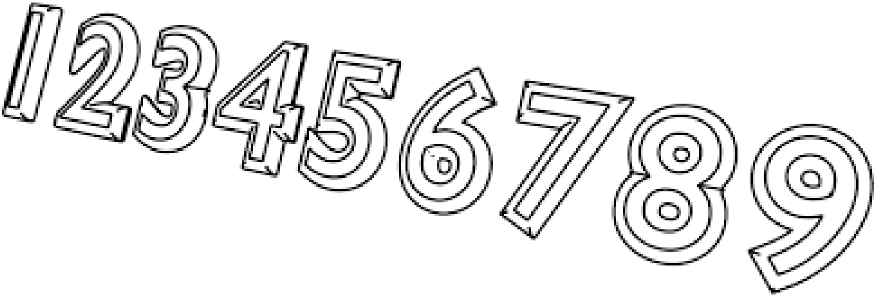
Number Theory and the RSA Cryptosystem

Gwen Liu

Mentor: Greyson Potter

Outline

Why number theory?



Euclidean Algorithm and Linear Equation Theorem

Linear Equation Theorem

Can always find a pair (x, y) such that $ax + by = gcd(a, b)$

Given: $22x + 60y = gcd(22, 60)$

$$\begin{aligned}
60 &= 2 \times 22 + 16 \\
22 &= 1 \times 16 + 6 \\
16 &= 2 \times 6 + 4 \\
6 &= 1 \times 4 + 2 \\
4 &= 2 \times 2 + 0
\end{aligned}$$

Congruences

We say that "a is congruent to $b \pmod{m}$"
$a \equiv b \pmod{m}$

Example

- $7 \equiv 2 \pmod{5}$
- $47 \equiv 35 \pmod{6}$

Fermat's little theorem

Theorem (Fermat's little theorem)

For a prime p and integer a, we have $a^{p-1} \equiv 1 \pmod{p}$

Example

- $3^6 \equiv 1 \pmod{7}$
-

$x \pmod{7}$	1	2	3	4	5	6
$3x \pmod{7}$	3	6	2	5	1	4

-

$$\underbrace{(3\cdot 1)(3\cdot 2)(3\cdot 3)(3\cdot 4)(3\cdot 5)(3\cdot 6)}_{\text{numbers in second row}} \equiv \underbrace{1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6}_{\text{numbers in first row}} \pmod{7}.$$

Euler's φ function and Euler's formula

Euler's φ function

The number of integers between 1 and m that are relatively prime to m.

Euler's formula

If $gcd(a, m) = 1$, then $a^{\varphi(m)} \equiv 1 \pmod{m}$

Powers modulo m

Solves really large powers $\pmod m$: $5^{100000000000} \pmod{12826832}$

Example

- $7^{327} \pmod{853}$

- $$\begin{aligned}
7^1 & & & \equiv 7 & & \equiv 7 \pmod{853} \\
7^2 &\equiv \left(7^1\right)^2 & &\equiv 7^2 & &\equiv 49 & &\equiv 49 \pmod{853} \\
7^4 &\equiv \left(7^2\right)^2 & &\equiv 49^2 & &\equiv 2401 & &\equiv 695 \pmod{853} \\
7^8 &\equiv \left(7^4\right)^2 & &\equiv 695^2 & &\equiv 483025 & &\equiv 227 \pmod{853} \\
7^{16} &\equiv \left(7^8\right)^2 & &\equiv 227^2 & &\equiv 51529 & &\equiv 349 \pmod{853} \\
7^{32} &\equiv \left(7^{16}\right)^2 & &\equiv 349^2 & &\equiv 121801 & &\equiv 675 \pmod{853} \\
7^{64} &\equiv \left(7^{32}\right)^2 & &\equiv 675^2 & &\equiv 455625 & &\equiv 123 \pmod{853} \\
7^{128} &\equiv \left(7^{64}\right)^2 & &\equiv 123^2 & &\equiv 15129 & &\equiv 628 \pmod{853} \\
7^{256} &\equiv \left(7^{128}\right)^2 & &\equiv 628^2 & &\equiv 394384 & &\equiv 298 \pmod{853}
\end{aligned}$$

- $$\begin{aligned}
7^{327} &= 7^{256+64+4+2+1} \\
&= 7^{256} \cdot 7^{64} \cdot 7^4 \cdot 7^2 \cdot 7^1 \\
&\equiv 298 \cdot 123 \cdot 695 \cdot 49 \cdot 7 \pmod{853}.
\end{aligned}$$

k^{th} roots modulo m

$x^k \equiv b \pmod{m} \implies x$=??

Method

φ function $\implies ku - \varphi v = 1$ with Euclidean algorithm $\implies$ successive squaring

Example

- $x^{131} \equiv 758 \pmod{1073}$
- $\varphi(1073) = 28 \times 36 = 1008$
- $131u - 1008v = 1 \implies 131 \times 731 - 1008 \times 95 = 1$
- Notice: $x^{131^{731}} = x^{131 \times 731} = x^{1+1008 \times 95} = x \times x^{1008 \times 95}$
- Euler's : $x^{1008} \equiv 1 \pmod{1073}$
- $x^{131^{731}} \equiv x \pmod{1073}$
- $x \equiv x^{131^{731}} \equiv 758^{731} \pmod{1073} \equiv 905 \pmod{1073}$

Key Generation and Distribution

1. Choose two distinct prime numbers p and q
2. Compute $m = p \times q$
3. Compute $\varphi(m) = (p - 1) \times (q - 1)$ since p and q are prime
4. Choose a number k that is relatively prime to phi(m)

Private

- p, q - the two primes
- $\varphi(m)$

Public

- k
- m

This is called a public-key cryptosystem.

RSA Encryption

Now...anyone who wants to send us a message uses the values of m and k to encode in the following manner:

1. Convert message into a string of digits:

A	B	C	D	E	F	G	H	I	J	K	L	M
11	12	13	14	15	16	17	18	19	20	21	22	23

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
24	25	26	27	28	29	30	31	32	33	34	35	36

2. Break the string of digits into numbers less than m
3. Use successive squaring to compute $a^k \pmod{m}$
4. Example: $p = 73$, $q = 97$, $m = 7081$, $k = 347$

H	E	L	L	O
1815		2222		25
$1815^{347} (mod\ 7081)$		$2222^{347} (mod\ 7081)$		$25^{347} (mod\ 7081)$
2212		6844		6593

RSA Decryption

Decryption requires using the k^{th} roots modulo m method which requires finding $\varphi(m)$, easy for us if we know the factors p and q since $\varphi(m) = (p-1)(q-1)$:

2212		6844		6593
$x^{347}(mod\ 7081)$		$x^{347}(mod\ 7081)$		$x^{347}(mod\ 7081)$
1815		2222		25
H	E	L	L	O

Code!

5301435910, 4794709296

m = 6022651441

k = 57737

References

Silver, Joseph, H.
A Friendly Introduction to Number Theory.
Pearson, 2012.

https://www.math.brown.edu/johsilve/frint.html