Homework 4 for Math 480A

http://wiki.wstein.org/2008/480a

Due Wednesday April 30, 2008

Each problem has equal weight, and parts of problems are worth the same amount as each other. There are **4 problems**. I have office hours MWF 2:30-3:30 in Sieg 312, unless otherwise stated. You can email me about problems; all responses will be cc'd to `sage-uw`, so you may want to subscribe to that mailing list.

1. Consider the first problem on the homework assignment that you're grading this week, which should list a bug in Sage. (If for some reason you are not grading a problem, or the homework you're grading does not have a solution to that problem, consider instead the bug that *you* reported in your homework assignment 3.) The Sage bug tracking system is at `http://trac.sagemath.org/sage_trac/`.

   (a) Determine whether or not that bug has already been recorded in the Sage bug tracking system. If so, give a link to the URL for the bug.

   (b) If the bug is not reported anywhere in trac, decide whether you think it is a real bug. Justifying your answer.

   (c) If you believe it really is a bug, search this mailing list to see if it has been reported there: `http://groups.google.com/group/sage-support/`. If not, report it!

   (d) (optional) If you're the ultimate bad ass, fix the bug.

   Here is a quote to ponder from:
   `http://reference.wolfram.com/mathematica/tutorial/TestingAndVerification.html`

   > "The standards of correctness for Mathematica are certainly much higher than for typical mathematical proofs. But just as long proofs will inevitably contain errors that go undetected for many years, so also a complex software system such as Mathematica will contain errors that go undetected even after millions of people have used it.
   >
   > Nevertheless, particularly after all the testing that has been done on it, the probability that you will actually discover an error in Mathematica in the course of your work is extremely low.
   >
   > Doubtless there will be times when Mathematica does things you do not expect. But you should realize that the probabilities are such that it is vastly more likely that there is something wrong with your input to Mathematica or your understanding of what is happening than with the internal code of the Mathematica system itself."

2. (a) How many primes are there ≤ 123456789?

   (b) Find a probable prime p with exactly 2008 decimal digits using the Sage command `next_probable_prime`. Show the Sage code you used to find this (probable) prime. Also, how long did the computation take?

   (c) Give an estimate (with justification) for roughly how long it would take in Sage to *prove* that the probable prime p that you found in the previous step is in fact prime. By "prove" I *mean* that the `is_prime` command outputs `True` given your (probable) prime p as input.

3. Consider the sequence $p_1, p_2, p_3, \ldots$ of all prime numbers $\leq 10^6$. Here $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, etc.

   (a) For how many integers n do we have $p_{n+1} = p_n + 2$?

   (b) For how many integers n do we have $p_{n+1} = p_n + 4$?

   (c) For how many integers n do we have $p_{n+1} = p_n + 6$?

   (d) Make some conjectures based on the above computations.

4. I encrypted a meaningful sequence of 8 letters using DES with mode ECB and key `abcdefgh` just as in class using this sort of code:

```
from Crypto.Cipher import DES
obj=DES.new('abcdefgh', DES.MODE_ECB)
obj.encrypt('????????')
```

   The result is

```
d*=\x90\xc1\x03\xe8\x80
```

   What did I encrypt?