Some Solutions to HW04 Problems

BILL, RECORD LECTURE!!!!

BILL RECORD LECTURE!!!

HW04, Problem 2

Write programs for
EXP
TESTPRIME
TESTSAFEPRIME
HOWMANYSAFEPRIMES.

STUDENT ISSUES

STUDENT ISSUES

a) Program Taking too long.

STUDENT ISSUES

a) Program Taking too long.
Often it was $a^n \pmod{p}$ is taking too much time. Need to do mod p after EVERY calculation so numbers don't get large.

STUDENT ISSUES

a) Program Taking too long.
Often it was $a^n \pmod{p}$ is taking too much time. Need to do mod p after EVERY calculation so numbers don't get large.
b) My answers are a wee bit diff from what I think we should get.

STUDENT ISSUES

a) Program Taking too long.
Often it was $a^n \pmod{p}$ is taking too much time. Need to do mod p after EVERY calculation so numbers don't get large.
b) My answers are a wee bit diff from what I think we should get.

- Test does NOT always work *Carmichael Numbers* are composites n such that $(\forall a \in \{1, \ldots, n-1\})[a^n \equiv 1 \pmod{n}]$. These will be declared PRIME even though they are NOT.

STUDENT ISSUES

a) Program Taking too long.
Often it was $a^n \pmod{p}$ is taking too much time. Need to do mod p after EVERY calculation so numbers don't get large.
b) My answers are a wee bit diff from what I think we should get.

- Test does NOT always work *Carmichael Numbers* are composites n such that $(\forall a \in \{1, \ldots, n-1\})[a^n \equiv 1 \pmod{n}]$. These will be declared PRIME even though they are NOT.
- n composite, not Carmichael, $\implies (\exists a)[a^{n-1} \not\equiv 1 \pmod{n}]$. Can get unlucky and pick a_1, a_2, a_3, a_4, a_5 such that $(\forall i)[a_i^{n-1} \equiv 1 \pmod{n}]$.

STUDENT ISSUES

a) Program Taking too long.
Often it was $a^n \pmod{p}$ is taking too much time. Need to do mod p after EVERY calculation so numbers don't get large.
b) My answers are a wee bit diff from what I think we should get.

- Test does NOT always work *Carmichael Numbers* are composites n such that $(\forall a \in \{1, \ldots, n-1\})[a^n \equiv 1 \pmod{n}]$. These will be declared PRIME even though they are NOT.
- n composite, not Carmichael, $\implies (\exists a)[a^{n-1} \not\equiv 1 \pmod{n}]$. Can get unlucky and pick a_1, a_2, a_3, a_4, a_5 such that $(\forall i)[a_i^{n-1} \equiv 1 \pmod{n}]$.
  PROJECT IDEA how common is this?

HW04, Problem 3

a) Run HOWMANYSAFEPRIME on 10000, 20000, ..., 90000.
Find prop of safe primes in $\{1, \ldots, 10000\}$, ..., $\{1, \ldots, 90000\}$.

HW04, Problem 3

a) Run HOWMANYSAFEPRIME on 10000, 20000, ..., 90000.
Find prop of safe primes in $\{1, \ldots, 10000\}$, ..., $\{1, \ldots, 90000\}$.
b) Use a to conj $f(x + 10000) - f(x)$, (f=HWMNYSFPRMS).

HW04, Problem 3

a) Run HOWMANYSAFEPRIME on 10000, 20000, ..., 90000.
Find prop of safe primes in $\{1, \ldots, 10000\}$, ..., $\{1, \ldots, 90000\}$.
b) Use a to conj $f(x+10000) - f(x)$, (f=HWMNYSFPRMS).

COMMENTS

Math Conj Numb of safe primes $\le n$ is $\frac{cn}{\ln n} + O(1)$. Implies:

$$f(x+10000) - f(x) = c\left(\frac{x+10000}{\ln(x+10000)} - \frac{x}{\ln x}\right) \sim c\left(\frac{10000}{\ln x}\right)$$

HW04, Problem 3

a) Run HOWMANYSAFEPRIME on 10000, 20000, ..., 90000.
Find prop of safe primes in $\{1, \ldots, 10000\}$, ..., $\{1, \ldots, 90000\}$.
b) Use *a* to conj $f(x+10000) - f(x)$, (f=HWMNYSFPRMS).

COMMENTS

Math Conj Numb of safe primes $\le n$ is $\frac{cn}{\ln n} + O(1)$. Implies:

$$f(x+10000) - f(x) = c\left(\frac{x+10000}{\ln(x+10000)} - \frac{x}{\ln x}\right) \sim c\left(\frac{10000}{\ln x}\right)$$

Your data to small to show this, but should have shown:

$$f(x+10000) - f(x) \text{ is a decreasing function}$$

$$\lim_{x\to\infty} f(x+10000) - f(x) = 0$$

HW04, Problem 3

a) Run HOWMANYSAFEPRIME on 10000, 20000, ..., 90000.
Find prop of safe primes in $\{1,\ldots,10000\}$, ..., $\{1,\ldots,90000\}$.
b) Use a to conj $f(x+10000)-f(x)$, (f=HWMNYSFPRMS).

COMMENTS

Math Conj Numb of safe primes $\le n$ is $\frac{cn}{\ln n}+O(1)$. Implies:

$$f(x+10000)-f(x)=c\left(\frac{x+10000}{\ln(x+10000)}-\frac{x}{\ln x}\right)\sim c\left(\frac{10000}{\ln x}\right)$$

Your data to small to show this, but should have shown:

$$f(x+10000)-f(x) \text{ is a decreasing function}$$

$$\lim_{x\to\infty} f(x+10000)-f(x)=0$$

PROJECT IDEA Estimate c.

HW04, Problem 4,5

a) Write programs for TESTGEN and FINDGEN
b) Run and find NUMBGEN for a variety of numbers given.
c) Make a conjectures about Prop of NUMBGEN, called g.

HW04, Problem 4,5

a) Write programs for TESTGEN and FINDGEN
b) Run and find NUMBGEN for a variety of numbers given.
c) Make a conjectures about Prop of NUMBGEN, called g.
COMMENTS
Thm $(\exists c)$

$$g(p) = \frac{cp}{\ln \ln p} + O(1).$$

HW04, Problem 4,5

a) Write programs for TESTGEN and FINDGEN
b) Run and find NUMBGEN for a variety of numbers given.
c) Make a conjectures about Prop of NUMBGEN, called g.
COMMENTS
Thm $(\exists c)$

$$g(p) = \frac{cp}{\ln \ln p} + O(1).$$

Doubt your data would have lead you to this equation, not enough data, and c is unknown.

HW04, Problem 4,5

a) Write programs for TESTGEN and FINDGEN
b) Run and find NUMBGEN for a variety of numbers given.
c) Make a conjectures about Prop of NUMBGEN, called g.

COMMENTS

Thm $(\exists c)$

$$g(p) = \frac{cp}{\ln \ln p} + O(1).$$

Doubt your data would have lead you to this equation, not enough data, and c is unknown.
However, your data should lead you to:

$$g(p) \text{ is an increasing function}$$

and some conj function that goes to infinity, perhaps lin function with factor < 1.

HW04, Problem 4,5

a) Write programs for TESTGEN and FINDGEN
b) Run and find NUMBGEN for a variety of numbers given.
c) Make a conjectures about Prop of NUMBGEN, called g.
COMMENTS
Thm $(\exists c)$

$$g(p) = \frac{cp}{\ln \ln p} + O(1).$$

Doubt your data would have lead you to this equation, not enough data, and c is unknown.
However, your data should lead you to:

$$g(p) \text{ is an increasing function}$$

and some conj function that goes to infinity, perhaps lin function with factor < 1.
PROJECT IDEA Find c.