

§ 20 Application to arithmetic

"little theorem" of Fermat, Euler's φ function

Motivation : given two integers a and n , when do we have $a^x \equiv 1 \pmod{n}$? ($\Leftrightarrow n$ divides $a^x - 1$)

(Related : what can we say about x from $a^x \equiv b \pmod{n}$? "discrete logarithm problem")

History

- The "little theorem" of Fermat (1640)

when n is prime, $n \nmid a$, then $a^{n-1} \equiv 1 \pmod{n}$

- Euler's φ function (totient function) (1763)

set $\varphi(n)$ = number of k s.t. $1 \leq k < n$, $\gcd(k, n) = 1$

Then ~~a~~ $\gcd(a, n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$

Rem : when n is prime $\varphi(n) = n-1$, $\gcd(a, n) = 1 \Leftrightarrow n \nmid a$

$\Rightarrow$ we should look at the subset

$$\mathbb{Z}_n^* = \{k \mid \gcd(k, n) = 1\} \subset \mathbb{Z}_n$$

and product binary op. on $\mathbb{Z}_n^*$

We will check (Th'm 20.6)

- $\mathbb{Z}_n^*$ is closed under the prod. bin. op.

$$k, l \in \mathbb{Z}_n^* \Rightarrow kl \in \mathbb{Z}_n^*$$

- in fact, $\mathbb{Z}_n^*$ becomes a group with product bin. op.

$$k \in \mathbb{Z}_n^* \Rightarrow \exists l \in \mathbb{Z}_n^* : kl = 1 \text{ in } \mathbb{Z}_n$$

- $\varphi(n) = |\mathbb{Z}_n^*|$ order of the group (num. of elems.)

Recall the consequence of Lagrange's thm
(7 feb., Thm 10.10)

if G is a finite group, $a \in G$, $m = |G|$
then $a^m = e$
(we have $a^k = e$ for $k = |\langle a \rangle|$, k divides n)
 $\langle a \rangle \cong \mathbb{Z}_k$ Lagrange's thm.

Use this for $G = \mathbb{Z}_n^\times$ and get $a^{\varphi(n)} \equiv 1 \pmod n$
for $\gcd(a, n) = 1$
($a \in \mathbb{Z}_n^\times$)

Prop $\mathbb{Z}_n^\times$ is closed under prod. bin. op.

Proof. Step 1. $k \in \mathbb{Z}_n^\times$ means k is not a zero-divisor in $\mathbb{Z}_n$

is a zero-div. in $\mathbb{Z}_n \Leftrightarrow a$ has some divisors of n

$\hookrightarrow a$ s.t. $ab = 0$

for nonzero b

$a = xy$, $x \neq 1$

x divides n

(then $b = \frac{n}{x}$ will do)

Step 2 k, l not zero divisors $\Rightarrow kl$ not a zero-div.

If $klb = 0$ then $b' = lb$ satisfies $kb' = 0$

k not zero-div $\Rightarrow b' = 0$

l not zero-div $\Rightarrow b = 0$ $\square$

Prop $\mathbb{Z}_n^\times$ is a group by the prod. bin. op.

Proof Step 1 $1 \in \mathbb{Z}_n^\times$ is an identity elem.

Step 2 ~~we~~ Fix $a \in \mathbb{Z}_n^\times$; then $ak \neq al$
if $k, l \in \mathbb{Z}_n^\times$, $k \neq l$

$ak = al$ in $\mathbb{Z}_n^\times \subset \mathbb{Z}_n$ means $a(k-l) = 0$ in $\mathbb{Z}_n$

a is not a zero-div. $\Rightarrow k-l = 0$ in $\mathbb{Z}_n$

Step 3 $\exists b \in \mathbb{Z}_n^\times$: $ab = 1$

Write $\mathbb{Z}_n^\times = \{a_1, \dots, a_r\}$ $a_i \neq a_j$ for $i \neq j$

then $aa_1, \dots, aa_r$ are distinct elements
of $\mathbb{Z}_n^\times$ that has only r elements.

$\leadsto$ any $c \in \mathbb{Z}_n^\times$ is of the form aa_i

we can take $c=1$

□

- we will later see $\mathbb{Z}_p^\times \cong \mathbb{Z}_{p-1}$ (§23)

- $\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$

$$(\Leftrightarrow \varphi(n) = p_1^{e_1-1} (p_1-1) \cdots p_r^{e_r-1} (p_r-1)$$

$$\text{if } n = p_1^{e_1} \cdots p_r^{e_r})$$

1. The first part of the paper discusses the importance of understanding the underlying structure of the data. This is particularly relevant in the context of machine learning, where the model's performance is heavily dependent on the quality of the input data.

2. The second part of the paper focuses on the development of a new algorithm for solving the problem of finding the minimum variance unbiased estimator (MVUE) for the parameters of a normal distribution.

3. The third part of the paper presents a detailed analysis of the proposed algorithm, showing that it achieves the Cramér-Rao lower bound (CRLB) for the variance of the estimator.

4. The fourth part of the paper provides a numerical comparison of the proposed algorithm with existing methods, demonstrating its superior performance in terms of both accuracy and computational efficiency.

5. The fifth part of the paper concludes with a discussion of the implications of the results and suggests directions for future research.

