Matte och Programmeringsläger för Tjejer
Talteori 1

Louise Westin

10-12 maj 2019

Vi kommer att gå igenom

- Induktion
- Euklides algoritm
- Bezouts identitet
- Primtalen - hur använder vi dem smart?
- Aritmetikens fundamentalsats
- Modulär räkning och restklasser

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 $a_1, a_2, ..., a_n$ är det största talet som delar a_i för alla $1 \leq i \leq n$. Vi betecknar detta tal med $(a_1, a_2, ...a_n)$, $sgd(a_1, a_2, ...a_n)$ eller $gcd(a_1, a_2, ...a_n)$.

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 $d_1 = 1$. □

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 $d_1 = d_2$. □

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 $a_1 \geq a_2 > a_3 > ... > a_{k+1}$.

$$a_1 = q_1 a_2 + a_3$$

$$a_2 = q_2 a_3 + a_4$$

$$...$$

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

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

Uppgift 2. Använd Euklides algoritm för att beräkna:

1. gcd(723, 42)
2. gcd(189, 35)
3. gcd(832, 257)

Bezouts identitet

Om vi *går baklänges* i Euklides algoritm får vi

$$a_3 = a_1 - q_1 a_2$$

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

$$\ldots$$

$$a_{k+1} = ua_1 + va_2, \text{ för några heltal } u, v.$$

Alltså kan vi skriva (a_1, a_2) som $ua_1 + va_2$ 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 $2^{2^m} - 1$ är delbart med d. Eftersom att d delar både $2^{2^m} - 1$ och $2^{2^m} + 1$ måste d även dela $(2^{2^m} + 1) - (2^{2^m} - 1) = 2$. Men $2^{2^m} + 1$ är udda och således måste $d = 1$, vsb.

Uppgift 3. Visa att om a delar c, b delar c och $(a, b) = 1$ så är c delbart med ab.

Primtal

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 $p_1, p_2, ...p_n$. Vi betraktar nu talet $P = p_1p_2...p_n + 1$. Nu ser vi att det är inte delbart med något av talen $p_1, p_2, ..., p_n$ och således är P antingen ett primtal själv eller delbart med något primtal som inte finns bland $p_1, p_2, ..., p_n$ vilket är en motsägelse. □

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 $p \Leftrightarrow x = x_1p$. Det medför att $y = x_1y + px_1 > y$, motsägelse.

2. Antag sedan att y är delbart med $p \Leftrightarrow y = y_1p \Rightarrow y_1p - x = xy_1 \Leftrightarrow x = y_1(p - x) \Rightarrow y_1$ delar $x \Leftrightarrow x = x_1y_1 \Rightarrow x_1(1 + y_1) = p \Leftrightarrow x_1 = 1, y_1 = p - 1 \Rightarrow x = p - 1, y = p^2 - p$.

Uppgift 4. Hitta alla p sådana att p, $p + 10$ och $p + 20$ är primtal.

Uppgift 5. 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 omm $(a - b)$ 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* $f(a) = f(b)$

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 $3^{2009} = 3 \pmod{10}$.

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

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

vilket ger vårt önskade resultat.

Uppgift 6. Bestäm eller visa följande:

1. Bestäm alla positiva heltal n för vilka $2^n - 1$ är delbart med 7.
2. Visa att det inte finns något positivt heltal n för vilket $2^n + 1$ är delbart med 7.

Uppgift 7. Visa att $(a+b)^p \equiv a^p + b^p$ (mod p) för alla heltal a, b och primtal p.

Uppgift 8. 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 9. 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 $x_1^3 + x_2^3 + ... + x_t^3 = 2002^{2002}$ 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 8.5 att vi nog bör kolla modulo 9.

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

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