Primes, Modular Arithmetic, and Secret Messages

With Molly Yoder

Important Mathmaticians

- Pierre Fermat (1601 – 1665)
- Carl Friedrich Gauss (1777 – 1855)
- Augustin-Louis Cauchy (1789 –1857)
- Gustav Lejeune Dirichlet (1805 – 1859)
- Bernhard Riemann (1826 – 1866)



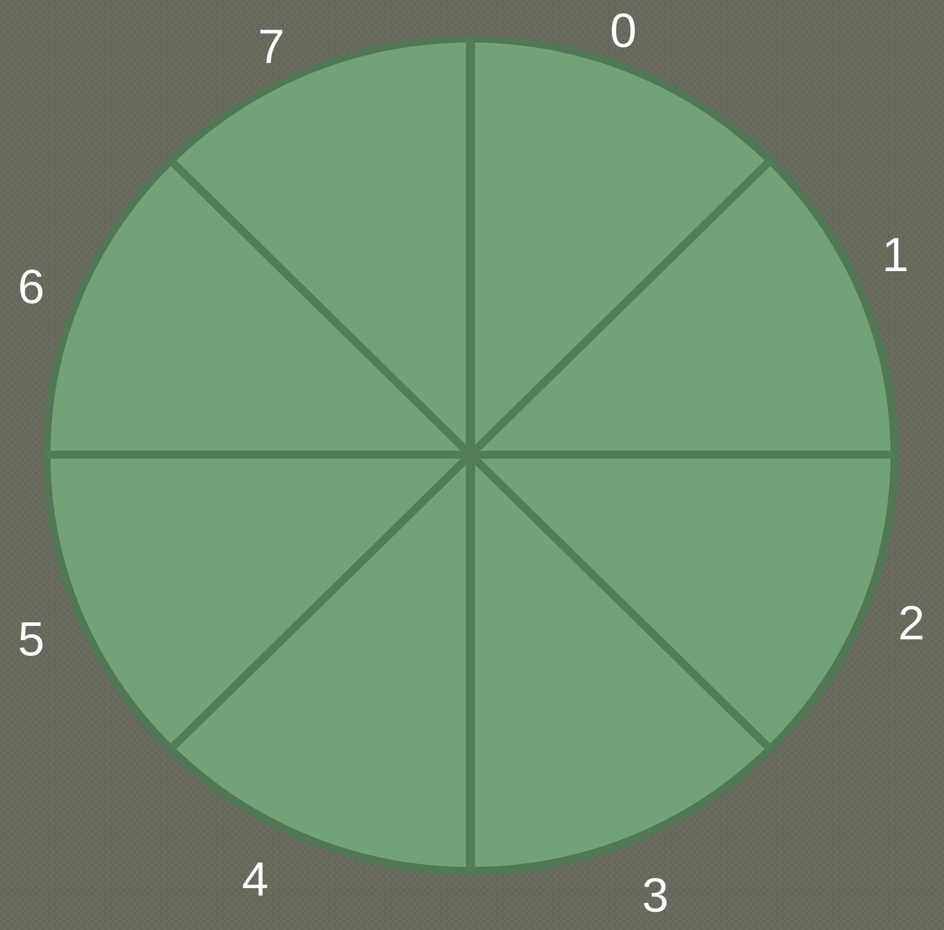


The History that Motivated RSA

- It was a search for prime numbers that intrigued the smart people of the world.
- It was in this search that they discovered many useful properties of primes.
- Some of these properties involving modular arithmetic.

Modular Arithmetic

Modular arithmetic was introduced by Leonhard Euler in 1750 and further developed by Gauss in 1801. Gauss invented what he called a clock calculator. Dividing the face of the “clock ” into N divisions such that all numbers fit into one of these sections on mod N.

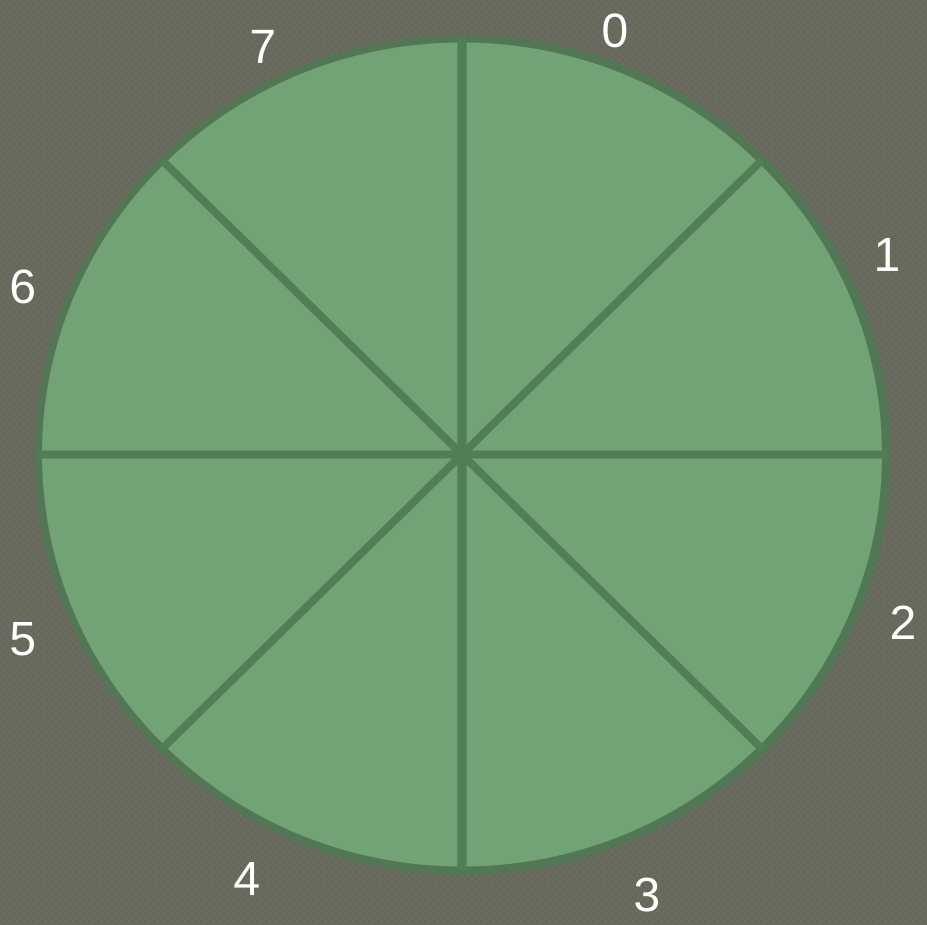


Modular Arithmetic

If we consider a clock with 8 divisions, we can easily see this property take shape when we consider the following:

1 % 8 = ?	2 % 8 = ?
3 % 8 = ?	4 % 8 = ?
5 % 8 = ?	6 % 8 = ?
7 % 8 = ?	8 % 8 = ?
9 % 8 = ?	10 % 8 = ?

-6 % 8 = ? -11 % 8 = ?

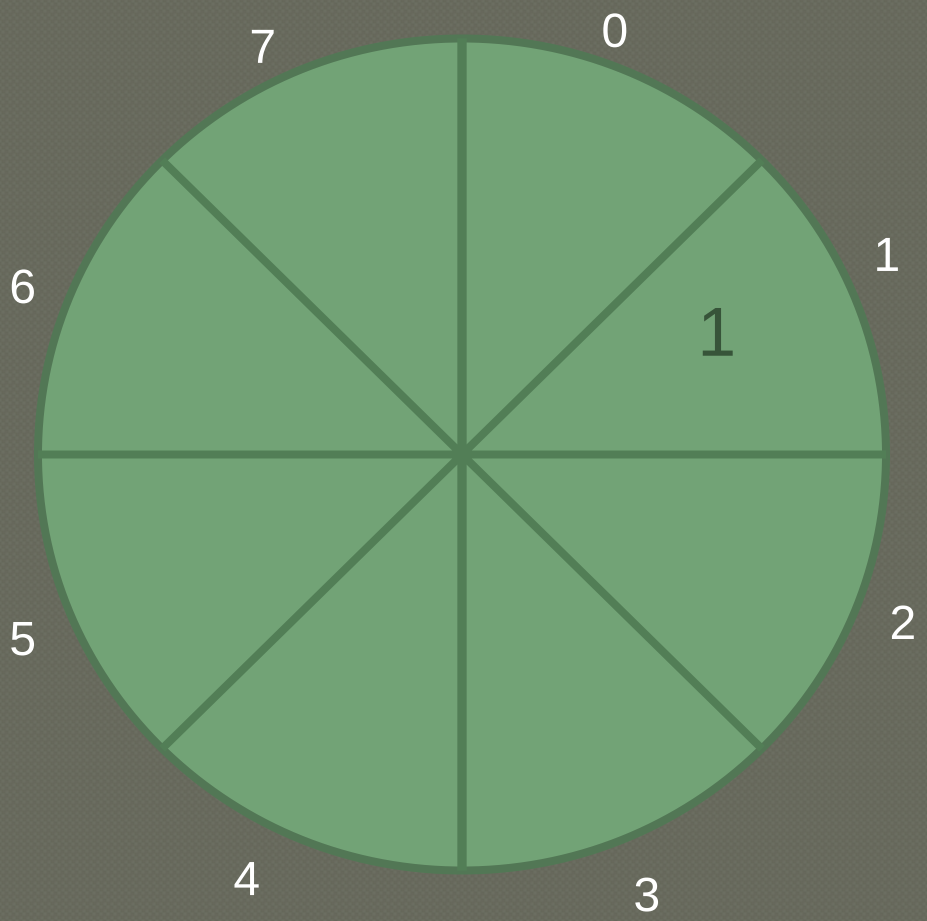


Modular Arithmetic

If we consider a clock with 8 divisions, we can easily see this property take shape when we consider the following:

1 % 8 = 1   2 % 8 = ?
3 % 8 = ?   4 % 8 = ?
5 % 8 = ?   6 % 8 = ?
7 % 8 = ?   8 % 8 = ?
9 % 8 = ?   10 % 8 = ?

-6 % 8 = ?   -11 % 8 = ?

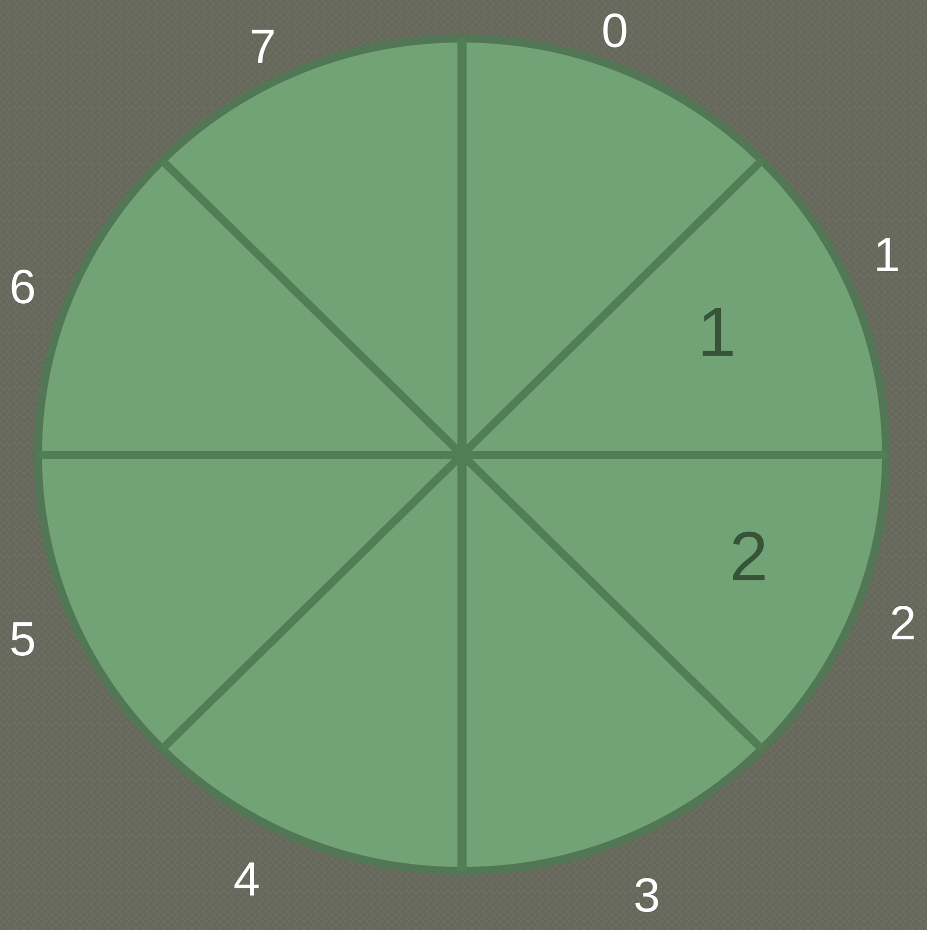


Modular Arithmetic

If we consider a clock with 8 divisions, we can easily see this property take shape when we consider the following:

1 % 8 = 1   2 % 8 = 2
3 % 8 = ?   4 % 8 = ?
5 % 8 = ?   6 % 8 = ?
7 % 8 = ?   8 % 8 = ?
9 % 8 = ?   10 % 8 = ?

-6 % 8 = ?   -11 % 8 = ?



Modular Arithmetic

If we consider a clock with 8 divisions, we can easily see this property take shape when we consider the following:

1 % 8 = 1   2 % 8 = 2
3 % 8 = 3   4 % 8 = ?
5 % 8 = ?   6 % 8 = ?
7 % 8 = ?   8 % 8 = ?
9 % 8 = ?   10 % 8 = ?

-6 % 8 = ?   -11 % 8 = ?

Modular Arithmetic

If we consider a clock with 8 divisions, we can easily see this property take shape when we consider the following:

1 % 8 = 1   2 % 8 = 2
3 % 8 = 3   4 % 8 = 4
5 % 8 = ?   6 % 8 = ?
7 % 8 = ?   8 % 8 = ?
9 % 8 = ?   10 % 8 = ?

-6 % 8 = ?   -11 % 8 = ?

Modular Arithmetic

If we consider a clock with 8 divisions, we can easily see this property take shape when we consider the following:

1 % 8 = 1   2 % 8 = 2
3 % 8 = 3   4 % 8 = 4
5 % 8 = 5   6 % 8 = ?
7 % 8 = ?   8 % 8 = ?
9 % 8 = ?   10 % 8 = ?

-6 % 8 = ?   -11 % 8 = ?

Modular Arithmetic

If we consider a clock with 8 divisions, we can easily see this property take shape when we consider the following:

1 % 8 = 1   2 % 8 = 2
3 % 8 = 3   4 % 8 = 4
5 % 8 = 5   6 % 8 = 6
7 % 8 = ?   8 % 8 = ?
9 % 8 = ?   10 % 8 = ?

-6 % 8 = ?   -11 % 8 = ?

Modular Arithmetic

If we consider a clock with 8 divisions, we can easily see this property take shape when we consider the following:

1 % 8 = 1   2 % 8 = 2
3 % 8 = 3   4 % 8 = 4
5 % 8 = 5   6 % 8 = 6
7 % 8 = 7   8 % 8 = ?
9 % 8 = ?   10 % 8 = ?

-6 % 8 = ?   -11 % 8 = ?

Modular Arithmetic

If we consider a clock with 8 divisions, we can easily see this property take shape when we consider the following:

1 % 8 = 1   2 % 8 = 2
3 % 8 = 3   4 % 8 = 4
5 % 8 = 5   6 % 8 = 6
7 % 8 = 7   8 % 8 = 0
9 % 8 = ?   10 % 8 = ?

-6 % 8 = ?   -11 % 8 = ?

Modular Arithmetic

If we consider a clock with 8 divisions, we can easily see this property take shape when we consider the following:

1 % 8 = 1   2 % 8 = 2
3 % 8 = 3   4 % 8 = 4
5 % 8 = 5   6 % 8 = 6
7 % 8 = 7   8 % 8 = 0
9 % 8 = 1   10 % 8 = ?

-6 % 8 = ?   -11 % 8 = ?

Modular Arithmetic

If we consider a clock with 8 divisions, we can easily see this property take shape when we consider the following:

1 % 8 = 1   2 % 8 = 2
3 % 8 = 3   4 % 8 = 4
5 % 8 = 5   6 % 8 = 6
7 % 8 = 7   8 % 8 = 0
9 % 8 = 1   10 % 8 = 2

-6 % 8 = ?   -11 % 8 = ?

Modular Arithmetic

If we consider a clock with 8 divisions, we can easily see this property take shape when we consider the following:

1 % 8 = 1   2 % 8 = 2
3 % 8 = 3   4 % 8 = 4
5 % 8 = 5   6 % 8 = 6
7 % 8 = 7   8 % 8 = 0
9 % 8 = 1   10 % 8 = 2

-6 % 8 = 2   -11 % 8 = ?

Modular Arithmetic

If we consider a clock with 8 divisions, we can easily see this property take shape when we consider the following:

1 % 8 = 1 2 % 8 = 2
3 % 8 = 3 4 % 8 = 4
5 % 8 = 5 6 % 8 = 6
7 % 8 = 7 8 % 8 = 0
9 % 8 = 1 10 % 8 = 2

-6 % 8 = 2 -11 % 8 = 5

Modular Arithmetic

We can use the properties of mod to do some larger expression that seem difficult to do by hand:

(8 *212654565321214) % 8 = ?

(1600007* 40000001) % 8 = ?

(2400007* 40000005) % 8 = ?

Modular Arithmetic

We can use the properties of mod to do some larger expression that seem difficult to do by hand:

(8 *212654565321214) % 8 = 0

(1600007* 40000001) % 8 = ?

(2400007* 40000005) % 8 = ?

Modular Arithmetic

We can use the properties of mod to do some larger expression that seem difficult to do by hand:

(8 *212654565321214) % 8 = 0

(1600007* 40000001) % 8 = (7 * 1) % 8 = 7

(2400007* 40000005) % 8 = ?

Modular Arithmetic

We can use the properties of mod to do some larger expression that seem difficult to do by hand:

(8 *212654565321214) % 8 = 0

(1600007* 40000001) % 8 = (7 * 1) % 8 = 7

(2400007* 40000005) % 8 = 3

Encryption

- Encryption goes as far back as the ancient Greeks and Spartans using a thing called a scytale.
- Another method called the Caesar cipher involves shifting the alphabet by a certain amount. Shift by 5 :

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
F G H I J K L M N O P Q R S T U V W X Y Z A B C D E

- But this seemed too simple so they would come up with a keyword to map the letters:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
V I C T O R Y A B D E F G H J K L M N P Q S U W X Z

RSA

Three Gentlemen from MIT, Ron Rivest, Adi Shamir, and Leonard Adleman developed public-key cryptography, a new idea to encryption. Rivest being a cse man, he asked two mathmaticans Shamir and Adleman to help him

him develop his ideas. It was a night of drunken madness that finally lead Rivest to the solution.

* this is in no way a promotion for excessive drinking or irresponsible behavior.

What's the Big Idea?

Fermat developed a theorem, called Fermat's Little Theorem which states:

$a^p \bmod p = a \bmod p$

RSA makes a slight modification:

$a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$

for distinct primes p and q

Such that, gcd(a,pq) = 1

What's the Big Idea?

- Pick two primes p and q, compute $n = p \times q$
- Pick two numbers e and d, such that:

$$e \times d = k(p-1)(q-1) + 1 \text{ (for some k)}$$

Publish n and e (public key), encode with:

$$(\text{original message})^e \bmod n$$

- Keep d, p and q secret (private key), decode with:

$$(\text{encoded message})^d \bmod n$$