Homework 8 Solutions

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.)

   Proof. We computed in sage:

   $$g^{3030} \equiv 14580 = 2^2 * 3^6 * 5 \quad (1)$$
   $$g^{6892} \equiv 18432 = 2^{11} * 3^2 \quad (2)$$
   $$g^{18312} \equiv 6000 = 2^4 * 3 * 5^3 \quad (3)$$

   □

   (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.

   Proof. We apply $\log_g$ to equations (1),(2),(3) above and get the following congruences modulo $p - 1$:

   $$\begin{aligned} 3030 &\equiv 2x_2 + 6x_3 + x_5 \\ 6892 &\equiv 11x_2 + 2x_3 \\ 18312 &\equiv 4x_2 + x_3 + 3x_5 \end{aligned}$$

   □

   (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.

   Proof. We are trying to solve the system:

   $$\begin{pmatrix} 2 & 6 & 1 \\ 11 & 2 & 0 \\ 4 & 1 & 3 \end{pmatrix} \begin{pmatrix} x_2 \\ x_3 \\ x_5 \end{pmatrix} = \begin{pmatrix} 3030 \\ 6892 \\ 18312 \end{pmatrix},$$

   modulo 2 and q. We do this using sage, and get that:

   $$\begin{aligned} x_2 &\equiv 8195 \mod q \\ x_3 &\equiv 1299 \mod q \\ x_5 &\equiv 7463 \mod q. \end{aligned}$$

Modulo 2, the target of our matrix is all even, so that we can directly observe (0,0,0) as a solution. We use sage to converm this and see that:

$$(x_2, x_3, x_5) \equiv (0, 0, 0) \mod 2.$$

Using `SunTzu` we are able to then compute:

$$\begin{aligned} x_2 &\equiv 17734 \mod p-1 \\ x_3 &\equiv 10838 \mod p-1 \\ x_5 &\equiv 17002 \mod p-1 \end{aligned}$$

□

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

Proof. We verify that:

$$19g^{-12400} \equiv 384 = 2^7 * 3, \tag{4}$$

which is indeed 5-smooth. □

(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 $\log_g 19$.

Proof. Applying $\log_g$ to Equation (4) we have:

$$\log_g 19 - 12400 = 7x_2 + x_3 = 7(17734) + 10838.$$

Thefore we can solve:

$$\log_g 19 = 7 * 17734 + 10838 + 12400 \equiv 13830 \mod p-1.$$

□

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

Proof. Indeed we can check using fast powering that $g^{13830} \equiv 19 \mod p$. □

3. (a) Let p be prime. Verify that the Legendre Symbol satisfies the following 2 identities

i. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Proof. One proof of this is given below in Problem 5(d). We can also used Euler's criterion (HW5 Probelm 8(a)) to compute:

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

□

ii. If $a \equiv b \mod p$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Proof. This follows from Euler's criterion, and the compatibility lemma from HW1 Problem 8:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}} \equiv \left(\frac{b}{p}\right).$$

□

(b) Verify that the Jacobi Symbol satisfies the following 3 identities.

i. $\left(\frac{a_1a_2}{b}\right) = \left(\frac{a_1}{b}\right)\left(\frac{a_2}{b}\right)$.

Proof. Give a prime factoriztion $b = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$, and apply part (a)(i):

$$\begin{aligned}\left(\frac{a_1a_2}{b}\right) &= \left(\frac{a_1a_2}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a_1a_2}{p_t}\right)^{\alpha_t} \\ &= \left(\frac{a_1}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a_1}{p_t}\right)^{\alpha_t} \left(\frac{a_2}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a_2}{p_t}\right)^{\alpha_t} \\ &= \left(\frac{a_1}{b}\right)\left(\frac{a_2}{b}\right).\end{aligned}$$

□

ii. $\left(\frac{a}{b_1b_2}\right) = \left(\frac{a}{b_1}\right)\left(\frac{a}{b_2}\right)$.

Proof. Give prime factorizations $b_1 = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ and $b_2 = q_1^{\beta_1} \cdots q_r^{\beta_r}$. Then $p_1^{\alpha_1} \cdots p_t^{\alpha_t} q_1^{\beta_1} \cdots q_r^{\beta_r}$ is a prime factorization of b_1b_2 so that we may directly compute:

$$\left(\frac{a}{b_1b_2}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a}{p_t}\right)^{\alpha_t} \left(\frac{a}{q_1}\right)^{\beta_1} \cdots \left(\frac{a}{q_r}\right)^{\beta_r} = \left(\frac{a}{b_1}\right)\left(\frac{a}{b_2}\right).$$

□

iii. If $a_1 \equiv a_2 \mod b$ then $\left(\frac{a_1}{b}\right) = \left(\frac{a_2}{b}\right)$.

Proof. Give a prime factorization $b = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$, and apply part (a)(ii) to compute:

$$\left(\frac{a_1}{b}\right) = \left(\frac{a_1}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a_1}{p_t}\right)^{\alpha_t} = \left(\frac{a_2}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a_2}{p_t}\right)^{\alpha_t} = \left(\frac{a_2}{b}\right).$$

□

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.

Proof.

$$\left(\frac{8}{15}\right) = \left(\frac{8}{3}\right)\left(\frac{8}{5}\right) = \left(\frac{2}{3}\right)\left(\frac{3}{5}\right) = (-1)(-1) = 1,$$

where we verify directly that 2 is not a square mod 3 and 3 is not a square mod 5.

$$\left(\frac{11}{15}\right) = \left(\frac{11}{3}\right)\left(\frac{11}{5}\right) = \left(\frac{2}{3}\right)\left(\frac{1}{5}\right) = (-1)(1) = -1,$$

where again 2 is not a square mod 3, but 1 is certainly a square mod 5.

$$\left(\frac{12}{15}\right) = \left(\frac{12}{3}\right)\left(\frac{12}{5}\right) = \left(\frac{0}{3}\right)\left(\frac{2}{5}\right) = (0)(-1) = 0.$$

□

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.

   Proof. Leg $g, g' \in g$. Then:

   $$\begin{aligned} \psi \circ \varphi(g *_G g') &= \psi(\varphi(g *_G g')) \\ &= \psi(\varphi(g) *_H \varphi(g')) \\ &= \psi(\varphi(g)) *_K \psi(\varphi(g')) \\ &= (\psi \circ \varphi(g)) *_K (\psi \circ \varphi(g')) \end{aligned}$$

   so that $\psi \circ \varphi$ is a homomorphism. □

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

   Proof. Closure under multiplication is clear, and the multiplicative unit is certainly 1. Associativity is inherited from $\mathbb{Z}$. The inverse of 1 is itself, and the inverse of -1 is -1. □

   (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?

   Proof. We first show that the map is well defined. Notice that:

   $$(-1)^x = \begin{cases} 1 & x \text{ is even} \\ -1 & x \text{ is odd} \end{cases}.$$

   If $x \equiv y \mod N$, then $x \equiv y \mod 2$ since $2|N$ (here we use N is even in an important way!). Therefore $(-1)^x = (-1)^y$ so the map is well defined. To see it is a homomorphism we fix $x, y \in \mathbb{Z}/N\mathbb{Z}$ and represent each by integers (the choice doesn't matter since the map is well defined). Then the normal exponentiation rules imply $(-1)^{x+y} = (-1)^x(-1)^y$ so that the map is indeed a homomorphism. □

   (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.

   Proof. By Homework 3 Problem 6(e), $a \in \mathbb{F}_p^*$ is a quadratic residue if and only if $\log_g(a)$ even. But this holds if and only if $(-1)^{\log_g a} = 1$. So $(-1)^{\log_g a}$ is 1 if and only if $\left(\frac{a}{p}\right) = 1$, completing the proof.

   By parts (a) and (c) this composition is a homomorphism, i.e., it commutes with multiplication. Since the composition is equal to the Legendre symbol, this implies 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 $p \nmid a$ 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.

Proof. Since $\mathbb{F}_p^*$ is closed under multipication, we see that $p \nmid a, b$ implies $p \nmid ab$. Let $c^3 \equiv a \mod p$ and $d^3 \equiv b \mod p$. Then $(cd)^3 = c^3 d^3 \equiv ab \mod p$ so that ab is indeed a cubic residue. □

(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.

Proof. Let $p = 7$, so that $\mathbb{F}_p^* = \{1, 2, 3, 4, 5, 6\}$. Cubing each gives the cubic residues $(\mathbb{F}_p^*)^3 = \{1, 6\}$. In particular, 3 and 4 are not cubic residues, but their product $12 \equiv 5 \mod 7$ is not a cubic residue either.

For the case of quadratic residues, the multiplicativity of the Legendre symbol shows that the product of two quadratic nonresidues is a quadratic residue, but we see this is not the case for cubic 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.

Proof. We consider the discrete log map:

$$\log_g(\cdot) : \mathbb{F}_p^* \to \mathbb{Z}/(p-1)\mathbb{Z}.$$

Notice that $\log_g(x^3) = 3\log_g(x)$, so in particular, cubing in $\mathbb{F}_p^*$ corresponds to multiplying by 3 in $\mathbb{Z}/(p-1)\mathbb{Z}$. We therefore have the following principle, which we label as a Lemma for future reference.

Lemma 1. *Let $a \in \mathbb{F}_p^*$ and let $c = \log_g a$. Then the discrete log map gives a bijection between the cube roots of a mod p and solutions to*

$$3x \equiv c \mod p - 1. \tag{5}$$

Proof. Let $b^3 \equiv a \mod p$. Then

$$\log_g b^3 \equiv 3\log_g b \equiv \log_g a = c \mod p - 1,$$

giving a solution to Equation 5. Conversely given a d such that $3d \equiv c \mod p-1$, we have:

$$(g^d)^3 \equiv g^{3d} \equiv g^c \equiv a \mod p.$$

□

With this in hand, solving part (c) is easy. In particular, Lemma 1 implies that a is a cubic residue if and only if there is a solution to Equation 5. By Homework 2 Problem 7(a) such a solution exists if and only if $\gcd(3, p-1)$ divides $c = \log_g a$. Since $p \equiv 1 \mod 3$, $p-1$ is divisible by 3, so that $\gcd(3, p-1) = 3$. In particular, we have showed that a is a cubic residue if and only if 3 divides $\log_g a$, as desired. □

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

Proof. Suppose a is a cubic residue. By Lemma 1, cube roots of a correspond to solutions to Equation 5. Since we know there is at least one, by Homework 2 Problem 7(b), there are precisely $\gcd(3, p-1)$. Since $p \equiv 1 \mod 3$ we have that $\gcd(3, p-1) = 3$, giving the result. □

(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?

Proof. We again apply Lemma 1, noticing that a has a cube root if and only if Equation 5 has a solution. Since $p \equiv 2 \mod 3$, we have $\gcd(3, p-1) = 1$, so that 3 is invertible in $\mathbb{Z}/(p-1)\mathbb{Z}$. In particular, Equation 5 always has a *unique* solution. By Lemma 1 we see that a always has a *unique* cube root! □

(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.

Proof. By Fermat's little theorem, we have $a^3 \equiv a \mod 3$ for any a, so that every element has a unique cube root: *itself*! □

(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.)

Proof. By Fermat's little theorem, we have $a^p \equiv a \mod p$ for any a, so that every element has a unique cube root: *itself*! □

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.

Proof. By Homework 5 problem 8(b), a has a square root mod N if and only if it has a square root mod p and a square root mod q. Furthermore, applying Homework 5 Problem 8(a), a has a square root mod p if and only if it is either $0 \mod p$, or else $a^{\frac{p-1}{2}} \equiv 1 \mod p$. This precisely means that the legendre symbol $\left(\frac{a}{p}\right) \neq -1$. Similar considerations hold for q so the following algorithm works:

(1) Input a, N and the factorization $N = pq$: An algorithm to determine if a has a square root modulo N.
(2) If $a^{\frac{p-1}{2}} \not\equiv -1 \mod p$ and $a^{\frac{q-1}{2}} \not\equiv -1 \mod q$, return `True`.
(3) Else return `False`.

□

(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?

Proof. By Sun-Tzu's theorem, given 2 congruences $x \equiv b \mod p$ and $x \equiv c \mod q$, there is a unique element of $\mathbb{Z}/N\mathbb{Z}$ solving two congruences. We can interpret this as saying the reduction map $d \mapsto (\overline{d}, \overline{d})$ gives a bijection:

$$\{d \in \mathbb{Z}/N\mathbb{Z}\} \leftrightarrow \{(b, c) \text{ where } b \in \mathbb{Z}/p\mathbb{Z} \text{ and } c \in \mathbb{Z}/q\mathbb{Z}\}. \tag{6}$$

By HW 5 Problem 8(b), that d is a square root of a modulo N if and only if it is one modulo p and modulo q. Therefore, Equation (6) restricts to a bijection:

$$\left\{ \begin{array}{c} \text{Square roots} \\ \text{of } a \text{ modulo } N. \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{Pairs } (b, c) \text{ where } b \text{ is a square root} \\ \text{of } a \text{ modulo } p \text{ and } c \text{ is one modulo } q. \end{array} \right\} \tag{7}$$

We are trying to compute the size of the left hand side of Equation (7), so this bijection means it suffices to compute the size of the right side. With this in mind, suppose a has a square root mod N. Then a has a square root b modulo p and a square root c modulo q. If a is nonzero mod p it has 2 square roots mod p: b and $p - b$. And similarly if a is nonzero mod q both c and $q - c$ are square roots. Therefore if a is prime to N the set on the right in Equation (7)

$$\{(b, c), (p - b, c), (b, q - c), (p - b, q - c)\}.$$

Therefore a has four square roots mod N. We briefly describe the other possibilities. Assume that we still have have a square root of a modulo N, and let $g = \gcd(a, N)$.

g=N: In this case $a \equiv 0 \mod N$ so the only square root of a is 0 itself. This corresponds to the pair $(0, 0)$ on the righthandside of Equation (7).

g=p: In this case $a \equiv 0 \mod p$, so it only has one square root modulo p. Therefore the righthandside of Equation (7) consists of the set $\{(0, c), (0, p - c)\}$, so that a has 2 square roots.

g=q: This case is symmetric to $g = p$, and a has 2 square roots.

We observe then that the only possibilities for the number of square roots of a are $1, 2, 4$ (if any), and that this number is controlled exactly by the value of g. Notice that a can never have exactly 3 square roots mod N. Compare this to the case where $p = q$ (studied in Homework 4 Problem 7), where the only possibilities were 1 and 2. □

(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.)

Proof. By Equation (7) above, all the square roots of a modulo N come from computing the square roots of a modulo p and modulo q, and *stitching them together* using the Sun-Tzu's theorem. Therefore the following algorithm works:

(1) Input a, N and the factorization $N = pq$: An algorithm to compute all the square roots of a modulo N.
(2) Compute all the square roots b_i of a modulo p.
(3) Compute all the square roots c_j of a modulo q.
(4) Use the Sun-Tzu algorithm from Homework 5 Problem 1 to compute $d_{ij} =$ `SunTzu(p,q,bi,cj)`, the unique element such that $d_{ij} \equiv b_i \mod p$ and $d_{ij} \equiv c_j \mod q$.
(5) Return the complete list of d_{ij}. These are the square roots of a.

□

(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.

Proof. Pick some nonzero $a \in \mathbb{Z}/N\mathbb{Z}$ and suppose $\gcd(a, N) = 1$, and suppose we can compute all the square roots (r_1, r_2, r_3, r_4) of a modulo N. Then we can choose a pair of square roots such that $r_i \neq \pm r_j \mod N$. Then both $r_i - r_j, r_i + r_j$ are nonzero modulo N. But:

$$(r_i - r_j)(r_i + r_j) = r_i^2 - r_j^2 \equiv a - a \equiv 0 \mod N.$$

So $(r_i - r_j)(r_i + r_k) = kN$ for a positive number k, and it looks like we've come pretty close to finding a factorization of N. Indeed, let $g = \gcd(N, r_i - r_j)$. Then g is one of $1, p, q, N$. We can eliminate N because we already saw that $r_i - r_j$ is nonzero modulo N. On the other hand if $g = 1$, then both p and q divide $r_i + r_j$, so that $pq = N$ does. But we also saw that $r_i + r_j$ is nonzero modulo N. Therefore $g = p$ or $g = q$, and we have found a nontrivial factor of N.

This only takes care of the case where $\gcd(a, N) = 1$, but of course, otherwise it would be other p or q and we would already have our factorization. We have therefore showed that the following algorithm works:

(1) Given N and a way to compute square roots, factor N.
(2) Choose nonzero $a \in \mathbb{Z}/N\mathbb{Z}$ and compute $g = \gcd(a, N)$.
(3) If $g \neq 1$ then return the factors $(g, N/g)$.
(4) Otherwise compute the four square roots r_1, r_2, r_3, r_4 of a modulo N.
(5) Find r_i, r_j such that $r_i \neq \pm r_j$ modulo N. Then compute $g = \gcd(r_i - r_j, N)$, and return the factors $(g, N/g)$.

□