Homework 05, MORALLY Due March 03

1. (40 points) For this problem FIRST write the program and make conjectures THEN look up whats true.

   A prime p such that p and $\frac{p-1}{2}$ are both prime is called a *safe prime*

   (a) (0 points) Write a program that will, given a number n, test if n is prime, using the naive algorithm of testing if $2, 3, 4, \ldots, \lceil \sqrt{n} \rceil$ divides n. (Do not hand anything in.)

   (b) (0 points) Write a program that will, given a number n, test if both n and $\frac{n-1}{2}$ are prime (use the program in Part 1). (Do not hand anything in.)

   (c) (4 points) Find the following numbers

   - The number of primes in $\{1, \ldots, 10000\}$. The number of safe primes.
   - The number of primes in $\{1, \ldots, 20000\}$. The number of safe primes.
   - $\vdots$
   - The number of primes in $\{1, \ldots, 200000\}$. The number of safe primes.

   Hand in a table of the following form— we give the first two lines and they are likely incorrect.

n	Numb of Primes in $\{1, \ldots, n\}$	Numb of Safe Primes in $\{1, \ldots, n\}$
10,000	100	10
20,000	200	20

   (d) (8 points) It is known that the number of primes $\leq n$ is ROUGHLY $\frac{n}{\ln n}$. Using your data make a conjecture about what the value of A is such that the number of primes is around $\frac{An}{\ln n}$.

   (e) (8 points) Find some function f so that the following statement fits your data pretty well:

   The number of safe primes $\leq n$ is roughly $f(n)$

GO TO NEXT PAGE FOR THE REST OF THIS PROBLEM

(f) (0 points) Write a program that will, given p, g,

a) Test if p is a safe prime. If not then output NO.

b) (p is a safe prime) Test if g is a generator (see slides).

(Do not hand anything in)

(g) (4 points) Find the first 20 safe primes after 100,000. Call them $p_1, \ldots, p_{20}$. Hand them in.

(h) (8 points) Hand in a table of the following form documenting the first 20 safe primes. We give the first two lines. We assume the first two safe primes over 100,000 are 100,001 and 100,003 (this might not be true).

p	Numb of generators in $\{1, \ldots, p\}$	fraction that are gen
100,001	20,000	0.199
100,003	21,000	0.210

(i) (8 points) Based on your data make a conjecture of the following form: For large safe primes p, the number of generators in $\{1, \ldots, p\}$ is αp where α is FILL IT IN

GO TO NEXT PAGE

2. (30 points) This problem has six parts. However, the first three are worth 0. Do them but don't hand them in. They are a review of what we did in class briefly.

   (a) (0 points—Do not hand in) Compute the following mod 8: $0^2, 1^2, \ldots, 7^2$.

   (b) (0 points—Do not hand in) Use Part 1 to find **all** sums of 3 squares mod 8.

   (c) (0 points—Do not hand in) Use Part 2 to prove that there are an infinite number of natural numbers that cannot be written as the sum of 3 squares.

   (d) (10 points) Compute the following mod 16: $0^4, 1^4, \ldots, 15^4$.

   (e) (10 points) Use Part 4 to find **all** sums of 15 fourth powers mod 16.

   (f) (10 points) Use Part 5 to prove that there are an infinite number of natural numbers that **cannot** be written as the sum of 15 fourth powers.

GO TO NEXT PAGE

3. (30 points)

(a) (15 points) Find a set $\mathbb{D} \subseteq \mathbb{R}$ such that the following all hold:

- Every element $x \in \mathbb{D}$ has both a successor element $\text{succ}(x)$ (so $x < \text{succ}(x)$ and there is nothing strictly between x and $\text{succ}(x)$) and a predecessor element $\text{pred}(x)$ (so $\text{pred}(x) < x$ and there is nothing strictly inbetween $\text{pred}(x)$ and x).
- There exists $x, y \in \mathbb{D}$ such that:
  i) $x < y$ and
  ii) $\text{succ}(x) \neq y$, $\text{succ}(\text{succ}(x)) \neq y$, ...

(b) (15 points) Find a set $\mathbb{D} \subseteq \mathbb{R}$ such that the following all hold:

- Every element $x \in \mathbb{D}$ has both a successor element $\text{succ}(x)$ (so $x < \text{succ}(x)$ and there is nothing strictly between x and $\text{succ}(x)$) and a predecessor element $\text{pred}(x)$ (so $\text{pred}(x) < x$ and there is nothing strictly inbetween $\text{pred}(x)$ and x).
- There exists an infinite number of pairs $(x_1, y_1), (x_2, y_2), \ldots \in D$ such that, for all $i \in \mathbb{N}$:
  1) $x_1 < y_1$ and $\text{succ}(x_1) \neq y_1$, $\text{succ}(\text{succ}(x_1)), \neq y_1, \ldots$
  2) $x_2 < y_2$ and $\text{succ}(x_2) \neq y_2$, $\text{succ}(\text{succ}(x_2)), \neq y_2, \ldots$
  $\vdots$
  i) $x_i < y_i$ and $\text{succ}(x_i) \neq y_i$, $\text{succ}(\text{succ}(x_i)), \neq y_i, \ldots$
  $\vdots$
  and so on

GO TO NEXT PAGE

4. (Honors Homework which you must do) Leo showed that every planar graph is 5-colorable. It is known that every planar graph is 4-colorable (this was a hard result).

   A graph has *crossing number* c if there is a way to draw it so that if you REMOVE c edges, the graph is planar.

   Planar graphs have crossing number 0.

   For each of the statements fill in the FILL IN and prove the result.

   You may use that every planar graph is 4-colorable.

   (a) Every graph that has crossing number 1 can be XXX-colored.

   (b) Every graph that has crossing number 17 can be YYY-colored.

   (c) Every graph that has crossing number c can be $f(c)$-colored. (You need to find the function f.)