Elementär talteori

Anne-Maria Ernvall-Hytönen

18 februari 2013

Innehåll

Kapitel 1

Inledning

Talteori har fascinerat människor genom tiderna. Redan Eukleides visade i sitt Elementa att det finns oändligt många primtal. Alla vet vad är en pythagoreiska triangel (jo, det är också talteori). Diagonalen av en 1×1-ruta var också intressant: Hur stor är den? Är det möjligt att skriva längden av diagonal i form $\frac{r}{s}$, var både r och s are hela tal? Nej, tyvärr är det inte möjligt. Pythagoreiska skolan tänkte att det var synd, och beslutade att ingen får prata om det. Och om någon vill prata att diagonalen är en *irrational tal*, sen måste de dö...

Under de sista 20 år har forskare hittat många underbara talteoretiska bevis: Först Wiles och Taylor visade Fermats sista sats, sen Mihăilescu visade att Catalans konjektur stämmer, och sen Green och Tao visade att det finns ... länga aritmetiska ... inom primtal. Men det finns massor av öppna problem, också: Till exempel ingen har utmanat att visa Riemanns hypotes. Många tror att den stämmer, men inte alla.

Under kursen hoppas jag att studerande lär sig de elementära talteoretiska begreppen, och hur man använder talteori (t.ex. i kryptografi).

Kursen är tillämplig för alla studerande. Jag har försökt att tänka vad behövs i skolorna och hurdana frågor är intressanta i allmänna matematiska studier.

I kompendiet finns det material som vi inte lär oss inom föreläsningarna. I föreläsningarna har vi exemplar som inte finns i kompendiet.

Litteraturförteckning

[1] Paulo Ribenboim, *My Numbers, My Friends*

[2] Kenneth H. Rosen, *Elementary Number Theory and its Applications*

[3] Kalle Väisälä, *Lukuteorian ja korkeamman algebran alkeet*

Kapitel 2

Delbarhet och primtal

2.1 Delbarhet

Vi börjar med delbarher:

Definition 1. Tal d *delar* tal n, om $\frac{n}{d}$ är ett helt tal. Vi skriver

$$d \mid n.$$

Tal d kallas *ett delare* till tal n. Om $\frac{n}{d}$ inte är ett helt tal, säger vi att tal d inte delar tal n, och vi skriver

$$d \nmid n.$$

T.ex. $5 \mid 25$ (eftersom $\frac{25}{5} = 5 \in \mathbb{Z}$), $1 \mid 100$ (eftersom $\frac{100}{1} = 100 \in \mathbb{Z}$), men $6 \nmid 31$ (eftersom $\frac{31}{6} \approx 5,167 \notin \mathbb{Z}$).

2.2 Primtal

Sats 2. *Om $d \mid a$ och $d \mid b$, gäller det också att*

$$d \mid (an + bm)$$

för $n, m \in \mathbb{Z}$

Bevis. Eftersom $d \mid a$ och $d \mid b$ har vi $\frac{a}{d} = k \in \mathbb{Z}$ och $\frac{b}{d} = \ell \in \mathbb{Z}$. Nu

$$\frac{an + bm}{d} = \frac{dkn + d\ell m}{d} = kn + \ell m \in \mathbb{Z}$$

□

Vi säger att ett positivt helt tal $p > 1$ är *ett primtal* om alla positiva delare till p är 1 och p själv.

De första primtalen är $2, 3, 5, 7, 11, \ldots$

Det är lätt att visa med induktion att det finns primtalsdelare till varje helt tal $n > 1$,

Det finns verkligen många bevis till den nästa satsen:

Sats 3. *Det finns oändligt många primtal.*

Bevis. Anta att satsen är fel, och att det bara finns ändligt många primtal. Låt de vara $q_1, q_2, \ldots, q_n$ Betrakta talet $m = q_1 q_2 \cdots q_n + 1$. Nu $q_1, q_2, \ldots, q_n < m$, och därför $m \neq q_1, q_2, \ldots, q_n$, så talet m inte är ett primtal. Där måste vara ett primtal q_k som är delare till m. Nu $q_k \mid m$ och $q_k \mid q_1 q_2 \cdots g_n$, och därför $q_k \mid (m - q_1 q_2 \cdots q_n) = 1$. Stämmer inte. Det finns oändligt månda primtal. □

2.2.1 Primfaktorer och unik primtalsfaktorisering

Definition 4. Talet p kallas *en primfaktor* till n om talet p är ett primtal och $p \mid n$.

Primfaktorer till 30 är 2, 3 och 5.

Egentligen kan vi inte visa nästa satsen just nu (den låter lätt men den är egentligen inte trivial), men vi kan visa den senare.

Sats 5 (Primtalsfaktorisering är unik)**.** *Positiv tal n kan skrivas bara på ett sett som en produkt*

$$p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

när vi antar att $\alpha_1, \alpha_2, \ldots, \alpha_k > 0$ (hela tal) och tal p_j är primtal med $p_j < p_\ell$, när $j < \ell$.

Det är ganska lätt att hitta en exempel med två olika primtalsfaktoriseringar: Trakta hela tal n med $n = 4k + 1$. Vi säger att ett tal p är ett primtal om p inte har delare i $\{5, 9, \ldots\}$. De första primtalen är sen $5, 9, 13, 17, 21, 29, \ldots$. Nu har vi

$$441 = 9 \times 49 = 21^2,$$

eftersom $9, 21, 49$ inte har delare i $\{4k + 1 : k \geq 1\}$.

2.3 Erastosthenes såll

Ett intressant problem är att hitta primtal. Det är ganska långsamt att besluta om ett tal n är primtal eller inte. En möjlighet är att kolla om något $1 < d < n$ är delare till n. (Egentligen det räcker att kolla bara $d \leq \sqrt{n}$. Dvs, talet n är ett primtal om och bara om

$$\frac{n}{d} \notin \mathbb{Z} \; \forall d \in \mathbb{Z}, \; 1 < d < n.$$

Det finns bättre sätt att kolla om talet n är primtal, även en algoritm som fungerar i polynomial tid (dessa algoritmer kan betraktas i projektarbet 2).

Nu vill vi hitta alla primtal i $\{2, 3, \ldots n\}$. En bra metod är att använda Erastosthenes såll:

1. Skriv en tabell av tal $\{2, 3, \ldots n\}$.

2. 2 är ett primtal, så ta borta varje tal som är större än två, men delbar med två.

3. 3 är det nästa talet i tabellen (som har inte tagits borta), och därför det är ett primtal. Ta borta varje tal som är större än 3, men delbar med 3.

4. 5 är det nästa kvar liggande talet i tabellen, och därför måste det vara ett primtal. Ta borta varje tal som är större än 5 men delbar med 5.

5. Fortsätta till $\sqrt{n}$ (eftersom varje tal som inte är ett primtal måste vara delbar med ett tal $\leq \sqrt{n}$.

Exempel 6. Hitta alla primatal mellan 2 och 40.
Lösning: Skriv en tabell:

2	3	4	5	6	7	8	9	10	11
12	13	14	15	16	17	18	19	20	21
22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	

Talet 2 är ett primtal. Ta borta varje tal som är delbar med två och större än två:

2	3	$\not{4}$	5	$\not{6}$	7	$\not{8}$	9	$\not{10}$	11
$\not{12}$	13	$\not{14}$	15	$\not{16}$	17	$\not{18}$	19	$\not{20}$	21
$\not{22}$	23	$\not{24}$	25	$\not{26}$	27	$\not{28}$	29	$\not{30}$	31
$\not{32}$	33	$\not{34}$	35	$\not{36}$	37	$\not{38}$	39	$\not{40}$	

Talet 3 är det nästa som ligger kvar. Därför måste det vara ett primtal. Ta borta varje tal som är delbar med tre och större än tre:

2	3	$\not{4}$	5	$\not{6}$	7	$\not{8}$	$\not{9}$	$\not{10}$	11
$\not{12}$	13	$\not{14}$	$\not{15}$	$\not{16}$	17	$\not{18}$	19	$\not{20}$	$\not{21}$
$\not{22}$	23	$\not{24}$	25	$\not{26}$	$\not{27}$	$\not{28}$	29	$\not{30}$	31
$\not{32}$	$\not{33}$	$\not{34}$	35	$\not{36}$	37	$\not{38}$	$\not{39}$	$\not{40}$	

Talet 5 är det nästa som ligger kvar. Därför måste det vara ett primtal. Ta borta varje tal som är delbar med fem och större än fem:

2	3	$\not{4}$	5	$\not{6}$	7	$\not{8}$	$\not{9}$	$\not{10}$	11
$\not{12}$	13	$\not{14}$	$\not{15}$	$\not{16}$	17	$\not{18}$	19	$\not{20}$	$\not{21}$
$\not{22}$	23	$\not{24}$	$\not{25}$	$\not{26}$	$\not{27}$	$\not{28}$	29	$\not{30}$	31
$\not{32}$	$\not{33}$	$\not{34}$	$\not{35}$	$\not{36}$	37	$\not{38}$	$\not{39}$	$\not{40}$	

Talet 7 är det nästa som ligger kvar, men $7 > 6,3 \approx \sqrt{40}$, så varje tal i $\{2, 3, \ldots, 40\}$ som inte är ett primtal måste ha ett primfaktor som är mindre än sju. Därför måste varje tal som ligger kvar vara ett primtal. Primtalen i $\{2, 3, \ldots, 40\}$ är $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37$.

2.3.1 Mersenneprimtal och GIMPS

Ett primtal som kan skrivas som

$$2^b - 1$$

kallas ett mersenneprimtal. Det är lätt att se att talet b måste också vara ett primtal. (Varför?) Vi skriver

$$M(p) = 2^p - 1.$$

Inte alla sådana tal är primtal, till exempel

$$M(11) = 2^{11} - 1 = 2047 = 23 \cdot 89.$$

I nätet finns GIMPS projektet (Great Internet Mersenne Prime Search):

`http://www.mersenne.org/`

I projektet försöks att betrakta stora mersennetal och besluta om de är primtal eller inte.

Vi vet bara 47 mersenneprimtal. Naturligtvis är tre det minst av dem. Det största hittat mersenneprimtal är $M(43112609)$ med 12978189 siffror!

Vi vet inte om det finns oändligt många mersenneprimtal. Troligen oändligt många...

2.4 Primtalsfördelning

2.4.1 Bertrands postulat

Primtalsfördelning har altid fascinerat människor. Hur nära till varandra måste eller kan två primtal vara?

Enligt primtalstvillingkonjektur finns det oändligt många primtal p och q med $p-q = 2$. Ingen har bevisat konjekturen. Ett annat problem: hur stort avstånd mellan två konsekutiva primtal är möjligt? Till exemples, är det möjligt att om p är ett primtal, sen det finns inga primtal som är mindre än $p + 3p$? Svaret är nej. Nästa satsen kallas Bertrands postulat, och den ger oss ett enkelt svar:

Sats 7. *Låt $n \geq 2$. Det finns alltid ett primtal mella n och $2n$.*

Beviset är en del av extra räkneövningarna för de som vill delta i kursen som en del av fördjupade studier.

2.4.2 Primtalssats

Primtalssats bevisades av Hadamard och de la Vallée Poussin oberoende av varandra i 1896. Enligt primtalssatsen är antalet primtal mindre än n ungefär $\frac{n}{\log n}$.

En intressant detalj i historia är Riemanns idee hur primtalssatsen kunde bevisas: Han tänkte att som en lemma borde man visa att funktionen

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s},$$

har alla sina icke-triviala nollställen på $\Re s = \frac{1}{2}$. Troligen har han rätt. Det här påståendet kallas Riemanns hypotes och det är kanske det mest berömdt öppet problemet inom matematik. Om man kunde visa Riemanns hypotes, kunde man också få en bättre approximation för antalet primtal.

2.5 Olika delarfunktioner

Det finns massor av olika funktioner som handlar om delare till tal. Vi skall betrakta två enkla funktioner:

$$\tau(n) = \sum_{d|n, d>0} 1$$

och

$$\sigma(n) = \sum_{d|n, d>0} d.$$

Det är lätt att se att om

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

sedan har vi

$$\tau(n) = \prod_{j=1}^{k} (\alpha_j + 1)$$

och

$$\sigma(n) = \prod_{j=1}^{k} \frac{p_j^{\alpha_j+1} - 1}{p_j - 1}.$$

2.5.1 Perfekta tal

Talet n kallas *ett perfekt tal* om summan av alla positiva delare till n är $2n$. Till exempel talet 6 är ett perfekt tal, eftersom delare till talet 6 är$1, 2, 3, 6$, och deras summa $1 + 2 + 3 + 6 = 12 = 2 \cdot 6$. Åt annat hand, inte alla tal är perfekta. Till exempel, positiva delare till talet 7 är 1 och 7, och deras summa $1 + 7 = 8 \neq 14 = 2 \cdot 7$, så talet 7 inte är perfekt.

I räkneövningarna skall vi visa att varje mersenneprimtal ger oss ett perfekt tal. Egentligen finns det inte andra jämna perfekta tal. Om och bara om det finns oändligt många mersenneprimtal, sen finns det också oändligt många jämna perfekta tal. Vi vet inte om det finns udda perfekta tal, men troligen inte.

Kapitel 3

Linjära diofantiska ekvationer

I detta kapitel betraktas linjärä diofantiska ekvationer, dvs. vi vill lösa ekvationer av typ

$$ax + by = c,$$

i hela tal.

3.1 Största gemensamma delare

Vi börjar med en definition

Definition 8. Låt a och b vara positiva hela tal. Den största gemensamma delare (sgd) till a och b är det största positiva talet $d \in \mathbb{Z}$, som delar både a och b.

Följande sats gör det enklare att beräkna det största gemensamma delare:

Sats 9. *Vi har sgd*(a, b) =*sgd*$(a - b, b)$.

Bevis. Om $d \mid a$ och $d \mid b$, sedan har vi också $d \mid (a - b)$. Därför måste $d \mid \text{syt}(a - b, b)$, dvs $\text{sgd}(a, b) \mid \text{syt}(a-b, b)$. Åt annat hand, om $d' \mid a-b$ och $d' \mid b$, sedan har vi $d' \mid (a-b)+b = a$, och därför$(a - b, b) \mid \text{sgd}(a, b)$. Beviset är färdigt. □

3.2 Euklides algoritm

Euklides algoritm än verkligen effekt metod att beräkna den största gemensamma delaren av talen a och b.

Gör så här:

Anta att $a > b$. Skriv $a = bq_1 + r_1$, med$0 \leq r_1 < b$. Om $r_1 = 0$, är vi färdiga (sen $b \mid a$, och därör $\text{sgd}(a, b) = b$). Om $r_1 \neq 0$, skriv $b = r_1q_2 + r_2$, med $0 \leq r_2 < r_1$. Om $r_2 = 0$, är vi färdiga. Om $r_2 \neq 0$, fortsätt genom att skriva $r_1 = r_2q_3 + r_3$, med $0 \leq r_3 < r_2$, och så vidare tills $r_k = 0$ för något k. Sedan har vi $(a, b) = r_{k-1}$.

Varför fungerar algoritmen: $\text{sgd}(a,b) = \text{sgd}(a-b,b) = \text{sgd}(a-2b-b) = \cdots = \text{sgd}(a-q_1 b, b) = \text{sgd}(r_1, b)$. Åt annat hand, $\text{sgd}(r_1, b) = \text{sgd}(r_1, r_2)$. Fortsätt som det här, och få $\text{syt}(a,b) = \text{syt}(r_{k-1}, r_{k-2}) = r_{k-1}$. Algoritmen stoppar när $r_k = 0$, dvs, när $r_{k-1} \mid r_{k-2}$, och därför $\text{sgd}(r_{k-1}, r_{k-2}) = r_{k-1}$.

Exempel 10. Betrakta talen 56 och 44, och beräkna deras största gemensamma delare:

$$56 = 1 \cdot 44 + 12,$$

och därför måste vara $\text{sgd}(56, 44) = \text{sgd}(44, 12)$. Vi har också de följande

$$\begin{aligned} 44 &= 3 \cdot 12 + 8 \\ 12 &= 1 \cdot 8 + 4 \\ 8 &= 2 \cdot 4 + 0, \end{aligned}$$

och därför måste vara $\text{sgd}(56, 44) = 4$.

3.3 Linjära diofantiska ekvationer

Vi vill börja med att visa att ekvationen $ax + by = c$ inte alltid har heltalslösningar.

Sats 11. *Om $\text{sgd}(a,b) \nmid c$, har diofantiska ekvationen*

$$ax + by = c$$

inga lösningar.

Bevis. Nu $\text{sgd}(a,b) \mid a, b$, dvs $\text{sgd}(a,b) \mid ax + by$ för alla hela talen x ja y. Åt annat hand, talet luku c inte är delbar med $\text{sgd}(a,b)$, och därför är ekvationen inte möjlig. □

Nu vill vi visa att annars har ekvationen alltid en lösning (egentligen oänlidligt många lösningar), och vi konstruerar hur man hittar en.

Sats 12. *Ekvationen $ax + by = \text{syt}(a,b)$ har en lösning.*

Bevis. Anta att $a > b$. Skriv Euklides algoritm för att beräkna den största gemensamma delare till a ja b:

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\cdots \\ r_{k-2} &= q_k r_{k-1} + r_k \\ r_{k-1} &= q_{k+1} r_k, \end{aligned}$$

och nu $\text{sgd}(a,b) = r_k$. Lös kvoten i ekvationer:

$$\begin{aligned} r_1 &= a - q_1 b \\ r_2 &= b - q_2 r_1 \\ r_3 &= r_1 - q_3 r_2 \\ &\dots \\ r_{k-1} &= r_{k-3} - q_{k-1} r_{k-2} \\ r_k &= r_{k-2} - q_k r_{k-1}. \end{aligned}$$

Den sista ekvationen presenterar talet r_k med hjälp av talen r_{k-1} och r_{k-2}. Den andra sista ekvationen presenterar talet r_{k-1} med hjälp av talen r_{k-2} och r_{k-3}. I allmänhet är ekvationen av form $r_j = r_{j-2} - q_j r_{j-1}$. Stoppa in formeln för r_{k-1} i den sista ekvationen:

$$r_k = r_{k-2} - q_k r_{k-1} = r_{k-2} - q_k \left(r_{k-3} - q_{k-1} r_{k-2}\right) = (1 + q_k q_{k-1}) r_{k-2} - q_{k-1} r_{k-3}$$

Stoppa in formeln $r_{k-2} = r_{k-4} - q_{k-2} r_{k-3}$:

$$\begin{aligned} r_k = (1 + q_k q_{k-1}) r_{k-2} - q_{k-1} r_{k-3} &= (1 + q_k q_{k-1})(r_{k-4} - q_{k-2} r_{k-3}) - q_{k-1} r_{k-3} \\ &= (1 + q_k q_{k-1}) r_{k-4} - (q_{k-2} + q_k q_{k-1} q_{k-2} - q_{k-1}) r_{k-3}, \end{aligned}$$

och nu det samma för talet r_{k-3}, sedan för talet r_{k-4}, osv, tills vi har en formel av typ

$$r_k = a c_1 + b c_2$$

för $r_k = \text{sgd}(a,b)$ med c_1 ja c_2 beroende av talen q_j. Beviset är färdigt. En lösning är talen c_1 och c_2. □

Sats 13. *Om $sgd(a,b) \mid c$, har ekvationen $ax + by = c$ en lösning.*

Bevis. Om $\text{sgd}(a,b) = c$, har vi redan hittat en lösning. Anta att $c = d\text{sgd}(a,b)$. Låt (x_0, y_0) vara en lösning till ekvationen $ax + by = \text{sgd}(a,b)$. Nu är (dx_0, dy_0) en lösning till ekvationen $ax + by = c$ eftersom $adx_0 + bdy_0 = d\text{syt}(a,b) = c$. □

Sats 14. *Alla lösningar till homogeniska ekvationen $ax + by = 0$ ges av $x = \frac{b}{sgd(a,b))}k$ och $y = -\frac{a}{sgd(a,b))}k$.*

Bevis. Betrakta ekvationen $ax + by = 0$. Nu $ax = -by$, dvs $\frac{a}{\text{sgd}(a,b)}x = -\frac{b}{\text{sgd}(a,b)}y$. Eftersom $\text{sgd}(\frac{a}{\text{sgd}(a.b)}, \frac{b}{\text{sgd}(a,b)}) = 1$, har vi (använda Lemman 17 för primtalsfaktoriseringen) $\frac{b}{\text{sgd}(a.b)} \mid x$ och $\frac{a}{\text{sgd}(a.b)} \mid y$. Skriv $x = \frac{b}{\text{sgd}(a.b)}x'$ och $y = \frac{a}{\text{sgd}(a.b)}y'$ att få $\frac{a}{\text{sgd}(a,b)} \cdot \frac{b}{\text{sgd}(a,b)}x' = -\frac{b}{\text{sgd}(a,b)} \cdot \frac{a}{\text{sgd}(a,b)}y'$, och nu $x' = -y'$. Parametrisera $x' = -y' = k$, och nu är lösningarna $(\frac{b}{\text{syt}(a,b))}k, -\frac{a}{\text{syt}(a,b)}k)$. □

Sats 15. *Om diofantiska ekvationen $ax + by = c$ har en lösning (x_0, y_0), sen har den oändligt många lösningar, och de ges av $\left(x_0 + (\frac{b}{syt(a,b))}k, y_0 - \frac{a}{syt(a,b)}k\right)$ med k heltal.*

Bevis. Låt (x_1, y_1) och (x_2, y_2) vara lösningar till ekvationen $ax + by = c$. Nu $a(x_1 - x_2) + b(y_1 - y_2) = 0$, och därför måste $(x_1 - x_2, y_1 - y_2)$ vara en lösning till homogeniska ekvationen $ax + by = 0$. Beviset är färdigt. □

Exempel 16. Lös diofantiska ekvationen $44x + 56y = 4$. Vi har tidigare beräknat $\text{sgd}(56, 44)$. Vi skriver den igen:

$$\begin{aligned} 12 &= 56 - 1 \cdot 44 \\ 8 &= 44 - 3 \cdot 12 \\ 4 &= 12 - 1 \cdot 8. \end{aligned}$$

Nu måste vi stoppa in:

$$4 = 12 - 8 = 12 - (44 - 3 \cdot 12) = 4 \cdot 12 - 44 = 4(56 - 44) - 44 = 4 \cdot 56 - 5 \cdot 44.$$

En lösning är därför $x = -5$ och $y = 4$. Homogeniska ekvationen $44x + 56y = 0$ har lösningarna $x = 14k$ och $y = -11k$. Alla lösningarna till ekvationen $44x + 56y = 4$ är därför $x = -5 + 14k$ och $y = 4 - 11k$.

3.4 Varför primtalsfaktoriseringen är unik

Vi behöver den följande lemman för att bevisa att primtalsfaktorisering är unik:

Lemma 17. *Låt p vara ett primtal. Om $p \mid ab$, och $p \nmid b$, sedan $p \mid a$.*

Bevis. Eftersom p är ett primtal och $p \nmid b$, vi måste ha $\text{sgd}(p, b) = 1$. Nu finns det x och y, med $px + by = 1$. Eftersom $p \mid ab$, har vi $p \mid aby$, dvs $p \mid a(1 - px)$. Eftersom $p \mid apx$, gäller det $p \mid apx + a(1 - px) = a$. Beviset är färdigt. □

Nu är det lätt att visa att primtalsfaktorisering är unik. Anta att satsen inte var sann: Talet n har två olika primtalsfaktoriseringar, dvs, vi har

$$p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = q_1^{\beta_1} q_2^{\beta_2} \cdots q_\ell^{\beta_\ell}.$$

Vi kan nu anta att $p_j \neq q_i$ för alla i, j.

Nu $p_1 \mid q_1^{\beta_1} q_2^{\beta_2} \cdots q_\ell^{\beta_\ell}$. Eftersom $p_1 \neq q_1, q_2, \ldots, q_\ell$, gäller det $p_1 \nmid q_1^{\beta_1}, q_2^{\beta_2}, \ldots, q_\ell^{\beta_\ell}$. Eftersom $p_1 \nmid q_1^{\beta_1}$, har vi $p_1 \mid q_2^{\beta_2} q_3^{\beta_3} \cdots q_\ell^{\beta_\ell}$. Men nu $p_1 \nmid q_2^{\beta_2}$, så det måste gälla att $p_1 \mid q_3^{\beta_3} q_4^{\beta_4} \cdots q_\ell^{\beta_\ell}$. Vi kan fortsätta på det samma sätt, och på slutet har vi $p_1 \mid q_\ell^{\beta_\ell}$, som kan inte vara sant. Nu har visat att primtalsfaktorisering måste vara unik.

Kapitel 4

Kongruenser

Vi säger att talen a och b är kongruenta modulo n om

$$n \mid (a - b).$$

Vi skriver

$$a \equiv b \pmod{n}.$$

Således $a - b = kn$ med k något helt tal. Om $n \nmid (a - b)$, skriver vi

$$a \not\equiv b \pmod{n}.$$

Till exempel, $3 \equiv 7 \pmod{4}$ och $105 \equiv 55 \pmod{25}$.

Sats 18. *Följdande gäller: Om*

$$a \equiv b \pmod{n} \quad ja \quad c \equiv d \pmod{n},$$

sedan har vi

$$a \pm c \equiv b \pm d \pmod{n} \quad ja \quad ac \equiv bd \pmod{n}.$$

Bevis. Vi har $n \mid (a-b)$ och $n \mid (c-d)$, och därför $n \mid ((a-b)+(c-d)) = (a+c)-(b+d)$ och $n \mid (a-b)-(c-d) = ((a-c)-(b-d))$. Första två påståenden är nu bevisad.

Nu den sista: Eftersom $n \mid a - b$ och $n \mid c - d$, har vi

$$n \mid (c(a-b) + b(c-d)) = ac - bd.$$

□

Som en korollar har vi följande satsen

Sats 19. *Om* $a \equiv b \pmod{n}$*, sedan gäller också* $a^m \equiv b^m \pmod{n}$ *för alla icke-negativa hela talen* m*.*

Det är märkvärdigt att det inte är så lätt att dela kongruenser med något helt tal. Ta en exempel. Ekvationen

$$2 \equiv 6 \pmod 4$$

gäller, men om vi delar ekvationen med talet 2, får vi $1 \equiv 3 \pmod 4$ som inte är sann. Orsaken är att $\text{sgd}(2,4) > 1$ (2: delare, 4: modulo). Om vi delade modulon med två, också, vore allt finnt. Åt annat hand, om vi vill dela ekvationen $2 \equiv 6 \pmod 4$ med tre, till exempel, är det kanske inte hellt klar vad man borde göra. Det är bäst att tänka att att dela är att multiplicera med inversen. Följande metoden fungerar bra:

För att dela ekvationen $a \equiv b \pmod n$ med talet d, multiplicera ekvationen med inversen till d, dvs, med ett sådant tal d', att

$$dd' \equiv 1 (\text{mod } n).$$

Nu $n \mid dd' - 1$, och därför $dd' - 1 = xn$, alltså $dd' - xn = 1$. Den här är en linjär diofantisk ekvation. Lösningarna till ekvationen är talen $d' = d_0 + nk$ och $x = x_0 + dk$, där (d_0, x_0) är en lösning. Vi har $d' \equiv d_0 \pmod n$, och därför gäller det att att dela ekvationen med d är det samma som att multiplicera ekvationen med d_0.

I synnerhet har vi att om $da \equiv db \pmod n$ med $\text{sgd}(n,d) = 1$, sedan gäller också $a \equiv b \pmod n$.

Mängden $\{a_1, a_2, \ldots a_n\}$ är ett *fullständigt restsystem* modulo n, om $a_j \not\equiv a_i \pmod n$, när $n \neq j$. Till exempel, mängden $\{0, 1, 2, \ldots, n-1\}$ är ett fullständigt restsystem modulo n. Om mängden $\{a_1, a_2, \ldots, a_n\}$ är ett fullständigt restsystem, sen mängden

$$\{a_1, a_2, \ldots, a_n\} \setminus \{a_j : \text{sgd}(a_j, n) > 1\}$$

kallas ett *reducerat restsystem.*

Exempel 20. Mängden $\{3, 4, 5, 6, 7\}$ är ett fullständigt restsystem modulo 5. Också mängden $\{100, 101, 102, 103, 104\}$ är ett fullständigt restsystem modulo 5. Mängden $\{3, 4, 6, 7\}$ är ett reducerat restsystem modulo 5.

Exempel 21. Vi vill visa att talet n är delbar med 9 om och bara om summan av siffrorna till n är delbar med 9.

Vi kan skriva talet n som

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots a_1 10 + a_0.$$

Nu $10 \equiv 1 \pmod 9$, joten $10^k \equiv 1^k \equiv 1 \pmod 9$. Därför

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots a_1 10 + a_0 \equiv a_k + a_{k-1} + \cdots + a_1 + a_0 \pmod 9.$$

4.1 Fermats lilla sats och Eulers sats

Beräkning av kongruenser blir mycket lättare med hjälp av Fermats lilla sats och Eulers sats.

Sats 22 (Fermats lilla sats)**.** *Låt p vara ett primtal och sgd$(a,p)=1$. Nu*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Bevis. Mängden $\{a, 2a, 3a, \ldots, (p-1)a\}$ är ett reducerat restsystem modulo p, eftersom om $aj \equiv ak \pmod{p}$, sedan $j \equiv k \pmod{p}$, alltså $j = k$, eftersom $0 < j, k \leq p-1$, och $\text{sgd}(p, aj) = 1$. Därför

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1),$$

(reducerade restsystem på bägge sidor). Därför

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

Den här ekvationen kan delas med $(p-1)!$, eftersom $\text{sgd}((p-1)!, p) = 1$, och nu

$$a^{p-1} \equiv 1 \pmod{p}.$$

□

Exempel 23. Vi vill visa att $7 \mid 5^{600} - 1$. Nu $\text{sgd}(7,5) = 1$. Eftersom

$$5^6 \equiv 1 \pmod{7},$$

gäller också

$$5^{600} = \left(5^6\right)^{100} \equiv 1^{100} = 1 \pmod{7}.$$

Därför $5^{600} - 1 \equiv 0 \pmod{7}$, dvs $7 \mid 5^{600} - 1$.

4.1.1 Eulers φ-funktion och Eulers sats

Eulers φ-funktion innehåller information antalet talen mindre än n med största gemensamma delare med n lika till 1:

$$\varphi(n) = \left|\{1 \leq m \leq n : \ \text{syt}(n,m) = 1\}\right|.$$

Till exempel $\varphi(8) = 4$ och $\varphi(30) = 8$.

Om $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ (primtalsfaktorisering till n), har vi

$$\varphi(n) = \prod_{j=1}^{k} p_j^{\alpha_j}(p_j - 1).$$

Beviset finns i räkneövningarna.

Eulers sats är en generalisering av Fermats lilla sats, och beviset är lika.

Sats 24. *Låt sgs$(a,n)=1$. Nu*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

4.2 Kongruensekvationer

En ekvation av typ

$$P \equiv Q \pmod{n}$$

där P och Q are några formuler kallas en *kongruensekvation*. Till exempel, ekvationen

$$m^2 \equiv 1 \pmod{8}$$

är en kongruensekvation. Alla udda m ($m \equiv 1 \pmod{2}$ är lösningar till ekvationen, alltså $m \equiv 1, 3, 5, 7 \pmod{8}$ (se första räkneövningarna).

En annan exempel är en linjär kongruensekvation i en variabel, till exempel

$$4x + 3 \equiv 5 \pmod{7}.$$

Nu $4x \equiv 2$ (mod7). Det är möjligt att gissa lösningarna eftersom modulon är liten, men en bättre metod att lösa ekvationen är att först byta ekvationen till en diofantisk ekvation:

$$4x + 7y = 2.$$

Lösningarna till ekvationen är $x = 4 + 7k$ och $y = -2 - 4k$. Alltså $x \equiv 4 \pmod{7}$.

Naturligtvis är det möjligt att betrakta kongruensekvationer i flera variabel, också. Till exempel, ekvationen

$$x^2 + y^2 \equiv 3 \pmod{4}$$

har inga lösningar, eftersom jämna kvadrater är delbar med fyra, dvs $\equiv 0 \pmod{4}$ och udda kvadrater är $\equiv 1 \pmod{4}$.

Linjära kongruensekvationer i en variabel är de viktigaste kongruensekvationerna på denna kursen. De är lätt att lösa. Låt $\text{sgs}(a, n) = 1$. Betrakta ekvationen

$$ax + b \equiv c \pmod{n}.$$

Gör så här:

1. Talet b till andra sidan av ekvationen: $ax \equiv c - b \pmod{n}$
2. Beräkna inversen till a modulo n genom att hitta en lösning till den diofantiska ekvationen $ax - ny = 1$. Låt lösningen vara (a', n')
3. Multiplicera ekvationen med talet a'. Nu

$$x \equiv a'(c - b) \pmod{n}.$$

Det finns olika möjligheter att lösa en kongruensekvation. I metoden ovanför är det möjligt att gissa en lösning till den diofantiska ekvationen eller att lösa ekvationen $ax - nu = c - b$ istället för 2) och 3).

4.3 Kinesiska restklassatsen

Enligt den kinesiska restklassatsen finns det en lösning till den följande system av kongruenekvationer:

Sats 25. *Låt talen $m_1, m_2, \ldots, m_k$ vara sådana att sgd$(m_i, m_j) = 1$ när $i \neq j$. Nu har systemet*

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \cdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

en unik lösning i modulo $M = m_1 m_2 \cdots m_k$.

Bevis. I räkneövningarna visar vi att

$$x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots a_k M_k y_k \pmod{M}$$

är en lösning med följande antagnigar: $M_j = \frac{M}{m_j}$. Nu sgd$(m_j, M_j) = 1$, och därför har talet M_j en invers modulo m_j, säg y_j, alltså $M_j y_j \equiv 1 \pmod{m_j}$.

Vi vill nu visa att lösningen är unik. Anta att x_0 ja x_1 är lösningar till ekvationerna. Nu $x_0 - x_1 \equiv 0 \pmod{m_1}$, $x_0 - x_1 \equiv 0 \pmod{m_2}$, osv, och därför $m_1 \mid x_0 - x_1$, $m_2 \mid x_0 - x_1$, osv, alltså $M \mid x_0 - x_1$ (eftersom sgd$(m_i, m_j) = 1$ nät $i \neq j$). □

I praktik är följande metoden verkligen bra. Vi tar en exempel.

Exempel 26. Lös system av kongurensekvationerna

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases}$$

Vi börjar med den första ekvationen. Eftersom $x \equiv 2 \pmod{5}$, har vi $x = 5y + 2$. Stoppa in i den andra ekvationen:

$$5y + 2 \equiv 3 (\text{mod } 7),$$

alltså $5y \equiv 1$ (mod 7). Vi behöver nu lösa den diofantiska ekvationen $5y+7t = 1$. Lösningar till ekvationen är $y = 3+7k$ ja $t = -2-5k$. Stoppa in formeln $y = 3+7k$ i formeln $x = 5y+2$:

$$x = 5y + 2 = 5(3 + 7k) + 2 = 15 + 35k + 2 = 35k + 17 \equiv 17 \pmod{35},$$

och därför är lösningen $x \equiv 17 \pmod{35}$.

Kapitel 5

Primitiva rötter

I detta kapitlet är p ett primtal.

Enligt Fermats lilla sats gäller

$$a^{p-1} \equiv 1 \pmod{p},$$

när p är ett primtal och $\text{sgd}(a, p) = 1$. En annan fråga är: När gäller $a^s \not\equiv 1 \pmod{p}$ för varje positivt heltal $s < p - 1$. Vi kan definera

Definition 27. En primitiv rot modulo p, med p primtal är ett sådant tal g, att $\text{sgd}(p, g) = 1$ och $g^s \not\equiv 1 \pmod{p}$, när $1 \leq s < p - 1$.

Till exempel, talet 2 är en primitiv rot modulo 5, eftersom $2^1 \equiv 2 \pmod{5}$, $2^2 \equiv 4 \pmod{5}$ och $2^3 \equiv 3 \pmod{5}$.

Primitiva rötter är intressanta, till exempel eftersom det är möjligt att använda de för att presentera det reducerade restsystemet:

Sats 28. *Låt g en primitiv rot modulo p. Nu är mängden $\{g^0, g^1, g^2, \ldots, g^{p-2}\}$ ett reducerat restsystem modulo p.*

Bevis. Ett reducerat restsystem modulo p har $p-1$ tal, eftersom den enda restklassen som inte finns i det reducerade restsystem är den restklassen som innehåller talet 0.

Antalet talen $g^0, g^1, g^2, \ldots, d^{p-2}$ är $p - 1$, så det räcker att visa att inga två tal är kongruenta med varandra modulo p. Om nu

$$g^s \equiv g^r,$$

när $s > r$, då gäller $g^{s-r} \equiv 1 \pmod{p}$. Vi antog att talet g är en primitiv rot, och eftersom $s-r$ är positivt, vi måste ha $s-r \geq p-1$. Det här kan inte vara sant. Beviset är färdigt. □

Nästa satsen är jätteviktig, men att visa den krävs några hjälpsatser. Vi skall först presentera satsen, sen hjälpsatsen, och på slutet satsens bevis.

Sats 29. *Varje primtal har minst en primitiv rot.*

5.1 Hjälpsatser om polynom

Vi skall visa att vi kan operera likadant med polynom modulo p som med polynom i $\mathbb{R}$. (Kom ihåg att talet p är ett primtal!)

Sats 30 (Lagrange sats)**.** *Polynom av grad n har högst n icke-kongruenta rötter modulo p.*

Bevis. Vi använder induktion.:

1. Polynomet $ax + b$ har högst en rot modulo p: $x \equiv -ba^{-1} \pmod{p}$.

2. Vi antar att ett polynom av grad $k-1$ har högst $k-1$ icke-kongruenta rötter.

3. Betrakta polynomet $f(x) = a_k x^k + a_{k-1}x^{k-1} + \cdots + a_1 x + a_0$ av grad k. Anta att polynomet har $k+1$ icke-kongruenta rötter, och låt de vara $c_0, c_1, \ldots, c_k$. Nu

$$f(c_0) - f(x) = a_k c_0^k + a_{k-1}c_0^{k-1} + \cdots + a_1 c_0 + a_0 - a_k x^k - a_{k-1}x^{k-1} - \cdots - a_1 x - a_0 = \\ a_k(c_0^k - x^k) + a_{k-1}(c_0^{k-1} - x^{k-1}) + \cdots + a_1(c_0 - x) = (c_0 - x)g(x),$$

   där g är ett polynom av grad $k-1$. Vi vill nu visa att talen $c_1, c_2, \ldots, c_k$ måste vara rötter till polynomet $g(x)$. Vi har

$$f(c_0) - f(c_j) \equiv 0 \pmod{p},$$

   och därför måste talen c_j vara rötter till polynomet $f(c_0) - f(x)$. Nu

$$f(c_0) - f(c_j) = (c_0 - c_j)g(c_j) \equiv 0 \pmod{p}.$$

   Eftersom talen c_j och c_0 är inte kongruenta modulo p, gäller $\text{sgd}(p, c_0 - c_j) = 1$, och därför $p \mid g(c_j)$ för alla $1 \leq j \leq k$. Det kan inte vara. Beviset är färdigt.

□

Sats 31. *Om $d \mid p-1$, har polynomet $x^d - 1$ exakt d icke-kongruenta rötter modulo p.*

Bevis. Enligt Fermats lilla sats har polynomet $x^{p-1} - 1$ $p-1$ icke-kongruenta rötter modulo p. Skriv $p - 1 = rd$. Nu

$$x^{p-1} - 1 = (x^d - 1)(x^{(r-1)d} + x^{(r-2)d} + \cdots + x^d + 1).$$

Eftersom polynomet $x^{(r-1)d} + x^{(r-2)d} + \cdots x^d + 1$ har högst $(r-1)d$ icke-kongruenta rötter måste polynomet $x^d - 1$ ha d icke-kongruenta rötter. □

5.2 Hjälpsatser om Eulers φ-funktion

Eulers φ-funktion har följande definition

$$\varphi(n) = |\{1 \leq m \leq n : \text{ syt}(n, m) = 1\}|.$$

Obs! Den tidigare versionen av kompendiet hade mindre än talet $n$och inte "inte större än talet n". Orsaken är att med "inte större än n"är det lättare att dela med multiplikation: Nu är $\varphi(1) = 1$, och inte 0. Allt annat stannat det samma.

Om $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ (primtalsfaktorisering till talet n), då

$$\varphi(n) = \prod_{j=1}^{k} p_j^{\alpha_j - 1}(p_j - 1).$$

Nu är det klart att funktionen φ är multiplikativ, alltså om $\text{sgd}(n, m) = 1$, då

$$\varphi(n)\varphi(m) = \varphi(nm).$$

Vi vill nu visa följande satsen som är verkligen viktig i beviset att det alltid finns minst en primitiv rot:

Sats 32. *Vi har*

$$\sum_{d|n} \varphi(d) = n.$$

Bevis. Först talen $n = 1$ och $n = p^k$, sedan induktion:

Låt $n = 1$. Nu

$$\sum_{d|1} \varphi(d) = 1.$$

Låt $n = p^k$. Nu

$$\sum_{d|p^k} = \varphi(1) + \sum_{1 \leq \ell \leq k} \varphi(p^\ell) = 1 + \sum_{1 \leq \ell \leq k} (p-1)p^{\ell-1} = 1 + (p-1)\frac{p^k - 1}{p - 1} = p^k.$$

Anta nu att

$$\sum_{d|p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}} \varphi(d) = p_1^{\alpha_1} \cdots p_k^{\alpha_k}.$$

Betrakta talet $n = p_1^{\alpha_1} p_2^{/alpha_2} \cdots p_k^{\alpha_k} p_{k+1}^{\alpha_{k+1}}$. Varje delare till n år antingen delare till talet

$p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ eller delbar med p^ℓ för något ℓ. Alltså

$$\sum_{d|p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_{k+1}^{\alpha_k+1}} \varphi(d) = \sum_{0\le\ell\le\alpha_{k+1}} \sum_{d|p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}} \varphi(p^\ell d)$$

$$= \sum_{1\le\ell\le\alpha_{k+1}} \sum_{d|p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}} \varphi(p^\ell d) + \sum_{d|p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}} \varphi(d) = \sum_{1\le\ell\le\alpha_{k+1}} \sum_{d|p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}} \varphi(p^\ell)\varphi(d) + p_1^{\alpha_1}\cdots p_k^{\alpha_k}$$

$$= \sum_{1\le\ell\le\alpha_{k+1}} (p-1)p^{\ell-1}p_1^{\alpha_1}\cdots p_k^{\alpha_k} + p_1^{\alpha_1}\cdots p_k^{\alpha_k} = (p-1)\frac{p^{\alpha_{k+1}}-1}{p-1}p_1^{\alpha_1}\cdots p_k^{\alpha_k} + p_1^{\alpha_1}\cdots p_k^{\alpha_k}$$

$$= p_1^{\alpha_1}\cdots p_k^{\alpha_k}p_{k+1}^{\alpha_{k+1}},$$

och beviset är färdigt. □

5.3 Hjälpsatser om primitiva rötter

Definition 33. Låt *ordningen* hos n modulo p, $\mathrm{ord}_p(n)$ vara följande tal när $\mathrm{sgd}(p,n)=1$:

$$n^{\mathrm{ord}_p(n)} \equiv 1 \pmod{p},$$

och om $s < \mathrm{ord}_p(n)$, då $n^s \not\equiv 1 \pmod p$. Alltså, om talet g är en primitiv rot, gäller $\mathrm{ord}_p(g) = p-1$.

Vi behöver nu några hjälpsatser om ordningar.

Lemma 34. *Gäller*

$$ord_p(n) \mid p-1.$$

Bevis. Låt s vara den minsta ordningen som inte delar talet $p-1$. Skriv delekvationen:

$$p-1 = qs + r,$$

där $0 \le r < s$.Nu $n^r = n^{p-1-qs} \equiv 1 \pmod p$, som kan inte vara sant. □

Lemma 35. *Om $n^s \equiv 1 \pmod p$, då $ord_p(n) \mid s$.*

Bevis. Anta att $\mathrm{ord}_p(n) \nmid s$. Enligt definitionen $\mathrm{ord}_p(n) < s$, så vi kan skriva:

$$s = q\mathrm{ord}_p(n) + r,$$

där $r < \mathrm{ord}_p(n)$. Nu

$$n^r = n^{s-q\mathrm{ord}_p(n)} \equiv 1 \pmod p,$$

vilket kan inte vara sant eftersom enligt ordningens definition borde talet r vara ordningen hos talet n. □

Vi behöver ännu en hjälpsats.

Lemma 36. *Låt $ord_p(n) = s$. Nun ordningen hos talet n^j är $\frac{ord_p(n)}{syt(j, ord_p(n))}$.*

Bevis. Låt $s = \text{ord}_p(n^j)$. Skriv $\text{sgd}(j, \text{ord}_(n)) = d$, $j = j_0 d$ och $\text{ord}_p(n) = kd$, där $\text{sgd}(j, k) = 1$. Nu

$$\left(n^j\right)^{\frac{\text{ord}_p(n)}{\text{sgd}(j,\text{ord}_p(n))}} = n^{j_0 d \frac{\text{ord}_p(n)}{d}} = n^{j_0 \text{ord}_p(n)} \equiv 1 \pmod{p}.$$

Åt annat hand måste vi visa att för inget tal mindre än $\frac{\text{ord}_p(n)}{\text{sgd}(j,\text{ord}_p(n))}$ gäller $(n^j)^s \equiv 1 \pmod{p}$. Nu $s \mid \frac{\text{ord}_p(n)}{\text{sgd}(j,\text{ord}_p(n))}$. Ät annat hand

$$(n^j)^s = n^{js} \equiv 1 \pmod{p},$$

och därför $\text{ord}_(n) \mid js$, dvs $kd \mid j_0 ds$, dvs $k \mid j_0 s$. Eftersom $\text{sgd}(j_0, k) = 1$, gäller $k \mid s$, dvs $\frac{\text{ord}_p(n)}{\text{sgd}(\text{ord}_p(n),j)} \mid s$. □

Nu kan vi fortsätta till beviset.

5.4 Beviset att det alltid finns minst en primitiv rot

I beviset visar vi inte bara att det alltid finns minst en primitiv rot, men vi beräknar antalet primitiva rötter samt antalet tal vilka har varje ordning.

Låt $f(k)$ vara antalet tal i $1, 2, \ldots, p-1$ där $\text{ord}_p(n) = k$, dvs

$$f(k) = \left|\{1 \leq m \leq p-1 : \ \text{ord}_p(m) = k\}\right|.$$

Vi vet att om $k \nmid p-1$, då $f(k) = 0$. Åt annat hand, varje tal i mängden $\{1, 2, \ldots, p-1\}$ måste vara i någon mängd $\{1 \leq m \leq p-1 : \ \text{ord}_p(m) = k\}$. Därför

$$p - 1 = \sum_{1 \leq m \leq p-1} f(k) = \sum_{d \mid p-1} f(d).$$

Betrakta nu talen med ordningen d. Om sådana tal inte finns, gäller $f(d) = 0$. Om sådana tal finns, låt talet a vara sådant.Nu är talet a en rot till polynomet $x^d - 1$. Egentligen är talen $a, a^2, \ldots, a^d$ rötter till polynomet. Vi vet också att polynomet har exakt d rötter som är inte kongruenta med varandra. Talen a^j är inte kongruenta, eftersom om $a^j \equiv a^i \pmod{p}$, då $a^{j-i} \equiv 1 \pmod{p}$, och därför är ordningen hos talet a är högst $|j - i| < p - 1$. Åt annat hand, ordningarna hos alla dessa talen är inte d utan ordningen hos a^j är $\frac{d}{\text{syt}(d,j)}$, dvs, den är d om och endast om $\text{sgd}(j, d) = 1$. Eftersom $1 \leq j \leq d$, finns det $\varphi(d)$ sådana tal. Vi har nu visat att $0 \leq f(d) \leq \varphi(d)$. Nu

$$\sum_{d \mid p-1} f(d) = \sum_{d \mid p-1} \varphi(d),$$

och därför $f(d) = \varphi(d)$, eftersom summorna är lika och $f(d) \leq \varphi(d)$.

5.5 Wilsons sats

Nästa sats kallas Wilsons sats. Det är möjligt att visa satsen med hjälp av primitiva rötter, eller genom polynomens egenskaper. Beviset är en räkneövning.

Sats 37 (Wilsons sats)**.** *Det gäller*

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

Åt annat hand, det är också möjligt att visa att om $(n-1)! \equiv -1 \pmod{n}$, då är n ett primtal. Detta finns också i räkneövningarna.

Kapitel 6

Irrationalitet

Talet a kallas *rationellt* om det är möjligt att skriva

$$a = \frac{r}{s},$$

där r och s är hela tel och $s \neq 0$. Om talet a inte kan presenteras på ett sådant set, kallas a *irrationellt*.

Nästa sats är berömd, och troligaste det lättaste irrationalitetsbeviset.

Sats 38. *Talet $\sqrt{2}$ är irrationellt.*

Bevis. Anta att $\sqrt{2} = \frac{r}{s}$, där talen s och r är positiva och $\text{sgd}(r, s) = 1$.Nu

$$2 = \frac{r^2}{s^2},$$

dvs $2s^2 = r^2$. Alltså $2 \mid r^2$, och därför $2 \mid r$. Skriv $r = 2r_1$. Nu $2s^2 = r^2 = 4r_1^2$, och därför $s^2 = 2r_1^2$, dvs $2 \mid s^2$, alltså $2 \mid s$. Det här kan inte vara sant, eftersom talen r och s inte har gemensamma delare. □

Varför kan man inte visa likadant att talet $\sqrt{4} = 2$ är irrationellt (det säkert är inte)? Vad går fel?

Naturligtvis finns det oändligt många rationella tal. Åt annat hand, det är möjligt att visa att mångden av rationella tal är lika stor som mängden av hela tal:

Sats 39. *Mängden av rationella tal är uppräknelig.*

Bevis. Det räcker att betrakta positiva tal. Låt $\frac{r}{s}$ vara et rationellt tal, och anta att $\text{sgd}(r, s) = 1$. Låt

$$h\left(\frac{r}{s}\right) = r + s.$$

Numerera nu talen i följande stegen:

1. om $h(\alpha) < h(\beta)$, då kommer α förran β.

2. om $h(\alpha) = h(\beta)$, där $\alpha = \frac{r_\alpha}{s_\alpha}$ och $\beta = \frac{r_\beta}{s_\beta}$, då kommer α förran β om och endast om $s_\alpha < s_\beta$.

□

Så, till exempel, $h(1) = h\left(\frac{1}{1}\right) = 2$, och $h(\alpha) > 1$ för alla positiva rationella tal. Också $h(\alpha) > 2$ när $\alpha \neq 1$. Nu $h\left(\frac{r}{s}\right) = 3$ bara om $\frac{r}{s} = \frac{1}{2}$ eller $\frac{r}{s} = \frac{2}{1}$. Eftersom $1 < 2$, kommer $\frac{2}{1}$ förran $\frac{1}{2}$. Vi kan nu fortsätta till $h(\alpha) = 4$. Nu måste vara $\alpha = \frac{3}{1}$ eller $\alpha = \frac{1}{3}$, eftersom $\frac{2}{2}$ är inte möjligt (sgd$(2, 2)$>1). Alltså, början av listan är

$$1 = \frac{1}{2},\ 2 = \frac{2}{1},\ \frac{1}{2},\ 3 = \frac{3}{1},\ \frac{1}{3},\ 4 = \frac{4}{1},\ \frac{3}{2},\ \frac{2}{3}, \ldots$$

6.1 Varför talet e är irrationellt?

Det är ganska lätt att visa att talet e är irrationellt. Säkert är det svårare, än till exempel, att visa att talet $\sqrt{2}$ är irrationellt.

Sats 40. *Talet e är irrationellt.*

Bevis. Anta att vi kan skriva $e = \frac{a}{b}$, där $a, b \in \mathbb{Z}0$, $a, b > 0$ och sgd$(a, b) = 1$. Nu

$$eb = a,$$

och

$$n!eb = n!a$$

för varje $n \in \mathbb{Z}$. Använd formeln

$$e = \sum_{k \geq 0} \frac{1}{k!}.$$

(Taylors formel för e^x där $x = 1$. Nu

$$bn!\left(\left(1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!}\right) + \left(\frac{1}{(n+1)!} + \frac{1}{(n+2)!} + \cdots\right)\right) = n!a.$$

Talet $n!a$ är säkert ett helt tal. Också termen

$$bn!\left(1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!}\right) = b\left(n! + n! + \frac{n!}{2!} + \cdots + 1\right)$$

är heltal. Nu måste termen

$$bn!\left(\frac{1}{(n+1)!} + \frac{1}{(n+2)!} + \cdots\right)$$

vara också ett helt tal. Uppskatta talet:

$$bn!\left(\frac{1}{(n+1)!}+\frac{1}{(n+2)!}+\cdots\right)=b\left(\frac{1}{n+1}+\frac{1}{(n+1)(n+2)}+\cdots\right)$$
$$<b\left(\frac{1}{n+1}+\frac{1}{(n+1)^2}+\frac{1}{(n+1)^3}+\cdots\right)=b\cdot\frac{1}{n+1}\cdot\frac{1}{1-\frac{1}{n+1}}=\frac{b}{n}.$$

Nu vet vi att detta hela talet måste vara mindre än $\frac{b}{n}$, och när $n > b$, betryder det att detta hela talet kan inte vara större än 0.Åt annat hand,

$$bn!\left(\frac{1}{(n+1)!}+\frac{1}{(n+2)!}+\cdots\right)>bn!\cdot\frac{1}{(n+1)!}=\frac{b}{n+1}>0.$$

Nu ser vi att talet är större än 0. Det kan det inte vara, eftersom vi har just visat att talet är inte större än 0. Antagningen var fel, satsen är bevisad. □

6.2 Algebriska talen

Talet kallas *algebraiskt* om det är en rot till ett polynom vars koefficienter är heltal. Till exempel, talet

$$\sqrt{2}$$

är algebraiskt, eftersom det är en rot till polynomet $x^2 - 2$.

Sådana talen som inte är algebraiska, kallas transcendenta. Till exempel, talen π och e är transcendenta.

Typiskt är det inte lätt att ett visst tal är transcendent. Naturligtvis finns det några undantag. Mest av talen är transcendenta: det finns bara uppräkneligt många algebraiska tal.

Typiskt har ett polynom inte en lösningsformel: Galois och Abel har visat att polynom av grad ≥ 5 har ingen lösningsformel.

Kapitel 7

Kryptografi

G. H. Hardy har sagt om talteori:

No one has yet discovered any warlike purpose to be served by the theory of numbers or relativity, and it seems unlikely that anyone will do so for many years."

Ordet kryptografi betyder sådana matematiska metoder som kan används för att göra informationen svårläslig. Många av sådana metoder är byggt på talteori.

7.1 RSA

RSA fungerar bra eftersom det är verkligen svårt och långsamt att hitta faktorer till stora tal. Det är egentligen möjligt att visa att om det är möjligt att bryta RSA, då är det möjligt att hitta faktorer snabbt.

I RSA har man alltid en offentlig nyckel (offentlig nyckel är sådan som alla kan veta), (n, e), där $n = pq$ och p och q udda primtal, $p \neq q$. Det är jätteviktigt att använda talet n utan att berätta sin primtalsfaktorisering, eftersom det är verkligen svårt att hitta p och q om man bara vet talet n.

Den hemliga nyckeln är $(p, q, \varphi(n), d)$, där $ed \equiv 1 \pmod{\varphi(n)}$, alltså talet e måste väljas på ett sådant sätt att inversen finns, dvs $\text{sgd}(e, \varphi(n)) = 1$. Talet d är lätt att beräkna genom att lösa en diofantisk ekvation om vi vet vilka talen är e och $\varphi(n)$ (för att beräkna $\varphi(n)$ måste vi veta vad är p och q).

Sammanfattning: Offentlig nyckel (n, e), hemlig nyckel $(p, q, \varphi(n), d)$, och vi antar att $pq = n$, $p \neq q$, p och q uuda primtal, $ed \equiv 1 \pmod{\varphi(n)}$, och $\varphi(n)$är Eulers funktion. Alltså, vi antar att $\text{sgd}(e, \varphi(n)) = \text{syt}(d, \varphi(n)) = 1$.

Nu kan vi kryptera talet $1 \leq w \leq n$ på sådant sätt:

$$w' \equiv w^e \pmod{n}$$

och dekryptera:

$$w'' \equiv w'^d \pmod{n}.$$

Nu $w \equiv w'' \pmod{n}$, eftersom

$$w'' \equiv w'^d \equiv w^{ed} \pmod{n},$$

och enligt Eulers sats

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

alltså $w^{ed} = w^{1+k\varphi(n)} \pmod{n}$, om $\text{sgd}(w, n) = 1$.

Exempel 41. Låt $n = 83 \cdot 103 = 8549$. Nu $\varphi(n) = (83-1)(103-1) = 82 \cdot 102 = 8364$. Välj $e = 13$. Det är möjligt eftersom $\text{sgd}(13, 8364) = 1$. Lös nu d:

$$de - +k\varphi(n) = 1,$$

dvs

$$13d + k8364 = 1.$$

Nu

$$\begin{aligned} 364 &= 643 \cdot 13 + 5 \\ 13 &= 2 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 12 \quad = 2 \cdot 1 + 0, \end{aligned}$$

alltså

$$1 = 3 - 1 \cdot 2,$$

och vi kan stoppa in

$$1 = 3{-}1(5{-}3) = 2{\cdot}3{-}5 = 2(13{-}2{\cdot}5){-}5 = 2{\cdot}13{-}5{\cdot}5 = 2{\cdot}13{-}5(8364{-}643{\cdot}13) = 3217{\cdot}13{-}5{\cdot}8364.$$

Vi kan välja $d = 3217$. Vi vill nu krypta talet 87. Det räcker att beräkna $87^{13} (\text{mod } 8549)$. Nu

$$87^{13} \equiv 7929 \pmod{8549}.$$

Dekryptering är lika enkelt: Vi måste beräkna

$$7929^{3217} \pmod{8549}.$$

Troligen det bästa sätt är att beräkna genom att beräkna kvadrater. Skriv nu

$$3217_{10} = 110010010001_2$$

som binär. Nu

$$7929^{3217} = 7929^{2048} \cdot 7929^{1024} \cdot 7929^{128} \cdot 7929^{16} \cdot 7929.$$

Följande metoden fungerar snabbt. Vi använder kvadrater för att beräkna alla talen i produkten.

$$7929^{16} \equiv \left(7929^2\right)^8 \equiv 8244^8 \equiv 305^8 \equiv 7535^4 \equiv 2316^2 \equiv 3633 \pmod{8549}.$$

Eftersom $128 = 16 \cdot 8$, gäller det

$$7929^{128} \equiv 3633^8 \pmod{8549}.$$

Nu kan vi beräkna

$$3633^8 \equiv 7582^4 \equiv 3248^2 \equiv 38 \pmod{8549}.$$

Eftersom $1024 = 8 \cdot 128$, kan vi beräkna

$$7929^{1024} \equiv 38^8 \pmod{8549},$$

alltså

$$38^8 = 1444^4 \equiv 7729^2 \equiv 5578 \pmod{8549}.$$

Nu $2048 = 2 \cdot 1024$, så det räcker att beräkna

$$7929^{2048} \equiv 5578^2 \equiv 4273 \pmod{8549}.$$

Och nu

$$7929^3217 \equiv 4273 \cdot 5578 \cdot 38 \cdot 3633 \cdot 7929 \equiv 87 \pmod{8549}.$$

7.1.1 Svagheter i systemet

VI vill nu visa att $p - q$ får inte vara för litet:

Sats 42. *Om $\left|\frac{p-q}{2}\right|^2 < 2\sqrt{n} + 1$, är det snabbt att hitta faktorer till talet $n = pq$. (dvs. vi kan bryta RSA).*

Bevis. Om $p = q$, är det lätt att hitta faktorer. Anta nu att $p > q$, och skriv $p = t + r$ och $q = t - r$, där t och r är positiva hela tal. Nu $p - q = 2r$, dvs $r^2 < 2\sqrt{n} + 1$ och

$$n = pq = (t + r)(t - r) = t^2 - r^2.$$

Åt annat hand

$$(\lceil\sqrt{n}\rceil + 1)^2 = \lceil\sqrt{n}\rceil^2 + 2\lceil\sqrt{n}\rceil + 1 > n + 2\sqrt{n} + 1 > n + r^2.$$

Nu $t^2 = n + r^2$, och därför $t^2 > n$. Nu $t^2 < (\lceil\sqrt{n}\rceil + 1)^2$, alltså $t = \lceil\sqrt{n}\rceil$. Vi kan använda detta för att lösa r:

$$r^2 = \lceil\sqrt{n}\rceil^2 - n,$$

och nu

$$p = \lceil\sqrt{n}\rceil + r$$

och

$$q = \lceil\sqrt{n}\rceil - r.$$

□

- Wiener har visa att det är möjligt att bryta RSA när $d < \frac{1}{3}n^{1/4}$
- Boneh och Durfee visade att det är möjligt att bryta RSA när $d < n^{0,292}$.
- Man tror att det är möjligt att bryta RSA när $d < \sqrt{n}$.

7.2 Diffie-Hellman-protokoll för nyckelutbyte

Diffie-Hellman-protokol för nyckelutbyte passar bra när två personer behöver något gemensamt tal, som andra människor får inte veta, och när bara en öppen kommuniceringsmetod kan användas (t.ex. affischtavla, tidning, osv).

1. Först skall personerna (låt de vara Bonnie och Clyde) besluta ett primtal och en primitiv rot, t.ex. Bonnie väljer ett primtal p och en primitiv rot g och sen publicerar informationen.
2. Nu skall Bonnie och Clyde välja sina egna exponenter b och c, och de berättar ingen (inte ens till varandra).
3. Bonnie beräknar $b' = g^b$ modulo p och Clyde beräknar $c' = g^c$ modulo p, och de publicerar talen b' och c'.
4. Bonnie beräknar nu c'^b modulo p och Clyde beräknar b'^c modulo p, och nu har de ett gemensamt tal, eftersom

$$c'^b \equiv (g^c)^b = g^{cb} \equiv (g^b)^c \equiv b'^c \pmod{p}.$$

Det är verkligen viktigt att reducera modulo p, eftersom annars vore det för lätt att hitta b och c med hjälp av logaritmer.