37181 DISCRETE MATHEMATICS

Lecture 15: Number theory

PLAN

- Number theory
- Simple encryption
- Repeated squaring
- Euler's φ function

Recall, we have defined $\mathbb{N}$ (and $\mathbb{Z}$) with $+$ and $\times$.

We defined $\quad a \mid b \quad$ if ...

We defined $\quad a \equiv b \bmod d \quad$ if ...

Recall, we have defined $\mathbb{N}$ (and $\mathbb{Z}$) with $+$ and $\times$.

We defined $\quad a \mid b \quad$ if . . .

We defined $\quad a \equiv b \bmod d \quad$ if . . .

Define $[a]_d$ to be the remainder $0 \leqslant r < d$ of a on division by d.

Lemma

$[[a]_d + [b]_d]_d = [a+b]_d$

Proof:

$\square$

Lemma

$[[a]_d[b]_d]_d = [ab]_d$

Proof:

$\square$

Suppose someone tricks you into believing that

$$233 \cdot 577 = 135441$$

Use congruences (*i.e.* mod) to prove them wrong. [1]

[1] From Lauritzen, Concrete Abstract Algebra. Do it without a calculator.

Here is a trick to computer $[x]_3$ really fast: if

$$x = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10 + a_0$$

(that is, as a base-10 number $x = a_n \dots a_0$)

then since $10 = 9 + 1 \equiv 1 \mod 3$, we can simply add up the digits then reduce mod 3.

Proof:

$\square$

Here is a trick to computer $[x]_3$ really fast: if

$$x = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10 + a_0$$

(that is, as a base-10 number $x = a_n \ldots a_0$)

then since $10 = 9 + 1 \equiv 1 \mod 3$, we can simply add up the digits then reduce mod 3.

Proof:

$\square$

Same argument works for reducing mod 9.

Assign numbers $0, \ldots, 25$ to the letters $A, \ldots, Z$.

Define a function $f : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$ by

$$f(X) = \alpha X + \beta \bmod 26$$

If you choose α, β wisely (*i.e.* so that f is a bijection), the function f will have a *decoding function* (inverse)

APPLICATIONS: AFFINE CIPHER (TO SEND SECRET MESSAGES)

Assign numbers $0, \ldots, 25$ to the letters $A, \ldots, Z$.

Define a function $f : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$ by

$$f(X) = \alpha X + \beta \bmod 26$$

If you choose α, β wisely (*i.e.* so that f is a bijection), the function f will have a *decoding function* (inverse)

$$g(X) = \alpha^{-1}(X - \beta) \bmod 26$$

Question: what does α^{-1} (multiplicative inverse) mean working mod 26?

Assign numbers $0, \ldots, 25$ to the letters $A, \ldots, Z$.

Define a function $f : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$ by

$$f(X) = \alpha X + \beta \bmod 26$$

If you choose α, β wisely (*i.e.* so that f is a bijection), the function f will have a *decoding function* (inverse)

$$g(X) = \alpha^{-1}(X - \beta) \bmod 26$$

Question: what does α^{-1} (multiplicative inverse) mean working mod 26?

Answer: a number so that when you multiply them, they give 1 (mod 26).

Eg: $25.25 = 625 = 624 + 1$ so 25 is the inverse of 25.

Recall: $\gcd(a, b)$ is the greatest positive integer that divides both a and b.

Recall: $\gcd(a, b)$ is the greatest positive integer that divides both a and b.

Formal: $d = \gcd(a, b)$ if $d > 0$, $d \mid a, d \mid b$, and if $c \mid a, c \mid b$ then $c \mid d$.

Recall: $\gcd(a, b)$ is the greatest positive integer that divides both a and b.

Formal: $d = \gcd(a, b)$ if $d > 0$, $d \mid a, d \mid b$, and if $c \mid a, c \mid b$ then $c \mid d$.

Recall Euclidean algorithm to compute it.

Given x, we want to find y so that $x.y \equiv 1 \bmod 26$. So we run Euclid alg backwards.

Eg, if $\alpha = 3$, find $\alpha^{-1} \pmod{26}$.

Eg, if $\alpha = 3$, find $\alpha^{-1} \pmod{26}$.

$26 = 8.3 + 2$
$3 = 1.2 + 1.$
Rewrite $1 = \ldots$

Ex: find inverse mod 26 for $\alpha = 11$ and $\alpha = 13$

The following message was encoded using an affine cipher $f(X) = 3X + 1$.

`wniirpraik`

Decode it.

APPLICATIONS

The following message was encoded using an affine cipher $f(X) = 3X + 1$.

$$\texttt{wniirpraik}$$

Decode it.

Hint: $g(X) = \alpha^{-1}(X-1)$. So find "3^{-1} mod 26".

This might be useful:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
t	u	v	w	x	y	z												
19	20	21	22	23	24	25												

If $\gcd(a, b) = 1$ we say a, b are *relatively prime*.

Ex: which pairs of numbers are relatively prime out of: $58, 491, 62$?

Credit card numbers, ISBN numbers, barcodes contain a *check digit*.

ISBN numbers (after 2007) are 13 digits long and the rule is:

$$\sum_{j=0}^{6} a_{2j+1} + \sum_{j=1}^{6} 3a_{2j} \equiv 0 \bmod 10$$

Credit card numbers, ISBN numbers, barcodes contain a *check digit*.

ISBN numbers (after 2007) are 13 digits long and the rule is:

$$\sum_{j=0}^{6} a_{2j+1} + \sum_{j=1}^{6} 3a_{2j} \equiv 0 \bmod 10$$

Ex: Check the ISBN is correct for Lauritzen: $978 - 0 - 521 - 53410 - 9$.

Credit cards use a different formula: see `https://en.wikipedia.org/wiki/Luhn_algorithm` and the worksheet.

REPEATED SQUARING

Suppose you need to know 3^{900} mod 34.

Calculator?

REPEATED SQUARING

Suppose you need to know $3^{900} \bmod 34$.

Calculator? Hmm. Here is a cool trick.

Suppose you need to know $3^{900} \bmod 34$.

Calculator? Hmm. Here is a cool trick.

- write 900 base 2 (in binary) as $\sum b_i 2^i$ with $b_i \in \{0, 1\}$.
- Compute

  $3^1 =$

  $3^2 =$

  $3^4 = 3^2.3^2 =$

  $3^8 = 3^4.3^4 =$

  $3^{16} = \ldots$

  and each time, reduce mod 34.

APPLICATIONS

Ex: Compute $121^{12} \bmod 13$

Ex: Compute $2^{1000} \bmod 7$

Let $n \in \mathbb{N}_+$. Define

$$\varphi(n) = |\{x \in \mathbb{N} \mid 1 \leqslant x < n, \gcd(x, n) = 1\}$$

to be the number of numbers between $0, n$ which are relatively prime to n.

Ex: $\varphi(13) =$

Ex: $\varphi(20) =$

Ex: $\varphi(36) =$

Lemma

If p is prime, then $\varphi(p) = p - 1$.

Lemma

If p is prime, then $\varphi(p) = p - 1$.

Proof.

If $1 \leqslant i < p$ then $\gcd(i, p) = 1$ (if not, $\exists d \in \mathbb{Z}$, $1 < d \leqslant i$ with $d \mid i$ and $d \mid p$ but only $1, p$ divide p.) $\square$

Lemma

If p is prime, then $\varphi(p^2) =?$.

NEXT

Next lecture:

- more on Euler's phi function
- Euler's theorem
- Fermat's little theorem