CS 70 Spring 2017 | Discrete Mathematics and Probability Theory Rao | DIS 4a

## 1 Simplifying Some "Little" Exponents

For the following problems, you must both calculate the answers and show your work.

(a) What is $7^{3,000,000,000} \mod 41$?

(b) What is $2^{2017} \mod 11$?

(c) What is $2^{(5^{2017})} \mod 11$?

**Solution:**

(a) Notice that $3,000,000,000$ is divisible by 40. So this is congruent to 1, by Fermat's Little Theorem, i.e. $7^{3,000,000,000} \equiv 7^{40\times 75,000,000} \equiv 1^{75,000,000} \pmod{41} \equiv 1 \pmod{41}$.

(b) By Fermat's Little Theorem, or direct calculation, we see that $2^{10} \equiv 1 \pmod{11}$. Thus, $2^{2017} \equiv 2^{10\times 201+7} \equiv (2^{10})^{201} \times 2^7 \equiv 1^{201} \times 2^7 \equiv 128 \equiv 7 \pmod{11}$.

(c) Building on the idea from the previous part, we just need to determine the exponent's value modulo 10. As the exponent $5^{2017}$ is divisible by 5, but is not divisible by 2, we have that it must be equal to 5 modulo 10. It follows that $2^{(5^{2017})} \equiv 2^5 \equiv 32 \equiv -1 \equiv 10 \pmod{11}$.

## 2 RSA Warm-Up

Consider an RSA scheme modulus $N = pq$, where $p$ and $q$ are prime numbers larger than 3.

(a) Recall that $e$ must be relatively prime to $p-1$ and $q-1$. Find a condition on $p$ and $q$ such that $e = 3$ is a valid exponent.

(b) Now suppose that $p = 5$, $q = 17$, and $e = 3$. What is the public key?

(c) What is the private key?

(d) Alice wants to send a message $x = 10$ to Bob. What is the encrypted message she sends using the public key?

(e) Suppose Bob receives the message $y = 24$ from Alice. What equation would he use to decrypt the message?

**Solution:**

(a) Both $p$ and $q$ must be of the form $3k+2$. $p = 3k+1$ is a problem since then $p-1$ has a factor of 3 in it. $p = 3k$ is a problem because then $p$ is not prime.

(b) $N = p \cdot q = 85$ and $e = 3$ are displayed publicly. Note that in practice, $p$ and $q$ should be much larger 512-bit numbers. We are only choosing small numbers here to allow manual computation.

(c) We must have $ed = 3d \equiv 1 \mod 64$, so $d = 43$. Reminder: we would do this by using extended gcd with $x = 64$ and $y = 3$. We get $\gcd(x,y) = 1 = ax+by$, and $a = 1$, $b = -21$.

(d) We have $E(x) = x^3 \mod 85$. $10^3 \equiv 65 \mod 85$, so $E(x) = 65$.

(e) We have $D(y) = y^{43} \mod 85$. $24^{43} \equiv 14 \mod 85$, so $D(y) = 14$.

## 3 RSA Short

Background: Alice wants a signature of $x$ from Bob but doesn't want Bob to know $x$.

Let $(N,e)$ be Bob's public key, and $d$ be his decryption key. Alice chooses a random $r$ that is relatively prime to $N$, and sends Bob $r^e x \pmod N$ to sign, and Bob returns $m = (r^e x)^d \pmod N$ to Alice.

Give an expression that yields Bob's signature of $x$: $x^d \pmod N$. Your expression may use the variables $m$, $x$, $r$, $N$ and $e$.

**Solution:**

$r^{-1}m \pmod N$, where $r$ is the multiplicative inverse of $r$.

Verification: $r^{-1}m = r^{-1}(r^e x)^d = r^{-1}(r^{ed})x^d = r^{-1}rx^d = x^d \pmod N$.

What is going on here? This Chaum's blind signature scheme where one signs a message that one can't read. It is important for electronic cash in a sense. See Chaum's electronic cash proposal for an elucidation.

## 4 RSA with Multiple Keys

Members of a secret society know a secret word. They transmit this secret word $x$ between each other many times, each time encrypting it with the RSA method. Eve, who is listening to all of their communications, notices that in all of the public keys they use, the exponent $e$ is the same. Therefore the public keys used look like $(e,N_1),\ldots,(e,N_k)$ where no two $N_i$'s are the same. Assume that the message is $x$ such that $0 \le x < N_i$ for every $i$.

(a) Suppose Eve sees the public keys $(7,35)$ and $(7,77)$ as well as the corresponding transmissions. Can Eve use this knowledge to break the encryption? If so, how? Assume that Eve cannot compute prime factors efficiently.

(b) The secret society has wised up to Eve and changed their choices of $N$, in addition to changing their word $x$. Now, Eve sees keys $(3, 5 \times 23)$, $(3, 11 \times 17)$, and $(3, 29 \times 41)$ along with their transmissions. Argue why Eve cannot break the encryption in the same way as above.

**Solution:**

(a) Yes. Note that gcd(77, 35) = 7. She can figure out the gcd of the two numbers using the gcd algorithm, and then divide 35 by 7, getting 5. Then she knows that the $p$ and $q$ corresponding to the first transmission are 7 and 5, and can break the encryption.

(b) Since none of the $N$'s have common factors, she cannot find a gcd to divide out of any of the $N$'s. Hence the approach above does not work.