A12 Fördjupning. Fermats lilla sats

Fermats lilla sats säger att för ett godtyckligt heltal a och ett godtyckligt primtal p gäller att $a^p - a$ är delbart med p. Satsen har många tillämpningar, bl.a. för konstruktionen av krypteringsmetoden RSA >>. Man kan också använda satsen för att studera vilka periodlängder som är möjliga för digitalutvecklingar av rationella tal ...

Kommentar Pierre de Fermat (1601-1665) var inte yrkesmatematiker utan domare i Toulouse. Han bevisade sin "lilla" sats, men det tror man inte att han gjorde med den mer berömda "Fermats stora sats". Fermats stora sats säger att det finns inga positiva heltal x,y,z,n där $n > 2$ och $x^n + y^n = z^n$. Denna sats bevisades för ca 7 år sedan av engelsmannen Andrew Wiles. Satsen i sig är inte så intressant, men den har inspirerat matematiker genom århundradena att utveckla teorier för att kunna bevisa satsen. Dessa teorier har sedan en mängd intressanta tillämpningar. Satsen blev berömd efter Fermats död eftersom man hittade en marginalanteckning i ett verk av Diofantos som Fermat läste. I marginalen formulerar Fermat satsen och skriver att han har hittat ett underbart bevis, men att det tyvärr inte får plats i marginalen ... Du kan läsa mer om detta i boken "Fermats gåta" av Simon Singh.

Fermat brevväxlade också med Pascal om ett problem om hur två spelare rättvist skall dela på den gemensamma potten om spelet avbryts vid en viss ställning. Denna brevväxling utgör grunden till sannolikhetsläran.

Oftast använder man Fermats lilla sats i en något annorlunda formulering:

För varje primtal p och varje heltal a som inte är delbart med p, så gäller att $a^{p-1} - 1$ är delbart med p.

Vi skall nu bevisa satsen i den ursprungliga formuleringen. Låt oss som uppvärmning se om vi kan bevisa satsen för små värden på p. Antag att p=2. Satsen säger då att $a^2 - a$ är ett jämnt tal för varje heltal a. Men $a^2 - a = a(a-1)$ och a och $a - 1$ är två på varandra följande heltal och då måste ett av talen vara jämnt. Det följer att $a^2 - a$ är jämnt och därmed är satsen bevisad för p=2. Stärkta av detta ger vi oss i kast med fallet p=3. Vi skall alltså bevisa att $a^3 - a$ är delbart med 3 för alla heltal a. Men $a^3 - a = a(a^2 - 1) = a(a + 1)(a - 1)$ och $a - 1, a, a + 1$ är 3 på varandra följande heltal och då måste ett av dem vara delbart med 3! Ja, då är det väl bara att säga o.s.v. och därmed är satsen bevisad, eller? Nej, tyvärr fungerar inte metoden för nästa primtal p=5. Man kan dock klara även detta fall med lite extra arbete. Man kan dela in problemet i 5 olika fall, beroende på om a ger rest 0,1,2,3 eller 4 då man delar med 5. Så kan man göra för varje specifikt primtal p, men det är svårt att se något mönster i dessa bevis som skulle gå att generalisera till ett bevis som duger för ett godtyckligt primtal p.

Vi byter fot och låter primtalet p vara fixt men godtyckligt och koncentrerar oss istället på att försöka bevisa påståendet för små värden på a. För a=0 eller a=1 är påståendet trivialt eftersom 0 är delbart med alla heltal. Om påståendet är bevisat för alla positiva heltal a, så följer påståendet även för negativa heltal a, ty $a^p - a$ ändrar bara tecken om vi byter a mot $-a$ (om $p > 2$). Därför kan vi i fortsättningen anta att a är ett heltal ≥ 2. Vi försöker nu bevisa påståendet

för a=2, dvs för alla primtal p gäller att

$$2^p - 2 \text{ är delbart med } p$$

Idé: Använd Binomialteoremet! Vi har

$$2^p = (1+1)^p = 1 + \binom{p}{1} + \binom{p}{2} + \ldots + \binom{p}{2} + \binom{p}{1} + 1$$

Eftersom vi har en etta i början och slutet, så gäller att $2^p - 2$ är en summa av binomialkoefficienterna i mitten. Om vi kan visa att alla dessa är delbara med p, så skulle vi vara klara (med beviset i fallet a=2). Låt oss titta på en allmän binomialkoefficient $\binom{p}{k}$, där $0 < k < p$ och p är ett primtal:

$$\binom{p}{k} = p \cdot (p-1) \cdot \ldots \cdot (p-k+1)/(1 \cdot 2 \cdot 3 \cdot \ldots \cdot k)$$

Även om högra ledet ser ut som ett äkta bråktal, så vet vi att det är ett heltal, eftersom det är en binomialkoefficient. Detta betyder att nämnaren måste gå att förkorta bort i täljaren. Men varje faktor i nämnaren är $< p$, så när denna faktor förkortas bort, så kan inte primtalet p användas som står längst till vänster i täljaren (här använder vi Aritmetikens fundamentalsats!). Slutsatsen blir att när bråket är färdigförkortat, så har vi kvar ett heltal som innehåller faktorn p, dvs vi har bevisat att

Binomialkoefficienten $\binom{p}{k}$ är delbar med p för alla primtal p och för alla k där $0 < k < p$.

Exempel Vi har att

$$\binom{13}{6} = \frac{13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8}{2 \cdot 3 \cdot 4 \cdot 5 \cdot 6} = 13 \cdot 11 \cdot 3 \cdot 4 = 13 \cdot 132$$

Med hjälp av detta resultat, så är vi (som vi påpekade ovan) klara med beviset i fallet a=2. Låt oss gå vidare med a=3! (Det kanske kan tyckas hopplöst, eftersom talramsan är så lång och vårt försök förut att bevisa satsen för p=2, p=3, osv inte ledde till något generellt bevis. Det vi kan hoppas på är att vi denna gång kan finna ett mönster.) Påståendet för a=3 lyder (p är ett godtyckligt primtal):

$$3^p - 3 \text{ är delbart med } p$$

Låt oss som förut använda Binomialteoremet:

$$3^p = (2+1)^p = 2^p + \binom{p}{1}2^{p-1} + \binom{p}{2}2^{p-2} + \ldots + \binom{p}{2}2^2 + \binom{p}{1}2 + 1$$

Om vi nu drar bort 3 från båda leden och flyttar sista termen -2 som bildas i högra ledet till andra plats, så får vi:

$$3^p - 3 = 2^p - 2 + \binom{p}{1}2^{p-1} + \binom{p}{2}2^{p-2} + \ldots + \binom{p}{2}2^2 + \binom{p}{1}2$$

Med hjälp av vårt resultat om binomialkoefficienterna ovan, så får vi att summan av termerna efter $2^p - 2$ i högerledet är delbart med p. Vad kan vi då säga om

$2^p - 2$? Jo, men det har vi ju just bevisat är delbart med p!! Voilà, vi är klara även med fallet a=3.

Gör nu själv beviset i fallet a=4!

Efter att ha gjort detta, så inser man att beviset är detsamma för vilket heltal a som helst. Om man bara vet att satsen är sann för talet innan, dvs $a-1$, så ger argumentet ovan att satsen också är sann för a. Men då kan vi ju upprepa resonemanget och nå vilket heltal a som helst och därmed är satsen till fullo bevisad.

Vi har avsiktligt varit långrandiga i beviset ovan och vi har gjort en del överläggningar som till sist visat sig onödiga. Om man nu skall sammanfatta beviset, så vill man ju helst göra detta så kort som möjligt för att påvisa hur elegant och enkelt ens argument är. Därför ser beviset ut ungefär enligt följande i en normal framställning.

Det räcker att visa påståendet för positiva heltal a. För a=1 är påståendet trivialt. Antag att påståendet är sant för a. Då gäller att

$$(a+1)^p - a - 1 = a^p - a + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \ldots + \binom{p}{2}a^2 + \binom{p}{1}a$$

Men $a^p - a$ är delbart med p enligt antagandet och varje binomialkoefficient i högerledet är delbar med p eftersom p är ett primtal och därför inte kan förkortas bort med någon faktor i nämnaren $2 \cdot 3 \ldots \cdot k$ av $\binom{p}{k}$. Alltså är $(a+1)^p - (a+1)$ delbart med p.

Påståendet är nu sant för alla positiva heltal a enligt induktionsprincipen, eftersom påståendet är sant för a=1 och om det är sant för a, så är det sant även för $a+1$. V.S.B.