Math 480b -- Homework 4

Homework 4

Due April 29, 2009

There are 5 problems.

Email solution worksheet with your *name* in the title to `sagehw@gmail.com`.

Problem 1 (Setup a real-world sized Diffie-Hellman key exchange): You would like to agree on a secret key using Diffie-Hellman, in order to communicate with Amazon.com securely. You and Amazon.com agree to use the prime $p = 2^{512} - 569 = 1340780...3527$, and generator $g = 2$. Amazon.com chooses a secret number a and tells you that

$g^a =$
2082728043114064665587780447758292084140753843961131178330477750084710957889630331734974721072528037029283561132545662418008

Choose a random number between 1 and p, and compute the secret key ($= g^{ab}$) that you and Amazon.com will agree on.

```
# so you don't have to cut and paste g^a:
g_to_a =
20827280431140646655877804477582920841407538439611311783304777500847109578896303317349747210725280370292835611325454
```

Problem 2 (Crack a Diffie-Hellman key exchange) : Jim and Pam publically agree on the prime $p = 10007$ and generator $g = 5$. They each chose secret random numbers a and b, then Jim publishes $g^a = 1096$ (mod p) and Pam publishes $g^b = 3941$ (mod p). Crack their code! What secret key do they agree on?

[Hints: To solve this problem, you will have to figure out what g^{ab} is. You *can't* do this by just multiplying g^a and g^b, since $g^a g^b = g^{a+b}$. Instead, you have to find a such that $g^a = 1096$ (working modulo p). You can do the latter either with a for loop, or using the log command, as illustrated below.]

```
# illustrate computing a "discrete log", i.e., log of the number 1096 to the base g=5.
log(mod(1096,10007), mod(5,10007))
```

```
939
```

Problem 3: You saw above that the log command can solve the discrete log problem when $p = 10007$ fairly quickly. E.g., given g, p, and g^a, it finds a. What happens if $g =$**primitive_root(p)** and p has 10 digits? 15 digits? 20 digits? How big must p be until the log command breaks down (i.e., stops working)?

```
#example --
p = next_prime(10^10)
g = primitive_root(p)
```

```
time log(mod(7,p), mod(g,p))
```

```
2889974065
Time: CPU 0.00 s, Wall: 0.00 s
```

Problem 4:

1. Encrypt the message "They are coming!" using the RSA cryptosystem with public key $(n, e) = (2021027, 5)$ and the encryption interact from the worksheet in class on Monday, April 20, 2009.
2. Decrypt the message

   ```
   [1488785, 736175, 261088, 274391, 1093291, 467950, 1810412, 1048576]
   ```

   using the private key $(n, d) = (2021027, 1614413)$.

Problem 5:

Let E be the elliptic curve mod 11 defined by $y^2 = x^3 + x + 2$. What is the sum of the points $(2, 10)$ and $(4, 2)$ on E?