Primtal

Jonathan Nilsson och Magnus Jakobsson

Malmö Universitet

8 Mars 2022

Passen

Vi ses jämna veckor under vårterminen. Varje pass har ett unikt tema, exempelvis

- Primtal
- Knutteori
- Spelteori
- Talföljder
- Grafteori
- Kardinalitet
- Topologi

Vi laddar upp förberedelseuppgifter en vecka innan varje pass.

Idag - Talteori och primtal

- Presentation
- Kort genomgång av förberedelseuppgifter
- Problemlösning
- Genomgång av lösningar

Primtal

Definition

Ett **primtal** är ett heltal större än 1 som inte kan skrivas som en produkt av två mindre positiva heltal.

Primtal

Definition

Ett **primtal** är ett heltal större än 1 som inte kan skrivas som en produkt av två mindre positiva heltal.

Alternativt: Ett positivt heltal p är ett primtal om det har precis två positiva delare, 1 och p.

Primtal

Definition

Ett **primtal** är ett heltal större än 1 som inte kan skrivas som en produkt av två mindre positiva heltal.

Alternativt: Ett positivt heltal p är ett primtal om det har precis två positiva delare, 1 och p.

De första primtalen

2, 3, 5, 7

Primtal

Definition

Ett **primtal** är ett heltal större än 1 som inte kan skrivas som en produkt av två mindre positiva heltal.

Alternativt: Ett positivt heltal p är ett primtal om det har precis två positiva delare, 1 och p.

De första primtalen

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97

Primtal

Definition

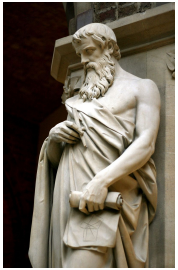
Ett **primtal** är ett heltal större än 1 som inte kan skrivas som en produkt av två mindre positiva heltal.

Alternativt: Ett positivt heltal p är ett primtal om det har precis två positiva delare, 1 och p.

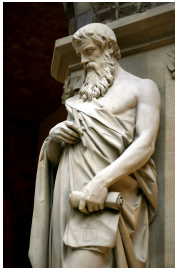
De första primtalen

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, ...

Hur många primtal finns det?



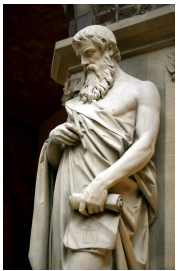
Hur många primtal finns det?



Sats (Euklides ca 300 f.kr.)

Det finns oändligt många primtal.

Hur många primtal finns det?



Sats (Euklides ca 300 f.kr.)

Det finns oändligt många primtal.

Bevis: Antag att det bara finns ändligt många primtal $p_1, p_2, \ldots, p_n$. Låt $m = p_1 \cdot p_2 \cdots p_n + 1$. Då är inget av talen $p_1, p_2, \ldots, p_n$ en faktor till m, så m måste själv vara ett primtal. Motsägelse!

Eratosthenes såll

Eratosthenes ca 200 f.kr.

Hittade en algoritm för att hitta alla primtal under ett givet tal. Med en dator är denna metod effektiv för att hitta alla primtal under några miljarder.

Eratosthenes såll - algoritm

1	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	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72
73	74	75	76	77	78	79	80	81	82	83	84
85	86	87	88	89	90	91	92	93	94	95	96

Eratosthenes såll - algoritm

1	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	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72
73	74	75	76	77	78	79	80	81	82	83	84
85	86	87	88	89	90	91	92	93	94	95	96

Vi stryker alla primtal delbara med 2

Eratosthenes såll - algoritm

1	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	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72
73	74	75	76	77	78	79	80	81	82	83	84
85	86	87	88	89	90	91	92	93	94	95	96

Vi stryker alla primtal delbara med 2 och 3

Eratosthenes såll - algoritm

1	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	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72
73	74	75	76	77	78	79	80	81	82	83	84
85	86	87	88	89	90	91	92	93	94	95	96

Vi stryker alla primtal delbara med 2 och 3 och 5

Eratosthenes såll - algoritm

1	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	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72
73	74	75	76	77	78	79	80	81	82	83	84
85	86	87	88	89	90	91	92	93	94	95	96

Vi stryker alla primtal delbara med 2 och 3 och 5 och 7. Resten är primtal!

Eratosthenes såll - Pythonprogram

```python
def Eratosthenes(n):
    sammansatta={0,1}
    i=2
    while i*i < n+1:
        sammansatta|={k*i for k in range(2,1+n//i)}
        i+=1
    return set(range(n))-sammansatta
```

```
In [24]: Eratosthenes(100)
Out[24]:
{2,
 3,
 5,
 7,
 11,
 13,
```

Programmet hittar alla primtal under 10 miljoner på ca 20 sekunder.

Eratosthenes såll - Pythonprogram

```python
def Eratosthenes(n):
    sammansatta={0,1}
    i=2
    while i*i < n+1:
        sammansatta|={k*i for k in range(2,1+n//i)}
        i+=1
    return set(range(n))-sammansatta
```

```
In [24]: Eratosthenes(100)
Out[24]:
{2,
 3,
 5,
 7,
 11,
 13,
```

Programmet hittar alla primtal under 10 miljoner på ca 20 sekunder.
För långsamt då n har mer än ~ 10 siffror, även för superdatorer.

Primtalstest

Hur kan man testa om ett visst tal är ett primtal?

Primtalstest

Hur kan man testa om ett visst tal är ett primtal?

Fermats primtalstest

Om p är ett primtal så gäller $p|(a^p - a)$ för alla heltal a.

Primtalstest

Hur kan man testa om ett visst tal är ett primtal?

Fermats primtalstest

Om p är ett primtal så gäller $p|(a^p - a)$ för alla heltal a.
Så om $p \not|(a^p - a)$ för något a kan p ej vara ett primtal.

Primtalstest

Hur kan man testa om ett visst tal är ett primtal?

Fermats primtalstest

Om p är ett primtal så gäller $p|(a^p - a)$ för alla heltal a.
Så om $p \not|(a^p - a)$ för något a kan p ej vara ett primtal.

$6 \not|(2^6 - 2)$ så 6 är inte ett primtal.

Primtalstest

Hur kan man testa om ett visst tal är ett primtal?

Fermats primtalstest

Om p är ett primtal så gäller $p|(a^p - a)$ för alla heltal a.
Så om $p \not|(a^p - a)$ för något a kan p ej vara ett primtal.

$6 \not|(2^6 - 2)$ så 6 är inte ett primtal.
$143 \not|(2^{143} - 2)$ så 143 är inte ett primtal.

Primtalstest

Hur kan man testa om ett visst tal är ett primtal?

Fermats primtalstest

Om p är ett primtal så gäller $p|(a^p - a)$ för alla heltal a.
Så om $p \not|(a^p - a)$ för något a kan p ej vara ett primtal.

$6 \not|(2^6 - 2)$ så 6 är inte ett primtal.
$143 \not|(2^{143} - 2)$ så 143 är inte ett primtal.

Primtalstestning

Med liknande test finns det snabba algoritmer som testar om ett på givet tal på ett par tuset siffror är ett primtal.

Primtalstest

Hur kan man testa om ett visst tal är ett primtal?

Fermats primtalstest

Om p är ett primtal så gäller $p|(a^p - a)$ för alla heltal a.
Så om $p \not|(a^p - a)$ för något a kan p ej vara ett primtal.

$6 \not|(2^6 - 2)$ så 6 är inte ett primtal.
$143 \not|(2^{143} - 2)$ så 143 är inte ett primtal.

Primtalstestning

Med liknande test finns det snabba algoritmer som testar om ett på givet tal på ett par tuset siffror är ett primtal. Observera att testet inte säger vad faktorerna är!

Det största kända primtalet

I mars 2022 är det största kända primtalet

$$2^{82,589,933} - 1$$

Talet har 24 miljoner siffror

Del II

Faktorisering

Primtalsfaktorisering

Aritmetikens fundamentalsats

Varje positivt heltal kan faktoriseras på ett unikt sätt som en produkt av primtal.

Primtalsfaktorisering

Aritmetikens fundamentalsats

Varje positivt heltal kan faktoriseras på ett unikt sätt som en produkt av primtal.

$$70 = 2 \cdot 5 \cdot 7$$

Primtalsfaktorisering

Aritmetikens fundamentalsats

Varje positivt heltal kan faktoriseras på ett unikt sätt som en produkt av primtal.

$$70 = 2 \cdot 5 \cdot 7$$

$$72 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 = 2^3 \cdot 3^2$$

Primtalsfaktorisering

Aritmetikens fundamentalsats

Varje positivt heltal kan faktoriseras på ett unikt sätt som en produkt av primtal.

$$70 = 2 \cdot 5 \cdot 7$$

$$72 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 = 2^3 \cdot 3^2$$

$$29031942 = 2 \cdot 3 \cdot 2 \cdot 3 \cdot 3 = 2^3 \cdot 3^2 \cdot 1213 \cdot 3989$$

Primtalsfaktorisering

Aritmetikens fundamentalsats

Varje positivt heltal kan faktoriseras på ett unikt sätt som en produkt av primtal.

$$70 = 2 \cdot 5 \cdot 7$$

$$72 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 = 2^3 \cdot 3^2$$

$$29031942 = 2 \cdot 3 \cdot 2 \cdot 3 \cdot 3 = 2^3 \cdot 3^2 \cdot 1213 \cdot 3989$$

En motsägelse?

$17 \cdot 143 = 2431 = 13 \cdot 181$

Primtalsfaktorisering

Aritmetikens fundamentalsats

Varje positivt heltal kan faktoriseras på ett unikt sätt som en produkt av primtal.

$$70 = 2 \cdot 5 \cdot 7$$

$$72 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 = 2^3 \cdot 3^2$$

$$29031942 = 2 \cdot 3 \cdot 2 \cdot 3 \cdot 3 = 2^3 \cdot 3^2 \cdot 1213 \cdot 3989$$

En motsägelse?

$17 \cdot 143 = 2431 = 13 \cdot 181$

Ingen motsägelse $2431 = 11 \cdot 13 \cdot 17$ är primtalsfaktoriseringen.

Produkten av två stora tal

Talet 172535628569329134547437953692 79 är en produkt av två primtal. Vilka?

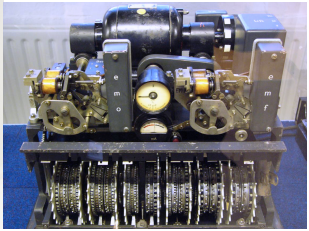
Produkten av två stora tal

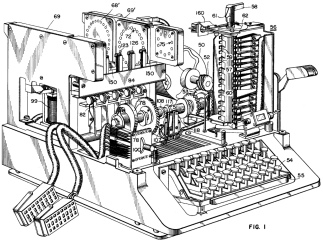
Talet 172535628569329134547437953692 79 är en produkt av två primtal. Vilka?

För tal på ett par hundra siffror är detta problem för svårt, även för datorer.

Kryptering

I princip all webbkommunikation krypteras enligt RSA eller ECC-protokollet. För att knäcka en RSA-kod måste man faktorisera ett tal på 512 bits, alltså ett tal på drygt 100 siffror.





Shors algoritm

Shors algoritm

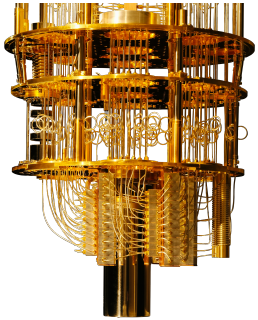
En algoritm som togs fram av Peter Shor 1994 som kan faktorisera stora primtal.

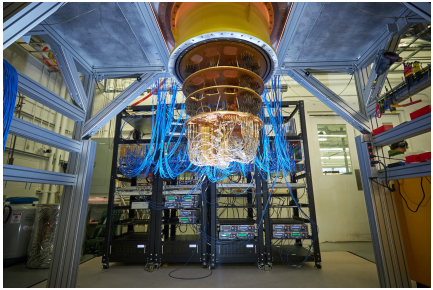
Shors algoritm

Shors algoritm

En algoritm som togs fram av Peter Shor 1994 som kan faktorisera stora primtal.

Problem: Algoritmen fungerar endast på kvantdatorer.





Högsta primtalsfaktoriseringar gjorda på kvantdatorer:
$21 = 3 \cdot 7$ år 2012, $1099551473989 = 1048589 \cdot 1048601$ år 2019.

Del IV

Teoretiska problem

Tvillingprimtal

Om p och $p+2$ båda är primtal kallas de **primtalstvillingar**.
Exempelvis är 11 och 13, eller 2027 och 2029 primtalstvillingar.

Tvillingprimtal

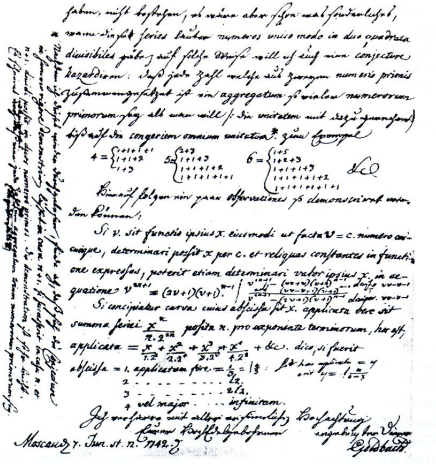
Om p och $p+2$ båda är primtal kallas de **primtalstvillingar**.
Exempelvis är 11 och 13, eller 2027 och 2029 primtalstvillingar.

Tvillingprimtalsförmodan (Twin prime conjecture)

Det finns oändligt många primtalstvillingar

De flesta matematiker tror att detta är sant men ingen har lyckats bevisa det ännu.

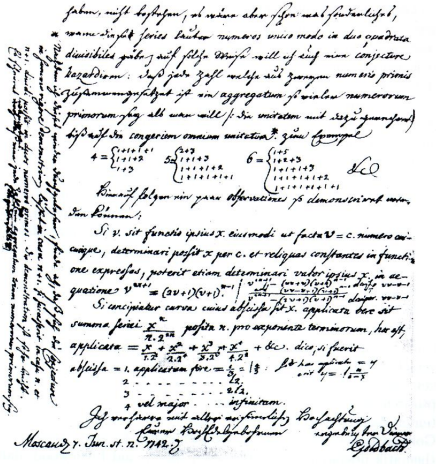
Goldbachs förmodan



Goldbachs förmodan (1742)

Varje jämnt tal större än 2 är summan av två primtal

Goldbachs förmodan

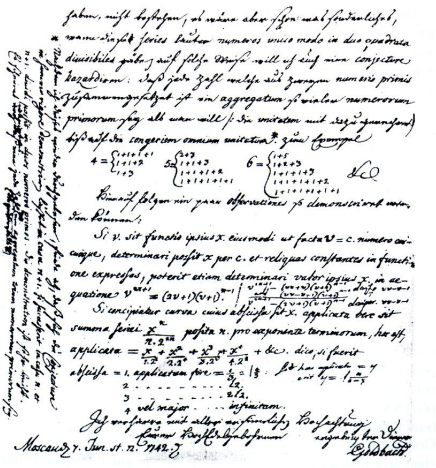


Goldbachs förmodan (1742)

Varje jämnt tal större än 2 är summan av två primtal

$$10 = 3 + 7 \qquad 52 = 47 + 5 \qquad 1000 = 317 + 683$$

Goldbachs förmodan



Goldbachs förmodan (1742)

Varje jämnt tal större än 2 är summan av två primtal

$$10 = 3 + 7 \qquad 52 = 47 + 5 \qquad 1000 = 317 + 683$$

Med datorer har man verifierat att förmodan gäller för alla jämna tal upp till $4 \cdot 10^{18}$, men detta är inget bevis!

Fermats primtal

Pierre de Fermat (1603-1665)

Fermats primtal

Pierre de Fermat (1603-1665)

Fermats primtalsförmodan (1600-talet)

$2^{2^n} + 1$ är ett primtal för varje heltal $n \geq 0$.

Fermats primtal

Pierre de Fermat (1603-1665)

Fermats primtalsförmodan (1600-talet)

$2^{2^n} + 1$ är ett primtal för varje heltal $n \geq 0$.

$2^{2^0} + 1 = 3$ $2^{2^1} + 1 = 5$ $2^{2^2} + 1 = 17$ $2^{2^3} + 1 = 257$ $2^{2^4} + 1 = 65537$ är alla primtal

Fermats primtal

Pierre de Fermat (1603-1665)

Fermats primtalsförmodan (1600-talet)

$2^{2^n} + 1$ är ett primtal för varje heltal $n \geq 0$.

$2^{2^0} + 1 = 3 \quad 2^{2^1} + 1 = 5 \quad 2^{2^2} + 1 = 17 \quad 2^{2^3} + 1 = 257 \quad 2^{2^4} + 1 = 65537$ är alla primtal

Euler visade 1732 att Fermat hade fel genom att beräkna att

$$2^{2^5} + 1 = 4294967297 = 641 \cdot 6700417.$$

Fermats primtal

Pierre de Fermat (1603-1665)

Fermats primtalsförmodan (1600-talet)

$2^{2^n} + 1$ är ett primtal för varje heltal $n \geq 0$.

$2^{2^0} + 1 = 3 \quad 2^{2^1} + 1 = 5 \quad 2^{2^2} + 1 = 17 \quad 2^{2^3} + 1 = 257 \quad 2^{2^4} + 1 = 65537$ är alla primtal

Euler visade 1732 att Fermat hade fel genom att beräkna att

$$2^{2^5} + 1 = 4294967297 = 641 \cdot 6700417.$$

Fråga som kvarstår: finns det fler Fermatprimtal än de ovan?

Frågor?