

Resträkning och ekvationer

TORSTEN EKEDAHL

Stockholms Universitet

Beskrivning av uppgiften. Specialarbetet består i att sätta sig in i hur man räknar med rester vid division med primtal, hur man löser ekvationer vid resträkning. Till sist ska man beräkna antalet lösningar till en viss sorts ekvationer och jämföra den statistiska fördelningen av dessa antal med en fördelning som man hoppas att de ska uppfylla.

Resträkning. Vi säger att två tal är *kongruenta* modulo ett tredje om de har samma rest vid division med detta tal. Till exempel så är 12 kongruent med 5 modulo 7 eftersom de båda har resten 5 vid division med 7. Man skriver också detta som $12 \equiv 5 \pmod{7}$. (Referens till detta och det som följer närmast är [Hardy-Wright:Kap. V, spec 5.2, 5.3].) Kongruenser uppfyller de vanliga räknelagarna: $12 \equiv 5 \pmod{7}$ och $(13) \equiv (20) \pmod{7}$ så $12 \cdot 13 \equiv 5 \cdot 20 \pmod{7}$ och $12 + 13 \equiv 5 + 20 \pmod{7}$. Vi har naturligtvis också t ex $2^{12} \equiv (2^3)^4 \equiv 8^4 \equiv 1^4 \pmod{7}$. Man kan också tala om kongruensekvationer: $x \equiv 3 \pmod{7}$ är en lösning till ekvationen $x^2 + 2x - 1 \equiv 0 \pmod{7}$ eftersom $3^2 + 2 \cdot 3 - 1 = 14 \equiv 0 \pmod{7}$. På samma sätt är $(x, y) \equiv (6, 0) \pmod{7}$ en lösning till ekvationen $y^2 \equiv x^3 - 1 \pmod{7}$. Man kan räkna antalet lösningar till sådana ekvationer. Först konstaterar vi att om ett tal (eller ett par av tal) är en lösning till en kongruensekvation beror bara på resterna av talet (talen) vid division med det tal som resterna räknas modulo (i våra exempel 7). Därför är det naturligt att gå genom varje rest precis en gång. Om vi till exempel vill se hur många lösningar ekvationen $x^2 + 2x - 1 \equiv 0 \pmod{7}$ har så ska vi låta x anta värdena $0, 1, \dots, 6$:

$$0^2 + 2 \cdot 0 - 1 = -1 \not\equiv 0 \pmod{7}$$

$$1^2 + 2 \cdot 1 - 1 = 2 \not\equiv 0 \pmod{7}$$

$$2^2 + 2 \cdot 2 - 1 = 7 \equiv 0 \pmod{7}$$

$$3^2 + 2 \cdot 3 - 1 = 14 \equiv 0 \pmod{7}$$

$$4^2 + 2 \cdot 4 - 1 = 23 \not\equiv 0 \pmod{7}$$

$$5^2 + 2 \cdot 5 - 1 = 34 \not\equiv 0 \pmod{7}$$

$$6^2 + 2 \cdot 6 - 1 = 47 \not\equiv 0 \pmod{7}$$

Vi ser alltså att ekvationen $x^2 \cdots x - 1 \equiv 0 \pmod{7}$ har två lösningar. På motsvarande sätt kan vi räkna antalet lösningar till ekvationen $y^2 \equiv x^3 - 1 \pmod{7}$ och då måste vi låta både x och y anta värdena $0, 1, \dots, 6$ dvs i allt måste vi räkna igenom $7 \cdot 7 = 49$ olika fall. Vi kan gör räkningarna på ett enklare sätt än att gå igenom alla dessa 49 fall och verifiera om vänsterledet har samma rest som högerledet vid division med 7. Om vi väljer en rest (t ex 3) för x så kan vi börja med att fråga oss om det överhuvudtaget finns ett y så att ekvationen $y^2 \equiv 3^3 - 1 \pmod{7}$ är uppfylld. Då $3^3 - 1 \equiv 5 \pmod{7}$ så betyder det att vi frågar oss om ekvationen $y^2 \equiv 5 \pmod{7}$ har någon lösning eller inte. Om vi går igenom alla möjligheter för y får vi:

$$0^2 \equiv 0 \pmod{7}$$

$$1^2 \equiv 1 \pmod{7}$$

$$2^2 \equiv 4 \pmod{7}$$

$$3^2 \equiv 2 \pmod{7}$$

$$4^2 \equiv 2 \pmod{7}$$

$$5^2 \equiv 4 \pmod{7}$$

$$6^2 \equiv 1 \pmod{7}$$

Vi ser alltså att ekvationen $y^2 \equiv 5 \pmod{7}$ inte har någon lösning och därför när vi försöker räkna lösningarna till $y^2 \equiv x^3 - 1 \pmod{7}$ så kan vi utesluta alla par (x, y) där $x = 3$. Å andra sidan, om $x = 2$

får vi $2^3 - 1 \equiv 0 \pmod{7}$ och från tabellen ovan ser vi att ekvationen $y^2 \equiv 0 \pmod{7}$ har precis en lösning så att bland paren (x, y) för vilka $x = 2$ får vi 1 lösning till ekvationen $y^2 \equiv x^3 - 1 \pmod{7}$. Vi kan gå igenom alla rester x och vi får då:

$$0^3 - 1 \equiv 6 \pmod{7}$$

$$1^3 - 1 \equiv 0 \pmod{7}$$

$$2^3 - 1 \equiv 0 \pmod{7}$$

$$3^3 - 1 \equiv 5 \pmod{7}$$

$$4^3 - 1 \equiv 0 \pmod{7}$$

$$5^3 - 1 \equiv 5 \pmod{7}$$

$$6^3 - 1 \equiv 5 \pmod{7}$$

Vi ser alltså att vi får sammanlagt 3 lösningar till ekvationen $y^2 \equiv x^3 - 1 \pmod{7}$; 1 för varje x -värde 1, 2 resp 4.

Vi kan byta ut 7 mot ett annat tal; av anledningar som kommer att bli klara om ett ögonblick vill vi låta detta tal vara ett udda primtal p . Om vi vill räkna antalet lösningar till ekvationen $y^2 \equiv x^3 - 1 \pmod{p}$ så kan vi resonera som i det speciella fallet 7. För ett givet värde x_0 på x får vi tre fall:

- I. $y^2 \equiv x_0^3 - 1 \pmod{p}$ har ingen lösning.
- II. $y^2 \equiv x_0^3 - 1 \pmod{p}$ har en lösning och $x_0^3 - 1 \not\equiv 0 \pmod{p}$.
- III. $x_0^3 - 1 \equiv 0 \pmod{p}$.

I det första fallet så finns det inga par (x_0, y) som är lösningar till ekvationen $y^2 \equiv x^3 - 1 \pmod{p}$. I det andra fallet finns det precis två lösningar: Det finns minst två lösningar ty om (x_0, y) är en lösning så är $(x_0, -y)$ en annan och y och $-y$ är olika rester eftersom p är ett *udda* tal. Å andra sidan finns det högst två lösningar till ekvationen $y^2 \equiv t \pmod{p}$. Om $y_0^2 \equiv t \pmod{p}$ och $y_1^2 \equiv t \pmod{p}$ så $y_0^2 \equiv y_1^2 \pmod{p}$ och därför $(y_0 - y_1)(y_0 + y_1) = y_0^- y_1^2 \equiv 0 \pmod{p}$, men om två tal ej är delbara med p så är deras produkt inte heller delbar med

p [Hardy-Wright: 1.3 Thm 3] (här använder vi att p är ett primtal, vi har t ex $2 \not\equiv 0 \pmod{6}$ och $3 \not\equiv 0 \pmod{6}$ men $2 \cdot 3 \equiv 0 \pmod{6}$). Därför har vi antingen $y_0 - y_1 \equiv 0 \pmod{p}$ dvs y_0 och y_1 är samma rester eller $y_0 + y_1 \equiv 0 \pmod{p}$ dvs y_0 och $-y_1$ är samma rester, vilket ger högst två möjligheter för en lösning till $y^2 \equiv t \pmod{p}$. Till sist, i fall III finns bara en lösning (x_0, y) ty vi måste ha $y^2 \equiv 0 \pmod{p}$ vilket igen medför att $y \equiv 0 \pmod{p}$ (eftersom y är ett primtal).

Vi ser alltså att för att räkna antalet lösningar (x, y) till $x^2 \equiv y^3 - 1 \pmod{p}$ så kan vi gå genom alla möjligheter för x ($x = 0, 1, 2, \dots, p-1$), räkna ut resten av $x^3 - 1$ vid division, kontrollera i vilket av fallen I-III vi befinner oss i och, till sist, för varje värde av x lägga 0, 2 resp 1 till antalet lösningar om vi är i fall I, II resp III.

Snabbheten i olika metoder. Det kan tyckas att vi har kommit på en mycket bättre metod än att gå igenom alla par (x, y) om vi följer detta recept och vi som i fallet $p = 7$ börjar med att skriva upp en lista på alla rester som är kvadrater. Låt oss göra en uppskattning av antalet saker vi måste göra för att komma fram till antalet lösningar. I det fall där vi går igenom alla par måste vi för varje par räkna ut y^2 och $x^3 - 1$, räkna ut deras skillnad, ta resten vid division med p och sedan se om denna rest är noll eller inte. Detta innebär 5 multiplikationer, 2 subtraktioner, en division och en jämförelse. Vi vill bara ha en grov uppskattning av hur lång tid det tar att göra våra beräkningar så vi nöjer oss med att konstatera att det tar en viss fix tid att kontrollera om ett par (x, y) uppfyller $y^2 \equiv x^3 - 1 \pmod{p}$ eller ej. I allt tar det alltså en fix tid gånger p^2 , antalet par, för att bestämma antalet lösningar (vi bryr oss inte om att multiplikationer osv tar längre tid ju fler siffror de inblandade talen är, denna tid växer rätt långsamt med p). Eftersom tiden växer

som en multipel av *kvadraten* på p så blir den snabbt stor och denna metod blir snabbt opraktisk. Om vi tittar på den andra metoden så börjar vi med att göra en lista på alla kvadrater vilket tar en fix tid gånger p , sedan räknar vi ut för varje x resten av $x^3 - 1$ och letar sedan i listan för att se om denna rest förekommer. Då listan har längd $\frac{p+1}{2}$ så är söktiden för att se om en rest är en kvadrat eller ej en fix tid gånger p och då vi måste söka för varje x blir den totala söktiden en fix tid gånger p^2 ! Vi kan förbättra tiden om vi istället börjar att göra en lista över *alla* rester vid division och sedan prickar för de som är kvadrater. Att göra detta tar en fix tid gånger p . I steget där vi tidigare sökte igenom listan för att se om resten av $x^3 - 1$ var en kvadrat eller ej kan vi nu gå in i listan och se om resten av $x^3 - 1$ är förprickad eller ej. Detta tar bara en fix tid för varje x så vi ser att den totala tiden för att bestämma antalet lösningar till $y^2 \equiv x^3 - 1 \pmod{p}$ är en fix tid gånger p , vilket är en avsevärd förbättring.

Ett problem med denna senare metod är att vi måste ha en lista av längd p med kvadraterna förprickade vilket tar plats om p är stort. Det finns ett lite mer avancerat sätt att göra det hela på som också tar en fix tid gånger p . Det hela går ut på att hitta ett sätt att avgöra om det för en given rest t finns en lösning till ekvationen $y \equiv t \pmod{p}$ utan att göra upp en lista på alla rester av kvadrater. Närmare bestämt är det så att $t^{\frac{p-1}{2}}$ har rest $p-1$ vid division med p om det ej finns någon lösning, har rest 1 vid division med p om det finns en lösning och t ej har rest 0 vid division med p och har, naturligtvis, rest 0 om t har rest 0 vid division med p (se [Hardy-Wright: 6.5, 6.6 Thm 83]). Detta är det sk Eulers kriterium. Till exempel så $3^3 = 27 \equiv 6 = 7 - 1 \pmod{7}$ och $2^3 = 8 \equiv 1 \pmod{7}$ och vi ser från tabellen ovan att $y \equiv 3 \pmod{7}$ ej har någon lösning medan $y \equiv 2 \pmod{7}$ har det. Till en början kan det tyckas att

detta inte är till någon hjälp då det behövs $\frac{p-1}{2}$ multiplikationer för att beräkna $t^{\frac{p-1}{2}}$. Detta är dock inte sant, det går att göra med ett mycket mindre antal! Ta beräkandet av 3^{11} som ett exempel. Vi börjar med att skriva 11 binärt: $10 = 2^3 + 2 + 1$. Vi beräknar sedan först $3^2 = 9$, sedan $3^{2^2} = 9^2 = 81$ och $3^{2^3} = 81^2 = 6561$. Till sist får vi $3^{11} = 3^{2^3+2+1} = 3^{2^3} \cdot 3^2 \cdot 3^1 = 6561 \cdot 9 \cdot 3 = 177147$. Vi ser på detta sätt att antalet operationer som behövs för att beräkna $t^{\frac{p-1}{2}}$ är proportionellt, inte mot p utan mot längden på den binära utvecklingen av $\frac{p-1}{2}$. Detta är av samma storleksordning som den tid det tar att multiplicera eller addera två tal av storlek ungefär p en tid som vi redan flera gånger har låtsats är konstant.

Vi får alltså följande recept för att beräkna antalet lösningar till ekvationen $y^2 \equiv x^3 - 1 \pmod{p}$, som har fördelen att vara snabb och ej kräva att vi gör långa listor.

Gör följande för $x = 0, 1, \dots, p - 1$:

STEG 1: Beräkna resten vid division med p av $x^3 - 1$. Kalla denna rest t .

STEG 2: Beräkna resten av $t^{\frac{p-1}{2}}$ vid division med p om t ej är 0. Kalla denna rest r .

STEG 3: Om t är 0 lägg 1 till antalet lösningar. Om r är 1 lägg 2 till antalet lösningar annars gör inget.

För att få en uppfattning om antalet lösningar är det en bra idé att dra p från antalet lösningar (anledningen till detta blir klar om några rader). Vi kallar det tal vi då får för a_p . Då p är lika med antalet x som vi går igenom så får vi följande recept för att beräkna a_p .

Sätt a_p lika med 0. Gör följande för $x = 0, 1, \dots, p - 1$:

STEG 1: Beräkna resten vid division med p av $x^3 - 1$. Kalla denna rest var t .

STEG 2: Beräkna resten av $t^{\frac{p-1}{2}}$ vid division med p om t ej är 0. Kalla denna rest r .

STEG 3: Om t är 0 lägg 0 till a_p . Om r är 1 lägg 1 till a_p annars lägg -1 till a_p .

Förväntade fördelningar. Man kan visa att t är lika med 0 för högst $3x$ (se [Hardy-Wright:VII Thm 107]). Detta fall kommer därför inte att påverka a_p speciellt mycket. I de andra fallen så verkar det rimligt att resten av $x^3 - 1$ för $x = 0, 1, \dots, p-1$ skulle vara en kvadrat ungefär lika ofta som det inte var det (eftersom det finns lika många rester skilda från 0 som är kvadraten av en rest som det finns rester som inte är det). Därför bör det vara så att vi lägger 1 till a_p ungefär lika många gånger som vi lägger till -1. Om detta är sant så bör a_p vara ungefär 0. Mer precist kan vi till och med tänka oss att det är helt slumpmässigt om, för ett givet x , resten $x^3 - 1$ är kvadraten av en rest eller inte. I så fall kan vi naturligtvis inte hoppas på att a_p skulle vara exakt 0. Å andra sidan om det är slumpmässigt så vet vi från sannolikhetsläran att med hög sannolikhet ska a_p högst vara i storleksordningen \sqrt{p} . Ett mycket berömt matematiskt resultat säger att vi alltid har $-2\sqrt{p} \leq a_p \leq 2\sqrt{p}$. Detta bekräftar till en del vår "statistiska modell" att det är slumpmässigt om $x^3 - 1$ har rest en kvadrat eller inte men visar också att situationen är mer komplicerad eftersom om det vore slumpmässigt på samma sätt som slantsingling så skulle vi alltid få åtminstone något a_p som är större än $2\sqrt{p}$ (närmare bestämt en viss proportion av a_p :na skulle vara större än $2\sqrt{p}$ eller för den delen större än ett godtyckligt tal gånger \sqrt{p}). För att få en bättre idé om vad vi kan säga om a_p :na så skalar vi dem med faktorn $2\sqrt{p}$ och sätter $b_p = a_p/2\sqrt{p}$. På så sätt kommer vi alltid att ha att $-1 \leq b_p \leq 1$. Vad kan vi nu säga om dessa tal? Erfarenheten visar att vi inte kan säga något förnuftigt om de enskilda b_p :na utan endast något om deras statistiska fördelning dvs

om vi beräknar b_p för ett antal p så kan vi se hur stor proportion av b_p :na ligger i intervallet mellan a och b för olika a och b med $-1 \leq a \leq b \leq 1$. Ett annat matematiskt resultat, inte lika berömt som det förra, säger att b_p :na är jämnt fördelade bortsett från att hälften av dem är 0 dvs om vi beräknar b_p för tillräckligt många p så kommer andelen b_p som ligger i intervallet mellan a och b att komma godtyckligt nära $\frac{b-a}{4}$ plus $\frac{1}{2}$ om 0 ligger i intervallet (4:an i nämnaren kommer från att vi vill ha proportionen 1 när $a=-1$ och $b=1$). Med andra ord, bortsett från 0, är inget värde på b_p mer sannolikt än något annat.

Vi kan ersätta $x^3 - 1$ med ett annat tredjegradspolynom t ex $x^3 + 2x + 1$. Om vi definierar a_p och b_p på samma sätt men nu för ekvationen $y^2 \equiv x^3 + 2x + 1 \pmod{p}$ så gäller fortfarande att $-2\sqrt{p} \leq a_p \leq 2\sqrt{p}$ och därför $-1 \leq b_p \leq 1$. Denna gång ska b_p :na däremot inte vara jämnt fördelade. Istället ska proportionen av de b_p som finns i intervallet mellan a och b vara nära

$$\frac{2}{\pi} \int_a^b \sqrt{1-x^2} dx$$

(denna integral kan naturligtvis räknas ut men den ser trevligare ut som den är). Att detta gäller för $x^3 + 2x + 1$ är något man inte, till skillnad från fallet $x^3 - 1$, vet utan för tillfället endast hoppas på. Även om man inte kan bevisa det är det något man kan undersöka rimligheten av genom att beräkna b_p för ett antal p och jämföra de proportioner man får med vad man hoppas på.

Situationen för ett godtyckligt tredjegradspolynom förväntas vara densamma som för ett av de polynom vi diskuterat. Detta är inte sant för några sällsynt förekommande polynom: de som har ett nollställe gemensamt med sin derivata som t ex $x^3 + x^2$; $x = 0$ är ett nollställe till både $x^3 + x^2$ och dess derivata $3x^2 + 2x$. Om vi

istället tittar på $x^3 + 2x + 1$ så är dess derivata $3x^2 + 2$ så om de har ett gemensamt nollställe x så är

$$\begin{aligned}x^3 + 2x + 1 &= 0 \\3x^2 + 2 &= 0.\end{aligned}$$

Om vi multiplicerar den första ekvationen med 3 och den andra med x och subtraherar får vi

$$\begin{aligned}4x + 3 &= 0 \\3x^2 + 2 &= 0.\end{aligned}$$

Om vi multiplicerar den första ekvationen med $3x$ och den andra med 4 och sedan subtraherar får vi

$$\begin{aligned}4x + 1 &= 0 \\9x - 8 &= 0.\end{aligned}$$

Om vi multiplicerar den första ekvationen med 9 och den andra med 4 och sedan subtraherar får vi

$$41 = 0.$$

Av detta ser vi att $x^3 + 2x + 1$ inte har något nollställe gemensamt med sin derivata. Om vi istället hade räknat rester vid division med 41 så hade vi på slutet istället fått

$$41 \equiv 0 \pmod{41}$$

vilket faktiskt är sant och man kan kontrollera att $x = 10$ är en gemensam lösning till $x^3 + 2x + 1 \equiv 0 \pmod{41}$ och $3x^2 + 2 \equiv 0 \pmod{41}$. Precis som vi inte är intresserade av polynom som har ett nollställe gemensamt med sin derivata så är vi heller inte intresserade

av vissa "dåliga" primtal. Dessa är de primtal för vilka det polynom vi är intresserade av har ett nollställe gemensamt med sin derivata vid resträkning vid division med primtalet i fråga. I fallet $x^3 + 2x + 1$ borde vi alltså hoppa över 41 när vi beräknar b_p :na och i alla fall när vi räknar ut proportionen av b_p i ett visst intervall. Då det bara rör sig om ett värde har det dock inte någon större betydelse.

Om vi nu betraktar ett tredjegradspolynom som ej har något nollställe gemensamt med sin derivata så gäller igen att $-1 \leq b_p \leq 1$ för alla udda primtal p . Vidare hoppas man att den statistiska fördelningen antingen ska vara som i fallet $x^3 - 1$ dvs proportionen b_p i intervallet från a till b ska vara ungefär $\frac{b-a}{4}$ plus $\frac{1}{2}$ om 0 ligger i intervallet eller som i fallet $x^3 + 2x + 1$ dvs proportionen b_p i intervallet från a till b ska vara ungefär $\frac{2}{\pi} \int_a^b \sqrt{1-x^2} dx$. Det finns ett sätt att bestämma direkt om det första fallet ska gälla och när det är så så vet man att den statistiska fördelningen är den man hoppas på. Å andra sidan finns det inget exempel på ett polynom som inte faller i den första kategorin för vilket man vet att den statistiska fördelningen är den man önskar. Vad man har gjort är att beräkna b_p för ett antal polynom och ett antal primtal och se om proportionerna är de de borde vara. Det är dessutom det andra fallet som är det vanligaste; om man tar ett polynom på måfå så är chansen mycket liten att den faller i den första kategorin.

Om man tittar på polynom av andra gradtal så händer följande. Om graden är 1 händer inget spännande: a_p är alltid 0. Om graden är 2 är det knappast mer intressant: a_p är alltid 0 eller -1. Om graden är 4 är situationen precis som i fallet grad 3. Om graden är 5 eller större är situationen mer komplicerad t ex om graden är 5 vet man bara att $-4\sqrt{p} \leq a_p \leq 4\sqrt{p}$ och för fördelningen av b_p :na finns det fler än två möjligheter.

Närmare beskrivning av specialarbetet. Man ska till en början förstå kongruensräkning; i den mån ovanstående inte är tillräckligt kan man läsa mer i t ex [Hardy-Wright: Kap V, VI, VII]. Det finns möjlighet att lägga mer eller mindre tid på denna del, t ex är det inte nödvändigt att veta varför Eulers kriterium fungerar för att använda det. Den andra delen av specialarbetet skall sedan ägnas åt att undersöka fördelningen av b_p :na för några tredjegradspolynom och primtal. Det är knappast realistiskt att genomföra detta för hand men den enklaste formen av programmerbar fickräknare är tillräcklig (några exempel måste naturligtvis räknas ut för hand för att kontrollera att man har programmerat rätt). Alla de steg som beskrivits ovan går att programmera, även om en del saker fordrar eftertanke som t ex att man måste se till att heltalsberäkningarna utförs exakt och inte i flyttalsform. Resultaten skall sedan jämföras med den förväntade fördelningen. Detta kan ske i tabell- eller diagramform men man kan också tänka sig någon form av statistisk analys. I det fall det finns intresse för numeriska beräkningar kan man jämföra hastigheten av de olika metoder som beskrivits ovan och göra olika försök att öka genom att ändra i programmen.

Litteratur

Hardy, G.H. & Wright, E.M., *An Introduction to the theory of numbers*. Fifth edition, Oxford Univ. Press, Oxford 1977.