Homework 8

Due Thursday, November 4

Implementation Part

1. Let's begin by writing functions that efficiently compute Legendre and Jacobi symbols.

   (a) Write a function `legendreSymbol(a,p)` which takes as input an integer a and an *odd* prime p, and returns the Legendre symbol $\left(\frac{a}{p}\right)$ in $\mathcal{O}(\log(p))$ time.

   (b) Write a function `jacobiSymbol(a,b)` which takes as input integers a and b where b is odd and positive and returns the Jacobi symbol $\left(\frac{a}{b}\right)$ *without factoring* b. We remind you of the following properties of Jacobi symbols which should help with your computation.

   - This only depends on the residue of a modulo b.
   - If $a \equiv -1, 0, 1, 2 \mod b$ this is easy to compute directly (using quadratic reciprocity for -1 and 2).
   - If b is prime then this is a Legendre symbol! (`probablyPrime` will help determine this quickly).
   - You can use quadratic reciprocity to relate $\left(\frac{a}{b}\right)$ and $\left(\frac{b}{a}\right)$. Since we can reduce b modulo a this gives us a strictly smaller problem! (**Warning:**, if a is even the $\left(\frac{b}{a}\right)$ doesn't make sense! You will have to factor out the 2's from a use the multiplicativity of the Jacobi function to deal with this case!)

   (c) Compute the following Jacobi symbols. For the first 3 you can check your work by hand.

$$\left(\frac{8}{15}\right), \left(\frac{11}{15}\right), \left(\frac{12}{15}\right), \left(\frac{171337608}{536134436237}\right).$$

Written Part

2. This problem is part written, part implementation. We'll walk through a toy example of using the index-calculus to solve a discrete log. There will be some calculations you'll want to do in Sage. Turn in these calculations as part of the implementation part, labelling the cells as "Calculations for Problem 2".

   Let $g = 17$ and $p = 19079$. Let's compute $\log_g 19$.

   (a) Verify in Sage that $g^i \mod p$ is 5-smooth for $i = 3030, 6892, 18312$. Record their factorizations. (You may use Sage's `factor` function.)

   (b) Let $x_\ell = \log_g \ell$ for $\ell = 2, 3, 5$. Use the factorizations from part (a) to right down 3 linear equations modulo $p - 1$ that x_2, x_3, x_5 satisfy.

   (c) Notice that $p - 1 = 2 * q$ where $q = 9539$ is prime. Therefore you can use Gaussian elimination to solve for x_2, x_3, and x_5 modulo 2 and modulo q. You are welcome to use Sage to do this. Now use Sun-Tzu's theorem to compute x_2, x_3, x_5.

   (d) Verify in Sage that $19g^{-12400}$ is 5-smooth. Record it's factorization.

   (e) Use the factorization from part (d) to write $\log_g 19$ in terms of of x_2, x_3, x_5. Therefore, using part (c), compute $\log_g 19$.

   (f) Verify that your answer is correct using fast powering.

3. (a) Let p be prime. Verify that the Legendre Symbol satisfies the following 2 identities
   i. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.
   ii. If $a \equiv b \mod p$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

   (b) Verify that the Jacobi Symbol satisfies the following 3 identities.
   i. $\left(\frac{a_1 a_2}{b}\right) = \left(\frac{a_1}{b}\right)\left(\frac{a_2}{b}\right)$.
   ii. $\left(\frac{a}{b_1 b_2}\right) = \left(\frac{a}{b_1}\right)\left(\frac{a}{b_2}\right)$.
   iii. If $a_1 \equiv a_2 \mod b$ then $\left(\frac{a_1}{b}\right) = \left(\frac{a_2}{b}\right)$.

4. Compute the Jacobi symbols $\left(\frac{8}{15}\right), \left(\frac{11}{15}\right), \left(\frac{12}{15}\right)$ by hand and confirm your solutions from 1(c) are correct.

5. Here we give another characterization of the Legendre symbol from a group theoretic perspective.

   (a) Let G, H, K be groups, and let $\varphi : G \to H$ and $\psi : H \to K$ be homomorphisms. Show that the composition $\psi \circ \varphi : G \to K$ is a homomorphism.

   (b) Show that the set $\{\pm 1\}$ is a group under multiplication.

   (c) Let N be a positive even integer. Show that the map $\mathbb{Z}/N\mathbb{Z} \to \{\pm 1\}$ given by the rule $x \mapsto (-1)^x$ is a well defined homomorphism (where the group law for $\mathbb{Z}/N\mathbb{Z}$ is addition). What goes wrong if N is odd?

   (d) Let p be an odd prime, and let $g \in \mathbb{F}_p$ be a primitive root. Show that the composition

$$\mathbb{F}_p^* \xrightarrow{\log_g(\cdot)} \mathbb{Z}/(p-1)\mathbb{Z} \xrightarrow{(-1)^x} \{\pm 1\}$$

   is equal to the Legendre function $x \mapsto \left(\frac{x}{p}\right)$. Use this together with part (a)-(c) to give another proof that the Legendre symbol is multiplicative.

6. On previous assignments we've extesively studied the notion of squares modulo p (i.e., *quadratic residues mod* p), and one thing we noticed is that the situation differed depending on whether p was even or odd (i.e., it depended on the residue of p modulo 2). Here we begin our exploration of cube roots modulo p, and we will notice that the story depends on the the residue of p modulo 3. First a definition:

   Definition 1. *Let p be a prime number. An integer a is called a cubic residue mod p if $p \not| a$ and there exists an integer c satisfying $c^3 \equiv a \mod p$.*

   Let's begin by studying the case where $p \equiv 1 \mod 3$. **For parts (a)-(d), assume** $p \equiv 1 \mod 3$.

   (a) Let a, b be cubic residues modulo p. Show that ab is a cubic residue mod p.

   (b) Give an example to show that if a and b are cubic nonresidues mod p, then ab could also be a nonresidue. Explain why this is different from the situation of quadratic residues.

   (c) Let g be a primitive root for $\mathbb{F}_p$. Show that a is a cubic residue modulo p if and only if $\log_g a$ is a multiple of 3.

   (d) Show that if a is a cubic residue modulo p, then a has precisely 3 cube roots modulo p.

(e) Part (c) showed that if $p \equiv 1 \mod 3$ then one third of the elements of $\mathbb{F}_p^*$ have cube roots. The case where $p \equiv 2 \mod 3$ is quite different. Suppose $p \equiv 2 \mod 3$. Show that every integer has a cube root modulo p. If $p \not| a$, how many cube roots does a have mod p?

(f) Like in the case of square roots mod 2, the case of cube roots mod 3 is different still. Show that every integer has *precisely 1* cube root modulo 3.

(g) In fact, it is a general principle that pth roots modulo p are very simple. Prove that if p is prime every integer has precisely one pth root modulo p. (*Hint*: Fermat's little theorem.)

7. In class we suggested that the problem of factoring a number N is in some sense equivalent to being able to compute square roots modulo N. In this problem we will make this precise, for $N = pq$ a product of 2 distinct **odd** primes. Simultaneously, we will verify that most integers have four square roots mod pq, which was an important input in the quadratic sieve.

   (a) Suppose you know the factorization of N into pq. Describe an algorithm to efficiently compute whether a has a square root modulo N, and prove the correctness of your algorithm.

   (b) Suppose $\gcd(a, N) = 1$. Show that if a has one square root modulo N, then it exactly 4 square roots modulo N. In the case where $\gcd(a, N) \neq 1$, how many square roots might a have? Why?

   (c) Suppose you know the factorization of N into pq. Describe an algorithm to compute all the square roots of a modulo N if they exist. Prove the correctness of your algoritm. (You may assume you have a fast algorithm to compute square roots modulo primes.)

   (d) Conversely, suppose you have an oracle that can tell you all the square roots of a modulo N if they exist. Describe a way to use constultation with this oracle to factor N. Prove your method works.