# 37181 DISCRETE MATHEMATICS

©Murray Elder, UTS

Lecture 15: Number theory

# PLAN

- Number theory
- Simple encryption
- Repeated squaring
- Euler's $\varphi$ function


©Murray Elder, UTS

$\mathbb{N}$+ $\mathbb{N} = \{0, 1, 2 \ldots\}$
" $\{1, 2, 3, \ldots\}$

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

We defined $a \mid b$ if ... $\exists\, s \in \mathbb{Z}$ $(b = s \cdot a)$
'divides

We defined $a \equiv b \bmod d$ if ... $d \mid (b - a)$

equivalent, modulo

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

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

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

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

$[31]_5 = 1$.

$[31]_5 = [25+6]$

$= [[25]_5 + [6]_5]$

$= [0+1]$

$= 1$

**Lemma**

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

Proof: Let $a = pd + s$ $\quad [a]_d = s$

$b = qd + t$ $\quad [b]_d = t$

$0 \le s, t < d$

$LHS = [[a]_d + [b]_d]_d = [s+t]_d$

$RHS = [pd + s + qd + r]_d = [(p+q)d + (r+s)]_d$

$= [r+s]_d$

$(pd + r + s) - (r+s) = 0$

□

$[100]_9 = [[10]_9 \cdot [10]_9]_9$
$= [1 \cdot 1]_9$
$= 1.$

**Lemma**

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

Proof: Let $a = pd + s$
$b = qd + t$

$ab = (pd+s)(qd+t) = pqd^2 + pdt + qsd + st$ □

$\Rightarrow$ RHS. $[ab]_d = [st]_d$

LHS: $[st]_d$ ✓ LHS = RHS.

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

Suppose someone tricks you into believing that

$$233 \cdot 577 = 135441$$

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

Try $d=2$

$$[[233]_2[577]_2]_2 = 1 \cdot 1 = 1$$

$[135441]_2$

$d=5$ $3 \cdot 2 = 6 \to 1$.

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

$d = 3$

$3 \overline{)233}$ $\begin{matrix} 77 \\ \\ \end{matrix}$ $\rightarrow$ rem 2.

$[233] = 2$.

$3 \overline{)577}$ $\begin{matrix} 189 \\ \\ \end{matrix}$ $\rightarrow$ rem 1

LHS $= [2 \cdot 1] = 2$.

$3 \overline{)13541}$ $\begin{matrix} 4517 \\ \\ \end{matrix}$ $\rightarrow$ 0 rem.

RHS $= 0$

$\therefore$

$\therefore$ $233.577 \neq 135441$.

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:

$$[x]_3 = [[a_n 10^n]_3 + [a_{n-1} 10^{n-1}]_3 + \cdots + [a_1 10]_3 + a_0]$$

$$= [[a_n][10][10]\cdots[10]_3 + \cdots]$$

$$= [a_n + a_{n-1} + \cdots + a_0]_3$$

□

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:

$[x]_9$

□

Same argument works for reducing mod 9.

# APPLICATIONS: AFFINE CIPHER (TO SEND SECRET MESSAGES)

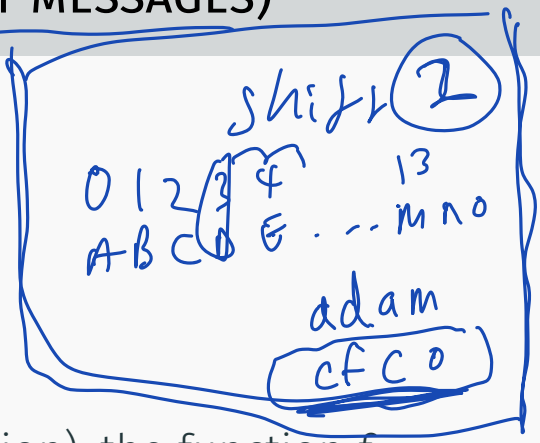
Assign numbers $0, \ldots, 25$ to the letters $A, \ldots, Z$.

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

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

$\alpha \in \mathbb{Z}_{26}$ $\beta \in \mathbb{Z}_{26}$

If you choose $\alpha, \beta$ wisely (*i.e.* so that $f$ is a bijection), the function $f$ will have a *decoding function* (inverse)




$\alpha = 0$ : $f(X) = \beta$.

$\mathbb{Z}/26\mathbb{Z}$

$\alpha = 1$ : shift $f(X) \equiv X + \beta$

# 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 $\alpha, \beta$ 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 $\alpha^{-1}$ (multiplicative inverse) mean working mod 26?

$g(f(X)) \stackrel{?}{=} X$

$g(f(X)) = g(\alpha X + \beta) = \alpha^{-1}(\alpha X + \beta - \beta) = [\alpha^{-1} \cdot \alpha \cdot X]_{26} = [\alpha^{-1}\alpha]_{26}[X]_{26} = 1$

# 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 $\alpha, \beta$ 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 $\alpha^{-1}$ (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 $c \mid d$.

$[[25]_{26}[25]_{26}]_{26}$ $[[-1]_{26}[25]_{26}]_{26} = [-1 \cdot 25]_{26} = 1$

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.

$\alpha^{-1}\alpha$

$26 = 1 \cdot 25 + 1$

$1 = 26 - 25$

$\alpha = 3$,
$\alpha^{-1} = 9$.

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

$26 = 8 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$

$1 = 3 - 2$

$= 3 - (26 - 8 \cdot 3)$

$= 9 \cdot 3 - 26$

$1 = 9 \cdot 3 - 26$

$26 \mid 9 \cdot 3 - 1$

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

$26 = 8 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1.$

Rewrite $1 = \ldots$ $3 - 2 = 3 - (26 - 8 \cdot 3)$

$= 3 - 26 + 8 \cdot 3 = 9 \cdot 3 - 26$

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

$[9 \cdot 3]_{26} = 1.$

$26 = 2 \cdot 11 + 4$

$11 = 2 \cdot 4 + 3$

$4 = 1 \cdot 3 + 1$

$1 = 4 - 3 = 4 - (11 - 2 \cdot 4) = 4 - 11 + 2 \cdot 4$

$= 3 \cdot 4 - 11 = 3(26 - 2 \cdot 11) - 11$

$= 3 \cdot 26 - 6 \cdot 11 - 11$

$= 3 \cdot 26 - 7$

$1 \equiv -7 \cdot 11 \mod 26$ so $\alpha = 11$, $\alpha^{-1} = 19$

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

$\alpha$ $\beta$

wniirpraik

Decode it.

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

$= 9(X - 1)$

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

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 | | | | | | | | | | | | |

$26 = 2 \cdot 13 + 0$

$\gcd(26, 13) = 13.$

So 13 doesn't have a multiplic. inverse mod 26

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

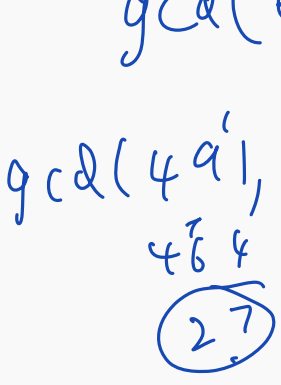
Ex: which pairs of numbers are relatively prime out of: $58, 491, 62$?

$\gcd(62, 58) \neq 1.$

$\gcd(491, 58) \neq 1$

$491 = 8 \cdot 58 + 27$

$58 = 2 \cdot 27 + 4$



$$491 = 7 \cdot 62 + 57$$
$$62 = 1 \cdot 57 + 5$$
$$57 = 11 \cdot 5 + 2$$
$$5 = 2 \cdot 2 + 1$$

$$\gcd(491, 62) = 1$$

---

Ex:
$$1 = 5 - 2 \cdot 2$$
$$= 5 - 2(57 - 11 \cdot 5)$$
$$= 5 - 2 \cdot 57 + 22 \cdot 5$$
$$= 23 \cdot 5 - 2 \cdot 57$$
$$= 23(62 - 57) - 2 \cdot 57$$
$$= 23 \cdot 62 - 23 \cdot 57 - 2 \cdot 57$$
$$= 23 \cdot 62 - 25 \cdot 57$$
$$= 23 \cdot 62 - 25(491 - 7 \cdot 62)$$
$$= 23 \cdot 62 - 25 \cdot 491 + 175 \cdot 62$$
$$= 198 \cdot 62 - 25 \cdot 491$$

$62 \times 7 = 434$

$25 \times 7 = 175$

... multiplicative inverse of 62 is

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

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

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

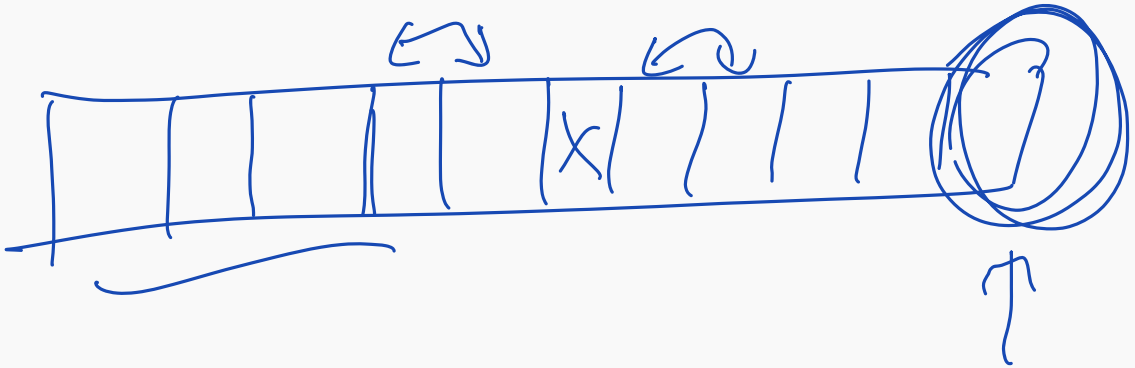
Credit card numbers, ISBN numbers, barcodes contain a *check digit*.

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 $3^{900} \bmod 34$.

Calculator?

$$\left[3^{900}\right]_{34}$$

$$= \left[3 \cdot 3^{899}\right]_{34}$$

# REPEATED SQUARING

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

Calculator? Hmm. Here is a cool trick.

Write 900 in binary

# REPEATED SQUARING

Suppose you need to know $3^{90} \bmod 34$.

Calculator? Hmm. Here is a cool trick.

- write 90 base 2 (in binary) as $\sum b_i 2^i$ with $b_i \in \{0, 1\}$.
- Compute
  $3^1 = 3$
  $3^2 = 9$
  $3^4 = 3^2 \cdot 3^2 = 9 \cdot 9 = 81 \equiv 13$
  $3^8 = 3^4 \cdot 3^4 \equiv 13 \cdot 13 = 169 \equiv -1 \bmod 34$
  $3^{16} = (-1)(-1) = 1$
  and each time, reduce mod 34.

$90 = 2^6 + 2^4 + 2^3 + 2^1$

in binary. $1011010_2$


©Murray Elder, UTS

$$3^{32} = 3^{16} \cdot 3^{16} = 1 \cdot 1 = 1$$

$$3^{64} = 3^{32} \cdot 3^{32} = 1 \cdot 1 = 1$$

---

$$3^{90} = 3^{64+16+8+2}$$

$$= 3^{64} \cdot 3^{16} \cdot 3^{8} \cdot 3^{2}$$

$$\equiv 1 \cdot 1 \cdot (-1) \cdot 9$$

$$\equiv -9$$

$$\equiv 25$$

$$\begin{array}{r} 34 \\ +9 \\ \hline 25 \end{array}$$

$12 = 8 + 4$

$1100_2$

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

$121 \equiv -9 \equiv 4 \bmod 13$

$121^2 \equiv 4 \cdot 4 = 16 \equiv 3$

$121^4 \equiv 3 \cdot 3 = 9 \equiv -4 \bmod 13$

$121^8 = 121^4 \, 121^4 = (-4)(-4) = 16 \equiv 3.$

$121^{12} \equiv 121^{8+4} = 121^8 \cdot 121^4 = (3)(-4) = -12 \equiv 1 \bmod 13.$

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

# EULER'S PHI FUNCTION

$\varphi : \mathbb{N}_+ \to \mathbb{N}$

size of set

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 1 and $n-1$ which are relatively prime to $n$.

Ex: $\varphi(13) =$ 12

$1, 2, 3, 4, 5, \ldots 12$

$\gcd(5, 13) = 1$

Ex: $\varphi(20) =$ 8

Ex: $\varphi(36) =$

1 2 3 4 5 6 7 8 9 10

1 2 3 4 5 6 7 8 9 10

11 12 13 14 15 16 17 18 19 20


©Murray Elder, UTS

**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 $p$.) $\square$

# EULER'S PHI FUNCTION

**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


©Murray Elder, UTS