# PRIMES

Def: an int $n > 1$ is prime if its only divisors are 1 & $n$. Otherwise, $n$ is composite.

Ex: 23, 7, 5, 101, 1993 are prime

25, 8, 24, 4, 6 are composite

**Fundamental Theorem of Arithmetic:**

A composite # $n$ can be factored uniquely as a product of primes.

ex: $50 = 2 \cdot 5 \cdot 5$

Prove $\sqrt{2} \neq \frac{a}{b}$, $a, b \in \mathbb{Z}$

Suppose $\sqrt{2} = \frac{a}{b}$

$$2 = \frac{a^2}{b^2}$$

$$2 \cdot b^2 = a^2$$

$$2 \cdot 2^{2n_1} q_2^{n_2} \cdots = 2^{2n_1} p_2^{2n_2} \cdots$$

$$2^{2n_1+1} \cdots = 2^{2n_1} \cdots$$

※

$a = p_1^{n_1} p_2^{n_2} p_3^{n_3} \cdots$

$a = 2^{n_1} \cdot p_2^{n_2} \cdot p_3^{n_3} \cdots$

$a^2 = 2^{2n_1} p_2^{2n_2} p_3^{2n_3} \cdots$

$b = 2^{n_1} q_2^{n_2} q_3^{n_3} \cdots$

$b^2 = 2^{2n_1} q_2^{2n_2} q_3^{2n_3} \cdots$

# Is it prime?

Trial Division: Is $n$ divisible by $2, 3, 4, \ldots, n-1$?

or this div. by primes

$2, 3, 4, \ldots, \sqrt{n}$

## Sieve of Eratosthenes

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| (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) |

# How many primes are there?

Prove: Suppose $n$ is the largest prime.

$n+1$ must be composite
$n+2$, $n+3$, etc.

---

$B = (2 \cdot 3 \cdot 5 \cdot 7 \cdot \ldots \cdot n) + 1$

Then $B > n$ so $B$ is composite.

$2 \nmid B$

$3 \nmid B$

$\ldots$

$n \nmid B$ $\therefore B$ is prime

$\not\exists$

# The PRIME NUMBER THEOREM

How many primes are there $\leq n$?

as $n \to \infty$, $\#\text{primes} \leq n \simeq \log_e(n)$

## Mersenne Primes $(2^p - 1)$

Is $2^p - 1$ prime if $p$ is prime?

$2^{\textcircled{2}} - 1 = 3$

$2^{\textcircled{3}} - 1 = 7$

$2^4 - 1 = 15$ X

$2^{\textcircled{5}} - 1 = 31$

$2^6 - 1 = 63$ X

$2^{\textcircled{7}} - 1 = 127$

$2^8 - 1 = 255$ X

$2^9 - 1 = 511$ X

# The PRIME NUMBER THEOREM

How many ~~primes~~ primes are there $\leq n$?

as $n \to \infty$, $\#\text{primes} \leq n \simeq \log_e(n)$

## Mersenne Primes $(2^p - 1)$

Is $2^p - 1$ prime if $p$ is prime?

$2^{\textcircled{2}} - 1 = 3$

$2^{\textcircled{3}} - 1 = 7$

$2^4 - 1 = 15$ X

$2^{\textcircled{5}} - 1 = 31$

$2^6 - 1 = 63$ X

$2^{\textcircled{7}} - 1 = 127$

$2^8 - 1 = 255$ X

$2^9 - 1 = 511$ X

# Perfect Numbers (71)

10 is div. by 1, 2, 5 $\quad 1+2+5 = 8 < 10$

24 is div. by 1, 2, 3, 4, 6, 8, 12 $\quad 1+2+3+4+6+8+12 = 36 > 24$

6 is div. by 1, 2, 3 $\quad 1+2+3 = 6$

28 is div. by 1, 2, 4, 7, 14 $\quad 1+2+4+7+14 = 28$

---

$6 = 3 \cdot 2 = (2^2 - 1)(2^1)$

$28 = 7 \cdot 4 = (2^3 - 1)(2^2)$

are there any odd perfect #s?

Twin primes: $n$, $n+2$ both prime

e.g. 3, 5

5, 7

11, 13

17, 19

29, 31

---

Goldbach's Conjecture: Any even # > 2 can be written as a sum of 2 primes.

$4 = 2+2$

$6 = 3+3$

$8 = 3+5$

$10 = 3+7$ $(= 5+5)$

$12 = 5+7$

$$\frac{p \to q \quad \neg p}{\neg q}$$

(fallacy of denying the hyp)

Let $p$ be the prop "I am teaching"

Let $q$ be the prop "I am breathing"

4a) prove $p \to q, \neg r \to \neg q, \neg r \Rightarrow \neg p$

$$\frac{\begin{array}{l} p \to q \\ \neg r \to \neg q \\ \neg r \end{array}}{\neg p}$$

Direct proof:

| | | |
|---|---|---|
| 1. | $p \to q$ | Hyp. |
| 2. | $\neg r \to \neg q$ | Hyp. |
| 3. | $\neg r$ | Hyp. |
| 4. | $\neg q$ | Detachment, 2.3. |
| 5. | $\neg p$ | Contrapositive, 1. 4. |

6 ∈ ED

Indirect proof

| | | |
|---|---|---|
| 1. | $p$ | Neg. of conclusion |
| 2. | $p \to q$ | Hyp. |
| 3 | $q$ | Detachment, 1.2. |
| 4. | $\neg r \to \neg q$ | Hyp |
| 5. | $r$ | Contrapositive, 3. 4. |
| 6. | $\therefore \neg p$ ✗ 6 ∈ ED | Hyp 5, 6 |

4c) Prove $a \vee b,\ c \wedge d,\ a \to \neg c \Rightarrow b$

Proof

| | | |
|---|---|---|
| 1. | $c \wedge d$ | hyp |
| 2. | $c$ | Conj. simpl. 1. |
| 3. | $a \to \neg c$ | hyp |
| 4. | $\neg a$ | Contrapositive, 2.3. |
| 5. | $a \vee b$ | hyp. |
| 6. | $b$ | disj. simpl |

QED

---

Proof: Assume $\neg b$ (Neg. of Concl.)

| | | |
|---|---|---|
| 2. | $a \vee b$ | hyp |
| 3. | $a$ | disj. simpl. 1, 2 |
| 4. | $a \to \neg c$ | hyp |
| 5. | $\neg c$ | detachment, 3, 4 |
| 6. | $c \wedge d$ | hyp |
| 7. | $c$ | conj. simp. 6 |
| | $\therefore b$ ✱ | 5, 7 |

QED

# Greatest Common Divisor (GCD)

ex: GCD(100, 15) = 5

GCD(21, 8) = 1 "21 & 8 are relatively prime"

GCD(100, 50) = 50

$\frac{10^{0} \div 5}{15 \div 5} = \frac{20}{3}$

Euclid's Algorithm:

GCD(100, 15)

$100 = \underline{6} \cdot 15 + \underline{10}$

$15 = \underline{1} \cdot 10 + \underline{5}$

$10 = \underline{2} \cdot (5) + \underline{0}$

↑ GCD

# Greatest Common Divisor (GCD)

ex: GCD(100, 15) = 5

GCD(21, 8) = 1 "21 & 8 are relatively prime"

GCD(100, 50) = 50

$\frac{10^{0} \div 5}{15 \div 5} = \frac{20}{3}$

---

Euclid's Algorithm:

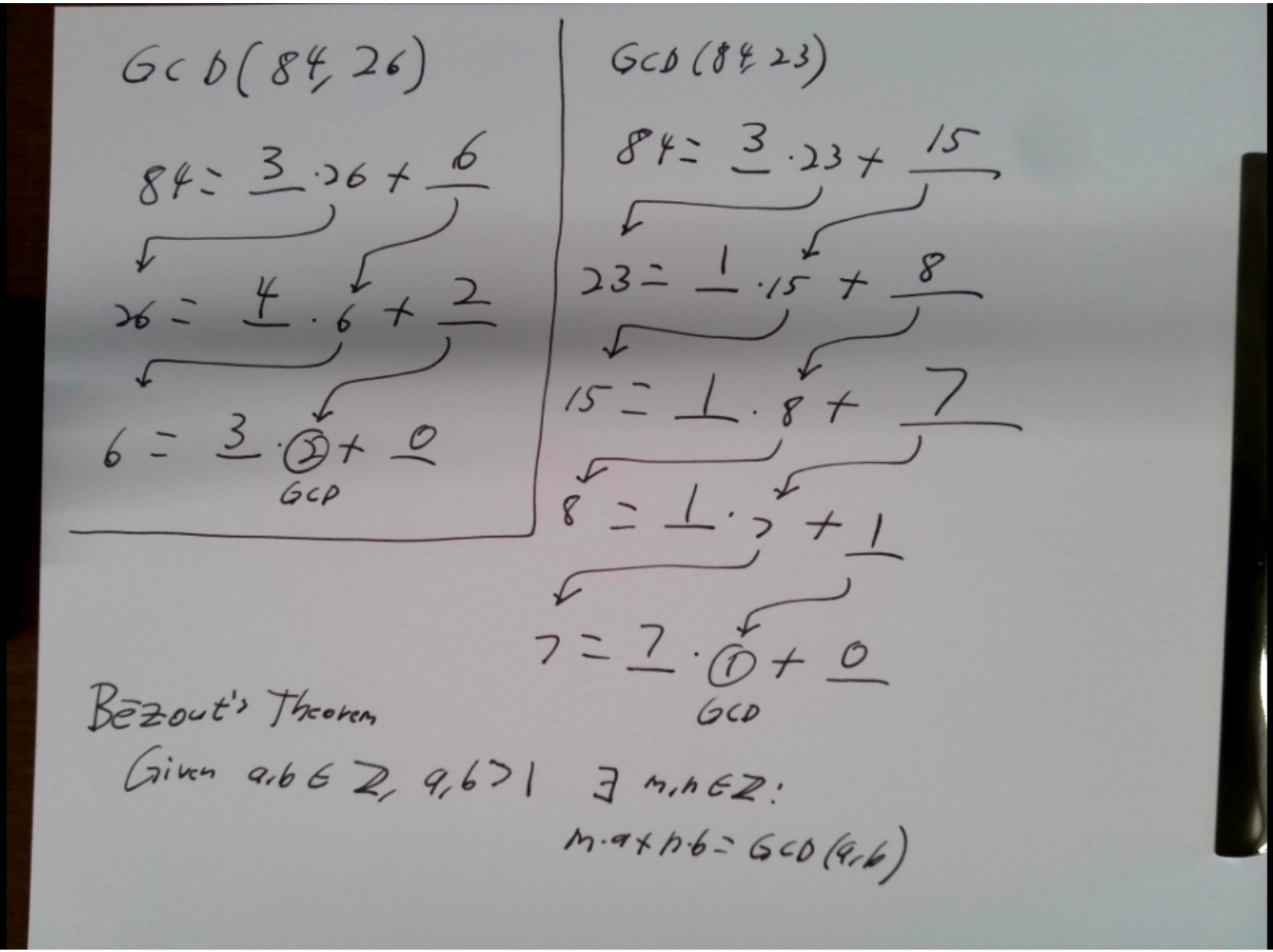
GCD(100, 15)

$100 = \underline{6} \cdot 15 + \underline{10}$

$15 = \underline{1} \cdot 10 + \underline{5}$

$10 = \underline{2} \cdot (5) + \underline{0}$

↑ GCD


GCD(84, 26)
84 = 3 · 26 + 6
26 = 4 · 6 + 2
6 = 3 · 2 + 0
GCD
GCD(84, 23)
84 = 3 · 23 + 15
23 = 1 · 15 + 8
15 = 1 · 8 + 7
8 = 1 · 7 + 1
7 = 7 · 1 + 0
GCD
Bezout's Theorem
Given a, b ∈ ℤ, a, b > 1 ∃ m, n ∈ ℤ:
m · a + n · b = GCD(a, b)

Fermat's Little Theorem

If $p$ is a prime and $p \nmid a$

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

---

ex: if $p=7$, $a=2$

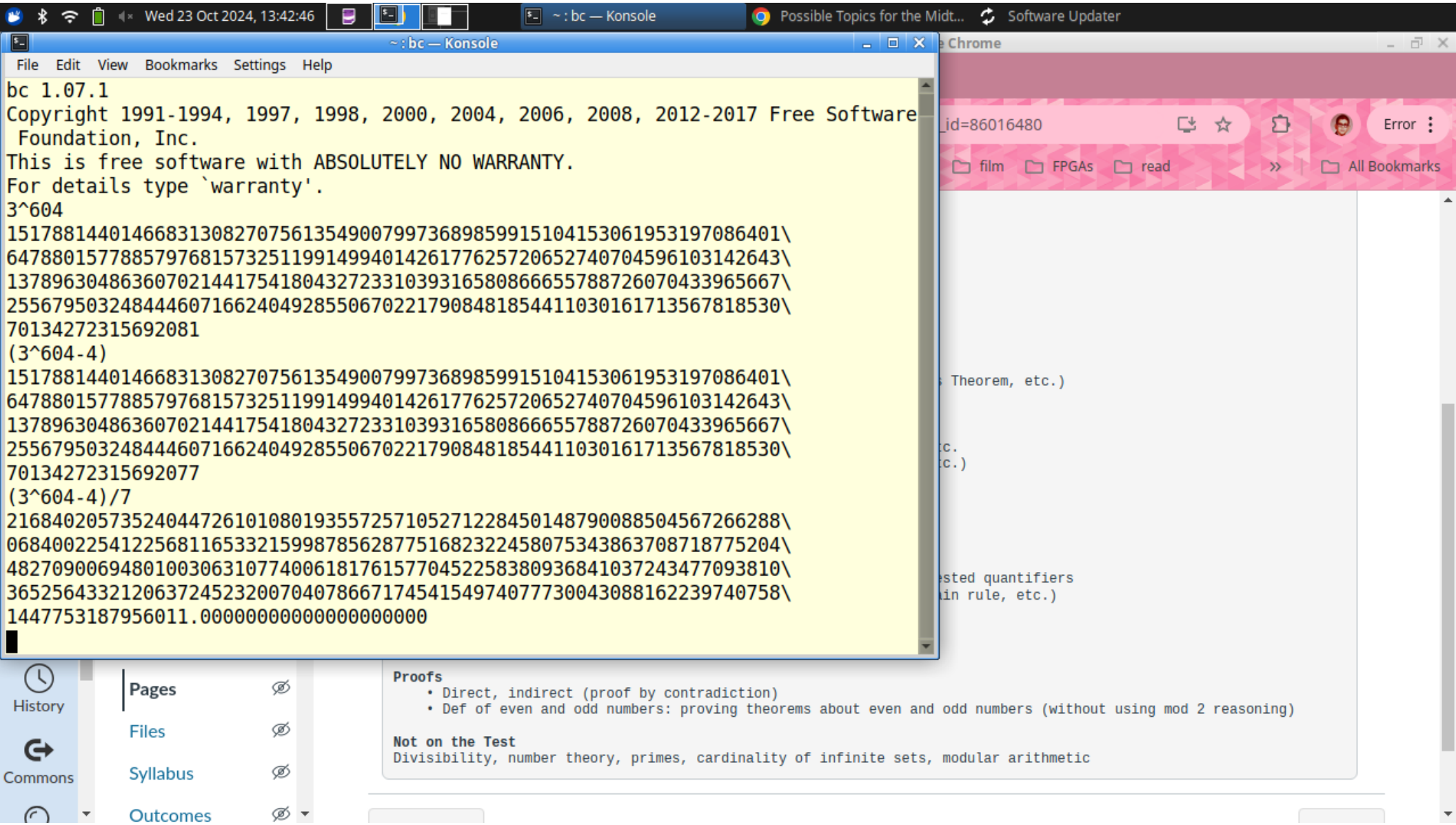
FLT says: $2^6 \equiv 1 \pmod{7}$

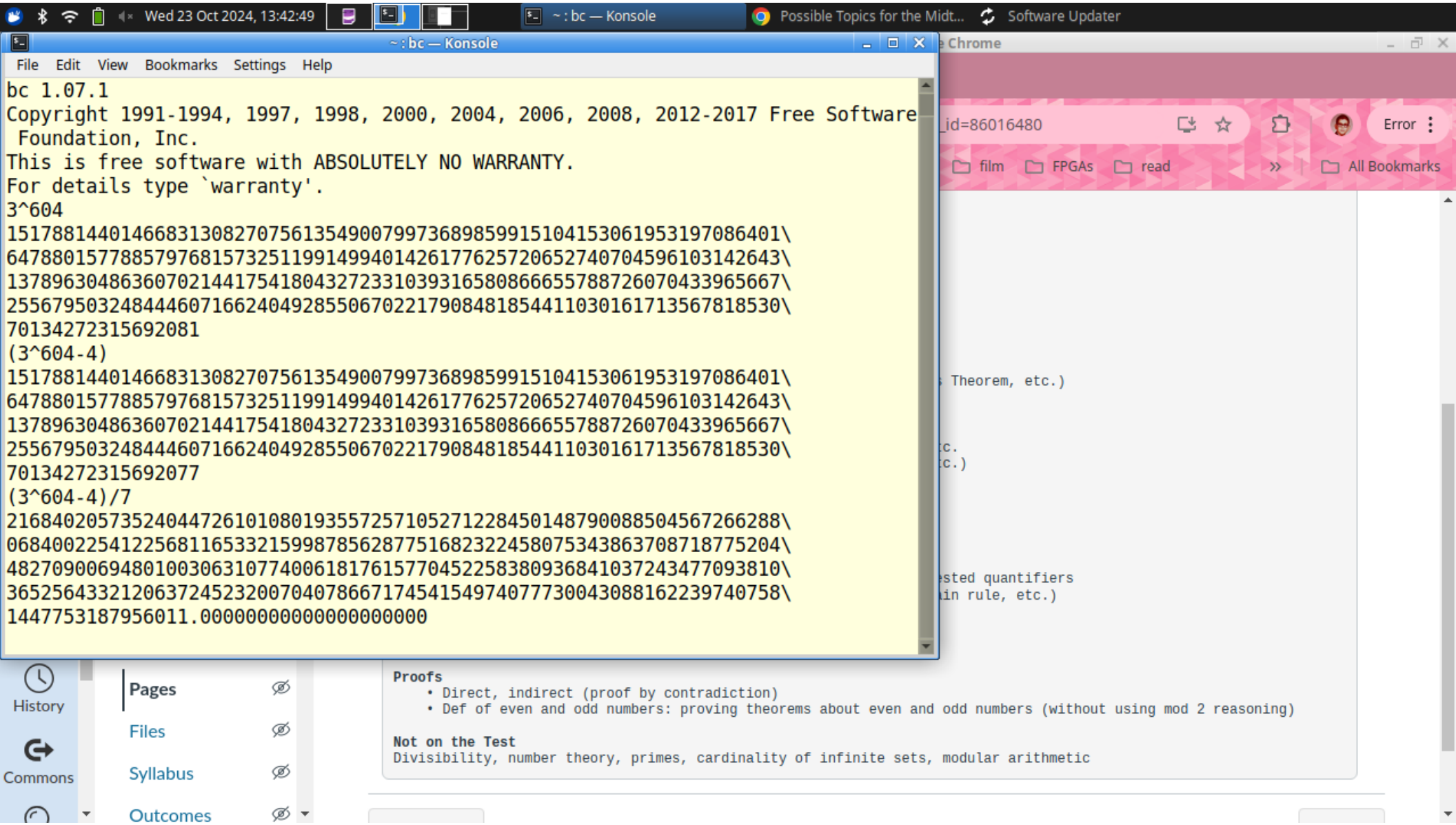
$\downarrow$

$64 = 1 + 63$

$\downarrow$

$7 \cdot 9$


Wed 23 Oct 2024, 13:42:46
~ : bc — Konsole
Possible Topics for the Midt...
Software Updater
~ : bc — Konsole
File Edit View Bookmarks Settings Help
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'.
3^604
151788144014668313082707561354900799736898599151041530619531970864 01\
647880157788579768157325119914994014261776257206527407045961031426 43\
137896304863607021441754180432723310393165808666557887260704339656 67\
255679503248444607166240492855067022179084818544110301617135678185 30\
70134272315692081
(3^604-4)
151788144014668313082707561354900799736898599151041530619531970864 01\
647880157788579768157325119914994014261776257206527407045961031426 43\
137896304863607021441754180432723310393165808666557887260704339656 67\
255679503248444607166240492855067022179084818544110301617135678185 30\
70134272315692077
(3^604-4)/7
216840205735240447261010801935572571052712284501487900885045672662 88\
068400225412256811653321599878562877516823224580753438637087187752 04\
482709006948010030631077400618176157704522583809368410372434770938 10\
365256433212063724523200704078667174541549740777300430881622397407 58\
1447753187956011.000000000000000000000
Pages
Files
Syllabus
Outcomes
History
Commons
Chrome
id=86016480
Error
film
FPGAs
read
All Bookmarks
Theorem, etc.)
ested quantifiers
in rule, etc.)
Proofs
• Direct, indirect (proof by contradiction)
• Def of even and odd numbers: proving theorems about even and odd numbers (without using mod 2 reasoning)
Not on the Test
Divisibility, number theory, primes, cardinality of infinite sets, modular arithmetic


Wed 23 Oct 2024, 13:42:49
~ : bc — Konsole
Possible Topics for the Midt...
Software Updater
~ : bc — Konsole
File Edit View Bookmarks Settings Help
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'.
3^604
151788144014668313082707561354900799736898599151041530619531970864 01\
647880157788579768157325119914994014261776257206527407045961031426 43\
137896304863607021441754180432723310393165808666557887260704339656 67\
255679503248444607166240492855067022179084818544110301617135678185 30\
70134272315692081
(3^604-4)
151788144014668313082707561354900799736898599151041530619531970864 01\
647880157788579768157325119914994014261776257206527407045961031426 43\
137896304863607021441754180432723310393165808666557887260704339656 67\
255679503248444607166240492855067022179084818544110301617135678185 30\
70134272315692077
(3^604-4)/7
216840205735240447261010801935572571052712284501487900885045672662 88\
068400225412256811653321599878562877516823224580753438637087187752 04\
482709006948010030631077400618176157704522583809368410372434770938 10\
365256433212063724523200704078667174541549740777300430881622397407 58\
1447753187956011.000000000000000000000
Pages
Files
Syllabus
Outcomes
History
Commons
Chrome
id=86016480
Error
film
FPGAs
read
All Bookmarks
Theorem, etc.)
ested quantifiers
in rule, etc.)
Proofs
• Direct, indirect (proof by contradiction)
• Def of even and odd numbers: proving theorems about even and odd numbers (without using mod 2 reasoning)
Not on the Test
Divisibility, number theory, primes, cardinality of infinite sets, modular arithmetic

Uses of FLT:

Find $3^{604} \pmod 7$

By FLT, $3^6 \equiv 1 \pmod 7$

$3^{600} \equiv (3^6)^{100} \equiv 1^{100} \equiv 1 \pmod 7$

$3^{601} \equiv 3$

$3^{602} \equiv 9 \equiv 2$

$3^{603} \equiv 6$

$3^{604} \equiv 18 \equiv \boxed{4}$

# Chinese Remainder Theorem

Suppose $x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 2 \pmod 7$

in this case, $x = 23$