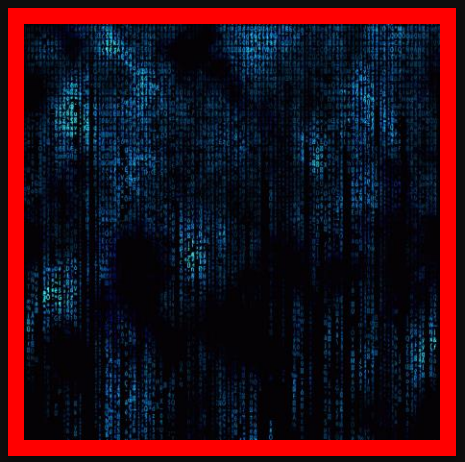
NUMBER THEORY



Anwitaman DATTA
SCSE, NTU Singapore

Acknowledgement: The following lecture slides are based on, and uses material from the text book **Cryptography and Network Security** (various eds) **by William Stallings**

NUMBER THEORY BASICS

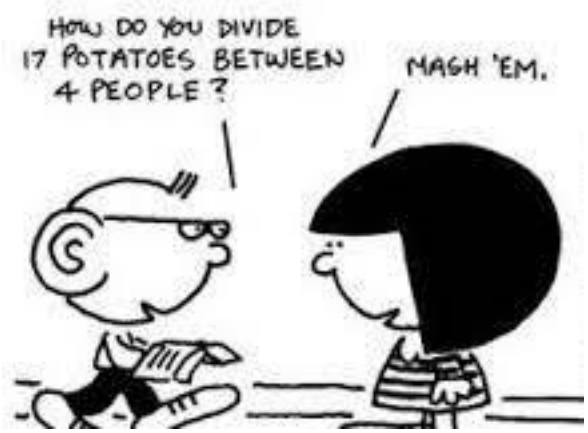
Part-I

- Euclidean algorithm and Bézout's identity
- Modular arithmetic
- Groups, rings and fields
- Galois fields and polynomial arithmetic

Divisibility

Consider

- a positive integer n
- any integer m



Euclidean division algorithm

- we have m = q*n+r
- for some integer q and $0 \leq r < n$
- we call q the quotient, r the remainder

e.g. with n = 7,
If m = 17, q = 2, r = 3
If m = 35, q = 5, r = 0
If m = -5, q = -1, r = 2

Divisibility

Consider

- a positive integer n
- any integer m

Euclidean division algorithm

- we have $m = q*n+r$
- for some integer q and $0 \leq r < n$
- we call q the quotient, r the remainder

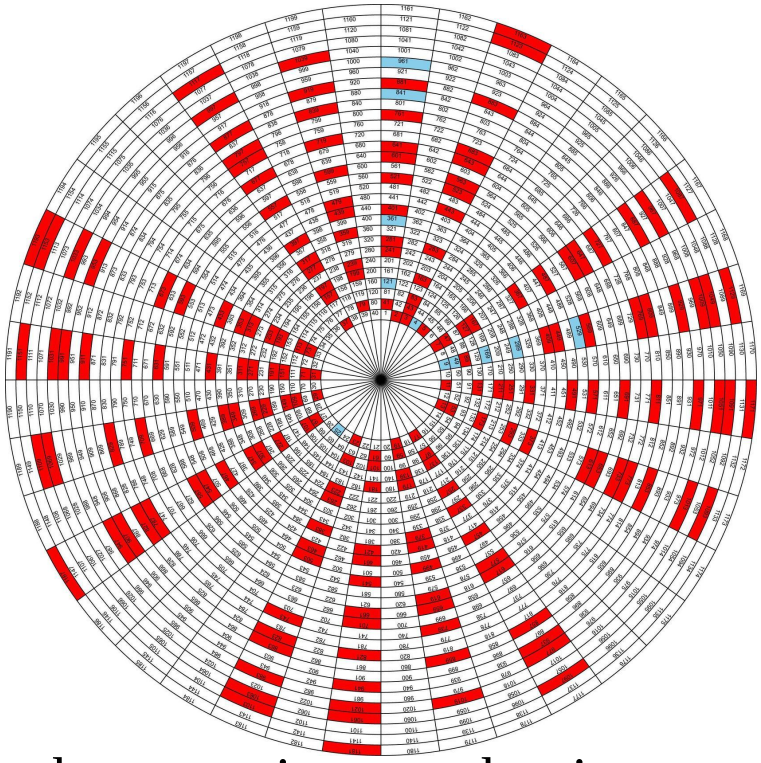
Note

- Given n & m:
  q and r are unique
- m mod n = r
- if r=0, we say that:
  n divides m
  m is divisible by n
  denoted as: n|m

Prime numbers

Definition:

- A positive integer **p > 1**
  iff its *only divisors* are ±1 and ±p



Trivia: As of December 2017, the largest known prime number is $2^{74,207,281} - 1$, a number with **22,338,618** digits. It was found in January 2016 by the Great Internet Mersenne Prime Search (GIMPS)

Image source: https://www.geek.com/wp-content/uploads/2013/10/primes.jpg

Greatest common divisor

- greatest common divisor of integers a and b, gcd(a,b) is the ***largest (positive) integer*** *that divides both of them*
  i.e., gcd(a,b) = max[k, such that k|a and k|b]

Note:
d=gcd(a,b) iff:
1. d is a divisor of both a and b
2. any divisor of a and b is a divisor of d

Two integers are ***relatively prime***, if their gcd is one
(i.e., only common positive integer factor is 1)

Greatest common divisor

properties

$gcd(a,b) = gcd(a,-b) = gcd(-a,b) = gcd(-a,-b) = gcd(|a|,|b|)$
$gcd(a,b) = gcd(b,a)$

$gcd(a,0) = |a|$

As a convention: $gcd(0,0) = 0$

Example: $gcd(45,30) = gcd(-30,45) = 15$

Computing gcd

Euclidean algorithm

Since gcd(a,b) = gcd(b,a) = gcd(|a|,|b|),
w.l.g., assume: $a \geq b > 0$

say:
$d=gcd(a,b)$
$a=q_1*b+r_1$ where $0 \leq r_1 < b$
case:
If $r_1=0$ then $b|a \rightarrow gcd(a,b)=b$

If $r_1 \neq 0$ then
since, $d|b \wedge d|a, \therefore d|(a-q_1*b)$, i.e. $d|r_1$
therefore, $d=gcd(b,r_1)$

Eukleides of Alexandria
4th-3rd century BC

```
function gcd(a, b) †
    if b = 0
        return a;
    else
        return gcd(b, a mod b);
```

† Note: The accompanying pseudocode is written slightly differently

Computing gcd

Euclidean algorithm

we have:

d=gcd(a,b)=gcd(b,r_1)

now consider gcd(b,r_1):

using same line of reasoning

gcd(b,r_1)=gcd(r_1,r_2)

where b= q_2*r_1+r_2

$$
\begin{aligned}
a &= q_1 b + r_1 && 0 < r_1 < b \\
b &= q_2 r_1 + r_2 && 0 < r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3 && 0 < r_3 < r_2 \\
&\vdots && \vdots \\
r_{n-2} &= q_n r_{n-1} + r_n && 0 < r_n < r_{n-1} \\
r_{n-1} &= q_{n+1} r_n + 0 \\
d &= \gcd(a, b) = r_n
\end{aligned}
$$

so we have:

d=gcd(a,b)=gcd(b,r_1) =gcd(r_1,r_2)

```
function gcd(a, b)
    if b = 0
        return a;
    else
        return gcd(b, a mod b);
```

gcd(1160718174,316258250)

exercise

gcd(1160718174,316258250)

$a = q_1 b + r_1$	$1160718174 = 3 \times 316258250 + 211943424$	$d = \gcd(316258250, 211943424)$
$b = q_2 r_1 + r_2$	$316258250 = 1 \times 211943424 + 104314826$	$d = \gcd(211943424, 104314826)$
$r_1 = q_3 r_2 + r_3$	$211943424 = 2 \times 104314826 + 3313772$	$d = \gcd(104314826, 3313772)$
$r_2 = q_4 r_3 + r_4$	$104314826 = 31 \times 3313772 + 1587894$	$d = \gcd(3313772, 1587894)$
$r_3 = q_5 r_4 + r_5$	$3313772 = 2 \times 1587894 + 137984$	$d = \gcd(1587894, 137984)$
$r_4 = q_6 r_5 + r_6$	$1587894 = 11 \times 137984 + 70070$	$d = \gcd(137984, 70070)$
$r_5 = q_7 r_6 + r_7$	$137984 = 1 \times 70070 + 67914$	$d = \gcd(70070, 67914)$
$r_6 = q_8 r_7 + r_8$	$70070 = 1 \times 67914 + 2156$	$d = \gcd(67914, 2156)$
$r_7 = q_9 r_8 + r_9$	$67914 = 31 \times 2516 + 1078$	$d = \gcd(2156, 1078)$
$r_8 = q_{10} r_9 + r_{10}$	$2156 = 2 \times 1078 + 0$	$d = \gcd(1078, 0) = 1078$

Bézout's identity

gcd(a,b) = a*x+b*y for integers x and y

Étienne Bézout
1730-1783

Assuming a and b are both positive integers:

- x and y are necessarily of opposite signs
- given a, b: is there a unique (x,y) pair?
- how to find x and y? Extended Euclidean algorithm

Extended Euclidean algorithm

Formal details: self-study

⌘ Modular arithmetic

NUMBER THEORY BASICS

Part-I

$Z_n = \{0,1,\ldots n\text{-}1\}$

Congruence mod n

- All integers can be represented by the **set of residues** $\{0,1,\ldots n\text{-}1\}$

$0 \equiv k*n \bmod n$, for integer k

$x \equiv k*n+x \bmod n$, for integers k & x

Equivalence class mod n: $\{x, \pm n+x, \pm 2n+x, \ldots \pm kn+x, \ldots\}$

a.k.a. residue class

e.g. mod 9, we have $\{\ldots,-27,-18,-9, 0, 9,18,27,\ldots\}$ represented by 0, $\{\ldots,-26,-17,-8, 1, 10,19,28,\ldots\}$ represented by 1, and so on …

➥ modular arithmetic web demo

Disclaimer

A note on **abuse of notations** in this course

≡ and = used interchangeably

"a mod n = (c+d) mod n"
"a = c+d mod n"
"a ≡ c+d mod n"
"a mod n ≡ (c+d) mod n"

used interchangeably

e.g.
71≡ 50 mod 7
71 mod 7 = 50 mod 7
71 = 50 mod 7

Modular arithmetic properties

$$[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$$
$$[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$$
$$[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$$

Try to prove these relations!

These "simplify" calculations with large numbers …
e.g., exponentiation

Modular arithmetic properties

Property	Expression
Commutative Laws	$(w + x) \bmod n = (x + w) \bmod n$ $(w \times x) \bmod n = (x \times w) \bmod n$
Associative Laws	$[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$ $[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$
Distributive Law	$[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$
Identity Elements	$(0 + w) \bmod n = w \bmod n$ $(1 \times w) \bmod n = w \bmod n$
Additive Inverse $(-w)$	For each $w \in Z_n$, there exists a z such that $w + z \equiv 0 \bmod n$

However

if $(a \times b) \equiv (a \times c) \pmod{n}$ **then** $b \equiv c \pmod{n}$ **if** a is relatively prime to n

So, multiplicative inverse may not exist for all elements in Z_n

Example: Z_8

w	$-w$	w^{-1}
0	Exercise	
1		
2		
3		
4		
5		
6		
7		

Example: Z_8

w	$-w$	w^{-1}
0	0	—
1	7	1
2	6	—
3	5	3
4	4	—
5	3	5
6	2	—
7	1	7

⌘ Groups, rings and fields

NUMBER THEORY BASICS

Part-I

Groups

Denoted as {**G**, •}

- a set of elements: **G**
- with an operator: •

Example

- {Z,+} is a group
- {Z,×} is NOT a group

Satisfying:

(A1) Closure: If a and b belong to G, then $a \bullet b$ is also in G.

(A2) Associativity: $a \bullet (b \bullet c) = (a \bullet b) \bullet c$ for all a, b, c in G.

(A3) Identity element: There is an element e in G such that $a \bullet e = e \bullet a = a$ for all a in G.

(A4) Inverse element: For each a in G, there is an element a' in G such that $a \bullet a' = a' \bullet a = e$.

Groups

Order of a group: number of elements in a group
It can be finite or infinite.

Abelian group

(A5) Commutativity: $a \bullet b = b \bullet a$ for all a, b in G.

Cyclic group

- If $\exists g \in G$, s.t. every element in G is a power of g, i.e. g^k
- g is (called) the **generator** of the group
- exponentiation: repeated application of the group operator
  $a^k = a \bullet a \bullet a \ldots \bullet a$

Rings

Denoted as **{R,+,×}**

- a set of elements: **R**
- with two operators: *addition* + and *multiplication* ×

(A1–A5) R is an abelian group with respect to addition; that is, R satisfies axioms A1 through A5. For the case of an additive group, we denote the identity element as 0 and the inverse of a as $-a$.

(M1) Closure under multiplication: If a and b belong to R, then ab is also in R.

(M2) Associativity of multiplication: $a(bc) = (ab)c$ for all a, b, c in R.

(M3) Distributive laws: $a(b + c) = ab + ac$ for all a, b, c in R.

$(a + b)c = ac + bc$ for all a, b, c in R.

Rings

Commutative ring

(M4) Commutativity of multiplication: $ab = ba$ for all a, b in R.

Integral domain: commutative ring that also satisfies

(M5) Multiplicative identity: There is an element 1 in R such that $a1 = 1a = a$ for all a in R.

(M6) No zero divisors: If a, b in R and $ab = 0$, then either $a = 0$ or $b = 0$.

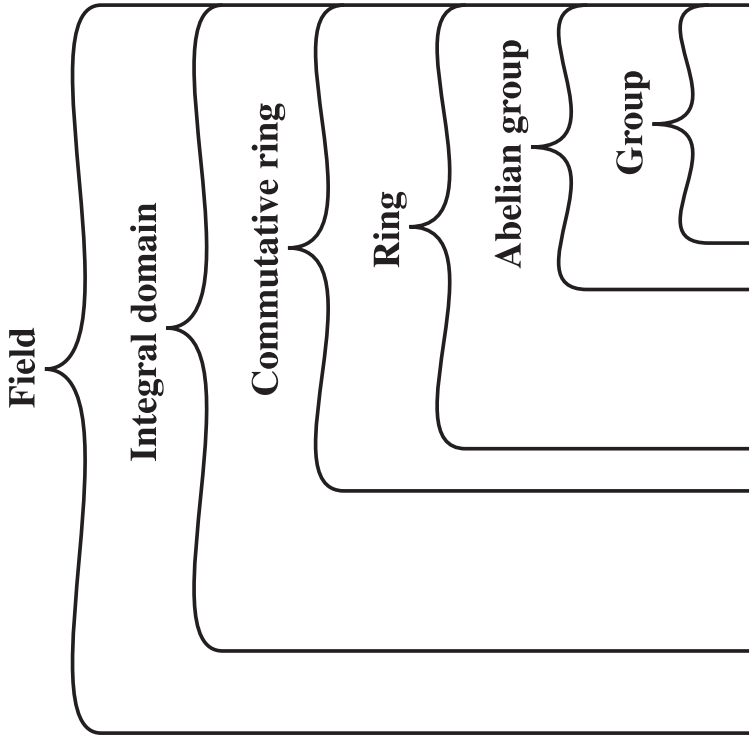
Fields

Denoted as **{F,+,×}**

(A1–M6) F is an integral domain; that is, F satisfies axioms A1 through A5 and M1 through M6.

(M7) Multiplicative inverse: For each a in F, except 0, there is an element a^{-1} in F such that $aa^{-1} = (a^{-1})a = 1$.

Recap



(A1) Closure under addition:	If a and b belong to S, then $a + b$ is also in S
(A2) Associativity of addition:	$a + (b + c) = (a + b) + c$ for all a, b, c in S
(A3) Additive identity:	There is an element 0 in R such that $a + 0 = 0 + a = a$ for all a in S
(A4) Additive inverse:	For each a in S there is an element $-a$ in S such that $a + (-a) = (-a) + a = 0$
(A5) Commutativity of addition:	$a + b = b + a$ for all a, b in S
(M1) Closure under multiplication:	If a and b belong to S, then ab is also in S
(M2) Associativity of multiplication:	$a(bc) = (ab)c$ for all a, b, c in S
(M3) Distributive laws:	$a(b + c) = ab + ac$ for all a, b, c in S $(a + b)c = ac + bc$ for all a, b, c in S
(M4) Commutativity of multiplication:	$ab = ba$ for all a, b in S
(M5) Multiplicative identity:	There is an element 1 in S such that $a1 = 1a = a$ for all a in S
(M6) No zero divisors:	If a, b in S and $ab = 0$, then either $a = 0$ or $b = 0$
(M7) Multiplicative inverse:	If a belongs to S and $a \quad 0$, there is an element a^{-1} in S such that $aa^{-1} = a^{-1}a = 1$

NUMBER THEORY BASICS

Part-I

⌘ Galois fields

Galois (finite) field

Évariste Galois
(1811-1832)

Finite fields of order p: GF(p)

$Z_p=\{0,1,\ldots,p-1\}$ with modulo operations,
where p is a prime number

- recall: Z_p is a multiplicative ring in general
- since p is prime: all non-zero elements are relatively prime
  and *have multiplicative inverse*
  hence, it is a field

Remark: we will look at GF(p^n) later

Galois fields: example

GF(2)

$+$	0	1
0	0	1
1	1	0

Addition

$\times$	0	1
0	0	0
1	0	1

Multiplication

w	$-w$	w^{-1}
0	0	—
1	1	1

Inverses

Galois fields: example

GF(7)

exercise

Addition
Multiplication
and Inverse tables

Galois fields: example

GF(7)

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

(a) Addition modulo 7

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

(b) Multiplication modulo 7

w	$-w$	w^{-1}
0	0	–
1	6	1
2	5	4
3	4	5
4	3	2
5	2	3
6	1	6

Finding multiplicative inverse

$b^{-1} \bmod p$?

exhaustive search? Okay for small p, but …

Exploit ***Bézout's identity***: gcd(p,b)=p*x+b*y

- How? because: **$b^{-1} \bmod p = y$** from the identity
- Why? Exercise!
- How do we find (x and) y? *Extended Euclidean algorithm*

NUMBER THEORY BASICS

Part-I

⌘ polynomial arithmetic

Polynomial arithmetic

Consider a polynomial of **degree n** (integer n ≥ 0)
defined over a set **S** (coefficient set)

$$g(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_o = \sum_{i=0}^{n} a_i x^I$$

$a_i \in S$, $a_n \neq 0$

Polynomial arithmetic

Consider a polynomial of **degree n** (integer n ≥ 0)
defined over a set **S** (coefficient set)

$$g(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_o = \sum_{i=0}^{n} a_i x^I$$

$a_i \in S$, $a_n \neq 0$

Sum/Difference of two polynomials (possibly of different degrees):
term wise sum/difference subject to the properties of S
i.e. coefficient set is a group

$$\sum_{i=0}^{n} a_i x^i \pm \sum_{i=0}^{n} b_i x^i = \sum_{i=0}^{n} (a_i \pm b_i) x^i$$

a_j or b_j are 0 for coefficients > degree of respective polynomials

Polynomial arithmetic

Consider a polynomial of **degree n** (integer n ≥ 0)
defined over a set **S** (coefficient set)

$$g(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_o = \sum_{i=0}^{n} a_i x^I$$

$a_i \in S$, $a_n \neq 0$

Multiplication of two polynomials (possibly of different degrees):

assuming that the coefficient set is a ring

$$\sum_{i=0}^{n} a_i x^i \times \sum_{i=0}^{m} b_i x^i = \sum_{k=0}^{n+m} (a_0 \times b_k + a_1 \times b_{k-1} + \ldots + a_{k-1} \times b_1 + a_k \times b_0) x^k$$

a_j or b_j are 0 for coefficients > degree of respective polynomials

Polynomial arithmetic

Consider a polynomial of **degree n** (integer n ≥ 0)
defined over a set **S** (coefficient set)

$$g(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_o = \sum_{i=0}^{n} a_i x^I$$

$a_i \in S$, $a_n \neq 0$

Division of two polynomials (possibly of different degrees)?

Say: S is the set of integers.
$f(x) = 5x^3$
$g(x) = 4x^2$.

what is f(x)/g(x)?

Polynomial over a field

Division is defined

since the coefficients are elements of a field

polynomial ring: set of such polynomials

Given: polynomials f(x) and g(x) of degrees n and m respectively

with $n \geq m$

we have†: $f(x)=q(x)g(x)+r(x)$

degree of q(x) & r(x)?

†Notion of quotient/remainder/divisibility analogous to what we have seen for integers

Irreducible polynomials

A polynomial f(x) over a field F
which cannot be expressed as
a product of polynomials of lower degrees
- a.k.a prime polynomials

ignoring constant polynomials

Is x^4+1 irreducible over GF(2)?

How about x^3+x+1?

gcd in polynomial ring

Analogous definition as for integers

- (extended) **Euclidean algorithm** is applicable!
- as is **Bézout's identity** (to determine *multiplicative inverse*†)

Exercise: polynomials over GF(2)

$a(x)=x^6+x^5+x^4+x^3+x^2+x+1$

$b(x)=x^4+x^2+x+1$

gcd[a(x),b(x)]?

†Notion still to be discussed in the current context

GF(2^n)?

n-bits to represent 2^n integers

- e.g., cryptographic algorithms use arithmetic operations on integers
- processors use (multiple) byte(s) sized operations

But: Z_{2^n} unsuitable

Z_8

w	$-w$	w^{-1}
0	0	—
1	7	1
2	6	—
3	5	3
4	4	—
5	3	5
6	2	—
7	1	7

unsuitable

Modular polynomial arithmetic

Consider a set of polynomials of **degree n-1** or less, **over Z_p**

Exercise: how many such polynomials exist? Try p=3, n=2

Modular polynomial arithmetic

Consider the set of polynomials of **degree n-1** or less, **over Z_p**

Such a set of polynomials is a finite field: $GF(p^n)$

- Subject to proper definition of + and × operators

Arithmetic of coefficients are modulo p

- i.e. the rules of Z_p are applied

if multiplication yields a polynomial of degree ≥ n

- reduce it modulo an *irreducible polynomial* m(x) of degree n

Modular polynomial arithmetic

Example: polynomials over $GF(2^8)$ †

Given:

- irreducible polynomial $m(x) = x^8+x^4+x^3+x+1$
- $f(x) = x^6+x^4+x^2+x+1$
- $g(x) = x^7+x+1$

Compute:

- $g(x)+f(x)$?
- $g(x)*f(x)$?

†next slide

$GF(2^n)$

Assertion:

- Polynomials modulo an irreducible n^{th}-degree polynomial m(x) forms a finite field

  intuition: analogous argument, as with Z_p being GF(p)

Example: $GF(2^3)$

- Degree three irreducible polynomials instances:
  - $x^3 + x^2 + 1$
  - $x^3 + x + 1$ ☚ lets use this

Multiplication in $GF(2^3)$

Polynomial arithmetic modulo $x^3 + x + 1$

	×	000 0	001 1	010 x	011 $x + 1$	100 x^2	101 $x^2 + 1$	110 $x^2 + x$	111 $x^2 + x + 1$
000	0								
001	1								
010	x								
011	$x + 1$								
100	x^2								
101	$x^2 + 1$								
110	$x^2 + x$								
111	$x^2 + x + 1$								

Exercise

Multiplication in $GF(2^3)$

Polynomial arithmetic modulo $x^3 + x + 1$

	×	000 0	001 1	010 x	011 $x + 1$	100 x^2	101 $x^2 + 1$	110 $x^2 + x$	111 $x^2 + x + 1$
000	0	0	0	0	0	0	0	0	0
001	1	0	1	x	$x + 1$	x^2	$x^2 + 1$	$x^2 + x$	$x^2 + x + 1$
010	x	0	x	x^2	$x^2 + x$	$x + 1$	1	$x^2 + x + 1$	$x^2 + 1$
011	$x + 1$	0	$x + 1$	$x^2 + x$	$x^2 + 1$	$x^2 + x + 1$	x^2	1	x
100	x^2	0	x^2	$x + 1$	$x^2 + x + 1$	$x^2 + x$	x	$x^2 + 1$	1
101	$x^2 + 1$	0	$x^2 + 1$	1	x^2	x	$x^2 + x + 1$	$x + 1$	$x^2 + x$
110	$x^2 + x$	0	$x^2 + x$	$x^2 + x + 1$	1	$x^2 + 1$	$x + 1$	x	x^2
111	$x^2 + x + 1$	0	$x^2 + x + 1$	$x^2 + 1$	x	1	$x^2 + 1$	x^2	$x + 1$

	×	000 0	001 1	010 2	011 3	100 4	101 5	110 6	111 7
000	0	0	0	0	0	0	0	0	0
001	1	0	1	2	3	4	5	6	7
010	2	0	2	4	6	3	1	7	5
011	3	0	3	6	5	7	4	1	2
100	4	0	4	3	7	6	2	5	1
101	5	0	5	1	4	2	7	3	6
110	6	0	6	7	1	5	3	2	4
111	7	0	7	5	2	1	6	4	3

Alternate representation of GF(2^n)

Generator of a finite field F of order q

- an element g whose q-1 first powers generate all non-zero elements of F

Root of polynomial m(x)

- an element r s.t. m(r)=0
- if the root g of an irreducible polynomial is a *generator of the finite field* defined on that polynomial, then we call it a primitive root

Alternate representation of GF(2^n)

Example GF(2^3) with polynomial $x^3 + x + 1$

Consider the root g of the polynomial $m(x)=x^3 + x + 1$

- we have: $m(g) = g^3 + g + 1 = 0$

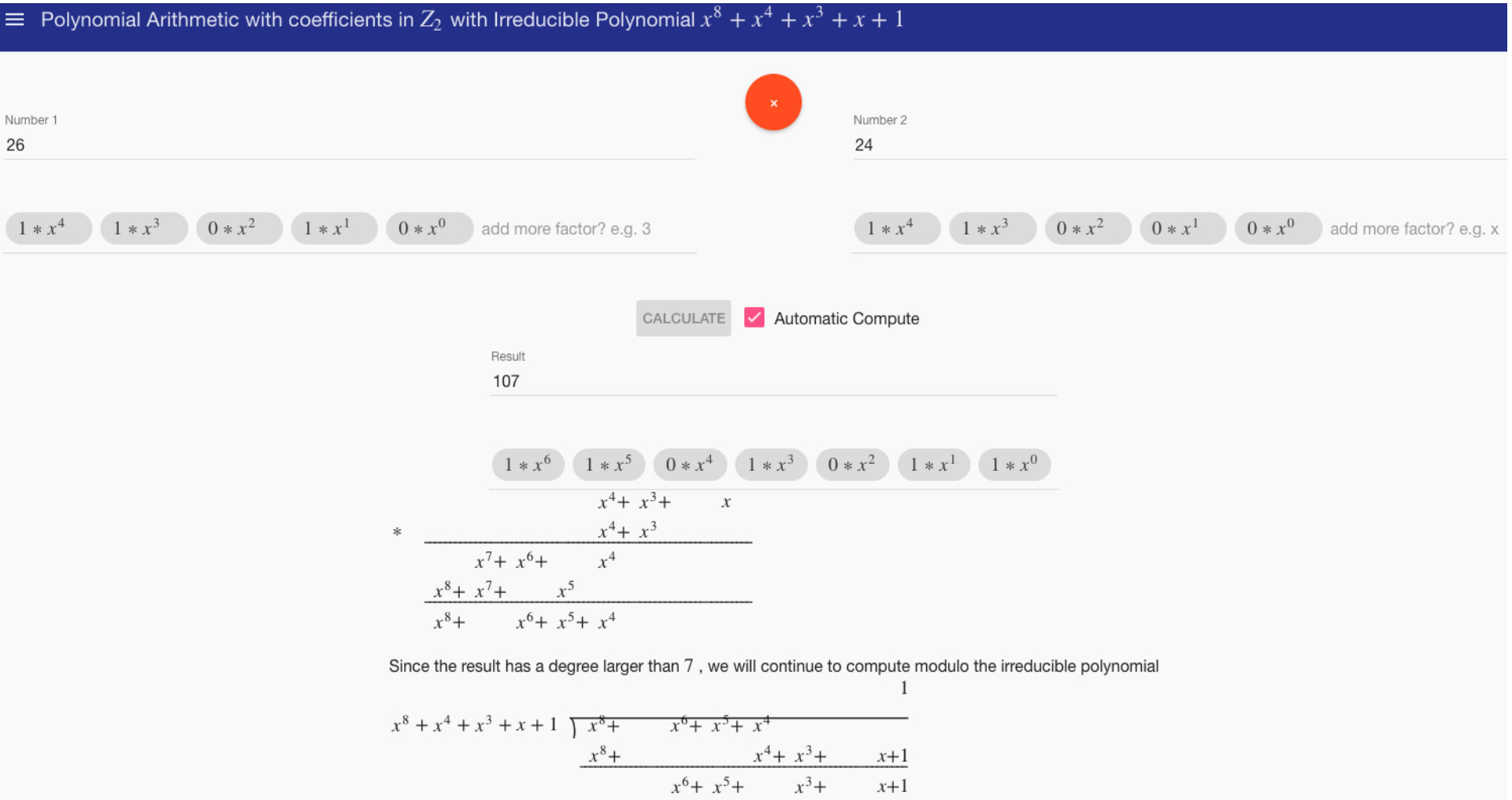
$\Rightarrow g^3 = g + 1$

Compute:

- $g^4, g^5, g^6, g^7, g^8, g^9$

Web demo

➥ polynomial arithmetic web demo



So far …

- Euclidean algorithm and Bézout's identity
- Modular arithmetic
- Groups, rings and fields
- Galois fields and polynomial arithmetic

NUMBER THEORY

BASICS

Part-I

Next …

- Fermat and Euler's theorem
- Primality (Miller-Rabin) test
- Chinese remainder theorem
- Discrete logarithm

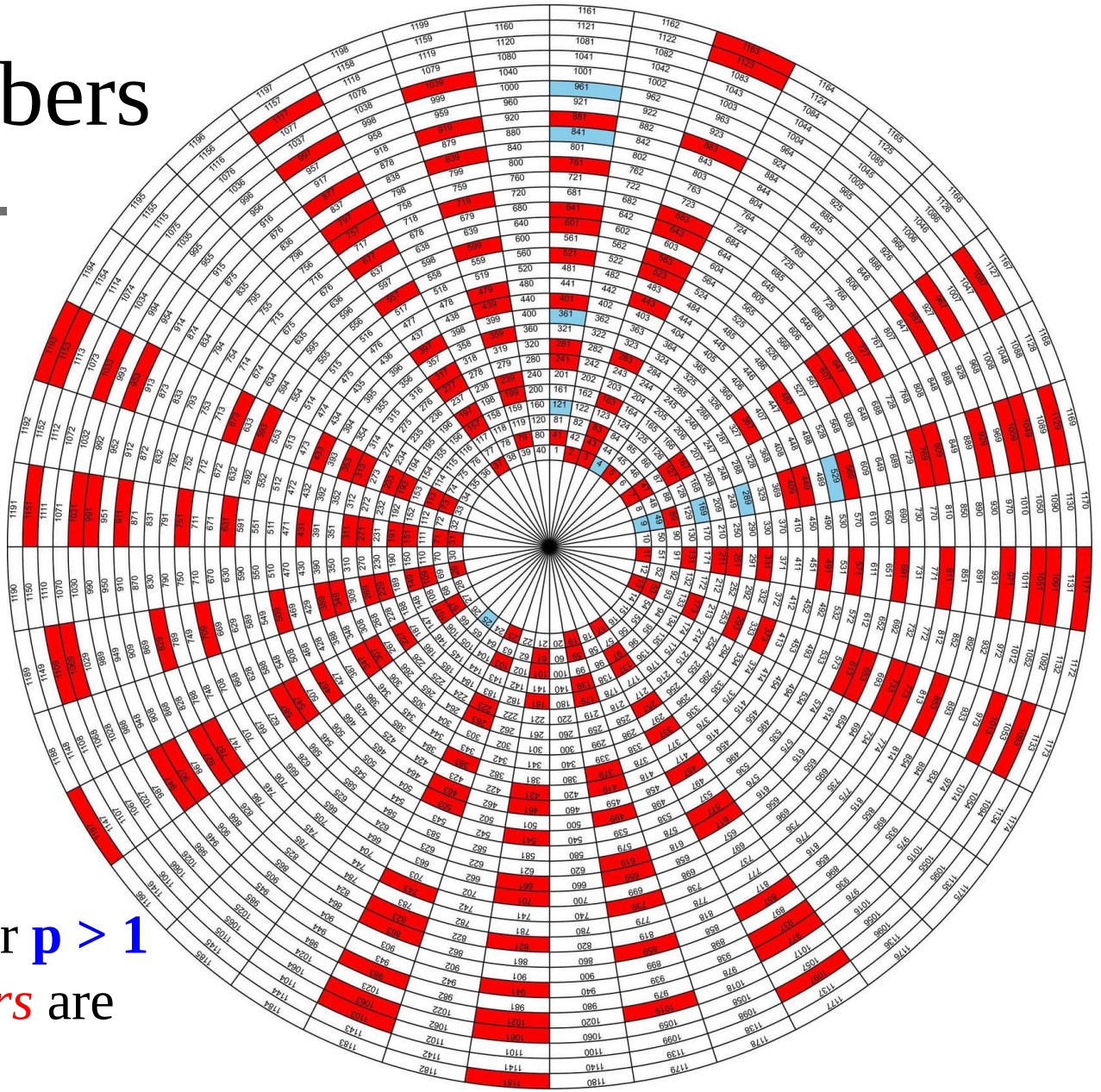
NUMBER THEORY

BASICS

Part-II

Prime numbers

Revisited



Definition:

- A positive integer **p > 1** ***iff*** its *only divisors* are ±1 and ±p

Any integer

Represented as a product of its prime factors

- Any positive **integer *a*** can be expressed as

$$a = \prod_{p \in P} p^{a_p}$$

with $a_p \geq 0$

where ***P*** is the set of prime numbers

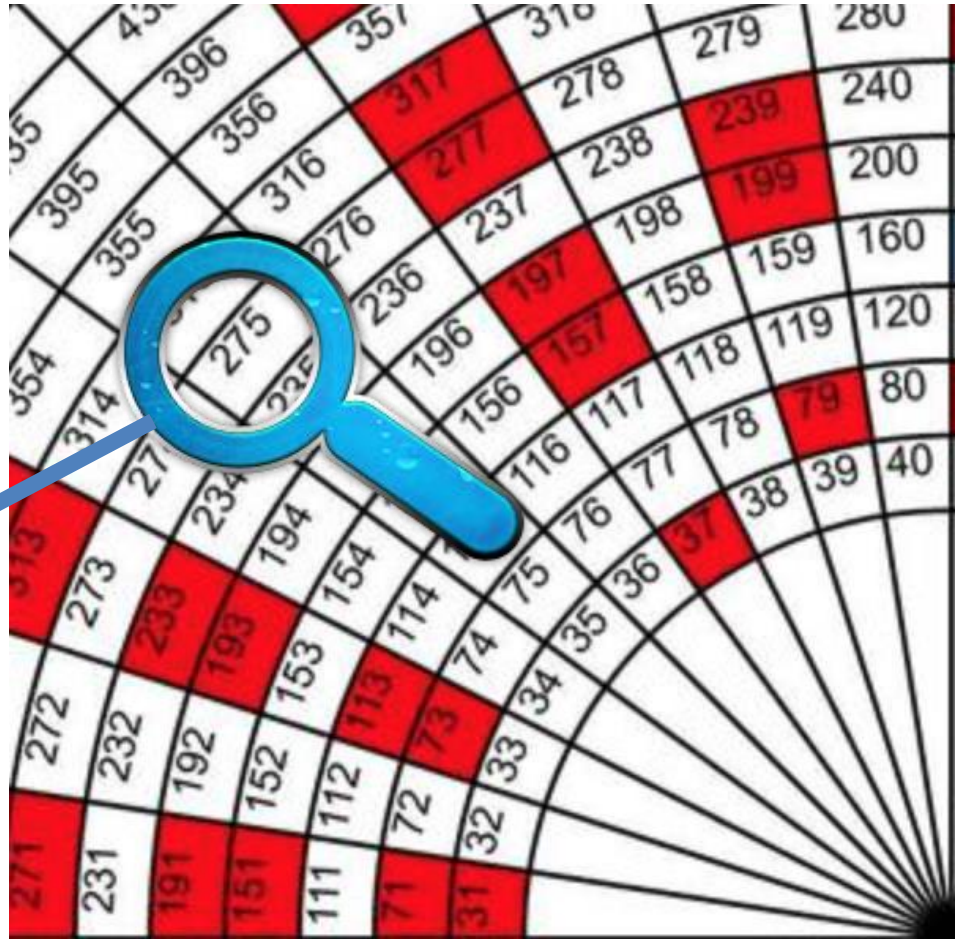
Any integer

Represented as a product of its prime factors

$$a = \prod_{p \in P} p^{a_p}$$

with $a_p \geq 0$

where P is the set of prime numbers



e.g.

$275 = 2^0 \cdot 3^0 \cdot 5^2 \cdot 7^0 \cdot 11^1 \cdot 13^0 \ldots$

Some simple observations

Multiplication of integers

Given:

$$a = \prod_{p \in P} p^{a_p} \quad \text{and} \quad b = \prod_{p \in P} p^{b_p}$$

We have, for the product:

$$k = a \times b = \prod_{p \in P} p^{k_p}$$

With:

$$k_p = a_p + b_p \; \forall p \in P$$

Some simple observations

Multiplication of integers

Example:

$275 = 2^0 \cdot 3^0 \cdot 5^2 \cdot 7^0 \cdot 11^1 \cdot 13^0 \ldots$

$1170 = 2^1 \cdot 3^2 \cdot 5^1 \cdot 7^0 \cdot 11^0 \cdot 13^1 \ldots$

275×1170

$= 2^1 \cdot 3^2 \cdot 5^3 \cdot 7^0 \cdot 11^1 \cdot 13^1 \ldots$

$= 321750$

Given:

$$a = \prod_{p \in P} p^{a_p} \quad \text{and} \quad b = \prod_{p \in P} p^{b_p}$$

We have, for the product:

$$k = a \times b = \prod_{p \in P} p^{k_p}$$

With:

$$k_p = a_p + b_p \ \forall p \in P$$

Some simple observations

Divisibility and gcd

Given:

$$a = \prod_{p \in P} p^{a_p} \quad \text{and} \quad b = \prod_{p \in P} p^{b_p}$$

If $a|b$, ***then:*** $a_p \leq b_p$ **for each *p***

Likewise:

If $k=\gcd(a,b)$, **then:** $k_p = \min(a_p, b_p)$ **for each *p***

Some simple observations

Divisibility and gcd

Example:

$275 = 2^0 \cdot 3^0 \cdot 5^2 \cdot 7^0 \cdot 11^1 \cdot 13^0 \ldots$

$1170 = 2^1 \cdot 3^2 \cdot 5^1 \cdot 7^0 \cdot 11^0 \cdot 13^1 \ldots$

$\gcd(275,1170)$
$= 2^0 \cdot 3^0 \cdot 5^1 \cdot 7^0 \cdot 11^0 \cdot 13^0 \ldots$
$= 5$

Given:

$$a = \prod_{p \in P} p^{a_p} \quad \text{and} \quad b = \prod_{p \in P} p^{b_p}$$

If $a|b$, *then:* $a_p \leq b_p$ **for each** p

Likewise:

If $k=\gcd(a,b)$, then: $k_p = \min(a_p, b_p)$ **for each** p

Fermat's (little) theorem

Not to be confused with Fermat's Last Theorem

If:

- A **prime number *p***
- A **positive integer *a*** not divisible by ***p***

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

Proof: **Exercise!**

Pierre de Fermat
1607-1665

Note: The converse of the statement is however false!

Euler's theorem

Generalization of Fermat's theorem

For any *integers* ***a*** and ***n*** that are
***relatively* prime**

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

Proof: Similar to Fermat's theorem (self-study)

Leonhard Euler
1707-1783

With, **Euler's totient function ϕ(n):**

- number of positive integers
  less than *n* and **relatively prime with *n***
- Convention: $\phi(1)=1$
- **Examples:** $\phi(19)$=??
  $\phi(20)$=??

Euler's totient function: $\phi(n)$

$\phi(1)=1$	convention
$\phi(p)=p-1$	if p is prime
$\phi(m\times n)=\phi(m)\times\phi(n)$	if m and n are relatively prime
$\phi(p^e)=p^e-p^{e-1}$	if p is prime

We can combine the above four rules to find the value of $\phi(n)$. For example, if n can be factored as

$$n = p_1^{e_1} \times p_2^{e_2} \times \ldots \times p_k^{e_k}$$

then we combine the third and the fourth rule to find

$$\phi(n) = (p_1^{e_1} - p_1^{e_1-1}) \times (p_2^{e_2} - p_2^{e_2-1}) \times \ldots \times (p_k^{e_k} - p_k^{e_k-1})$$

⌘ Primality (Miller-Rabin) test

NUMBER THEORY BASICS

Part-II

How to find primes at large?

The AKS primality test

Deterministic: Primes is in P (2004)

Manindra **Agrawal**

Neeraj **Kayal**

Nitin **Saxena**

Algorithm	trials	time
Rabin-Miller	1	0.003 sec
Rabin-Miller	10	0.03 sec
Rabin-Miller	100	0.3 sec
ECPP		2.0 sec
AKS		37 weeks (est)

$10^{100} + 267$

impractical!

e.g. source: “Primality testing” by Richard P. Brent

Miller-Rabin primality test

Probabilistic algorithm

Garry Lee **Miller**

Michael Oser **Rabin**

Miller-Rabin primality test

Background

Property 1:

- If a is a positive integer, and p is a prime:

$a^2 \bmod p = 1$ iff:

$a \bmod p = 1$

OR

$a \bmod p = p-1 \ (\equiv -1)$

Miller-Rabin primality test

Background

Property 2:

- **IF** ***a*** (**<** ***p***) is a positive integer, where ***p*** (> 2) is a prime:

  For some integer ***k***, and odd integer ***q***, $\boldsymbol{p-1 = 2^k q}$

  THEN One of the following holds:

$$a^q = 1 \pmod{p}$$

$$\exists j \in \{1, 2, ..., k\}, a^{2^{j-1}q} \equiv -1 \pmod{p}$$

Miller-Rabin primality test: Idea

If the candidate number ***n*** is prime, then property 2 would hold, so:

- If property 2 does NOT hold: **n is NOT prime** (certainly)
- If it holds: **we cannot conclude anything**

so?

Miller-Rabin primality test: Idea

If the candidate number ***n*** is prime, then property 2 would hold, so:

- If property 2 does NOT hold: **n is NOT prime** (certainly)
- If it holds: **we cannot conclude anything**

If ***n*** is actually not prime, then for any random $1<a<n-1$:

- Output is inconclusive with a probability less than 0.25
  (proof of assertion beyond the scope of this course)
- Heuristic: **Repeat the test** with multiple choices of ***a***

Miller-Rabin primality test: Algorithm

```
TEST (n)
1. Find integers k, q, with k > 0, q odd, so that
   (n − 1 = 2^k q);
2. Select a random integer a, 1 < a < n − 1;
3. if a^q mod n = 1 then return("inconclusive");
4. for j = 0 to k − 1 do
5. if a^(2^j q) mod n = n − 1 then return("inconclusive");
6. return("composite");
```

If ***n*** is actually not prime, then for any random 1<***a***<***n***-1:

- Output is inconclusive with a probability less than 0.25
  (proof of assertion beyond the scope of this course)
- Heuristic: **Repeat the test** with multiple choices of ***a***

Miller-Rabin primality test: Algorithm

Example: n=57

```
TEST (n)
1. Find integers k, q, with k > 0, q odd, so that
   (n − 1 = 2^k q);
2. Select a random integer a, 1 < a < n − 1;
3. if a^q mod n = 1 then return("inconclusive");
4. for j = 0 to k − 1 do
5. if a^(2^j q) mod n = n − 1 then return("inconclusive");
6. return("composite");
```

n-1=56=$2^3 \times 7$. So, we have k=3,q=7

Miller-Rabin primality test: Algorithm

Example: n=57

```
TEST (n)
1. Find integers k, q, with k > 0, q odd, so that
   (n − 1 = 2^k q);
2. Select a random integer a, 1 < a < n − 1;
3. if a^q mod n = 1 then return("inconclusive");
4. for j = 0 to k − 1 do
5. if a^(2^j q) mod n = n − 1 then return("inconclusive");
6. return("composite");
```

n-1=56=$2^3 \times 7$. So, we have k=3,q=7

Let's select a random a such that 1<a<n-1, say a=3

Miller-Rabin primality test: Algorithm

Example: n=57

```
TEST (n)
1. Find integers k, q, with k > 0, q odd, so that
   (n − 1 = 2^k q);
2. Select a random integer a, 1 < a < n − 1;
3. if a^q mod n = 1 then return("inconclusive");
4. for j = 0 to k − 1 do
5. if a^(2^j q) mod n = n − 1 then return("inconclusive");
6. return("composite");
```

n-1=56=$2^3 \times 7$. So, we have k=3,q=7

Let's select a random a such that 1<a<n-1, say a=3

Compute 3^7 mod 57=21 ($\neq 1$)

Miller-Rabin primality test: Algorithm

Example: n=57

```
TEST (n)
1. Find integers k, q, with k > 0, q odd, so that
   (n − 1 = 2^k q);
2. Select a random integer a, 1 < a < n − 1;
3. if a^q mod n = 1 then return("inconclusive");
4. for j = 0 to k − 1 do
5. if a^(2^j q) mod n = n − 1 then return("inconclusive");
6. return("composite");
```

n-1=56=$2^3 \times 7$. So, we have k=3,q=7

Let's select a random a such that 1<a<n-1, say a=3

Compute 3^7 mod 57=21 (≠1)

(may) have to compute **for j=0 to 2**

j=0 Compute 3^7 mod 57=21 (≠57-1)

Miller-Rabin primality test: Algorithm

Example: n=57

```
TEST (n)
1. Find integers k, q, with k > 0, q odd, so that
   (n − 1 = 2^k q);
2. Select a random integer a, 1 < a < n − 1;
3. if a^q mod n = 1 then return("inconclusive");
4. for j = 0 to k − 1 do
5. if a^(2^j q) mod n = n − 1 then return("inconclusive");
6. return("composite");
```

n-1=56=$2^3 \times 7$. So, we have k=3,q=7

Let's select a random a such that 1<a<n-1, say a=3

Compute 3^7 mod 57=21 (≠1)

(may) have to compute **for j=0 to 2**

j=1

Compute 3^7 mod 57=21 (≠57-1)

3^{14} mod 57=42 (≠57-1)

Miller-Rabin primality test: Algorithm

Example: n=57

```
TEST (n)
1. Find integers k, q, with k > 0, q odd, so that
   (n − 1 = 2^k q);
2. Select a random integer a, 1 < a < n − 1;
3. if a^q mod n = 1 then return("inconclusive");
4. for j = 0 to k − 1 do
5. if a^(2^j q) mod n = n − 1 then return("inconclusive");
6. return("composite");
```

n-1=56=$2^3 \times 7$. So, we have k=3,q=7

Let's select a random a such that 1<a<n-1, say a=3

Compute 3^7 mod 57=21 (≠1)

(may) have to compute **for j=0 to 2**

j=2

Compute 3^7 mod 57=21 (≠57-1)

3^{14} mod 57=42 (≠57-1)

3^{28} mod 57=54 (≠57-1)

Miller-Rabin primality test: Algorithm

Example: n=57

```
TEST (n)
1. Find integers k, q, with k > 0, q odd, so that
   (n − 1 = 2^k q);
2. Select a random integer a, 1 < a < n − 1;
3. if a^q mod n = 1 then return("inconclusive");
4. for j = 0 to k − 1 do
5. if a^(2^j q) mod n = n − 1 then return("inconclusive");
6. return("composite");
```

n-1=56=$2^3 \times 7$. So, we have k=3,q=7

Let's select a random a such that 1<a<n-1, say a=3

Compute 3^7 mod 57=21 (≠1)

computed **for j=0 to 2**

Compute 3^7 mod 57=21 (≠57-1)

3^{14} mod 57=42 (≠57-1)

3^{28} mod 57=54 (≠57-1)

Conclude with ***certainty*** that

57 is COMPOSITE

Miller-Rabin primality test: Algorithm

Example: n=61

```
TEST (n)
1. Find integers k, q, with k > 0, q odd, so that
   (n − 1 = 2^k q);
2. Select a random integer a, 1 < a < n − 1;
3. if a^q mod n = 1 then return("inconclusive");
4. for j = 0 to k − 1 do
5. if a^(2^j q) mod n = n − 1 then return("inconclusive");
6. return("composite");
```

n-1=60=$2^2 \times 15$. So, we have k=2,q=15

Miller-Rabin primality test: Algorithm

Example: n=61

```
TEST (n)
1. Find integers k, q, with k > 0, q odd, so that
   (n − 1 = 2^k q);
2. Select a random integer a, 1 < a < n − 1;
3. if a^q mod n = 1 then return("inconclusive");
4. for j = 0 to k − 1 do
5. if a^(2^j q) mod n = n − 1 then return("inconclusive");
6. return("composite");
```

n-1=60=$2^2 \times 15$. So, we have k=2,q=15

Let's select a random a such that 1<a<n-1, say a=3

Miller-Rabin primality test: Algorithm

Example: n=61

```
TEST (n)
1. Find integers k, q, with k > 0, q odd, so that
   (n − 1 = 2^k q);
2. Select a random integer a, 1 < a < n − 1;
3. if a^q mod n = 1 then return("inconclusive");
4. for j = 0 to k − 1 do
5. if a^(2^j q) mod n = n − 1 then return("inconclusive");
6. return("composite");
```

n-1=60=$2^2 \times 15$. So, we have k=2,q=15

Let's select a random a such that 1<a<n-1, say a=3

Compute 3^{15} mod 61=60 ($\neq 1$)

Miller-Rabin primality test: Algorithm

Example: n=61

```
TEST (n)
1. Find integers k, q, with k > 0, q odd, so that
   (n − 1 = 2^k q);
2. Select a random integer a, 1 < a < n − 1;
3. if a^q mod n = 1 then return("inconclusive");
4. for j = 0 to k − 1 do
5. if a^(2^j q) mod n = n − 1 then return("inconclusive");
6. return("composite");
```

How useful is that?

n-1=60=$2^2 \times 15$. So, we have k=2,q=15

Let's select a random a such that 1<a<n-1, say a=3

Compute 3^{15} mod 61=60 (≠1)

j=0 Compute 3^{15} mod 61=60 (=61-1)

(may) have to compute **for j=0 to 1**

Condition already satisfied, so return

INCONCLUSIVE

- Chinese remainder theorem

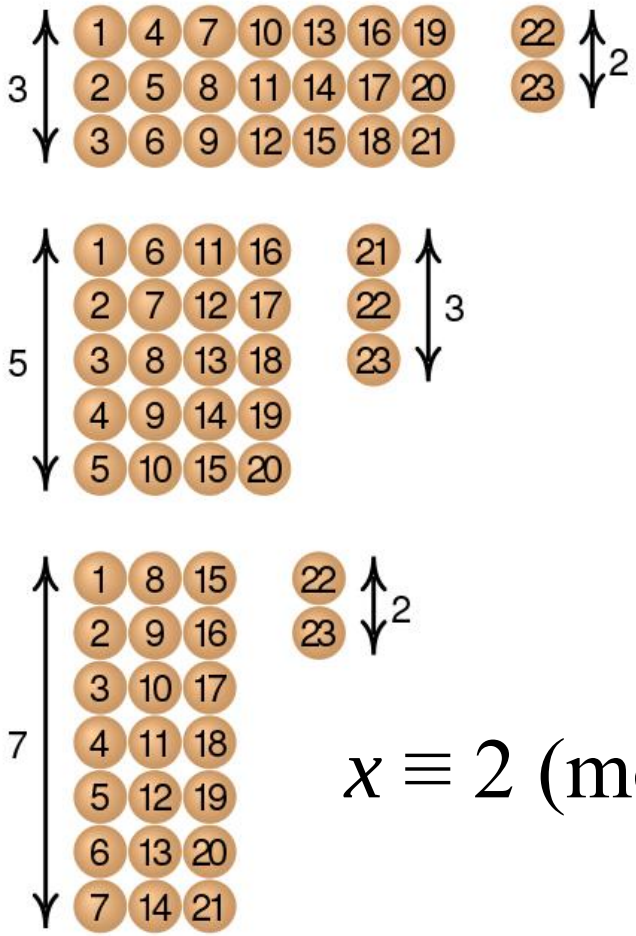
NUMBER THEORY BASICS

Part-II

There are certain things whose number is unknown. If we **count them by threes, we have two left over; by fives, we have three left over; and by sevens, two are left over**. How many things are there?

- 3rd-century book Sunzi Suanjing by the Chinese mathematician Sunzi

$$x \equiv 2 \pmod 3 \equiv 3 \pmod 5 \equiv 2 \pmod 7$$



It is possible to reconstruct integers in a certain range from their residues modulo a set of pairwise relatively prime moduli.

$$x \equiv 2 \pmod 3 \equiv 3 \pmod 5 \equiv 2 \pmod 7$$

$$x = 23 + 105k \text{ where } k \in Z$$

Image source: https://en.wikipedia.org/wiki/Chinese_remainder_theorem

Chinese Remainder Theorem

Consider:

$$M = \prod_{i=1}^{k} m_i$$

where m_i are pairwise relatively prime
i.e. $\gcd(m_i, m_j) = 1$ if $i \neq j$

Any integer $A \in Z_M$ can be represented by a *k-tuple*

$A \leftrightarrow (a_1, a_2, \ldots, a_k)$, where:

$$a_i \in Z_{m_i}$$

$$a_i = A \bmod m_i$$

Chinese Remainder Theorem

Assertion 1:

The ***mapping*** $A \leftrightarrow (a_1, a_2, \ldots, a_k)$, where:

$$a_i \in Z_{m_i}$$
$$a_i = A \bmod m_i$$

is a ***one-to-one correspondence (bijection)*** between

$$Z_M \leftrightarrow Z_{m_1} \times Z_{m_2} \times \ldots \times Z_{m_k}$$

Chinese Remainder Theorem

Assertion 1: proof sketch

$A \rightarrow (a_1, a_2, \ldots, a_k)$

Given A, the ***mapping*** $(a_1, a_2, \ldots, a_k)$ is by definition unique

$$a_i = A \bmod m_i$$

Chinese Remainder Theorem

Assertion 1: proof sketch

$A \leftarrow (a_1, a_2, \ldots, a_k)$

Given $(a_1, a_2, \ldots, a_k)$, we can show that A can be computed as follows:

Define: $M_i = M/m_i$ (note: $= m_1 \times m_1 \times \ldots m_{i-1} \times m_{i+1} \ldots m_k$) for $1 \le i \le k$

Let $c_i = M_i \times (M_i^{-1} \bmod m_i)$ for $1 \le i \le k$

Note: $c_j \equiv M_j \equiv 0 \bmod m_i$ if $j \neq i$

Then: $$A \equiv \left(\sum_{i=1}^{k} a_i c_i \right) (mod\ M)$$

Why?

Chinese Remainder Theorem

Assertion 1: example

Consider $M=10=2\times5$

So: $m_1=2, m_2=5 \Rightarrow M_1=10/2=5, M_2=210/5=2$

$c_1= 5 \times (5^{-1} \bmod 2) = 5\times1=5$

$c_2= 2 \times (2^{-1} \bmod 5) = 2\times3 =6$

Consider $A=8$, then we have $8 \leftrightarrow (0,3)$, i.e. $a_1=0, a_2=3$

$$\sum_i a_i c_i \pmod{M} = 0 \times 5 + 3 \times 6 \pmod{10} = 8$$

Chinese Remainder Theorem

Assertion 2: this property is used in RSA public key cryptography

Operations performed on the elements of Z_M can be equivalently performed on the corresponding k-tuples by performing the operation independently in each coordinate position in the appropriate system.

$$(A + B) \bmod M \leftrightarrow ((a_1 + b_1) \bmod m_1, \ldots, (a_k + b_k) \bmod m_k)$$

$$(A - B) \bmod M \leftrightarrow ((a_1 - b_1) \bmod m_1, \ldots, (a_k - b_k) \bmod m_k)$$

$$(A \times B) \bmod M \leftrightarrow ((a_1 \times b_1) \bmod m_1, \ldots, (a_k \times b_k) \bmod m_k)$$

NUMBER THEORY BASICS

Part-II

- Discrete logarithm

Primitive root

Recall Euler's theorem:

For any *integers* ***a*** and ***n*** that are ***relatively* prime**

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

Consider a **more general statement:**

$$\exists m \in \{1, 2, ..., n-1\}, a^m \equiv 1 \pmod{n}$$

- The **smallest value of *m*** satisfying the property is called the **order of *a* (mod *n*)**
- If the **order of an element $x \in Zn$ is $\phi(n)$** then we call the element ***x*** **a primitive root of *n***

Primitive root

Example with Z_{19}

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1
6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1
8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1
9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1
10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1
12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1
13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	6	8	17	10	7	3	5	1	14	9	7	13	9	12	16	15	1
15	16	12	9	2	11	13	5	18	14	6	7	8	7	8	6	14	1
16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1
17	4	11	16	6	7	5	9	18	8	17	11	16	6	7	5	9	1
18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1

There are six primitive roots, namely 2, 3, 10, 13, 14 & 15.

Notice that elements of lower orders create periodic sequences

Primitive root

- If ***x*** is a primitive root in Z_n then $x^1, x^2, \ldots, x^{\phi(n)}$ are distinct

- For a prime ***p***, if ***x*** is a primitive root in Z_p then

$$x^1, x^2, \ldots, x^{p-1}$$

are all the non-zero elements in Z_p
(but not necessarily in an order)

Logarithm

- Inverse of exponentiation: $y=x^m \Rightarrow \log_x(y)=m$

  $\log_x(1) = 0$

  $\log_x(x) = 1$

  $\log_x(yz) = \log_x(y)+\log_x(z)$

  $\log_x(y^r) = r\times\log_x(y)$

- Discrete logarithm: *Logarithm in modular arithmetic*

  It has an analogous interpretation (inverse of exponentiation) as with logarithms for real numbers

Discrete logarithm

- Consider a primitive root $a \in Z_p$ for some prime p

For any non-zero integer b, we can find a unique i, $0 \leq i \leq p-1$ with: $b \equiv a^i \pmod{p}$

Why unique?

This exponent i is the ***discrete logarithm*** of the number b for the base a, mod p

Denoted as: $\mathbf{dlog_{a,p}(b)}$

Discrete logarithm: properties

- Analogous to logarithm for real numbers

$\text{dlog}_{a,p}(1) = 0$ [because $a^0 \bmod p = 1 \bmod p = 1$]

$\text{dlog}_{a,p}(a) = 1$ [because $a^1 \bmod p = a$]

$\text{dlog}_{a,p}(xy) = [\text{dlog}_{a,p}(x) + \text{dlog}_{a,p}(y)] \pmod{\phi(p)}$

$\text{dlog}_{a,p}(y^r) = [r \times \text{dlog}_{a,p}(y)] \pmod{\phi(p)}$

Follows from Euler's theorem†

† Refer to the Stallings textbook for details of the derivation

Discrete logarithm: example

- Discrete logarithm to the **base 2, mod 19**

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$log_{2,19}(a)$	18	1	13	2	16	14	6	3	8	17	12	15	5	7	11	4	10	9

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	[illegible]	10	1
3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1
6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1
8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1
9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1
10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1
12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1
13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1
17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1
18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1

Discrete logarithm: example

- **Exercise:** Discrete logarithm to the **base 10, mod 19**

$\mathbf{dlog_{10,19}(7) = ???}$

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1
6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1
8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1
9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1
10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1
12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1
13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1
17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1
18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1

Discrete logarithm: example

- **Exercise:** Discrete logarithm to the **base 10, mod 19**

$\mathbf{dlog_{10,19}(7) = ???}$

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1
6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1
8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1
9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1
10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1
12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1
13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1
17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1
18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1

What we have learned so far

NUMBER THEORY BASICS

- Properties of prime numbers and their exploitation
- Modular arithmetic
- Finite fields
- Discrete logarithms