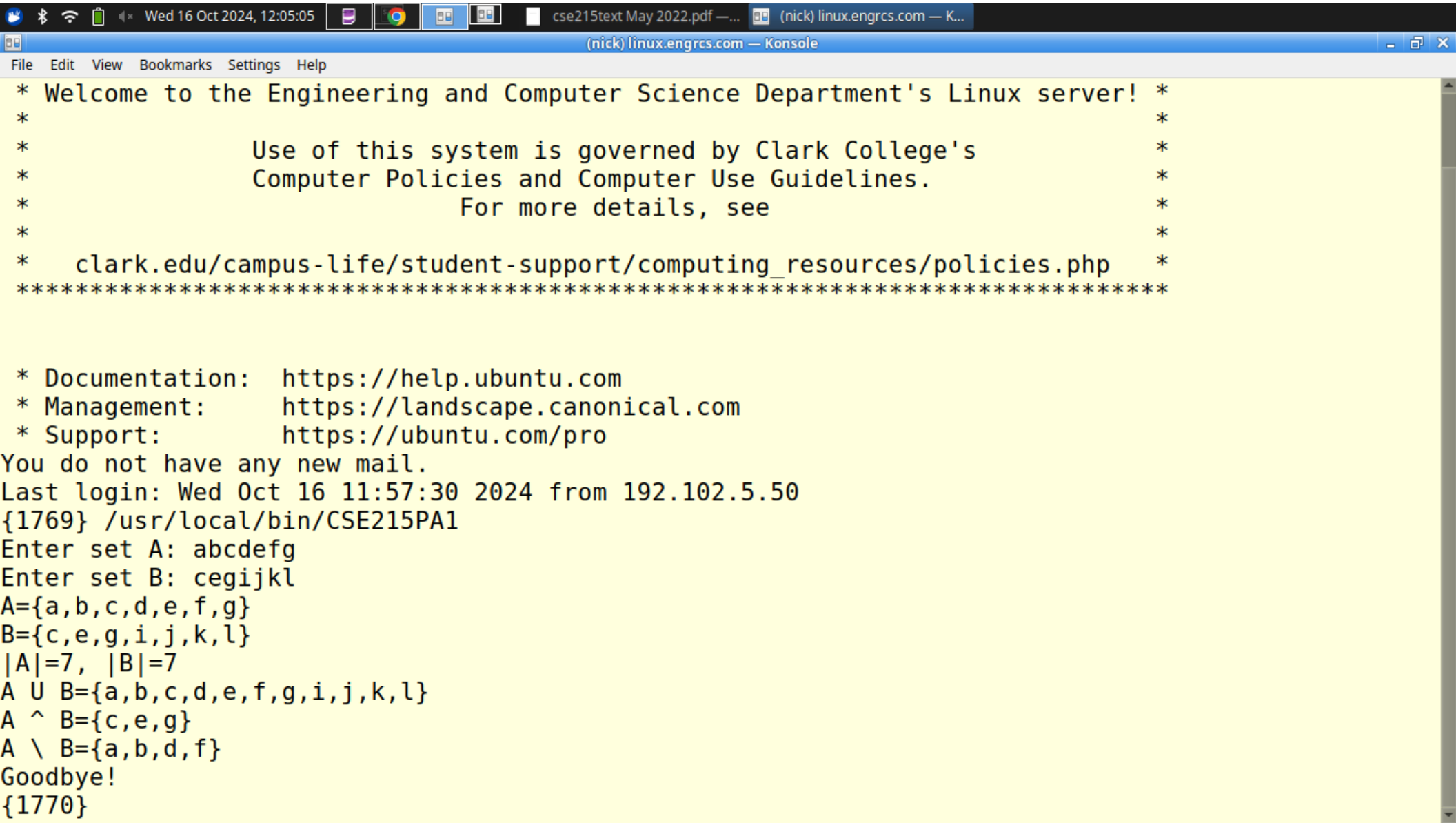

Wed 16 Oct 2024, 12:05:05
cse215text May 2022.pdf —...
(nick) linux.engrcs.com — K...
(nick) linux.engrcs.com — Konsole
File Edit View Bookmarks Settings Help
* Welcome to the Engineering and Computer Science Department's Linux server! *
* *
* Use of this system is governed by Clark College's *
* Computer Policies and Computer Use Guidelines. *
* For more details, see *
* *
* clark.edu/campus-life/student-support/computing_resources/policies.php *
****
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/pro
You do not have any new mail.
Last login: Wed Oct 16 11:57:30 2024 from 192.102.5.50
{1769} /usr/local/bin/CSE215PA1
Enter set A: abcdefg
Enter set B: cegijkl
A={a,b,c,d,e,f,g}
B={c,e,g,i,j,k,l}
|A|=7, |B|=7
A U B={a,b,c,d,e,f,g,i,j,k,l}
A ^ B={c,e,g}
A \ B={a,b,d,f}
Goodbye!
{1770}


Wed 16 Oct 2024, 12:06:06
cse215text May 2022.pdf —...
(nick) linux.engrcs.com — K...
(nick) linux.engrcs.com — Konsole
File Edit View Bookmarks Settings Help
|A|=7, |B|=7
A U B={a,b,c,d,e,f,g,i,j,k,l}
A ^ B={c,e,g}
A \ B={a,b,d,f}
Goodbye!
{1770} /usr/local/bin/CSE215PA1
Enter set A: aaaaaaaa
Enter set B: aaaaabbbbbbb
A={a}
B={a,b}
|A|=1, |B|=2
A U B={a,b}
A ^ B={a}
A \ B={}
Goodbye!
{1771} /usr/local/bin/CSE215PA1
Enter set A:
Enter set B: x
A={}
B={x}
|A|=0, |B|=1
A U B={x}
A ^ B={}
A \ B={}
Goodbye!
{1772}

input: "abcbabcd"

Set: empty

for each letter in input:

if letter ∉ Set,

add to set

Union (A, B)

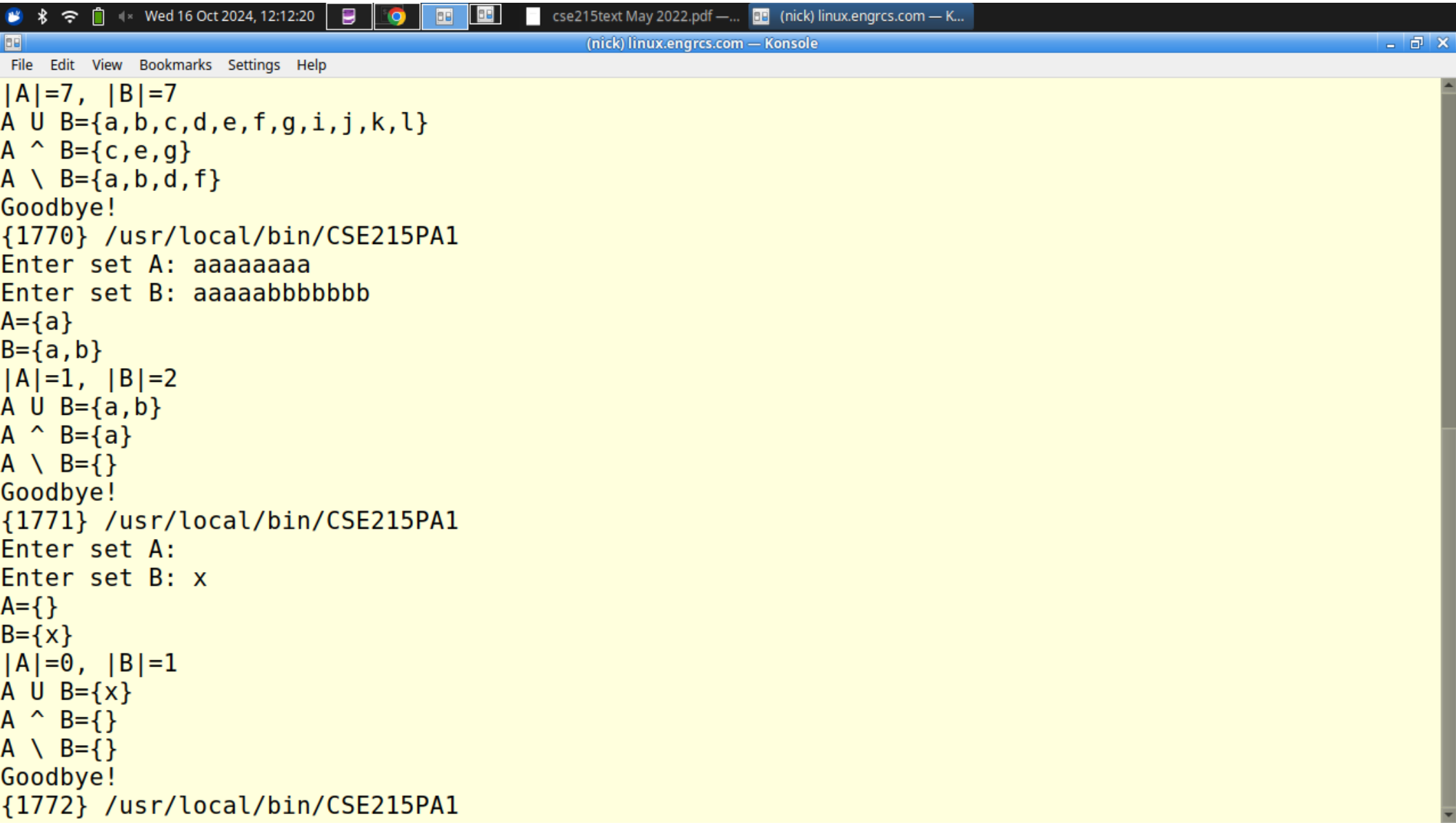
Set: empty

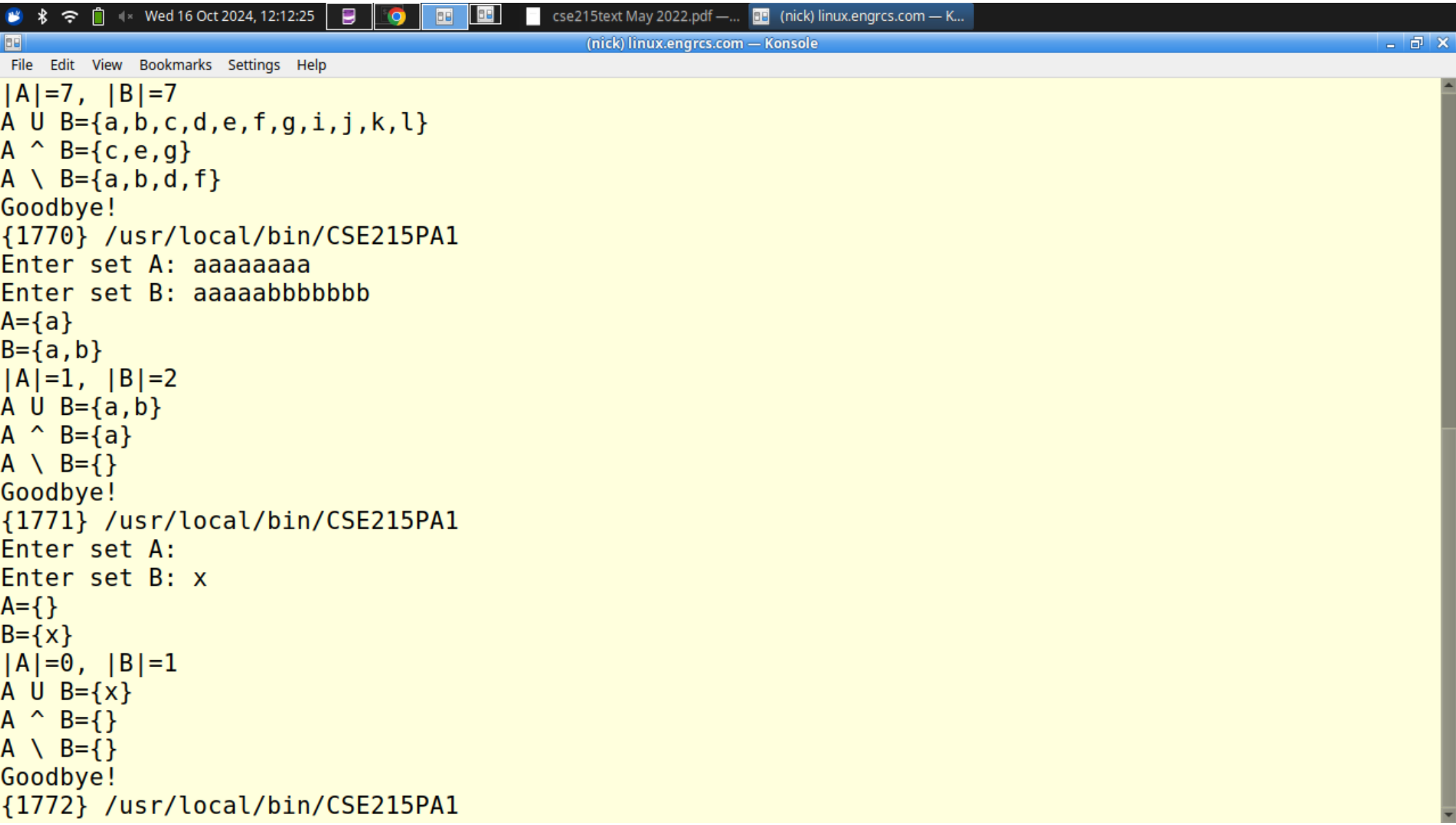
for each letter in A

if ∉ B, add to R

Set Set

for each letter in B ...


Wed 16 Oct 2024, 12:12:20
cse215text May 2022.pdf —...
(nick) linux.engrcs.com — K...
(nick) linux.engrcs.com — Konsole
File Edit View Bookmarks Settings Help
|A|=7, |B|=7
A U B={a,b,c,d,e,f,g,i,j,k,l}
A ^ B={c,e,g}
A \ B={a,b,d,f}
Goodbye!
{1770} /usr/local/bin/CSE215PA1
Enter set A: aaaaaaaa
Enter set B: aaaaabbbbbbb
A={a}
B={a,b}
|A|=1, |B|=2
A U B={a,b}
A ^ B={a}
A \ B={}
Goodbye!
{1771} /usr/local/bin/CSE215PA1
Enter set A:
Enter set B: x
A={}
B={x}
|A|=0, |B|=1
A U B={x}
A ^ B={}
A \ B={}
Goodbye!
{1772} /usr/local/bin/CSE215PA1


Wed 16 Oct 2024, 12:12:25
cse215text May 2022.pdf —...
(nick) linux.engrcs.com — K...
(nick) linux.engrcs.com — Konsole
File Edit View Bookmarks Settings Help
|A|=7, |B|=7
A U B={a,b,c,d,e,f,g,i,j,k,l}
A ^ B={c,e,g}
A \ B={a,b,d,f}
Goodbye!
{1770} /usr/local/bin/CSE215PA1
Enter set A: aaaaaaaa
Enter set B: aaaaabbbbbbb
A={a}
B={a,b}
|A|=1, |B|=2
A U B={a,b}
A ^ B={a}
A \ B={}
Goodbye!
{1771} /usr/local/bin/CSE215PA1
Enter set A:
Enter set B: x
A={}
B={x}
|A|=0, |B|=1
A U B={x}
A ^ B={}
A \ B={}
Goodbye!
{1772} /usr/local/bin/CSE215PA1

input: "abcbabcd"

Set: empty

for each letter in input:

if letter ∉ Set,

add to set

Union (A, B)

Set: empty

for each letter in A

if ∉ B, add to R

Set Set

for each letter in B ...

Number Theory ($a, b, \text{etc.} \in \mathbb{Z}$)

Divisibility

Definition: We say "a divides b" if

$$\exists q \in \mathbb{Z} : b = a \cdot q$$

(Or, we might say: $\frac{b}{a}$ is a whole number)

ex: 5 divides 20

3 divides 21

5 divides 5

1 divides 5

-3 divides 21

3 does not divide 20

a divides b

b is divisible by a

a is a factor of b

b is a multiple of a

DEF/new Symbol

$a \mid b$ means "a divides b" $\left(\frac{b}{a} \in \mathbb{Z}\right)$

Note: $a \mid b$ is a proposition.

$5 \mid 20$ $\quad$ $5 \nmid 21$

$3 \mid 21$

The Division Algorithm. $\quad 5 \nmid 21$

$\frac{21}{5} = \sim R \sim$ (quotient, remainder)

$\frac{20}{5} = \sim R 0$

$\frac{21}{5} = 4 \text{ R } 1$ ← ≥ 0

$5 \text{ R } -4$ < 5

$\frac{21}{5} = 3 \text{ R } 6$

$2 \text{ R } 11$

$1 \text{ R } 16$

$0 \text{ R } 21$

$-1 \text{ R } 26$

Theorem: If $a|b$ and $b|c$ then $a|c$

↪ If $a|b$ and $a|c$ then $a|(b+c)$

prove this

Proof:

1.	$a \mid b$	Hyp.
2.	$a \mid c$	Hyp.
3.	$\exists q \in \mathbb{Z} : b = a \cdot q$	def of "$\mid$", 1.
4.	$\exists s \in \mathbb{Z} : c = a \cdot s$	def of "$\mid$", 2.
5.	$b+c = a \cdot q + a \cdot s$ $= a(q+s)$	Subs, 3. 4. alg.
6.	$q+s \in \mathbb{Z}$	3. 4. closure of ints.
7.	$a \mid (b+c)$ Q.E.D.	5. 6. def of "$\mid$"

Theorem: If $a|b$ and $b|c$ then $a|c$

↪ If $a|b$ and $a|c$ then $a|(b+c)$

prove this

Proof:

1.	$a \mid b$	Hyp.
2.	$a \mid c$	Hyp.
3.	$\exists q \in \mathbb{Z} : b = a \cdot q$	def of "$\mid$", 1.
4.	$\exists s \in \mathbb{Z} : c = a \cdot s$	def of "$\mid$", 2.
5.	$b+c = a \cdot q + a \cdot s$	Subs, 3. 4.
	$= a(q+s)$	alg.
6.	$q+s \in \mathbb{Z}$	3. 4. closure of ints.
7.	$a \mid (b+c)$	5. 6. def of "$\mid$"

Q.E.D.

Modular Arithmetic

fix a ~~divor~~ divisor (such as 5)
& think about remainders when we divide by 5.

$\frac{21}{5}$ R 1

$21+7=28$

$\frac{7}{5}$ R 2

$\frac{28}{5}$ R 3

$\frac{56^{200}}{5}$ R $1^{200} = 1$

$\frac{8}{5}$ R 3

$\frac{7+7}{5}$ R 4

$\frac{56}{5} = 1$

$56 = 7 \cdot 8$

$2 \cdot 3 = 6$

$\frac{6}{5}$ R 1

Wed 16 Oct 2024, 12:47:19 ~ : bash — Konsole ~ : bash — Konsole PA1.pdf: CSE215 8764 - F24 ...

3 Assumptions

You may assume input lines are no more than 120 characters each, and include only lette

4 Recom

Start this assign
you will represen
a membership-te
With those two f
calculating the u

~ : bash — Konsole

File Edit View Bookmarks Settings Help

```
676452257703085491266229207630814075308381189124091247604389453263775\
5494022488452059
60^200
426825223812027400796974891518773732342988745354489429495479078935115\
292954961973901907213934075709729681281546667612983095446524051759525\
423840155919198453760000000000000000000000000000000000000000000000000\
000000000000000000000000000000000000000000000000000000000000000000000\
000000000000000000000000000000000000000000000000000000000000000000000\
0000000000000000
59^202
515354831215699868918688692514307204385506622826181074819239926024385\
876746327503086046574058601900535414909268713394382101424057778682175\
944018195057208703676794841415929163800975846329389185075644535951115\
471320214685797660638319301103690143023526439651008866727743449447685\
129106832044820439847075232502180304431944901583213836086589777425625\
754147326818671481
59^205
105843059880249223378651364979895899329490964689418242965300676766965\
294067283996256309159333581599730062978650699088224801608371562527965\
733124512882654466352436447735162115732280618343283621441650799149105\
398868274371954437744237379741374777884028836649084550039677221904115\
533587832058533177115352464176065288743928411942258874441627721897895\
795884023834691930096299
[2002]
```

DEF: If $\frac{a}{b}$ has a remainder of r,

we say

$$a \equiv r \pmod{b}$$

"a is congruent to r, modulo b"

---

ex: $21 \equiv 1 \pmod{5}$

$57 \equiv 2 \pmod{5}$

$21 + 57 \equiv 1 + 2 \equiv 3 \pmod{5}$

$21 \cdot 57 \equiv 1 \cdot 2 \equiv 2 \pmod{5}$

Theorem: If $a \equiv b \pmod{m}$

and $c \equiv d \pmod{m}$

Then $a+c \equiv b+d \pmod{m}$

and $a \cdot c \equiv b \cdot d \pmod{m}$

(and $a-c \equiv b-d \pmod{m}$)

1. Define propositions P and Q and use them to give a real-world example of two fallacies we discussed (denying the hypothesis and affirming the conclusion).

Do the following problems using the formal proof techniques we've been discussing in class. Make sure:

- you begin by stating clearly what you are trying to prove
- you write the word "Proof"
- everything after that is a proposition
- each proposition is true (because it follows from prior steps and laws of logic; because it is a hypothesis; or because it is an assumption);
- each proposition has a number to its left
- each proposition has a justification (reason why it is true) to its right
- your final proposition is the proposition you are trying to prove
- you end with the words "QED"

Also, if you're trying to prove P→Q, don't make the mistake of showing Q→P

2. Prove that if n is even, then 10n-2 is even.

3. Prove that if n is even, then n*n+n is even.

4. Prove that if n*n is even then n is even.

5. Prove that if n*n is odd then n is odd.

6. Prove (for all integers a, x and y) that if a|x and a|y then a|(2*x-3*y)

1. Define propositions P and Q and use them to give a real-world example of two fallacies we discussed (denying the hypothesis and affirming the conclusion).

Do the following problems using the formal proof techniques we've been discussing in class. Make sure:

- you begin by stating clearly what you are trying to prove
- you write the word "Proof"
- everything after that is a proposition
- each proposition is true (because it follows from prior steps and laws of logic; because it is a hypothesis; or because it is an assumption);
- each proposition has a number to its left
- each proposition has a justification (reason why it is true) to its right
- your final proposition is the proposition you are trying to prove
- you end with the words "QED"

Also, if you're trying to prove P→Q, don't make the mistake of showing Q→P

2. Prove that if n is even, then 10n-2 is even.

3. Prove that if n is even, then n*n+n is even.

4. Prove that if n*n is even then n is even.

5. Prove that if n*n is odd then n is odd.

6. Prove (for all integers a, x and y) that if a|x and a|y then a|(2*x-3*y)

Think Mod 5

X	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

no 0

1 in every row & column

mod 4

X	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

0 appears

not nesc. 1 in each row & column

Think Mod 5

X	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

no 0

1 in every row & column

mod 4

X	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

0 appears

not nesc. 1 in each row & column

Modular Exponentiation

Want to compute $a^e \pmod m$

ex: Calculate $7^{200} \pmod 5$

STEP 1

$7^1 \equiv 2$

$7^2 \equiv (7^1)^2 \equiv (2)^2 \equiv 4$

$7^4 \equiv (7^2)^2 \equiv (4)^2 \equiv 16 \equiv 1$

$7^8 \equiv (7^4)^2 \equiv (1)^2 \equiv 1$

$7^{16} \equiv 1$

$7^{32} \equiv 1$

$7^{64} \equiv 1$

$7^{128} \equiv 1$

STEP 2

$200 = 128 + 64 + 8$

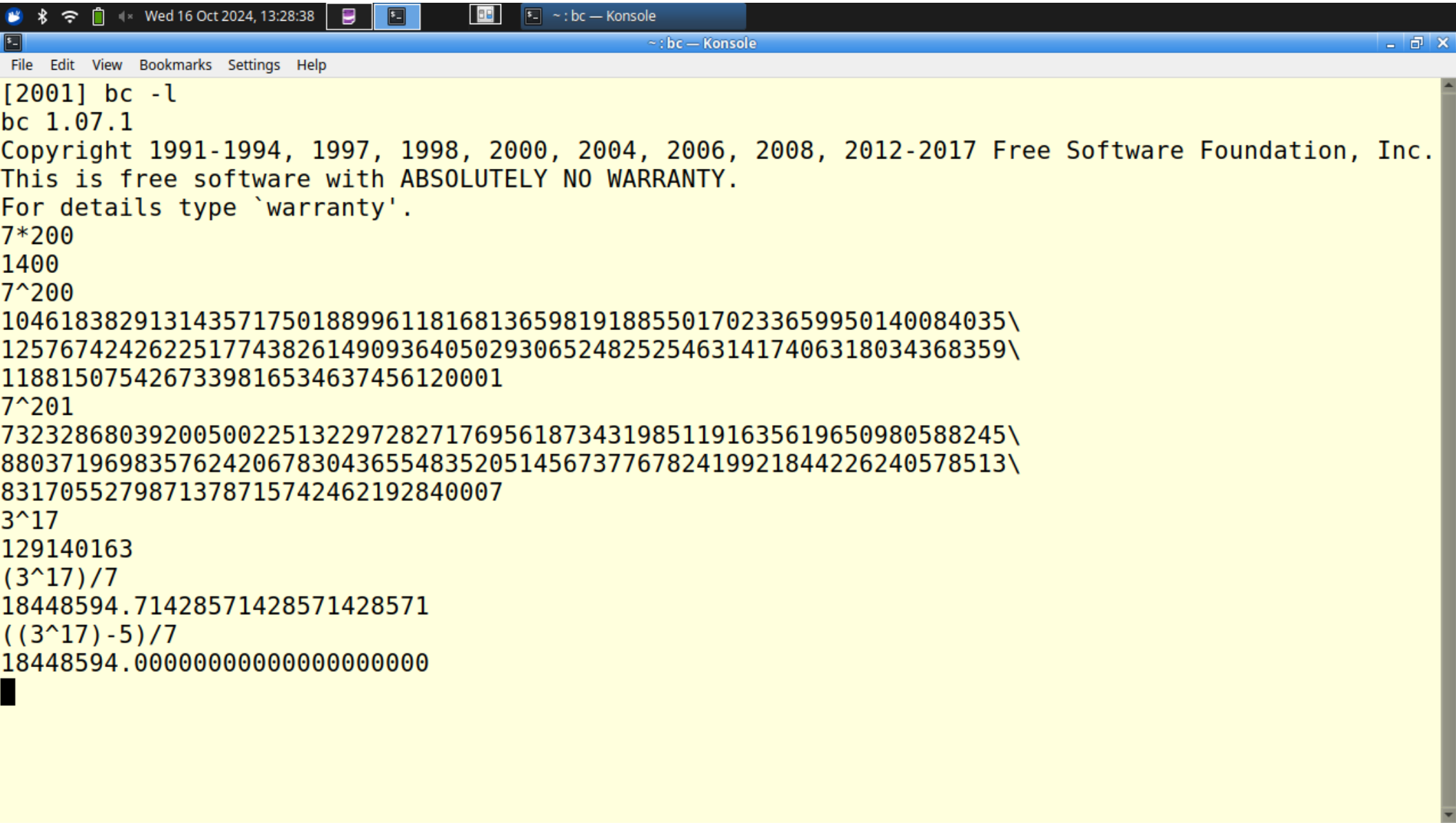
STEP 3 (Law of Exponents)

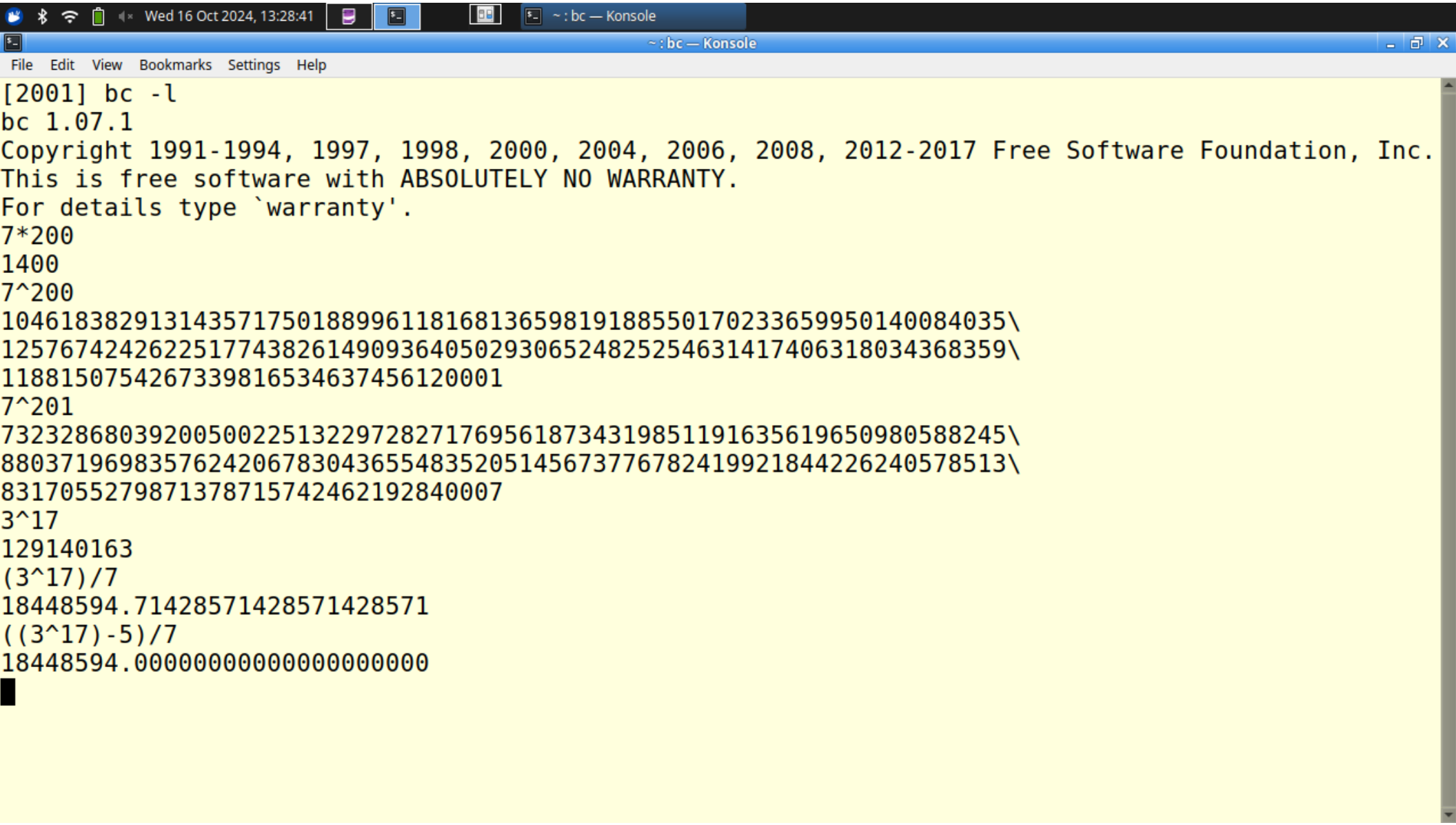
$7^{200} = 7^{(128+64+8)}$

$= 7^{128} \cdot 7^{64} \cdot 7^8$

$\equiv 1 \cdot 1 \cdot 1$

$\equiv 1$


Wed 16 Oct 2024, 13:28:38
~ : bc — Konsole
~ : bc — Konsole
File Edit View Bookmarks Settings Help
[2001] bc -l
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*200
1400
7^200
104618382913143571750188996118168136598191885501702336599501400840 35\
125767424262251774382614909364050293065248252546314174063180343683 59\
11881507542673398165346374561200 01
7^201
732328680392005002251322972827176956187343198511916356196509805882 45\
880371969835762420678304365548352051456737767824199218442262405785 13\
831705527987137871574246219284000 7
3^17
129140163
(3^17)/7
18448594.71428571428571428571
((3^17)-5)/7
18448594.00000000000000000000


Wed 16 Oct 2024, 13:28:41
~ : bc — Konsole
~ : bc — Konsole
File Edit View Bookmarks Settings Help
[2001] bc -l
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*200
1400
7^200
104618382913143571750188996118168136598191885501702336599501400840 35\
125767424262251774382614909364050293065248252546314174063180343683 59\
11881507542673398165346374561200 01
7^201
732328680392005002251322972827176956187343198511916356196509805882 45\
880371969835762420678304365548352051456737767824199218442262405785 13\
831705527987137871574246219284000 7
3^17
129140163
(3^17)/7
18448594.71428571428571428571
((3^17)-5)/7
18448594.00000000000000000000

Calculate $3^{17} \pmod 7$

using modular exponentiation

$3^1 \equiv 3$

$3^2 \equiv 9 \equiv 2$

$3^4 \equiv 2^2 \equiv 4$

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

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

$17 = 16 + 1$

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

$= 3^{16} \cdot 3^1$

$3^{17} \equiv 4 \cdot 3 \equiv 12 \equiv 5$

$3 \equiv ? \; 3 \pmod{7}$

$\frac{3}{7} = 0 \; R3$

$3 \equiv ? \pmod{18000000}$

$\frac{3}{18000000} = 0 \; R3$