

15-251: Great Theoretical Ideas In Computer Science

Recitation 7 Solutions

RSA Encryption

In lecture, we saw how RSA encryption is used. There are many important quantities used in this algorithm:

- p, q : Two very large prime numbers.
- n : $n = pq$ is part of the public key.
- $\phi(n)$: Since p, q prime, $\phi(n) = (p - 1)(q - 1)$.
- e : e , the “encryption exponent” also part of the public key, is some member of $\mathbb{Z}_{\phi(n)}^*$
- d : d , the private key or “decryption exponent”, is the inverse of e in $\mathbb{Z}_{\phi(n)}^*$, i.e., $e \times d \equiv_{\phi(n)} 1$
- m : This is the message that will be sent

To send a message to Alice using Alice’s public key (n, e) , Bob sends $m^e \bmod n$. Alice decrypts his message by calculating $(m^e)^d \bmod n$.

1. If Alice chose $p = 7, q = 11, e = 13$, how would she decode the encrypted message 3?

Solution: First we must find d , Alice’s private key. $\phi(n) = 60$, so we must find $13d \equiv_{60} 1$. We use the extended Euclidean Algorithm:

$$\begin{aligned} 60 &= 13 \times 4 + 8 \\ 13 &= 8 \times 1 + 5 \\ 8 &= 5 \times 1 + 3 \\ 5 &= 3 \times 1 + 2 \\ 3 &= 2 \times 1 + 1 \end{aligned}$$

Now we work backwards:

$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (5 - 3) = 3 \times 2 - 5 \\ &= (8 - 5) \times 2 - 5 = 8 \times 2 - 5 \times 3 \\ &= 8 \times 2 - (13 - 8) \times 3 = 8 \times 5 - 13 \times 3 \\ &= (60 - 13 \times 4) \times 5 - 13 \times 3 = 60 \times 5 - 13 \times 23 \end{aligned}$$

Thus, the decryption exponent $d \equiv_{60} -23$. Adding 60 to make this positive, $d = 37$. So, the message is $3^{37} \bmod 77$. To calculate this,

$$\begin{aligned} 3^{37} &\equiv_{77} (3)^{36}(3) \equiv (81)^9(3) \equiv 4^9(3) \\ &\equiv_{77} (64)^3 3 \equiv (-13)^3 3 \equiv (169)(-39) \\ &\equiv_{77} (15)(38) \equiv 570 \equiv 31 \end{aligned}$$

Note that you can check your work by encoding 31 to see if you do get 3: indeed, $(31)^{13} \pmod{77}$, which is $((31)^3)^4 \times 31 \pmod{77} = (-8)^4 \times 31 \pmod{77} = 15 \times 31 \pmod{77} \equiv 3$.

2. Now encrypt the message 68. (Treat this as a decimal value).

Solution: We send $68^{13} \pmod{77}$:

$$\begin{aligned}
 68^{13} &\equiv_{77} (-9)^{13} \\
 &\equiv_{77} (81)^6(-9) \\
 &\equiv_{77} 4^6(-9) \\
 &\equiv_{77} 64^2(-9) \\
 &\equiv_{77} (-13)^2(-9) \\
 &\equiv_{77} 169(-9) \\
 &\equiv_{77} 15(-9) \\
 &\equiv_{77} -135 \\
 &\equiv_{77} 19
 \end{aligned}$$

Thus the encrypted message to send is 19.

Symmetry Group of a Circle

Recall from lecture that D_n is the group of all rotations and reflections of a regular n -gon, where the operation is composition. Let D_∞ be the group of all rotations and reflections of a circle.

3. How many elements are in D_∞ ?

Solution: There are infinitely many ways to rotate a circle, and infinitely many axes about which it can be reflected, so D_∞ has an infinite number of elements. More specifically, it has the same cardinality as the real numbers.

4. What is the identity of D_∞ ?

Solution: As in any symmetry group, the identity is the transformation that does nothing to the object, or the one that rotates it by 0 radians.

5. How many elements have order 1? What are they?

Solution: If a has order 1, then $a^1 = e$, so $a = e$, so the identity is the only element of order 1.

6. How many elements have order 2? What are they?

Solution: Rotating the circle by π radians twice will get us back to the original circle, and performing the same reflection twice will also get us back to the original circle. So, there are uncountably many elements of order 2.

7. How many elements have order 3? What are they?

Solution: Two elements have order 3: rotating the circle by $\frac{2\pi}{3}$ clockwise and rotating the circle by $\frac{4\pi}{3}$ clockwise.

8. How many elements have finite order? What are they?

Solution: All of the previously-described elements have finite order, and there are uncountably many of them. In addition, a rotation has finite order if it rotates the circle by a rational fraction of a full rotation. This is because if we have $a, b \in \mathbb{Z}$, and our rotation is by $\frac{a2\pi}{b}$, we can repeat it b times and get a full circle rotations, which is equivalent to the identity.

9. How many elements have infinite order? What are they?

Solution: Similar to the last problem, if we rotate by an irrational portion of a full rotation, then

we will never reach the identity element by applying the rotation over and over, since otherwise, we would be able to represent our rotation as $\frac{a2\pi}{b}$ as in the previous part.

10. Can D_∞ be generated by a single element?

Solution: No. If the element is a reflection, then it can only generate 2 elements. If it is a rotation, it cannot generate a reflection.

Subgroups

We use the notation $H \leq G$ to say “ H is a subgroup of G ”.

11. Let $H \subseteq G$. Prove that $H \leq G$ if and only if H is nonempty and for all $x, y \in H$, $xy^{-1} \in H$.

Note that this property is useful when proving that a subset of a group is a subgroup.

Solution: For the forward direction, let H be a subgroup of G . Since H is a group, it has an identity element, so it is nonempty. Also, if $x, y \in H$, then $y^{-1} \in H$ (since H must contain inverses), and thus $xy^{-1} \in H$ (since H is closed).

For the other direction, suppose H satisfies those properties: we need to show that H has all necessary properties of a group.

- **Associative:** The operation is associative in G , so for any $a, b, c \in H$, we know that $(ab)c = a(bc)$ because these elements are also in G .
- **Identity:** We know H is nonempty, so consider any element $a \in H$. Letting $x = a$ and $y = a$, we know that $aa^{-1} \in H$, so $e \in H$.
- **Inverses:** Consider any $a \in H$. Letting $x = e$ and $y = a$, we know that $ea^{-1} = a^{-1} \in H$.
- **Closure:** Let $a, b \in H$. Then we know that $b^{-1} \in H$, so we can let $x = a$ and $y = b^{-1}$, and we know that $a(b^{-1})^{-1} = ab \in H$.

12. Prove that if $H \leq G$ and $K \leq G$, then $H \cap K \leq G$.

Solution: We can use result proved in the previous part.

- **To show $H \cap K$ is nonempty:** The identity element $e \in H$ and $e \in K$, so $e \in H \cap K$, and hence $H \cap K$ is nonempty.
- **To show that for $x, y \in H \cap K$, $xy^{-1} \in H \cap K$:** Consider $x, y \in H \cap K$, we know that $x, y \in H$, so $xy^{-1} \in H$. Also, we know $x, y \in K$, so $xy^{-1} \in K$. So, $xy^{-1} \in H \cap K$.