MAT 301 Problem Set 2

[Posted: Jan 21, 2013. <u>Updated: Jan 23, 3:15pm</u>, Due: Feb 4, 2013. Worth: 100 points]

1. **(20 points)** Come up with an upper bound on the fraction of generators that $\mathbb{Z}_p^*$ can have, for a prime p. That is, come up with an absolute constant $0 \le c \le 1$ such that for all primes $p > 2$,

$$\mathcal{G}_p \stackrel{\mathsf{def}}{=} \frac{\left|\{g : g \text{ is a generator of } \mathbb{Z}_p^*\}\right|}{|\mathbb{Z}_p^*|} \le c$$

   Furthermore, describe an infinite sequence of prime numbers $\{p_k\}$ such that

$$\mathcal{G}_{p_k} \to c \text{ as } k \to \infty$$

2. **(10 points)** Compute $2^{50} \pmod{51}$.

   Why doesn't your answer violate Fermat's little theorem?

   More generally, if $2^{m-1} \neq 1 \pmod{m}$ for a number m, what interesting fact does that tell you about m?

3. **(5 points)** Compute the following quantities quickly, utlizing one of the two fast exponentiation methods you saw in class. (Note, though, that I am not asking you to exactly optimize the number of steps.) Show your work.

   - $2^{42} \pmod{63}$.
   - $2^{2013} \pmod{13}$.

4. **(5 points)** Compute the last two digits of 3^{1999}.

5. **(15 points)** Given a prime number p, the prime factorization of $\phi(p) = p - 1$ as

$$p - 1 = \prod_{\mathsf{primes}\ q_i} q_i^{e_i} \qquad\qquad \text{(for positive integers } e_i\text{)}$$

   and a number $g \in \mathbb{Z}_p^*$, come up with a procedure to check whether g is a generator modulo p.

   (Recall: we saw how to do this in class for safe primes p. This questions asks you how to generalize this for arbitrary primes.)

   Your procedure should run fast, in the sense it should take about 100 to 1000 steps for a 100 digit number p, and not something like 10^{100} steps. I will not ask you to analyze the number of steps your procedure takes, but you should do it if it interests you.

6. **(10 points)** Compute the following discrete logarithms.

   - Is 2 a generator in the group $\mathbb{Z}_{19}^*$? Compute $\mathsf{dlog}_2\ 15$ in the group $\mathbb{Z}_{19}^*$.

- Is 2 a generator in the group $\mathbb{Z}_{23}^*$? Compute $\mathsf{dlog}_2\, 7$ in the group $\mathbb{Z}_{23}^*$.

7. **(15 points)** What are the two possible values of $2^{(p-1)/2} \pmod p$ for any prime p? Prove your answer correct.

8. **(20 points)** We will study the notion of square roots in the group $\mathbb{Z}_p^*$ for prime p. $x \in \mathbb{Z}_p^*$ is a square root of $b \in \mathbb{Z}_p^*$ if
$$x^2 = b \pmod p$$
If b has a square root in $\mathbb{Z}_p^*$, then b is called a *square*, otherwise it is called a *non-square*.

   It is a theorem that for every prime p, every number $b \in \mathbb{Z}_p^*$ has either two square roots or no square roots at all.

   - Find the square roots of (a) 2 mod 7, (b) 7 mod 11, and (c) 5 mod 11.
   - If x is a square root of b mod p, what is the other square root of b?
   - How many square roots does 1 have modulo 8? Why doesn't your answer contradict the theorem above?
   - Let p be an odd prime and g be a generator in $\mathbb{Z}_p^*$. Then, any number b can be written as $g^k \pmod p$ for some integer k. Prove that b is a square *if and only if* k is even.

The following is a *challenge question*. It carries no points whatsoever, and you are not required to answer it. However, for those of you who like the challenge, I recommend you try it out and write down a solution.

Challenge Question: This comes in two parts.

- How do you determine quickly if $b \in \mathbb{Z}_p^*$ is a square or not?
- Recall that in the description of the Diffie-Hellman key exchange protocol, we let g be an element of order q in $\mathbb{Z}_p^*$, where $p = 2q + 1$ is a safe prime. What happens if instead, we let g be a generator of $\mathbb{Z}_p^*$? Show that the adversary Eve can learn *one bit* of information about the eventual shared key $K = K_A = K_B$ given g, $g^a \pmod p$ and $g^b \pmod p$ alone.