1. RSA with a partner

Find a partner and run through the RSA algorithm. This means:

- One of you picks two primes $p$ and $q$.\(^1\) Compute $N = pq$.
- Pick an encryption key $e$ (relatively prime to $(p-1)(q-1)$) and compute the decryption key $d$, which is a multiplicative inverse of $e \mod (p-1)(q-1)$.
- Tell your partner $N$ and $e$; keep $p$, $q$, and $d$ secret.
- Your partner chooses a message $m$, encrypts it by computing $E(m) = m^e \mod N$, and tells you $E(m)$.
- You decrypt by computing $D(m) = m^d \mod N$. Confirm with your partner that you have succeeded in transmitting the correct message.
- Switch places with your partner, and repeat.

2. Baby Fermat

Assume that $a$ does have a multiplicative inverse $\mod m$. Let us prove that its multiplicative inverse can be written as $a^k \mod m$ for some $k \geq 0$.

- Consider the sequence $a, a^2, a^3, \ldots \mod m$. Prove that this sequence has repetitions.
  **Answer:** There are only $m$ possible values $\mod m$, and so after the $m$-th term we should see repetitions.
- Assuming that $a^i \equiv a^j \mod m$, where $i > j$, what can you say about $a^{i-j} \mod m$?
  **Answer:** If we multiply both sides by $(a^*)^j$, where $a^*$ is the multiplicative inverse, we get $a^{i-j} \equiv 1 \mod m$.
- Prove that the multiplicative inverse can be written as $a^k \mod m$. What is $k$ in terms of $i$ and $j$?
  **Answer:** We can rewrite $a^{i-j} \equiv 1 \mod m$ as $a^{i-j-1}a \equiv 1 \mod m$. Therefore $a^{i-j-1}$ is the multiplicative inverse of $a \mod m$.

3. Bijections

Consider the function

$$f(x) = \begin{cases} 
  x, & \text{if } x \geq 1; \\
  3x - 2, & \text{if } \frac{1}{2} \leq x < 1; \\
  -x, & \text{if } -1 \leq x < \frac{1}{2}; \\
  2x + 3, & \text{if } x < -1. 
\end{cases}$$

- If the domain and range of $f$ are $\mathbb{N}$, is $f$ injective (one-to-one), surjective (onto), bijective?
  **Answer:** Yes, Yes, Yes.

---

\(^1\)In practice, we use very large primes for RSA, but for the purpose of this exercise, choose smaller numbers to make the computations less complicated.
• If the domain and range of $f$ are $\mathbb{Z}$, is $f$ injective (one-to-one), surjective (onto), bijective?

**Answer:** No, No, No.

• If the domain and range of $f$ are $\mathbb{R}$, is $f$ injective (one-to-one), surjective (onto), bijective?

**Answer:** No, Yes, No.

4. RSA

In this problem you play the role of Amazon, who wants to use RSA to be able to receive messages securely.

a. Amazon first generates two large primes $p$ and $q$. She picks $p = 13$ and $q = 19$ (in reality these should be 512-bit numbers). She then computes $N = pq$. Amazon chooses $e$ from $e = 37, 38, 39$. Only one of those values is legitimate, which one? $(N, e)$ is then the public key.

**Answer:** Since 38 and 39 are not relatively prime to $p - 1 = 12$ and $q - 1 = 18$, they cannot be inverted mod $(p - 1)\cdot(q - 1) = 216$, so a decryption key cannot be obtained for them. Thus, only $e = 37$ works. The public key then is $(N, e) = (247, 37)$.

b. Amazon generates her private key $d$. She keeps $d$ as a secret. Find $d$. Explain your calculation.

**Answer:** We compute $d \equiv e^{-1} \equiv 37^{-1} \pmod{216}$.

```
e-gcd(216,37)
e-gcd(37,31)
e-gcd(31,6)
e-gcd(6,1)
e-gcd(1, 0)
return (1,1,0)
return (1,0,1)
return (1,1,-5)
return (1,-5,6)
return (1,6,-35)
```

Thus $d \equiv -35 \equiv 181 \pmod{216}$.

c. Bob wants to send Amazon the message $x = 102$. How does he encrypt his message using the public key, and what is the result?

*Note:* For this problem you may find the following trick of fast exponentiation useful. To compute $x^k$, first write $k$ in base 2 then use repeated squaring to compute each power of 2. For example, $x^7 = x^{4+2+1} = x^4 \cdot x^2 \cdot x^1$.

**Answer:** The encrypted message is $y \equiv x^e \equiv 102^{37} \pmod{247}$. Using fast exponentiation, we compute:

```
102^2 \equiv 30 \pmod{247}
102^4 \equiv 30^2 \equiv 159 \pmod{247}
102^8 \equiv 159^2 \equiv 87 \pmod{247}
102^{16} \equiv 87^2 \equiv 159 \pmod{247}
102^{32} \equiv 159^2 \equiv 87 \pmod{247}
```

Then, $y \equiv 102^{37} \equiv 102^{32} \cdot 102^4 \cdot 102 \equiv 102 \pmod{247}$. Notice that the encrypted message is the same as the original!
d. Amazon receives an encrypted message $y = 141$ from Charlie. What is the unencrypted message that Charlie sent her?

**Answer:** We decrypt the message by raising to the $d$th power: $x \equiv y^d \equiv 141^{181} \pmod{247}$. We compute the powers:

$$
\begin{align*}
141^2 &\equiv 121 \pmod{247} \\
141^4 &\equiv 121^2 \equiv 68 \pmod{247} \\
141^8 &\equiv 68^2 \equiv 178 \pmod{247} \\
141^{16} &\equiv 178^2 \equiv 68 \pmod{247} \\
141^{32} &\equiv 68^2 \equiv 178 \pmod{247} \\
141^{64} &\equiv 178^2 \equiv 68 \pmod{247} \\
141^{128} &\equiv 68^2 \equiv 178 \pmod{247}
\end{align*}
$$

Then $x \equiv 141^{181} \equiv 141^{128} \cdot 141^{32} \cdot 141^{16} \cdot 141^4 \cdot 141 \equiv 141 \pmod{247}$.

By now, you may have guessed that $\forall x \in \{0, \ldots, 246\}, x^{37} \equiv x \pmod{247}$. We can prove this by noting that $e = 37 \equiv 1 \pmod{p-1}$ and $e = 37 \equiv 1 \pmod{q-1}$. Thus, $e = 1 + j(p-1) = 1 + k(q-1)$ for some $j$ and $k$. By Fermat’s little theorem, $x^{e-1} = x^{j(p-1)} \equiv 1 \pmod{p}$ and $x^{e-1} = x^{k(q-1)} \equiv 1 \pmod{q}$ where $x$ is coprime with $p$ and $q$. Then by the Chinese remainder theorem, $x^{e-1} \equiv 1 \pmod{pq}$, so $x^e \equiv x \pmod{pq}$. Though we omit it here, we can also show that $x^e \equiv x \pmod{pq}$ when $x$ is not coprime with $p$ and $q$. See the very similar RSA proof for details.

Moral of the story: stick with $e = 3$!