$p \to q,\ \neg r \to \neg q,\ \neg r \Rightarrow \neg p$

$p \to \neg q,\ \neg r \to q,\ p \Rightarrow r$

$a \vee b,\ c \wedge d,\ a \to \neg c \Rightarrow b$

	$p \to q$	Hyp.
	$\neg q \to \neg p$	Contrapositive 1.
	$\neg r \to \neg q$	Hyp
	$\neg r$	Hyp
	$\neg q$	Dir. Reas. 3, 4
	$\neg p$	Dir. Reas, 2, 5
	QED	

1.	$\neg r \to q$	hyp
2.	$\neg q \to r$	C.P. 1
3.	$p \to \neg q$	hyp
4.	p	hyp
5.	$\neg q$	Dir. Reas. 3, 4
6.	r	Dir. Reas. 2. 5.
	QED	
4.	$p \to r$	Chain Rule, 2, 3
5.	p	Hyp
6.	r	Dir. Reas, 4. 5.
	QED	

prove $a \vee b,\ c \wedge d,\ a \rightarrow \neg c \Rightarrow b$

Proof:

1. $a \vee b$ Hyp.
2. $a \rightarrow \neg c$ Hyp.
3. $c \rightarrow \neg a$ Contrapositive, 2.
4. $c \wedge d$ Hyp.
5. c Conjunctive Simplification
6. $\neg a$ Dir. Reas. 3.5.
7. b Disjunctive Simplification, 1, 6

QED

$p \to q,\ \neg r \to \neg q,\ \neg r \Rightarrow \neg p$

proof:

1.	p	Neg. of Conc.
2.	$p \to q$	Hyp
3.	q	Dir. reas. 1, 2
4.	$\neg r \to \neg q$	Hyp.
5.	$q \to r$	Cont. Pos. 4.
6.	r	Dir. reas. 3, 5
7.	$\neg r$	Hyp
	$\times$	6, 7

$\therefore \neg p$

QED

Prove: $p \to \neg q,\ \neg r \to q,\ p \Rightarrow r$

Proof:

1. $\neg r$ — Neg. of concl.
2. $\neg r \to q$ — Hyp.
3. q — Dir. Reas. 1, 2
4. $p \to \neg q$ — Hyp
5. p — Hyp
6. $\neg q$ — Dir. Reas. 4, 5

$\#$ 3, 6

$\therefore r$

QED

4. $p \to \neg q$ — Hyp
5. $q \to \neg p$ — C.P. 4
6. $\neg p$ — Dir. Reas. 3, 5
7. p — Hyp

$\#$ 6, 7

$\therefore r$

QED

Prove $a \vee b,\ c \wedge d,\ a \to \neg c \Rightarrow b$

Proof:

1.	$\neg b$	Neg. of concl.
2.	$a \vee b$	Hyp.
3.	a	Disj. simpl. 1, 2
4.	$a \to \neg c$	Hyp.
5.	$\neg c$	Dir. Reas. 3, 4
6.	$c \wedge d$	Hyp.
7.	c	Conj. simpl. 6
	$\times\!\!\times$	5, 7

$\therefore b$

QED

6. Let D be the prop "Students do well in discrete math"

Let H be the prop "Students study hard"

Let S be the prop "students skip classes"

Let W be the prop "students do well in courses"

$D \to H, W \to \neg S, H \to W \Rightarrow D \to \neg S$

Proof: 1. $D \to H$ Hyp

2. $H \to W$ Hyp

3. $D \to W$ Chain rule, 1,2

4. $W \to \neg S$ Hyp

5. $D \to \neg S$ Chain rule, 3,4

QED

Twin primes: 3, 5   11, 13   29, 31

Goldbach's Conjecture:

Any even number ≥ 4 can be written as the sum of 2 primes.

ex: $4 = 2+2$, $6 = 3+3$, $8 = 3+5$, $10 = 5+5$
$= 3+7$

$$10^{\left(10^{\left(10^{1{,}000{,}000{,}000{,}000}\right)}\right)}$$

$2^2 - 1 = 3$ $\quad$ $2^3 - 1 = 7$ $\quad$ $2^5 - 1 = 31$

$(2^2-1)\cdot(2^{2-1})$ $\quad$ $(2^3-1)(2^{3-1})$ $\quad$ $(2^5-1)(2^{5-1})$

$3 \cdot 2$ $\quad$ $7 \cdot 4$ $\quad$ $31 \cdot 16$

6 $\quad$ 28 $\quad$ 496

$\downarrow$ $\quad$ $\downarrow$

$1, 2, 3$ $\quad$ $1, 2, 4, 7, 14$

N is a perfect number if $N =$ the sum of all factors of N $(< N)$

Is there an odd perfect number?

$2^2-1=3$ $\quad$ $2^3-1=7$ $\quad$ $2^5-1=31$

$(2^2-1)\cdot(2^{2-1})$ $\quad$ $(2^3-1)(2^{3-1})$ $\quad$ $(2^5-1)(2^{5-1})$

$3\cdot 2$ $\quad$ $7\cdot 4$ $\quad$ $31\cdot 16$

6 $\quad$ 28 $\quad$ 496

$\downarrow$ $\quad$ $\downarrow$

1, 2, 3 $\quad$ 1, 2, 4, 7, 14

N is a perfect number if N = the sum of all factors of N (< N)

Is there an odd perfect number?

$$\frac{25 \div 5}{10 \div 5} = \frac{5}{2}$$

$5 = GCD(25, 10)$

---

if $GCD(a,b) = 1$, then a&b are called "relatively prime."

ex: 27, 32

If $GCD(a,b) = 1$, then we can find integers m, n such that $a \cdot m + b \cdot n = 1$

"Bézout's Theorem"

Euclid's Algorithm: alg. for finding GCD

ex: find GCD(735, 252) = 21

735 = $\underline{2}$ · 252 + $\underline{231}$

252 = $\underline{1}$ · 231 + $\underline{21}$

231 = $\underline{11}$ · 21 + $\underline{0}$

$GCD(100, 36)$

$100 = 4 \cdot 25$

$36 = 4 \cdot 9$

$100 = 2 \cdot 36 + 28$

$36 = \underline{1} \cdot 28 + \underline{8}$

$28 = \underline{3} \cdot 8 + 4$

$8 = \underline{2} \cdot 4 + \underline{0}$

$GCD(36, 100)$

$36 = \underline{0} \cdot 100 + \underline{36}$

$100 = \underline{\ \ } \cdot 36 + \underline{\ \ \ \ }$

$GCD(32,27) =$

$32 = \underline{1} \cdot 27 + \underline{5}$

$27 = \underline{5} \cdot 5 + \underline{2}$

$5 = \underline{2} \cdot 2 + \underline{1}$

$2 = \underline{2} \cdot 1 + \underline{0}$

Chinese Remainder theorem

ex: Suppose

$$
\begin{aligned}
x &\equiv 2 \pmod{3} \\
x &\equiv 3 \pmod{5} \\
x &\equiv 2 \pmod{7}
\end{aligned}
$$

$x \equiv 23$

Chinese Remainder theorem

ex: Suppose $$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{5} \\ x &\equiv 2 \pmod{7} \end{aligned}$$

$x \equiv 23$

Calculations

Modula

Modular Exponentiation

Ex: Calculate $3^{17} \pmod 7$

$3^1 \equiv 3$

$3^2 \equiv 9 \equiv 2$

$3^4 \equiv (3^2)^2 \equiv 2^2 \equiv 4$

$3^8 \equiv 4^2 \equiv 16 \equiv 2$

$3^{16} \equiv 2^2 \equiv 4$

$17 = 16 + 1$

$3^{17} = 3^{(16+1)} = 3^{16} \cdot 3^1$

$3^{17} \equiv 3^{16} \cdot 3^1$

$\equiv 4 \cdot 3$

$\equiv 12 \equiv 5$

Mon 20 Oct 2025, 13:32:46 Take a Photo ~ : bc — Konsole

Ex: Calculate 7^{100} (mod 10)

~ : bc — Konsole

File Edit View Bookmarks Plugins Settings Help

```
[2001] bc
bc 1.07.1
Copyright 1991-1994, 1997, 1998, 2000, 2004, 2006, 2008, 2012-2017 Free Software Foundation, Inc.
This is free software with ABSOLUTELY NO WARRANTY.
For details type `warranty'.
7^100
32344765096247579913446477691002168108572031989046254009338953313916\
91459636928060001
```

Ex: Calculate $7^{100} \pmod{10}$

$7^1 \equiv 7$

$7^2 \equiv 49 \equiv 9$

$7^4 \equiv 9^2 \equiv 81 \equiv 1$

$7^8 \equiv 1^2 \equiv 1$

$7^{16} \equiv 1^2 \equiv 1$

$7^{32} \equiv 1$

$7^{64} \equiv 1$

$100 = 64 + 32 + 4$

$$7^{100} \equiv 7^{(64+32+4)}$$

$$\equiv 7^{64} \cdot 7^{32} \cdot 7^{4}$$

$$\equiv 1 \cdot 1 \cdot 1$$

$$\equiv 1$$

Fermat's Little Theorem

If p is prime and $p \nmid a$

then $a^{p-1} \equiv 1 \pmod{p}$

ex: find $7^{222} \pmod{11}$

by FLT: $\boxed{7^{10} \equiv 1 \pmod{11}}$

$$7^{220} \equiv 7^{22\cdot 10} \equiv (7^{10})^{22}$$

$$\equiv 1^{22} \equiv 1$$

$$7^{220} \equiv 1$$

$$7^{221} \equiv 7\cdot 1 \equiv 7$$

$$7^{222} \equiv 7\cdot 7 \equiv 49 \equiv 5 \pmod{11}$$

Mon 20 Oct 2025, 13:39:12 Take a Photo ~ : bc — Konsole

~ : bc — Konsole

File Edit View Bookmarks Plugins Settings Help

```
Copyright 1991-1994, 1997, 1998, 2000, 2004, 2006, 2008, 2012-2017 Free Soft
ware Foundation, Inc.
This is free software with ABSOLUTELY NO WARRANTY.
For details type `warranty'.
7^222-5
40903915558252355961885564235233827390274916808670721972378015470397\
48510167086731647965490040420428497588553556624278606102559317203211\
8590958393531614633803778811048702555046770492868044
(7^222-5)/11
37185377780229414510805058395667115809340833462427929065798195882179\
53191060987937861786809127654934997807775960567526005547781197457465\
326450763048328603073070801004427505004251862988004.0000000000000000\
0000
```

$$7^{220} \equiv 7^{22\cdot 10} \equiv (7^{10})^{22} \equiv 1^{22} \equiv 1$$

$$7^{220} \equiv 1$$

$$7^{221} \equiv 7\cdot 1 \equiv 7$$

$$7^{222} \equiv 7\cdot 7 \equiv 49 \equiv 5 \pmod{11}$$

3,657,123,552 (mod 3)

$2 + 5\cdot 10 + 5\cdot 10^2 + 3\cdot 10^3 + 2\cdot 10^4 + 1\cdot 10^5 + \ldots,$

$\equiv 2 + 5\cdot 1 + 5\cdot 1^2 + 3\cdot 1^3 + 2\cdot 1^4 + 1\cdot 1^5 + \ldots$

$\equiv 2 + 5 + 5 + 3 + 2 + 1 + 7 + 5 + 6 + 3$

---

mod 9 $\quad 10 \equiv 1 \quad 10^2 \equiv 1^2 \equiv 1 \quad 10^3 \equiv 1^3 \equiv 1 \ldots,$

18, 27, 36, 45, 54, 63, 72, 81

MOD 11

$25751 =$

$$1 + 5 \cdot 10 + 7 \cdot 10^2 + 5 \cdot 10^3 + 2 \cdot 10^4$$

$$= 1 + 5 \cdot (-1) + 7 \cdot (-1)^2 + 5 \cdot (-1)^3 + 2 \cdot (-1)^4$$

$$= 1 - 5 + 7 - 5 + 2$$