Homework 5 Written Solutions

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.

   Proof. Let N be the product of the m_i. The algorithm we wrote returns an x such that $x \equiv \log_{g_i} h_i \mod m_i$ where $g_i = g^{N/m_i}$ and $h_i = h^{N/m_i}$. In particular, we see that

$$g^{xN/m_i} \equiv h^{N/m_i} \mod p.$$

   Applying the discrete log map $\log_g$ we get that

$$x\frac{N}{m_i} \equiv \log_g h \frac{N}{m_i} \mod |g|. \tag{1}$$

   Notice that $\gcd(N/m_1, \cdots N/m_t) = 1$ so that there exists $u_1, \cdots, u_t \in \mathbb{Z}$ with

$$u_1\frac{N}{m_1} + \cdots + u_t\frac{N}{m_t} = 1.$$

   Therefore taking the linear combinations of the Congruences 1 above as i vary, and scaling each with u_i gives:

$$\begin{aligned} x &= x\sum u_i \frac{N}{m_i} \\ &= \sum u_i \left(x\frac{N}{m_i}\right) \\ &\equiv \sum u_i \left(\log_g h \frac{N}{m_i}\right) \mod |g| \\ &= \log_g h \sum u_i \frac{N}{m_i} \\ &= \log_g h, \end{aligned}$$

   completing the proof. □

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 $\mathcal{O}(1)$.

   Proof. We first discuss the time complexity of `SunTzuPairs(m1,m2,a1,a2)`. Other than basic algebraic manipulations, all the algorithm does is run the extended Euclidean algorithm on m_1 and m_2 in order to compute their gcd and invert m_1 modulo m_2. This we saw in class that this takes $2 + \log_2(m) = \mathcal{O}(\log m)$ steps where $m = \min(m_1, m_2)$.

   Now for `CRT`. Other than basic list manipulations, all `SunTzu` does is call `SunTzuPairs` repeatedly. On the i'th step it calls `SunTzuPairs` on $m_1 m_2 \cdots m_i, m_{i+1}$ which we saw takes $\mathcal{O}(\log(\min(m_1 \cdots m_i, m_{i+1}))) = \mathcal{O}(\log(m_{i+1}))$. Adding these all up we see that `SunTzu` runs in

$$\mathcal{O}\left(\sum \log(m_i)\right) = \mathcal{O}\left(\log\left(\prod m_i\right)\right) = \mathcal{O}(\log N)$$

   as desired. □

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 $ab|c$.

   Proof. Notice $1 = au + bv$. Multiplying through by c we have $c = cau + cbv$. Since $c = kb = la$ for some k, l by assumption, we can substitute this in and get:

   $$c = kbau + labv = ab(ku + lv),$$

   so that ab divides c as desired. □

   (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 $y \equiv z \mod m_1 m_2 \dots m_t$

   Proof. We proceed by induction. The base case where $t = 1$ is tautological. For the general case, suppose y and z satisfy all t congruences. Then in particular they satisfy the first $t - 1$ congruences so that by induction we may assume that:

   $$y \equiv z \mod m_1 m_2 \cdots m_{t-1}.$$

   Since they both satisfy the t'th congruence we also know that

   $$y \equiv z \mod m_t.$$

   In particular, both $m_1 \cdots m_{t-1}$ and m_t divide $y - z$. Since $\gcd(m_1 \cdots m_{t-1}, m_t) = 1$ we may apply part (a) and conclude that the product $m_1 m_2 \cdots m_t$ divides $y - z$ whence the result follows. □

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.)

Proof. Let g be a primitive root for $\mathbb{F}_p^*$. Then $a \equiv g^k \mod p$ from some k, and we showed in HW2 Problem 8(d) that a is a square if and only if k is even. If $k = 2l$ is even then

$$a^{\frac{p-1}{2}} \equiv (g^{2l})^{\frac{p-1}{2}} = g^{l(p-1)} \equiv 1 \mod p.$$

Conversely, suppose that

$$a^{\frac{p-1}{2}} \equiv g^{\frac{k(p-1)}{2}} = 1.$$

Then $|g|$ divides $k(p-1)/2$. Since $|g| = p-1$ there is some integer l such that $(p-1)l = k(p-1)/2$. Solving for k gives $k = 2l$ so that it is even. Therefore a is a square completing the proof. □

(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.)

Proof. The forward direction is immediate, as any square root of a modulo m would serve as a square root modulo any divisor of m as well. Conversely, suppose a has a square root mod $p_i^{\alpha_i}$ for all i. In particular, for all i there exists some $b_i \in \mathbb{Z}$ such that $b_i^2 \equiv a \mod p_i^{\alpha_i}$. One can then consider the system of congruences:

$$\begin{aligned} x &\equiv b_1 \mod p_1^{\alpha_1} \\ x &\equiv b_2 \mod p_2^{\alpha_2} \\ &\vdots \\ x &\equiv b_t \mod p_t^{\alpha_t} \end{aligned}$$

By Sun-Tzu's theorem there exists some b such satisfying all these congruences. We claim that this is the square root of a modulo m. Indeed, since

$$b^2 \equiv b_i^2 \equiv a \mod p_i^{\alpha_i},$$

for each i, b^2 solves the system of congruences:

$$\begin{aligned} x &\equiv a \mod p_1^{\alpha_1} \\ x &\equiv a \mod p_2^{\alpha_2} \\ &\vdots \\ x &\equiv a \mod p_t^{\alpha_t}. \end{aligned}$$

But obviously so does a. By the uniqueness part of the Chinese remainder theorem (Probem 8(b) on this assignment), we may conclude that $b^2 \equiv a \mod m$. □

(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).

Proof. The forward direction is immediate, as any square root of a modulo m would serve as a square root modulo any divisor of m as well. Conversely, suppose $m = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ as a product of odd primes none dividing a, and suppose a is a square modulo each p_i. Then by HW4 Problem 7(a), a is a square modulo every power of p_i, hence modulo each $p_i^{\alpha_i}$. Then we are done by part (b). □

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

Proof. By part (c) we know a is a square modulo m if and only if it is a square modulo p for each prime p dividing m, and by part (a) this holds if and only if $a^{\frac{p-1}{2}} \equiv 1 \mod p$, hence we are done. □

(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.

A first thing to notice is that the formula $a^{\frac{p-1}{2}} \equiv 1 \mod p$ doesn't make sense for $p = 2$ (as $2-1$ is not divisible by 2), and for general prime is certainly false for a divisble by p (as the left hand side will always equal 0, not 1). Therefore the best we could hope for is a statement like the following: a is a square modulo m if and only if it is a square modulo p for each prime p dividing m. Unfortunately, this is not true in general. As part (b) of this problem always works, the trouble must arise in part (c), where we pass between a having a square root modulo p and modulo p^α, which was the content of HW4 Problem 7.

Let's begin by considering the case where m is even. Notice that every integer is a square modulo 2. Indeed, every integer is congruent either to 0 or 1 modulo 2, which are both squares. But what about modulo 4? The squares modulo for are

$$\{0^2, 1^2, 2^2, 3^2\} = \{0, 1, 0, 1\},$$

so 2 and 3 are not squares modulo 4. So 3 is a square modulo 2, and it is not divisible by 2 but it is not a square modulo 4. This shows us that the *oddness* of the prime in HW4 Problem 7 was a crucial ingredient, the result is just *not true* for the prime 2. Similar trouble arises passing from squares mod 4 to mod 8, and so on. In particular, the best we could do in the even case is something like the following:

Proposition 1. *Let $m = 2^k m'$ be an integer, and a another integer not divisible by any prime dividing m. Then a is a square modulo m if and only if both of the following conditions hold:*

i. a is a square modulo 2^k.

ii. a is a square modulo p for every odd prime p dividing m.

It is worth noticing that as an immediate consequence we have if m is odd then a is a square modulo m if and only if it is a square modulo $2m$.

Next let's consider an odd prime p, and suppose a is divisible by p. Then a is certainly a square mod p (it is 0!). Is it a square modulo a power of p? Well, that depends. Consider for example p. It is a square mod p, but is it a square mod p^2? No! Indeed, if $a^2 \equiv p \mod p^2$, then $p | a^2$ so that $p | a$. But then $p^2 | a^2$ so that $a^2 \equiv 0 \mod p^2$, a contradiction. Arguing similarly we can see that p is not a square modulo p^α for any $\alpha \geq 2$. On the other hand, what about p^2?. It is a square modulo any power of p, (indeed, it is a square in $\mathbb{Z}$). Similarly, any even power of p is a square. As one more example, we check p^3. It is a square modulo p, p^2, p^3 (since it is 0), but not modulo p^4 or any higher power of p (why?). Arguing in this way, and generalizing slightly, one could arrive at the following result (whose proof we leave to the interested reader):

Proposition 2. *Let p be an odd prime and let a be an integer. Factor $a = a'p^k$ where a' is not divisible by p. Then a is a square modulo p^α if and only if one of the following holds:*

i. $k > \alpha$

ii. α *is even and* a' *is a square modulo* p.

Using Propositions 1 and 2 one could state a completely general form of Theorem 1, but it wouldn't be quite as clean to state. We encourage the reader to do so!

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

Proof. The algorithm proposed in the solutions of HW3 Problem 6(f) was the following: raise a to the $\frac{p-1}{2}$. If the result is 1, then $\log_g a$ is even, else it is odd. The proof follows immediately from part (a), together with HW2 Problem 8 which says that the log is even if and only if a is a square. □