4^2 - 4 \equiv 0, \quad 5^2 - 5 \equiv 2.$$

Rötterna modulo 6 är alltså 0, 1, 3 och 4. Vi har alltså fyra rötter modulo 6, men detta kontradikterar inte Lagranges sats eftersom talet 6 inte är ett primtal.

4. Bevisa Wilsons sats, alltså att om p är ett primtal, så gäller

$$(p-1)! \equiv -1 \pmod{p}.$$

Lösning. Vi ser lätt att resultatet stämmer om $p = 2$, eftersom $(2-1)! = 1 \equiv -1 \pmod{2}$. Antag alltså att $p \neq 2$.

Låt g vara någon primitiv rot modulo p (en sådan existerar enligt Sats 29). Då kan vi enligt Sats 28 skriva alla faktorer i produkten $(p-1)! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1)$ som potenser $g, g^2, g^3, \ldots, g^{p-1}$ modulo p i någon ordning, eftersom faktorerna i $(p-1)!$ bildar ett reducerat restsystem modulo p. Därmed följer det att

$$(p-1)! \equiv 1 \cdot g \cdot g^2 \cdot g^3 \cdot \ldots \cdot g^{p-1} \equiv g^{p(p-1)/2} \equiv (g^p)^{(p-1)/2} \equiv g^{(p-1)/2} \pmod{p},$$

var vi i den sista kongruensen använde Fermats lilla sats.

Enligt Fermats lilla sats gäller

$$\left(g^{(p-1)/2}\right)^2 \equiv g^{p-1} \equiv 1 \pmod{p},$$

dvs. $g^{(p-1)/2} \equiv \pm 1 \pmod{p}$, och eftersom g är en primitiv rot, gäller $g^{(p-1)/2} \not\equiv 1 \pmod{p}$. Alltså måste det gälla att $g^{(p-1)/2} \equiv -1 \pmod{p}$.

5. Bevisa andra hållet av Wilsons sats: Om

$$(n-1)! \equiv -1 \pmod{n},$$

så är n ett primtal.

Lösning. Vi gör ett motantagande: låt n vara ett sammansatt tal, för vilket $(n-1)! \equiv -1 \pmod{n}$. Ifall $n = 4$, så gäller $(4-1)! = 3! = 6 \equiv 2 \not\equiv -1 \pmod{4}$. Ifall n av formen p^2 för något primtal $p \neq 2$, så hittas i produkten $1 \cdot 2 \cdot \ldots \cdot (n-1)$ i alla fall talen p och $2p$, och därmed är $(n-1)! \equiv 0 \not\equiv -1 \pmod{n}$.

Till sist, ifall n är ett sammansatt tal som inte är en kvadrat av ett primtal, så kan vi välja någon primtalsfaktor $p \mid n$, och konstatera att det i produkten $1 \cdot 2 \cdot \ldots \cdot (n-1)$ hittas talen p och $\frac{n}{p}$, alltså gäller det igen att $(n-1)! \equiv 0 \not\equiv -1 \pmod{n}$.

6. Bevisa att det finns oändligt många primtal av formen $4k+3$. (Tips: Tänk på hur man bevisade att det finns oändligt många primtal. Kunde man på något sätt generalisera detta bevis?)

Lösning. Vi gör ett motantagande: Det finns endast ändligt många primtal av formen $4k + 3$. Låt dessa primtal vara $q_1, q_2, \ldots, q_n$. (Listan är inte tom, eftersom talet 3 för till listan.) Då kan konstatera att alla andra udda primtal är kongruenta med 1 modulo 4.

Vi undersöker talet

$$N = 4q_1 q_2 \cdots q_n - 1.$$

Vi kan skriva talet N som en produkt av primtalen $p_1 p_2 \cdots p_m$. Eftersom N är udda, är alla des primtalsfaktorer p_ℓ udda, dvs. $p_\ell \equiv 1$ eller $p_\ell \equiv -1 \pmod{4}$. Eftersom inget av primtalen $q_1, \ldots, q_n$ har någon gemensam faktor med N, måste det gälla att $p_1 \equiv p_2 \equiv \ldots \equiv p_m \equiv 1 \pmod{4}$. Men nu gäller

$$-1 \equiv N \equiv p_1 p_2 \cdots p_m \equiv 1 \cdot 1 \cdot \ldots \cdot 1 \equiv 1 \pmod{4},$$

vilket är en motsägelse.