

# Talteori grupp SMT1

Lars Åström

11-12 december 2015

Vi kommer att gå igenom

- Induktion
- Euklides algoritm
- Bezouts identitet
- Primtalen - hur använder vi dem smart?
- Aritmetikens fundamentalsats
- Modulär räkning och restklasser
- Fermats lilla sats och Eulers sats
- Diofantiska ekvationer
- Kinesiska restsatsen

## Induktion

Induktion är när vi visar ett grundfall och därefter använder *dominoeffekten* (om det gäller för  $k$  gäller det även för  $k + 1$ ) för att visa resten.

**Exempel 1.** Låt  $F_i$  vara det  $i$ -te fibonaccitalet så att  $F_1 = F_2 = 1$ . Visa att 
$$\sum_{i=1}^n F_i^2 = F_n \cdot F_{n+1}$$

**Lösning.** Vi använder våra tre induktionssteg:

1. Påståendet gäller då  $n = 1$  ty  $1^2 = 1 \cdot 1$ .

2. Antag att  $\sum_{i=1}^k F_i^2 = F_k \cdot F_{k+1}$

3. Nu får vi att  $\sum_{i=1}^{k+1} F_i^2 = F_{k+1}^2 + \sum_{i=1}^k F_i^2 = F_{k+1}^2 + F_k \cdot F_{k+1} = F_{k+1}(F_k + F_{k+1}) = F_{k+1} \cdot F_{k+2}$ , vilket vi ville visa.

Enligt induktionsprincipen gäller nu påståendet för alla  $n$ .

**Uppgift 1.** Visa att  $\sum_{i=1}^{n-1} \frac{i}{(i+1)!} = 1 - \frac{1}{n!}$ .

## Euklides algoritm

Vi börjar med att införa en beteckning.

**Definition 1.** Den största gemensamma delaren till några heltal  $a_1, a_2, \dots, a_n$  är det största talet som delar  $a_i$  för alla  $1 \leq i \leq n$ . Vi betecknar detta tal med  $(a_1, a_2, \dots, a_n)$ ,  $sgd(a_1, a_2, \dots, a_n)$  eller  $gcd(a_1, a_2, \dots, a_n)$ .

**Lemma 1.** Om  $d = (a, b)$  så kan  $a$  och  $b$  skrivas som  $a = a_1 \cdot d$  respektive  $b = b_1 \cdot d$  och  $(a_1, b_1) = 1$ .

*Bevis.* Eftersom  $d$  delar både  $a$  och  $b$  kan vi göra omskrivningen. Antag nu att  $(a_1, b_1) = d_1$ . Eftersom  $d_1$  delar  $a_1$  och  $b_1$  så delar  $dd_1$   $a$  och  $b$ . Men  $d$  är den största gemensamma delaren till  $a$  och  $b$  alltså måste  $d_1 = 1$ .  $\square$

**Lemma 2.** Om  $a = q \cdot b + r$  så är  $(a, b) = (b, r)$ .

*Bevis.* Låt  $d_1 = (a, b)$  och  $d_2 = (b, r)$ . Eftersom  $d_1$  delar  $a$  och  $b$  och  $a = q \cdot b + r$  så måste  $d_1$  även dela  $r$ . Alltså delar  $d_1$  både  $b$  och  $r \rightarrow d_1 \leq d_2$  ty  $d_2$  är den största gemensamma delaren till  $b$  och  $r$ . På liknande sätt fås att  $d_2 \leq d_1$  och således är  $d_1 = d_2$ .  $\square$

Nu är vi redo att ta oss an *Euklides algoritm*. Vi ska nu försöka att hitta  $(a_1, a_2)$ . Låt  $a_i$  och  $q_i$  vara heltal för alla  $i$  samt låt  $a_1 \geq a_2 > a_3 > \dots > a_{k+1}$ .

$$a_1 = q_1 a_2 + a_3$$

$$a_2 = q_2 a_3 + a_4$$

...

$$a_k = q_k a_{k+1}$$

Nu har vi fått  $(a_k, a_{k+1}) = a_{k+1}$  ty  $a_{k+1}$  delar  $a_k$ . Enligt Lemma 1 är alltså  $(a_1, a_2) = (a_2, a_3) = \dots = (a_k, a_{k+1}) = a_{k+1}$ .

## Bezouts identitet

Om vi går baklänges i Euklides algoritim får vi

$$a_3 = a_1 - q_1 a_2$$

$$a_4 = a_2 - q_2 a_3 = a_2(1 + q_1 q_2) - q_1 a_1$$

...

$$a_{k+1} = u a_1 + v a_2, \text{ för några heltal } u, v.$$

Alltså kan vi skriva  $(a_1, a_2)$  som  $u a_1 + v a_2$  för några heltal  $u, v$ . Speciellt gäller att om två tal  $m, n$  är relativt prima (dvs.  $(m, n) = 1$ ) så finns det heltal  $u, v$  sådana att  $um + vn = 1$ .

**Lemma 3.** Om  $n$  delar  $ab$  och  $(n, a) = 1$  så är  $b$  delbart med  $n$ .

*Bevis.* Vi använder Bezouts identitet och får att det existerar heltal  $u, v$  så att

$$un + va = 1 \Leftrightarrow unb + vab = b.$$

Men nu ser vi att  $n$  delar vänstersidan och således måste  $n$  dela  $b$ . □

**Exempel 2.** Låt  $F_n = 2^{2^n} + 1$ . Visa att  $(F_m, F_n) = 1$  för alla  $m \neq n$ .

**Lösning.** Antag först att  $m > n$  och låt  $(F_m, F_n) = d$ . Eftersom

$$2^{2^{n+1}} - 1 = (2^{2^n} + 1)(2^{2^n} - 1)$$

måste  $d$  dela  $2^{2^{n+1}} - 1$ . Mha induktion får vi nu att  $2^{2^n} - 1$  är delbart med  $d$ . Eftersom att  $d$  delar både  $2^{2^n} - 1$  och  $2^{2^n} + 1$  måste  $d$  även dela  $(2^{2^n} + 1) - (2^{2^n} - 1) = 2$ . Men  $2^{2^n} + 1$  är udda och således måste  $d = 1$ , vsb.

**Uppgift 2.** Visa att om  $a$  delar  $c$ ,  $b$  delar  $c$  och  $(a, b) = 1$  så är  $c$  delbart med  $ab$ .

## Primaltal

**Definition 2.** Ett primtal är ett heltal,  $p \geq 2$ , vars enda positiva delare är 1 och  $p$ .

**Sats 1.** Det finns oändligt många primtal.

*Bevis.* Antag att det finns ändligt många primtal och att de är  $p_1, p_2, \dots, p_n$ . Vi betraktar nu talet  $P = p_1 p_2 \dots p_n + 1$ . Nu ser vi att det är inte delbart med något av talen  $p_1, p_2, \dots, p_n$  och således är  $P$  antingen ett primtal själv eller delbart med något primtal som inte finns bland  $p_1, p_2, \dots, p_n$  vilket är en motsägelse.  $\square$

**Exempel 3.** Hitta alla positiva heltal  $x, y$  och primtal  $p$  sådana att  $\frac{1}{x} - \frac{1}{y} = \frac{1}{p}$ .

**Lösning.** Uppgiften är ekvivalent med att  $p(y - x) = xy$ . Alltså är antingen  $x$  eller  $y$  delbart med  $p$ .

1. Antag först att  $x$  är delbart med  $p \Leftrightarrow x = x_1 p$ . Det medför att  $y = x_1 y + p x_1 > y$ , motsägelse.
2. Antag sedan att  $y$  är delbart med  $p \Leftrightarrow y = y_1 p \Rightarrow y_1 p - x = x y_1 \Leftrightarrow x = y_1(p - x) \Rightarrow y_1$  delar  $x \Leftrightarrow x = x_1 y_1 \Rightarrow x_1(1 + y_1) = p \Leftrightarrow x_1 = 1, y_1 = p - 1 \Rightarrow x = p - 1, y = p^2 - p$ .

**Uppgift 3.** Hitta alla  $p$  sådana att  $p, p + 10$  och  $p + 20$  är primtal.

**Uppgift 4.** Hitta alla positiva heltal  $x, y$  så att  $\sqrt{x} + \sqrt{y} = \sqrt{2009}$ .

## Modulär räkning och restklasser

**Definition 3.** Vi säger att två tal  $a$  och  $b$  är kongruenta modulo  $m$  om  $(a - b)$  är delbart med  $m$ . Vi betecknar detta med  $a \equiv b \pmod{m}$ .

**Sats 2.** För alla heltal  $a, b, m$  gäller att

1.  $a \equiv a \pmod{m}$
2. Om  $a \equiv b \pmod{m}$  och  $b \equiv c \pmod{m}$  så är  $a \equiv c \pmod{m}$
3. Om  $a_1 \equiv b_1 \pmod{m}$  och  $a_2 \equiv b_2 \pmod{m}$  så är  $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$
4. Om  $a \equiv b \pmod{m} \Rightarrow ac \equiv bc \pmod{m}$  (Observera att omvändningen inte alltid gäller)
5. Om  $a \equiv b \pmod{m}$  så är  $a^k \equiv b^k \pmod{m}$  för alla positiva heltal  $k$
6. Om  $a \equiv b \pmod{m}$  och  $f(n)$  är ett polynom med heltalskoefficienter så är  $f(a) \equiv f(b)$
7. Om  $a \equiv b \pmod{m}$  så är  $(a, m) = (b, m)$

8. Om  $ak \equiv bk \pmod{m}$  så är  $a \equiv b \pmod{\frac{m}{(m,k)}}$

Bevis lämnas som övning åt läsaren.

**Exempel 4.** Visa att  $3^{2009} \equiv 3 \pmod{10}$ .

**Lösning.** Vi noterar att  $3^4 = 81 \equiv 1 \pmod{10}$ . Nu gör vi omskrivningen

$$3^{2009} = (3^4)^{502} \cdot 3 \equiv 1^{502} \cdot 3 \equiv 3 \pmod{10},$$

vilket ger vårt önskade resultat.

**Uppgift 5.** Visa att  $(a+b)^p \equiv a^p + b^p \pmod{p}$  för alla heltal  $a, b$  och primtal  $p$ .

**Uppgift 6.** Verifiera att följande kongruenser gäller för alla heltal  $n$ :

1.  $n^2 \equiv 0$  eller  $1 \pmod{3}$  och  $\pmod{4}$
2.  $n^2 \equiv -1, 0$  eller  $1 \pmod{5}$
3.  $n^2 \equiv 0, 1, 2$  eller  $4 \pmod{7}$
4.  $n^2 \equiv 0, 1$  eller  $4 \pmod{8}$
5.  $n^3 \equiv -1, 0$  eller  $1 \pmod{9}$
6.  $n^4 \equiv 0$  eller  $1 \pmod{16}$

**Uppgift 7.** Hitta alla heltal  $x, y, z$  sådana att

1.  $x^2 + y^2 = 3^{2016}$
2.  $x^4 + y^4 + z^4 = 2^{2016}$

**Exempel 5.** (IMO Shortlist 2002, N1) Vilket är det minsta  $t$  sådant att  $x_1^3 + x_2^3 + \dots + x_t^3 = 2002^{2002}$  har en lösning?

**Lösning.** Vi börjar med att notera att

$$(10 \cdot 2002^{667})^3 + (10 \cdot 2002^{667})^3 + (2002^{667})^3 + (2002^{667})^3 = 2002^{2002}$$

Vår hypotes är alltså att 4 är det minsta  $t$  som kan ge lösning. Eftersom vi har kuber så säger uppgift 6.5 att vi nog bör kolla modulo 9.

$$2002^{2002} \equiv 4^{2002} \equiv (4^3)^{667} \cdot 4 \equiv 1 \cdot 4 \equiv 4 \pmod{9}$$

Men om  $t < 4$  kan vi alltså inte få någon lösning eftersom  $x^3 \equiv -1, 0$  eller  $1 \pmod{9}$ .

## Fermats lilla sats och Eulers sats

**Sats 3.** (Fermats lilla sats) För alla heltal  $a$  och primtal  $p$  är  $a^p \equiv a \pmod{p}$ .

*Bevis.* Vi använder uppgift 5. Mha induktion kan man visa att

$$(x_1 + x_2 + \dots + x_n)^p = x_1^p + x_2^p + \dots + x_n^p \pmod{p}$$

genom att använda uppgift 5 upprepade gånger. Med  $n = a$  och  $x_1 = x_2 = \dots = x_a = 1$  får vi

$$a^p = (1 + 1 + \dots + 1)^p \equiv 1^p + 1^p + \dots + 1^p = a \pmod{p}$$

□

**Sats 4.** (Eulers sats) Låt  $\phi(n)$  beteckna antalet tal som är relativt prima med och mindre än  $n$ . Då är  $a^{\phi(n)} \equiv 1 \pmod{n}$  för alla  $a$  sådana att  $(a, n) = 1$ .

För bevis: se internet.

Anmärkning: Då  $n$  är ett primtal är Eulers sats exakt samma sak som Fermats lilla sats.

**Exempel 6.** Låt  $\{a_i\}_{i \geq 1}$  vara en följd av heltal som ges av  $a_n = 2^n + 3^n + 6^n - 1$ . Hitta alla positiva heltal  $m$  sådana att  $(m, a_n) = 1$  för alla  $n$ .

**Lösning.** Vi ser först att t.ex.  $a_2$  är delbart med både 2 och 3. Vi ska nu visa att det för varje primtal  $p$  finns ett  $n$  sådant att  $a_n$  är delbart med  $p$ . Vi betraktar  $6 \cdot a_{p-2}$  och antar att  $p > 3$ . Då är  $(6, p) = 1$  vilket innebär att om  $p$  delar  $6a_{p-2}$  så delar det även  $a_{p-2}$ . Men

$$\begin{aligned} 6a_{p-2} &= 6 \cdot 2^{p-2} + 6 \cdot 3^{p-2} + 6 \cdot 6^{p-2} - 6 = \\ &= 3(2^{p-1} - 1) + 2(3^{p-1} - 1) + (6^{p-1} - 1) \equiv 0 \pmod{p} \end{aligned}$$

(Kongruensen kommer direkt av Fermats lilla sats.) Alltså har vi att inget primtal är relativt primt med alla talen i sekvensen och således kommer inget sammansatt tal vara det heller. Alltså blir 1 det enda  $m$  sådant att  $(m, a_n) = 1$  för alla  $n$ .

**Uppgift 8.** Låt  $p$  och  $q$  vara olika primtal och låt  $n = p^{q-1} + q^{p-1} - 1$ . Visa att  $pq$  delar  $n$ .

## Diofantiska ekvationer

Diofantiska ekvationer är ekvationer där vi enbart är intresserade av heltalslösningar. Ett vanligt exempel är en linjär diofantisk ekvation på formen:

$$a_1x_1 + a_2x_2 + \dots + a_nx_n = b \quad (1)$$

**Sats 5.** (1) har lösningar om och endast om  $d = (a_1, a_2, \dots, a_n)$  delar  $b$ .

*Bevis.* Låt  $a'_i = \frac{a_i}{d}$  för alla  $1 \leq i \leq n$  och  $b' = \frac{b}{d}$ . Nu är  $(a'_1, a'_2, \dots, a'_n) = 1$  och Bezouts identitet (fast generaliserad) ger att det finns  $x'_1, x'_2, \dots, x'_n$  sådana att  $x'_1a'_1 + x'_2a'_2 + \dots + x'_na'_n = 1$ . Med  $x_i = x'_i \cdot b'$ ,  $1 \leq i \leq n$  ges lösningar till (1).  $\square$

**Sats 6.** Om  $x_1 = c, x_2 = d$  är en lösning till det linjära ekvationssystemet

$$a_1x_1 + a_2x_2 = b \quad (2)$$

ges alla lösningar av  $x_1 = c + a_2t, x_2 = d - a_1t$ , där  $t$  är ett reellt tal.

*Bevis.* Vi subtraherar  $a_1c + a_2d = b$  från ekvationen i (2) och får

$$a_1(x_1 - c) + a_2(x_2 - d) = 0.$$

Vi variabelsubstituerar  $t = \frac{x_1 - c}{a_2}$ , dvs.  $x_1 = c + a_2t$  och får

$$a_1a_2t + a_2(x_2 - d) = 0 \Leftrightarrow x_2 = d - a_1t,$$

vilket var vad vi skulle komma fram till.  $\square$

**Exempel 7.** Hitta alla Pythagoriska tripplar, dvs. alla heltalslösningar till  $x^2 + y^2 = z^2$ .

**Lösning.** Låt  $(x, y) = k$  och sätt  $x = ka, y = kb, z = kc$ . Nu har vi att  $a, b$  och  $c$  är parvis relativt prima ty  $(a, b) = 1$ . Vi antar nu att  $a$  är jämnt och att  $b$  och  $c$  är udda (både  $a$  och  $b$  kan inte vara udda pga modulo 4). Vi ska nu visa följande lemma.

**Lemma 4.** Vi ska nu visa att  $\frac{c+b}{2}$  och  $\frac{c-b}{2}$  är relativt prima.

*Bevis.* Antag att  $(\frac{c+b}{2}, \frac{c-b}{2}) = d$ . Eftersom  $d$  delar både  $\frac{c+b}{2}$  och  $\frac{c-b}{2}$  så delar  $d$  även  $\frac{c+b}{2} + \frac{c-b}{2} = c$  och  $\frac{c+b}{2} - \frac{c-b}{2} = b$ . Men  $(b, c) = 1$  och således är  $d = 1$ .  $\square$

Vi flyttar över  $b^2$  till andra sidan och faktorerar:

$$\left(\frac{a}{2}\right)^2 = \frac{c+b}{2} \cdot \frac{c-b}{2}.$$

Men eftersom  $\left(\frac{c+b}{2}, \frac{c-b}{2}\right) = 1$  och deras produkt är en kvadrat måste både  $\left(\frac{c+b}{2}\right)$  och  $\left(\frac{c-b}{2}\right)$  vara heltalskvadrater. Med  $\left(\frac{c+b}{2} = m^2\right)$  och  $\left(\frac{c-b}{2} = n^2\right)$  ges lösningarna  $a = 2mn$ ,  $b = m^2 - n^2$  och  $c = m^2 + n^2$  ges alla lösningar till ekvationen

$$a^2 + b^2 = c^2, \text{ där } (a, b, c) = 1.$$

Till vår ursprungsekvation ges alltså alla lösningar av

$$x = 2kmn, y = k(m^2 - n^2) \text{ och } z = k(m^2 + n^2).$$

## Kinesiska restsatsen

Den kinesiska restsatsen är en väldigt kraftfull sats som visar den entydiga existensen i ett kongruenskvationssystem. Den användes bland annat i bevisets för Fermats stora sats (även kallad Fermats sista sats) och används flitigt i olika tävlingar.

**Sats 7.** *Låt  $x, a_1, a_2, \dots, a_k$  vara heltal och  $n_1, n_2, \dots, n_k$  vara parvis relativt prima positiva heltal. Då har*

$$x \equiv a_1 \pmod{n_1}$$

$$x \equiv a_2 \pmod{n_2}$$

...

$$x \equiv a_k \pmod{n_k}$$

*en entydig lösning  $\pmod{n_1 n_2 \dots n_k}$ .*

Beviset är ganska meckigt men straight forward och kan läsas på internet.

**Uppgift 9.** (USAMO 2008, uppgift 1, OBS! Mycket svår!)

Visa att det för alla  $n$  går att hitta heltal  $k_1, k_2, \dots, k_n$ , alla större än 1, sådana att  $k_1 k_2 \dots k_n - 1$  är produkten av två på varandra följande tal. (Tips: Försök först reducera problemet till att visa att det finns oändligt många primtal som delar  $m^2 + m + 1$  för något  $m$ .)