Fermat's Little Theorem and the RSA Cryptosystem

Discrete Mathematics 27100 Winter 2022

1 Review: Injective, Surjective, and One to One Functions

Definition 1.1. *Given sets X and Y, a function $f : X \to Y$ is a mapping which takes each element $x \in X$ and returns an element $f(x) \in Y$.*

Definition 1.2. *We say that a function $f : X \to Y$ is injective if fpr all $x, x' \in X$ such that $x' \neq x$, $f(x') \neq f(x)$.*

Definition 1.3. *We say that a function $f : X \to Y$ is surjective if $\forall y \in Y\ (\exists x \in X(f(x) = y))$.*

Definition 1.4. *We say that a function $f : X \to Y$ is one to one if it is both injective and surjective. If so, we define $f^{-1} : Y \to X$ to be the function where for all $y \in Y$, $f^{-1}(y)$ is the unique element of X such that $f(f^{-1}(y)) = y$.*

Example 1.5.

For any natural number $n \geq 2$, the function $f : \mathbb{Z} \to \mathbb{Z}_n$ where $f(x) = x \mod n$ is surjective but not injective.

The function $f : \mathbb{Z} \to \mathbb{Z}$ where $f(x) = x^2$ is neither injective nor surjective.

The function $f : \mathbb{Z} \to \mathbb{Q}$ where $f(x) = \frac{x}{2}$ is injective but not surjective.

The function $f : \mathbb{Z} \to \mathbb{Z}$ where $f(x) = x - 5$ is a one to one function and its inverse is $f^{-1}(y) = y + 5$.

Proposition 1.6. *If f is a one to one function then $\forall x \in X, f^{-1}(f(x)) = x$*

Proof. Let $x' = f^{-1}(f(x))$ and observe that $f(x') = f(f^{-1}(f(x))) = f(x)$. Since f is injective and $f(x') = f(x)$, $x' = x$, as needed. □

Proposition 1.7. *If $f : X \to Y$ has an inverse, i.e. there exists a function $f^{-1} : Y \to X$ such that*

1. $\forall x \in X(f^{-1}(f(x)) = x)$
2. $\forall y \in Y(f(f^{-1}(y)) = y)$

then f is a one to one function.

Proof. To see that f is injective, assume that $x, x' \in X$, $x \neq x'$, and $f(x) = f(x') = y$ for some $y \in Y$. If so, then on the one hand $f^{-1}(y) = f^{-1}(f(x)) = x$ but on the other hand $f^{-1}(y) = f^{-1}(f(x')) = x'$ so $x = x'$, which is a contradiction.

To see that f is surjective, observe that for all $y \in Y$, $f^{-1}(y) \in X$ and $f(f(^{-1}(y)) = y$. □

2 Fermat's Little Theorem

Fermat's Little Theorem says the following:

Theorem 2.1 (Fermat's Little Theorem)**.** *For all primes $p \in \mathcal{P}$ and all $a \in \mathbb{Z}$ such that $p \nmid a$, $a^{p-1} \equiv 1 \mod p$*

Example 2.2.

1. *If $p = 5$ and $a = 3$ then $a^{p-1} = 3^4 = 81 \equiv 1 \mod 5$*
2. *If $p = 7$ and $a = 2$ then $a^{p-1} = 2^6 = 64 \equiv 1 \mod 7$*

Proof. One way to prove Fermat's Little theorem is with the following beautiful trick. Given an integer $a \in \mathbb{Z}$ such that $p \nmid a$, consider the function $f : [p-1] \to [p-1]$ where $f(x) = a * x \mod p$.

Lemma 2.3. *If p is prime and a is an integer such that $p \nmid a$, the function $f : [p-1] \to [p-1]$ where $f(x) = a * x \mod p$ is a one to one function.*

Proof. A common way to show that a function $f : X \to Y$ is a one to one function is to construct its inverse $f^{-1} : Y \to X$ and then show that $\forall x \in X, f^{-1}(f(x)) = x$ and $\forall y \in Y, f(f^{-1}(y)) = y$. Here we can do this as follows

1. Since $gcd(a, p) = 1$, by Bézout's identity, $\exists r, s \in \mathbb{Z} : ra + sp = 1$. Observe that $ra = 1 - sp \equiv 1 \mod p$ and take $f^{-1} : [p-1] \to [p-1]$ where $f^{-1}(y) = ry \mod p$
2. For all $x \in [p-1]$, $f^{-1}(f(x)) \equiv rax \equiv x \mod p$ so $f^{-1}(f(x)) = x$
3. For all $y \in [p-1]$, $f(f^{-1}(y)) \equiv ary \equiv y \mod p$ so $f(f^{-1}(y)) = y$

□

Since $f : [p-1] \to [p-1]$ is a one to one function,

$$\prod_{j=1}^{p-1} j \equiv \prod_{j=1}^{p-1} f(j) \equiv \prod_{j=1}^{p-1} aj \equiv a^{p-1} \prod_{j=1}^{p-1} j \mod p$$

Since $\prod_{j=1}^{p-1} j$ is invertible in $\mathbb{Z}_p$, $a^{p-1} \equiv 1 \mod p$ □

Remark 2.4. *In fact, Fermat's Little Theorem can be generalized to the following theorem which can be proved in almost exactly the same way.*

Theorem 2.5. *Given a natural number $n \geq 2$, for all $a \in \mathbb{Z}$ such that $gcd(a, n) = 1$,*

$$a^{|\{x \in \mathbb{Z}_n : x \text{ is invertible}\}|} \equiv 1 \mod n$$

For details, see the appendix.

Remark 2.6. *In a few lectures, we will see another proof of Fermat's Little Theorem using binomial coefficients.*

3 The RSA Cryptosystem

In the RSA cryptosystem, the setup is as follows:

1. Public key: A natural number $n = pq$ where $p, q \in \mathbb{P}$ together with an exponent e such that e is invertible in $\mathbb{Z}_{lcm(p-1,q-1)}$.
2. Private key: A natural number d where $de \equiv 1 \mod (p-1)$ and $de \equiv 1 \mod (q-1)$. In particular, as we will see, we can take $d = e^{-1}$ in $\mathbb{Z}_{lcm(p-1,q-1)}$.

Messages are encrypted and decrypted as follows:

1. To send a message $x \in \mathbb{Z}_n$, the sender sends $m = x^e \mod n$
2. To decrypt a sent message m, the receiver computes $m^d \mod n$

To see why this works, let's say the sender has a message x and sends $m = x^e \mod n$. The receiver then computes $m^d \mod n = x^{de} \mod n$. We now show that $x^{de} \equiv x \mod p$ and $x^{de} \equiv x \mod q$.

If $p \mid x$ then $x^{de} \equiv x \equiv 0 \mod p$. Otherwise, since $de \equiv 1 \mod (p-1)$, $\exists a \in \mathbb{Z}(de = 1 + a(p-1))$. Now observe that by Fermat's Little Theorem,

$$x^{de} = x^{1+a(p-1)} = x \cdot (x^{p-1})^a \equiv x \mod p$$

Thus, either way, $x^{de} \equiv x \mod p$. Following similar logic, $x^{de} \equiv x \mod q$

Now observe that since $gcd(p, q) = 1$, by the Chinese remainder theorem, there is a unique integer m between 0 and $n-1$ such that $m \mod p = x \mod p$ and $m \mod q = x \mod q$. On the one hand, since $x \mod p = x \mod p$ and $x \mod q = x \mod q$, $m = x$. On the other hand, since $x^{de} \equiv x \mod p$ and $x^{de} \equiv x \mod q$, $x^{de} \mod p = x \mod p$ and $x^{de} \mod q = x \mod q$ so $m = x^{de} \mod n$. Thus, $x^{de} \mod n = x$, as needed.

To find d, let $z = lcm(p-1, q-1)$ and set d to be the multiplicative inverse of e in $\mathbb{Z}_z$. Now since $de \equiv 1 \mod z$, $\exists a \in \mathbb{Z}(de = 1 + az)$. Since $(p-1) \mid z$ and $(q-1) \mid z$, $de = 1 + az \equiv 1 \mod (p-1)$ and $de = 1 + az \equiv 1 \mod (q-1)$, as needed.

Example 3.1. *Consider the RSA cryptosystem with $n = 77$, $p = 7$, $q = 11$, and $e = 13$. To encrypt the message $x = 2$, the sender computes $2^{13} \mod 77$ which can be done as follows:*

1. $2^2 = 4$
2. $2^4 = (2^2)^2 = 16$
3. $2^8 = (2^4)^2 = 256 \equiv 25 \mod 77$ *as* $256 = 3 * 77 + 25$
4. $2^{13} = 2^8 * 2^4 * 2^1 \equiv 25 * 16 * 2 = 800 \equiv 30 \mod 77$ *as* $800 = 10 * 77 + 30$

Thus, to send the message $x = 2$, the sender sends $m = 2^{13} \mod 77 = 30$.

To find d, observe that $lcm(p-1, q-1) = \frac{(p-1)(q-1)}{gcd(p-1,q-1)} = \frac{6*10}{2} = 30$ so we just need to find the multiplicative inverse of $e = 13$ in $\mathbb{Z}_{30}$. To do this, we can use Euclid's algorithm on 30 and 13:

1. *Dividing 30 by 13 we obtain a remainder of* $4 = 30 - 2 * 13$

2. *Dividing* 13 *by* 4 *we obtain a remainder of* $1 = 13-3*4 = 13-3*(30-2*13) = 7*13-3*30$.

Thus, in $\mathbb{Z}_{30}$, $13^{-1} = 7$ *so we can take* $d = 7$. *Indeed, we can compute* m^d *as follows:*

1. $30^2 \mod 77 = 900 \mod 77 = 53$ *as* $900 = 11 * 77 + 53$
2. $30^4 \mod 77 = (30^2)^2 \mod 77 = 53^2 \mod 77 = 2809 \mod 77 = 37$ *as* $2809 = 77 * 36 + 37$
3. $30^3 \mod 77 = 30^2 * 30 \mod 77 = 30 * 53 \mod 77 = 1590 \mod 77 = 50$ *as* $1590 = 77 * 20 + 50$
4. $30^7 \mod 77 = 30^4 * 30^3 \mod 77 = 37 * 50 \mod 77 = 1850 \mod 77 = 2$ *as* $1850 = 77 * 24 + 2$

Thus, $30^7 \mod 77 = 2$ *and we recover the original message* $x = 2$.

Remark 3.2. *Note that in order to find* d *in this way, we need to know the prime factorization* $n = p * q$ *of* n.

3.1 Security of RSA

The security of RSA rests on the following assumptions:

1. Finding the prime factorization of a number $n = p * q$ is hard (once we have p, q, and e we can find d as described above)
2. There is essentially no other way other than factoring n to find the private key d.

The second assumption is very believable (though we can't prove it). For the first assumption, we don't know for sure that factoring is hard for classical computers (and it can in fact be solved by a quantum computer using Shor's algorithm) but the factoring problem has withstood hundreds of years of attack.

A Generalizing Fermat's Little Theorem

Definition A.1. *Given a natural number* $n \geq 2$, *we define* $\mathbb{Z}_n^\times = \{a \in \mathbb{Z}_n : a \text{ is invertible}\}$

Example A.2.

1. $\mathbb{Z}_7^\times = \{1, 2, 3, 4, 5, 6\}$
2. $\mathbb{Z}_{10}^\times = \{1, 3, 7, 9\}$
3. $\mathbb{Z}_{15}^\times = \{1, 2, 4, 7, 8, 11, 13, 14\}$

Fermat's Little Theorem can be generalized as follows:

Theorem A.3. *Given a natural number* $n \geq 2$, *for all* $a \in \mathbb{Z}_n^\times$, $a^{|\mathbb{Z}_n^\times|} \equiv 1 \mod n$

Proof. This generalization of Fermat's Little Theorem can be proved using the same trick. Given an integer $a \in \mathbb{Z}$ such that $gcd(a, n) = 1$, consider the function $f : \mathbb{Z}_n^\times \to \mathbb{Z}_n^\times$ where $f(x) = a * x \mod n$.

Lemma A.4. *If a is an integer such that $gcd(a, n) = 1$ then the function $f : \mathbb{Z}_n^\times \to \mathbb{Z}_n^\times$ where $f(x) = a * x \mod n$ is a one to one function.*

Proof. We first note that a is invertible in $\mathbb{Z}_n$ as $gcd(a, n) = 1$. Since the product of two invertible elements of $\mathbb{Z}_n$ is invertible in $\mathbb{Z}_n$, f is indeed a function from $\mathbb{Z}_n^\times$ to $\mathbb{Z}_n^\times$.

We again construct the inverse $f^{-1} : \mathbb{Z}_n^\times \to \mathbb{Z}_n^\times$ of f and then show that $\forall x \in X(f^{-1}(f(x)) = x)$ and $\forall y \in Y(f(f^{-1}(y)) = y)$. Here we can do this as follows

1. Since $gcd(a, n) = 1$, by Bézout's identity, $\exists r, s \in \mathbb{Z}(ra + sn = 1)$. Observe that $ra = 1 - sn$ so $ra \equiv 1 \mod p$. Take $f^{-1} : \mathbb{Z}_n^\times \to \mathbb{Z}_n^\times$ where $f^{-1}(y) = ry \mod p$
2. For all $x \in \mathbb{Z}_n^\times$, $f^{-1}(f(x)) \equiv rax \equiv x \mod n$ so $f^{-1}(f(x)) = x$
3. For all $y \in \mathbb{Z}_n^\times$, $f(f^{-1}(y)) \equiv ary \equiv y \mod n$ so $f(f^{-1}(y)) = y$

□

Since $f : \mathbb{Z}_n^\times \to \mathbb{Z}_n^\times$ is a one to one function,

$$\prod_{j \in \mathbb{Z}_n^\times} j \equiv \prod_{j \in \mathbb{Z}_n^\times} f(j) \equiv \prod_{j \in \mathbb{Z}_n^\times} aj \equiv a^{|\mathbb{Z}_n^\times|} \prod_{j \in \mathbb{Z}_n^\times} j \mod n$$

Since $\prod_{j \in \mathbb{Z}_n^\times} j$ is invertible in $\mathbb{Z}_n$, $a^{|\mathbb{Z}_n^\times|} \equiv 1 \mod n$. □