

MATH 4450/6450
HOMEWORK 6 SOLUTIONS AND COMMENTS

Comments about the book problems: It sounds like people had some issues with 9.7.3. The point was that for this combined signature/encryption scheme to work right, Bob's modulus n_B should be bigger than Alice's n_A . Otherwise, Bob can only retrieve $m \bmod n_B$, which won't tell you what the original m was. (Did anyone decide what Alice's message was supposed to be in problem 3?)

Extra Problem 1: Suppose p and q are primes which are both congruent to 3 mod 4, and let $n = pq$.

(a) Suppose $a \in \mathbb{Z}_n^*$. Show that the congruence $x^2 \equiv a \pmod n$ has either 0 or 4 solutions. In the latter case, we say that a is a quadratic residue mod n . Explain why exactly 1/4 of the elements of \mathbb{Z}_n^* are quadratic residues mod n . (Don't use the hypothesis that p and q are 3 mod 4 here; it's not necessary.)

(b) Let a be a quadratic residue mod n , so that by part (a) it has four square roots. Show that exactly one of these square roots is a quadratic residue mod n . (Hint: show that exactly one of the square roots of $a \bmod p$ is a quadratic residue mod p , and similarly for q . You will most certainly use the hypothesis that the primes are 3 mod 4.)

(c) Suppose that y is a quadratic residue mod n . Define $S(y)$ to be the unique square root of $y \bmod n$ which is also a quadratic residue (so part (b) showed that $S(y)$ was well-defined). Prove the following lemma:

$$a \text{ is a quadratic residue mod } n \Leftrightarrow \left(\frac{a}{n}\right) = 1 \text{ and } a \equiv S(a^2) \pmod n$$

(d) Suppose I had a machine that, given a quadratic residue $x \bmod n$, could predict the parity of $S(x) \bmod n$ with probability P . Show that I could then produce a machine that, given a number a such that $\left(\frac{a}{n}\right) = 1$, could predict whether a was a square mod n with probability P .

Remark: If you can't solve the "quadratic residuosity" problem for n , then you can't make the machine in part (d) if you want P to be bigger than 1/2. And (with a little hand-waving) this means that you can't distinguish between the output of a Blum-Blum-Shub generator (with $k = 1$) and a random sequence of bits, because you can't predict the bit to the left of any given bit with accuracy better than 1/2.

Solution: (a) The congruence $x^2 \equiv a \pmod p$ has 0 or 2 solutions. The congruence $x^2 \equiv a \pmod q$ has 0 or 2 solutions. (Note: It's quite important that a be relatively prime to n ; otherwise one or both of these congruences could have 1 solution!)

If either of the prime-modulus congruences has 0 solutions, then of course the congruence $x^2 \equiv a \pmod n$ will have 0 solutions. And, by the Chinese Remainder Theorem, if both of

the prime-modulus congruences have 2 solutions, then the congruence $x^2 \equiv a \pmod n$ will have 4 solutions. For how many elements $a \in \mathbb{Z}_n^*$ will this happen? Well, exactly half of the elements of \mathbb{Z}_p^* are squares, and exactly half of the elements of \mathbb{Z}_q^* are squares; so (again by the Chinese Remainder Theorem) we'll get

$$\frac{p-1}{2} \cdot \frac{q-1}{2} = \frac{\phi(n)}{4}$$

quadratic residues in \mathbb{Z}_n^* , which is exactly $1/4$ of the elements of \mathbb{Z}_n^* . \square

(b) The square roots of $a \pmod p$ are $\pm x_1$, and the square roots of $a \pmod q$ are $\pm x_2$. So the square roots of $a \pmod n$ are congruent to $\pm x_1 \pmod p$ and $\pm x_2 \pmod q$. Now let x be a square root of a . Clearly x is a quadratic residue mod n if and only if it reduces to a quadratic residue mod p and mod q .

But exactly one of the two elements $x_1, -x_1$ is a quadratic residue mod p , because

$$\left(\frac{-x_1}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{x_1}{p}\right) = -\left(\frac{x_1}{p}\right)$$

(where the last step is because $p \equiv 3 \pmod 4$). Similarly, exactly one of the two elements $x_2, -x_2$ is a quadratic residue mod q . So exactly one of the four square roots of $a \pmod n$ reduces mod p and mod q to a quadratic residue, and hence exactly one of the four square roots of $a \pmod n$ is a quadratic residue. \square

(c) (\Rightarrow): If a is a quadratic residue mod n , then it reduces to a quadratic residue mod p and mod q , so

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right) \left(\frac{a}{q}\right) = 1 \cdot 1 = 1$$

and $S(a^2) = a$, so of course they're congruent mod 2.

(\Leftarrow): Suppose $\left(\frac{a}{n}\right) = 1$. Then there are two possibilities: either $\left(\frac{a}{p}\right)$ and $\left(\frac{a}{q}\right)$ are both 1, or they're both -1 . In the former case, $S(a^2) = a$ and clearly a is a quadratic residue mod n . In the latter case, note that (because p and q are $3 \pmod 4$) $\left(\frac{-a}{p}\right) = 1$ and $\left(\frac{-a}{q}\right) = 1$. So $n - a$ is the square root of $a^2 \pmod n$ which is itself a quadratic residue. But a is not congruent to $n - a \pmod 2$, because n is odd. So if $\left(\frac{a}{n}\right) = 1$ and $a \equiv S(a^2) \pmod 2$, then we must be in the former case and a is a quadratic residue mod n . \square

(d) Suppose I give you an a such that $\left(\frac{a}{n}\right) = 1$. Then throw $x = a^2$ into your machine. If it predicts that $S(a^2)$ has the same parity as a , then I predict that a will be a quadratic residue. If it predicts that $S(a^2)$ has the opposite parity as a , then I predict that a will not be a quadratic residue. I'll be right exactly when your machine is right; that is, I'll be right with probability P . \square

Extra Problem 2: Omitted, since everyone's answer will be different.