CS 70 Fall 2018 | Discrete Mathematics and Probability Theory Alistair Sinclair and Yun Song | HW 5

# 1 Quick Computes

Simplify each expression using Fermat's Little Theorem.

(a) $3^{33} \pmod{11}$

(b) $10001^{10001} \pmod{17}$

(c) $10^{10}+20^{20}+30^{30}+40^{40} \pmod{7}$

**Solution:**

(a) $3^{33} \pmod{11} \equiv 3^3 \cdot (3^{10})^3 \pmod{11} \equiv 27 \cdot 1^3 \pmod{11} \equiv 5 \pmod{11}$

(b) $10001^{10001} \pmod{17} \equiv 10001^1 \cdot (10001^{16})^{625} \pmod{17} \equiv 10001 \pmod{17} \equiv 5 \pmod{17}$

(c)

$$\begin{aligned}
10^{10}+20^{20}+30^{30}+40^{40} \pmod{7} &\equiv 10^4 \cdot 10^6 + 20^2 \cdot 20^{18} \\
&\quad + 30^0 \cdot 30^{30} + 40^4 \cdot 40^{36} \pmod{7} \\
&\equiv 10^4 + 20^2 + 30^0 + 40^4 \pmod{7} \\
&\equiv 3^4 + 6^2 + 2^0 + 5^4 \pmod{7} \\
&\equiv 3^4 + (-1)^2 + 2^0 + (-2)^4 \pmod{7} \\
&\equiv 81 + 1 + 1 + 16 \pmod{7} \\
&\equiv 4 + 1 + 1 + 2 \pmod{7} \equiv 1 \pmod{7}
\end{aligned}$$

# 2 RSA Practice

Bob would like to receive encrypted messages from Alice via RSA.

(a) Bob chooses $p = 7$ and $q = 11$. His public key is $(N, e)$. What is $N$?

(b) What number is $e$ relatively prime to?

(c) $e$ need not be prime itself, but what is the smallest prime number $e$ can be? Use this value for $e$ in all subsequent computations.

(d) What is $\gcd(e,(p-1)(q-1))$?

(e) What is the decryption exponent $d$?

(f) Now imagine that Alice wants to send Bob the message 30. She applies her encryption function $E$ to 30. What is her encrypted message?

(g) Bob receives the encrypted message, and applies his decryption function $D$ to it. What is $D$ applied to the received message?

**Solution:**

(a) $N = pq = 77$.

(b) $e$ must be relatively prime to $(p-1)(q-1) = 60$.

(c) We cannot take $e = 2,3,5$, so we take $e = 7$.

(d) By design, $\gcd(e,(p-1)(q-1)) = 1$ always.

(e) The decryption exponent is $d = e^{-1} \pmod{60} = 43$, which could be found through Euclid's extended GCD algorithm.

(f) The encrypted message is $E(30) = 30^7 \equiv 2 \pmod{77}$. We can obtain this answer via repeated squaring.

$$\begin{aligned}30^7 &\equiv 30 \cdot 30^6 \equiv 30 \cdot (30^2 \bmod 77)^3 \equiv 30 \cdot 53^3 \equiv (30 \cdot 53 \bmod 77) \cdot (53^2 \bmod 77) \equiv 50 \cdot 37 \\ &\equiv 2 \pmod{77}.\end{aligned}$$

(g) We have $D(2) = 2^{43} \equiv 30 \pmod{77}$. Again, we can use repeated squaring.

$$\begin{aligned}2^{43} &\equiv 2 \cdot 2^{42} \equiv 2 \cdot (2^2 \bmod 77)^{21} \equiv 2 \cdot 4^{21} \equiv (2 \cdot 4 \bmod 77) \cdot 4^{20} \equiv 8 \cdot (4^2 \bmod 77)^{10} \\ &\equiv 8 \cdot 16^{10} \equiv 8 \cdot (16^2 \bmod 77)^5 \equiv 8 \cdot 25^5 \equiv (8 \cdot 25 \bmod 77) \cdot 25^4 \equiv 46 \cdot (25^2 \bmod 77)^2 \\ &\equiv 46 \cdot (9^2 \bmod 77) \equiv 46 \cdot 4 \equiv 30 \pmod{77}.\end{aligned}$$

# 3 Squared RSA

(a) Prove the identity $a^{p(p-1)} \equiv 1 \pmod{p^2}$, where $a$ is coprime to $p$, and $p$ is prime. (Hint: Try to mimic the proof of Fermat's Little Theorem from the notes.)

(b) Now consider the RSA scheme: the public key is $(N = p^2q^2, e)$ for primes $p$ and $q$, with $e$ relatively prime to $p(p-1)q(q-1)$. The private key is $d = e^{-1} \pmod{p(p-1)q(q-1)}$. Prove that the scheme is correct for $x$ relatively prime to both $p$ and $q$, i.e. $x^{ed} \equiv x \pmod N$.

(c) Prove that this scheme is at least as hard to break as normal RSA; that is, prove that if this scheme can be broken, normal RSA can be as well. We consider RSA to be broken if knowing $pq$ allows you to deduce $(p-1)(q-1)$. We consider squared RSA to be broken if knowing $p^2q^2$ allows you to deduce $p(p-1)q(q-1)$.

**Solution:**

(a) We mimic the proof of Fermat's Little Theorem from the notes.
Let $S$ be the set of all numbers between 1 and $p^2-1$ (inclusive) which are relatively prime to $p$. We can write

$$S = \{1,2,\ldots,p-1,p+1,\ldots,p^2-1\}$$

Define the set

$$T = \{a,2a,\ldots,(p-1)a,(p+1)a,\ldots,(p^2-1)a\}$$

We'll show that $S \subseteq T$ and $T \subseteq S$, allowing us to conclude $S = T$:

- $S \subseteq T$: Let $x \in S$. Since $\gcd(a,p) = 1$, the inverse of $a$ exists $\pmod{p^2}$. For ease of notation, we use $a^{-1}$ to denote the quantity $a^{-1} \pmod{p^2}$. We know $\gcd(a^{-1},p) = 1$, because $a^{-1}$ has an inverse $\pmod{p^2}$ too. Combining this with the fact that $\gcd(x,p) = 1$, we have $\gcd(a^{-1}x,p) = 1$. This tells us $a^{-1}x \in S$, so $a(a^{-1}x) = x \in T$.
- $T \subseteq S$: Let $ax \in T$, where $x \in S$. We know $\gcd(x,p) = 1$ because $x \in S$. Since $\gcd(a,p) = 1$ as well, we know the product $xs$ cannot share any prime factors with $p$ as well, i.e. $\gcd(xs,p) = 1$. This means $xs \in S$ as well, which proves the containment.

We now follow the proof of Fermat's Little Theorem. Since $S = T$, we have:

$$\prod_{s_i \in S} s_i \equiv \prod_{t_i \in T} t_i \pmod{p^2}$$

However, since we defined $T = \{a,2a,\ldots,(p-1)a,(p+1)a,\ldots,(p^2-1)a\}$:

$$\prod_{t_i \in T} t_i \equiv \prod_{s_i \in S} as_i \equiv a^{|S|} \prod_{s_i \in S} s_i \pmod{p^2}$$

We can now conclude $(\prod_{s_i \in S} s_i) \equiv a^{|S|}(\prod_{s_i \in S} s_i) \pmod{p^2}$.
Each $s_i \in S$ is coprime to $p$, so their product $\prod_{s_i \in S} s_i$ is as well. Then, we can multiply both sides of our equivalence with the inverse of $\prod_{s_i \in S} s_i$ to obtain $a^{|S|} \equiv 1 \pmod{p^2}$. Using HW4, 4(b), we know $|S| = p(p-1)$, which gives the desired result.

**Alternate Solution:** We can use Fermat's Little Theorem, combined with the Binomial Theorem, to get the result. Since $\gcd(a,p) = 1$ and $p$ is prime, $a^{p-1} \equiv 1 \pmod{p}$, so we can write $a^{p-1} = \ell p + 1$ for some integer $\ell$. Then,

$$(a^{p-1})^p = (\ell p + 1)^p = \sum_{i=0}^{p} \binom{n}{i} (\ell p)^i = 1 + p \cdot (\ell p) + \binom{p}{2} (\ell p)^2 + \cdots + (\ell p)^p,$$

and since all of the terms other than the first term are divisible by $p^2$, $a^{p(p-1)} \equiv 1 \pmod{p^2}$.

(b) By the definition of $d$ above, $ed = 1 + kp(p-1)q(q-1)$ for some $k$. Look at the equation $x^{ed} \equiv x \pmod{N}$ modulo $p^2$ first:

$$x^{ed} \equiv x^{1+kp(p-1)q(q-1)} \equiv x \cdot (x^{p(p-1)})^{kq(q-1)} \equiv x \pmod{p^2}$$

where we used the identity above. If we look at the equation modulo $q^2$, we obtain the same result. Hence, $x^{ed} \equiv x \pmod{p^2q^2}$.

(c) We consider the scheme to be broken if knowing $p^2q^2$ allows you to deduce $p(p-1)q(q-1)$. (Observe that knowing $p(p-1)q(q-1)$ is enough, because we can compute the private key with this information.) Suppose that the scheme can be broken; we will show how to break ordinary RSA. For an ordinary RSA public key $(N = pq, e)$, square $N$ to get $N^2 = p^2q^2$. By our assumption that the squared RSA scheme can be broken, knowing $p^2q^2$ allows us to find $p(p-1)q(q-1)$. We can divide this by $N = pq$ to obtain $(p-1)(q-1)$, which breaks the ordinary RSA scheme. This proves that our scheme is at least as difficult as ordinary RSA.

**Remark**: The first part of the question mirrors the proof of Fermat's Little Theorem. The second and third parts of the question mirror the proof of correctness of RSA.