Homework 5

Due Thursday, October 7

Implementation Part

1. Implement Sun-Tzu's algorithm for solving concurrent congruences (in the book this is called the Chinese Remainder Theorem). Specifically, define a function `SunTzu(moduli,residues)` which satisfies the following:

Input	Output
A list of moduli $m_1, \cdots, m_t$ (positive integers)	If moduli are pairwise coprime
A list of integers $a_1, \cdots, a_t$	x satisfying $x \equiv a_i \mod m_i$ for all i.
	Otherwise an error message.

Hints:

- One way you could do this is to make an auxiliary function `SunTzuPairs(m1,m2,a1,a2)` which solves the problem for 2 congruences, and have `SunTzu` feed recursively into `SunTzuPairs`
- Naively checking the moduli are coprime takes running the Euclidean algorithm $\mathcal{O}(t^2)$ times, but you should be able to do so only running it $\mathcal{O}(t)$ time.

2. Implement the Pohlig-Hellman algorithm to solve the DLP for an element $g \in \mathbb{F}_p^*$ of order $N = m_1 m_2 ... m_t$ (for coprime m_i). Specifically, define a function `pohligHellman(g,h,p,factors)`

Input	Output
A prime p	$\log_g(h)$ if it exists
An element $g \in \mathbb{F}_p^*$	
An element $h \in \mathbb{F}_p^*$	
The prime power factors $m_1, \cdots m_t$ of $\lvert g \rvert$	

Hints

- The structure should loosely be as follows. Reduce the problem to solving the DLP for elements of smaller order, let `babyGiant` solve those problems (make sure to tell it the order is smaller, otherwise you aren't saving any time), and then use `SunTzu` to stitch them together.
- It is difficult in general to compute $|g|$ (about as difficult as factoring $p-1$), and so checking if the m_i are indeed the prime factors of $|g|$ may be difficult. Instead, check that $g^{m_1 m_2 ... m_t} = 1$. In this case your algorithm should still work (see Problem 6).

3. Use `SunTzu` to solve to following sets of congruences, and check that the solution given works.

   (a) $x \equiv 9 \mod 23$ and $x = 25 \mod 41$

(b)

$$\begin{aligned} x &\equiv 1 \mod 2 \\ x &\equiv 2 \mod 3 \\ x &\equiv 4 \mod 5 \\ x &\equiv 6 \mod 7 \\ x &\equiv 10 \mod 11 \\ x &\equiv 1 \mod 13 \\ x &\equiv 16 \mod 17 \end{aligned}$$

4. Let's test out Pohlig-Hellman.

   (a) Let $p = 113$. Last week we used baby steps-giant steps to compute $\log_3 19$ modulo p. Notice that 112 factors as $2^4 * 7$. Use this information and Pohlig-Hellman to compute $\log_3 19$ and see if your answer matches.

   (b) Let $p = 302353671346363311 49$. Last week we tried using baby steps-giant steps to compute the discrete log $\log_6 3295$ modulo p. You might have had trouble getting it to run. I did. What if I told you that $p-1$ has the following prime factorization?

   $$p - 1 = 2^2 * 3^2 * 13 * 41143 * 335341 * 4682597.$$

   Now use Pohlig-Hellman to speed up your computation. (It speeds it up considerably!). Use fast powering to make sure you got the right answer (it is very satisfying!).

Written Part

5. For `pohligHellman` instead of checking that the m_i were indeed the prime power factors of $|g|$, we just checked that $g^{m_1 m_2 \cdots m_t} = 1$. Prove that if this condition holds (and the m_i are still coprime) that `pohligHellman` returns the correct logarithm.

6. Show that `SunTzu` runs in $\mathcal{O}(\log N)$ steps where $N = m_1 m_2 \cdots m_t$ is the product of the moduli. (You may assume your basic operations $+, -, \times, \div, \%$ are all $\mathcal{O}(1)$.

7. Let's prove the uniqueness part Sun-Tzu's theorem.

   (a) Let a, b, c be positive integers and suppose that:

   $$a|c, \quad b|c, \quad \gcd(a, b) = 1.$$

   Then $ab|c$.

   (b) Suppose $m_1, \cdots, m_t$ are pairwise coprime positive integers, and suppose $a_1, \cdots, a_t \in \mathbb{Z}$. Show that if y and z are both solutions to the system of congruences

   $$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \\ &\vdots \\ x &\equiv a_t \mod m_t, \end{aligned}$$

   then $y \equiv z \mod m_1 m_2 \ldots m_t$

Let's finish by proving the following theorem:

Theorem 1. *Let m be an odd number and a an integer not divisble by any of the prime factors of m. Then a has a square root mod m if and only if $a^{\frac{p-1}{2}} \equiv 1 \mod p$ for every prime factor p of m.*

8. (a) Let a be an integer not divisble by an odd prime p. Show that a has a square root mod p if and only if $a^{\frac{p-1}{2}} \equiv 1 \mod p$. (*Hint:* Use HW2 Problem 8.)

   (b) Let $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ and a an integer. Show that a has a square root mod m if and only if it has a square root mod $p_i^{\alpha_i}$ for each i. (*Hint:* Use Sun-Tzu's Theorem.)

   (c) Let m be an odd number and suppose a is an integer not divisible by any prime factor of m. Show a has a square root mod m if and only if it has a square root mod p for every prime p dividing m. (*Hint:* Use HW4 Problem 7).

   (d) Deduce Theorem 1 from parts (a),(b), and (c) above.

   (e) Can you relax any of the hypotheses of Theorem 1? For example, what if m is even? Or what if some prime factor of m divides a? Compute some examples and informally discuss your thoughts.

   (f) Explain why part (a) also solves the bonus question of HW3 Problem 6(f).