Week 5, lecture 1: More on Euler Phi function. Applications to cryptography

MA180/185/190 Algebra

Angela Carnevale

Euler's Phi function

Applications: cryptography

Recap

Chinese Remainder Thm

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ x \equiv a_3 \pmod{n_3} \end{cases}$$

was a soln if n_1, n_2, n_3 are pairwise coprime. If x_0 is a soln, then $x_0 + n_1 \cdot n_2 \cdot n_3 \cdot t$, $t \in \mathbb{Z}$ is also a soln.

Primes → every integer can be written as product of primes

→ Fermat's little thm

if p prime and $\gcd(a,p)=1$ then

$$\boxed{a^{p-1} \equiv 1 \pmod{p}}$$

Recap

Euler's Phi function

$\phi(n) = \#$ integers between 0 and $n-1$ and are coprime to n

$\longrightarrow$ m, n coprime $\Rightarrow$ $\phi(mn) = \phi(m) \cdot \phi(n)$ (1)

$\longrightarrow$ p prime $\Rightarrow$ $\phi(p^e) = p^e - p^{e-1}$ (2)

$n = 168 = 2 \cdot 84 = 2^2 \cdot 42 = 2^3 \cdot 21 = 2^3 \cdot 3 \cdot 7$

$\phi(168) = \phi(2^3) \cdot \phi(3) \cdot \phi(7) = (2^3 - 2^2) \cdot 2 \cdot 6 = 48$

Euler's Phi function and powers

Theorem (Euler's Totient theorem)

If $\gcd(a, m) = 1$ then

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Note. In the special case in which m is a prime number, this is Fermat's little theorem.

Example. Determine the last two digits of 3^{176}. This is the same as $3^{176} \bmod (100)$

Note that $\gcd(3,100)=1$ so Euler's thm applies.

$$\phi(100) = \phi(2^2 \cdot 5^2) \overset{1}{=} \phi(2^2)\phi(5^2) \overset{2}{=} (2^2 - 2^1)\cdot(5^2-5^1) = 40$$

by the remainder thm $176 = 4 \cdot 40 + 16$ so $3^{176} = (3^{40})^4 \cdot 3^{16}$

So $3^{176} \equiv (3^{40})^4 \cdot 3^{16} \underset{\text{Euler's thm}}{\equiv} 3^{16} \pmod{100}$

Euler's Phi function and powers

We can simplify further our computation by observing that $3^5 = 243 \equiv 43 \pmod{100}$

So $3^{16} \equiv (3^5)^3 \cdot 3 \equiv (243)^3 \cdot 3 \equiv (43)^3 \cdot 3 \equiv 43^2 \cdot 43 \cdot 3 \equiv 49 \cdot 43 \cdot 3 \equiv 21 \pmod{100}$

using that $16 = 5 \cdot 3 + 1$

since $243 \equiv 43 \pmod{100}$

$43^2 = 1849 \equiv 49 \pmod{100}$

We can use Euler's theorem to compute with large powers modulo any number (provided the base is coprime to the modulus).

Example. Evaluate $5^{50} \pmod{168}$.

→ First, note that $\gcd(5,168) = 1$ so Euler's thm applies.

→ Recall: we computed $\phi(168) = 48$

So $5^{50} = \underbrace{5^{48}}_{\text{this is } 5^{\phi(168)} \text{ so it's } \equiv 1 \pmod{168}} \cdot 5^2 \equiv 1 \cdot 5^2 \equiv 25 \pmod{168}$.

Euler’s Phi function

Applications: cryptography

Cryptography

Idea: encrypt messages to be able to send them through public channels while protecting the content.

We call plaintext the message that we would like to send to some receiver.

We call ciphertext the encrypted message to be sent through some public channel.

Ideally, our encryption method should be hard to crack and reversible.

Private key cryptography is based on some agreement between sender and receiver whereby they agree on parameters that determine the encrypting function.

Our first example, affine ciphers is an example of private key cryptography.

Affine ciphers

One way to encrypt information is to use **affine** transformations. Consider the following 26-letter alphabet:

$$A = 1,\ B = 2, \dots, Z = 26 = 0.$$

Using the above correspondence between the alphabet and $\mathbb{Z}_{26}$ we then use affine transformations of the form $f_E : \mathbb{Z}_{26} \to \mathbb{Z}_{26}, x \mapsto ax + b$ to **encrypt** our message by replacing each letter with its image under f_E.

Note.

- we will see soon that for this to be a function that can be decoded, we'll need $a \in \mathbb{Z}_{26}$ to be invertible. This tells us that the invertible encription functions on a 26-letter alphabet are $\phi(26) \cdot 26$
- In its simplest form, this method to encrypt messages was already used by Julius Caesar! (1st century BC)

Affine ciphers: encoding

Example. Suppose we want to encrypt the word MATHS using the affine transformation $f_E(x) = 3x + 11$. According to our correspondence above, the letter in MATHS correspond to:

Apply f_E

$M \leftrightarrow 13 \rightsquigarrow 3 \cdot 13 + 11 = 50 \equiv 24 \pmod{26} \rightsquigarrow X$

$A \leftrightarrow 1 \rightsquigarrow 3 \cdot 1 + 11 \equiv 14 \pmod{26} \rightsquigarrow N$

$T \leftrightarrow 20 \rightsquigarrow 3 \cdot 20 + 11 \equiv 19 \pmod{26} \rightsquigarrow S$

$H \leftrightarrow 8 \rightsquigarrow 3 \cdot 8 + 11 \equiv 35 \equiv 9 \pmod{26} \rightsquigarrow I$

$S \leftrightarrow 19 \rightsquigarrow 3 \cdot 19 + 11 \equiv 68 \equiv 16 \pmod{} \rightsquigarrow P$

The <u>ciphertext</u> corresp. to MATHS undeo f_E is

XNSIP

Affine ciphers: decoding

If we happen to know the affine transformation f_E used to encrypt a message (and the alphabet used), we can decode a message by inverting the function f_E and applying the inverse transformation to the ciphertext.

We know that $f_E(x) = ax + b$, so to recover x we write:

$ax+b = y$ so $x = a^{-1}(y-b) = a^{-1} \cdot y - a^{-1} \cdot b$

Note.

- Here we used the fact that a in the affine transformation is invertible in $\mathbb{Z}_{26}$.
- In general, one can use alphabets containing more symbols, upper and lower case letters, numbers etc.

Affine ciphers: decoding

Example (continued). The following message was encrypted using the affine transformation in the previous example: WDAZ

What's the plaintext?

New challenge: a ciphertext

We receive the following ciphertext:

OT WOZMZ
LZII UXSZ UZPXUTSJ WOTR NZRRFJZ

(here the space between words was maintained).

We know it was encrypted via an affine transformation, but we don't know the key.

Can you decode the message?

Hint. Can you guess what 2-word letter could open such message?