6.875: Solutions for Homework 1

Yevgeniy Dodis

Problem 1

Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, where p_i are distinct *odd* primes and $\alpha_i > 0$. Let $y \in \mathbb{Z}_n^*$ be a quadratic residue.

(a) Show that y has *exactly* 2^k distinct square roots $(\bmod\, n)$.

(b) Why did we require that none of the $p_i = 2$?

Solution: Fix throughout $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, $q_i = p_i^{\alpha_i}$ so that all q_i are relatively prime to each other.

Theorem 1 *For any $S > 0$ and any $y \in \mathbb{Z}_n^*$, there is a one-to-one correspondence between the set of solutions to the equation*

$$x^S \equiv y \bmod n \tag{1}$$

and the k-tuple solutions to the system

$$x_i^S \equiv y \bmod q_i, \qquad i = 1, \dots, k \tag{2}$$

Thus, if R is the number of solutions to (1) and R_i is the number of solutions to equation i of (2), then $R = R_1 \cdot \ldots \cdot R_k$.

Proof Sketch: By the Chinese Remainder Theorem (CRT) we can represent any $x \in \mathbb{Z}_n^*$ *uniquely* as a k-tuple $(x_1, \dots x_k)$, where $x_i \equiv x \bmod p_i^{a_i}$. We claim that this relation defines the need one-to-one correspondence. Indeed, if $x^S \equiv y \bmod n$, then $x^S \equiv y \bmod q_i$, i.e. $(x \bmod q_i)^S \equiv y \bmod q_i$, i.e. $x_i^S \equiv y \bmod q_i$. Conversely, if $x_i^S \equiv y \bmod q_i$, then $(x \bmod q_i)^S \equiv y \bmod q_i$, then $x^S \equiv y \bmod q_i$. By the uniqueness part of the CRT *applied to y and* $(x^S \bmod n)$, since both of them have the same residues $\bmod q_i$ for all i, we must have $x^S \equiv y \bmod n$. □

Remark: The punch line of this observation is the fact that when analyzing something about equation $x^S \equiv y \bmod n$, we might as well look at the system $x_i^S \equiv y \bmod q_i$, effectively reducing the problem to the case when n is a prime power! And this case is typically easier to reason about. For example, $\mathbb{Z}_{p^\alpha}^*$ is cyclic for odd p, etc.

Theorem 2 *Assume none of p_i is 2. Then, for any S, if $f(x) = x^S \bmod n$, then any y in the image of f (i.e. of the form $z^S \bmod n$) has* exactly *R preimages, where*

$$R = gcd(S, \varphi(p_1^{\alpha_1})) \cdot \ldots \cdot gcd(S, \varphi(p_k^{a_k}))$$

Proof Sketch: By the previous theorem, we only need to show that the equation $x_i^S \equiv y \bmod p_i^{\alpha_i}$ has *exactly $gcd(S, \varphi(p_i^{\alpha_i}))$* solutions provided $p_i \neq 2$ and y is in the image of f, i.e. $y \equiv z^S \bmod n$ for some z (and hence $y \equiv z^S \bmod p_i^{\alpha_i}$). Let's get rid of now redundant subscript i. Thus, it remains to show that for an odd prime p, if $y \equiv z^S \bmod p^\alpha$, the equation $x^S = y \bmod p^\alpha$ has exactly $gcd(S, \varphi(p^\alpha))$ solutions.

Let $q = p^\alpha$. Since p is odd (here is where we use it), we know that $\mathbb{Z}_q^*$ is cyclic, i.e. there is a generator $g \in \mathbb{Z}_q^*$ s.t. $\mathbb{Z}_q^* = \{g^i \mid i = 0, \ldots, \varphi(q)-1\}$. For any $x \in \mathbb{Z}_q^*$ we let the index of x, $index(x)$, be the unique exponent $i \in \{0, \ldots, \varphi q - 1\}$ s.t. $x = g^i \bmod q$. Let $index(y) = j$ and i be the index of unknown x. Thus, it suffices to show that the number of solutions to the equation $g^{iS} \equiv g^j \bmod q$, where $i \in \{0, \ldots, \varphi(q)-1\}$, is $gcd(S, \varphi(q))$. Since g is a generator, the above equation is equivalent to

$$iS \equiv j \bmod \varphi(q) \tag{3}$$

and we know there is at least one solution (equal to the index of z). Let i_0 be the solution of the smallest index and $d = gcd(S, \varphi(q))$. Let $i_r = i_0 + r \cdot \frac{\varphi(q)}{d}$, where $r = 0, \ldots, d-1$. Each i_r is a solution to (3) as

$$i_r S \equiv \left(i_0 + r \cdot \frac{\varphi(q)}{d}\right) S \equiv i_0 S + \left(r \frac{S}{d}\right) \varphi(q) \equiv i_0 S \equiv j \bmod \varphi(q)$$

The d values of i_r are also *distinct* as r ranges from 0 to $d-1$ only (and also $r_d \equiv r_0$). Take now any solution i. As $i_0 S \equiv j \bmod \varphi(q)$ and $iS \equiv j \bmod \varphi(q)$, we get that $(i - i_0)S \equiv 0 \bmod \varphi(q)$, i.e. $(i - i_0)\frac{S}{d} \equiv 0 \bmod \frac{\varphi(q)}{d}$. As $gcd(\frac{S}{d}, \frac{\varphi(q)}{d}) = 1$, we get that $i \equiv i_0 \bmod \frac{\varphi(q)}{d}$, so that $i = i_r$ for some r. $\square$

Part (a) immediately follows from the preceding theorem for $S = 2$ since $gcd(2, \varphi(p^\alpha) = gcd(2, (p-1)p^{\alpha-1}) = 2$, as $p-1$ is even for odd p, so that the number of solutions is $\prod_{i=1}^k gcd(2, \varphi(p_i^{\alpha_i})) = 2^k$.

We remark that for $S = 2$ one did not need to prove the general theorem above. I did it since it will be useful for the next problem. We can show that the equation $x^2 \equiv y \bmod p^\alpha$ has exactly 2 solutions (provided y is a quadratic residue) by elementary means (e.g. without using the fact that $\mathbb{Z}_{p^\alpha}$ is cyclic). Indeed, assume $z^2 \equiv y \bmod p^\alpha$. Then z and $-z$ are at least 2 *distinct* solutions: here we use $p \neq 2$ to say $z \not\equiv -z \bmod p^\alpha$. We show that these are the only solutions by saying that $x^2 \equiv z^2 \bmod p^\alpha$ implies $(z-x)(z+x) \equiv 0 \bmod p^\alpha$. If $x \not\equiv \pm z \bmod p^\alpha$ we must have that p divides *both* $(z-x)$ and $(z+x)$, but then p divides their sum $2z$. Since $p \neq 2$, p divides z contradicting the fact that z is relatively prime with p^α. So we have exactly 2 solutions.

To get a counter-example when some $p_i = 2$, take $n = 2 \cdot 3 = 6$. There are only 2 square roots of 1: 1 and 5, while the formula would give us $2^2 = 4$.

Problem 2

Assume RSA is invertible in polynomial time. Give an efficient algorithm that, given two integers n and S, decides whether S is relatively prime to $\varphi(n)$.

Solution:

Theorem 3 *For any n, the function $f(x) = x^S \bmod n$ is a bijection from $\mathbb{Z}_n^*$ onto $\mathbb{Z}_n^*$ if and only if S is relatively prime to $\varphi(n)$. Moreover, if $gcd(S, \varphi(n)) > 1$ then any $y \in \mathbb{Z}_n^*$ in the image of f has at least 2 preimages.*

Proof: If $gcd(S, \varphi(n)) = 1$, the f is the standard RSA function and there is an inverse D of S in $\mathbb{Z}_n^*$. Then $(x^S)^D = x \bmod n$, so f is injective (and, thus, bijective).

Let now $d = gcd(S, \varphi(n)) > 1$. We give 2 arguments that any y in the image of f has at least 2 preimages (in particular, f is not a injective in this case). We assume w.l.o.g. that $n > 2$.

Argument 1: Assume $n = 2^j n'$, where $n' = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ is odd. Assume for contradiction that some y in the image of f has unique preimage z. By Theorems 1 and 2, y has *at least* $R = gcd(S, \varphi(p_1^{\alpha_1})) \cdot$

$\ldots \cdot gcd(S, \varphi(p_k^{\alpha_k}))$ preimages. This is because the equation $x^S \equiv y \bmod 2^j$ has at least one solution (y is in the image) and the equation $x^S \equiv y \bmod n'$ has exactly R solutions. Then we must have $R = 1$, i.e. S is relatively prime to all $\varphi(p_i^{\alpha_i})$, $i = 1 \ldots k$. But as φ is a multiplicative function, i.e. $\varphi(n') = \varphi(p_1^{\alpha_1}) \cdot \ldots \cdot \varphi(p_k^{\alpha_k})$, this is equivalent to saying that S **is relatively prime with** $\varphi(n')$, i.e. $gcd(S, \varphi(n')) = 1$. If $j = 0$, i.e. $n = n'$ is odd, we are done as we get $d = 1$, a contradiction.

So assume that $j \geq 1$, i.e. n is even. If $n' \neq 1$ (i.e. n is not a power of 2), then $\varphi(n')$ is *even* as it is divisible by an even number $(p_1 - 1)$. But then S must be *odd* and hence $d = gcd(S, \varphi(2^j n')) = gcd(S, 2^{j-1}\varphi(n')) = 1$, a contradiction.

So the only case to consider is when $n = 2^j$, $j > 1$. $\mathbb{Z}_n^*$ consists of odd numbers less than n. Since $1 < d = gcd(S, 2^{j-1})$ and $j > 1$, we must have that S is even. Let $y = z^S \bmod 2^j$. As z is odd and $j > 1$, $z \not\equiv -z \bmod 2^j$. Also, since S is even, $(-z)^S \equiv z^S \equiv y \bmod n$, so y has at least 2 preimages, a contradiction. □

I want to mention that the argument seems convoluted because of the annoying case that n can be even. However, for odd n the result is immediate from Theorem 2.

Argument 2 (due to Yan Zhong Ding): We will use the following famous theorem due to Cauchy.

Theorem 4 (Cauchy) *Let G be a group. Then for any prime p dividing $|G|$, there is a element $g \in G$ of order p, i.e. $g^p = 1$ but $g^i \neq 1$, $1 < i < p$.*

Take $G = \mathbb{Z}_n^*$, $|G| = \varphi(n)$. Since $d > 1$, let $p > 1$ be any prime dividing d (and thus $\varphi(n)$ and S). By Cauchy theorem, there is an element $x \in \mathbb{Z}_n^*$ of order $p > 1$. Then $zx \not\equiv x \bmod n$. However, $(zx)^S \equiv z^S x^S \equiv y(x^p)^{S/p} \equiv 1 \bmod n$, so y has at least 2 (in fact, at least p) preimages. □

We now use this theorem to solve our problem which is now equivalent to the following question:

Is it true that any $y \in \mathbb{Z}_n^*$ in the image of $f(x) = x^S \bmod n$ has *exactly* one preimage or rather *all* y have at least 2 preimages?

Let A be the RSA-inverting algorithm, that is on input y, n and S' where S' is relatively prime with $\varphi(n)$, A produces the unique preimage of y. The behavior of A on any other input is unknown (in particular, when S' is not relatively prime to $\varphi(n)$). Here is our testing algorithm.

1. Pick a random $z \in \mathbb{Z}_n^*$.
2. Feed $y = z^S \bmod n$, n and S to A. Get answer x.
3. If $x = z$ output "yes", else output "probably no".

If $gcd(S, \varphi(n)) = 1$, the algorithm is correct with probability 1, since then our algorithm will uniquely invert RSA function producing z. Otherwise, y has at least 2 preimages, one of which is z. Even though A is not required to work correctly when $gcd(S, \varphi(n)) > 1$, this is even better for us since we want to catch this case. The point is, however, that we can not assume that the algorithm will complain or will somehow inform us that S is not relatively prime with n (as many of you have assumed for some reason). Instead, we should assume the worst case: that A is maliciously trying to fool us whenever the input is not of the right form. However, since the preimage z of y was chosen at random, and there is at least one more preimage we could have started with, A produces $x \neq z$ with probability at least 1/2.

Problem 3

Assume one is using RSA with the same modulus n but different (relatively prime) public exponents e_1 and e_2 to encrypt a message m. Prove that the adversary can reconstruct m from the 2 encryptions (i.e. from $c_1 = m^{e_1} \bmod n$ and $c_2 = m^{e_2} \bmod n$).

Solution: Since e_1 and e_2 are relatively prime, by the extended GCD algorithm, we can find integers u and v such that $ue_1 + ve_2 = 1$. But then $m \equiv m^1 \equiv m^{ue_1+ve_2} \equiv (m_1^e)^u \cdot (m_2^e)^v \equiv c_1^u \cdot c_2^v \bmod n$.

Problem 4

Assume Alice, Bob and Carol have 3 randomly chosen moduli n_A, n_B and n_C, s.t. 3 is a common RSA exponent for all of them (i.e. $gcd(3, \varphi(n_X)) = 1$, $X = A, B, C$). A user U encrypts the same message m using their public keys. Show that an adversary can reconstruct m from the 3 encryptions (i.e. from $m^3 \bmod n_A$, $m^3 \bmod n_B$ and $m^3 \bmod n_C$).

Solution: Since the moduli are randomly chosen, we assume w.l.o.g. that they are all relatively prime to each other. Let $n = n_A n_B n_C$. By the CRT, we can find $y \in \mathbb{Z}_n$ s.t. $y \equiv m^3 \bmod n_X$, $X = A, B, C$. By the uniqueness of the CRT, we must have $y \equiv m^3 \bmod n$. But $m < n_X$, $X = A, B, C$, therefore, $m^3 < n_A n_B n_C = n$. Thus, $y = m^3$ over regular integers. Now we can simply extract cubic root over integers to reconstruct m.